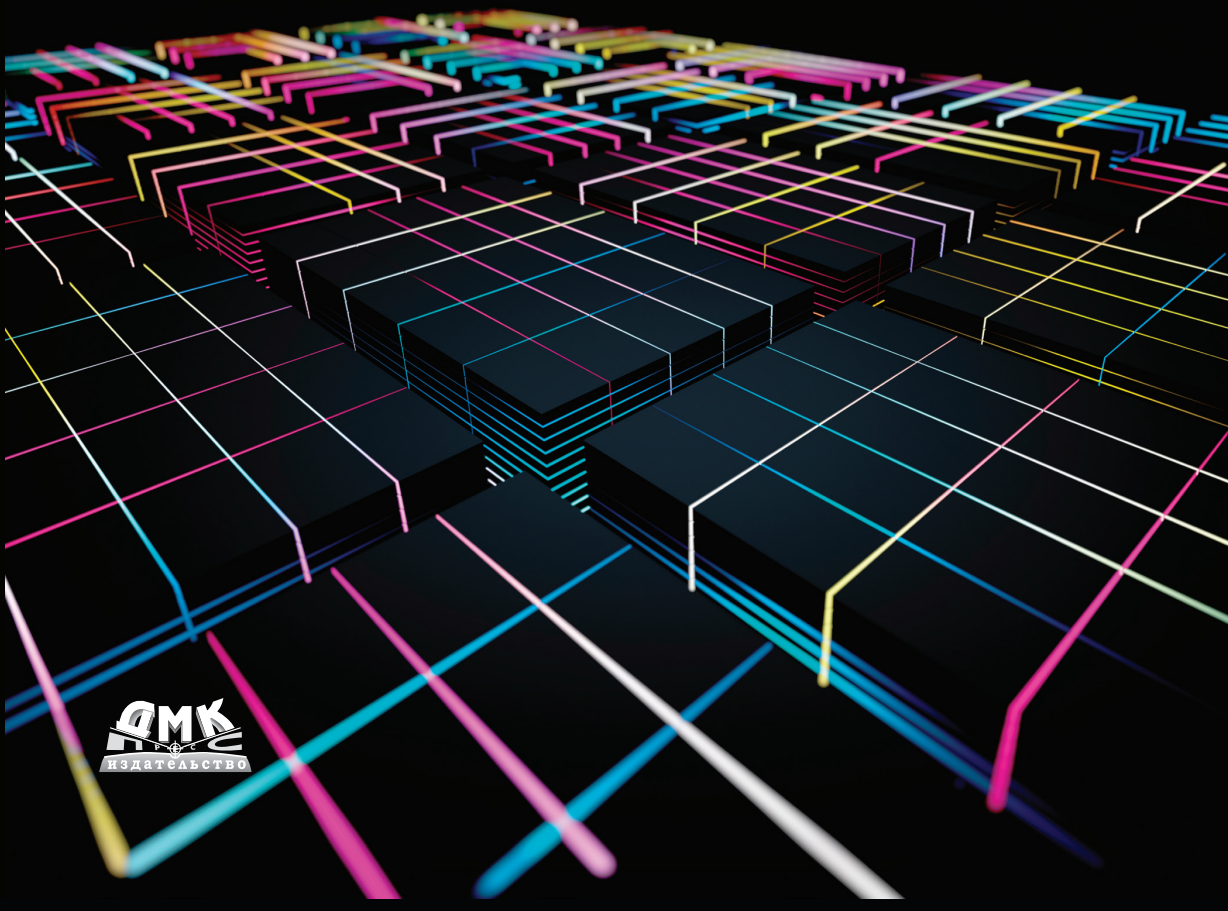
Апокалипсис криптографии

Подготовка к квантовому прорыву

Роджер А. Граймс



Роджер А. Граймс

Апокалипсис криптографии

Cryptography Apocalypse

Preparing for the Day When Quantum Computing Breaks Today's Crypto

Roger A. Grimes

WILEY

Апокалипсис криптографии

Подготовка криптографии к квантовым вычислениям

Роджер А. Граймс

ДМК Пресс
издательство
Москва, 2020

УДК 004.382
ББК 32.973-018
Г75

Граймс Р. А.
Г75 Апокалипсис криптографии / пер. с англ. В. А. Яроцкого. – М.: ДМК Пресс, 2020. – 290 с.: ил.

ISBN 978-5-97060-837-1

В связи с бурным развитием технологий требования к компьютерной безопасности постоянно изменяются. Шифры, которые на сегодняшний день можно считать надежными, при использовании квантового компьютера будет легко взломать, и эта реальность уже не за горами. Вот почему необходимо уже сейчас готовиться к квантовому криптографическому прорыву, и эта книга послужит для читателя бесценным руководством к действию.

Автор, известный специалист по компьютерной безопасности, показывает, какие приложения могут оказаться самыми уязвимыми перед квантовыми вычислениями, как лучше использовать современные технологии шифрования и как внедрить новую постквантовую криптографию для обеспечения безопасности пользователей, данных и инфраструктуры.

Издание адресовано работникам служб информационной безопасности, которые принимают во внимание угрозы, возникающие с появлением квантовых вычислений, и планируют защитить свои организации от взломов информационных систем.

УДК 004.382
ББК 32.973-018

ISBN 978-1-119-61819-5 (англ.)
ISBN 978-5-97060-837-1 (рус.)

Я посвящаю эту книгу моей жене Трише,
женщине замужем в полном смысле этого слова

Краткое содержание

Содержание

Об авторе

Роджер А. Граймс борется с хакерами более трех десятилетий (с 1987 года). Он получил десятки компьютерных сертификатов (включая CISSP, CISA, MCSE, CEH и Security+) и даже сдал очень жесткий экзамен на сертифицированного общественного бухгалтера (Certified Public Accountant, CPA), хотя это не имеет никакого отношения к компьютерной безопасности, и он худший из когда-либо существовавших бухгалтеров. Ему платили как профессиональному тестировщику компьютерной безопасности компаний и их веб-сайтов более 20 лет, и процесс тестирования никогда не занимал у него более трех часов. Он создал и обновил классы компьютерной безопасности, был инструктором и учил тысячи студентов, как взламывать или защищать криптокоды. Роджер – частый докладчик на национальных конференциях по компьютерной безопасности. Он написал сам и в соавторстве десять книг по компьютерной безопасности и более тысячи журнальных статей. С августа 2005 года ведет колонку обозревателя компьютерной безопасности в журналах InfoWorld и CSO (www.infoworld.com/blog/security-adviser/) и более двух десятилетий работает консультантом по компьютерной безопасности. Роджер часто дает интервью в журнальной прессе, на радио и телевидении (в том числе для журнала Newsweek и программы All Things Considered на радиостанции NPR). В настоящее время он консультирует большие и малые компании по всему миру, объясняя, как остановить злоумышленников и вредоносные программы в кратчайшие сроки и наиболее эффективным способом. Он следит за литературой и изучает квантовую физику с 1983 года.

Вы можете связаться с Роджером и подробнее узнать о его деятельности:

- E-mail: roger@banneretcs.com
- LinkedIn: www.linkedin.com/in/rogeragrimes/
- Twitter: @rogeragrimes
- CSOOnline: www.csoonline.com/author/Roger-A.-Grimes/

Благодарности

Я хотел бы поблагодарить издательство Wiley и Джима Минтеля (Jim Mintel) за то, что они дали этой книге зеленый свет. Я более года делал презентации для энтузиастов по теме данной книги, не имея возможности видеть их лица. Спасибо моему работодателю – компании KnowBe4, Inc., и ее замечательному генеральному директору Стью Сьюверману (Stu Sjouwerman), а также Кэти Уоттман (Kathy Wattman), Кендре Ирми (Kendra Irmie) и Мэри Оуэнс (Mary Owens), которые позволили мне разработать оригинальную презентацию и представить ее в различных организациях графства. Спасибо моей основной команде поддержки этих квантовых презентаций в компании KnowBe4: Эми Митчелл (Amy Mitchell), Джессике Шелтон (Jessica Shelton) и Энди Риду (Andy Reed). Я хочу поблагодарить всех, у кого брал интервью и с кем обменивался электронными письмами в стремлении лучше понять, как квантовые компьютеры повлияют на наш мир, включая криптографию. Не думаю, что моя голова когда-либо болела сильнее, чем когда я придумывал, как представить очень сложные понятия, пытаясь донести их до аудитории наиболее доходчивым способом. Эту задачу усложняло то обстоятельство, что большая часть квантовой физики и криптографии определена в терминах современной математики. В нескольких разделах я сдался и просто процитировал то, что написали или сказали эксперты. В качестве характерного примера приведу цитату из главы 6, где я пытаюсь описать один из квантовоустойчивых шифров: «команда NTRU Prime описывает свой шифр как “эффективную реализацию высоконадежной криптографии на идеальной решетке с инертным модулем группы Галуа”... другие же используют определения вроде “неприводимые, нециклотомические полиномы”». Всякий раз, видя это описание, я не могу удержаться от улыбки, поскольку, не понимая, что оно значит (как и вся терминология передовой современной математики), я должен был бы отделываться примерно такими общими фразами: «Это по-настоящему сложная математическая задача».

С учетом сказанного любые фактические ошибки, допущенные в этой книге, принадлежат только мне. Я приложил все силы, чтобы убедиться, что ни одна ошибка не попала в книгу. И горжусь тем, что старался быть абсолютно корректным в передаче фактов. В книге, которая охватывает так много сложных тем, возможно, я допустил ошибки. По-видимому, найдутся эксперты по квантовой криптографии, которые будут осуждать меня за то, что я не упомянул какие-то ключевые понятия. Пожалуйста, учтите, что я всего лишь человек, который изо всех сил старался быть максимально точным. Я заранее прошу прощения за любые ошибки. Хочу поблагодарить всех великих учителей и писателей, которые пытались более доступно объяснить квантовую механику и вычислительную технику и мне, и всем остальным. В этой книге я часто привожу примеры и аналогии, к которым прибегали другие авторы,

тексты и выступления которых я читал, слушал и смотрел в течение последних 20 лет. Иногда я понимал вещи, трудные для понимания, только потому, что эти люди проложили мне дорогу. Я старался отдать должное автору любых примеров или объяснений и сослаться на него, если мог вспомнить или найти этого автора. Прошу прощения у всех, кого я не упомянул. Мне будет стыдно за это. Я хочу поблагодарить все команды, которые ответили на мой призыв, за помощь в исправлении и уточнении моего обзора представленных ими в NIST алгоритмов (глава 6). Они стремились объяснить мне суть своих криптографических решений. Не все команды ответили (или ответили вовремя) на мои вопросы. Вот те, кто сделал это: Питер Швабе (Peter Schwabe) из CRYSTAL-Kyber; Томас Прест (Thomas Prest) из FALCON; Дуглас Стебила (Douglas Stebila) из FrodoKEM; Филипп Габори (Philippe Gaborit) из HQC, ROLLO и RQC; Вадим Любашевский из Dilithium; Сяньхуэй Лу (Xianhui Lu) из LAC; Марко Балди (Marco Baldi) из LEDCrypt; Уорд Бьюлленс (Ward Beullens) из LUOV; Йост Райневельд (Joost Rijneveld) из MQDSS & SPHINCS+; Симона Самардзиска (Simona Samardziska) из MQDSS; Томас Пеппельман (Thomas Poeppelmann) из NewHope; Джон Шанк (John Schanck) из NTRU; Нина Биндель (Nina Bindel) из qTESLA; Скотт Флюрер (Scott Fluhrer) из SPHINCS+ и Майк Гамбург (Mike Hamburg) из ThreeBears. Спасибо всем!

Я хотел бы выразить особую благодарность профессору Техасского университета в Остине, исследователю квантовых процессов Скотту Ааронсону (Scott Aaronson); физику, писателю Филипу Беллу (Philip Bell); Кену Мафли (Ken Mafli) из Townsend Security и Даниэлю Бургарту (Daniel Burgarth). Наконец, большое спасибо сотрудникам издательства Wiley, которые терпели мои вечные переработки текста, – это Ким Уимпсетт (Kim Wimpsett), Пит Гоган (Pete Gaughan) и Атияппан Лалиткумар (Athiyappan Lalitkumar). В конце концов, им пришлось меня остановить и наконец-то отправить книгу в печать.

Примечание Я часто намеренно или непреднамеренно использовал слово «шифр» для описания любого криптографического алгоритма. Технически шифр относится только к алгоритмам кодирования, а алгоритмы цифровой подписи являются схемами. Иногда я использовал слово «шифр», чтобы было проще писать о криптографии во всех девяти главах. Пожалуйста, извините меня за любое злоупотребление техническими терминами.

Предисловие

В конце 1990-х годов мир был озадачен компьютерной проблемой, известной под аббревиатурой Y2K, которую предстояло решить с наступлением 2000 года. Она заключалась в том, что к этому моменту большинство устройств, компьютеров и программ в мире записывали даты с использованием только двух последних цифр года и потому на программном уровне разницы между 1850, 1950 и 2050 годами для них не существовало. Когда 1999 год превратился в 2000-й, многие из этих компьютеров и программ не могли правильно обрабатывать данные с использованием двузначных дат в новом столетии, и прогнозировалось много отказов программ и устройств, которые уже использовали даты в будущем (например, программ планирования и гарантий). Симптомы неисправных устройств и программ варьировались от заметных ошибок до ошибок, наличие которых непросто обнаружить (что может быть чрезвычайно опасным), и полной неработоспособности устройств и программ.

Трудность заключалась и в том, что хотя было известно, что значительный процент устройств и программ подвержен влиянию этой проблемы, никто не знал, что оставалось правильным и не требовало обновления, а что необходимо было обновить или заменить до 1 января 2000 года. Оставалось два-три года, чтобы найти, что необходимо исправить, а что нет. Как и в случае многих медленно, но неизбежно надвигающихся катастроф глобального масштаба, большинство людей вплоть до последних нескольких месяцев мало что предпринимало для решения проблемы. Запоздалые попытки предотвратить то, что произойдет, когда часы переместятся в новый век, вызвали в мире накануне этой даты некоторую панику. В 1999 году даже был создан фантастически плохой фильм-катастрофа (www.imdb.com/title/tt0215370), в котором показаны падающие с неба самолеты и прочие приметы наступившего хаоса.

В конце концов, едва ли кто-либо хотел, чтобы с приходом Y2K настоящая жизнь была похожа на кино. Проблемы были, но по большей части мир продолжал жить обычной жизнью. Были устройства и программы, которые не могли обработать новые даты должным образом, но большинство основных систем работали правильно. Не было ни падающих самолетов, ни пожаров, ни прорванных дамб. Многих людей, ожидавших катастрофы, результаты даже несколько разочаровывали, так что со временем аббревиатурой Y2K стали обозначать события, по поводу которых поднимают слишком много шума, создавая преждевременную панику, притом что реальный ущерб оказывается незначительным.

Большинство людей сегодня не осознают, что «катастрофическая» Y2K всех разочаровала именно потому, что у нас были годы для подготовки и предупреждения последствий. Большинство основных систем были про-

верены на наличие проблем 2000 года и по мере необходимости заменены или обновлены. Если бы мир не осознал проблемы Y2K и вообще ничего бы не сделал, ее последствия наверняка были бы намного, намного хуже (хотя я все же не уверен, что самолеты стали бы падать). Нельзя сказать, что Y2K демонстрирует эффект неразорвавшейся бомбы. Благополучный переход к новой дате явился предсказуемым результатом многолетней подготовки, демонстрирующей успех того, что человечество может сделать, столкнувшись с надвигающейся цифровой проблемой.

Грядущий квантовый судный день

Большая часть мира этого еще не осознает, но мы приближаемся к еще более весомому, по сравнению с Y2K, моменту, который, вероятно, уже и теперь вызывает серьезные проблемы и наносит ущерб. Хуже того, мы не можем исключить весь ущерб, даже если начнем готовиться заранее. Сегодня существуют организации, уже наносящие вред программам, избежать которого системы не могут. Государства и конкурирующие компании, должно быть, уже извлекают для себя преимущества из этого обстоятельства.

Квантовые компьютеры, вероятно, в ближайшем будущем взломают традиционные криптокоды с открытым ключом, в том числе шифры, защищающие большинство цифровых секретов мира. Эти протоколы и компоненты включают HTTPS, TLS, SSH, PKI, цифровые сертификаты, RSA, DH, ECC, большинство сетей Wi-Fi, многие сети VPN, смарт-карт, HSM, большинство криптовалют и большинство устройств многофакторной аутентификации, которые полагаются на криптографию с открытым ключом. Даже если бы список содержал только HTTPS и TLS, то он уже охватывал бы бóльшую часть интернета. В тот день, когда квантовые вычисления нарушат традиционную публичную криптографию, все секреты, защищенные этими протоколами и механизмами, выйдут наружу.

Еще более важно, что любой, кто сейчас перехватит и сохранит эти защищенные в настоящее время секреты, после квантового криптографического взлома будет иметь возможность вернуться и раскрыть секреты. Сколько у вас или вашей организации есть секретов, которыми вы готовы поделиться с миром через несколько лет? Это новая проблема Y2K, с которой мы имеем дело уже сегодня.

Есть много выполнимых решений, которые можно реализовать сегодня, хотя некоторые из них либо выходят за рамки имеющихся возможностей средней компании, либо, если их преждевременно реализовать, могут привести к значительным нарушениям ведущихся работ. Подготовка к грядущему квантовому взрыву требует образования, критичного выбора и планирования. Люди и организации, которые четко понимают, что нас ждет впереди, могут предпринять правильные шаги уже сейчас, чтобы быть как можно более подготовленными. Они могут остановить сегодня необоснованное подслушивание и начать переводить свои управляемые активы в более устойчивую среду. Данная книга содержит необходимые для этого знания и дает вам план, помогающий минимизировать риски вашей организации от прихода

квантового криптовзлома. Если достаточное количество организаций будут готовиться к этому уже сейчас, мы можем избежать квантовых проблем и сделать их столь же малосущественными, как это было с проблемой Y2K.

Для кого эта книга

Эта книга в первую очередь предназначена для тех, кто отвечает за управление безопасностью компьютерной техники своей организации и, в частности, компьютерную криптографию. Это люди, которые, разрабатывая проекты, будут отвечать на вызовы постквантовой миграции. Данная книга также для менеджеров и других лидеров, понимающих важность хорошей криптографии и ее влияние на их организацию. Наконец, любой, интересующийся квантовой механикой, квантовыми компьютерами и квантовой криптографией, найдет здесь много неизвестных ему фактов, делающих эту книгу достойной прочтения.

Что вы найдете в этой книге

Книга «Апокалипсис криптографии» подготавливает читателя к квантовому прорыву в вычислениях. Она состоит из девяти глав, разделенных на две части.

Часть I «Учебник по квантовым вычислениям» – это базовый учебник по квантовой механике и вычислениям, рассказывающий о том, как можно взломать сегодняшнюю криптографическую защиту.

Глава 1 «Введение в квантовую механику»

Если вы не понимали квантовую механику, читая о ней впервые, не расстраивайтесь – квантовая механика досаждала самым блестящим умам, которые украшали нашу планету за последнее столетие. Нас, простых смертных, можно простить за то, что мы не сразу усваиваем ее основные идеи. Глава 1 объясняет свойства, наиболее важные для понимания того, как квантовая механика влияет на наш цифровой мир. Если я проделал свою работу хорошо и правильно, вы поймете это лучше, чем 99 % других представителей нашей компьютерной цивилизации.

Глава 2 «Введение в квантовые компьютеры»

Квантовые компьютеры используют квантовые свойства и обеспечивают возможности, логические и арифметические результаты, которых просто невозможно достигнуть с помощью традиционных бинарных компьютеров. Глава 2 охватывает различные типы квантовых компьютеров, которые, скорее всего, станут окружать нас в следующем десятилетии и будут поддерживать различные квантовые свойства.

Глава 3 «Как квантовые вычисления могут взломать существующие криптокоды?»

Наиболее распространенный вопрос, который задают, когда человеку говорят, что квантовые компьютеры, вероятно, взломают традиционные

криптокоды с открытым ключом, – каким образом? В главе 3 рассказывается, почему традиционным бинарным компьютерам нелегко взломать большинство шифров с открытым ключом и что позволит квантовым компьютерам легче справиться с задачей. Здесь показано, что квантовые компьютеры, скорее всего, будут иметь возможность взломать, а также что будет устойчивым к квантовым вычислительным мощностям.

Глава 4 «Когда случится криптопрорыв?»

После вопроса о том, как квантовые компьютеры могут сломать традиционные криптокоды с открытым ключом, второй наиболее часто задаваемый вопрос, – когда это произойдет. Хотя этого никто (достоверно) не знает, предположительный ответ таков: скорее раньше, чем позже. В главе 4 обсуждаются различные сроки и их вероятность.

Глава 5 «Каким будет постквантовый мир?»

Как и изобретение интернета, квантовое доминирование разделит мир на «до» и «после». Квант решит проблемы, которые мучили нас на протяжении веков, и даст нам новые проблемы, и это в будущем начнет раздражать нас. Глава 5 опишет постквантовый мир и как он будет влиять на нас.

Часть II «Подготовка к квантовому взрыву» поможет вам и вашей организации наиболее эффективно подготовиться к грядущему квантовому доминированию.

Глава 6 «Квантовоустойчивая криптография»

Глава 6 охватывает более двух десятков квантовоустойчивых шифров и схем, которые Национальный институт стандартов и технологий (NIST) рассматривает во втором туре своего постквантового конкурса. Два или более из этих квантовоустойчивых алгоритмов станут следующими национальными стандартами криптографии. Вы узнаете о конкурентах, их сильных и слабых сторонах.

Глава 7 «Квантовая криптография»

Глава 7 посвящена традиционной бинарной квантовоустойчивой криптографии, которая не использует квантовые защитные свойства. Глава 7 охватывает шифры и схемы, которые квантовые свойства используют, чтобы обеспечить их криптографическую устойчивость. В долгосрочной перспективе вы, вероятно, будете использовать криптографию на основе квантов, а не только квантовоустойчивую криптографию. Узнайте, как это выглядит.

Глава 8 «Квантовые сети»

Глава 8 охватывает квантовые сетевые устройства, такие как квантовые повторители и приложения, которые ищут квантовую защиту сети. Она описывает текущее состояние квантовых сетей и как это, вероятно, будет выглядеть в ближайшем и долгосрочном будущем. Скорее всего, настанет время, когда весь интернет будет основан на квантах. Читайте о таких сетях и их компонентах и о том, как мы к ним придем.

Глава 9 «Готовимся сейчас»

Ради одной только этой главы книга заслуживает внимания. Здесь будет показано, как уже сегодня организации любого рода могут начать подготовку к грядущему квантовому криптографическому взрыву. Из главы 9 вы узнаете, что можно сделать сегодня, чтобы защитить ваши наиболее важные долгосрочные секреты, какие размеры криптографических ключей нужно увеличить, что и когда должно быть заменено. Обобщенный план, применявшийся ранее для глобальных обновлений криптографии, может быть использован и для преодоления апокалипсиса криптографии.

В приложении перечислены десятки ссылок на квантовые информационные ресурсы, в том числе книги, видео, блоги, официальные документы и веб-сайты.

Если я хорошо справился со своей работой, к концу этой книги вы лучше, чем прежде, поймете квантовую физику, поймете, как она сломает сегодняшнюю традиционную криптографию с открытым ключом, и будете в состоянии надлежащим образом подготовить и лучше защитить ваши важные цифровые секреты.

Отзывы и пожелания

Мы всегда рады отзывам наших читателей. Расскажите нам, что вы думаете об этой книге – что понравилось или, может быть, не понравилось. Отзывы важны для нас, чтобы выпускать книги, которые будут для вас максимально полезны.

Вы можете написать отзыв на нашем сайте www.dmkpress.com, зайдя на страницу книги и оставив комментарий в разделе «Отзывы и рецензии». Также можно послать письмо главному редактору по адресу dmkpress@gmail.com; при этом укажите название книги в теме письма.

Если вы являетесь экспертом в какой-либо области и заинтересованы в написании новой книги, заполните форму на нашем сайте по адресу http://dmkpress.com/authors/publish_book/ или напишите в издательство по адресу dmkpress@gmail.com.

Список опечаток

Хотя мы приняли все возможные меры для того, чтобы обеспечить высокое качество наших текстов, ошибки все равно случаются. Если вы найдете ошибку в одной из наших книг – возможно, ошибку в основном тексте или программном коде, – мы будем очень благодарны, если вы сообщите нам о ней. Сделав это, вы избавите других читателей от недопонимания и поможете нам улучшить последующие издания этой книги.

Если вы найдете какие-либо ошибки в тексте, пожалуйста, сообщите о них главному редактору по адресу dmkpress@gmail.com, и мы исправим это в следующих тиражах.

Нарушение авторских прав

Пиратство в интернете по-прежнему остается насущной проблемой. Издательства «ДМК Пресс» и Wiley очень серьезно относятся к вопросам защиты авторских прав и лицензирования. Если вы столкнетесь в интернете с незаконной публикацией какой-либо из наших книг, пожалуйста, пришлите нам ссылку на интернет-ресурс, чтобы мы могли применить санкции.

Ссылку на подозрительные материалы можно прислать по адресу электронной почты dmkpress@gmail.com.

Мы высоко ценим любую помощь по защите наших авторов, благодаря которой мы можем предоставлять вам качественные материалы.

Учебник по квантовым вычислениям

1 Введение в квантовую механику

> Ничего удивительного в том, что те, кто впервые встречается с квантовой механикой, не могут понять ее.
>
> *Нильс Бор, квантовый физик, лауреат Нобелевской премии 1922 года*

> Любая достаточно развитая технология неотличима от магии.
>
> *Артур Чарльз Кларк, писатель-фантаст*

В главе 1 будут обсуждаться основы квантовой механики, особенно аспекты, касающиеся квантовых вычислений. Данная глава намеренно не охватывает все аспекты полностью, поскольку для этого потребовалась бы целая книга, а не просто глава на эту тему. Не будет описана каждая частица, ее свойства или возможное взаимодействие, и будут опущены все сложные математические уравнения. Эта глава даст вам понимание квантовой физики, достаточное, чтобы объяснить, как квантовые компьютеры способны быстро решать считавшиеся ранее нерешаемыми математические задачи, на которых основаны многие распространенные, обеспечивающие защиту, типы шифрования. Понимание квантовой механики и квантовых вычислений совершенно не требуется для подготовки к грядущей эпохе криптографических взломов, но оно поможет вам усвоить самые азы для обсуждения соответствующих проблем.

Что такое квантовая механика?

В этом разделе я буду объяснять квантовую механику, но если это ваша первая встреча с данной темой, отнеситесь к ней с некоторой осторожностью. Квантовая механика невероятно крута, и иногда мы не способны полностью понять, что происходит. Многое в ней кажется таким странным для нашего нынешнего понимания того, как устроен мир, что большинству людей, которые впервые сталкиваются с квантовой механикой, понять ее очень нелегко. Даже после почти 30 лет попыток полностью осознать сущность этой области знаний и ее значение мой мозг психологически все еще не готов к этому. Я не одинок. Приятно снисходительно сказать, что только на первый взгляд квантовая механика противоречит интуиции и выглядит неестественно, но часто это совсем не так. Это идет вразрез со многим, чему нас учили ранее об устройстве нашего мира и Вселенной. Один плюс один

не всегда равняется двум. Это идет также вразрез с тем, что мы можем легко увидеть, потрогать и почувствовать, хотя вся наша реальность возможна именно благодаря этому.

Хотя лучшие умы нашей цивилизации неоднократно доказывали, что в существовании квантовой механики нет ни тени сомнения, то, что она влечет за собой, звучит так странно для обычного человека, что часто остается для него невероятным и волшебным. Понимание значения квантовой механики даже впервые ставит вопрос о существовании реальности.

Довольно распространенная реакция на квантовую теорию заключается в предположении, что все, кто проповедует ее, должно быть, находятся под воздействием какой-то научной фантастики, что это результат массового заблуждения, потому что речь идет о том, чего быть не может. Как однажды сказала мне одна моя подруга, после того как я попытался (явно неудачно) объяснить ей квантовую механику: «Ты можешь верить во все, что хочешь, но это просто чушь собачья»... правда, слова «собачья» она не произнесла.

Даже Альберт Эйнштейн, который помогал открытию некоторых из наиболее важных принципов, лежащих в основе квантовой механики, не вполне верил в некоторые ее другие принципы. Он потратил десятилетия, пытаясь понять их, и понял их лучше, чем многие другие. Это его глубокое понимание ее основ создавало для него проблемы. Он даже ставил эксперименты, пытаясь доказать или опровергнуть их. Он не мог логически проверить или объяснить многие странные свойства квантовой механики и «пугающие при взгляде с расстояния» результаты. После десятилетий ожидания экспериментального подтверждения своих предположений он просто перешел к изучению других научных областей. Видимо, его мозг просто устал постоянно думать об этом. Так что не столь великие умы вполне можно извинить.

С учетом сказанного я написал эту главу учебника по квантовой механике так, как хотел бы, чтобы это было объяснено мне самому, когда я впервые начал изучать ее. Я надеюсь, что данная глава поможет сократить вам время обучения.

Квант противоречит интуиции

Хотя квантовая механика лежит в основе всей реальности, она не всегда выглядит так, как то, что мы наблюдаем в нашей повседневной жизни. Например, собака одной масти не может быть белой и черной масти в одно и то же время; белая собака, находящаяся в комнате, не становится черной, когда выходит из нее, и собака не может разделиться на две собаки прямо на ваших глазах, а затем снова слиться воедино. Но на атомном и субатомном уровнях особенности квантовой механики состоят как раз в подобных странностях. Какие же свойства квантов, о которых я говорю, столь странные? Вот некоторые примеры:

- одна квантовая частица может находиться в двух местах и быть одновременно двумя совершенно разными частицами;
- одна квантовая частица может разделиться на две, а позже столкнуться или смешаться и восстановиться или исчезнуть;

- в реально пустом пространстве, где абсолютно ничего нет (о чем ученым известно), квантовые частицы могут просто появиться «из воздуха» и затем исчезнуть;
- кажется, что квантовая частица ведет себя одним образом, когда ее не измеряют, и другим, будучи измеренной, как будто природа позаботилась о воздействии процедуры измерения. Похоже, это даже изменит путь частицы или сделает ее поведение обратным во времени, если вы решите измерить ее после того, как она прошла свой первоначальный путь;
- две квантовые частицы могут быть «спутаны» таким образом, что когда вы меняете одну, другая каждый раз тоже мгновенно меняется таким же образом, независимо от того, насколько далеко они друг от друга, хоть через вселенную;
- квантовое состояние – это всегда все возможные состояния (называемые суперпозицией состояний), но единственное, конечное состояние с уверенностью предсказано быть не может;
- каждый возможный ответ будет ответом в какой-то момент, хотя каждый из этих ответов может быть из своей отдельной совокупности. Для каждой возможной комбинации на атомном уровне могут быть разные совокупности вариантов ответа – так называемые мультиверсы (multiverses);
- телепортация, подобная показанной в научно-фантастическом сериале Star Trek («Звездный путь»), возможна.

Квантовая механика реальна

В «странные» свойства квантовых частиц трудно поверить. Тем не менее эти квантовые свойства и результаты не только были проверены и доказаны, но они являются одними из самых проверенных и признанных научных теорий в мире. Они постоянно проверялись и оспаривались. Все эксперименты, которые были проведены, чтобы опровергнуть основные принятые теорией принципы квантовой механики, потерпели неудачу. Многие из неудач, в том числе и Эйнштейна, только в еще большей мере подтверждали квантовую теорию. Большинство Нобелевских премий по физике за последние 75 лет были присуждены ученым, которые улучшили наше понимание квантовой механики. В последние несколько десятилетий интерес к этой теме возрастает, и наше понимание квантовой механики с каждым годом улучшается.

Хотя перечисленные в предыдущем разделе факты могут при первом прочтении показаться невероятными, подлинность квантовой физики оказывается для нас все большей и большей реальностью и становится в один ряд с тем фактом, что Солнце дает жизнь нашей планете или что любой раскаленный материал дает красное свечение, а также с фактами существования цифровых камер, оптоволоконых кабелей, лазеров, компьютерных чипов, носителей и коммуникаций интернета. Очень вероятно, что реальность как раз и состоит в том, что каждая составляющая этой реальности основана на квантовой механике.

Квантовая механика дает нам очень мощные компьютеры, которые раньше были немыслимы. Квантовые компьютеры и устройства изменят наш мир многими невероятными способами, которые мы можем или не можем понять сейчас, так же, как это было для нынешнего поколения с интернетом, USB-накопителями и iPod'ами. Потенциальные квантовые изобретения значительно изменят нашу жизнь к лучшему, и самые важные из них появятся очень скоро.

Интересно, что хотя большая часть квантовой теории была подтверждена повторными наблюдениями, экспериментами и математикой, ученые до сих пор не знают, почему многие квантовые свойства таковы, какие они есть, или почему дают именно такие результаты. Физики-теоретики часто гадают о том, почему квантовая механика такова, какова она есть. Вы можете услышать предположения разного рода, обсуждаемые различные их *интерпретации* или *взгляды*, такие как *копенгагенская интерпретация* или взгляд «*Много миров*» (будет рассмотрен ниже, в разделе «Эффект наблюдателя» этой главы). Существует более десятка интерпретаций, каждая из которых пытается объяснить какую-то часть квантовой механики, даже не зная, точна эта интерпретация или нет.

Важно понимать, что независимо от предположения, почему или как происходит какое-то квантовое действие либо появляется его результат, действие или результат действительно возникают, притом всегда ожидаемым образом, что экспериментально и математически доказано независимо от интерпретации. Никогда не было серьезного квантового предсказания, не подкрепленного достоверными экспериментами. Мы не всегда можем знать, почему поведение квантов – скажем точнее: квантовое действие – таково, но мы знаем, что оно реально происходит. Это может показаться магией, но таково истинное положение дел, даже если мы не можем объяснить или увидеть это в общепринятом смысле.

Это беспокоит тех, кто не относится к ученому кругу. Просить их поверить в то, чего они не видят или не чувствуют и что категорически противоречит интуиции и всему тому, чему их учили раньше, значит требовать слишком многого. Это совсем не то, как они раньше привыкли оценивать науку. Например, они могут не понимать высказывания физика и математика относительно гравитации, но они могут видеть результат каждый раз, когда бросают мяч, спотыкаются и падают, смотрят, как яблоки падают с дерева, или наблюдают вращение Луны вокруг Земли. Они могут не понимать математику, но понимают, как и почему работает гравитация… ну, хорошо, по крайней мере большинство. Многие люди спрашивают, как мы можем верить, что все, о чем говорит наука, существует, не зная, как или почему это произошло. Как мы можем верить во что-то, чего не можем увидеть своими глазами, особенно что-то невероятное и нелогичное?

То, чего скептики обычно не знают, – так это то, что бóльшая, если не самая большая, часть прогресса науки в прошлом веке, особенно физики, и особенно квантовой физики, почти всегда сначала была обязана доказательствам экспериментальным и/или с помощью математики, без понимания, почему и как. Много раз ученые, имея только очень смутные теории, для того чтобы поддержать то, что можно было наблюдать лишь поверхностно, сумели доказать их

математически. Отсюда и появился термин «физик-теоретик». Такой ученый часто начинает с реальных событий и поддержки рискованной интеллектуальной теории, чтобы объяснить то, что наблюдает. Если он (или кто-то еще) может предоставить математическое уравнение, которое последовательно описывает наблюдаемое явление, то большинство ученых будут полагаться на математику как на убедительное доказательство существования такого поведения или события. Это вовсе не то представление, в которое верит физик. Математика даже важнее, чем это представление или прямое наблюдение физика. Кто-то однажды сказал: «Единственная абсолютная истина в мире – это математика». Имелось в виду, что все, кроме хорошо поддерживаемого математического уравнения, подвержено личным взглядам и интерпретациям. Либо математика поддерживает что-то, либо нет. Либо математика подтверждает что-то, либо нет. Это не предмет суждений наблюдателей. Если ученый видит какое-то явление, которому пока нет объяснения, и может последовательно поддерживать его соответствие математической формуле и если каждый эксперимент подтверждает результат, точно описанный математикой, то научный факт считается доказанным. Математика является доказательством. Прямое, убедительное, подтверждающее наблюдение необязательно.

Неоспоримое наблюдаемое событие, которое могло бы убедить тех, кто далек от науки, часто происходит спустя десятилетия или даже столетия. Обычно к тому времени ученые и их последователи уже давно имеют в распоряжении соответствующую теорию, верят в нее и рассматривают событие как достоверный факт, подтвержденный математически. В их представлении это последнее неоспоримое, физическое доказательство считается почти ненужной формальностью.

Многие прошлые научные постулаты, как очень маленькие, так и очень большие, включая открытие атомов, электронов и черных дыр, были сначала обнаружены учеными, создающими теории и разрабатывающими математические формулы относительно ранее необъяснимых наблюдаемых явлений. В предыдущих наблюдениях черных дыр и недавно обнаруженных планет Солнечной системы наблюдатели заметили тонкие отклонения в орбитах тел и излучении света, которые, как они понимали, можно было объяснить только неизвестными ранее сторонними эффектами. Теория черных дыр появилась в 1784 году благодаря Джону Митчеллу (John Mitchell) и математически была поддержана общей теорией относительности Эйнштейна в 1915 году. Дальнейшие, в течение следующей половины столетия, связанные с ними наблюдения подтвердили математически и существование черных дыр, даже притом, что их не могли «увидеть». С 1970-х годов ученые воспринимают реальность черных дыр как данность. Первый снимок, который рядовой обыватель может считать «реальным доказательством» черных дыр, появился лишь в апреле 2019 года (https://phys.org/news/2019-04-scientists-unveil-picture-black-hole.html).

История квантовой механики идет по тому же пути. В ней участвуют сотни блестящих физиков, наблюдающих очень маленькие объекты, поведение которых они не могли бы объяснить, используя традиционную (т. е. классическую) физику. С появлением математических уравнений они стали наблюдать и изучать новые, странные явления, наличие которых, казалось, все больше подтверждалось. Они делали предположения о том, почему и как что-то происходило, а затем проводили эксперименты, чтобы доказать или

опровергнуть свои догадки. Со временем дополнительные эксперименты и наблюдения создали ныне известные постулаты квантовой механики. Некоторые блестящие умы, такие как Эйнштейн, ошибались относительно некоторых фактов, а ранее малоизвестные физики сделали карьеру (и получили Нобелевские премии), приведя доказательства других. В целом вклады сотен отдельных ученых и их скептицизм создали квантовую механику такой, какую мы знаем сегодня, временами кажущуюся странной и необъяснимой.

Основные свойства квантовой механики

В этом разделе я расскажу о популярных свойствах квантовой механики, таких как фотоэлектрический эффект, двойственность волна–частица, вероятности, принцип неопределенности, спиновые состояния, туннельный эффект, суперпозиция, эффект наблюдателя и квантовая спутанность.

Примечание Итак, что такое квант в квантовой физике? Когда физики используют термин *quantum* или *quanta* (от латинского quantus – «количество» или «сколько»), они заявляют, что все, что они описывают, является наименьшей возможной единицей чего-либо (например, света или энергии) и не может быть разделено на более мелкие единицы. И любой математический расчет с участием квантов не может разделить кванты на что-то меньшее, чем целое число.

Квантовая механика, или *квантовая физика*, состоит из свойств и действий квантовых частиц и взаимодействия. Так называется и область исследований с участием квантовых свойств и частиц. Почти всегда эти слова используются как взаимозаменяемые.

Хотя вся наша реальность состоит из квантовых частиц и их взаимодействия, квантовая механика существует на микроскопическом уровне для очень, очень малых элементарных объектов, таких как фотоны, кварки, электроны и атомы. Если элементный объект проявляет квантовые свойства, он известен как *квантовая частица*. Самые маленькие известные частицы обычно проявляют квантовые свойства. Квантовые свойства могут распространяться и на более крупные объекты, на так называемом *макроскопическом уровне*, но наука еще не продвинулась настолько, чтобы понять однозначно, происходит это или нет, и если происходит, то как. Понимание того, как свойства очень маленьких объектов передаются большим объектам и воздействуют на них, – конечная цель весьма популярной так называемой *Всеобщей теории* (Theory of Everything).

Примечание Макроскопический уровень включает в себя любой объект, превышающий микроскопический уровень атома и субатомные частицы, но часто понимается как начинающийся с объектов, которые могут быть обнаружены невооруженным глазом. Большинство ученых сходятся во мнении, что человеческий глаз может обнаружить объект, равный ширине человеческого волоса (0,4 мм), или около 100 000 атомов элемента.

Фотоны и квантовая механика

Вы будете часто читать о фотонах (первоначально названных Эйнштейном *квантами энергии*), используемых в экспериментах по квантовой механике. *Фотон* является наименьшей из возможных делимых единиц света и квантового поведения. Они очень маленькие. Для среднего напряженного человеческого глаза регистрация очень слабого проблеска света, отправленного почти мгновенно, потребует не менее ста фотонов. Любой луч света или изображение, которое мы обычно видим, включает в себя от миллионов до триллионов фотонов.

Квантовые физики часто проводят эксперименты с использованием одиночных (или относительно небольших количеств) фотонов или других элементарных частиц, потому что, используя небольшие их количества, ученые могут удалить другие ненужные эффекты, которые в противном случае только усложнят эксперименты, результаты и математические доказательства. Доказательство квантовых свойств было впервые получено в экспериментах с использованием фотонов при исследовании излучения, электромагнитных волн и фотоэлектрического эффекта (за которое Эйнштейн был удостоен своей единственной Нобелевской премии в 1921 году). Работа Эйнштейна имела решающее значение для становления квантовой теории. Даже его работы по опровержению квантовой механики лишь улучшили ее понимание нами.

В течение долгого времени ученые смогли генерировать одиночные протоны, посылая их в экспериментах разными путями и измеряя то, что происходит, используя светочувствительное оборудование, так называемые *фотоумножительные трубы* (photomultiplier tubes). Фотоумножитель способен принять один обнаруженный фотон и размножить его в достаточно большом количестве других фотонов, которые могут создать электрический ток, чтобы можно было зарегистрировать и подтвердить начальное обнаружение одиночного фотона. Представляйте себе это как падающее домино. Падение одной кости домино может вызвать падение многих других костей домино. По этой причине, когда вы будете читать о квантово-физических экспериментах, вы часто будете читать о фотонах (и подобных элементарных квантовых частицах). Распространенными также являются эксперименты с использованием отдельных электронов, атомов и молекул. Давайте обсудим, что доказали некоторые из этих экспериментов.

Фотоэлектрический эффект

Понимание и количественная оценка фотоэлектрического эффекта в начале 1900-х годов (Планк, Эйнштейн и др.) послужили началом основ современной квантовой механики. Свет, который мы видим, – это только один тип и диапазон электромагнитного излучения того, что называется электромагнитным спектром. Электромагнитный спектр описывает все виды электромагнитного излучения, включая свет, который мы можем видеть, и все типы, которые мы видеть не можем (такие как рентгеновские лучи, микроволновые печи, гамма-волны и радиоволны). Различные типы элект-

ромагнитного излучения отличаются в первую очередь длиной волны (для примера: видимый свет имеет длину волны от 400 до 700 нанометров (нм), рентгеновские лучи – от 0,10 до 10 нм), частотой (нередко измеряется количеством циклов в секунду, называемых герц [Гц]), интенсивностью, направлением и другими свойствами. Все виды электромагнитного излучения движутся прямолинейно, если излучение ничем не ограничено (объектом, гравитацией и т. д.), со скоростью света (299 792 458 м/с в вакууме).

Примечание Частота и длина волны могут быть преобразованы друг в друга через скорость света, и по существу это одна и та же переменная.

У света есть импульс и энергия (но нет массы). Планк и Эйнштейн поняли, что когда свет (или другие формы электромагнитного излучения) падает на другой материал, материал часто испускает электроны (которые всегда заряжены отрицательно) в результате передачи энергии от фотона материалу, как показано на рис. 1.1. Чем выше интенсивность света, тем больше электронов испускается. Фотоэлектрический эффект возникает, когда свет попадает на большинство материалов, но наиболее легко наблюдается, когда свет падает на металлы и другие хорошо проводящие материалы. Фотоэлектрический эффект – это когда энергия солнца преобразуется в электричество с помощью солнечных батарей. Фотоэлектрический эффект лежит также в основе работы цифровых камер и записи изображений.

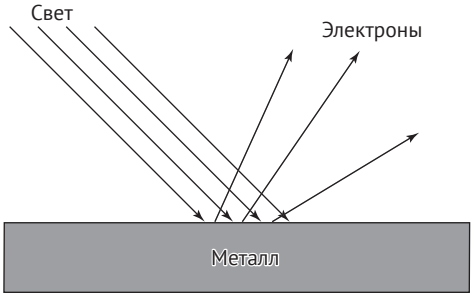


Рис. 1.1. Фотоны ударяются о металл, который затем испускает электроны
Рисунок 1.3 из кн.: Steven Holzner. Quantum Physics For Dummies, Revised Edition; Wiley, 2013

Двойственность волна–частица

Сотни лет то, что ученые обнаруживали на микроскопическом уровне, классифицировалось или как частица, или как волна. *Частицы* – это (микроскопические) объекты, которые следуют четко определенным, легко обнаруживаемым физическим законам, объекты, которые мы можем наблюдать так же, как и повседневные макроскопические объекты (такие как камни или шары). Частицы путешествуют предсказуемыми путями, подвержены гравитации и могут взаимодействовать с другими частицами и объектами. Их довольно легко описать, предсказать и математически моделировать.

Волна – это непрерывное возмущение в поле, которое колеблется между различными точками пространства, или какая-то другая переменная. Волна может передавать энергию через основную среду, не нарушая другие объекты в среде. Это, например, происходит, когда плавающий объект, допустим лодка на воде, встречается с волной. Волна поднимает лодку вверх и вниз по мере прохождения, но не сильно нарушает ее общее положение на воде, если волна не настолько велика, что становится гребнем. Волны проявляют себя не только в том, что мы видим (например, океанские волны, рябь в озере или вибрации в струне), но также и в другом, что мы не видим (например, звук, радио, радиация и микроволны).

Примечание Волны могут осциллировать, как переменные, не меняя пространства или положения среды. Например, электромагнитные волны – это меняющиеся электрические и магнитные поля.

Волны колеблются в непрерывной, повторяющейся, связанной схеме. *Форма волны* каждого конкретного типа волн имеет верхний пик, или гребень, за ним следует нижняя долина, или впадина, и это повторяется снова и снова. Расстояние между вершиной и впадиной называется *амплитудой*. Число полных подъемов и впадин волны за определенный период времени определяет ее *частоту*.

Ученые думали, что частицы и волны обладают совершенно разными физическими свойствами. Частицы функционируют больше как камни или бейсбольные мячи. Они с трудом «огибают» предметы. Они ударяют с импульсом и силой. Их траектории при столкновении и возникающие при этом отскоки могут быть предопределены и рассчитаны заранее. Можно легко увидеть каждую отдельную часть составляющих большую массу частиц, как вид отдельных камней, составляющих кучу камней. Частица, ударившаяся в стену, похожа на жука, попавшего в лобовое стекло. Волны имеют противоположные свойства.

В середине 1800-х годов после многих теорий и экспериментов это было «устоявшейся наукой», в то время как свет и фотоны, которые составляют его, перемещались как волны. Но начиная с начала 1900-х годов, когда были обнаружены фотоны и другие электромагнитные частицы и использованы в большем количестве субатомных экспериментов, ряд ученых стал замечать, что фотоны и другие частицы вели себя и как волна, и как частица (то есть проявляли двойственность волна–частица). В то время это считалось чуть ли не научным кощунством. Однако Эйнштейн подтвердил эту новую точку зрения, продемонстрировав, что свет действует так же, как частица, и получил за это открытие свою единственную Нобелевскую премию по физике. Эйнштейн писал о своем открытии:

> *Кажется, мы должны использовать иногда одну теорию, иногда другую, а иногда можем использовать и обе. Мы столкнулись с новым видом трудностей. У нас есть две противоречивые картины реальности. Отдельно ни одна из них полностью не объясняет явления света, но вместе они это делают.*

Один из лучших способов думать о двойственности волновых частиц – это представить, что у вас есть резиновый шарик, который когда ведет себя как частица, подпрыгивает и отпрыгивает назад и вперед, ударяясь о другие объекты, в зависимости от его траектории и свойств материала, о который он ударяется. Теперь представьте, что шар падает в озеро и исчезает (под поверхностью). Его энергия немедленно превращается в волны в виде ряби на поверхности. Затем волновая рябь ударяется о доковую станцию, находящуюся в воде. Резиновый шар в этот момент появляется на доке, а волны исчезают. Это и есть двойственность волна–частица в зависимости от ситуации. Фотон действует иногда как волна, а иногда как частица. За эту прекрасную аллегорию надо сказать спасибо Доминику Уоллиману (Dominic Walliman).

Это частица

Ученые продемонстрировали двойственность волна–частица с помощью простого эксперимента с использованием высокоинтенсивного (лазерного) света, фона и промежуточного блокирующего материала с одной и двумя прорезями в нем. Ученые направили пучок фотонов сквозь щель блокирующего материала и затем посмотрели, куда попали фотоны на заднем фоне. Когда использовалась одна щель и пучок фотонов был пропущен через нее, фотоны, пройдя через щель, попали на задний фон почти прямо по направлению пучка. Отдельные фотоны расположились довольно близко друг к другу, имитируя форму щели. Картина напоминала выстрел меткого стрелка и путь пули при выстреле сквозь щель. Если винтовка находилась каждый раз в одном и том же положении, можно было ожидать, что пуля попадет почти в то же место, с небольшими отклонениями в зависимости от опыта стрелка, точности винтовки, индивидуальных параметров пули и любых других внешних мешающих факторов. Если винтовка была направлена при стрельбе под разными углами, пули могли располагаться более спонтанно. Это как раз и происходило, когда пропускался пучок фотонов. Фотоны демонстрировали свойства частицы.

Интерференция волн

Нечто удивительное случилось, когда в промежуточном блокирующем материале добавили вторую щель. Когда был пропущен один фотон, он все еще попадал на заднем плане за щелями, со следом одной частицы (то есть как пулевое отверстие), но уже не прямо за прорезями. Когда же пучок фотонов содержал все большее и большее их количество, казалось, фотоны попадали в области, которые не были расположены непосредственно позади щели. Были области с различными предпочтениями – кластеры областей с большим количеством совокупных попаданий, и области, в которые попадало меньше фотонов. Создавалось чередование светлых и темных вертикальных полос (как показано на рис. 1.2).

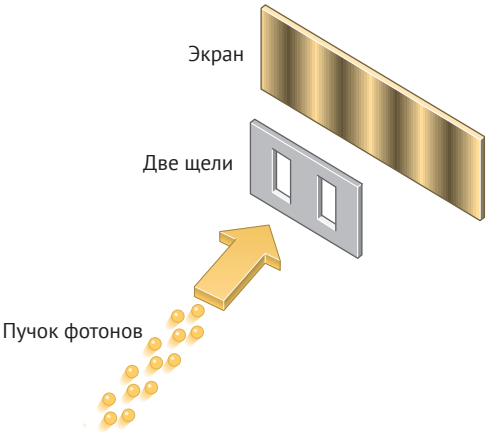


Рис. 1.2. Эксперимент с двумя щелями и источником света, подтверждающий двойственность волна–частица
Рисунок 29.1 из кн.: David Young, Shane Stadler. Cutnell & Johnson Physics, 11th Edition; *Wiley, 2018*

Ученые сразу поняли, что то, что они видят, являлось результатом действия пущенных одновременно фотонов, перемещающихся как волна (и падающих на задний план как частица). Полосы появлялись потому, что когда фотон перемещается как волна, он попадает в обе щели и создает две результирующие волны по другую сторону каждой щели, с которой взаимодействует каждая часть оригинальной одиночной волны, проходившая через щель. По другую сторону две результирующие волны перемешивались друг с другом, формируя полосы. Но фотон, падающий на задний фон, являлся следом частицы (как показано в видео из Википедии: https://upload.wikimedia.org/wikipedia/commons/e/e4/Waveparticle_duality.ogv). Это была замечательная находка.

Полоса на экране создается взаимодействующими друг с другом волнами. Если одна световая волна, находящаяся на вершине гребня, встречает в какой-то момент другую световую волну на вершине ее гребня, то это создает максимально возможную комбинированную, синхронизированную световую волну, которая имеет наиболее яркий свет. Это также означает, что их объединенные впадины создают темные полосы. Любая другая комбинация, отличная от совпадения двух наибольших вершин и двух наибольших впадин, будет создавать менее смешанные волны – менее яркие или менее темные.

Вначале, когда это было обнаружено, ученые просто не могли поверить утверждениям, математике и результатам. Потребовались десятилетия, чтобы наука окончательно признала, что свет ведет себя и как частица, и как волна одновременно. Теперь мы без сомнения знаем, что все субатомные частицы, составляющие всю материю, действуют с двойственностью волна–частица. Этот вывод укрепил решимость ученых более полно исследовать квантовую механику и попытаться «связать» ее с остальным нашим большим миром. Сегодня любой может выполнить простой эксперимент, чтобы увидеть эту двойственность волны и частицы света.

Эксперимент с двумя щелями

Приятно иметь возможность воссоздать один из ранних экспериментов по двойственности частиц и волн и непосредственно наблюдать работу квантов. Вы можете воспроизвести этот эксперимент, используя лазерную указку, фольгу и сплошной фон, например стену. Используйте сильную однотонную (не белую) лазерную указку. Чем более она мощная, тем лучше. Белый свет – это смесь всех цветов света, и это затрудняет эксперимент, потому что отдельные цвета, из которых состоит белый свет, имеют разные частоты. Поместите фольгу на поверхности разделочной доски и вырежите рядом две равные по длине вертикальные прорези длиной около 1 дюйма, так близко, насколько это возможно (речь идет о расстоянии в миллиметры). Затем в затемненной комнате осветите лазерным лучом указки эти две прорези на расстоянии фута или более от фольги, отстоящей от поверхности заднего фона также на расстоянии фута или более. Возможно, вам придется поэкспериментировать с расстояниями, на которых отстоят друг от друга лазерная указка, промежуточный материал и стена, но если все сделано правильно, вы увидите полосы. Вероятно, это будет видно не так резко, как в серьезных физических экспериментах с лучшим лабораторным оборудованием, но вы получите полосы.

Природа частиц света доказана при проведении такого же эксперимента, хотя мы не можем с уверенностью увидеть это без специальной аппаратуры обнаружения, потому что каждый отдельный запущенный фотон будет обнаружен как одна частица непосредственно на щелях или при попадании на поверхность заднего фона. Применение для обнаружения частиц фотонных детекторов подтвердит, что каждый фотон проходит через щель и ударяет в фоновую поверхность как частица. Когда измерениям подвергаются все излучаемые фотоны при проведении многих и многих экспериментов, эффект всегда проявляется в наличии светлых и темных чередующихся полос, подтверждая волновые свойства света в очередной раз. Этот эксперимент доказывает, что свет (как и все квантовые частицы и молекулы) имеет двойственность волна–частица.

Примечание Если вы хотите увидеть реальные примеры этого эксперимента, зайдите на YouTube и введите в поисковике «волновой эксперимент с двумя щелями» или что-то в этом роде. Вы, как правило, найдете десятки видео, демонстрирующих эксперимент. Один такой отличный, анимированный пример эксперимента размещен на странице https://www.youtube.com/watch?v=fwXQjRBLwsQ.

Обнаружение странности

Теперь все становится действительно странным. Когда ученые помещают детекторы фотонов на одну или обе щели, чтобы установить, через какие щели фотон действительно проходит, фотон действует как частица и все волнообразное поведение немедленно исчезает. Позвольте мне повторить это. Перед тем как детекторы ставятся перед двумя щелями или сзади двух щелей, фотоны действуют как волны. А после того как детекторы установлены

и включены, по пока не понятной до конца причине фотоны сразу начинают действовать как частицы, как будто щель одна. Это как будто частицы сами видят процесс обнаружения и изменяют свое поведение. Ученые даже провели эксперименты, в которых они не включают детекторы до тех пор, пока фотоны не прошли через щель, а когда включают детекторы, оказывается, что фотоны ведут себя как частицы (когда, казалось бы, они должны были пройти через щели как волны). Как будто фотон задним числом корректирует в будущем свое начальное поведение в прошлом, основанное на начальном обнаружении. Мы не можем сказать, действительно ли это (то есть изменение прошлого) происходит или к какому времени это относится, прошлому или реальному. Что происходит и как, никто не знает. Мы знаем только то, что поведение меняется каждый раз, когда используется детектор, а что при этом происходит, нам пока понять трудно. Это явление известно как часть эффекта наблюдателя, который будет подробнее описан далее и выступает объяснением той истории изменения представления о свете, с которой начиналась эта глава.

Принцип вероятности

Понимание того, как электроны вращаются вокруг ядра, привело к лучшему пониманию того, как устроен наш мир, особенно на квантовом уровне. Например, будучи еще школьниками, мы все, наверное, узнали, что каждый атомный элемент состоит из электронов, протонов и нейтронов. Каждый атом (самая маленькая единица обычного вещества) состоит из ядра (состоящего из положительно заряженных фотонов) и (без заряда) нейтронов, окруженных отрицательно заряженными электронами. Электроны «вращаются» вокруг ядра из-за электромагнитного притяжения. В начальной школе большинство из нас узнало, что электроны кружатся в орбитальных полосах, известных как оболочки.

В начальной школе, вероятно с целью упрощения, электронные орбитальные оболочки (см. рис. 1.3) показываются на атомном уровне, как правильные круги или, возможно, овалы, часто идеальные орбиты, подобные орбитам планет; но квантовая физика показала нам, что движение электронов не происходит по идеальным кругам или даже овалам. Электронные оболочки в форме ровного круга – плод чьего-то воображения, и сегодня такие рисунки используются исключительно для того, чтобы продемонстрировать наличие электронных оболочек, не углубляясь в детали. Но это не то, что происходит в действительности. Электроны вращаются вокруг ядра по более сложным схемам, продиктованным принципами квантовой механики и вовлеченным в процесс энергией. На рис. 1.4 показан двумерный репрезентативный пример орбит электронов вокруг ядра на определенном энергетическом уровне. Эти области вероятной орбиты известны как *атомные орбиты*, или *электронные облака*. Вероятностный характер процесса очень важен в квантовой механике и более подробно будет объяснен в следующем разделе.

Ситуацию несколько осложняет то, что никто не может заранее сказать, где конкретный электрон может оказаться на орбите в некоторый момент времени; можно только судить о вероятности того, что он окажется в опре-

деленных (прогнозируемых) атомных орбитальных областях. Не существует математического уравнения, которое могло бы убедительно доказать, что такой-то электрон будет точно в точке А в какое-то определенное время. Лучшее, что квантовая механика может сказать, – то, что когда вы попытаетесь найти эту точку А, выяснится, что электрон может оказаться в ней только с определенной вероятностью. И если вы проведете измерение много раз, появление этого электрона в точке А может быть предсказано лишь в процентах вероятности.

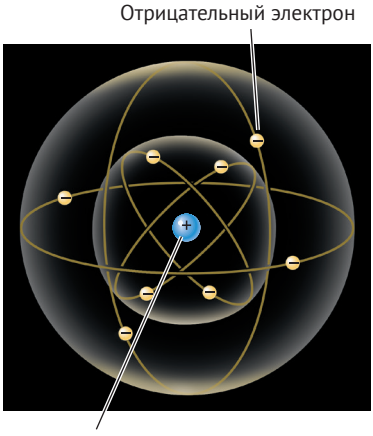


Рис. 1.3. Ядро атома, окруженное упрощенными орбитами электронов
Рисунок из книги: David Young, Shane Stadler. Cutnell & Johnson Physics, 11th Edition; *Wiley, 2018*

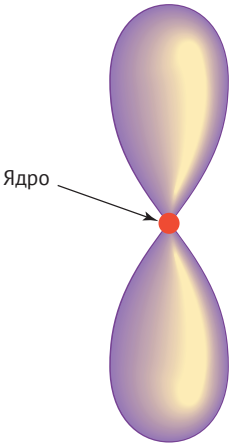


Рис. 1.4. Двумерная орбита атома для электронов, вращающихся по орбите

Принцип вероятности применим к любому свойству квантовой частицы, а не только к электронам. Нельзя угадать заранее не только состояние, их конкретные свойства или положение, но при измерении их состояние или

положение является во время любого одного измерения абсолютно случайной величиной в широких пределах вероятностного предсказания. И эта случайность конкретного ответа или состояния вовсе не случайна. Она является фундаментальным принципом, присущим квантовой механике. Ключевое отличие квантовой механики от традиционной классической физики состоит в том, что точное состояние или положение квантового объекта либо свойства не может быть точно предсказано заранее. В классической физике A + B = C и всегда будет равно C. Более того. Если я знаю A и C, я могу предсказать B. Но в квантовой механике точное место электрона на орбите, или свойства кванта, или размещение любой квантовой частицы может быть описано вероятностями и только вероятностями. Никто не знает заранее, каким будет какой-то один ответ при измерении. Известно лишь то, что будет одним из ряда возможных ответов, и если проводить измерения много раз, измеренные результаты будут соответствовать прогнозируемой вероятности. Это лучшее, что может сказать любой человек, завершая измерения.

Эти найденные и измеренные области возможных ответов и *вероятность* того, что электрон находится в определенном месте или с определенным квантовым свойством, могут быть точно предсказаны. Если вы запустите конкретный эксперимент с электроном снова и снова (скажем, тысячу раз), чтобы точно определить, где электрон был в конкретный момент времени, вы не сможете предсказать положение какого-либо конкретно измеряемого электрона в одном из этих измерений. Квантовая механика говорит, что любое одно измерение будет случайным событием. Но совокупность мест вокруг ядра, где в конечном итоге находился электрон, найденная и измеренная во многих экспериментах, создаст графическую схему, подобную соответствующим предсказаниям атомных орбит.

Несмотря на то что мы не можем знать точный ответ, диапазон возможных результатов измерения известен. Когда известна вероятность конкретного квантового состояния дискретной квантовой системы, это состояние описывается математической формулой, известной как *волновая функция*. Физики используют волновые функции для описания и предсказания того, что произойдет в широком диапазоне вероятностей при конкретном квантовом взаимодействии или конкретного свойства. Конкретный ответ для одного измерения неизвестен, но известен диапазон вероятных ответов и соответственно вероятность каждого возможного ответа. Волновая функция математически описывает все, что мы знаем о квантовой частице, включая все ее свойства, какими могут быть эти свойства и вероятность их появления при измерении. Волновая функция представляет для физиков полную карту квантовой частицы. Используя волновую функцию, ученые могут предсказать, что произойдет, когда различные частицы будут взаимодействовать друг с другом.

Этот принцип вероятности квантовой физики важен постольку, поскольку он означает, что мы не можем предсказать, каким будет какое-либо конкретное состояние квантового свойства до его измерения. В качестве очень упрощенной (не квантовой) иллюстрации предположим, что мы пытались определить, какого цвета была собака, черной или белой. С квантовой точки зрения, мы не можем определить заранее, до измерения, какого она была

цвета. Мы могли бы предсказать возможные ответы (например, «черная» или «белая») и даже вероятность того, что каждый ответ явится наблюдаемым ответом на основе некоторой заранее определенной математики (скажем, 50 % времени собака будет белой, а 50 % – черной, если мы проведем эксперимент много раз). Но нам придется подождать, пока собака не появится, чтобы увидеть, какого же цвета собака действительно наблюдалась и измерялась. И не только это, но и цвет собаки, определяемый в любой конкретный момент времени, будет случайным.

Примечание Это своеобразное квантовое свойство расстраивает физиков, склонных к классике, и делает квантовую механику столь настораживающей. В традиционной физике, если вы знаете все о вовлеченных объектах, знаете их свойства и их взаимодействие, вы всегда сможете заранее найти ответ или результат. Когда эксперимент закончится или результат будет получен, он будет соответствовать предсказанному ответу в соответствии с ранее полученными математическими соотношениями. «Это наука! Вот как она работает!» Квантовая механика, напротив, говорит, что независимо от того, насколько хорошо вы знаете математику, объекты и способы их взаимодействия, вы никогда не сможете предсказать конкретный ответ или квантовый результат в каком-либо одном эксперименте. Лучшее, что вы вообще сможете сделать, – предсказать вероятность различных ответов.

Ситуация даже сложнее. «Ответ», который дает нам квантовый компьютер сегодня (в 2019 году), может быть неправильным, и часто мы получаем неправильный ответ. Помните, квантовые ответы – это только ответы внутри данного диапазона вероятностей. Но если мы сможем запустить квантовый сценарий и получить квантовый ответ большое количество раз, мы можем получить правильный вероятностный ответ, так как получим просто правильный ответ чаще и последовательно в последовательном цикле экспериментов. По сути, чтобы получить правильный ответ, вычисления необходимо запускать снова и снова, пока возвращаемый вероятностный ответ не будет настолько статистически достоверным, что это должно и стать правильным ответом. Приведем аналогию из макроскопического мира. Предположим, что шестигранный кубик имеет смещенный центр масс, так что при подбрасывании одно из чисел на нем будет выпадать чаще других (так называемый загруженный кубик). Вы знаете, что смещение центра существует, но не знаете, в каком направлении относительно поверхностей кубика. Когда вы бросаете кубик один раз, он может лечь или не лечь в соответствии со смещением в сторону поверхности. Но когда вы подбрасываете его много раз, то, скорее всего, одно из чисел выпадет чаще, чем любые другие, подтверждая смещение с высокой достоверностью. Допустим, вы планируете подбрасывать загруженный кубик десять раз. Первый раз, когда вы бросаете, выпадает двойка. Теперь у вас есть ответ, но только с уверенностью 10 % (1 из 10 бросков). Вы подбрасываете кубик во второй раз и получаете единицу. Теперь у вас есть другой ответ, но тоже с уверенностью 10 % (1 из 10 бросков). На третьем броске вы снова получаете единицу и имеете 20 % уверенности

(2 из 10 бросков). На четвертом броске вы получаете пять. Затем в следующие пять подбрасываний получаете единицу, что дает вам 70 % уверенности (в 7 из 10 случаев выпадала единица). И при последнем подбрасывании вы получаете тройку. Всего у нас будет четыре разных возможных ответа, но одна сторона кубика была ответом наибольшее количество раз, и любой разумный человек придет к выводу, что сторона кубика с единицей – именно та, в которую смещен центр тяжести. В квантовом компьютере количество измерений и полученных ответов, скорее всего, будет много больше, чем десять раз, и соответственно будет получена максимальная вероятность правильного ответа.

Для любого отдельного измерения всегда, однако, велика вероятность, что оно дает неправильный ответ. И как бы настораживающе это ни звучало, так работают все квантовые измерения. И вы уже живете и выживаете в такой действительности с самого дня рождения.

Принцип неопределенности

Принцип неопределенности Гейзенберга гласит, что чем точнее измеряется положение квантовой частицы, тем менее точно может быть известен ее импульс, и наоборот. Неопределенность также применима к другим зависимым парам квантовых свойств (известных как *сопряженные переменные*), но не ко всем свойствам. Могут быть пары свойств, которые вы можете измерить одновременно, просто не у всех пар. Некоторые пары связаны друг с другом таким образом, что это мешает точно измерить оба свойства одновременно. Это не из-за некоторого изъяна в том, как человечество может или не может точно измерить что-либо. Это квантовый закон природы, проистекающий из двойственности волна–частица и принципа вероятности. Один из этих законов квантовой механики гласит, что вы не можете точно измерить обе позиции или импульс квантовой частицы в одно и то же время, и, когда вы пытаетесь более точно измерить одну величину, измерение другой величины этой зависимой пары становится менее точным.

Давайте воспользуемся еще одной макроскопической аллегорией – попыткой измерить скорость автомобиля. В макроскопическом классическом мире скорость автомобиля – это просто измерение пройденного расстояния за определенный временной период. Если машина проехала 100 километров ровно за 1 час, вы бы сказали, что скорость в среднем составляет 100 км/ч. Но в квантовом мире, при рассмотрении квантовых свойств очень маленьких частиц, обе переменные времени и расстояния вообще не фиксируются. Они меняются в диапазоне вероятностей, и любое отдельное измерение может привести к другому ответу из этого диапазона. Это делает измерение сложным с самого начала.

В нашем примере измерения скорости машины есть очень похожая аллегория, если в любом отрезке пути, по которому вы провели измерение, автомобиль движется быстрее и медленнее 100 км/ч. Действительно маловероятно, что какой-либо сложный объект с автономным питанием будет двигаться с одинаковой скоростью во все моменты времени. Чтобы определить скорость, с которой автомобиль двигался одну секунду, надо учитывать

сопротивление ветра, изменения в состоянии дорожного покрытия, изменения температуры и сотни факторов внутри самого двигателя, определяющие мощность и крутящий момент, которые он развивает в данный момент времени. Хотя если в конечном итоге получилось 100 км/ч на протяжении всего пути, то, конечно, его скорость, вероятно, была ровно 100 км/ч чаще, чем любая другая скорость.

Это и составляет принцип вероятности. Если измерять радаром скорость машины, то можно обнаружить, что в каждой точке пути машина имеет разную скорость, однако при окончательном результате 100 километров ровно за 1 час существует вероятность того, что скорость машины, равная 100 км/ч, была больше любой другой скорости в большинстве точек пути. Впрочем, всегда есть вероятность, что машина шла половину пути со скоростью ровно 98 км/ч, а затем другую половину пути – со скоростью ровно 101 км/ч, хотя это и менее вероятно.

Принцип неопределенности гласит, что чем большее время затрачивается для точного измерения скорости, тем одновременно менее точно может быть измерено расстояние, и нет никакого способа это исправить. В квантовом мире нет такого параметра, как высокая точность скорости. Как концепция он не существует. Это закон природы. Чтобы продолжить нашу скоростную аллегорию, предположим, что наши спортивные судьи захотели быть сверхточными, и для этого они решили заполучить лучшую в мире фотовспышку, чтобы фотографировать машину, когда она пересекает финишную черту. Чтобы уловить тот момент, когда машина пересекла черту, затвор камеры должен открыться и закрыться очень быстро. В эту микросекунду автомобиль будет «заморожен» во времени. На картинке в тот самый момент, когда машина пересекла черту, машина, кажется, не двигалась вообще. Финишную линию камера может запечатлеть точно в момент, когда машина пересекает линию, но в этот момент машина не будет двигаться (или двигаться очень заметно). Камере, пытаясь получить точный момент, когда время истекло, придется удалить скорость из измерения. И если бы вы имели другую камеру, которая измеряла истинную скорость автомобиля, она была бы не в состоянии точно запечатлеть момент, когда машина пересекла линию.

Усложним дело. Что собой представляет линия? Любая линия на макроуровне выглядит как прямая линия. Но увеличьте любую нарисованную или начерченную линию, и при увеличении проявятся ее отдельные, едва заметные неровности. Чтобы быть наиболее точным, вам нужно сделать снимок или нажать на секундомер точно в момент, когда автомобиль пересек первый атом нарисованной линии. И ваш глаз, и линза камеры должны будут щелкнуть точно, когда машина пересекла этот первый атом, а мы ведь не можем знать, в какой момент машина на самом деле пересекла первый атом финишной линии, пока этот момент не пришел к сетчатке глаза или линзе камеры. А это определяют фотоны и скорость света.

К тому времени, когда первый записывающий фотон придет, машина уже окажется за первым атомом относительно тех измерений, которые будут сделаны. Мы знаем, что этот первый атом состоит из субатомных частиц – электронов, протонов и нейтрино. Чтобы быть наиболее точным, вам придется остановить секундомер или запустить камеру тогда, когда автомобиль

встретит первый электрон на внешней орбите электронной оболочки первого атома, а мы, согласно квантовой теории, не знаем, где будет находиться этот первый электрон, а при одном отдельно взятом измерении он может находиться где угодно и оказаться не там, где будет его наиболее вероятное местоположение. В конечном итоге вы не сможете выполнить действительно точный расчет скорости, потому что вам нужно получить наибольшую точность атрибута (то есть электрона), который движется, а частица движется как волна в соответствии с волновой функцией. Пытаясь добиться большей точности, вы понимаете, что просто невозможно получить действительно точную меру чего-либо, тем более для сопряженных пар параметров, поскольку определение одного зависит от другого. Все движется во все времена (даже камень состоит из движущихся электронов), все является частицей и волной, все ведет себя по-разному, каждый результат конкретного измерения является случайным, и это может быть даже не «правильный» (наиболее вероятный) результат. И с сопряженными парами точное измерение одного значения зависит от другого, которое по определению должно измеряться менее точно. В нашем примере концепция «километр/час» (то есть положение и импульс) на самом деле на квантовом уровне не существует. Просто не существует. Это принцип неопределенности.

Вы должны понимать, что неопределенность в парах измерений не связана с отсутствием возможностей измерительного оборудования. Многие люди, впервые услышав о принципе неопределенности, думают, что это связано с несовершенством измерительной аппаратуры, которая недостаточно точна. Они полагают, что это связано с недостатком измерительных приборов. Это не так. Мы могли бы иметь самое точное измерительное оборудование, которое может очень точно (по нашим меркам) измерить время и расстояние, но это не имеет значения. Не то чтобы само измерение было неточным. Проблема связана с (квантовыми) законами природы, которые определяют, насколько точно мы можем измерить любое квантовое состояние, которое зависит от двух зависимых сопряженных переменных. Поскольку мы измеряем одну сторону зависимой пары более точно, просто невозможно так же точно измерить другую часть уравнения. Фактически это просто гарантированная инверсия отношения.

Примечание Принципы вероятности и неопределенности не должны быть истолкованы как означающие, что квантовая механика и квантовые свойства не могут быть математически точными. Наоборот, математика и результаты квантовой механики невероятно точны и имеют непревзойденный большинством других наук уровень доверия. Принцип неопределенности также не следует смешивать с эффектом наблюдателя, который будет обсуждаться ниже.

Спиновые состояния и заряды

Есть 12 *фундаментальных* квантовых частиц (также известных как *элементарные*), которые составляют всю материю во Вселенной. Фундаментальные частицы, как мы знаем, не могут быть разбиты на более мелкие, цельные

частицы. Познакомьтесь с ними, если вы не знали о них раньше. Названия некоторых из этих частиц довольно причудливы. Основными квантовыми частицами являются электрон, *мюон* (muon), *тау* (tau), *электронное нейтрино* (electron neutrino), *тау-нейтрино* (tau neutrino), *мюон-нейтрино* (muon neutrino) (все части семейства *лептонов*, lepton family) и *вверх* (up), *вниз* (down), *верхний* (top), *нижний* (bottom), *очарованный* (charm), *странный* (strange) (последние шесть являются частью семейства *кварков*, quark family). Фундаментальные квантовые частицы составляют все другие субатомные частицы. Например, каждый протон состоит из двух кварков *up* и одного кварка *down*. Нейтрон состоит из двух кварков *down* и одного кварка *up*. Электрон сам является элементарной частицей и не состоит из чего-либо. Электрон не содержит субатомных частиц, на которые его можно было бы разбить. Электроны, протоны и нейтроны составляют атомы, атомы составляют элементы и молекулы и т. д.

Примечание Мы никогда не можем быть уверены, что обнаружили каждую элементарную частицу или даже что существующие лептоны и кварки элементарны, хотя современная наука непреклонна в том, что это частицы с наименьшим общим знаменателем. Но из истории известно, что то же самое раньше говорили о клетках, атомах и протонах. Итак, кто знает, что мы обнаружим, когда попытаемся до конца разгадать ту грандиозную головоломку, которую являет собой реальность?

Каждая элементарная квантовая частица имеет массу, заряд и спин. Все понимают, что такое масса, так что давайте быстро обсудим два других. *Заряд* – это величина тока по сравнению с электроном. Например, у кварка *up* есть две трети заряда электрона, а у кварка *down* есть отрицательная треть заряда электрона. Поскольку у протона есть два кварка *up* и один кварк *down*, протон имеет 3/3 (2/3 + 2/3 – 1/3) заряда электрона, или точно равен заряду одного электрона. По этой причине в большинстве стабильных атомов число протонов в ядре равно числу орбитальных электронов. Элементарные частицы также имеют *спин*, обратно пропорциональный числу оборотов частицы, которые частица должна сделать, чтобы вернуться к своей первоначальной ориентации. Все элементарные частицы имеют спин одна вторая (one-half), что означает, что они должны провернуться дважды, чтобы вернуться в исходное положение. Почему я рассказываю вам о квантовых зарядах и спинах? Потому что ответы, которые мы получаем от квантовых компьютеров, часто являются результатом зарядов и спинов. Как мы увидим в главе 2 «Введение в квантовые компьютеры», для получения ответов в различных типах квантовых компьютеров используются различные квантовые свойства и состояния.

Квантовое туннелирование

Квантовое туннелирование – это необъяснимая способность квантовых частиц проходить через барьеры, что классическая физика признает невозможным. Общий макроскопический подобный пример – шар, находящийся у подно-

жия холма или стены. Предположим, что человек пытается перебросить мяч через стену, но у него не хватает на это физических сил. Он безуспешно пытается снова и снова. Классическая физика, изучив руку человека и силу всего тела, говорит, что человек никогда не сможет этого сделать. Но по причинам, которые невозможно объяснить, иногда бросок мяча удается, и мяч оказывается по другую сторону стены. Некоторые теории говорят, что мяч просто необъяснимым образом поднимается над стеной. Другие – что в какой-то момент стена опускается или мяч проходит через стену, не оставляя в этом месте следа.

Мы еще не знаем, как это работает и когда именно субатомная частица добьется успеха, вопреки всем своим предыдущим неудачным попыткам, но такое явление существует и является основой всей известной жизни. Туннелирование – это то, как наше Солнце генерирует тепло и свет с помощью термоядерного синтеза. Туннелирование – это то, как распадается радиоактивный элемент. Туннелирование является основой фотосинтеза, который поддерживает жизнь большинства растений на Земле, а заодно и человеческую жизнь. Квантовое туннелирование используется в некоторых типах квантовых вычислений.

Суперпозиция

Суперпозиция является квантовым свойством, которое говорит, что частица может существовать во всех возможных состояниях, пока состояние, наконец, не наблюдается и измеряется, чтобы дать один ответ. Например, скажем, конкретная математическая задача, на которую вы не знаете ответа, возможно, имеет ответ или А, или Б. Суперпозиция говорит, что до тех пор, пока ответ находится в квантовом состоянии, до того, как его можно наблюдать или измерить, он является в одно и то же время и А, и Б. Это не А или Б. Это и то, и другое.

Это связано с тем, что, как обсуждалось выше, при любом конкретном измерении квантового свойства результат может быть любым из диапазона возможных. И фактически полученный результат любого отдельного измерения может произвольным образом оказаться любым из возможных результатов. В классическом мире А – это А, а Б – это Б. Одна буква не может случайным образом оказываться то А, то Б. Но в квантовом мире именно это и происходит.

Возможно, вы слышали о знаменитой квантовой головоломке Эрвина Шредингера. Шредингер создал сценарий (мысленный эксперимент), в котором кота помещают в закрытую коробку с закрытой бутылкой смертельного яда, радиоактивным элементом и счетчиком Гейгера. Радиоактивный элемент мог распадаться или не распадаться. Радиоактивный распад является квантовым событием, и в момент, когда какой-либо конкретный атом элемента решает распасться – это случайное событие. Если счетчик Гейгера обнаруживает излучение (от радиоактивного распада), срабатывает система, разбивающая бутылку с ядом, и кот погибает.

Шредингер приводил этот мысленный эксперимент в качестве примера квантовой суперпозиции, наблюдаемой как макроскопическое событие,

чтобы продемонстрировать, насколько странной может быть суперпозиция, если представить ее на макроскопическом уровне. Шредингер пытался продемонстрировать, насколько курьезной выглядела в его времена квантовая механика при ее описании. Он проводил мысленный эксперимент не для поддержки квантовой механики. Он делал это, чтобы показать, насколько она абсурдна, и сообщить, что мы не понимаем, что происходит на самом деле. Если бы ученый дожил до наших дней, то, вероятно, посмеялся бы над тем, что его намеренно абсурдный мысленный эксперимент на самом деле наиболее часто используют в качестве наглядного примера того, как в действительности работает квантовая механика, потому что это было совсем не тем, что он тогда собирался продемонстрировать.

До открытия коробки для наблюдения за котом принцип суперпозиции гласит, что радиоактивный элемент и распался, и не распался. Кот для нас одновременно и жив, и мертв. В классическом физическом (реальном) мире кот в любой конкретный момент времени будет либо жив, либо мертв – или одно, или другое. А вот квантовая физика доказала на квантовом уровне: до тех пор, пока мы не посмотрим, открыв коробку, кот (в результате радиоактивного распада) и жив, и мертв одновременно, а не находится в каком-то половинчатом состоянии, при котором кот отравлен, но не полностью. Нет, это означает, что он и на 100 % здоров, и на 100 % мертв в одно и то же время! Что кажется бессмысленным на макроскопическом уровне, является абсолютной реальностью на квантовом уровне.

Если вы собираетесь понять квантовую механику и квантовые компьютеры, то должны воспринять понятие суперпозиции. Тут не приходится возражать, что вы иначе видите и понимаете мир, потому что на квантовом уровне мир будет именно таким. У меня ушло много времени на то, чтобы понять последствия мысленного эксперимента Шредингера. Я полагал, что когда мы открываем коробку, кот был жив или мертв, либо одно, либо другое, и так было с какого-то определенного момента времени. Но это не то, что говорит суперпозиция. Суперпозиция, которая была снова и снова доказана, говорит, что кот был и жив, и мертв, и пребывал в обоих состояниях, пока, наконец, не будет наблюдаться и измеряться. После того как «состояние» кота измерено, кот либо постоянно жив, либо мертв с этого момента и далее; это и будет результатом измерения при данном наблюдении. Такой результат ошеломил величайшие научные умы и до сих пор не перестает поражать. Тем не менее эксперимент за экспериментом подтверждает, что суперпозиция на квантовом уровне – это реальность.

Квантовая механика и, как следствие, квантовые компьютеры мгновенно генерируют все возможные ответы сразу, и пока не будет замечено и измерено, «правильными» являются все возможные ответы. Как только мы наблюдаем или измеряем ответ, только один ответ становится для нас постоянной реальностью.

Чтобы усложнить ситуацию, напомним: как отмечалось выше, никто не может предсказать, каким в итоге окажется этот наблюдаемый ответ. Никто не может сказать: «Конечно, кот мертв!» или «Конечно, кот жив!» – истинным будет только то, что кот до измерения и жив, и мертв, а в момент измерения будет жив или мертв при измерении, но только в пределах определенной ве-

роятности результатов, и среди возможных вариантов конкретный результат является при измерении случайным. Если чье-то предположение оказалось верным, то только потому, что этому человеку повезло (или сыграли свою роль вероятности). Если это сбивает вас с толку или уже слегка дурманит вам голову, учтите: мы еще даже не дошли до самых странных мест. Так что «оставайтесь на линии».

Эффект наблюдателя

В квантовом мире простое наблюдение квантовой системы меняет ее, хотя квантовые физики не знают, почему, или не согласны в этом друг с другом. Десятилетия экспериментов показали, что это свойство, как и все квантовые свойства, обсуждаемые в этой главе, является реальным и точным. Ученые не задаются вопросом, правда ли это, а ищут ответ на вопрос, почему или как это происходит. Например, в каждом эксперименте с двумя щелями, когда ученые помещают фотонный детектор, чтобы измерить, через какую щель проходит фотон, фотон всегда ведет себя только как частица (и результирующие волновые полосы не возникают). Если ученые выключат детектор, волновые полосы возвращаются. Как будто природа видит, что происходит измерение, оберегает и меняет то, что происходит. Возможно, она показывает нам не то, что происходит на самом деле, но это то, как мы описываем происходящее на основе наших экспериментальных наблюдений и результатов, потому что у нас нет других способов передать то, что мы видим. Мы еще не знаем, что происходит.

Это привело ко многим различным конкурирующим интерпретациям. Одна интерпретация говорит, что невозможно наблюдать за системой без какого-либо вмешательства в нее. Например, просто чтобы наблюдать за чем-то, часто требуется свет (то есть фотон) или какое-либо искусственно установленное оборудование для получения результата, и эти дополнения влияют на возможные квантовые результаты. На примере фотона: фотон должен «ударить» по тому, что измеряет, и отскочить назад к детектору (или нашему глазному яблоку), чтобы мы могли обнаружить это, и сам по себе «удар» *должен* вызвать какое-то взаимодействие.

Другая популярная интерпретация (*копенгагенская интерпретация*) говорит, что когда квантовая волновая функция многих вероятных возможностей наконец наблюдена и измерена, волновая функция «ломается» (это явление известно под названием *коллапс волновой функции*) и переходит в конечное состояние. Наблюдение, создающее в результате коллапс, является помехой. Чтобы понять копенгагенскую интерпретацию, вы должны еще раз убедиться, что вы понимаете и верите в суперпозицию, в то, что любой квантовый ответ или состояние из всех ответов или состояний до измерения является возможным одновременно. Акт измерения квантового сценария сводит все состояния или ответы в единый окончательный ответ или состояние. Это измерение сворачивает все одновременно возможные ответы в один окончательный, постоянный ответ (который может являться или не являться вероятностным «правильным» ответом и может не быть тем же самым ответом, если измеряется или наблюдается как-либо иначе).

Копенгагенская интерпретация имеет наибольшую поддержку в квантовом мире для объяснения, почему наблюдение чего-то меняет его. Хотя странность, присущая созданному Шредингером мысленному эксперименту «Парадокс кота в коробке», была именно тем, что ученый хотел продемонстрировать: насколько противоречит интуиции копенгагенская интерпретация с учетом того, чему мы верили ранее. Немногие ученые знали, что копенгагенская интерпретация не была даже близко к тому объяснению, в которое трудно поверить.

Другая интерпретация, «*Много миров*», гласит, что все возможные ответы относительно коллапса волновой функции принадлежат теперь другим вселенным и что каждый квантовый коллапс создает ряд новых вселенных, равных всем возможным ответам вероятностной волновой функции перед коллапсом. Вот это да! Теперь, учитывая, что вероятны триллионы и триллионы квантовых результатов каждую секунду, это создаст множество вселенных в огромном море многовариантности (*мультиверсов*, multiverses). Каким бы безумием это ни казалось, были проведены некоторые базовые эксперименты, включая тот, о котором стало известно в 2019 году (https://www.iflscience.com/physics/quantum-experiment-sees-two-versions-of-reality-existing-at-the-same-time/) и который поддерживает идею, что нельзя исключить квантовые мультиверсы. Большинство людей не верят тому, что объяснение множеством вселенных является правильным, но поскольку математика пока этого не исключает, кто знает!..

Эффект наблюдателя оказывает огромное влияние на квантовые вычисления. Мы хотим, чтобы наши квантовые компьютеры дали нам замечательные ответы на задачи, которые чрезвычайно трудно решить другим способом, но они должны быть изготовлены и работать, минимизируя или утилизируя эффект наблюдателя, чтобы при желании мы могли получать точные ответы.

Теорема об отсутствии клонирования

Родственным принципом, который невероятно важен для квантовой информатики, является *отсутствие клонирования*. Это теорема, в которой говорится, что квантовые состояния не могут быть скопированы напрямую. Вспомним, что измерение квантового состояния приводит это квантовое состояние в классическое постоянное состояние. И в соответствии с эффектом наблюдателя простое наблюдение или измерение квантового состояния меняет его. Это не значит, что «копирование» не может быть произведено, но это должно делаться косвенно. Подробнее об этом – в следующих главах. Теорема об отсутствии клонирования имеет много последствий для квантовых вычислений. Отрицательной стороной является то, что вы не можете создать резервную копию квантового состояния в середине квантового вычисления, как это можно сделать при работе с классическим компьютером. Это явление затрудняет копирование и исправление ошибок в квантовых компьютерах и сетевых устройствах. Но есть и положительная сторона: это отличное свойство для квантовой криптографии, предотвращающее многие сценарии подслушивания, которые намного проще создавать в классическом мире.

Жуткая запутанность

Теперь пришло время обсудить квантовое свойство, которое часто считается самым странным и досаждало Эйнштейну в последние дни его жизни. Квантовые частицы могут «запутаться» таким образом, что когда квантовое свойство (такое как поляризация, спин, импульс или заряд) одной частицы из пары изменяется, свойства другой пары частиц также немедленно изменяются предсказуемым образом, даже если две частицы разделены очень большими расстояниями. Мы не знаем, почему это происходит или как и почему Эйнштейн назвал это явление «жуткое действие на расстоянии» («spooky action at a distance»).

Примечание Запутывание – это только процесс измерения и чтения. Ученые знают, что когда они измеряют свойство одной частицы в паре, другая частица в паре будет иметь то же измеряемое значение. Но если ученые пытаются каким-либо образом манипулировать запутанными частицами, чтобы получить конкретное желаемое новое состояние – скажем, изменить свойство частицы с «0» на «1», – запутывание немедленно прерывается. Мы можем читать информацию, но не передавать ее. Реализация определенного желаемого состояния требует измерения состояния, а измерение состояния нарушает квантовые свойства.

В природе запутывание – естественный процесс. Это происходит всякий раз, когда любая квантовая частица взаимодействует с другой квантовой частицей, – то есть фактически все время. Запутанность растет с каждой встреченной частицей. Это нельзя просто остановить. В конечном итоге запутывание приводит к созданию объектов, состоящих из многих частиц, зависящих теперь друг от друга. С точки зрения физики вы больше не можете говорить о любой запутанной частице как об одной частице. Каждое наблюдение должно быть получено из результатов измерения всех запутанных частиц, участвующих в этой запутанности. В реальном мире запутывания происходит много, притом очень быстро. Квант частицы может легко запутаться с миллиардом других квантовых частиц за миллионные доли секунды.

Хотя квантовые частицы всегда запутываются сами по себе, для целей квантового тестирования ученые намеренно создают или запутывают лишь небольшое количество квантовых частиц. Причина в том, что когда вы пытаетесь понять какой-то истинный результат в эксперименте, меньшее количество обычно дает больше. Рассчитывать выяснить что-то, что является результатом взаимодействия миллиардов частиц, – мечта из разряда недостижимых.

Таким образом, в экспериментах, где запутанность желательна, ученые будут усердно работать над тем, чтобы изолировать экспериментальную среду и предотвратить любое нежелательное запутывание, создав свои собственные запутывания в гораздо меньших масштабах. Экспериментальная запутанность может быть осуществлена многими способами; один из самых распространенных – взять один фотон с большой энергией и разделить его

на две части – два фотона с более низкой энергией. Есть несколько других распространенных методов запутывания, но их технически слишком сложно описать, и это не входит в задачу данной книги.

Что касается эксперимента, запутывание должно включать две очень близкие квантовые частицы. Ученым пока не удалось запутать две частицы, которые находятся далеко друг от друга, хотя расстояние все время увеличивается. Однажды запутавшиеся, две частицы могут быть перемещены очень, очень далеко друг от друга и все еще сохраняют переплетение своих связей. Хотя когда расстояние увеличивается, существует вероятность того, что взаимодействие запутанных частиц с другими запутанными частицами будет увеличиваться, затрудняя ученым или делая невозможным измерить то, чего они хотели от оригинальной частицы, – создать намеренное запутывание.

Ирландский физик Джон С. Белл усилил теорию квантовой запутанности в серии неоспоримых экспериментов, описание которых он опубликовал в 1987 году в своей основополагающей белой книге под названием «Описуемое и неописуемое в квантовой механике» (Speakable and unspeakable in quantum mechanics, https://web.archive.org/web/20150412044550/; http://philosophyfaculty.ucsd.edu/faculty/wuthrich/GSSPP09/Files/BellJohnS1981Speakable_BertlmannsSocks.pdf). Белл исключил «скрытые локальные переменные», которые, как предположил Эйнштейн, были другим возможным, более вероятным объяснением запутанности. Белл доказал, что скрытые местные переменные отсутствуют, что значительно усилило теорию запутывания и всю квантовую физику.

С тех пор его эксперименты повторялись с одинаковым успехом каждый раз и на разных квантовых частицах. Жуткая запутанность была продемонстрирована у фотонов, электронов, нейтрино и даже более крупных молекул, таких как «букиболлы» (buckyballs). Квантовая запутанность была даже продемонстрирована в макроскопических объектах, таких как алмазы (https://news.yahoo.com/two-diamonds-linked-strangequantum-entanglement-190805281.html). Хотя квантовым физикам вовсе не нужны картинки, чтобы поверить или доказать что-либо в квантовой механике, но тем не менее в июле 2019 года ученым удалось запечатлеть первую картину запутанных частиц (https://phys.org/news/2019-07-scientists-unveil-first-ever-image-quantum.html), которая одинаково сильно взволновала умы как ученых, так и не ученых.

Декогеренция

Последнее квантовое свойство, которое мы обсудим в этой главе, – это *декогеренция*. Это чрезвычайно важное в квантовой физике и вычислительной технике свойство. Это то, что мы и хотим иметь, и хотим избежать (до поры до времени). Когда квантовая частица или система находится в легко видимом наборе квантовых состояний, мы говорим, что она когерентна или находится в состоянии когерентности. Мы можем легко увидеть результаты ее квантового состояния, которое работает в соответствии со всеми вероятностными ответами волновой функции. Без жесткой изоляции среды любая квантовая частица или система начнет взаимодействовать и запутываться с другими квантовыми частицами. Фактически это миллиарды и миллиарды

взаимодействий в микросекунду. Это происходит даже в том случае, когда мы можем считать, что она находится в вакууме. Например, когда ученые создают искусственный вакуум внутри замкнутого пространства без света или других преднамеренно введенных квантовых частиц в нем, аппарат, используемый для создания вакуума, будет выщелачиваться в вакуум. Это неизбежно. Без экстремальных условий это происходит очень часто и очень быстро. При самых лучших условиях это все же еще случается. Этого нельзя предотвратить.

Каждое нежелательное взаимодействие вызывает запутанность, и теперь ученые, пытающиеся исследовать одну или несколько частиц либо свойств, должны иметь дело с результатами, полученными из более сложных сочетаний многих частиц, чего обычно они не хотели бы. Оригинальные частицы, с которыми они работают, присутствуют, но могут быть легко потеряны среди моря других запутанных частиц, и в таком случае ученым нелегко понять влияние или результаты для исходных частиц, которые они наблюдали и хотели измерить.

Представьте, что вы хотели последовать за одной каплей воды и она упала в океан. Или вы хотели следовать за одним фотоном на пляже в солнечный день. Капля воды все еще будет в океане, но теперь она рассеяна среди триллионов и триллионов других капель. Вы все еще могли бы следовать за исходной каплей, но это было бы очень сложно. Вы могли бы отслеживать свой оригинальный фотон на пляже, но не в условиях, когда он не только теряется среди триллиона других фотонов, но и взаимодействует с другими фотонами и другими, как микро-, так и макрочастицами (например, пыль, воздух, ветер). Для любых практических целей уже после нескольких взаимодействий было бы трудно отследить какую-либо отдельную частицу и выяснить, что вызывали или не вызывали все другие запутывания.

Из-за этого для квантовых экспериментов и внутри квантовых компьютеров и других устройств внутренние структуры должны быть очень хорошо изолированы от внешнего мира. Ученые, изучающие кванты, хотят предотвратить столько нежелательного запутывания, сколько в человеческих силах. Используют стерильные поверхности с применением одного стабильного элемента, холодные температуры и предельную защиту от внешнего мира. Но когда ученые или механизмы теряют способность отслеживать исходную частицу или свойство/свойства частицы и выяснить первоначально желаемый результат (который в конечном счете, несмотря ни на что, всегда будет получен), квантовая частица или система рассматривается как декогерентная или находящаяся в состоянии декогеренции. Важно отметить, что квантовость частицы или системы не превратилась во что-то еще. Она ни в коей мере не стала неквантовой/классической. Просто отслеживание и понимание происходящего значимым образом стало слишком трудным для наших скудных умов и оборудования.

Иногда декогеренция нам необходима. В квантовой информатике, когда мы хотим получить квантовый ответ и можем записать и обозначить результат, мы должны измерить его, а его измерение все это запутывает и меняет. Каким бы ни было измерительное устройство, оно также состоит из квантовых частиц и свойств и должно взаимодействовать с измеряемой частицей или

свойством. Даже если измерение включает в себя только свет, а свет состоит из фотонов, для того чтобы фотон дал результат и сообщил об этом, он должен «ударить» частицы и отскочить назад. Теперь этот фотон запутан с тем, что он измерял. Таким образом, само по себе измерение будет декогерировать квантовую систему. Это не внезапное изменение квантового состояния в нечто неквантовое, просто это сразу усложняет измерение.

Но тем не менее, чтобы записать квантовый результат конкретного эксперимента или вычисления, мы должны измерить его. Итак, мы хотим проводить измерения, когда и где декогеренция контролируется и минимизируется без того, чтобы измерительная аппаратура декогерировала эти измерения. Нам нужно провести измерения и декогеренцию, чтобы мы могли получить окончательное измерение и ответ. Мы не хотим, чтобы ответом было: иногда A, а иногда B. Нам нужно стабильное значение результата для записи. Можно ли представить, что каждый раз, когда нам нужен ответ, мы просто говорим «это диапазон всех возможных ответов в пределах их вероятностей» и остановиться на этом? Мы не могли бы просто сказать, что машина двигается со скоростью 100 км/ч. Мы должны были бы сказать, что это будет скорость где-то от 0 до 200 км/ч (или до другого возможного максимума), и представить вероятности. Это был бы бездумный способ описания мира, особенно когда все понимают, что машина, которую считают движущейся со скоростью 100 км/ч, вероятно, не будет все время ехать со скоростью 100 км/ч. Мы рассчитывали бы в конечном счете получить наиболее вероятный «правильный» ответ, а не некий спектр ответов, соответствующих математике волновой функции. Следовательно, мы хотели бы преднамеренно декогерировать систему только на время необходимого измерения. Мы хотим избежать декогеренции системы до измерения, и как только получим необходимое измерение, она может иметь любую декогеренцию, какая ей нравится. Хотя ученые также хотели бы и пытаются делать несколько измерений без декогеренции системы. Одна из самых больших проблем, если не самая большая, при получении научной информации о квантах – система должна быть защищена от преждевременной декогеренции, пока не проведено окончательное измерение.

Существует много других свойств, принципов и теорий центральной квантовой механики, таких как контекстуальность, которую мы могли бы обсудить, но то, что мы уже обсудили, является отличной основой для главы 2 «Введение в квантовые компьютеры».

Квантовые примеры в современном мире

Хотя квантовая механика в основном проявляется на субатомном уровне, ни одна из реальностей нашей жизни не была бы возможной без реального существования и воздействия квантовой механики. Квантовая механика заставляет Солнце светить, является причиной, по которой материя составляет целое, и выступает основой большинства вещей, которые мы наблюдаем на макроскопическом уровне. Когда вы видите докрасна раскаленную печь, это возможно только из-за наличия квантовых эффектов. Квантовая механика

отвечает за наши компьютерные микропроцессоры, транзисторы, резисторы и любые интегральные схемы. Дисковое хранилище и сетевые коммуникации возможны только в силу существования квантовой механики. Ваше соединение Wi-Fi не могло бы работать без существования квантовых свойств.

Вот другие объекты и явления макроскопического мира, которые возможны лишь непосредственно в связи с существованием квантовой механики:

- волоконно-оптические кабели;
- лазеры;
- сверхпроводимость;
- сверхтекучие жидкости;
- атомные часы;
- магнитно-резонансная томография (МРТ), –

и не забудем главную причину появления этой книги: квантовые компьютеры и квантовая криптография.

Все эти замечательные вещи, да и вся наша реальность существуют и действуют только в силу невероятных и странных причуд квантовой механики. Я расскажу больше о том, как помогает нам квантовая механика, в главе 5 «Каким будет постквантовый мир?».

Для дополнительной информации

Область квантовой физики огромна. Темы, рассмотренные в этой главе, в действительности представляют собой только вершину айсберга. Каждая отдельная тема освещается в десятках, а иногда и сотнях документов и книг. Никакая книга, белая книга или учебник не могут продемонстрировать справедливость квантовой механики. Любой, кто хочет узнать больше, должен просто выбрать ряд источников и постепенно погружаться в них. Часто требуется внимательно прочесть или пролистать несколько таких источников, прежде чем начнут проясняться хотя бы основы. С учетом сказанного, вот некоторые из моих любимых ресурсов, с которых может начать любой новичок в области квантовой физики:

- *Aaronson Scott* (2013). Quantum Computing Since Democritus. Cambridge: Cambridge University Press.
- *Bell Philip* (2018). Beyond Weird: Why Everything You Knew About Quantum Physics Is Different. Chicago: University of Chicago Press.
- *Orzel Chad* (2009). How to Teach [Quantum] Physics to Your Dog. New York: Scribner.
- *Orzel Chad* (2018). Breakfast with Einstein: The Exotic Physics of Everyday Object s. Dallas, TX: BenBella Books, Inc.
- Dr. Mark G. Jackson's Articles for Popular Audiences. http://physicsjackson.com/articles/.
- Quantum Physics Blog. https://www.techbubble.info/blog/quantum-physics.
- Scott Aaronson Blog. https://www.scottaaronson.com.
- Dr. Scott Aaronson's Democritus online courses. https://www.scottaaronson.com/democritus/.

- YouTube. Quantum Theory—Full Documentary HD. https://www.youtube.com/watch?v=CBrsWPCp_rs.
- YouTube. Quantum Physics for 7 Year Olds. https://www.youtube.com/watch?v=ARWBdfWpDyc.
- YouTube. Neil deGrasse Tyson Explains Quantum Entanglement. https://www.youtube.com/watch?v=q8CQAOwi2RI.

Если вы хотите узнать больше о квантовой механике, перейдите на YouTube и/или Amazon и введите в поиск «физика квантовой механики» – вашему вниманию будут предложены сотни вариантов.

Резюме

Если это ваше первое знакомство с квантовой механикой, я надеюсь, что для начала мне удалось показать ее дивную странность. Не стесняйтесь вернуться к этой главе и перечитать ее, даже после того как следующие главы расширят ваше представление о квантовой механике. Квантовые компьютеры используют такие невероятные свойства, как запутанность, неопределенность и суперпозиция, чтобы дать нам ответы, которые просто невозможно получить на традиционных бинарных компьютерах. В главе 2 «Введение в квантовые компьютеры» мы обсудим, как работают квантовые компьютеры и устройства, чтобы дать нам невероятные ответы и решения, на которые можно положиться, и рассмотрим современные достижения в этой области.

2 Введение в квантовые компьютеры

Квантовые компьютеры, аппаратура и программное обеспечение для преобразования, создания и обработки данных используют особые свойства квантовой механики, описанные в главе 1. Все эти странные и удивительные квантовые свойства, такие как суперпозиция и жуткая запутанность, полностью проявляются в квантовой информатике. В главе 2 приводится описание квантовых компьютеров, разбирается их отличие от традиционных компьютеров, рассмотрены различные типы квантовых компьютерных архитектур и перечислены компании, которые их производят.

В чем отличие квантовых компьютеров?

В этом разделе будет показано, чем квантовые компьютеры отличаются от традиционных бинарных классических компьютеров. Мы начнем с изучения разницы между битами и кубитами (q-bit).

Традиционные компьютеры используют биты

Традиционные компьютеры для хранения, передачи и преобразования данных используют двоичные цифры (0 или 1). Бит (двоичная цифра) может быть только в одном из двух состояний: это либо единица, либо ноль. Включен или выключен. И одновременно может быть только одно состояние. Существо двоичной природы состоит в том, что частицы (например, электроны или фотоны, или другие частицы) преобразуются как целые частицы. С момента появления цифровых компьютеров вплоть до изобретения квантовых компьютеров это был единственный способ преобразования цифровой информации. Квантовые компьютеры позволяют нам преобразовывать частицы недвоичным образом, используя их квантовые свойства.

В основе работы традиционных компьютерных чипов лежат принципы квантовой механики. Однако эти чипы могут преобразовывать и перемещать электроны между различными логическими элементами в подвергнутых воздействию легированных (то есть имеющих намеренно внедренные желаемые примеси) полупроводниках, только в двоичном виде. Измеряемые целые электроны, которыми они манипулируют, находятся в одном из двух состояний, которые равны 1 или 0. Традиционные компьютеры не измеряют вращение, поляризацию или любые другие возможные квантовые свойства.

Поскольку бит в один момент времени может представлять только одно из двух состояний, мы можем легко подсчитать, сколько битов необходимо для представления определенного количества информации. Например, 1 бит может содержать две разные частицы информации (то есть 0 или 1), но это будет всегда 1 бит информации: до, во время и после измерения. Два бита могут быть четырьмя различными возможными частями информации (т. е. 00, или 01, или 10, или 11), но при измерении будут представлять только 2 бита информации. Три бита могут содержать восемь возможных различных частей информации (то есть 000, или 001, или 010, или 100, или 010, или 011, или 110, или 111), но при измерении будут представлять только 3 бита информации и т. д. Каждая дополнительная бинарная цифра дает экспоненциальный рост возможностей (2^4, 2^5, 2^6 и т. д.).

Ранние компьютеры были напрямую запрограммированы путем включения или выключения отдельных битов с помощью физического манипулирования. У них были физические, электрические перемычки, которые были или не были подключены в компьютере, чтобы создавать или не создавать определенное соединение. По одной из версий, термин «компьютерная ошибка» (computer bug) возник в связи с тем, что насекомые (bugs – жучки) перегрызали часть кабелей и вызывали ошибки программирования. Длинные, гибкие соединительные кабели были заменены встроенными механическими переключателями и программированием бумажных «перфокарт», которые по существу манипулировали внутренними механическими переключателями, чтобы изменить в компьютере двоичные пути. Даже сегодня многие компьютерные устройства имеют остаточные перемычки, такие как «включено» и «выключено», которыми пользователь может физически манипулировать и определять двоичные варианты конкретных путей или решений в компьютере.

Механические переключатели были заменены электронными ключами, что в итоге привело к появлению транзисторов, резисторов и микропроцессоров, которые на элементарном уровне просто вводят необходимое количество двоичных «логических элементов» в как можно меньшее пространство. Но независимо от того, сколько двоичных коммутаторов мы можем втиснуть на печатную плату или кусок кремния, все осуществляется в двоичном виде. Просто больше двоичных путей вписывается в меньшее пространство.

Компьютерные языки самого низкого уровня, такие как язык ассемблера, представляют только один уровень абстракции, устранивший необходимость непосредственного введения битов в микропроцессор компьютера. Например, на языке ассемблера команда MOV AH, 1 инструктирует микропроцессор компьютера перемещать двоичное значение 1 в регистр AH (регистры – области памяти микропроцессора, которые хранят и помогают манипулировать данными).

Каждый двоичный язык программирования в конечном итоге разбивается на двоичные инструкции, которые затем физически манипулируют электронами микропроцессора компьютера в предопределенных *булевых* логических элементах (И, ИЛИ, НЕ и т. д.). Классические компьютерные системы сверху донизу построены на двоичных манипуляциях и хранении двоичных данных, и это направило мир по безразмерному, неординарному пути. Все

бинарное поведение было основано на квантовых частицах и их поведении, но оно не использовалось для хранения и передачи информации или проведения вычислений.

Однако существуют ограничения возможностей двоичных компьютеров. Есть манипуляции, которые бинарные компьютеры или просто делают недостаточно хорошо, или не могут выполнить вообще. Или они недостаточно быстры, чтобы быть настолько полезными, насколько нам нужно. Например, двоичные компьютеры недостаточно быстры, чтобы решать факторные математические уравнения разложения на множители с участием больших простых чисел. Большие простые числа часто используются в цифровой криптографии (это объяснено подробнее в главе 3 «Как квантовые вычисления могут взломать существующие криптокоды?»). Простое число – это любое целое число, большее 1, которое не может быть разделено ни на одно число, кроме самого себя или 1 и равно целому числу (без остатка). Последовательные простые числа начинаются с 1: 2, 3, 5, 7, 11, 13, 17, 19, 23 и т. д.

Двоичные компьютеры позволили вычислять факторные математические уравнения разложения на множители с участием больших простых чисел, чего люди без них не могли бы делать. Но для факторных уравнений, включающих очень большие простые числа, такие как те, которые участвуют в компьютерной криптографии, двоичным компьютерам потребовалось бы от сотен до миллионов лет. Вначале, чтобы подтвердить кандидата на простое число, двоичные компьютеры, по сути, должны были бы изучить каждое возможное число, а затем сверить его с каждым предыдущим числом, прежде чем этот кандидат подтвердит, что простое число является простым. Некоторые компьютерные специалисты называют это «угадай и проверь». Это не очень эффективный метод подтверждения простых чисел. Были разработаны некоторые большие математические уловки и алгоритмы, которые позволяют классическим компьютерам подтверждать простые числа с меньшими усилиями, чем тактика «угадай и проверь», но даже они недостаточно мощны, чтобы позволить традиционным компьютерам легко решить уравнение с двумя очень большими простыми числами.

В других случаях бинарные компьютеры просто не могут делать то, что требуется. Казалось бы, такая простая операция, как генерация действительного случайного числа или случайной строки символов, для классического компьютера физически невозможна (подробности приводятся в главе 3). То, как он устроен, и способы, которыми он в состоянии производить вычисления, исключают такую возможность. Классические компьютеры пытаются моделировать цифры случайным образом, но лучшее, что они могут сделать, – это имитации. Они не являются действительно случайными, и это вызывает проблемы с программами, которые зависят от действительно случайных чисел. Подробнее об этом – в главе 7 «Квантовая криптография».

Есть множество проблем, которые традиционные бинарные компьютеры, работающие с любой возможной скоростью, не могут решить в разумные сроки или не способны решить вообще. Это просто физика… но физика до тех перспектив, которые открывают квантовая механика и квантовые компьютеры.

Квантовые компьютеры используют кубиты

Квантовые компьютеры вместо битов используют кубиты. *Квантовые биты* (сокращенно *кубиты*, или *q-биты*) имеют удивительное квантовое свойство суперпозиции. Одиночный кубит – это система с двумя состояниями (1 и 0). Но в связи со свойством суперпозиции перед измерением он может иметь все возможные состояния одновременно. В квантовых компьютерах кубит может быть равным как 0 или 1, так и 0 и 1. Это связано с волновой функцией квантовой частицы и присущим ей набором вероятных возможностей.

Кубит часто сравнивают с монетой, использующейся для определения команды, которая будет начинать игру первой в футбольном матче. Видя, что выпало на монете – орел или решка, – судья сообщает, кто будет начинать игру. Но после того, как судья подбросил монету, она, вместо того чтобы приземлиться на одну или другую сторону, показывая орла или решку, может упасть точно на ребро и, покачиваясь, оставаться в таком положении несколько секунд. Существует возможность видеть все три стороны монеты, прежде чем она упадет на одну плоскую сторону (т. е. предоставит результат для измерения). Окончательный результат, когда она наконец падает на какую-либо сторону, может быть и орлом, и решкой, но в момент задержки на ребре монета может быть прочитана в одно и то же время и так, и этак (т. е. проявит суперпозицию). Это не идеальная метафора, но она делает понятной идею суперпозиции и окончательного, взвешенного ответа.

Бит равен либо 1, либо 0. Кубит перед окончательным измерением является как 1, так и 0. Это означает, что его битовое состояние экспоненциально по отношению к себе и ко всем дополнительным кубитам, добавленным к нему. Один кубит может быть двумя состояниями одновременно (т. е. 0 и 1), а 2-кубитная система может представлять четыре состояния одновременно (т. е. 00 и 01, и 10, и 11). 3-кубитная система может представлять восемь состояний одновременно (т. е. 000 и 001, и 010, и 100, и 010, и 011, и 110, и 111) и т. д. 3-кубитная система представлена на рис. 2.1.

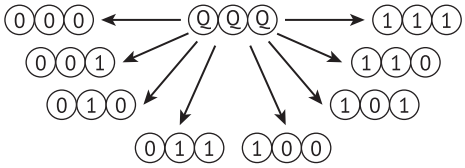


Рис. 2.1. Представление 3-кубитной системы

Для понимания кубитов важно то, что любое подобное число битов в двоичной системе имеет одинаковое количество возможных состояний, но в каждый момент времени только одно состояние. Бинарная монета никогда не может приземлиться на ребро. Таким образом, 3-битная система может вернуть только одно состояние/ответ в данный момент времени. 3-кубитная система может иметь все 8 состояний, участвующих в решении задачи, одновременно. 3-кубитная система – это 8-кратное улучшение состояния по сравнению с 3-битной системой. 4-кубитная система – 16-кратное улучше-

ние состояния по сравнению с 4-битной системой и т. д. Теперь представьте, что у вас есть тысячи кубитов, каждый из которых одновременно является системой с двумя состояниями, и из-за суперпозиции они являются всеми возможными состояниями тысяч кубитов одновременно. Скорость и логические возможности, как вы можете себе представить, фантастические.

Приведу лучший пример сравнения скоростей между битами и кубитами, который мне довелось услышать (не помню, от кого). Представьте, что мы хотим получить решение при каждом возможном ходе на шахматной доске. Шахматная доска имеет 64 квадрата (32 черных и 32 белых). Если бы каждый возможный ход был представлен полученным количеством рисовых зерен, необходимых для представления всех возможных ходов в шахматах, это создало бы гору риса размером с Эверест. А количество риса, необходимое, чтобы представить нечто подобное 2048-битному разложению на простые числа, равняется 1985 Эверестам из риса.

Теперь вы можете понять масштабы проблемы. Традиционному бинарному компьютеру либо потребуется очень, очень много времени, чтобы вычислить ответ, либо он никогда не решит такую задачу. Квантовый компьютер с несколькими тысячами кубитов может генерировать правильный ответ менее чем за две минуты. В этом сила квантовых компьютеров.

Кубиты возможны, потому что базовые объекты, используемые квантовым компьютером, являются квантовыми состояниями квантовых частиц. Традиционный двоичный компьютер может использовать электроны (или даже фотоны), но они создаются, управляются и измеряются как двоичные объекты или состояния. Они либо 0, либо 1, либо «вкл», либо «выкл». Квантовый компьютер, использующий квантовые частицы и измеряющий квантовые состояния этих частиц, видит все представленные квантовые состояния. Таким образом, измеряя состояние электрона, он видит все возможные состояния всех возможных квантовых свойств. При измерении частицы он видит все возможные состояния, такие как заряд, спин, полярность и т. д. Базовое состояние истинного квантового компьютера таково, что он может представлять все возможные состояния частиц одновременно, а не только двоичное состояние. В квантовом компьютере, в отличие от классических логических элементов, логическая единица известна как *квантовый логический элемент* (или просто *квантовый вентиль*). Квантовые вентили по своей природе способны на большее количество вариантов решения сложных проблем, чем классические логические элементы.

Примечание Несмотря на то что суперпозиция – это все возможные состояния одновременно, это не означает, что квантовые компьютеры могут мгновенно показать все возможные ответы на все возможные проблемы. Все компьютеры, включая квантовые, все еще должны вычислять и запускать программы для решения сложных проблем. Они получают каждый ответ не сразу. Есть необходимые вычисления и алгоритмы, которые необходимо выполнять, чтобы получить окончательный ответ. Но можно определенно сказать, что суперпозиция кубитов позволяет квантовым компьютерам решать многие проблемы быстрее, чем это делают традиционные компьютеры, а в некоторых случаях решения будут найдены настолько быстро, что

по сравнению с традиционными бинарными компьютерами это покажется мгновением.

Рост кубитов со временем

Первый квантовый компьютер с 1 кубитом был создан и продемонстрирован в 1998 году. С тех пор мы видим, что со временем число кубитов в квантовом компьютере растет. Вот график роста кубитов по годам на момент написания этой книги, основанный на заявлениях различных поставщиков:

- 2000: 5–7-кубитные компьютеры;
- 2006: 12-кубитный компьютер;
- 2007: 28-кубитный компьютер;
- 2012: 84-кубитный компьютер;
- 2015: 1000-кубитный компьютер;
- 2017: 2000-кубитный компьютер.

Примечание Как будет показано далее в этой главе, не все кубиты одинаковы. Некоторые их показатели, приводимые поставщиками, вызывают вполне оправданные сомнения.

Более полный список квантовых компьютеров с указанием их типа, поставщиков и количества кубитов приводится здесь: https://quantumcomputingreport.com/scorecards/qubit-count/. Как можно видеть, со временем количество квантовых состояний, представленных в квантовом компьютере, экспоненциально увеличивается. Нет никаких оснований сомневаться, что этот экспоненциальный рост будет продолжаться в будущем, так же как число интегральных схем в определенном пространстве в традиционных бинарных компьютерах удваивается каждые два года (как и предсказано законом Мура).

Это не означает, что экспоненциальный рост кубита гарантирован. Есть значительные проблемы, которые нужно преодолеть в масштабах квантовых компьютеров, как в краткосрочной, так и в долгосрочной перспективе. Но вполне вероятно, что ученые, занимающиеся квантовыми компьютерами, решат эти задачи, и с течением времени будет добавляться все больше и больше кубитов. Когда раздаются голоса критиков роста кубитов, полагающих, что мы уже достигли некоторого гораздо меньшего произвольного предела или что будущие достижения потребуют десятилетий, следует вспомнить тех критиков, которые утверждали, что в традиционные микропроцессоры невозможно добавить классические вентили. Каждый год «эксперты» рассказывают миру, что наконец достигнуты технические ограничения по количеству классических логических элементов в заданном пространстве одного компьютерного чипа, но в следующем году их становится больше. Производители чипов разработали или усовершенствовали некоторые технологии, которые позволяют им втиснуть больше вентилей в заданное пространство. Всегда появляется что-то, чего скептики не учитывают в своих расчетах. Сегодня у нас чрезвычайно быстрые 32/64-процессорные ядра, которые раз-

мещаются в одной микропроцессорной матрице. У квантовых критиков сейчас, может быть, стало больше опыта и математических расчетов, чтобы утверждать, что добавлять все больше кубитов в одно пространство однажды станет невозможным, но пока их количество понемногу растет. Мы еще не настолько близки к возможному максимуму. Мы еще только на первом фундаментальном уровне.

Не все кубиты равны

Важно признать, что квантовый компьютер с наибольшим количеством кубитов не обязательно самый быстрый и лучший. Наличие большего количества кубитов, безусловно, хорошо, но кубит кубиту рознь, и способность квантовых компьютеров решать что-либо определяется бóльшим количеством переменных, чем просто огромное количество кубитов. Некоторые типы квантовых компьютеров, как мы увидим позже в этой главе, лучше справляются с решением определенных типов задач.

Иные квантовые компьютеры независимо от того, сколько у них кубитов, не могут решить некоторые типы задач. Здесь можно провести сравнение с гоночными автомобилями. Мы можем создавать действительно быстрые машины, которые могут развивать скорость до 500 миль в час, но только при движении по прямой в течение нескольких минут. Такие машины похожи на горизонтальные ракеты и могут промчаться много миль, но только по прямой на очень ровной дороге. Они никогда не будут конкурировать с автомобилями NASCAR на овальной гоночной трассе в гонках, которые длятся часами. Каждый тип автомобиля разрабатывается для победы в конкретном типе гонок.

То же самое и с квантовыми компьютерами. Каждый базовый тип квантового компьютера оптимизируется для решения конкретного типа задач. И квантовые компьютеры, предназначенные для решения широкого круга задач, не будут так же быстро решать конкретные типы задач, как определенные типы квантовых компьютеров, сфокусированные на решение эксклюзивных задач.

Квантовая мощность – это больше, чем кубиты

Большее количество кубитов может сделать конкретный квантовый компьютер быстрее, но это отнюдь не гарантировано, так же как более высокая мощность автомобиля не всегда означает, что он выиграет гонку. Успех гоночной машины зависит от всего, что заставляет ее двигаться вперед быстрее, чем другие машины, включая двигатель, впрыск топлива, шины, трансмиссию и преобразование крутящего момента. То же самое с квантовыми компьютерами. Увеличение количества кубитов редко может причинить вред, но многие другие факторы могут ограничивать скорость.

IBM, ведущая компания в области квантовых вычислений, долгое время занимающаяся квантовыми компьютерами, поняла это еще на ранних этапах, увеличивая количество кубитов в таких компьютерах, в то время как у нее понемногу появлялись конкуренты. Компания IBM признала необходимость разработки метода, который мог бы использоваться для независимого сравнения мощности и скорости различных квантовых компьютеров. В итоге

была создана метрика, которую IBM назвала *квантовым объемом* (quantum volume). Он приравнивается к количеству квантовой работы, выполняемой конкретным типом квантового компьютера за определенный период времени. По данным IBM, вопросы, связанные с определением квантового объема, включают различные факторы, в том числе количество кубитов, связность (между кубитами и другими компонентами), время когерентности, а также учет ошибок затвора и измерений, перекрестных помех устройства, эффективность компилятора программного обеспечения. Институт инженеров по электротехнике и электронике (IEEE) предложил независимый стандарт PAR 7131 (Standard for Quantum Computing Performance Metrics & Performance Benchmarking, стандарт показателей производительности квантовых вычислений и сравнительного анализа производительности, https://standard.ieee.org/project/7131.html), в котором сделана попытка измерять, тестировать и сравнивать квантовую производительность: он включает в себя многие из тех же квантовых переменных, что и в квантовом объеме, но также добавляет к его критериям «время затвора, возможности генерации и считывания и точность затвора».

В работающем компьютере аппаратное обеспечение – только одна часть уровня производительности. Квантовые компьютеры, как и традиционные, для решения задач имеют программное обеспечение. Последнее, в виде аппаратной прошивки или программ, также оказывает влияние на общую производительность. Некоторые ученые предложили создать «квантовые головоломки», которые каждый из конкурирующих между собой квантовых компьютеров будет решать, а люди будут фиксировать время, которое понадобилось для решения. Головоломки должны быть различными для каждого основного типа квантового компьютера (они оптимизированы для решения различных типов проблем). К сожалению, любой поставщик квантового компьютера, оказавшегося не на первых местах при тестовом сравнении результатов, найдет миллион доказательств тому, что его квантовый компьютер был несправедливо ограничен условиями конкурса. То же самое всегда происходило с традиционными бинарными компьютерными тестами. Но показатели скорости не следует полностью сбрасывать со счетов. Они служат ценным критерием при некоторых сценариях.

Ключевой момент – понимание того, что количество кубитов само по себе не показатель выдающегося качества или скорости работы квантового компьютера, хотя в целом большое количество кубитов никогда не повредит. Прямо как в нашей автомобильной аналогии, если, например, вы начнете конкуренцию с другими производителями быстрых автомобилей, просто наращивая количество лошадиных сил. Одни только лошадиные силы выиграть гонку не помогут.

Квантовые компьютеры еще не готовы к прайм-тайму

На момент написания книги, в 2019 году, ни один из существующих квантовых компьютеров не работает быстрее, чем любой традиционный бинарный компьютер. Даже не приближается к этому. Не исключено, что у вашего но-

утбука более высокая производительность. На данный момент лучшее, что могут квантовые компьютеры, – продемонстрировать в небольшом масштабе квантовые свойства, способные в будущем решить проблемы, которые традиционные бинарные компьютеры решить не могут. И наоборот, традиционные бинарные компьютеры часто могут эмулировать или моделировать квантовые решения, нередко лучше, чем современные квантовые компьютеры. Но важно понимать, что хотя двоичные компьютеры могут моделировать квантовую механику, они не квантовые, и однажды их, скорее всего, обойдут чисто квантовые компьютеры; вопрос только, когда.

Квант скоро будет царствовать

В какой-то момент квантовые компьютеры смогут решать проблемы, которые традиционным компьютерам не под силу решить – а даже если и под силу, квантовые будут делать это значительно быстрее. Это время известно как *квантовый примат* (quantum supremacy, *квантовое превосходство*, термин, придуманный в компании IBM). Мы, кажется, очень близко подошли к такому моменту.

Многие компании полагали и публично заявляли, что они достигли квантового превосходства или близки к нему. Google, Intel и правительство/компании Китая объявляли, что они либо достигли квантового превосходства, либо подошли к этому рубежу. В 2017 году IBM, основываясь на ежегодном удвоении квантового объема, выдала прогноз, согласно которому квантовое превосходство будет достигнуто к 2020 году. Возможно, какой-нибудь квантовый компьютер в мире достигнет квантового превосходства еще до того, как эта книга будет издана. С другой стороны, есть некоторая вероятность существования какого-то непредвиденного технологического блокировщика, который вообще никогда не допустит квантового превосходства. Или, возможно, бинарные микропроцессоры явят миру потрясающий технологический прорыв, который снивелирует прогресс, который продемонстрировали квантовые компьютеры.

В течение нескольких лет в достижение квантового превосходства вкладываются серьезные деньги. Многие годы лучшие в мире компьютеры не могли одолеть лучших игроков в шахматы. Но наконец в 1996 году IBM-компьютер Deep Blue победил чемпиона по шахматам Гарри Каспарова. Много лет компьютер не мог побить человека в телеигре Jeopardy. Так было до тех пор, пока в 2011 году компьютер Watson IBM не сделал это. Квантовое превосходство обещает продвижение по тому же пути. Вокруг этого много рекламной шумихи, но в конечном итоге это произойдет. Вопрос не в «если», а в «когда».

СЦЕНАРИЙ АЛЬТЕРНАТИВНОГО КВАНТОВОГО ПРЕВОСХОДСТВА

Альтернативный сценарий квантового превосходства – это когда квантовые компьютеры начнут решать проблемы, которые не могут быть логически решены бинарными, причем не обязательно из-за недостаточной вычислительной мощ-

ности. Теоретически квантовые компьютеры могут эффективно решать любые классические задачи (хотя не всегда так же эффективно, как бинарные компьютеры), но обратное утверждение неверно. Классические компьютеры не могут решить все проблемы, которые под силу квантовым, по крайней мере за практически приемлемое время. Возможность альтернативного сценария квантового превосходства возникает там, где квантовые компьютеры не «быстрее» двоичных компьютеров, а просто способны решать проблемы, которые двоичные компьютеры неспособны решать. Большинство квантовых экспертов ожидают, что даже в этом отношении квантовые компьютеры со временем станут более способными и быстрыми.

Квантовые компьютеры улучшают кубиты, используя исправление ошибок

Многие эксперты по квантовым вычислениям говорят, что теоретически мы можем достичь квантового превосходства при 40–50 совершенных кубитах или не более 100 совершенных кубитах. По одной из оценок, квантовые компьютеры «могут составить карту всей информации во Вселенной от Большого взрыва и далее», используя всего 300 идеальных кубитов. К сожалению, совершенные кубиты пока ускользают от нас. Они полны ошибок, особенно в масштабах. В этом разделе будут рассмотрены некоторые способы, которые ученые в области квантовых вычислений пытаются применить, чтобы сделать кубиты лучше, включая улучшение времени когерентности, сильное охлаждение, контрольные кубиты и увеличение производительности других компонентов.

Преждевременная декогеренция кубитов

Без сомнения, самой большой проблемой квантового превосходства является преждевременная декогеренция кубитов. Как определено в главе 1, *декогеренция* – это состояние квантовой частицы, переходящее от легко наблюдаемой суперпозиции (т. е. мультисостояния) к ее окончательному, измеренному, единственному, классическому состоянию, прежде чем все возможные запутывания сделают невозможным получение полезной информации. Как только декогеренция произошла, преждевременно или нет, это уже нелегко изменить. Попробуйте вытащить определенную каплю воды обратно из океана или выделить один фотон в яркий солнечный день и выяснить все последствия его прошлых запутанностей!

В «совершенных» квантовых компьютерах декогеренция будет происходить в одной только точке, в которой «ответ» необходим и измерен. Это всегда будет целью. Кубит останется в своем когерентном состоянии столько времени, сколько необходимо для квантового расчета, и когда измерение сделано – и только тогда – произойдет декогеренция.

Примечание Предположим, что кубит имеет состояние 1, которое компьютер должен удерживать для выполнения вычислений или получения результата. Время когерентности (иначе – согласованности) показывает, как долго кубит будет стабильно поддерживать то, что является 1. Оно часто измеряется в миллисекундах, но в некоторых типах квантовых компьютеров длится от секунды до многих минут. Первая задача большинства производителей квантовых компьютеров – увеличение времени когерентности. Увеличенное время когерентности означает меньшее количество ошибок при большем времени вычисления и получения ответов.

Современные квантовые компьютеры полны преждевременной квантовой декогеренции и просто ошибок. И то, и другое может произойти из-за конструкции кубита, тепла, излучения, шума, вибрации, неисправных вентилей, неисправных измерителей, неправильной подготовки начального состояния, фонового ядерного спина и множества других событий. По сути, любое взаимодействие с внешним миром представляет собой угрозу. Уменьшение ошибок и шума является квантовым вызовом номер один. Он породил область, которая получила название *коррекция квантовой ошибки*. Для исправления ошибок предпринимаются попытки с использованием множества различных схем, включая как квантовые, так и классические методы. Никто еще не достиг совершенства, но каждый поставщик квантовых вычислителей пытается это сделать.

Частота появления ошибок обычно указывается как отношение времени квантования ко времени декогеренции. *Теорема о пороге квантовой ошибки* гласит, что любую квантовую систему, которая исправляет ошибки быстрее, чем их создает, можно использовать. По мере увеличения числа кубитов естественно увеличивается и частота ошибок. Чтобы квантовый компьютер был полезным, частота его ошибок должна быть ниже 1 %, а реально ниже 0,001 %. Для сравнения, классический процессор может выполнять триллионы вычислений без ошибок. В квантовом мире мы лишь надеемся снизить частоту ошибок до одной ошибки на тысячу вычислений. Лишь достижение этого, наряду с правильностью исправления ошибок, позволит вести серьезную квантовую работу. В 2019 году мы этого еще не достигли.

Примечание Классические компьютеры тоже допускают ошибки. Разница в том, что обычно в классическом мире для ошибок требуется большее количество происходящих событий. Приведу образное сравнение. Представьте, насколько большой порыв ветра необходим в классическом мире, чтобы перевернуть пенсовую монету (то есть бит), лежащую на земле. Но в квантовом мире требуется всего лишь небольшой ветерок, чтобы положить на землю пенни, стоящий на ребре (то есть кубит).

Ученые по квантовым вычислениям пытаются уменьшить квантовые ошибки, выявляя и исправляя наиболее значимые ограничивающие скорость компоненты или проблемы. Общие решения включают улучшение времени когерентности, строго изолируя квантовые компоненты от внешнего мира, используя сильное охлаждение и проверяющие кубиты, увеличивая произво-

дительность других компонентов, чтобы предупредить ошибки, и применяя квантовую запутанность как средство исправления ошибок.

Улучшение времени когерентности

Одним из методов исправления ошибок является улучшение качества и контроля связанного состояния каждого кубита, делая его более продолжительным, чем необходимое для расчета время, совершенствуя любые компоненты, влияющие на ошибки квантового компьютера, такие как шум квантовых вентилей или скорость соединений. Чем дольше кубит может оставаться связанным, тем, вероятно, будет меньше ошибок.

Изоляция от окружающей среды

С самого начала создания классических компьютеров компьютерные ученые осознали преимущества эксплуатации компьютеров в контролируемой окружающей среде, изоляции их от внешних экстремальных условий. Во всех компьютерных помещениях регулируется температура (тепло – враг компьютерных компонентов), комнаты охлаждаются фильтрованным воздухом с контролем влажности, в них поддерживается чистота. Вряд ли найдется много компьютеров, которые проработали бы долго в обычных погодных условиях и без какой-либо защиты от внешних влияний. Но большинство современных классических компьютеров созрели аппаратно до такой степени, что могут успешно работать в обычных погодных условиях, если только они не подвергаются действительно экстремальным воздействиям (компьютер упал в воду, на него наступили и т. д.). Наиболее популярные типы вычислительных устройств работают в современном мире ежедневно. Большинство ноутбуков, планшетов и персональных компьютеров отлично работают за пределами компьютерного помещения с контролируемой средой. Квантовые компьютеры к таковым еще не относятся. Это все еще очень хрупкие машины, и они должны быть защищены не только от экстремальных погодных условий, но даже от вполне нормальных условий. На самом деле большинство из них (по крайней мере, их квантовые компоненты) могут наиболее эффективно работать в определенных экстремальных условиях, в частности при очень низкой температуре. Они должны быть защищены от радиоволн, нормального фона излучений, электромагнитных помех, громких звуков и вибрации. Но большинство квантовых ученых вполне представляют себе день, когда, как и классические компьютеры, квантовые компьютеры будут устроены таким образом, что станут более устойчивыми и в меньшей степени нуждающимися в особой изоляции от внешней среды.

Сверхпроводимость

Чтобы минимизировать проблемы преждевременной декогеренции, большинство квантовых компьютеров должны охлаждать свои кубиты (и другие близлежащие компоненты) почти до нуля градусов Кельвина (0 К – около –460 °F, или –273 °C). Показано, что тепло приводит к увеличению числа ошибок и позволяет излучать больше нежелательных блуждающих квантовых частиц; это верно в отношении всех квантовых компьютерных технологий, даже тех, которые якобы не нуждаются в сверхнизких температурах.

Они могут не «нуждаться» в таковых, но, похоже, работают при более низких температурах лучше, с меньшим количеством ошибок. Для этого большинство квантовых компьютеров (на самом деле просто их кубит-чипы и тесно связанная с ними аппаратура) охлаждаются с использованием внешних криогенных или других холодильников.

Можно заметить, как большинство производителей квантовых компьютеров гордятся тем, насколько сильно охлаждается их аппаратура: «Наши температуры в 200 раз ниже, чем в дальних уголках Вселенной!» Многие заявят, что рабочая температура составляет от менее сотен до тысячных долей градусов Кельвина (часто рекламируется от 0,02 до 0,01 K). Другие хвастаются способностью своих компьютеров противостоять ошибкам при более высоких температурах и будут рекламировать компьютеры, работающие при значениях немного выше комнатной температуры, например от 4 до 20 K (20 K – это –424 °F, или –253 °C).

В физике уже давно идет гонка среди тех, кто может создавать самые низкие температуры, но никто еще не достиг абсолютного нуля (0 K), и это, вероятно, невозможно. Но если бы это было возможно, все энергии и импульсы частиц при абсолютном нуле имели бы минимально физически возможные значения (нечто, называемое *точкой нулевой энергии*). При абсолютном нуле большинство движущихся и даже твердотельных веществ не смогут функционировать как обычно. С учетом сказанного квантовый компьютер будущего, вероятно, сможет нормально работать при более высоких температурах, даже приближенных к условиям работы современных классических компьютеров, потому что охлаждение стоит дорого и ограничивает возможности использования компьютерной техники.

Но на текущем этапе более низкие температуры обычно улучшают время когерентности и уменьшают ошибки. Низкая температура также создает квантовое свойство, называемое *сверхпроводимостью*, при которой электрическое сопротивление в материалах, охлажденных ниже пороговых значений критической температуры, равно или почти равно нулю. Сверхпроводимость увеличивает электронные потоки и допускает более сильные электромагнитные взаимодействия. Многие квантовые компьютеры используют сверхпроводимость для создания кубитов. Сверхпроводимость применяется во многих других приложениях. Назовем такие, как скоростной поезд на магнитной подушке, медицинское оборудование и сверхсильные магнетики.

Повторяющиеся вычисления

Один из способов борьбы с ошибками – выполнение одного и того же вычисления не менее трех раз и сохранение результатов в классическом состоянии. После многократного выполнения одного и того же вычисления компьютер рассмотрит сохраненные результаты, и если есть расхождения, будет принят тот результат, который встречается с наибольшей частотой. Однако этот метод исправления ошибок замедляет работу компьютера тем сильнее, чем больше дублирующих операций используется, и нет никакой гарантии, что наиболее частый результат – на самом деле правильный.

Использование квантовой запутанности для исправления ошибок

В классическом компьютерном мире, если ожидается много ошибок, значение бита можно скопировать и сохранить в одном или нескольких «резервных» битах одновременно. Если между битами есть несоответствие, то берется самое популярное значение. Но в квантовом мире в соответствии с теоремой о клонировании и согласно принципу наблюдателя кубиты не могут быть скопированы напрямую, пока они находятся в своих квантовых состояниях. Вместо этого запутанность может использоваться для создания косвенных копий, хотя запутанные связи чувствительны и легко потерять след, когда происходит декогеренция.

Проверочные кубиты

Другой метод исправления ошибок использует дополнительные кубиты как проверочные, аналогично тому, как проверочные биты используются в классическом двоичном мире. Проверочные кубиты реализуются в своего рода логическом методе проверки, который выявляет ошибки и помогает их исправить. Например, дополнительный проверочный кубит используется, чтобы гарантировать, что результирующий кубайт складывается определенным образом – скажем, компьютер может добавить 0 или 1 к контрольной позиции кубита кубайта, чтобы убедиться, что сумма всех кубитов заканчивается как четная величина. Если квантовый компьютер обнаруживает отрицательную сумму, возвращающуюся из суммы в байтах, может быть объявлена ошибка, и квантовая операция будет повторена. Возможно, вы знакомы с подобной популярной классической технологией исправления ошибок в двоичном компьютерном мире, которая называется *резервный массив независимых дисков* (Redundant Array of Independent Disks, RAID). Большая проблема с такой простой проверкой четности заключается в том, что нет никакого способа гарантировать, что ошибки не происходят таким образом, что не обнаруживаются только четные или нечетные значения. Но это лучше, чем ничего; и более сложные методы, и похожие сценарии проверки ошибок были использованы, чтобы сделать наш существующий двоичный мир невероятно надежным. Производители квантовых компьютеров используют аналогичные методы квантовой проверки ошибок, чтобы сделать квантовые компьютеры более надежными.

Проверяющие ошибки кубиты, добавляемые в систему только для обеспечения отказоустойчивости, называются *вспомогательными* (ancillary) кубитами. Производители квантовых компьютеров пытаются максимально увеличить количество кубитов в связи с необходимостью «тратить» некоторые ресурсы на проверку ошибок. Текущее состояние многих квантовых компьютеров и устройств уже сейчас требует очень много вспомогательных кубитов, чтобы иметь один стабильный кубит. Количество вспомогательных кубитов, необходимых для создания одного стабильного кубита, измеряется количествами от нескольких кубитов до миллионов. Это неординарная проблема диапазона и масштабирования. Тем не менее иногда достижение наибольшей производительности обеспечивается за счет увеличения количества кубитов, используемых в качестве вспомогательных. Все поставщи-

ки с нетерпением ждут того дня, когда смогут минимизировать количество вспомогательных кубитов.

Примечание Повторяющиеся вычисления и проверка ошибок с помощью вспомогательных кубитов никак не помогают выявить и полностью исправить ошибку и являются неэффективным процессом. Кроме того, так как квантовые ответы имеют вероятностный характер, они могут давать разные ответы при каждом запуске независимо от фактической частоты ошибок.

Повышение производительности других компонентов

Еще один практический способ победить ошибки декогеренции – увеличить пропускную способность, связность, подготовку состояний и производительность чтения. При уменьшении времени, необходимого для вычисления квантового результата и его чтения, желаемое вычисление и чтение результирующего значения могут быть выполнены до того, как произойдет ошибка и кубит преждевременно декогерирует. Для примера давайте предположим, что квантовый компьютер имеет много ошибок декогеренции, которые начинают происходить в районе 100 миллисекунд. Если вычисления могут быть выполнены в течение 100 мс, этот квантовый компьютер может избежать наихудших эффектов декогеренции и получить более точные результаты. Относительные значения производительности различных квантовых компьютеров приводятся и сравниваются на веб-сайте https://quantumcomputingreport.com/scorecards/qubit-quality/.

ПРЕИМУЩЕСТВА КЛАССИЧЕСКИХ КОМПЬЮТЕРОВ

Ввиду проблем квантовой механики и квантовых компьютеров традиционные бинарные компьютеры в ближайшее время никуда не денутся. Мы понимаем, как двоичные компьютеры работают на фундаментальном уровне (даже в той части, в которой их работа основывается на квантовой механике). Классическим компьютерам не приходится заботиться о декогеренции, эффекте наблюдателя или теореме об отсутствии клонирования, и они не так чувствительны к внешним воздействиям, как квантовые устройства. Они ведь на самом деле прекрасно работают в реальном мире. Они не требуют для работы идеальных климатических условий. Они довольно недороги. Каждый может приобрести новый ноутбук менее чем за 300 долларов, портативное устройство за 100 долларов и полнофункциональные мини-компьютеры размером со спичечный коробок за 25 долларов. Мы смогли разместить миллиарды и миллиарды интегральных схем на маленьком кусочке легированного кремния. Мы объединяем десятки процессорных ядер в один чип. Данные и результаты, которые они обеспечивают, стабильны в течение длительного времени в памяти и на процессорах, и нам не приходится

беспокоиться о том, как внешний мир повлияет на них. Существуют некоторые типы плохо обрабатываемых вычислений, с которыми бинарные компьютеры справляются очень хорошо. Квантовое превосходство в один прекрасный день может все заметно изменить, но трудно оставить не у дел эту рабочую лошадку, стабильные бинарные компьютеры. По этой причине классические компьютеры, скорее всего, будут еще долго сопровождать нас в нашей жизни. Подробнее об этом – в главе 5 «Каким будет постквантовый мир?».

Важный вывод этого раздела книги: мощность конкретного квантового компьютера при решении проблем – не просто функция числа его кубитов. Сегодня много кубитов, вероятно, будут вовлечены в исправление ошибок. Общая производительность зависит от других разнообразных факторов, таких как подготовка вентилей, связь между вентилями, исправление ошибок и производительность считывания. Даже когда количество кубитов и скорость исправления ошибок у квантовых компьютеров одинаковы, эти компьютеры могут относиться к различным типам, созданным для решения различных типов задач, поэтому надо быть осторожными с любыми сопоставлениями, основанными только на кубитах. Не следует полагать, что компьютер на 2000 кубитов непременно лучше, чем компьютер на 100 кубитов, да еще и для всех видов задач.

Типы квантовых компьютеров

Существуют десятки различных типов квантовых компьютеров, теоретических моделей, архитектур и реализаций. Их так много, что зарождающаяся область квантовых вычислителей даже не успевает определиться с тем, какие модели являются «основными», как уже появляется другая. Это не обязательно плохо. Это демонстрирует, что поле конкурентно, пытается найти лучшие решения и открыто для любых, возможно новых, подходов, которые позволяют решать сложные проблемы разными способами.

По мере того как мир квантовых вычислений созревает и решает свои проблемы, можно ожидать, что более слабые кандидаты будут выбывать, и появится ряд сильных решений (или только одно превосходное решение). Но сейчас у нас много типов и масса конкурентов. На данный момент «лучшего» квантового компьютера нет, хотя многие производители скажут вам, что они работают над самым лучшим.

Примечание Когда в данной книге используется термин «производитель или продавец квантовых компьютеров», важно учитывать, что большинство проектов по квантовым компьютерам разрабатываются фактическим поставщиком компьютера с существенной помощью сторонних организаций. Большинство поставщиков тесно сотрудничают с одним или несколькими университетами, коммерческими и частными лабораториями, компания-

ми, военными подразделениями – и в ряде случаев из разных стран. Часто другие поставщики поставляют такие критические компоненты, как квантовые чипы, холодильная техника и другие строительные блоки квантового компьютера. «Заказчиками» нередко являются те же организации, которые помогают построить тестируемый квантовый компьютер; они обеспечивают критическую обратную связь, выдвигают предложения продавцу и даже поставляют некоторые компоненты. В этот многообещающий период развития квантовых вычислений большинство проектов – это труд большого коллектива, причем каждый стремится как можно скорее добиться превосходства в построении стабильного квантового вычислителя.

Давайте рассмотрим некоторые примеры квантовых компьютеров с указанием ряда производителей и опишем преимущества и недостатки каждого типа компьютера.

Сверхпроводящие квантовые компьютеры

Квантовые компьютеры, основанные на сверхпроводящих архитектурах, были одними из первых прототипов и до сих пор являются одними из самых популярных. Десятки поставщиков, в том числе компании Google, Microsoft, IBM, D-Wave Systems, Rigetti Computing и Intel, имеют один или несколько сверхпроводящих квантовых компьютеров, которые для создания и управления кубитами полагаются на особые свойства сверхпроводников. В сверхпроводящих квантовых компьютерах два слабо связанных сверхпроводника расположены конец к концу и разделены очень тонким изолятором. Парный или связанный (незапутанный) набор электронов или фермионов (называемый *куперовской парой*) передается между концами двух сверхпроводников (местоположение, известное как *джозефсоновский переход*) через изолятор к другому сверхпроводнику с использованием квантового туннелирования. На рис. 2.2 показан джозефсоновский переход, используемый для передачи двух куперовских парных электронов между двумя сверхпроводниками. Каждая куперовская пара охлаждена до низких температур, что создает *волновую функцию конденсата* при ее передаче на другой сверхпроводник. Это заставляет частицы иметь самые низкие квантовые энергии и позволяет наблюдать их свойства на макроскопическом уровне. Изменения фазы и другие изменения квантовых свойств могут наблюдаться для создания и использования кубитов. Многие, если не большинство, квантовые компьютеры, созданные сегодня, используют ту или иную форму сверхпроводящих квантовых схем.

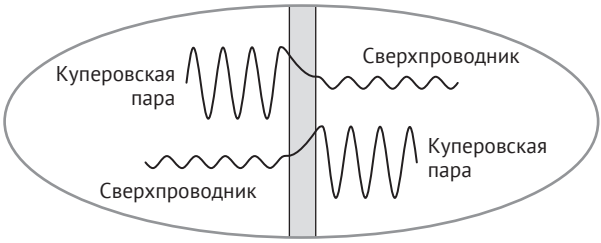


Рис. 2.2. Представление джозефсоновской функции с двумя куперовскими парами квантовых частиц между двумя сверхпроводниками

Для получения большей информации по сверхпроводниковым квантовым компьютерам обратитесь к следующим веб-сайтам:

- https://en.wikipedia.org/wiki/Superconducting_quantum_computing;
- https://web.physics.ucsb.edu/~martinisgroup/classnotes/finland/LesHouches-JunctionPhysics.pdf;
- www.nature.com/articles/s41534-016-0004-0;
- www.ncbi.nlm.nih.gov/pmc/articles/PMC3417795/;
- https://qudev.phys.ethz.ch/content/courses/ASC04_SCqubits_Review.pdf.

Квантовые компьютеры на основе алгоритма отжига

Отжиг, как правило, подразумевает нагревание чего-либо для перехода в другое желаемое состояние, например нагревание стекла для его переплавки в другую форму или перегрев металла с последующим его охлаждением, улучшающий его твердость или чистоту. Квантовые компьютеры на основе алгоритма отжига (компьютеры квантового отжига) начинают со своих кубитов в суперпозиции состояний, причем каждое состояние имеет равную вероятность конечного результата. Затем компьютер применяет термический (классический) и/или квантовый туннельный отжиг к каждому кубиту, используя *устройство электромагнитной связи* (electromagnetic coupler). Оно меняет состояния с равной вероятностью на состояния с неравной вероятностью (увеличивая, таким образом, вероятность отдельных состояний). Затем квантовые состояния будут пытаться минимизировать свою энергию до минимально возможного энергетического состояния (что-то подобное происходит и в классическом мире). Самые низкие энергетические состояния имеют наибольшую вероятность окончательного ответа. Хорошее объяснение этого процесса дается в следующих видео:

- www.youtube.com/watch?v=UV_RlCAc5Zs;
- www.youtube.com/watch?v=kq9VqR0ZGNc;
- www.youtube.com/watch?v=Yy93LMGQbpo.

Примечание Компьютеры отжига тесно связаны с *адиабатическими* квантовыми компьютерами.

Если это техническое объяснение недостаточно доходчиво, хороший способ представить процесс отжига – проведение аналогии с шариком (состоянием) на одной стороне волнистого неровного синусоидального холма (см. рис. 2.3). Волнообразная форма варьируется в зависимости от конкретной (математической) проблемы. Шарик без какого-либо внешнего влияния хочет оставаться неподвижным в своей нынешней, самой низкой области окружения. Без внешнего воздействия он не сможет перебраться через какой бы то ни было холм в какое-либо другое состояние, даже если другие области ниже, чем та, в которой он сейчас находится (то есть ответ с наибольшей вероятностью). Процесс отжига помогает шарику достичь более низких областей. Если используется термическая внешняя помощь, шарику дается дополнительная энергия, которая позволяет ему пройти через начальные и другие последовательные холмы, пока он не достигнет самой низкой общей области (то есть самой низкой энергии в конечном состоянии). Если используется квантовое туннелирование, шар просто проходит через каждый холм, как поезд, идущий через туннель, пока не найдет общее низшее состояние.

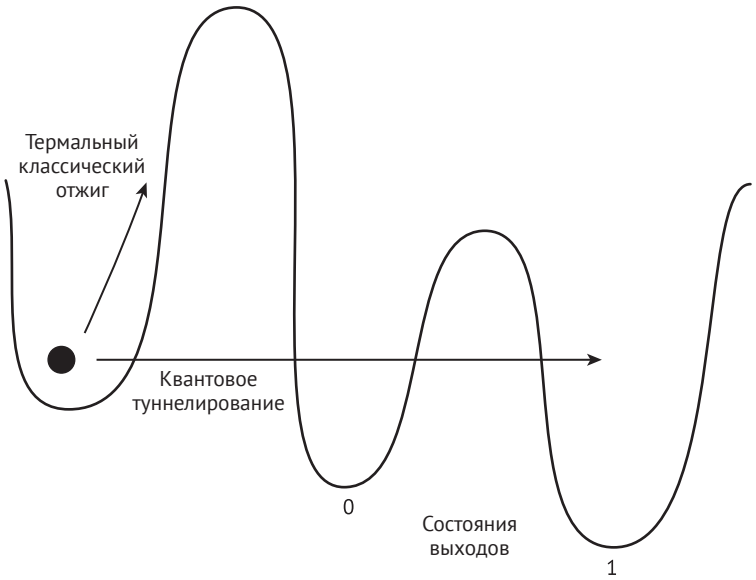


Рис. 2.3. Графическое представление процесса квантового отжига

Примечание В природе и мире в целом «правильный ответ» часто находится в самом низком, наименее хаотичном энергетическом состоянии. Согласно этой закономерности с горы ссыпается песок и вода всегда стремится быть на уровне моря. Многие типы квантовых компьютеров также работают, помогая квантовым частицам достигать своих самых низких естественных энергетических состояний.

Компьютеры квантового отжига D-Wave

D-Wave Systems – одна из первых компаний по производству квантовых компьютеров квантового отжига (www.dwavesys.com/home). Сотрудники D-Wave создали квантовые компьютеры с самым высоким количеством заявленных кубитов по сравнению с другими поставщиками квантовых вычислителей. По состоянию на 2019 год компания располагает компьютером с 2048 кубитами и, вероятно, будет иметь больше реальных клиентов и приложений, чем любой конкурент. Квантовые процессоры D-Wave охлаждаются до 0,015 K (0 K – почти –460 °F , или –273 °C), содержат специальное экранирование, блокирующее все возможные внешние электромагнитные помехи, и занимают относительно небольшую площадь.

Преимущества и недостатки компьютеров квантового отжига

Преимущества компьютеров с квантовым отжигом состоят в том, что они достаточно устойчивы к шумам внешней среды, легко масштабируются и не требуют почти абсолютного нуля градусов Кельвина (даже если они еще лучше работают при более низких температурах). Компания D-Wave доказала, что эти типы квантовых компьютеров могут быть произведены – и уже производятся – в значительных масштабах.

К сожалению, недостатки этого компьютера, вероятно, самые существенные по сравнению с другими типами квантовых компьютеров. Во-первых, компьютеры отжига могут решить только один тип конкретной квантовой задачи, известной как *оптимизация проблемы*. Эта проблема проистекает из того, что они работают, полагаясь в первую очередь на самый низкий уровень энергии, представляющий оптимальное решение. Например, компьютеры с квантовым отжигом не могут вычислять уравнения с большими простыми числами и использованием алгоритма Шора (более подробно этот вопрос обсуждается в главе 3).

Во-вторых, многие квантовые физики даже не будут считать компьютеры отжига настоящими, в полной мере квантовыми компьютерами. Они также сомневаются, что компьютеры отжига в долгосрочной перспективе могут превзойти классические компьютеры или быть достаточно полезными для решения широкого круга неклассических задач. Выдвигается много аргументов за и против, и особенно в связи с тем, что речь идет о продукции компании D-Wave (она является одной из первых и самых известных производителей квантовых компьютеров). Тем не менее различные исследовательские работы, кажется, увеличивают доказательства в поддержку гипотезы D-Wave о том, что ее квантовые компьютеры, использующие квантовый туннельный отжиг, могут решать более широкий круг проблем, чем ранее теоретически предполагалось.

Универсальные квантовые компьютеры

По сравнению с ограниченными случаями использования квантового отжига, универсальный квантовый компьютер – теоретический святой Грааль квантовых компьютеров на другом конце спектра использования приложений. Универсальные квантовые компьютеры не являются специфической

разновидностью квантового компьютера, но обычно описывают квантовый компьютер, который не является компьютером ограниченного применения.

Универсальный квантовый компьютер – это скорее результат, чем конкретный тип квантового компьютера или архитектура, и является таковым, если может обрабатывать любой квантовый алгоритм. Некоторые критики считают, что это маркетинговый термин и ничего больше, но я с этим не согласен. Цель состоит в том, чтобы создать квантовый компьютер, который может решить любую проблему, будь она классическая, квантовая или проблема моделирования. Универсальный квантовый компьютер может не только решать самые разнообразные задачи, но и моделировать все другие типы более ограниченных квантовых компьютеров.

Сотрудники IBM напряженно работают над созданием первого и лучшего универсального квантового компьютера, который назван IBM Q (www.research.ibm.com/ibm-q/). Они неуклонно увеличивают количество кубитов компьютеров IBM Q и с 2017 года предсказывают и успешно реализуют удвоение квантового объема каждый год. А наряду с наращиванием кубитов, количество которых теперь достигло 50 (см. рис. 2.4), улучшают их стабильность и уменьшают количество ошибок.

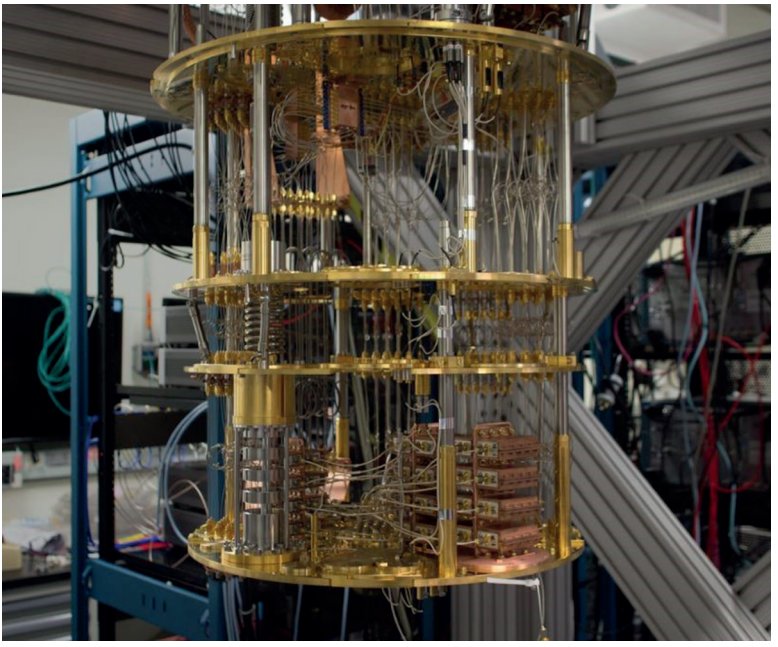


Рис. 2.4. Универсальный 50-битный квантовый компьютер IBM (с любезного разрешения компании IBM)

Инженеры компании Google (https://ai.google/research/teams/applied-science/quantum-ai/) также работают над универсальным квантовым компьютером, имеющим в настоящее время 72 кубита. На рис. 2.5 показан квантовый процессор Bristlecone компании Google, основа 72-кубитового компьютера. Goo-

gle планировала достичь квантового превосходства в 2019 году, хотя прежде делала такой же прогноз относительно 2018 года. Таким образом, инженеры Google считают, что они близки к этому, и, очевидно, полагают, что при современной технологии исправления ошибок квантовый порог превосходства составляет около 100 кубитов.

Преимущества и недостатки универсальных квантовых компьютеров

Производители универсальных квантовых компьютеров могут использовать любую технологию, чтобы обеспечить наибольшее и наиболее широкое число сценариев обработки. Недостаток в том, что эти компьютеры требуют наибольшего числа кубитов и являются одним из самых сложных типов.

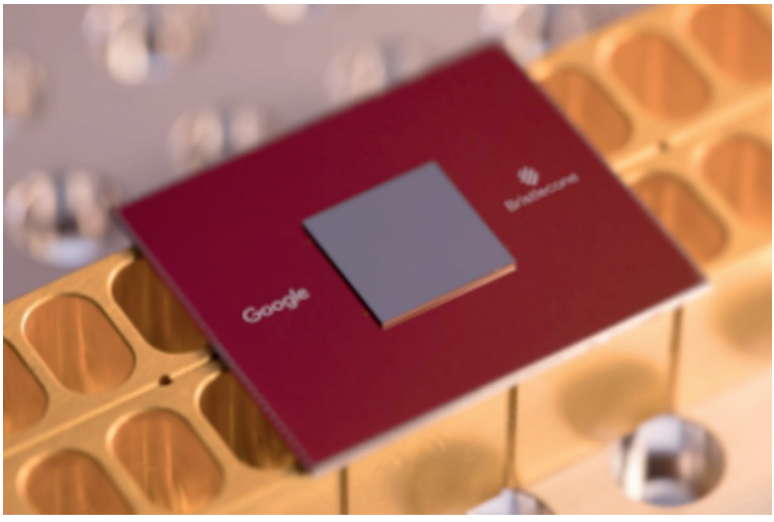


Рис. 2.5. Квантовый процессор Bristlecone компании Google, основа ее 72-битного компьютера

Топологические квантовые компьютеры

Топология – математический термин, используемый для описания свойств при переходе объекта из одного состояния в другое, без разделения и разрушения объекта. Это исследование связей объектов между собой, но не обязательно связанных на расстоянии. Типичный пример, который вы увидите при демонстрации квантовой топологии, – кольцо в виде бублика, трансформирующееся в сосуд цилиндрической формы и обратно. Оба объекта совершенно разные, не считая того факта, что отверстие в сосуде появилось из дырки от бублика, и могут постоянно трансформироваться друг в друга, сохраняя при этом математическую связность.

Квантовые топологические кубиты состоят из относительно недавно открытых двумерных «квазичастиц», названных *неабелевыми анионами* (non-abelian anyons). Анион может быть побужден к созданию трехмерной (время плюс

два пространственных измерения) квантовой «косы». Отдельные анионы не могут быть использованы для создания кубитов. Для создания кубита берется коллекция нескольких анионов. Эти коллекции анионов могут перемещаться относительно друг друга, создавая различные типы квантовых операций, а их совместное перемещение создает новые частицы. Эти перемещения и новые частицы создают заплетенные в виде косы цепочки.

Примечание Если понимание данного типа квантового компьютера и обсуждение каких-либо связанных с ним проблем кажутся вам трудными, вы не одиноки. Анионы оставались теорией в течение долгого времени, прежде чем кто-либо мог их создать, и с момента их создания прошло совсем немного времени. Даже после этого квантовые физики говорят, что создание этих частиц требует «экзотических фаз материи» – термин, которым они обычно не бросаются. Нобелевская премия по физике 2016 года была присуждена трем физикам, обнаружившим квантовую топологию (www.nobelprize.org/prizes/physics/2016/summary/).

Эти переплетенные косы анионов могут быть использованы для создания мощных квантовых логических элементов на аппаратном уровне, которые борются с декогеренцией и другими квантовыми ошибками лучше, чем большинство других моделей. В то время как декогеренция, присущая большинству других типов квантовых кубитов, существует в течение десятков миллисекунд или менее, косички могут длиться секунды. Предполагается, что только один тип квантового компьютера, ионная ловушка, рассматриваемая ниже, имеет возможность обеспечить более длительное время без исправления.

Топологические квантовые компьютеры обладают одним уникальным свойством, которое особенно интересно физикам. Топологические косы часто сравнивают с узлами на нитях. Вы можете двигать и изменять нить, но «узлы» являются квантовой информацией и остаются независимо от того, как вы манипулируете нитью или какие внешние воздействия этому мешают. Поскольку коса сохраняет прошлые квантовые состояния (т. е. историю квантовой информации), наблюдатели могут видеть, откуда началось состояние (или состояния) анионной косы и как оно (они) менялось со временем. Ни один другой тип квантового компьютера не обладает этим свойством. Для лучшего понимания анионов и квантово-топологических компьютеров посмотрите следующие видео:

- www.youtube.com/watch?v=igPXzKjqrNg;
- www.youtube.com/watch?v=RW44rIrAZHY;
- www.youtube.com/watch?v=qj-w6ISQL5Y;
- www.youtube.com/watch?v=Xyfsr-coriQ.

Компьютеры Majorana Fermion компании Microsoft

Компания Bell Labs Microsoft и несколько университетов усиленно занимаются квантовой топологией. В 2018 году Microsoft создала первый, очень простой 1-кубитный квантово-топологический компьютер, используя метод

майорановских фермионов (Majorana fermion), который связан с методом анионов, но не идентичен ему. Майорановские фермионы созданы путем расщепления электронов (которые являются элементарными частицами) на две меньшие запутанные квазичастицы, которые, по существу, формируют топологические кубиты, ведущие себя подобно анионам. Майорановские фермионы могут действовать как их собственная античастица, что означает, что если они встретятся друг с другом, то могут уничтожить друг друга. Каждая частица имеет античастицу (пример: нейтроны и электроны), но обычно этот тип частицы не является также своей собственной античастицей. Вы можете найти статью о майорановских фермионах на сайте www.sciencedaily.com/releases/2019/04/190401115906.htm.

Примечание Разделение электронов на более мелкие квазичастицы называется *фракционированием электронов*. В результате каждая из запутанных квазичастиц имеет половину заряда исходного электрона. Отличная статья о фракционировании электронов: https://phys.org/news/2015-05-electron.html.

Компания Microsoft возбудила сообщество, создав первый топологический квантовый компьютер, и хотя он имеет всего 1 кубит и независимые разработчики не имели доступа к этому компьютеру (как и автор), многие специалисты по квантовым вычислениям считают, что эта технология масштабируется до гораздо большего числа кубитов. Вероятно, он станет сильным конкурентом квантовых компьютеров будущего. В настоящее время семь лабораторий квантовых вычислений компании Microsoft по всему миру работают над квантовыми компьютерами, и они имеют полный квантовый стек (будет обсуждаться чуть позже).

Преимущества и недостатки квантово-топологических компьютеров

Топологические квантовые компьютеры относительно новы и имеют небольшое количество продемонстрированных кубитов (по сравнению с другими типами квантовых компьютеров). Но если Microsoft преуспеет в создании большего количества топологических кубитов, потенциальные выгоды будут огромными. Самые большие преимущества заключаются в том, что эти кубиты более стабильны, начиная с уровня аппаратного обеспечения, а косы сохраняют свою квантовую историю.

Топологические компьютеры все еще нуждаются в исправлении ошибок и контроле кубитов, но ошибки можно контролировать путем снижения температуры и увеличения расстояния между топологическими частицами. В связи с этим потребуется меньше общих кубитов, что также может снизить затраты.

Квантовые компьютеры с ионными ловушками

Ионы – это атомные частицы с общим суммарным зарядом. Каждый стабильный атом имеет одинаковое количество протонов (положительно заряженные частицы) и электронов (отрицательно заряженные частицы), так что

общий суммарный заряд отсутствует. Ион – это атом с неуравновешенным числом электронов и протонов; таким образом, у него есть положительный или отрицательный электрический заряд. Чтобы создать ионы, большинство компьютеров с ионной ловушкой (ion trap quantum computers) нагревают выбранные атомы (скажем, кальция или иттербия) до очень высоких температур с помощью лазера в изолированном вакууме. Затем они сжигают электроны на перегретых атомах, в результате чего атомы теряют электрон и получают чистый положительный заряд.

Квантовые компьютеры с ионной ловушкой используют электромагнитные поля и вакуум для приостановки и ограничения (т. е. ловли) ионов в свободном пространстве над кремниевым чипом с комнатной температурой. Затем для управления движением ионов, в том числе запутыванием пар кубитов, используются лазеры. Квантовая информация может быть передана через коллективное движение ионов или запутанных пар. Для получения дополнительной информации о квантовых компьютерах с ионной ловушкой смотрите следующие ресурсы:

- www2.physics.ox.ac.uk/research/ion-trap-quantum-computing-group/intro-to-ion-trap-qc;
- www.youtube.com/watch?v=9aOLwjUZLm0;
- https://arxiv.org/pdf/quant-ph/9708050.pdf;
- www.youtube.com/watch?v=WOQ_jWe62EA.

Квантовые компьютеры с ионными ловушками компании IonQ

Компания IonQ (https://ionq.co/), работающая с Национальными лабораториями Sandia (Sandia National Laboratories) и другими квантовыми пользователями и поставщиками, является одной из основных сторонников технологии ионной ловушки. IonQ была лидером в использовании кремниевых чипов комнатной температуры в квантовых компьютерах, хотя некоторые исследования показали, что может потребоваться охлаждение ионных ловушек до 4 K (все еще значительно выше температур порядка 1 K, требующихся в большинстве других типов квантовых компьютеров), поскольку это увеличивает число кубитов до более чем 32. На рис. 2.6 показан блок квантового процессора Ion Trap компании IonQ с искусственно выведенным вырезом «захваченных ионов» над квантовым процессором (QPU). Захваченные ионы находятся внутри этой крошечной щели в центре столь же крошечного QPU.

Преимущества и недостатки компьютеров с квантовыми ионными ловушками

У систем с захваченными ионами много преимуществ, в том числе то, что они могут работать при комнатной температуре, используя несколько выглядящих традиционно кремниевых чипов. Они могут иметь очень долгое время когеренции, измеряемое 10 минутами, высокую частоту перемешивания, могут иметь все кубиты, разбитые на пары (что невозможно для других типов квантовых компьютеров), и позволяют, по сравнению с другими типами компьютеров, проводить более точные измерения.

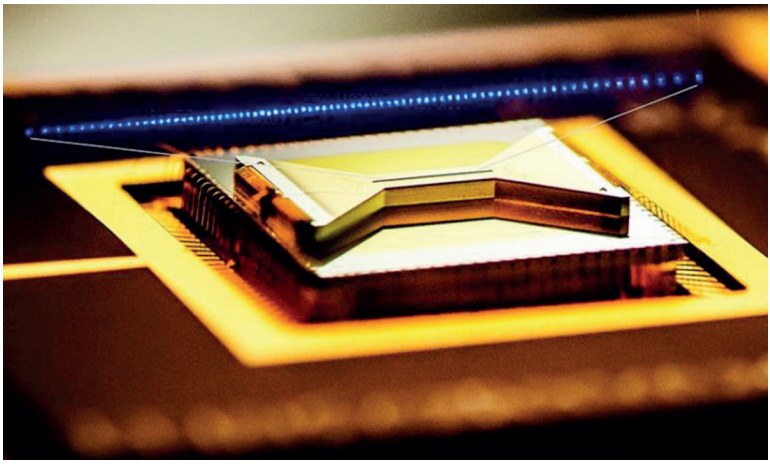


Рис. 2.6. Пример силиконового чипа IonQ ионной ловушки с индивидуальными линейными ионами, «вырезанными» для демонстрации деталей индивидуальных ионов *С любезного разрешения сотрудников компании IonQ Кая Худека (Kai Hudek) и Эмили Эдвардс (Emily Edwards)*

К сказанному надо добавить, что существуют исследовательские проекты с более чем 100 захваченными ионами, контролируемыми с разным уровнем успеха. Но пока число устойчивых кубитов у этого компьютера не приблизилось к числу кубитов некоторых других типов квантовых компьютеров. Однако, как и в случае майорановских фермионных квантовых компьютеров, если IonQ и другие производители квантовых компьютеров с ионной ловушкой смогут масштабировать захваченные ионы, этот тип квантового компьютера может в долгосрочной перспективе оказаться победителем.

На этом мы завершаем наш обзор некоторых наиболее важных квантовых компьютерных архитектур, моделей и поставщиков. Существуют десятки других реальных и теоретических типов квантовых компьютеров, описания, архитектуры и реализации которых не будут рассмотрены в этой книге, в том числе фотонные, кремниевые квантовые точки, алмазная вакансия, односторонняя, матрица квантовых вентилей, шумно-промежуточный масштаб-квант, тьюринговые, аналоговые и вращательные. Я не хочу пренебрегать какой-либо квантовой компьютерной архитектурой или указывать, что одна из них важнее другой. Кое-что здесь опущено просто для экономии места, поскольку эта глава и так уже слишком длинная. Я рассмотрел достаточно разных типов, чтобы дать вам почувствовать атмосферу конкурентного мира квантовых вычислений и показать некоторые из оставшихся проблем. Если вам интересно узнать о других типах и архитектурах квантовых компьютеров, можете начать с https://en.wikipedia.org/wiki/Quantum_computing#Quantum_computing_models.

Квантовые компьютеры в облаке

В настоящее время квантовые компьютеры являются чрезвычайно дорогими, достаточно большими и хитроумными устройствами, требующими для

работы и содержания квалифицированного персонала. Им часто требуются большие системы охлаждения и другие вспомогательные устройства, к которым обычные компании не имеют доступа. Это, однако, не означает, что вы или любой обычный человек не можете провести квантовые вычисления.

Многие поставщики квантовых вычислений давно уже предлагают доступ к своим квантовым компьютерам или квантовым симуляторам. Некоторые поставщики разрешают всем присоединяться и использовать облачный компьютер бесплатно в любых законных целях. Другие производители квантового облака требуют, чтобы пользователи заполняли подробную форму о своем проекте с указанием, почему он требует временны́х затрат квантового вычислителя, и каждая заявка рассматривается индивидуально. В иных случаях облачный сервис является 100%-ным коммерческим предложением или имеет частное членство предприятия. Если у вас есть законное основание «пообщаться» с квантовым компьютером, вы можете найти квантовый облачный сервис, который поможет вам в этом. Среди них:

- www.research.ibm.com/ibm-q/;
- https://cloud.dwavesys.com;
- www.rigetti.com/qcs;
- www.huaweicloud.com/en-us;
- https://us.alibabacloud.com/.

Многие наблюдатели квантовых компьютеров считают, что квантовые облачные вычисления являются моделью будущего, по крайней мере на среднесрочную перспективу. Компании и частные лица, которые не могут себе позволить квантовые компьютеры, могут воспользоваться преимуществами разделения времени квантовыми облачными вычислениями и платить только за то, что им необходимо.

Квантовые компьютеры, произведенные не в США

Хотя предыдущие разделы этой книги были сосредоточены на американских и близких им разработчиках квантовых компьютеров, многие страны, в том числе Австралия, Австрия, Бельгия, Канада, Китай, Дания, Финляндия, Франция, Германия, Италия, Япония, Ближний Восток (например, Саудовская Аравия, Катар и Объединенные Арабские Эмираты), Нидерланды, Польша, Россия, Сингапур, Южная Корея, Испания, Швеция, Швейцария и Великобритания, занимаются квантовой информатикой с той или иной степенью финансирования и участия. Большинство сходится во мнении, что из стран за пределами этого списка двумя крупнейшими квантовыми конкурентами являются Соединенные Штаты и Китай. Обе страны тратят десятки миллиардов на квантовые вычисления.

Соревнование не всегда ведется между странами. Многие компании, основанные в одной стране, участвуют в одном или нескольких проектах в других странах. Например, независимая фирма – разработчик квантовых приложений Cambridge Quantum Computing (https://cambridgequantum.com/), официальная штаб-квартира которой расположена в Великобритании, участвует в коммерческих, правительственных проектах, а кроме того, в проектах мно-

гих стран мира. Национальный проект США по выбору квантовоустойчивого шифра (подробно рассмотрен в главе 6) разрабатывают многие команды разработчиков не США, а также многонациональные команды.

Это не означает, что между странами определенно отсутствует конкуренция типа «гонка до луны». Она есть. И имеет смысл с той точки зрения, что страны, вырвавшиеся в лидеры, будут способны пожинать плоды раньше, а также потому (и это особенно важно в контексте данной книги), что квантовые вычисления будут использоваться для выведывания многих национальных секретов и для защиты новых.

Компоненты квантового компьютера

Независимо от того, какого типа квантовый компьютер и какую архитектуру он использует, сегодня все они довольно похожи и нуждаются примерно в одном и том же. В частности, им требуются:

- обслуживающий персонал;
- охраняемый, абсолютно чистый компьютерный зал с контролируемой средой;
- мощный поставщик электроэнергии;
- система охлаждения;
- системы хранения и доставки газа;
- проводка;
- трубопровод;
- внешние традиционные, классические компьютеры для мониторинга, контроля и управления;
- квантовый компьютер;
- поддерживающие схемы;
- электромагнитное экранирование;
- физически герметизированный кубитный квантовый процессор (QPU);
- площадка квантовых данных (включает QPU и все другие квантовые компоненты);
- контрольно-измерительная зона;
- аппаратные соединения, удаленные соединения и интерфейсы;
- классические компьютерные компоненты для хранения результатов и результирующих данных;
- сеть;
- внешняя отделка (аккуратный вид);
- операционная система (код запуска, управление, мониторинг, компилятор и т. д.);
- программные интерфейсы;
- алгоритмы;
- прикладное программное обеспечение.

Сегодня в работающем квантовом компьютере все компоненты, непосредственно к нему относящиеся, – собственно то, что большинство неспециалистов считают «квантовым компьютером», – занимают один или несколько

квадратных ярдов пространства. По сравнению с этим бинарный компьютер – спичечный коробок, если не чип. Как было и с большинством компонентов компьютерной системы, со временем каждый квантовый компонент и вся система компонентов, вероятно, будут становиться все меньше по размеру и все менее ресурсоемкими.

Примечание Вопрос в том, сможем ли мы когда-нибудь довести квантовые компьютеры до размеров настольного компьютера или ноутбука и приспособить к работе в горячем, шумном, со сложной внешней средой помещении, то есть поместить их в условия, в которых сегодня работают классические компьютеры. Многие квантовые эксперты считают, что это можно сделать. Почему? Во-первых, потому что наш мозг работает на принципах квантовой механики, и он такой же горячий, влажный и мало приспособленный к внешней среде. Природа нашла способ как-то с этим сладить. Однажды люди будут способны это понять. Люди, способные на крупные изобретения, преуспевают и в том, чтобы сделать их компактными.

Два компонента, прикладное программное обеспечение и так называемый «стек», заслуживают отдельного рассмотрения.

Квантовое программное обеспечение

Нужно нечто большее, чем аппаратное обеспечение и кубиты, чтобы квантовый компьютер мог решать сложные задачи. Каждое квантовое устройство поставляется с одной или несколькими операционными системами, алгоритмами, интерфейсами и прикладными программами. Как минимум, квантовый компьютер должен иметь встроенное программное обеспечение или управляющее программное обеспечение, которое позволяет компьютеру создавать, инициализировать, измерять, контролировать ошибки, проверять и списывать кубиты.

Каждое квантовое устройство должно реализовывать один или несколько квантовых алгоритмов (некоторые из них будут рассмотрены в следующей главе), которые обрабатывают вычисления базового уровня и математику на основе манипулирования кубитами и естественными законами. Не все квантовые устройства поддерживают все алгоритмы, хотя предполагается, что универсальные вентильные квантовые компьютеры должны это делать. Большинство квантовых компьютеров имеют компиляторы, языки программирования и языки сценариев, позволяющие разработчикам писать собственные квантовые компьютерные программы. Многие квантовые поставщики предоставляют частное программное обеспечение для своих клиентов либо бесплатно (чаще всего), либо как коммерческое. Некоторые поставщики квантовых устройств создают или поощряют своих клиентов работать с квантовым программным обеспечением с открытым исходным кодом. Другие предлагают свои собственные квантовые программы бесплатно, чтобы побудить разработчиков учиться и развиваться на опыте своих квантовых компьютеров. Это модель, хорошо зарекомендовавшая себя в классическом компьютерном мире.

Квантовый стек

Многие поставщики предоставляют «сеть» ресурсов, в том числе учебные пособия, инструменты программирования, инструменты моделирования и доступ к их облачным ресурсам. Немало поставщиков квантовых вычислений будут говорить о наличии «полного квантового стека». *Квантовый стек* – это основанная на кванте совокупность аппаратных средств, кубитов, комплект разработки квантового программного обеспечения, API-интерфейсы и приложения. Многие поставщики, в том числе IBM, Google, Microsoft, D-Wave, IonQ и другие, предлагают весь или часть стека. Вот несколько сайтов для квантового программного обеспечения и стеков:

- www.quantiki.org/wiki/list-qc-simulators;
- https://github.com/qosf/os_quantum_software;
- https://arxiv.org/abs/1812.09167;
- http://quantumalgorithmzoo.org/;
- https://qosf.org/;
- https://algassert.com/quirk;
- https://github.com/rigetti/pyquil;
- https://cambridgequantum.com/;
- https://marketplace.visualstudio.com/items?itemName=quantum.DevKit;
- https://quantumexperience.ng.bluemix.net/qx/edito.

Национальное руководство

В большинстве крупных стран существуют национальные программы и выделяются финансовые ресурсы в помощь правительственным организациям, отраслям и компаниям, работа которых может обеспечить стране превосходство в квантовых вычислениях.

Руководство национальной политикой

В США Национальный институт стандартов и технологий (NIST) имеет национальный консорциум, посвященный квантовым вычислениям (www.nist.gov/news-events/news/2018/09/nist-launches-consortium-support-development-quantum-industry). Белый дом выпустил федеральный документ под названием «Национальный стратегический обзор квантовой научной информации» (National Strategic Overview for Quantum Information Science, NIST), www.whitehouse.gov/wp-content/uploads/2018/09/National-Strategic-Overview-for-Quantum-Information-Science.pdf. NIST также спонсирует конкурс для определения официального постквантового шифра https://csrc.nist.gov/Projects/Post-Quantum-Cryptography (подробно рассматривается в главе 6). Многие из шифров, представленных на конкурс NIST, разработаны и финансируются другими странами и их правительствами.

Денежные гранты и инвестиции

Большинство стран вкладывают деньги в свои предприятия, которые оправдывают эти затраты. Ведущие страны, такие как США и Китай, ежегодно отводят на квантовые проекты миллиарды долларов. Даже небольшие вовлеченные в гонку страны тратят от многих миллионов до десятков миллионов долларов. Грантовое финансирование идет на улучшение квантовых исследований и разработку квантовых компьютеров в университетах, исследовательских лабораториях, на поддержку поставщиков, а также на правительственные и военные квантовые инициативы.

Вот некоторые примеры:

- www.aip.org/fyi/2019/national-quantum-initiative-signed-law;
- www.nextbigfuture.com/2018/10/us-mobilizing-funding-for-quantum-ai-to-match-china-inmulti-billion-race.html;
- www.scmp.com/news/china/economy/article/2140860/china-winning-race-us-develop-quantum-computers;
- https://quantumcomputingreport.com/news/;
- www.executivegov.com/2019/04/energy-department-announces-quantum-computing-funding-opportunity/.

Заинтересованные инвесторы могут передать часть своего капитала фирмам, связанным с квантовыми технологиями, используя квантовый биржевой фонд (National Strategic Overview for Quantum Information Science, ETF). Например, такому, как этот: https://www.defianceetfs.com/qtum. Частные инвесторы вкладывают сотни миллионов долларов непосредственно в частные компании; в том числе отмечу здесь www.nanalyze.com/2018/09/10-quantum-computing-startups/. В общем, многие частные инвестиции преследуют связанные с квантовыми вычислениями инвестиционные возможности. Вместе с тем, как и во всем остальном, инвесторы с опаской относятся к обещаниям в области квантовых информационных наук. Но многие обозреватели квантовой индустрии обращают внимание, что для получения огромного притока инвестиционного капитала достаточно слова «квант» в названии или проспекте компании, подобно тому как во время недавнего увлечения инвестициями в название включали слова «биткойн» или «криптовалюта». Многие люди потеряли состояния в начальных биткойн-инвестициях. В квантовом пространстве также будут победители и проигравшие.

Другая квантовая научная информация

Область квантовых информационных наук включает в себя больше, чем квантовые компьютеры как таковые. Помимо них развиваются многие устройства и программные компоненты, в частности:

- квантовые генераторы случайных чисел;
- квантовая сеть;
- квантовая криптография;
- квантовые приложения.

Многие фирмы фокусируются на этих типах квантовых устройств, вместо того чтобы пытаться конкурировать в очень затратной области квантовых компьютеров. Большинство из перечисленных пунктов будут обсуждаться более подробно в следующих главах. Квантовая информатика обещает открыть ряд приложений, которые значительно изменят наш мир. Вот лишь некоторые многообещающие перспективы:

- более быстрые вычисления;
- более быстрый оптимизированный поиск;
- лучший искусственный интеллект;
- лучшая криптография;
- более безопасная сеть;
- военное использование;
- улучшенное прогнозирование погоды;
- улучшенные лекарства и химикаты;
- улучшение понимания квантового мира, астрофизики и нашей Вселенной;
- идеальная конфиденциальность (использование так называемых полностью гомоморфных криптосистем);
- лучшее финансовое моделирование (торговля акциями, торговля производными инструментами и т. д.);
- более эффективное обнаружение мошенничества;
- управление трафиком для автономных транспортных средств;
- более качественные, долговечные и легкие батареи;
- квантовые деньги.

Мы рассмотрим большинство из этих тем более подробно в главе 5.

Дополнительные ресурсы

В интернете есть несколько хороших статей и книг по истории и состоянию квантовых исследований. Если вы заинтересованы в дополнительной информации, посмотрите эти сайты:

- https://mitpress.mit.edu/books/quantum-computing-everyone;
- www.irtf.org/mailman/listinfo/qirg;
- www.nist.gov/history-and-future-quantum-information;
- www.wired.com/story/wired-guide-to-quantum-computing/;
- https://en.wikipedia.org/wiki/Timeline_of_quantum_computing;
- https://en.wikipedia.org/wiki/Quantum_computing;
- https://towardsdatascience.com/the-need-promise-and-reality-of-quantum-computing-4264ce15c6c0.

Резюме

Глава 2 посвящена квантовым компьютерам, их типам и архитектурам, компонентам и другой квантовой научной информации. Мы обсудили основ-

ные различия между квантовым и традиционным двоичным компьютером и объяснили технологию, преимущества и недостатки подходов к архитектуре квантового вычислителя. Мы также рассмотрели научные направления работ основных поставщиков и их количественную информацию. В главе 3 обсудим, как квантовые компьютеры в течение нескольких лет могут сломать большинство форм традиционной криптографии с открытым ключом.

3 Как квантовые вычисления могут взломать существующие криптокоды?

В этой главе рассказывается о том, как квантовые вычисления могут взломать большинство форм традиционного шифрования с открытым ключом. Мы начнем с обсуждения основ криптографии, уделяя особое внимание тому, как большинство современных схем шифрования с открытым ключом обеспечивают защиту. Затем, основываясь на главе 2, вы узнаете, как квантовые компьютеры могут взломать эту защиту и какие криптокоды подвержены или не подвержены квантовому взлому.

Основы криптографии

Криптография[1] – это наука о защите и аутентификации людей, данных, транзакций и других объектов между уполномоченными сторонами, а также комплекс исследований и практических мер в данной области. Защита осуществляется с помощью шифрования, проверки целостности и алгоритмической реализации. Криптография обеспечивает, когда это необходимо, сохранение между уполномоченными, назначенными сторонами (или программным обеспечением, или устройствами от их имени) конфиденциальности и целостности данных, сообщений и участников. Этот раздел будет охватывать цифровое шифрование, аутентификацию и основы хеширования.

Примечание В данной главе будет использоваться термин «субъект». Он применяется для обозначения любой идентичности, которая может быть

[1] Само слово «криптография» ранее означало способ тайного письма. Позже, способ тайного обмена информацией между субъектами. – *Прим. перев.*

связана с криптографическим действием. Субъектом может быть пользователь, группа, компьютер, устройство, услуга, демон, компания, издатель или любой другой объект идентификации.

Шифрование

Шифрование – это популярный метод, позволяющий субъектам держать что-то в секрете. Один субъект может хотеть держать что-то в секрете для себя, или секрет может быть передан выбранной группе людей или устройств. Секрет может быть любым типом контента, идентификацией участвующих сторон и любым вовлеченным в транзакции объектом.

Шифрование в различных формах использовалось в течение тысяч лет, начиная с голосовых кодов и закодированных писем. Типичным примером являются простые шифры замещения, где буквы и цифры алфавита переставляются, чтобы создать закодированное сообщение, которое понимают только предполагаемые стороны. В самом простом случае стороны, использующие шифр замещения, могли бы договориться для переноса каждого символа незашифрованного сообщения вперед на одну букву в алфавите и таким образом зашифровать текст послания. Слово FROG станет GSPH (позиция F + 1 вперед = G, R + 1 = S, O + 1 = P и G + 1 = H). Всем авторизованным получателям, которых надлежит ввести в курс дела, нужно будет сказать, что результирующее закодированное сообщение может быть декодировано с помощью обратного процесса (то есть G – 1 = F, S – 1 = R. P – 1 = O и H – 1 = G). На рис. 3.1 приведен графический пример.

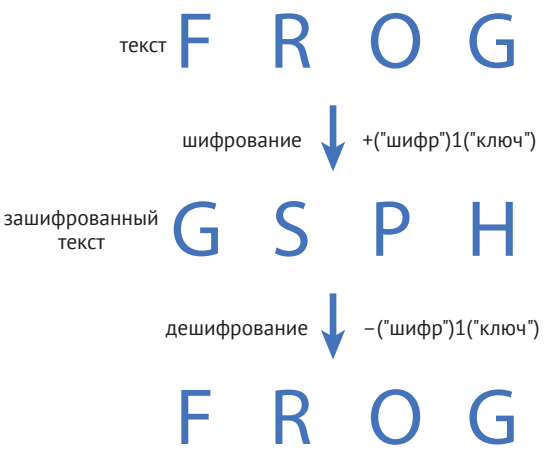


Рис. 3.1. Простой шифр подстановки

Исходный незашифрованный фрагмент называется текстовым сообщением. Закодированный именуется *зашифрованным сообщением*, или *зашифрованным текстом*. Процесс, используемый для преобразования исходного текстового сообщения в зашифрованную форму, называется *шифрованием*. Процесс, используемый для обратного перевода зашифрованного сообщения в оригинальную, открытую форму называется *расшифровкой (дешифро-*

ванием). Документированный процесс и шаги, используемые для шифрования или расшифровки сообщения, известны как *шифрование*, или *алгоритм шифрования*.

Примечание В компьютерном мире сообщение может представлять собой любой тип цифрового контента, включая текст, электронную почту, сообщения чата, данные, звук, картинки и видео.

Каждый шифр, по сути, представляет собой более сложную реализацию основных компонентов шифрования, чем рассмотренный выше в примере шифр простой замены (подстановки). Всегда присутствует текстовое сообщение, которое закодировано и декодируется с использованием алгоритма шифрования. В методе простого замещения *алгоритм шифрования* математически представляется как +X или –X (то есть + или –X или +–X), где X – количество позиций в алфавите для перемещения вперед или назад для шифрования/дешифрования.

Знаки «+» или «–» – это (простой) алгоритм шифрования. X – это *ключ шифра*. В современном мире алгоритмы шифрования представлены с использованием от простых до весьма сложных математических уравнений. Некоторые алгоритмы шифрования составлены из математических уравнений с применением традиционных математических операций, таких как сложение, вычитание, умножение и деление. Другие используют тригонометрию, исчисление и более сложные математические операции. В любом случае алгоритм шифрования позволяет зашифровать текстовое сообщение, которое расшифровывается предсказуемым образом, если тому, кто его декодирует, предоставлены алгоритм и ключ(и).

С появлением беспроводной и радиосвязи сами волны аналоговой передачи были закодированы, чтобы предотвратить непреднамеренное прослушивание. Когда стали широко использоваться компьютеры, цифровое шифрование применялось для защиты конфиденциальных цифровых сообщений. Как описано в главе 2 «Введение в квантовые компьютеры», традиционные двоичные компьютеры работают с битами (двоичными цифрами 0 и 1). Все цифровые данные и объекты на классических компьютерах хранятся в виде нулей и единиц. Когда необходимо шифрование, эти биты переставляются заранее определенным алгоритмическим способом, чтобы обеспечить неизвестность шифрования.

Примечание По-другому шифр называют «*криптографический примитив*».

Ключи шифрования

В нашем простом примере подстановки показано, что алгоритм шифрования представлен в виде +–X, где X – количество позиций для перемещения вперед или назад. X – это ключ шифра, то есть число битов, используемых для шифрования сообщения при помощи алгоритма шифрования. Немного более сложный пример подстановки – использование ключа 12. В этом случае слово FROG становится RDAS (F + 12 = R, R + 12 = D, O + 12 = A

и G + 12 = S). Шифр тот же, но ключ изменился. Если шифр сложен и ключ достаточно длинный, он может быть *нетривиальным* (это слово-шифровка – оно означает «очень-очень трудный», или «тот, который за всю жизнь не одолеешь») для расшифровки неуполномоченной стороной без знания ключа.

Примечание С хорошей криптографией и надежными шифрами каждому могут быть известны детали алгоритма шифрования. Сила криптографии заключается в силе алгоритмического процесса конвертации и достаточно длинного ключа. Втайне от посторонних должен храниться ключ, но не шифр. Криптографические решения, требующие, чтобы шифр также держался в секрете, как правило, считаются подозрительными и, вероятно, слабыми.

При прочих равных условиях защита ключа возрастает по мере его увеличения. С увеличением длины ключа для неавторизованной стороны становится труднее конвертировать защищенное, зашифрованное сообщение обратно в исходное состояние, даже если ей известен алгоритм шифрования. В нашем примере простой подстановки даже ребенку довольно легко понять, как подсчитать, сложить или вычесть одну дополнительную (+–1) буквенную позицию для кодирования и декодирования сообщения или даже сложить или вычесть двенадцать (+–12), поменяв позиции. Но если наш ключ предполагает +–1 234 567 980 изменений позиции в алфавите, обычному человеку будет труднее дешифровать сообщение (хотя шанс на успех все же остается).

В классическом компьютерном мире цифровые ключи шифрования представляют собой просто длинную серию, казалось бы, случайно генерируемых 1 и 0. Цифровой ключ выглядит как 10101010101101000101010101010110011100 1010101. Чтобы воспроизвести зашифрованное сообщение, цифровой ключ применяется к текстовому сообщению в соответствии с алгоритмом шифрования. Если все сделано правильно, ключ и зашифрованное сообщение выглядят как случайный набор непредсказуемых битов.

Сегодня цифровые ключи шифрования обычно имеют размер от 128 до 4096 бит, хотя они могут быть меньше или больше в других, менее распространенных сценариях. Является ли конкретная длина битов безопасной, зависит от многих факторов, в том числе от алгоритма задействованного шифра, скорости, с которой все возможные позиции битов (называемые *пространством ключей*) могут быть угаданы, и хитростей, которые можно применить, чтобы свести к минимуму возможность угадывания методом «грубой силы». Сильные алгоритмы шифрования, которые труднее взломать, могут использовать ключи с меньшим количеством битов, тогда как более слабые алгоритмы часто требуют большей длины ключа для того же периода защиты. Длина битов для новых ключей, использующих те же алгоритмы, имеет тенденцию к увеличению со временем, чтобы компенсировать возрастающую вычислительную мощность и другие факторы взлома. Криптографические атаки со временем только усиливаются, что ослабляет защитную силу, обеспечиваемую длиной ключа.

Вы можете легко найти и увидеть примеры ключей шифрования, открыв цифровой сертификат на любом компьютере или устройстве. На рис. 3.2 показан 2048-битный ключ, извлеченный из цифрового сертификата.

```
30 82 01 0a 02 82 01 01 00 ad 0c 9f 7d 67 bc
70 6d 79 ba 25 05 3a 64 60 a0 e2 23 f3 ec 17
3b 6e 75 9e 88 50 fb d9 de 9c 62 2b de 19 a8
52 57 f0 09 62 2c 5e 64 45 9c 60 39 b5 14 48
2e 27 a4 db 82 c8 02 da ba 1d 91 51 fb 90 fa
bf f7 55 65 f1 cc 98 1a 3f 6b 0f 74 18 8f d4
cc 3b 44 ca 4d 53 df 95 94 72 20 d1 45 1a a5
9b 3b a8 f2 71 79 0e 6e ad 5b 87 ca 9e d1 7f
72 b8 2b 93 e0 36 69 31 7b 60 9a 44 f8 f4 a5
45 de 15 62 01 93 cd b3 ea e6 d1 d5 3c 1a 6b
cd ea a2 fd 7d 56 35 d0 c5 aa 5f 0e 6f 6e b2
c7 fa 8c 57 10 58 d3 0a 14 b4 2a fd 09 c6 ac
17 8e 3a ba 2c e8 dc 51 9f 29 a8 cb 39 e2 5a
8a 60 96 62 d7 64 05 94 d1 d7 8c 5b e3 0f fd
01 ed b4 5f 32 de b9 b1 b3 ea 3e 4c 6e d0 90
c4 82 eb 58 dc 6c 14 f0 4e 9f 1f 74 a3 76 26
30 bc 9a 97 91 fd 7c c8 c6 5a fd f8 54 ae 09
48 5a 50 b3 0c 3b 8f 43 f6 5f 02 03 01 00 01
```

Рис. 3.2. 2048-битный ключ шифрования из цифрового сертификата

Примечание Почти все цифровые криптографические ключи в большинстве компьютеров и устройств конвертируются в шестнадцатеричное представление (например, в базовой шестнадцатеричной системе исчисления) вместо представления их в базовых битах (то есть 1 и 0).

Вы можете увидеть общие рекомендуемые минимальные размеры ключей для популярных шифров, посетив www.keylength.com/. Шифры обычно разбиваются на два основных типа: симметричный и асимметричный.

Симметричные шифры

Если алгоритм шифрования использует один и тот же ключ для шифрования и дешифрования сообщения, то это *симметричный* шифр. Так, в приведенных ранее примерах простой замены ключи, используемые для шифрования открытого текста сообщения (например, 12 или 1234567980), – это те же ключи, которые применяются для шифрования или дешифрования зашифрованного сообщения обратно в исходную форму.

При прочих равных условиях симметричные шифры устойчивы, быстрее и легче проверяются, чем асимметричные (которые будут рассмотрены ниже в этой главе), и для них требуются ключи меньшего размера. С криптографической точки зрения хорошие симметричные шифры легче определить как сильные и надежные. Они менее сложны математически, требуют меньше предположений и догадок. Их сложнее атаковать. Соответственно, симметричные шифры обеспечивают большую часть шифрования данных в мире.

С 1970-х годов мир использовал много разных стандартов симметричного шифрования, включая стандарт Data Encryption Standard (DES), Triple DES (3DES), Международный алгоритм шифрования данных (International Data Encryption Algorithm, IDEA) и Rivest Cipher 5 (RC5). Все эти старые симметричные шифры сегодня считаются слабыми и взломанными.

С 2001 года самый популярный симметричный шифр известен под названием «расширенный стандарт шифрования» – *Advanced Encryption Standard*

(AES). Периодически, при необходимости, Национальный институт стандартов и технологий NIST (www.nist.gov) проводит публичные конкурсы по выбору новых стандартов криптографических шифров, чтобы заменить устаревшие и ослабленные алгоритмы шифрования. Более десятка команд, планирующих участие в конкурсах AES, представили свои симметричные шифры в NIST для рассмотрения в качестве новых национальных стандартов симметричных шифров. В процессе открытого и тщательного рассмотрения NIST выбрал шифр *Rijndael* и переименовал его в Advanced Encryption Standard. В настоящее время AES использует ключи 128-, 192- и 256-битной длины. Он очень хорошо выдерживал криптографические проверки и атаки в течение многих лет.

Примечание Ключ шифрования, который известен и используется только одним субъектом и никому преднамеренно не передается, называется *закрытым*, или *секретным*, *ключом*. Ключ шифрования, преднамеренно разделенный между несколькими субъектами, известен как *общий ключ*. Ключ, который может быть известен любому субъекту и использоваться им, – *открытый ключ*. Ключ, созданный для временного использования, называется *сеансовым ключом*.

Слабые стороны симметричного шифра Нельзя сказать, что симметричные шифры не имеют своих слабых сторон и недостатков. Имеют. Общие недостатки симметричного шифра включают в себя отсутствие возможности аутентификации и проблемы масштабирования обмена ключами.

Поскольку один и тот же ключ используется для шифрования и дешифрирования сообщения, любая сторона, имеющая доступ к ключу, может как зашифровать, так и расшифровать сообщения и, возможно, притвориться любой другой вовлеченной стороной с теми же ключами. С чисто криптографической точки зрения, если кто-то обвинил одну из других сторон в шифровании чего-либо, потому что каждая сторона располагает одним и тем же же симметричным ключом, обвиняемая сторона не может (опять же, с криптографической точки зрения) отвергнуть обвинения; такая проблема называется *неотказность* (невозможность отказа). Это нежелательная черта в криптографическом мире.

Сие также означает, что симметричные ключи сами по себе по тем же причинам труднее использовать в большинстве сценариев аутентификации, особенно когда целостность данных или предметная аутентификация желательна. Например, предположим, что Фред, Вилма и Дино используют один и тот же ключ шифрования. Фред мог зашифровать некоторые данные и отправить их Вилме, но утверждает, что они получены от Дино или изначально были созданы и зашифрованы именно им. Поскольку все используют один и тот же ключ, с чисто криптографической точки зрения Дино не может определить и доказать, кто действительно отправил или зашифровал сообщение. Фред может даже принять сообщение, изначально зашифрованное и отправленное Вилмой, расшифровать его, изменить со злым умыслом, снова зашифровать и отправить Дино, утверждая, что это от Вилмы. Дино не сможет сказать, откуда пришло сообщение, и невозможно определить, было ли подделано исходное сообщение, перед тем как он расшифровал и открыл его.

Вторая большая проблема заключается в том, что симметричные шифры нелегко использовать, так как число участников обмена растет. В небольшой группе, скажем из двух-трех человек, относительно легко безопасно обменять общий симметричный ключ, хотя даже тогда все участвующие стороны должны убедиться, что общий ключ точно и надежно передан всем участникам. Любым двум пользователям было бы трудно без ошибок читать, записывать или надиктовывать 256-битный ключ. Многим из нас трудно сообщить другому лицу даже номер кредитной карты с 16 цифрами.

Допустим, у вас есть сценарий с общим симметричным ключом, в котором участвует 1000 человек. Один или несколько участников должны найти способ безопасной передачи согласованного ключа всем другим уполномоченным сторонам. Как это сделать: писать, звонить, пересылать электронное сообщение и т. д.? Если вы выбрали письменную форму, как безопасно отправить написанное другим сторонам? Можно ли доверять почтовой системе и тем, кто ее обслуживает? Можно ли гарантировать, что только предполагаемый получатель откроет отправленное по почте сообщение? Если вы решили общаться по телефону, насколько можно доверять телефонной сети? Возможно, кто-то вас может подслушать? Не исключено. Что делать отправителю, если получатель недоступен? Он оставляет ключ на голосовой почте? Если получатель слышит ключ, может ли получатель точно расшифровать его? Если используется электронная почта, насколько можно доверять системе электронной почты и всем точкам транзита между отправителем и получателем? В любой системе электронной почты есть один или несколько администраторов электронной почты, которые могут читать поступающие сообщения. В любом случае, независимо от того, как вы общаетесь, можете ли вы представить себе тысячи разных людей, пытающихся безопасно и точно разделить 256-битный симметричный ключ без единой ошибки? Трудность безопасного обмена общим симметричным ключом увеличивается экспоненциально пропорционально количеству вовлеченных участников.

Теперь предположим, что некоторые из тысячи участников хотят получить дополнительные, меньшие группы, причем для каждой подгруппы будут использоваться разные общие ключи. Участники будут ответственны за отслеживание того, какие ключи используются людьми и группами. Идем дальше. Предположим, что каждый участвующий пользователь нуждается в гарантированном шифровании между всеми и каждой стороной, которую не может видеть никакой другой человек или сторона. Это потребует, чтобы каждый из тысячи участников имел отдельный общий ключ для каждого возможного союза других участников. Каждому пользователю, желающему отправить конфиденциальное сообщение всем остальным пользователям, необходимо отправить сообщение, используя 999 различных симметричных ключей, и отслеживать, какие ключи принадлежали какому союзу. Для этого потребуется 499 500 (1000 участников × 999 участников за вычетом одного / 2) симметричных ключей.

Ясно, что это было бы обременительным мероприятием, особенно если бы участникам периодически требовалось менять ключи, обеспечить постоянную и надежную защиту от текущих атак. Философы и криптографы века-

ми искали лучший способ безопасного обмена частной информацией и/или симметричными ключами (последний называется *обмен ключами*).

Асимметричные шифры

Святой Грааль шифрования предполагал, что должен быть найден метод, который позволял бы двум или более сторонам обмениваться симметричными ключами по ненадежному (даже заведомо злонамеренному) каналу связи без необходимости заранее установить частный метод связи для обмена симметричными ключами для каждого участника. В середине 1970-х годов несколько разных команд независимо друг от друга, с разницей в несколько лет, разработали почти одинаковые решения.

Целочисленная факторизация. Усиление рабочей нагрузки Во всех решениях использовалась полиномиальная математическая задача (например, A × B = C), которая была настолько сложна по своей природе, что сама нагрузка, необходимая для того, чтобы вернуться к ее отдельным составным частям (то есть множителям), уже становилась защитой. Математическая задача должна быть столь трудной, что, если кто-то узнает C (результат A × B), он не сможет легко отобразить A или B. Необходимый объем выполняемой работы (полиномиальная рабочая нагрузка, также известная как проблема целочисленной факторизации) является основной защитой для большей части современной криптографии с открытым ключом.

Примечание Требуемая рабочая нагрузка аналогична целочисленной факторизации и используется в различных, хотя и взаимосвязанных, типах асимметричных шифров, включая *задачу дискретного логарифмирования* и задачу *дискретного логарифмирования эллиптической кривой*. Они используют разные типы очень трудноразрешимой математики, но применяют при этом принципиально разные подходы.

Сегодня самые популярные асимметричные криптографические решения используют два больших простых числа (A и B), которые при умножении (или алгоритмическом представлении) давали бы намного больший результат (например, C). В качестве C, как указывалось в главе 2, используется простое число – это целое число больше 1, которое может быть разделено только на само себя или 1, чтобы получилось целое число (2, 3, 5, 7, 11, 13, 17, 19, 23 и т. д.). Любая другая комбинация приводит к остатку или дроби. Традиционным двоичным компьютерам по своей природе трудно создать по требованию и проверить простые числа. Если очень большие простые числа имеют значения A и B, то, даже если кто-то знает C, ему очень сложно разложить результат на его основные составляющие (то есть A и B).

Чтобы было более понятно, начнем с простого примера. Давайте использовать общую криптографическую математику – уравнение, представляющее метод защиты целочисленной факторизации: p × q = n, где p и q – простые числа, а n – результирующий математический результат и открытый ключ пары ключей (объясню чуть позже). Если p и q – достаточно большие числа, то p и q очень трудно получить, если дано только n.

Для примера, простейшего из возможных, предположим, что n = 15. Какие два простых числа, умноженных вместе, дали бы результат 15? Это довольно легко понять, тем более что простые числа меньше 15 – это 2, 3, 5, 7, 11 и 13. Не понадобится много времени, дабы понять, что p или q должны быть 3 или 5, потому что 3 × 5 = 15 и никакая другая комбинация простых чисел не дает при умножении 15. Теперь давайте добавим немного сложности к этой задаче. Предположим, что n = 187. Какие два простых числа надо перемножить, чтобы получить 187? Теперь умственное усилие, которое требуется, чтобы разложить 187 на два перемноженных простых числа, возрастет. Человек со средними математическими способностями все еще может это сделать, но это уже не так легко. Ответ: p или q равны 17 или 11, так как 17 × 11 = 187. Но предположим, что n = 84 773 093; каковы p и q? Сейчас уже потребуются недюжинные усилия. Вам придется перечислить все простые числа меньше 84 773 093 и умножить их в разных комбинациях, чтобы увидеть, какие из них приведут к 84 773 093. Большинство людей не смогут сделать это быстро. Да это и не удастся быстро без компьютера. Если вам интересно, ответ таков: p и q = 9539 и 8887. Компьютеры все еще могут с этим справиться очень быстро. Но теперь допустим, что n равно числу, представленному 4096 битами. Это число настолько велико, что в большинство калькуляторов даже не удастся его ввести, или они выдадут ошибку, или покажут символ бесконечности. 4096-битное число – это число, представляющееся 1234 десятичными цифрами. Его можно представить как $2^{4096} – 1$ возможных чисел. Найти такое число методом грубой силы – невыполнимая задача, и тем более выяснить два суперогромных простых числа, которые в результате перемножения должны его составить.

Когда криптографы пытаются объяснить, сколько угадываний потребуется, чтобы назвать правильно два простых числа, используемых для генерации 4096-битного числа, они приводят смешные, абсурдные сравнения, потому что это, возможно, единственный способ объяснить обычному человеку, как по своей сути сложен такой факторинг суперогромных простых чисел. Все возможности для 4096-битного числа превышают число всех атомов в известной Вселенной. Еще одно сравнение. Если у вас был бы миллион чего-то, скажем монет, для каждой звезды во Вселенной (а в каждой из 10 трлн галактик нашей Вселенной по 100 млрд звезд), то у вас все еще будет достаточно монет, чтобы представлять 1 % из возможных чисел 4096-битного числа. Это может быть гораздо меньше, чем необходимо, чтобы получить два больших простых числа, которые были использованы для его создания.

Некоторые наивные наблюдатели, плохо знакомые с такими большими цифрами, считают, что все, что нам нужно, – гораздо большая мощность вычислений. Возможно, всей вычислительной мощи на Земле хватит для этого? Мы бы ошиблись в таком предположении. Не только не хватит классических компьютеров, вычислительной мощности, памяти и дискового пространства во всем мире сегодня и в будущем, но просто не хватит энергии атомов для их питания, попробуй они сделать это. Необходимая рабочая нагрузка (и время) для факторизации уравнений большого числа простых чисел – вот что обеспечивает защиту.

Примечание Вся цифровая защита шифра обеспечивается тем, что трудно угадать ключи от всех возможных комбинаций или вернуть какому-то факторному математическому уравнению его исходные компоненты. Различные создатели шифров придумали математическую задачу, которую нелегко решить, если у вас нет какой-то его части. Вы можете знать, что A + B = C, но даже если вы знаете A и C, то не можете легко выяснить, каково B. Трудность выяснения неизвестного значения – это то, что дает шифру его защитные возможности.

Пары открытых и закрытых ключей С помощью асимметричного криптографического метода использования большого простого числа каждая участвующая сторона генерирует (или получает) пару ключей, где два ключа пары криптографически связаны друг с другом. Один ключ хранится в секрете и никому не передается (*закрытый ключ*). Другой может быть распространен по всему миру (он называется *открытый ключ*). Один ключ шифрует, другой может расшифровать, и наоборот. Это очень важно для концепции асимметричной криптографии и всего, что она может сделать, поэтому вам следует понимать эти два момента, если вы хотите понять идею асимметричной криптографии. Поскольку один ключ используется для шифрования, а другой – для расшифровки, такой тип шифра известен как *асимметричный*.

Хотя оба ключа пары можно использовать для шифрования сообщения другому лицу и наоборот, важно, кто классифицирует закрытый и открытый ключи. Помните, что закрытый ключ никогда никому не передается. Поэтому если кто-то хочет отправить конфиденциальное сообщение другому лицу, отправитель должен использовать открытый ключ получателя для шифрования сообщения. Это будет сохранять конфиденциальность сообщения, пока получатель не использует свой закрытый ключ для расшифровки. Так как ни у кого больше нет личного ключа получателя, никто не может расшифровать сообщение.

Примечание При асимметричном шифровании мы должны использовать открытый ключ получателя для шифрования ему сообщений.

При асимметричном шифровании каждой участвующей стороне требуется собственная пара секретного и открытого ключей, но только по одной паре ключей на человека для безопасного общения друг с другом. Вместо необходимых для безопасной связи друг с другом 499 500 различных симметричных ключей при асимметричной системе нужно будет всего 1000 пар закрытых/открытых ключей (или всего 2000 ключей).

Цифровая подпись Пользователи асимметричной криптографии могут также применять свои пары ключей для аутентификации и цифровой подписи контента. *Цифровая подпись* служит подтверждением, что подписанный контент представляет собой именно то, что было в нем в момент подписания. Для подписи контента пользователь использует свой закрытый ключ для «шифрования» содержимого (или результат хеширования сообщения на

данный момент). Мы не называем этот процесс «шифрованием», поскольку любой, у кого есть соответствующий открытый ключ (который теоретически может быть у любого), мог расшифровать и прочитать сообщение. Такое сообщение не может считаться конфиденциальным или зашифрованным, раз любой способен прочитать его.

Вместо «шифрования» мы называем этот процесс цифровой подписью. Любой контент, подписанный закрытым ключом, может быть раскрыт только с использованием связанного открытого ключа. Если содержимое может быть проверено («расшифровано») с помощью соответствующего открытого ключа, оно должно быть подписано связанным закрытым ключом, потому что единственное, что может сделать связанный открытый ключ, – это «расшифровать» то, что подписано соответствующим закрытым ключом. Подобные процессы могут быть использованы для аутентификации идентификационных данных пользователя, участвующего в криптографических операциях, ряд которых будет рассмотрен позже в этом разделе. Обычные шифры цифровой подписи включают алгоритм цифровой подписи (Digital Signature Algorithm, DSA) и алгоритм DSA на эллиптических кривых (Elliptic Curve Digital Signature Algorithm, ECDSA).

Сообщение может быть зашифровано и подписано, если необходимы обе защиты. Если Фред должен отправить подписанное и зашифрованное сообщение для Вилмы, то он подписывает свое сообщение, используя свой личный ключ, и затем шифрует его с помощью открытого ключа Вилмы.

Примечание Цифровая подпись и проверка немного сложнее, чем указано в описании выше. Об этом мы еще поговорим позже.

Поскольку каждая сторона имеет свою собственную, уникальную пару ключей, и только эта пара ключей может шифровать и дешифровать сообщения между собой, асимметричная криптография также позволяет аутентифицировать субъект и сообщение. Каждая задействованная пара ключей может быть привязана к определенному субъекту. Это позволяет осуществить *отказ*.

Обмен ключами Ввиду того что симметричные ключи более безопасны при небольших размерах, они используются для выполнения большей части шифрования сообщений в мире, а асимметричные шифры часто применяются только для обеспечения безопасной передачи общих симметричных ключей между двумя сторонами. Асимметричная криптография позволяет обмен симметричными ключами по ненадежным сетям без необходимости предварительно устанавливать безопасный, доверенный канал. Краткое описание процесса обмена ключами выглядит примерно так:

1. Клиент и сервер соединяются друг с другом.
2. Сервер отправляет клиенту открытый ключ сервера своей пары асимметричных ключей.
3. Клиент использует открытый ключ сервера для шифрования созданного нового «сеансового» симметричного ключа клиента обратно на сервер.

4. Сервер и клиент теперь используют общий симметричный сеансовый ключ для отправки зашифрованного содержания друг к другу туда и обратно.

В реальном мире при использовании асимметричного обмена ключами для безопасной передачи общего симметричного ключа между клиентом и сервером есть еще несколько шагов и сложностей (которые будут рассмотрены позже), но это достаточное резюме основных шагов асимметричного обмена ключами на данный момент.

Распространенные типы асимметричной криптографии включают Rivest, Shamir, Adleman (RSA), Diffie–Hellman (DH), криптографию с эллиптическими кривыми (ECC) и Эль-Гамаль. RSA является самым популярным используемым асимметричным шифром, на который, возможно, приходится 95 % всех асимметричных шифров. Хотя все асимметричные шифры используются для обмена ключами, Diffie–Hellman, также известный как Diffie–Hellman–Merkle, часто ассоциируется с реализациями только для обмена ключами, как и менее используемый Elliptic Curve Diffie–Hellman (ECDH). Размеры ключей RSA и DH сегодня варьируются от 2048 до 4096 бит, и они удваиваются по длине примерно каждые 7–10 лет в целях противостояния криптографическим атакам, которые становятся все изощреннее.

Примечание Компания RSA Security, разработавшая шифр RSA, предлагала постоянный денежный приз для криптографа, который взломает все увеличивающиеся в размерах ключи RSA. Самый большой ключ RSA, который на сегодняшний день был публично взломан в 2010 году, использовал факторизацию 768 бит (https://eprint.iacr.org/2010/006.pdf). Он включал 232-значное число – большое, но не столь большое, как 2048-битный или 4096-битный ключи, которые обычно рекомендуются сегодня. Тем не менее даже до взлома 768-битного ключа RSA без объяснения причин перестала организовывать конкурс. Многие наблюдатели считают, что грядущую реализацию квантовых компьютеров для факторизации можно считать основным фактором (извините за каламбур) принятия такого решения.

Инфраструктура ключей доверия и открытых ключей Для того чтобы асимметричные системы шифрования работали, люди, общающиеся с ними, должны быть уверены, что открытый ключ каждого пользователя действителен и принадлежит тому, кому, по их мнению, он принадлежит. В начале применения асимметричного шифрования человеку, который хочет что-то отправить адресату, было достаточно того, что они уже знали свой открытый ключ, и адресат верил, что человек, который отправил послание, – это на самом деле тот, кто имеет действительный, связанный закрытый ключ.

Но поскольку число людей в асимметричном канале увеличивается, не каждый участник может знать всех других участников и доверять им. Одно из оснований доверять человеку с открытым ключом, которого вы не знаете, – это поручительство за такого человека со стороны того, кого вы хорошо знаете и кому доверяете. Например, предположим, что Вилма хотела общаться асимметрично с Дино, но не знала его и не имела никаких основа-

ний ему доверять. Но она была в курсе, что Фред знает Дино и доверяет ему, так что может поручиться за него и за действительность открытого ключа Дино. Фред мог подписать открытый ключ Дино своим личным ключом, который Вилма сможет затем проверить с помощью открытого ключа Фреда. Это называется *одноранговым* (peer-to-peer) *доверием,* или *веб-доверием*. Так работает популярная и довольно хорошая конфиденциальная программа шифрования Pretty Good Privacy, PGP. Но одноранговые системы доверия работают не так хорошо, когда количество участников увеличивается, особенно в глобальных асимметричных системах, где большинство участников не знают друг друга.

Инфраструктура открытых ключей (public key infrastructure, PKI) – это часто используемая криптографическая структура и семейство протоколов. Она применяется в компьютерном мире для обеспечения доверительных отношений между несвязанными сторонами. Вы можете прочитать или услышать множество различных описаний того, что такое PKI и зачем она нужна, но в своем базовом применении PKI обеспечивает аутентификацию идентификаторов субъектов, участвующих в криптографических транзакциях, и их асимметричных криптографических ключей. Без этого требования вам не понадобится PKI.

PKI выдает проверенным субъектам «цифровые сертификаты», которые являются криптографически защищенными документами, подтверждающими достоверность личности субъекта и связанной с ним пары асимметричных ключей. На практике субъект (или что-то от его имени) генерирует пару асимметричных ключей для использования субъектом. Субъект передает свой открытый ключ в PKI (помните, что мы не делимся закрытыми ключами). Затем *служба сертификации* PKI должна подтвердить личность субъекта, представляющего открытый ключ.

Уровень подтверждения личности, требуемый субъектом от PKI, определяет уровень *гарантии* (или *доверия*), который PKI может засвидетельствовать. Если уровень гарантии очень низкий (скажем, только действительный адрес электронной почты), выданный цифровой сертификат считается малодоверительным. Если уровень идентичности владения и доказательств существенный, как, скажем, в случае личного посещения и передачи подтвержденных копий свидетельства о рождении и национального удостоверения личности проверяющему человеку, гарантия считается высокой.

В любом случае основной задачей PKI является проверка личности субъекта, представляющего свой открытый ключ. Если личность субъекта подтверждена, PKI добавляет некоторую дополнительную информацию (например, действительность даты, имя субъекта (субъектов), серийный номер сертификата, а также название и идентификатор центра сертификации) и подписывает открытый ключ субъекта (и другую информацию) закрытым ключом PKI. Это создает цифровой сертификат. На рис. 3.3 показан пример части цифрового сертификата с полем открытого ключа. Теоретически любой субъект, который доверяет PKI (выдавшей определенный цифровой сертификат), будет доверять любому цифровому сертификату, созданному PKI и представленному субъектом. Субъект, представляющий цифровой сертификат, по сути, говорит: «Я тот, за кого себя выдаю, и человек, которому вы доверяете, проверил это».

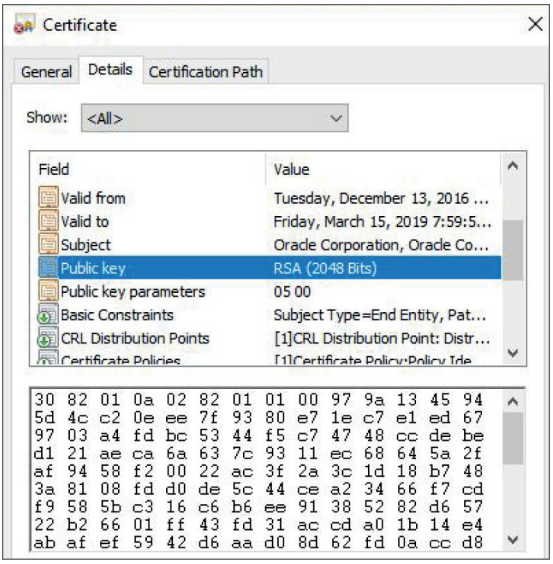


Рис. 3.3. Детали цифрового сертификата

PKI можно сравнить с Департаментом транспортных средств (DMV), используемым в Соединенных Штатах. Владельцы лицензии DMV должны в значительной степени подтвердить свою личность в DMV, чтобы получить водительские права. После того как личность водителя (т. е. субъекта) будет успешно подтверждена (гарантирована), DMV получит изображение субъекта, добавит другую информацию и выдаст лицензию DMV, скрепленную печатью с изображением государственного герба (что-то вроде реального цифрового сертификата). Если водителя остановили правоохранительные органы или он хочет купить что-то, требующее подтверждения возраста, его, вероятнее всего, попросят предъявить DMV-лицензию. Офицер или продавец доверяют лицензии DMV и поэтому будут полагаться на информацию, указанную в лицензии и полученную в процессе проверки.

Большая часть интернета работает на PKI. Если вы подключаетесь к веб-сайту с помощью протокола Hypertext Transfer Protocol Secure (HTTPS), то этот веб-сайт имеет цифровой сертификат HTTPS/TLS, подписанный и выданный PKI. Вы не можете лично доверять PKI, но это делает ваша операционная система или соответствующее программное обеспечение. Когда вы подключаетесь к веб-сайту через браузер по протоколу HTTPS, веб-сайт отправляет вам (или фактически вашему браузеру) копию своего цифрового сертификата. Цифровой сертификат, подписанный PKI, удостоверяет имя веб-сайта (часто по URL), открытый ключ веб-сайта и другую важную информацию. После проверки ваш браузер сгенерирует новый общий симметричный ключ сеанса, который затем безопасно отправляется на веб-сайт (с использованием открытого ключа веб-сайта). Потом и сервер, и клиент могут начать безопасную связь с использованием симметричного ключа (см. рис. 3.4).

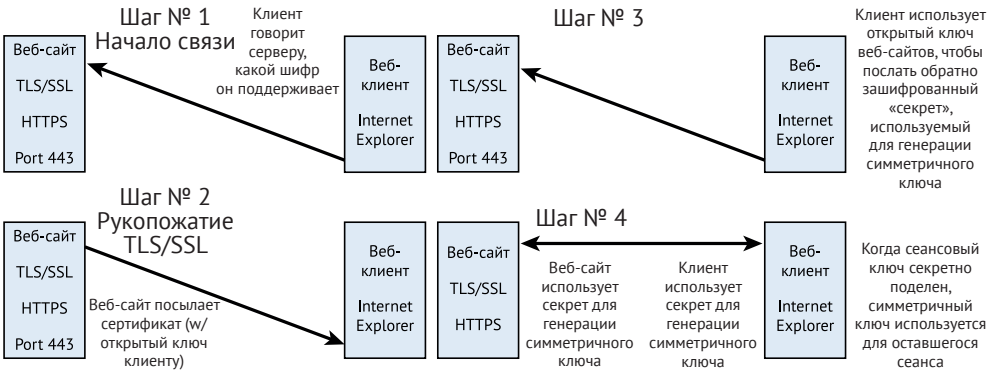


Рис. 3.4. Веб-сервер и клиент, использующие HTTPS и цифровой сертификат при взаимодействии друг с другом

Другой популярный пример использования PKI: при загрузке нового программного обеспечения популярных поставщиков оно будет поставляться с цифровым сертификатом, подтвержденным тем, кто подписал программное обеспечение (или связанный хеш, о чем мы подробнее поговорим позже). Это позволяет загрузчику (точнее, обычно браузеру от его имени) подтвердить, что программное обеспечение не изменилось с момента подписи тем, кто подписал программное обеспечение или хеш. Не важно, где это программное обеспечение перемещалось между подписавшей стороной и получателем, путешествовал ли он по доверенным или ненадежным каналам, сколько посредников участвовало или как давно произошло подписание (в разумных пределах). Подтвержденный цифровой сертификат и сопровождающий проверенный хеш сообщают пользователям, что они могут положиться на программное обеспечение таким, каким оно являлось на тот момент, когда было подписано и получено от того, о ком сказано в сертификате.

Недостатки асимметричных шифров Асимметричные шифры позволяют шифровать и обмениваться ключами через ненадежные каналы и могут быть использованы для проверки подлинности. Независимо от надвигающихся угроз, создаваемых квантовыми компьютерами, асимметричные шифры довольно хорошо выдержали десятилетия криптографических атак. Тем не менее у них есть свои проблемы.

Самый большой недостаток заключается в том, что асимметричные шифры по своей природе математически более сложны, чем симметричные, а в мире компьютерной безопасности сложность часто является врагом безопасности. Большинство асимметричных шифров используют два криптографически связанных ключа, разделенных только математическим уравнением, опирающимся на сложность факторизации. По сравнению с симметричными шифрами повышается вероятность того, что кто-то узнает, как «ускорить математику» или более быстро определить основную математику, лежащую в основе уравнения с простыми числами. И реальность показывает, что так и происходит (об этом позже). При прочих равных условиях асимметричные

ключи, чтобы компенсировать успехи в шифровании, обычно длиннее симметричных (но не всегда) и со временем увеличиваются в размерах быстрее и больше, чем симметричные ключи.

Хеширование

Другая важная интегральная криптографическая функция – хеширование. *Хеш-алгоритмы*, также называемые *хеш-функции* или просто *хеши*, используются для создания уникальных результатов вывода для уникальных входных данных контента. Они используют *односторонние* (one-way) криптографические функции, которые создают/выводят уникальный репрезентативный набор символов или битов (известных как хеш, результат хеширования, цифровая подпись или дайджест сообщения) для проверки уникального контента. Хеш-функции создают криптографические «цифровые отпечатки» контента, который они хешируют. Хеш-функции могут использоваться для криптографической подписи и проверки целостности контента и криптографических объектов.

Когда результат хеширования (часто известный просто как хеш или дайджест сообщения) криптографически привязан к конкретному субъекту криптографической идентификации (например, пользователю, устройству или услуге), он называется *цифровая подпись*. Проверенная цифровая подпись позволяет получателю подписанного контента быть уверенным, что подписанный контент не был изменен с момента его подписания аутентифицированным подписавшим. Безопасные, надежные хеш-функции имеют четыре важных свойства:

- для каждого уникального входа должен генерироваться уникальный результат вывода. Этот тип защиты называют *устойчивостью к конфликтам* (collision resistance);
- каждый раз, когда один и тот же вход хешируется, он должен давать один и тот же результат хеширования;
- никаких два разных входа не должны приводить к одному и тому же результату хеширования. Этот тип защиты известен как *второй уровень защиты прообраза от искажений* (second preimage resistance);
- если задан вывод хеша, содержимое ввода должно быть нетривиальным, чтобы получить ввод. Этот тип защиты получил официальное название *защита прообраза* (preimage resistance).

Хороший хеш имеет все перечисленные атрибуты и даже при длительной атаке сохраняет все возможности защитного хеша. Защита от повреждений связана со второй защитой прообраза и похожа на него, но это не то же самое. И то, что они оба хороши, не гарантирует защиту прообраза, поскольку это несвязанные атрибуты. Если хеш-код становится восприимчивым к любому из этих атрибутов, он считается слабым и не должен далее использоваться. Алгоритмы хеширования обычно приводят к результатам хеширования фиксированной длины независимо от входных данных. Общая длина хеша варьируется от 128 до 256 бит. На протяжении многих лет было много различных общепринятых стандартов хеша, включая Message Digest 5 (MD5),

Windows LANManager (LM), Windows NT (NT) и Secure Hash Algorithm-1 (SHA-1). Все эти предыдущие стандарты, кроме NT, считаются слабыми и взломанными.

На сегодняшний день наиболее популярным алгоритмом хеширования является Secure Hash Algorithm-2 (SHA-2 или SHA2), хотя в 2015 году NIST рекомендовал, чтобы вместо него использовался преемник SHA-2 – Secure Hash Algorithm-3 (SHA-3 или SHA3), поскольку SHA-2 со временем ослабевает в связи с усилением криптографических атак.

Пока что большинство все еще используют SHA-2. SHA-2 имеет много разных выходных размеров, в частности 224, 384, 256 и 512 бит.

В табл. 3.1 показаны некоторые результаты хеширования для слова «frog» (лягушка) с использованием обычных примеров хешей.

Таблица 3.1. Пример хешированных выходов для слова «frog»

Хеш-алгоритм	Результат хеширования для слова «frog»
MD5	938C2CC0DCC05F2B68C4287040CFCF71
SHA-1	B3E0F62FA1046AC6A8559C68D231B6BD11345F36
SHA-2	74FA5327CC0F4E947789DD5E989A61A8242986A596F170640AC90337B 1DA1EE4
SHA-3 (512)	6EB693784D6128476291A3BBBF799d287F77E1816b05C611CE114AF 239BE2DEE734B5Df71B21AC74A36BE12CD629890CE63EE87E0F53BE987 D938D39E8D52B62

Слабые стороны хеширования Как и асимметричные шифры, алгоритмы хеширования считаются несколько загадочными. Судя по всему, они выполняют работу, для которой предназначены, но никто не уверен, что хеш-алгоритм может соответствовать всем четырем из вышеперечисленных требований – или если они работают в настоящее время, то как долго это будет продолжаться, прежде чем кто-то найдет ошибку. Большинство предыдущих стандартов хеширования в свое время также считались безопасными и сильными, пока с течением времени не были ослаблены различными криптографическими атаками. Криптографы находят алгоритмы хеширования одними из самых сложных криптографических функций, в отношении которых можно что-то точно доказать или опровергнуть.

Применение криптографии

Основные криптографические функции симметричных шифров, асимметричных шифров и функции хеширования предоставляют широкий спектр услуг для компьютерного и, соответственно, для реального мира. Без них большая часть интернета и реального мира в том виде, в каком мы их сегодня знаем, были бы невозможны. Общие криптографические их применения включают в себя следующие:

- шифрование;
- аутентификацию;
- цифровую подпись;
- HTTPS/TLS;

- криптовалюты;
- смарт-карты, виртуальные смарт-карты;
- шифрование диска;
- сетевое шифрование;
- шифрование электронной почты;
- виртуальные частные сети;
- беспроводную безопасность;
- кодирование и подпись документов;
- стеганографию;
- анонимность;
- токенизацию;
- незаметность стирания данных.

Криптография защищает мировые сети, компьютеры, транспортные средства, правительства, валюты и цифровую идентификацию и помогает аутентифицировать и защищать весь цифровой контент. Мир без помощи надежной криптографии выглядел бы даже ближе к 1860-м, чем к 1960-м. На цифровую криптографию полагаются слишком во многом – вот почему все, что может легко и внезапно сломаться, вызывает трепет. Квантовые вычисления – самая большая угроза для самой популярной на сегодняшний день цифровой криптографии, с которой когда-либо сталкивался мир. Вы можете задаться вопросом, как любой компьютер может одолеть сегодняшнюю криптографию, особенно если учесть то, о чем я говорил выше, – что в даже известной Вселенной не хватило бы энергии, достаточной, чтобы превзойти ее достижения. Что ж, это было, когда у нас были только классические бинарные компьютеры и мы рассчитывали лишь на атаки методом грубой силы. Изобретение новых квантовых алгоритмов и реальных, работающих квантовых компьютеров изменило положение дел.

Как квантовые компьютеры могут взломать криптокоды

Квантовые компьютеры способны взломать многие формы традиционных криптокодов из-за присущих им квантовых свойств, описанных в главе 1 (таких как суперпозиция и запутывание), в сочетании с квантовыми алгоритмами, которые используют эти свойства и сокращают математику. Тема этого раздела – как квантовые компьютеры могут взломать многие виды современных криптокодов. Далее мы обсудим, что традиционные квантовые компьютеры криптографии могут и не могут взломать.

Сокращение времени

Существует расхожее мнение: единственное, что невозможно вернуть в нашей жизни, – время. Это не всегда верно, особенно в квантовом мире. Отчасти мы любим и используем компьютеры именно потому, что они способны выполнять некоторые задачи очень быстро. Тем не менее есть мно-

го потенциальных проблем, которые даже самые быстрые компьютеры не могут решить. Как уже упоминалось ранее, так обстоит дело со многими криптографическими математическими проблемами. Именно неспособность компьютера, и даже сети из миллионов очень быстрых компьютеров, решить некоторые из известных сегодня математических задач обеспечивает бóльшую часть защитных возможностей надежной криптографии.

Но это не значит, что никто не решается даже попытаться. Защитники и нападающие изобретают проблемы и их решения, способные сократить или продлить время, которое обычно требуется для совершения определенных действий. Эти решения и проблемы классифицируются по следующему признаку: насколько они увеличивают или уменьшают конкретный (наихудший) случай решения в реальных временных масштабах.

Если мы подключим дополнительные ресурсы для решения проблемы, например задействуем больший объем памяти, более быстрый процессор, отведем больше места на жестком диске или просто добавим больше компьютеров, и если такое добавление не приведет к более быстрому решению, мы называем его *решением с постоянным временем* (constant time solution). Например, если для создания 100 виджетов требуется один человек в день, а мы добавляем еще человека и они вместе по-прежнему делают только 100 виджетов в день, дополнительный ресурс показывает, что на выполнение работы в любом случае требуется фиксированное время. Если вы пытаетесь решить проблему быстрее, решения с постоянным временем ничем вам не помогут – такие усилия контрпродуктивны. Если вы пытаетесь защищаться от злоумышленника и если все, что у него есть, – постоянное время атаки, это ваше преимущество.

Если добавление ресурсов ускоряет решение, то это увеличивает шансы атакующего и уменьшает шансы защитника. Если при появлении дополнительного ресурса множится число виджетов, создаваемых каждым добавленным индивидуумом, это называется *линейным временем* (или *прямым временем*). Например, 1 человек делает 10 виджетов, 2 человека делают 20 виджетов, а 3 человека – 30 виджетов (каждый работник делает только 10 виджетов, но чем больше коллектив, тем больше результат).

Если при добавлении каждого дополнительного ресурса скорость удваивается по сравнению с предыдущим показателем, это называется *экспоненциальным временем*. Например, 1 человек делает 100 виджетов в день, 2 человека делают 200 виджетов, 3 человека – 400 виджетов, 4 человека – 800 виджетов и т. д. Так, по сути, и работают бинарные компьютеры (т. е. по формуле 2^n). Каждый добавленный бит удваивает мощность предыдущего бита (битов). Любые добавления ресурсов, будь то компьютерный ресурс или алгоритм, который может завершить решение быстрее, чем экспоненциальное время, создают угрозу для систем, которые защищаются с использованием экспоненциального времени или меньше его.

Математики и криптографы создали задачи и решения, которые требуют гораздо бóльших усилий, чем в случае экспоненциального времени. Решения шкалы времени, известные как полином, квадратный корень, квадратичный и факториал, – все это огромные улучшения экспоненциального времени, известные как *суперэкспоненциальное вре*мя масштабных решений.

Любой ресурс, обеспечивающий такие улучшения времени, является угрозой для защищаемого, полагающегося на экспоненциальную защиту времени. В частности, любая криптографическая атака, которая превышает экспоненциальное время, является угрозой для криптографических решений, полагающихся на экспоненциальную защиту времени. Кубиты и квантовые алгоритмы дают суперэкспоненциальные задачи и решения. Если вы рассуждаете о криптографической проблеме или решении, работающем только в экспоненциальном времени или меньше, то это обычно никого не волнует. Но если речь идет о решении, работающем в одной из суперэкспоненциальных шкал времени, особенно одним из самых быстрых методов, таких как факториал, это озаботит любого, кто знаком с криптографией, поскольку добавление каждого ресурса дает огромное преимущество в решениях проблем относительно «нормальной» экспоненциальной шкалы времени.

Для получения дополнительной информации о временны́х решениях обратитесь к следующим источникам: https://rob-bell.net/2009/06/a-beginners-guide-to-big-o-notation/ и https://stackoverflow.com/questions/4317414/polynomial-time-and-exponential-time.

Квантовые алгоритмы

Квантовые алгоритмы представляют собой серию (математических) шагов, основанных на квантовых теориях и свойствах, которые, если их осуществить на квантовом устройстве, дают определенный результат. На протяжении десятилетий большая часть того, что могли сделать квантовые компьютеры, описывалась только в теоретических работах. Работающие квантовые компьютеры и устройства, позволяющие испытать что-то новое, сместили акценты с теоретической квантовой механики на реальность. При наличии работающего квантового компьютера ученые смогли применить на практике алгоритмы, с помощью которых решается задача, и увидеть результаты. Большинство квантовых алгоритмов считаются революционными, поскольку при том увеличении скорости, которую обеспечивают квантовые компьютеры по сравнению с традиционными, можно получить ответы на проблемы, некогда считавшиеся нерешаемыми. В конечном счете большая часть современной криптографии может быть взломана с использованием квантовых свойств, компьютеров и алгоритмов.

Известны десятки квантовых алгоритмов. Довольно внушительный список основных алгоритмов представлен здесь: https://en.wikipedia.org/wiki/Quantum_algorithm и здесь: https://quantumalgorithmzoo.org/. Многие доказали, по крайней мере в теории, что квантовый компьютер может выполнить ряд задач лучше, чем классический. Другие, основываясь на квантовой теории, использовали квантовые компьютеры для более быстрого решения реальных проблем, чем это возможно при помощи традиционных компьютеров. Несколько алгоритмов стали настолько значимыми для квантовых вычислений и прогресса квантовой криптографии, что в квантовых и криптографических кругах их обсуждают по тысяче раз на день на всевозможных онлайн-ресурсах. Следующие три наиболее важных квантовых алгоритма, обещающих разрушить сегодняшнюю традиционную криптографию, рассматриваются ниже.

Алгоритм Гровера

После алгоритма Шора (Shor), о котором будет рассказано далее, алгоритм Лова Гровера (Lov Grover) является, вероятно, наиболее обсуждаемым и привлекательным квантовым алгоритмом. Алгоритм Гровера по существу доказал, что ответ на любую неструктурированную/неупорядоченную задачу поиска (математическую задачу) может быть получен намного быстрее с помощью квантовых компьютеров, чем с помощью традиционных классических бинарных компьютеров. Гровер показал, что, вместо того чтобы вычислять все возможные N решений линейно по одному, как было необходимо при применении классических компьютеров, это можно сделать на квантовых компьютерах с количеством кубитов $\log(N) + 1$, при их числе корень квадратный из N. Алгоритм Гровера обеспечивает квадратичное ускорение рабочей нагрузки.

Предположим, что математический ответ (или поиск) может быть любым из 1 000 000 возможных ответов (т.е. N = 1 000 000). Традиционный компьютер при наихудшем сценарии должен был бы выполнить 1 000 000 операций, чтобы найти этот ответ. Алгоритм Гровера показал, что квантовый компьютер с 7 кубитами (log (1 000 000) + 1 кубит) может найти тот же ответ, используя число операций, представляющее квадратный корень вышеназванного числа, то есть не более 1000 операций. Квадратный корень решения по существу удваивает рабочую нагрузку экспоненциальной задачи (помните, что каждое увеличение показателя на одну единицу удваивает предыдущую базовую сумму). Алгоритм Гровера может помочь взломать симметричные (и, в гораздо меньшей степени, асимметричные) криптографические ключи и решать некоторые типы криптографических хеш-функций гораздо быстрее на квантовых компьютерах, чем на классических компьютерах. Эксперты рекомендуют удвоить размер симметричных ключей и хешей, чтобы сохранить их относительную защиту в постквантовом мире.

Преобразование Фурье

Жан-Батист Жозеф Фурье, который умер в 1830 году, предложил несколько физических представлений, известных сегодня как ряды Фурье. Алгоритм преобразования Фурье принимает волну (или волновую функцию) и разлагает ее на составные части. Происходит примерно то же, что и при приготовлении некоторых блюд.

Примечание Аналогия с кулинарией позаимствована отсюда: https://better-explained.com/articles/an-interactive-guide-to-the-fourier-transform/.

Преобразование Фурье анализирует волну и разбивает ее на дискретные величины пиков волны: значение, амплитуда (то есть углы), частота и смещение. По сути, это позволяет разбить любую волновую функцию и восстановить ее в виде суммы частотных компонентов. Это способ связывания и преобразования квантовых частиц через их спектр двойственности волна–частица. Продолжим кулинарную аналогию. Представьте, что у вас есть вкусный овощной суп. Пусть волна будет готовым супом. Преобразование

Фурье позволит любому, кто придерживается того же рецепта (например, 1 чашка куриного бульона, 2 чашки нарезанной кубиками моркови, 1 чашка нарезанного кубиками лука и т. д., готовить при температуре 150 °C в течение одного часа), приготовить точно такой же суп, и наоборот. Многие другие квантовые решения и алгоритмы, такие как алгоритм Шора (см. ниже), своим успехом обязаны квантовому преобразованию Фурье. Преобразование Фурье позволяет квантам при вычислениях переходить от свойств частиц к волновым свойствам и обратно, в зависимости от преимуществ каждого свойства.

Алгоритм Шора

Математик Питер Шор (Peter Shor) – в современную эпоху традиционной асимметричной криптографии, пожалуй, самая известная фигура в мире квантовых вычислений и взлома. В 1994 году в своей статье под названием «Алгоритмы для квантовых вычислений: дискретные логарифмы и факторинг» (Algorithms for Quantum Computation: Discrete Logarithms and Factoring) он привел алгоритм, который, по сути, позволял квантовым компьютерам очень быстро вычислять большие коэффициенты в уравнениях с простыми числами (https://pdfs.semanticscholar.org/6902/cb196ec032852ff31cc178ca822a5f67b2f2.pdf). Алгоритм Шора обеспечил как минимум экспоненциальное улучшение времени и, вероятно, улучшение полиномиального времени для факторинга больших простых чисел. При использовании квантовых компьютеров с достаточно устойчивыми кубитами алгоритм Шора может обеспечить вычисление очень сложных уравнений с простыми числами за время от нескольких секунд до минут. Его алгоритм был и остается революционным. После этой публикации, еще до практического применения, которое позволило бы проверить теорию, компьютерный мир осознал последствия: квантовые компьютеры могут стать и, вероятно, в конечном итоге станут более мощными, чем классические компьютеры. Эксперты по криптографии тотчас поняли, что большинство современных шифровальных ключей с открытым ключом у них в руках! Прежде всего по этой причине публикуется данная книга. С тех пор мир криптографии будоражит предчувствие того момента, когда квантовые компьютеры начнут взламывать традиционные асимметричные шифры.

Не вдаваясь глубоко в математику (это не особенно сложно, просто ее много), можно сказать, что алгоритм Шора позволяет квантовым компьютерам быстрее вычислять простые числа с помощью уравнения, в котором чисто случайным предположением задается одно из простых чисел. Оно превращает его в гораздо более точное предположение, а затем таким путем быстро находятся фактические простые числа. Алгоритм Шора использует математические соотношения двух задействованных простых чисел так, что это резко сокращает необходимое количество догадок по сравнению с классическим методом. Требуется все еще очень много догадок, но когда эти предположения делаются с использованием квантового свойства суперпозиции, они могут быть сгенерированы компьютером с квантовыми логическими элементами почти мгновенно. Во всех этих догадках присутствует два правильных простых числа. Все догадки рассматриваются как «стадия 1» или «часть I» алгоритма Шора.

Примечание Сложно найти лучшее объяснение алгоритма Шора со всей основной математикой и уравнениями, чем вот в этом видео: www.youtube.com/watch?v=lvTqbM5Dq4Q.

На втором этапе Питер Шор также определил, как быстро выяснить, в какой из множества созданных догадок присутствуют два правильных простых числа. Хотя это осуществляется математически, гораздо проще объяснить это с помощью образного сравнения (рис. 3.5).

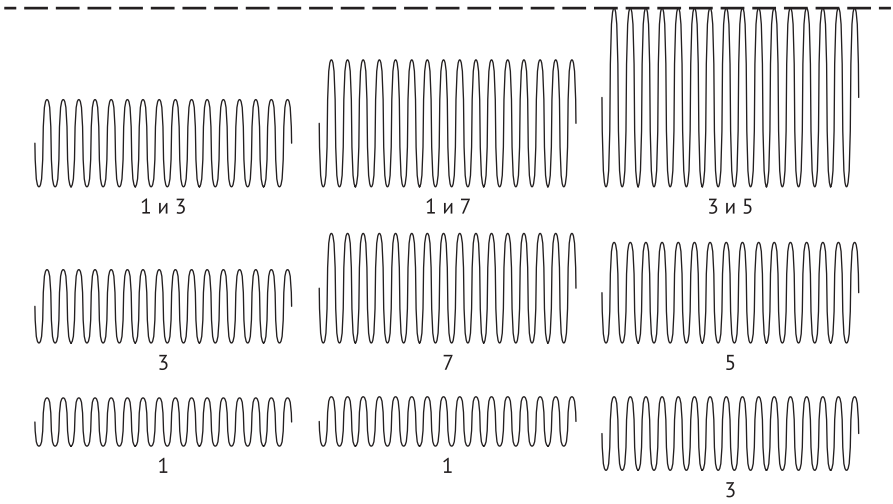


Рис. 3.5. Пример, позволяющий лучше понять уравнение с простыми числами. Два маленьких правильных простых числа создают при решении уравнения самый большой пик волны

Каждое предположение простого числа преобразуется в синусоиду (с использованием преобразования Фурье). После этого синусоида каждой догадки добавляется к другой возможной угадываемой синусоиде. Два правильных ответа создают синусоидальную волну с самыми высокими пиками и самыми низкими впадинами. Все синусоидальные волны других неправильных догадок мешают друг другу больше, вызывая меньшие пики и впадины и, следовательно, меньшую общую синусоидальную волну. В конце концов, все, что нужно квантовому компьютеру, чтобы найти два правильных очень больших простых числа, – найти самую высокую синусоиду. Этот последний шаг алгоритма Шора очень похож на то, как мы выделяем самого высокого человека на групповом фотоснимке. Для этого требуется несколько секунд, хотя иногда (теоретически) могут понадобиться и минуты. По сравнению с миллиардами лет, которые могут потребоваться классическому компьютеру, чтобы вычислить два правильных числа, квантовые компьютеры гораздо более привлекательны.

За пределами алгоритма Шора

Другие алгоритмы, созданные с тех пор, рекламируются как даже более быстрые, чем алгоритм Шора, включая GEECM (https://en.wikipedia.org/wiki/

Lenstra_elliptic-curve_factorization#Quantum_version_(GEECM)) и еще один новый, о котором недавно было объявлено: https://www.technologyreview.com/s/613596/how-a-quantumcomputer-could-break-2048-bit-rsa-encryption-in-8-hours/. Это означает, что алгоритм Шора – это, в сущности, лишь базовый уровень высокоскоростных решений уравнений с большими простыми числами, и очень вероятно, что они могут быть решены быстрее и/или с меньшим количеством кубитов, чем предсказывал Шор.

Кроме того, для вычисления больших простых чисел стали использовать адиабатические компьютеры, которые являются подклассом компьютеров квантового отжига (рассматривались в главе 2), соответствующие адиабатические вычисления и связанные с ними адиабатические теоремы. С 2019 года адиабатические компьютеры стали использовать гораздо бóльшие уравнения простых чисел, чем универсальные квантовые компьютеры, использующие алгоритм Шора. Но большинство наблюдателей считают, что универсальные квантовые компьютеры и алгоритм Шора, продолжая совершенствоваться, со временем намного превзойдут уровень, достигнутый адиабатическими компьютерами к настоящему времени. Это что-то вроде дилеммы черепахи и зайца. Значительный прогресс в вычислениях достигнут многими различными типами квантовых компьютеров и алгоритмов, и по большей части этот прогресс указывает на способность взламывать самые различные типы криптокодов.

Итак, на вопрос о том, как квантовые компьютеры осуществят взлом большей части современных криптокодов, отвечают два краткосрочных прогноза. Во-первых, квантовые компьютеры в общем могут достичь квантового превосходства в течение двух или немногим более лет и будут способны решать задачи, которые классические компьютеры легко решить не могут. Защита секретов алгоритмами шифрования, связанная с относительной «медлительностью» классических компьютеров, станет более узявимой.

Во-вторых, любой шифр, основанный на факторизации большого простого числа (или дискретном логарифме, или задаче эллиптической кривой дискретного логарифма) для его защиты, будет взломан, когда у квантовых компьютеров появится достаточно большое количество стабильных кубитов и алгоритмы квантового факторинга будут эффективнее применяться против современной криптографии. Проще говоря, квантовые компьютеры быстрее, а их квантовые свойства и использующие эти свойства квантовые алгоритмы могут «укорачивать математику», которая обеспечивала столь большую защиту в классическом компьютерном мире.

Что квант может и что не может сломать

Квантовые компьютеры и квантовые свойства не могут волшебным образом сломать все известные шифры криптографии. Они могут взломать только те шифры, которые полагаются на определенные функции, восприимчивые к квантовым свойствам и квантовым алгоритмам их защиты. В этом разделе мы обсудим, какие шифры квантовые компьютеры могут и какие не могут взломать.

Что квантовые компьютеры могут взломать

Как мы выяснили ранее, квантовые компьютеры теоретически способны взломать любой алгоритм шифрования, безопасность которого опирается на задачу целочисленной факторизации, задачу дискретного логарифма, задачу дискретной эллиптической кривой логарифма или любые другие задачи, тесно связанные с математикой. Как минимум, это означает, что следующие шифры и общие приложения (использующие эти шифры) могут быть взломаны в ближайшем будущем:

- Rivest, Shamir, Adleman (RSA);
- Diffie Hellman (обмен ключами);
- алгоритм цифровой подписи (DSA), также известный как криптография конечного поля (Finite Field Cryptography);
- криптография на основе эллиптических кривых (также известная как алгоритм цифровой подписи эллиптических кривых (Elliptic Curve Digital Signature Algorithm, ECDSA));
- ElGamal;
- PKI (включая цифровые сертификаты и цифровые подписи);
- HTTPS/TLS;
- большинство VPN;
- модули безопасности оборудования (Hardware Security Modules, HSM);
- смарт-карты;
- в большой степени безопасность Wi-Fi;
- криптовалюты;
- большинство двухфакторной аутентификации, основанной на цифровых сертификатах (например, FIDO (ключи Fast Identity Online, ключи Google security));
- классические генераторы случайных чисел (random number generators, RNG).

Включение в этот список хотя бы только HTTPS/TLS означает, что большая часть шифрования в интернете будет нарушена. Добавление в этот список криптографии, связанной с PKI, означает, что большая часть криптографии, связанной с бизнесом, будет взломана. Не вся традиционная криптография будет взломана, но окажется уязвимой самая ее основа, применяемая по большей части повсюду в мире.

Примечание Предположение о том, что шифрование практически наверняка может быть взломано, относится ко всем приложениям, перечисленным выше и обычно используемым сегодня, если они не применяют или не будут переведены в квантовоустойчивые шифры.

Что квантовые вычисления не могут взломать

В ходе изучения того, что квантовые компьютеры могут взломать, был составлен внушительный список шифров и приложений. Но не вся современная криптография восприимчива к квантовым компьютерам (по крайней мере, насколько нам сегодня известно). Криптография, которая, как мы знаем, не

восприимчива к квантовым компьютерам и алгоритмам, известна как *квантовоустойчивая*, *квантовобезопасная* или *постквантовая*. Все три термина взаимозаменяемо используются большинством криптографов. Следующая криптография известна как квантовоустойчивая:

- симметричные шифры, такие как AES (и приложения и протоколы, основанные исключительно на симметричных шифрах, в частности Kerberos и Network Switching Subsystem, используемые сотовыми телефонами GSM), при условии что они применяются с «безопасными» размерами ключей;
- новые хеши, такие как SHA-2, SHA-3 и т. д., при использовании с «безопасными» размерами хешей;
- SHAKE, потоковый шифр;
- квантовое распределение ключей (QKD), например BB84, BBM, B92, COW, DPS, E91 и SARG04;
- SNOW 3G, синхронный потоковый шифр на основе слов;
- сверхсингулярный изогенный обмен ключами Диффи–Хеллмана (SIDH);
- решетчатые шифры;
- многомерная криптография;
- криптография на основе кодов;
- некоторые формы криптографии с нулевым знанием;
- квантовые генераторы случайных чисел (рассматриваются в главе 7);
- квантовые шифры.

Многие из этих квантовоустойчивых шифров будут дополнительно рассматриваться в следующих главах.

Вся квантовоустойчивая криптография и ее приложения, которые в настоящее время считаются квантовоустойчивыми, могут стать уязвимыми для квантовых вычислений или новых алгоритмов в будущем, когда последуют новые достижения. Достаточно сказать, что существует много квантовобезопасных шифров и механизмов, призванных защитить нас в будущем, хотя и они подвержены риску. Часть II этой книги «Подготовка к квантовому взрыву» обсуждает эти квантовобезопасные шифры и их реализацию.

Примечание Взломано может быть все. Даже квантовобезопасные шифры, притом что самый блестящий квантовый ученый с мировым именем будет уверять вас, что они безопасны. Вы можете прочесть или услышать, что какие-либо квантовые шифры и другие криптографические устройства и функции «не могут быть взломаны». И хотя теоретически это может быть так, еще неизвестно, что преподнесет нам реальность. Люди должны сильно постараться, чтобы создать что-либо «невзламываемое», хотя бы начиная с теории или свойств «невзламываемого» шифра. Квантовый мир не исключение, хотя квантовые свойства могут очень сильно усложнить взлом.

Почему симметричные шифры и хеши являются квантовоустойчивыми Прежде чем мы продолжим, я хочу обсудить, почему симметричные шифры и хеши являются особенно квантовоустойчивыми. Современная цифровая криптография имеет дело с размерами защищающих битов, которые делают

проведение классических атак методом «грубой силы». Просто не хватает вычислительной мощности, чтобы взломать сгенерированные ключи шифрования, используемые современными алгоритмами шифрования. Это остается верным даже в случае невероятного ускорения квантовых компьютеров (например, с использованием алгоритма Гровера) и при всех невероятных свойствах квантовой механики. То, что квантовый компьютер может использовать суперпозицию для генерации сразу всех возможных ответов, не значит, что такому компьютеру просто выбрать правильный ответ и выдать его классическому миру. Должен быть алгоритм, способный выбрать правильный ответ из триллионов вариантов, которые квантовый компьютер может генерировать для получения конкретного ответа. Это большое достоинство квантовых алгоритмов. Они, по существу, используют квантовые свойства, чтобы «сократить» математику «грубой силы» и найти правильный ответ с меньшим количеством догадок из триллионов ответов.

Алгоритм Шора помогает квантовым компьютерам осуществлять факторизацию уравнений с большими простыми числами, используя математическую логику, что и позволяет находить решения и правильный ответ из многих догадок гораздо быстрее, чем просто с помощью методов «грубой силы». Частично причина того, что квантовые компьютеры могут взломать большинство открытых ключей криптографии, заключается в том, что математика, на которую опирается криптография с открытым ключом, имеет «слабость», которую квантовые компьютеры и алгоритмы могут использовать в своих интересах. Великолепие алгоритма Шора в том, что он в состоянии быстрее получить математическое решение, и это можно осуществить только с помощью квантовых компьютеров.

Но не все средства криптографической защиты оказываются уязвимыми квантовыми решениями. В отношении традиционных симметричных шифров и хешей верно, что алгоритм Гровера уменьшает время как корень квадратный, снижая защиту симметричных шифров вдвое. Это значительное снижение защиты, но не фатальное (как в случае, если бы сокращение времени было полиномиальным, квадратичным или факториальным). Любой квантовый компьютер, атакующий эти типы криптографии, действует намного быстрее, чем классический, но количество битов ключа все еще настолько велико, что подобное ускорение не значительно ослабит защитную силу шифров или хешей.

В целом считается, что простое удвоение размера традиционных симметричных ключей и хешей позволит им оставаться квантовобезопасными в обозримом будущем, если не будет найден какой-то новый, непредвиденный метод, связанный с квантовым взломом. Итак, сам по себе переход от AES-128 и SHA-256 к AES-256 и SHA-512 считается долгосрочным решением этих проблем, и вам следует делать это сегодня. Для дополнительных сведений по этому вопросу обратитесь к следующей отличной статье: https://arxiv.org/pdf/1804.00200.pdf.

Примечание Не все криптографы считают, что атаки на хеши становятся более эффективными благодаря квантовым компьютерам. Некоторые известные криптографы полагают, что квантовые компьютеры при некоторых

формах хеш-атак (т. е. при обнаружении конфликтов) действительно могут уступать классическим компьютерам. Хороший пример вы найдете здесь: https://r.yp.to/hash/collisioncost-20090517.pdf.

Примечание Не все хеши являются квантовобезопасными. Используя алгоритм Гровера, некоторые более слабые хеши могут быть взломаны быстрее. Но SHA-2, SHA-3 и другие современные алгоритмы хеширования считаются сильными и безопасными для известных грядущих квантовых атак при использовании соответствующего размера ключа или хеша.

Все еще теория

Важно помнить, что пока не будет достигнуто квантовое превосходство (что, как полагают многие производители, случится не позднее 2019 года), все вызывающие опасения криптовзломы остаются в значительной степени в области теории. Было доказано, что алгоритм Шора, как и предполагалось, на квантовых компьютерах работает. Но пока что наибольшее факторизованное уравнение с простыми числами при использовании алгоритма Шора на квантовом компьютере было равно $7 \times 3 = 21$, а такое решение по силам и ребенку. Ваш смартфон обладает большей вычислительной мощностью, чем большинство квантовых компьютеров.

Примечание Наибольшие простые числа, факторизованные алгоритмом Шора, очень маленькие, и уравнения с большими простыми числами вычислены квантовыми компьютерами, не использующими алгоритм Шора. Смотрите https://crypto.stackexchange.com/questions/59795/largest-integer-factored-by-shors-algorithm. Хотя, когда однажды будет создано достаточно стабильных кубитов, чтобы позволить Шору атаковать большие простые числа, эти рекорды будут быстро побиты. Кроме прочего, помните, что алгоритм Шора – только пол (или потолок, в зависимости от того, как вы на это смотрите) для необходимого количества кубитов. Он был создан в 1994 году, и мир криптографии уже полон других алгоритмов, которые утверждают, что это всего лишь старая школа.

Но совокупность квантовой механики и квантовых вычислений всегда была циклом теоретических начинаний, перемещаемых затем в реальный мир. Квантовая механика оставалась уделом теоретиков в течение десятилетий, пока не стала очевидной усилиями Эйнштейна в 1930-х годах. Первая модель квантового компьютера была теоретически обоснована в 1985 году Дэвидом Дойчем (David Deutsch), а затем, в 1998-м, появился первый рабочий квантовый компьютер. Алгоритм Шора был теоретически обоснован в 1994 году, а потом доказан на квантовом компьютере IBM в 2001-м. Квантовые компьютеры растут кубит за кубитом. Как в плане стабильности кубитов, так и в плане исправления ошибок с каждым днем наблюдается все больший прогресс. Теперь у нас есть несколько поставщиков с различными подходами к квантовым компьютерам; это придает уверенности, что кван-

товое превосходство не за горами. Как только оно будет достигнуто, разрушение традиционной криптографии не заставит себя ждать. Глава 4 «Когда случится криптопрорыв?» расскажет гораздо более подробно, когда квантовые компьютеры подорвут основы традиционной криптографии.

Резюме

В этой главе рассказывалось о том, как квантовые вычисления могут взломать большинство форм традиционного шифрования с открытым ключом. Мы начали с обсуждения основ криптографии, уделяя особое внимание тому, как обеспечивают защиту большинство современных схем шифрования с открытым ключом. Затем исследовали, как квантовые компьютеры могут преодолеть эту защиту и какой тип криптографии чрезмерно восприимчив к квантовому взлому. В главе 4 мы поведем речь о том, когда теоретические атаки квантовых компьютеров, скорее всего, станут реальностью.

4 Когда случится криптопрорыв?

В этой главе будут рассмотрены основные факторы, определяющие, когда произойдет квантовый криптопрорыв, какова вероятность этого и как это будет происходить. Будет дан ответ на вопрос, которого много других экспертов по квантовым вычислениям хотят избежать: когда именно случится криптопрорыв?

Это вечное «лет через 10»

С 1994 года, после появления квантового алгоритма Питера Шора, компьютерные ученые и криптографы во всем мире понимали, что квантовые компьютеры, если мы сумеем их создать, смогут взломать существующие шифры с открытым ключом и другие криптокоды. И если изобретение как таковое состоится, вопрос только в том, сколько лет спустя начнут происходить криптографические взломы.

В течение более чем двух десятилетий, когда большинству из нас задавали вопрос о том, когда это может произойти, мы отвечали: «В ближайшие 10 лет!» Когда спрашивали меня, я говорил то же самое. Отговорка «В ближайшие 10 лет!» на самом деле означала: «Мы не знаем. Возможно, в скором времени. Возможно, пройдут десятилетия!» Ответ был взят с потолка.

Позвольте мне теперь проявить честность. Никто не знает, когда это произойдет. Любой, кто утверждает иное, либо фантазирует, либо причастен к деятельности некой секретной группы, которая уже взломала шифры, но поклялась держать это в тайне. Есть даже некоторый шанс, что того, на что мы рассчитываем, никогда не случится. Мы можем обнаружить таинственную технологическую стену, которая разрушит наши надежды! Есть те, кто считает, что «никогда» – вполне вероятный результат. Есть и те, кто считает, что все, что мы называем квантовыми компьютерами, в действительности нечто другое, и все мы заблуждаемся. Но в общем среднестатистический криптограф, если его просят предсказать, когда произойдет квантовый криптографический взлом, вслед за квантовыми физиками часто говорит: «В течение 10 лет».

Однажды, около десяти лет назад, после того как я завершил одно из моих частых выступлений о квантовых вычислениях и вероятном квантовом прорыве, кто-то из слушателей спросил меня, что я думаю о том, когда этот прорыв может произойти. Я, как обычно, ответил: «В ближайшие 10 лет». Знаменитый криптограф, признанный авторитет в отрасли Брюс Шнайер, ко-

торого я считал своим негласным наставником, в этот момент поднимался на трибуну, чтобы выступить со следующим докладом. Проходя мимо меня, он тихо спросил: «Роджер, как давно ты это говоришь?» Я понял, что толкую про эти «ближайшие 10 лет» почти на протяжении двух десятилетий. Время шло, а мой ответ не менялся. Это заставило меня задуматься, понимаю ли я на самом деле, насколько далек от нас квантовый криптопрорыв, и ответить самому себе: нет, не понимаю. И никто этого не знает. Это было почти 10 лет назад.

Но если бы вы попросили меня дать прогноз сегодня, я бы сказал вам, что квантовый криптопрорыв уже произошел или, скорее всего, произойдет в ближайшие несколько лет. Я считаю, что велика вероятность того, что криптопрорыв произойдет в ближайшие один–три года, а вместе с тем и вероятность, что большинство в мире не будет готово к нему. Отсюда и основная причина, по которой я написал эту книгу: помочь вам как можно лучше подготовиться к грядущей реальности. Я не квантовый физик, и я не зарабатываю на квантовых компьютерах. Я сознательно рискую своей профессиональной репутацией, предрекая относительно скорый квантовый прорыв.

Итак, что же изменилось, чтобы я наконец позволил себе сделать твердую ставку и предсказать конкретный срок, которого никто не может знать наверняка? И не похож ли я в этом на сотни, если не тысячи, предсказателей судного дня, которые уже потерпели фиаско? Они предрекали библейские катастрофы, столкновения с астероидами, ускорение частиц, вихри, поедающее все антивещество, и рисовали прочие картины конца света по любой возможной причине. Что изменилось, чтобы я перестал говорить «лет через 10» и сократил этот период до ближайших нескольких лет? Я расскажу об этом в следующем разделе.

Факторы квантового криптопрорыва

Когда люди задаются вопросом, сломают ли квантовые компьютеры традиционные криптокоды, фактически речь идет о том, является ли реальностью квантовая механика, возможно ли ее практическое применение в мире квантовых компьютеров и насколько квантовые компьютеры способны явить подобный прорыв. В данном разделе мы обсудим многие из этих факторов и посмотрим, где мы находимся в настоящее время и где будем находиться в ближайшем будущем. Перечислю эти факторы один за другим.

Квантовая механика реальна?

Да, квантовая механика реальна. Как описано в главе 1, существование квантовой механики и большинства квантовых свойств (фотоэлектрический эффект, двойственность волна–частица, запутанность, неопределенность, туннелирование и другие) доказывалось снова и снова. Квантовая механика – одна из самых проверенных и точных наук в мире. Мы часто не знаем, как или почему работают те или иные квантовые свойства, и это тревожит всех, кто занимается квантовой механикой, но квантовая механика не предмет воображения. Мало того, что она реальна, но, как и предсказывали уче-

ные, она будет работать на практике, что доказывалось многократно. Иногда лучшие в мире умы пытались доказать, что «странные свойства» квантовой механики вызваны чем-то еще, чего мы не учитываем. Но каждый раз проведение экспериментов в надежде доказать, что квантовая механика – не квантовая механика, оборачивалось неудачей. И наоборот, многократно проведенные эксперименты, призванные показать, что квантовые свойства существуют и будут проявляться определенным образом, доказывали именно это. Это экспериментально доказанный и зафиксированный наукой факт.

Квантовые компьютеры реальны?

Да, квантовые компьютеры реальны. Хотя большинство современных квантовых компьютеров не очень мощные (квантовые компьютеры отжига – заметное исключение), они используют для вычислений, что проверено на практике, квантовые свойства. Это важно. Это еще один способ доказать, что квантовые свойства реальны. Пока не появились первые реально работающие квантовые компьютеры, была вероятность, что мы, простые люди, просто не способны уловить, использовать квантовые свойства и управлять ими для собственных нужд. Вплоть до создания первого квантового компьютера все, что у нас было, – это много теорий о том, как квантовый компьютер будет выглядеть и работать. И вот в 1998 году миру наконец впервые был явлен квантовый компьютер, и нам больше не нужно переживать по этому поводу. Это чертовски захватывающее событие произошло 21 год назад.

Главным фактором, удерживающим нас от беспокойства по поводу того, что квантовые компьютеры взломают традиционный открытый ключ сегодняшней криптографии, особенно после того, как в 1994 году был создан алгоритм факторинга простых чисел Питера Шора, было сомнение в том, что мы сумеем построить квантовый компьютер. Было много скептиков. Но четыре года спустя мы сделали это.

Без этого уникального достижения ни одно другое не было бы возможно. Но мы действительно это сделали. В настоящее время в одном только Западном полушарии имеется более 80 различных групп разработки квантового оборудования, о которых нам известно, и, вероятно, есть масса других во всем мире, о которых мы не знаем. Во главе угла стоял вопрос, можем ли мы вообще построить хоть один квантовый компьютер, и вот мы его построили. Пожалуй, наиболее серьезный барьер – мысль о том, что практическая реализация невозможна, – мы преодолели. Самым сложным было создание первого кубита. Мне кажется, что переход от 1 кубита к миллиону кубитов окажется гораздо менее сложной проблемой.

Примечание Любопытный факт: некоторые известные ученые говорят, что до настоящих квантовых вычислений дело пока еще не дошло, и в доказательство своей теории приводят научно или логически обоснованные аргументы. Но с появлением каждого нового типа квантового компьютера и последовательными доказательствами работоспособности квантовых алгоритмов и решений эти утверждения становятся все менее основательными.

Суперпозиция реальна?

Да, суперпозиция реальна. Вы не можете с помощью классических компьютеров найти решение сложных проблем, таких как факторинг больших простых чисел, без возможности генерировать множество ответов одновременно... фактически получить все допустимые ответы мгновенно. Были проведены сотни, если не тысячи экспериментов, которые доказали, что суперпозиция реальна. В 1996 году был продемонстрирован один атом, имеющий суперпозицию состояний (https://quantumsciencephilippines.com/seminar/seminar-topics/SchrodingerCatAtom.pdf). С тех пор на триллионах атомов (https://arxiv.org/abs/1310.8343) и в совокупности на десятках тысяч молекул была продемонстрирована суперпозиция. Что еще более важно, все квантовые компьютеры используют суперпозицию как одно из ключевых квантовых свойств. Они не могли бы существовать и работать так, как они работают, без суперпозиции.

Реален ли алгоритм Питера Шора?

Да, алгоритм Питера Шора реален. Без применения алгоритма Шора в реальном мире и быстрого вычисления уравнений с простыми числами традиционные шифры с открытым ключом и другие шифры могли бы в обозримом будущем оставаться в безопасности. Хотя пока квантовые компьютеры, которые использовали алгоритм Шора, не осуществили факторинг уравнения с большими простыми числами, они использовали алгоритм Шора и показали, что он работает точно так, как это предсказал Шор. Ранний квантовый компьютер IBM в 2001 году использовал алгоритм Шора для разложения уравнения на простые числа. На этот вопрос дан ответ. Нам просто нужны более устойчивые кубиты, чтобы решать уравнения с очень большими простыми числами. Тот факт, что алгоритм Шора доказал свою работоспособность, означает, что и другие квантовые алгоритмы, на которые он опирается, такие как преобразование Фурье, тоже точны и верны.

Достаточно ли у нас стабильных кубитов?

Нет, у нас недостаточно стабильных кубитов. На сегодня это святой Грааль квантовых вычислений. Алгоритм Шора для разложения любого уравнения с простыми числами требует $(2 \times n) + 3$ устойчивых кубита, где n – количество битов ключа для взлома. Таким образом, чтобы взломать 2048-битный ключ RSA, нам нужно 4099 стабильных кубитов, а для взлома 4096-битного ключа RSA – 8195 стабильных кубитов. Чтобы построить соответствующий компьютер, нам нужны стабильные кубиты. Алгоритм Шора не так полезен квантовому компьютеру на базе отжига (как обсуждено в главе 2). Пока (на момент написания статьи) мы имеем универсальные квантовые кубиты только в диапазоне 100, и даже они не настолько стабильны, как нам было бы нужно. Это еще очень далеко от более чем 4000 необходимых стабильных кубитов (или, по некоторым расчетам, 4 000 000 000 просто кубитов, с учетом вспомогательных). Вопрос в том, насколько быстро будет расти число стабильных кубитов.

Я отнесу этот вопрос на счет человеческой изобретательности. Стоит нам осознать полезность даже очень сложной аппаратной вещи, мы быстро переходим к ее массовому производству. В годы Второй мировой войны Алан Тьюринг и его команда (основываясь на предыдущей работе, проделанной сотнями сподвижников) наконец выяснили, что потребуется для того, чтобы взломать немецкие коды Enigma. Для этого Тьюрингу пришлось изобрести первые, реально работающие компьютеры, что он и сделал. А потом он понял, что ему нужны сотни компьютеров. И он получил их. Первые радиоприемники и телевизоры было делать очень сложно. Следующий миллион – совсем не так сложно. Как правило, требуются сотни и даже тысячи лет, чтобы создать что-то впервые. Но создание следующего миллиона экземпляров обычно не занимает и половины десятилетия. Получить первый суперстабильный кубит очень сложно. Добраться от одного до миллиарда – не так сложно.

Многие ученые работают над тем, чтобы оптимизировать факторизацию по алгоритму Шора и уменьшить количество необходимых кубитов. Алгоритм Шора – это потолок (то есть максимальное число нужных кубитов), а не пол. Вполне вероятно, что алгоритм Шора будет со временем значительно улучшен, а заодно улучшена и стабильность квантовых кубитов, так что необходимое их количество будет уменьшаться. Итак, сегодня, во всяком случае по официальным данным, у нас нет необходимого количества стабильных кубитов, но мы идем к цели, используя два синергетических подхода, которые должны встретиться. Один добавляет стабильность кубитам, а другой требует меньше стабильных кубитов.

Стабильность кубитов и исправление ошибок

Находятся ли сейчас когерентность и декогеренция кубитов там, где они нам нужны для квантового превосходства и квантового криптопрорыва? Нет. Но, как и с ростом количества кубитов, дела со стабильностью и исправлением ошибок становятся все лучше. Кажется, что ситуация с тем и другим улучшается ежеквартально. Есть даже существенный шанс добавить больше кубитов самым стабильным типам квантовых компьютеров, о которых мы знаем прямо сейчас, майорановского фермиона (Microsoft) и компьютера с ионными ловушками. И каждый их кубит является очень стабильным кубитом. Поставщики таких компьютеров могут тратить больше времени, денег и других ресурсов на простое добавление кубитов вместо попыток стабилизировать и исправить существующие у кубитов ошибки. Эта гонка дает возможность увидеть, какая из квантовых технологий выигрывает: много кубитов с большим количеством исправлений ошибок или стабильных кубитов – с меньшим.

Квантовые ресурсы и конкуренция

Весомый аргумент в пользу того, что мы, вероятно, решим существующие квантовые проблемы раньше, чем позже, – огромное количество ресурсов, которые выделяются для решения оставшихся проблем. Все ведущие страны тратят на это десятки миллиардов долларов. Для многих из них это становится приоритетом государственной важности, и даже более мелкие страны сотрудничают в этих вопросах с крупными. Все большие технологические

и компьютерные компании наряду с ведущими университетами стран участвуют в решении этих проблем. Это напоминает мне о другом глобальном проекте полувековой давности.

В 1950-х годах мало кто думал, что к 1969 году люди побывают на Луне. Что еще больше поражает, главный рывок Соединенных Штатов в вопросе запуска космонавтов на Луну не предвиделся, пока в 1961 году не появилась знаменитая декларация Джона Кеннеди. Восемь лет спустя, после многочисленных ошибок и катастроф, американские астронавты приземлились на Луне. Я не знаю другого проекта, на который было бы выделено столько же глобальных ресурсов ради борьбы за первенство. И в моем представлении квантовая гонка определенно похожа на лунный проект.

У нас есть постоянное улучшение?

Да, у нас есть устойчивое улучшение. Все эти глобальные ресурсы и конкуренция направлены на улучшение всех деталей квантовых вычислений. Количество кубитов увеличивается. Стабильность кубитов повышается. Исправление ошибок все более эффективно. Скорость квантовых логических элементов увеличивается. Число квантовых компьютеров растет, и изобретения по усовершенствованию квантовых устройств появляются почти еженедельно.

В настоящее время изобретается все больше квантовых алгоритмов, а старые доказывают свою работоспособность на реальных квантовых компьютерах. Доступно несколько квантовых процессоров. Теперь существует более десятка квантовых языков программирования, языки сценариев и компиляторы. Квантовая сеть больше не мечта. Используются квантовые генераторы случайных чисел. Многие поставщики считают, что квантовое превосходство уже не за горами. Похоже, нет никаких серьезных препятствий, которые считается невозможным одолеть.

Некоторые критики сравнивают квантовые вычисления и квантовый прорыв с ядерным синтезом. Термоядерная реакция происходит, когда ядра двух или более атомов объединяются, чтобы стать одним целым. При слиянии вырабатывается большое количество энергии. Так солнце генерирует тепло, энергию и свет, и долгое время считалось, что подобные энергетические технологии будут источником энергии на Земле. Но после более чем 80 лет исследований и разработок, израсходовав миллиарды долларов, мы оказались не ближе к таким технологиям, чем были вначале. Скептики называют квантовое вычисление очередным поводом потратить деньги. Они полагают, что квантовые команды дают чересчур оптимистичные прогнозы, обещая квантовые вычисления для получения большого финансирования.

Но есть огромная разница между исследованиями ядерного синтеза и квантовыми исследованиями. Исследования по слиянию ядер проводятся одно десятилетие за другим, но большинство практических экспериментов терпят неудачу. У нас все еще нет работающего термоядерного реактора. В квантовом мире мы имеем работающие устройства. У нас есть постоянное улучшение. Непрерывный прогресс. Это не похоже на науку, которая заходит в тупик или замедляется. Происходит наоборот.

Мнения экспертов

В течение долгого времени почти все эксперты по квантовым вычислениям соглашались с тем, что до квантового превосходства, по крайней мере, лет десять. Теперь мнения начинают расходиться, и все больше и больше экспертов начинают склоняться к тому, что до квантового превосходства лишь год или два. Многие эксперты по квантовым вычислениям считают, что до квантового криптопрорыва всего лишь несколько лет. Марк Джексон (Mark Jackson), научный руководитель по развитию бизнеса в компании «Кембриджские квантовые вычисления» (Cambridge Quantum Computing), – один из этих экспертов. Он и компания в целом помогают нескольким вычислительным проектам. Марк находится в гуще событий, сввязанных с квантовыми компьютерными технологиями, и понимает, на каком этапе мы в настоящее время и куда это придет в течение следующих нескольких лет. Он публично предсказал, что квантовый криптопрорыв возможен в течение следующих нескольких лет (менее 10). Это не отговорка «10 лет спустя», которую мы обычно произносили. Тогда у нас не было (до некоторого момента) даже квантового компьютера, не то что сотни работающих квантовых компьютеров, команд по всему миру и десятков миллиардов долларов на решение проблемы. Теперь это не завуалированное «на самом деле мы не знаем», а ответ, основанный на устойчивых, методических достижениях в существующей науке о квантовых вычислениях. И Джексон не одинок.

Когда случится квантовый киберпрорыв

Если учесть все факторы, необходимые для взлома традиционной криптографии, можно с твердостью заявить, что это произойдет скорее раньше, чем позже. Некоторые эксперты говорят, что они больше удивятся, если это не произойдет в первой половине ближайшего десятилетия, чем если это произойдет (впрочем, тут же добавляя, что никто не знает, когда что-либо случится, пока это не случится). Разумный человек должен рассматривать всевозможные временны́е сценарии и понимать, учитывая риски, какой из сценариев представляется наиболее обоснованным.

Временны́е сценарии

Существует четыре глобальных предположения на тему, когда может произойти (или не произойти) квантовый криптовзрыв: это уже произошло, но мы не знаем об этом; это произойдет в ближайшие несколько лет; это не произойдет в ближайшие несколько лет, но в конечном счете произойдет; или, наконец, этого никогда не случится. Возможны только эти варианты, и каждый в подробностях будет рассмотрен ниже.

Это уже произошло

Совершенно не исключено, что квантовое превосходство и квантовый криптопрорыв уже достигнуты, о чем известно узкой группе лиц, а мировая общественность об этом просто не знает. Считается, что если правительство крупной страны смогло получить квантовое превосходство и, в частности,

первым выполнить квантовый криптовзлом, оно будет иметь все основания сохранять это достижение в тайне.

Примечание Правительства мира умеют хранить секреты шифрования. Клиффорд Кокс (Clifford Cocks) из Штаба правительственной связи Великобритании (UK's government Communications Headquarters, CHQ) создал то, что мы сейчас называем шифром RSA, в 1973 году, а Малкольм Дж. Уильямсон (Malcolm J. Williamson) открыл в 1974 году то, что мы позже назовем Диффи–Хеллман. Вскоре после этого они были переданы Агентству национальной безопасности США (NSA). Диффи, Хеллман и Меркл (Diffie, Hellman, Merkle) воссоздали эти шифры в 1976 году и RSA в 1977 году, что признано официально. Но существование шифров ни правительство Великобритании, ни правительство США не признавали десятилетиями. Правительство Великобритании признало свою роль первого создателя криптографии с открытым ключом в 1997-м (24 года спустя).

Большинство шпионских агентств мира хотели бы осуществить квантовый криптографический взлом и хранить это в тайне как можно дольше. Тогда они могли бы шпионить за многими организациями и другими правительствами, которые все еще полагались бы на традиционную криптографию с открытым ключом, думая, что ее использование по-прежнему безопасно. Я думаю, что криптоэксперты правы, ожидая, что их правительства будут держать криптовзлом в секрете, если первыми получат доступ к нему, прежде чем некое лицо или организация сообщит об этом публично. Эту теорию можно развить дальше, потому что несколько стран и компаний (до 2019 года) утверждали, что они уже получили квантовое превосходство или были очень, очень близки к тому, чтобы получить его. Так произошло с Google, IBM и Alibaba. А потом вдруг большинство из этих голосов стихли. Многие задаются вопросом, почему. Лично я, не располагая никакими реальными данными на этот счет, оцениваю вероятность данного сценария («криптопрорыв уже состоялся») в 15 %.

В ближайшие несколько лет

Ваш автор и многие другие считают, что квантовое превосходство и квантовый криптовзрыв произойдут через несколько лет или раньше. Это определенно не точка зрения большинства, но ее поддержка растет с каждым днем. Квантовое превосходство, вероятно, будет достигнуто в следующем году или около того (Google, IBM и другие заявляли об этом). Я не думаю, что мы сильно рискуем ошибиться, если согласимся с тем, что предсказывают компании Google и IBM. Что означает квантовое превосходство, когда оно уже достигнуто, – другой вопрос.

Хотя квантовое превосходство, то есть момент, с которого квантовые компьютеры смогут делать вещи, на которые не способны классические компьютеры, ознаменует исторический перелом, вряд ли это означает, что мир сразу предстанет в другом измерении. День после достижения квантового превосходства – начало большой работы, которая, несомненно, приведет ко многим великим открытиям. Не все они будут реализованы единовременно. Это займет годы, на протяжении которых, как результат достижения

квантового превосходства, состоятся многие другие изобретения – так же, как после открытия и получения электричества были изобретены лампы накаливания, радио, телевидение и интернет.

Квантовый криптографический взлом очевидно воспоследует за квантовым превосходством, но насколько быстро, сейчас невозможно предсказать. Центральный вопрос заключается в том, сколько времени займет у поставщиков универсальных квантовых компьютеров переход от менее чем 100 стабильных кубитов к более чем 4000. Есть большая вероятность, что после стабилизации кубита и исправления ошибок этот показатель будет увеличиваться достаточно быстро.

В свое время, когда стало ясно, как разместить много транзисторов на кусочке кремния, их число на одном и том же пространстве стало удваиваться каждые 18–24 месяца (согласно прогнозу, известному как закон Мура). Количество созданных кубитов, которые можно использовать с определенным типом квантового компьютера, до сих пор росло менее предсказуемым образом, хотя тут можно провести частичную аналогию с первыми днями существования микропроцессоров. Таблица 4.1 показывает количество кубитов, используемых различными квантовыми компьютерами без отжига и с отжигом по годам (просто для сравнения).

Важно помнить, как это было описано в главе 2, что квантовый компьютер, его скорость и его возможности – это больше, чем просто количество кубитов. Если вы посмотрите на историю квантовых вычислений, почти все компоненты улучшаются, а также появляются новые компоненты и комбинации, которых не было раньше. Мы знаем, что на всех фронтах квантового производства наблюдается устойчивый прогресс. Я оценил вероятность этого сценария («до прорыва осталось несколько лет») в 30 %.

Таблица 4.1. Количество кубитов, используемых различными квантовыми компьютерами

Год	Без отжига	С отжигом
1998	3	
2000	7	
2006	12	
2007		28
2012		84
2015		1000
2017	50	2000
2018	72	

В относительно недалеком будущем

По сути, стандартный ответ – «в течение следующих 10 лет». Сторонники этой версии полагают, что на ближайшие годы вряд ли стоит рассчитывать, но квантовое превосходство и квантовый криптопрорыв когда-нибудь да состоятся. Так считает подавляющее большинство квантовых ученых. Одно из очевидных различий между этим мнением и ответом «в ближайшие несколько лет» заключается в том, что квантовые ученые, работающие непосредственно над квантовыми компьютерными продуктами, думают, что это произойдет

раньше, чем через 10 лет. И это показательно. Ученые не уверены в том, когда произойдет прорыв, но начинают чувствовать, что он вполне вероятен, скажем, в ближайшие пять–семь лет, и отказываются от мысли, что надо ждать еще 10 лет. Это большой сдвиг в мышлении. Конечно, всегда есть шанс, что квантовое превосходство и квантовый криптографический взлом произойдут через десятилетия. Никто точно не знает, когда это произойдет. Я оценил вероятность этого сценария («относительно недалекое будущее») в 50 %.

Этого никогда не случится

Чуть меньше экспертов по квантовым вычислениям предполагают, что прорыв никогда не произойдет. Они считают имеющиеся проблемы крупномасштабных квантовых вычислений непреодолимыми. Некоторые даже утверждают, что квантовые компьютеры, которые у нас есть сегодня, не являются квантовыми. Иными словами, мы всего лишь видим то, что хотим видеть в мире, который все еще недостаточно знаем. Такие специалисты полагают, что каждый тип созданного нами квантового компьютера в конечном итоге встретится с проблемами, которые помешают ему продвинуться дальше примитивных, похожих на подсчет на ручных счетах методов, которые мы используем сегодня. И эту критику нельзя игнорировать. Среди сторонников данной концепции одни из самых авторитетных ученых в нашем мире. Они знают гораздо больше о квантовых вычислениях, чем большинство из нас.

И все же я бы не стал вкладывать деньги в подобный временной сценарий. Когда говорят «никогда», часто подразумевают «не на нашем веку»; и в прошлом многие блестящие умы, в том числе Эйнштейн, до последнего своего дня ставили под сомнение полноту квантовой механики, хотя квантовые свойства, которые они обесценивали, в конечном итоге подтвердили свое существование. Я оцениваю вероятность этого сценария примерно в 5 % или даже менее. Что важно, подавляющее большинство самых сведущих в области квантовой механики ученых, да и правительство США не очень верят в такой сценарий (подробнее об этом в следующем разделе). Одно из моих любимых высказываний по теме принадлежит квантовому специалисту, профессору Остинского университета Скотту Аароносну (Scott Aaronson), который пишет в своей книге Quantum Computing Since Democritus («Квантовые вычисления со времен Демокрита»):

> «*Если бы оказалось, что масштабируемые квантовые вычисления невозможны, это взволновало бы меня в тысячу раз больше, чем если бы это оказалось возможным. Такое положение дел означало бы, что мы не вполне понимаем или совсем не понимаем квантовую механику как таковую; это была бы революция в физике!*»

Когда следует быть готовыми?

Вы можете спросить себя: «Если никто из экспертов по квантовым вычислениям не уверен, когда произойдет квантовый криптопрорыв, должны ли мы уже сейчас начинать готовиться к нему?» Вы можете опасаться, что придется тратить драгоценное время и ресурсы, заостряя внимание на чем-то, что, может быть, произойдет через много лет, если не десятилетий. Вы можете ду-

мать: «В мире компьютерной безопасности много такого, что по факту гораздо важнее, чем некоторые теоретические соображения, “журавль в небе” или Y2K-проблема!» И такая точка зрения простительна, особенно потому, что подавляющее большинство ваших коллег по компьютерной безопасности в настоящее время в полном неведении и ничего не предпринимают. Вы можете даже занять «консервативную позицию» и думать, что вы сэкономите ресурсы и сможете распорядиться ими, когда узнаете, что квантовое превосходство и квантовый криптовзлом на самом деле происходят. Вы можете полагать, что имеет смысл подождать реакции масс, когда реальная угроза наконец-то будет осознана, поскольку так будет безопаснее (подобно тому как косяк мелкой рыбы, двигаясь синхронно, скорее уйдет от хищника). Вы можете думать, что подождать официального заявления о прорыве и разумно, и экономически более эффективно.

Однако если оставить в стороне временны́е сценарии, которые существуют лишь на уровне прогнозов, ответ на вопрос, когда вы и ваша организация должны начать готовиться к квантовому превосходству и грядущему квантовому криптовзлому, существует: уже сейчас! Есть много вещей, которые лучше начать делать незамедлительно (смотрите часть II этой книги), и так будет дешевле и проще. И есть очень большая вероятность того, что при ожидании квантового прорыва может оказаться слишком поздно защищать секреты вашей организации. Если вашим конкурентам или заинтересованным государствам очень интересна ваша секретная информация, они могут уже сейчас скачивать ваши зашифрованные данные, ожидая того дня, когда их можно будет раскрыть с помощью квантовых вычислений. Даже если вы думаете, что у вас нет конфиденциальных данных, полезных для соперника, вам тем не менее явно дешевле и эффективнее начать подготовку к постквантовому миру сейчас. И я не одинок в этой рекомендации.

Агентство национальной безопасности (NSA) говорит – сейчас

В 2016 году Национальный институт стандартов и технологий США (NIST), Агентство национальной безопасности (NSA) и Центральная служба безопасности (CSS) заявили, что «сейчас» настало время начинать подготовку к переходу в постквантовый мир. Такое сообщение появилось в ответах на часто задаваемые вопросы о национальной безопасности и квантовых вычислениях в Коммерческом управлении информации NSA/CSS. Относительно постквантовой подготовки очень откровенно сказано: «Агентство национальной безопасности считает, что, учитывая достижения в области квантовых вычислений, это надо делать сейчас» (https://cryptome.org/2016/01/CNSA-Suite-and-Quantum-Computing-FAQ.pdf).

Если кто-то в вашей организации спрашивает, следует ли вам готовиться к квантовому превосходству и грядущему квантовому криптопрорыву, покажите им этот документ и, в частности, этот раздел. Все довольно ясно. И этому документу, как минимум, три года (по состоянию на 2019 год). Таким образом, независимо от возможных временных сценариев и их вероятности лучшие научные умы нашей страны и те, которые, скорее всего, близко знакомы с достижениями квантовых вычислений и оставшимися технологическими препятствиями, говорят миру, что надо готовиться сейчас. Похоже,

аргумент «цена–прибыль» относительно последнего возможного временно́го сценария («никогда») даже не рассматривается.

Национальная академия наук говорит – сейчас

В 2018 году Национальная академия наук США опубликовала отчет об исследовании соглашения под названием «Компьютеры: прогресс и перспективы» (*Quantum Computing: Progress and Prospects*, http://cs.brown.edu/courses/csci1800/sources/2018_NAE_QuantumComputing_PogressAndProspects.pdf). Ключевой вывод № 1: перспектива квантового взлома RSA-2048 бит откладывается как минимум на десять лет. Это один из самых смягченных выводов, который я там нашел относительно того, когда произойдет квантовый прорыв. Но за ним следует вывод № 10, в котором говорится:

> *Даже если квантовый компьютер, который может расшифровать текущие криптографические шифры, появится более чем через десятилетие, опасность такого устройства достаточно высока, а сроки перехода к новому протоколу безопасности велики и не определенны, приоритетность разработки, стандартизации и развертывания постквантовой криптографии имеет решающее значение, чтобы свести к минимуму вероятность потенциальной катастрофы безопасности и конфиденциальности.*

Проще говоря, начинать готовиться надо сейчас.

Неравенство Моски

В 2015 году Микеле Моска (Michele Mosca) из Университета Уотерлу заявил, что нам нужно начать беспокоиться о влиянии квантовых компьютеров, когда срок, в течение которого, как мы хотим, наши данные должны быть в безопасности, добавляется к тому времени, которое потребуется нашим компьютерным системам для перехода от классического к постквантовому состоянию. И это время больше того, которое потребуется квантовым компьютерам, чтобы разрушить существующую квантовую восприимчивость протоколов шифрования. Например, если вы хотите, чтобы ваши важные данные были в безопасности в течение 10 будущих лет, а переход займет 5 лет, вам следует начать переход к постквантовым системам за 15 лет до наступления постквантового мира. Когда Моска впервые заявил о своем заключении, он выбрал 2020 год как точку отсчета начала в будущем, но, по общему мнению, большинство организаций, нуждающихся в безопасности данных, преодолело эту точку в 2017 году. Вот отличная статья о неравенстве Моски соучредителя Кембриджского сообщества квантовых вычислений Ильяса Хана (Ilyas Khan): www.linkedin.com/pulse/moscas-inequality-whymatters-ilyas-khan-ksg/. Я еще раз подробно расскажу о неравенстве Моски в главе 9.

Сценарии криптопрорыва

Немного усложним ситуацию. Никто не уверен, как будут выглядеть сценарии прорыва, когда мы достигнем квантового превосходства. Останется ли

та сила, которая явит себя и, возможно, все взломает, в руках немногих, или это будет похоже на сценарий с изобретением криптографии с открытым ключом, которую весь мир использовал в течение нескольких лет? Давайте рассмотрим некоторые из вероятных сценариев квантового прорыва, допускающих, что он когда-либо состоится.

Новая технология надолго останется в распоряжении национальных государств

Многие страны тратят миллиарды долларов, чтобы первыми достичь квантового превосходства и квантового криптопрорыва. Создание квантовых компьютеров в необходимом масштабе требует десятков, если не сотен миллиардов долларов инвестиций. Один из возможных сценариев прорыва состоит в том, что одно или несколько национальных государств достигнут этих квантовых целей, вероятно, с промежутком в несколько лет, и именно у них появятся возможности, предоставляемые этим прорывом. Правительства наделят правом использования новой технологии узкий круг лиц, потому что она способна сломать сегодняшние цифровые коды. Они будут стремиться ограничить возможный ущерб и защитить секреты своего государства надлежащим образом, прежде чем квантовые возможности станут известны широкой публике.

Этот вариант в чем-то напоминает отношение большинства стран к атомному оружию. Эта возможность была достигнута за счет крупных затрат на уровне национального государства и сразу же получила высокую степень защиты. Каждая нация, которая вступает в «ядерный клуб», начинает, как и большинство других членов клуба, заботиться о том, чтобы предотвратить будущее членство других стран. На национальном и глобальном уровнях приняты законы, направленные на предотвращение попадания ядерного оружия в руки тех, кто находится за пределами уполномоченных сверхсекретных правительственных учреждений.

Вы можете скептически относиться к сопоставлению квантовых вычислений с ядерным оружием, но помните, что многие правительства считают сильную криптографию высшим национальным секретом. Великобритания и Соединенные Штаты долгое время держали в тайне тот факт, что Великобритания изобрела криптографию с открытым ключом, – прошли десятилетия, прежде чем он был использован в открытом доступе. Даже сегодня сотрудникам и компаниям во многих крупных странах, в том числе США, запрещается экспортировать надежную криптографию в другие страны. Преступлением может стать даже размещение сильной криптографии в интернете, вследствие чего другие страны могли бы загрузить и использовать ее. Сильная криптография считается «боеприпасами» и распространяется на основании закона США об экспортном контроле вооружения. Несоблюдение национальных законов об экспорте криптографии может считаться изменой и даже грозить нарушителю смертной казнью.

В прошлом многим гражданам угрожали обвинением в измене даже за то, что они делились в интернете широко используемыми алгоритмами шифро-

вания в программных продуктах. В начале 1990-х годов Филипп Циммерман (Philip Zimmerman, https://en.wikipedia.org/wiki/Phil_Zimmermann) стал международным «криптографическим мучеником», находясь под угрозой наказания правительством США за использование общих стандартов шифрования в его свободно загружаемой программе Pretty Good Privacy (PGP).

Достаточно сказать, что если национальное государство посчитает, что следует сохранить квантовые вычисления для себя, то оно так и сделает. Не исключено, что правительства могут разрешить вести квантовые вычисления, но объявят взлом традиционной криптографии незаконным, даже если эта технология станет доступна всем и каждому. Правительства могут даже создать законы, которые не позволят производителям квантовых компьютеров использовать свои компьютеры для взлома традиционных криптографических ключей. Может ли алгоритм Шора быть вне закона? Можно ли кого-либо арестовать за собственную реализацию алгоритма Шора, если он запрещен к использованию?

Опять же, вы можете скептически относиться к такой возможности, но подобная ситуация уже однажды сложилась с принтерами, сканерами и копировальными аппаратами (и другими устройствами, такими как факсы и программное обеспечение для редактирования фотографий), вынудив правительство США предотвратить печать фальшивых долларов. Многие не знают, что большинство копиров, принтеров и сканеров (и программного обеспечения) содержат кодирование, которое препятствует печати реалистичных копий банкнот. Я мог бы посоветовать вам попробовать скопировать и распечатать валюту, но даже такой совет не был бы законен.

Примечание Существует много законов США, которые запрещают копирование и печать валюты. Многие люди полагают, что все эти разговоры о кодах для предотвращения печати валюты – всего лишь слухи. Однако мой знакомый недавно попытался скопировать и распечатать долларовые купюры разного номинала на устройствах разного типа – и обнаружил, что он может делать довольно реалистичные копии и даже сохранять их в файлах, но все попытки распечатать валюту в размере один к одному оказались неудачными. Он мог печатать очень точные копии банкнот, но если печать настраивалась в 100%-ном масштабе, это приводило к ошибкам печати, отказам в печати и обрезанию копий. Возможно, не все устройства оснащены подобной защитой, но это произошло на устройствах, которые мой друг использовал в своем эксперименте. Вот видео YouTube с более подробной информацией: www.youtube.com/watch?v=1c-jBfZPVv4.

Применение крупнейшими компаниями

Существует аргумент, что стоимость разработки квантовых компьютеров защитит квантовую криптографию от взлома в рамках национальных государств, и она будет доступна только крупнейшим компаниям с достаточным количеством ресурсов для создания, покупки или аренды времени на больших квантовых компьютерах. Чтобы сломать самый распространенный се-

годня размер открытого ключа, алгоритм Шора требует применения квантового компьютера с более чем 4000 очень стабильных кубитов. По достижении такого масштаба он, вероятно, станет одним из самых дорогих компьютеров, по стоимости гораздо больше, чем мейнфреймы размером с комнату и даже миллионы облачных виртуальных машин. Экономика построения и применения чего-то нового, удивительного, очень сложного и редкого подсказывает, что крупномасштабные квантовые вычисления будут очень дорогими на протяжении многих лет.

Конечно, когда-нибудь квантовый компьютер (или процессор) может появиться на столе у каждого, но ждать этого придется как минимум десятилетия. Первый традиционный компьютерный микропроцессор (по крайней мере то, что производитель назвал микропроцессором) был создан в 1968 году. Хотя микропроцессоры были широко распространены и использовались в дорогих компьютерах и нескольких дорогих калькуляторах, идея компьютерного микропроцессора не была реализована в большинстве настольных компьютеров до 1990-х годов (и многие говорят, что по-прежнему реализована не во всем мире).

Таким образом, только по экономическим причинам правдоподобным сценарием прорыва может быть тот, при котором квантовые компьютеры поначалу будут доступны крупным компаниям, но в течение десятилетий мелкие компании и люди с ограниченными ресурсами не смогут позволить себе такую роскошь. Также вполне возможно, что крупнейшие компании могут ограничить способность квантового криптовзлома для предварительно авторизованных компаний в соответствии с национальными законами (как это было сделано с печатью валют).

Массовое распространение

Наиболее разумный сценарий прорыва – массовое распространение квантовых компьютеров лишь в среднесрочной перспективе. Даже сегодня около сотни небольших квантовых компьютеров с ограниченными вычислительными возможностями предлагается для использования небольшим компаниям и частным лицам – бесплатно или за повременную плату. Кажется маловероятным, что компании, создающие и предоставляющие собственные ресурсы ограниченных квантовых вычислений, не сделают их доступными для широких масс, тем самым способствуя распространению технологии (если это, конечно, не будет запрещено законом).

Наиболее вероятный сценарий прорыва

Если учитывать опыт прошлого, то наиболее вероятным сценарием прорыва будет сценарий, в котором национальные государства (и связанные с ними организации, компании и университеты) будут первыми юридическими лицами, которые смогут использовать крупномасштабные квантовые вычисления. Возможно, крупнейшие корпорации (такие как Google, IBM, Alibaba или Microsoft) первыми получат доступ к технологии, но даже если они обойдут

правительства, то последние, вероятно, окажутся приоритетными клиентами, за которыми последуют крупные организации.

И тогда в скором времени мы увидим, как компании всех размеров будут использовать квантовые компьютеры для сотен разных приложений. Квантовые компьютеры с разделением времени получат широкое применение в крупных организациях и университетах. Я думаю, что все это произойдет в течение нескольких лет после достижения квантового превосходства. В пределах ближайших десяти лет или около того все мы будем запускать какие-то функции квантовых вычислений на наших собственных устройствах. Либо они будут частью квантовых устройств, либо наши устройства будут связаны со службами, которые обрабатывают и доставляют квантовые вычисления, когда они нужны нашим устройствам и задачам.

Мы уже не раз оказывались на пороге технологического скачка. Это случилось с интернетом. Это произошло с традиционным криптографическим открытым ключом. Все эти достижения сначала приносили пользу правительству и крупным организациям, а затем в короткие сроки выходили в широкий мир. Правительства пытались (и все еще пытаются) держать сильную криптографию вдали от остального мира. Пока что эта стратегия не работала слишком долго – главным образом потому, что однажды особенно сильная криптографическая реализация, известная в теории, вскоре после этого становится практической реальностью. Пытаться остановить использование сильной криптографической идеи в мире – все равно что пытаться прекратить общение. Это часто одно и то же, особенно в цифровом мире.

Резюме

Подведем итог этой главы. Хотя мы не знаем, когда наступит квантовое превосходство и состоится криптопрорыв, общее мнение самых знающих компьютерных ученых и правительства США таково: вы должны начать готовиться сейчас. В главе 5 мы рассмотрим, как, вероятно, будет выглядеть постквантовый мир, чтобы вы могли получить полное представление о том, как начинать подготовку к нему.

5 Каким будет постквантовый мир?

Когда квантовое превосходство и предстоящий квантовый криптопрорыв произойдут, мир изменится навсегда. Будут история мира до этого и невероятное будущее после. Большинство изменений будут поступательными, пройдет множество этапов, подразумевающих различные применения новой технологии и появление приложений. Некоторые изменения осуществятся в сроки, измеряемые неделями и месяцами, другие – годами и десятилетиями. Но далеко идущие, важные перемены грядут.

В этой главе рассматриваются вероятные события, начиная с того, какие приложения могут быть взломаны квантовыми вычислениями в ближайшем будущем (чему уделяется основное внимание в книге), и продолжая появлением новых или улучшенных устройств и приложений благодаря квантовым свойствам. Как и большинство значительных технологических достижений прошлого, эти изменения могут, и будут, использоваться как в благих целях, так и со злым умыслом. Квантовые вычисления повлияют на нас во многих отношениях, не только раскрыв криптографические секреты. После того как в этой главе будут рассмотрены недостатки и улучшения, связанные непосредственно с криптографией, поговорим и о тех замечательных изобретениях и улучшениях, которые мы увидим помимо инноваций в сфере криптографии.

Примечание Слово «приложение» в этой главе используется для обозначения любого типа реализации технологий, а не только программного обеспечения.

Взломанные приложения

Основная задача при написании этой книги – показать, как все приложения, предназначенные для вычислений и использующие современные технологии, алгоритмы, протоколы и шифры, будут ослаблены или полностью сломаны квантовыми вычислениями. Они включают в себя любое приложение, которое имеет защиту на основе чего-то такого, что квантовые свойства смогут одолеть. Постквантовый мир будет полон ослабленных и полностью взломанных криптокодов (и большого количества квантовоустойчивой криптографии, как будет показано в главе 6 «Квантовоустойчивая криптография» и главе 7 «Квантовая криптография»). Как описано в предыдущих главах, это произойдет с любой защитой, которая основана на неспособ-

ности традиционных двоичных компьютеров выполнять сверхбыстрые вычисления (которые может преодолеть алгоритм Гровера) или факторинга математических формул с большими простыми числами и использованием алгоритма Шора.

Ослабленные хеши и симметричные шифры

Алгоритм Гровера по сути означает, что квантовые компьютеры смогут ослабить большинство существующих традиционных симметричных шифров и хешей, особенно когда они используются с ключами небольшого размера. Алгоритм Гровера, выполняемый на квантовых компьютерах, существенно, наполовину, снижает защиту большинства симметричных шифров. 128-битные шифры будут иметь только 64-битную эквивалентную защиту, 256-битные – лишь 128 бит эквивалентной защиты и т. д. Когда произойдет квантовый криптопрорыв, 128-битная защита симметричного ключа все еще будет считаться достаточно сильной, чтобы быть взломанной сразу, но взлом будет возможен в ближайшей перспективе. Если учесть традиционные улучшения в компьютерных процессорах (т. е. закон Мура), 128-битные симметричные ключи могут обеспечивать защиту лишь в течение нескольких лет, а не десятилетиями.

Любой симметричный шифр или хеш, использующий размеры ключей или хеш-величину меньше 256 бит, будет иметь сомнительные свойства для долгосрочной защиты (т. е. будет квантововосприимчив). Симметричная криптография с использованием ключей большего размера считается квантовоустойчивой и находится вверху шкалы безопасности при использовании соответствующих размеров ключей. Большинство криптографических экспертов рекомендуют использовать 256-битные и более крупные симметричные ключи для борьбы с угрозами квантовых атак в долгосрочной перспективе. Традиционно считается, что организации, нуждающиеся только в умеренных требованиях безопасности или необходимости защиты секретов в течение нескольких лет, могут использовать 192-битные симметричные ключи, но организации, которым необходима высокая безопасность или защита в течение многих лет, должны использовать 512-битные ключи. Хотя в качестве «моста» ключи от 192 до 256 бит могут быть использованы для сохранения важных и конфиденциальных данных, в конечном итоге они должны быть заменены на ключи бóльших размеров. По сути, вам следует строить ваш план в соответствии с неравенством Моски. Подробнее об этом – в главе 9 «Готовимся сейчас».

Примечание В криптографических хешах следует использовать такие же длины ключей, как и рекомендованные для симметричных шифров, даже если они не относятся к криптографическим типам.

Очень важно отметить, что даже для «криптографически сильных» симметричных шифров и хешей квантовые вычисления считаются угрозой, если используются 192-битные или меньшие размеры ключей и дайджестов. Например, даже в настоящее время доверенные и принятые хеши SHA-2 и SHA-3

не считаются квантовоустойчивыми, если они используют размеры ключей меньше 192 бит, потому что основной недостаток в сценариях квантового взлома заключается в защите размером ключа, а не слабости базового алгоритма. Размер ключа определяет «биты защиты», обеспечиваемые шифром или хешем. Например, шифр, использующий 128-битный ключ, насчитывает 2^{128} бит, о которых взломщик должен будет догадаться, чтобы быть уверенным в том, что он найдет правильный ответ (если только в алгоритме не было криптографической ошибки и это не ослабило общую защиту).

В большинстве реальных сценариев среднее число догадок будет равно половине 128 бит (что составляет 2^{127} бит), потому что в среднем половину времени число реальных догадок будет меньше 2^{127} догадок и половина времени потребовалась бы для более чем 2^{127} догадок (что в среднем и равно 2^{127} догадкам при большом количестве попыток). При чистом угадывании ключей или результатов хеширования «грубой силой» все определяется количеством битов защиты, о которых нужно догадаться. Математическое мастерство основного алгоритма не является фактором успеха, когда атаки совершаются путем чистых догадок.

Примечание Национальный институт стандартов и технологий (NIST) и другие организации рассматривают 128-битные симметричные шифры как «слабо квантовоустойчивые». Я не знаю никого, кто хотел бы перейти на безопасную квантовоустойчивую криптографию и иметь «слабую» защиту. Я не считаю 128-битные ключи действительно квантовобезопасными и отношусь к ним соответственно.

В табл. 5.1 приведены примеры различных традиционных хешей и шифров, которые не считаются устойчивыми (то есть восприимчивыми или сопротивляющимися) в постквантовом (post-quantum, PQ) мире.

Таблица 5.1. Слабые и квантовоустойчивые традиционные хеши и шифры в постквантовом мире

Хеши		**Симметричные шифры**	
Квантовоустойчивые	**Квантовоустойчивые (при выборе дайджеста 192 бита или больше)**	**Квантовоустойчивые**	**Квантовоустойчивые (при выборе размера ключа 192 бита или больше)**
MD-4, MD-5, SHA-1, LM, NT, SHAKE-128, RIPEMD (если используется ключ размером менее 192), PBKDF1, PBKDF2 (если используется ключ размером менее 192), BCRYPT	SHA-2, SHAKE, SHA-3, PBKDF2, RIPEMD, Argon2, Blake2	DES, 3DES, DESX, CAST, IDEA, SAFER Kuznyechik, Serpent-128 и -192, AES-128, Twofish (менее, чем 192 бита)	AES, Blowfish, Twofish, Serpent-256 bits, Chacha/Salsa20

Примечание Любая организация, заинтересованная в квантовой устойчивости, должна начать использование традиционных симметричных шифров и хешей с размерами ключей, равными или превышающими 256 бит, для большей гарантии – с 512 битами.

Если симметричный ключ взломан, злоумышленник может прочитать содержимое, которое этот ключ защищал. Это случалось в прошлом. Более ранние симметричные шифры, такие как DES (с 64-битными ключами, но только с 56-битной защитой), считались тогда достаточно сильными, чтобы защитить конфиденциальную информацию.

Увеличившаяся со временем вычислительная мощность сделала DES незащищенным. Сегодня информация, защищенная DES, может быть взломана в течение нескольких минут. Соответственно, текущая рекомендация симметричного шифра – это AES с 256 битами или для большей защиты 512 битами. Если вы хотите иметь квантовую безопасность в течение длительного времени, AES-192 является приемлемым шифром для квантовой защиты только на очень короткий срок, может быть на несколько лет.

Если хеш взломан, злоумышленник может создать другое, мошенническое содержимое, которое имеет такой же идентичный хеш-дайджест (который, как будет утверждать противник, является оригинальным законным контентом). Это прообраз, известный как вторая атака. Два разных содержимых, создающих один и тот же результат хеша, делают недействительным алгоритм хеширования для любого использования. Это случалось несколько раз и совсем недавно, в 2017 году, было подтверждено исследователями Google на примере хеша SHA-1. Google смогла создать два различных документа, которые привели к идентичным хешам SHA-1 (см. рис. 5.1). Подробнее о первом успешном «конфликте» хешей SHA-1 можно прочитать здесь: http://shattered.io/.

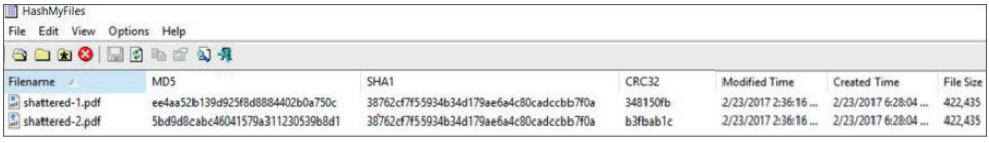


Рис. 5.1. Пример хешей и документов с разным содержанием, показывающий идентичность SHA-1 хешей от двух разных документов

Примечание Интересно, что, как видно на рис. 5.1, предположительно более слабые алгоритмы хеширования MD-5 и CRC32 правильно показывают два разных значения хеша, в то время как якобы более сильный хеш SHA-1 – нет. Это потому, что два разных документа были специально подобраны для использования уязвимости в алгоритме хеширования SHA-1 и исследователей не интересовало воздействие этих документов на другие алгоритмы. На самом деле применять уязвимости в программах MD-5 и CRC32 значительно проще, и это уже было использовано много лет назад. Однако создать два документа, которые давали бы во всех трех хешах одинаковые

хеш-значения для обоих документов, было бы еще труднее. Если бы «документ» был более сложным исполняемым файлом, было бы экспоненциально сложнее (а то и еще более сложно) создать вредоносный исполняемый файл с таким же хешем, как оригинальный, несложный исполняемый файл. Но в криптографии, если ваш шифр дает сбой, даже в несложном тесте, он непригоден полностью.

Примечание Хеш CRC32 не является криптографическим хешем. Циклические проверки избыточности (cyclic redundancy checks, CRC) обнаруживают ошибки кодов и позволяют быстро обобщить и как настоящий криптографический хеш позволяют быстро обобщить и сравнить два разных содержимых. Но CRC не имеют каких-либо необходимых свойств хорошего хеша, такого, например, как гарантия, что никаких два разных содержимых никогда не будут иметь один и тот же дайджест на выходе. CRC был популярным «хешем бедняков» в течение десятилетий, но теперь в большинстве приложений его заменили настоящие криптографические хеши.

Уроки истории показывают, что слабые симметричные шифры и хеши могут использоваться противниками в злонамеренных целях. Слабые симметричные шифры могут быть использованы для чтения несанкционированного контента, а слабые хеши – для получения неверных результатов сравнения, согласно которому два разных контента идентичны, чем можно воспользоваться, чтобы обмануть ничего не подозревающих пользователей. Ослабленные асимметричные шифры были использованы в нескольких высокопрофессиональных атаках, чтобы скомпрометировать ничего не подозревающих жертв.

Взломанные асимметричные шифры

Как сказано в предыдущих главах, после того как алгоритм Шора (или другие алгоритмы, которые улучшат его) будет запущен на квантовом компьютере с достаточным числом устойчивых кубитов, любой асимметричный шифр, который опирается на одну из трех математических задач: целочисленная факторизация, дискретный логарифм или дискретный логарифм эллиптической кривой, – будет непригодным шифром. Такими являются следующие традиционные алгоритмы асимметричного шифрования:

- Rivest, Shamir, Adleman (RSA);
- Diffie–Hellman (DH) и родственные примитивы;
- Elliptic Curve Cryptography (ECC) и родственные примитивы;
- ElGama.

Как и в отношении алгоритмов симметричного шифрования, размер ключа асимметричного шифра определяет, будет он считаться слабым или взломанным. Выполнение алгоритма Шора для вычисления любого уравнения с простыми числами требует $(2 \times n) + 3$ устойчивых кубита, где n – количество битов асимметричного ключа для взлома. Таким образом, чтобы взломать 2048-битный ключ RSA, нужно 4099 стабильных кубитов, а для взлома

4096-битного ключа RSA нужно 8195 стабильных кубитов. Теоретически вы можете постепенно увеличивать размеры асимметричных ключей, чтобы опередить число кубитов, которые получают квантовые компьютеры. И все же большинство квантовых экспертов считают, что гораздо лучше перейти на квантовоустойчивый асимметричный шифр, чтобы ваша защита не зависела от опережающего числа кубитов, которое вы не можете контролировать.

Примечание Обмен ключами с высокой квантовой восприимчивостью также является слабым, или взламываемым. Соответственно, к ним относятся и традиционные обмены ключами, такие как Диффи–Хеллман (DH) и эллиптическая кривая Диффи–Хеллмана (ECDH).

Ослабленные и взломанные генераторы случайных чисел

Компьютерная безопасность часто полагается на случайно сгенерированные числа для большей части операций (более подробно это объясняется в главе 7). Из-за этой зависимости большинство компьютеров имеют встроенные генераторы случайных чисел аппаратного уровня (random number generators, RNG) как в большинстве операционных систем, так и во многих приложениях на уровне программного обеспечения. К сожалению, неквантовый компьютер не может быть в этом отношении по-настоящему случайным и неспособен генерировать действительно случайные числа. И даже если традиционные компьютеры могли бы это делать, они не могли бы представить доказательство того, что какое-либо конкретно сгенерированное число выбрано действительно случайно. Вместо этого RNG неквантовых компьютеров стараются приблизить к истинной случайности (применяя то, что называется псевдослучайностью): для обычного человека и для приложения числа представляются как совершенно случайные, даже если это не так. Проблема состоит в том, что любое число, от которого требуется быть сгенерированным по-настоящему случайно, создает потенциальную уязвимость, когда таковым не является. Эта проблема ставила в затруднительное положение индустрию компьютерной безопасности с первых же дней компьютерной эры.

Было обнаружено, что многие, если не большинство, генераторы RNG уже десятилетиями содержат одну или несколько уязвимостей, которые были обнаружены при использовании традиционных методов и *стандартного времени вычислений* (т. е. ускорения экспоненциального или логарифмического решения не требуется, чтобы прийти к решениям в разумных рамках временно́го ограничения). История неудачных решений компьютерной безопасности изобилует примерами уязвимостей генераторов случайных чисел. В основном если противники смогут найти, как генератор псевдослучайных чисел их генерирует (это всегда будет повторяемый шаблон, который можно использовать для прогнозирования очередного числа), они могут использовать это, чтобы ослабить или взломать шифр либо приложение более высокого уровня.

Из-за этого наиболее популярные и зависимые генераторы RNG постоянно со временем улучшают псевдослучайность. Плохие RNG перестают

использовать, а существующие улучшаются и имеют менее очевидные недостатки. Сегодня многие неквантовые RNG *кажутся* почти случайными, даже если они таковыми не являются. Найти уязвимости и предсказуемые закономерности в их работе – задача не из легких. Тем не менее многие криптографические исследователи сосредоточены на поиске недостатков RNG. Поиск неслучайных повторяющихся образов несколько похож на попытку вычислить большие уравнения с простыми числами или взломать симметричные ключи.

Чем большей вычислительной мощностью вы располагаете, тем легче вам найти уязвимости генераторов RNG. Квантовые свойства и алгоритмы (такие как суперпозиция и алгоритм Гровера) увеличат вероятность того, что уязвимость традиционного RNG будет найдена быстрее. Есть даже большой шанс, что квантовые компьютеры смогут найти любую предсказуемую, повторяемую классическую схему работы RNG компьютера, раскрывая все его истинные уязвимости. Достаточно сказать, что квантовые вычисления могут ослабить, если не взломать традиционные RNG всегда, а соответственно и все, что от них зависит. Лучшее решение для слабых и взломанных традиционных генераторов случайных чисел заключается в использовании *квантовых* генераторов случайных чисел (рассматриваются в главе 7).

Слабые, или взломанные, зависимые приложения

Очевидно, что любое приложение, использующее квантововосприимчивый хеш, шифр или RNG, также считается квантововосприимчивым. Сегодня существует гораздо больше уязвимых приложений компьютерной безопасности, чем неуязвимых. Вот несколько распространенных примеров таких приложений.

Безопасность транспортного уровня

Простота, с которой можно взломать криптокоды безопасности транспортного уровня (Transport Layer Security, TLS), на которую в значительной степени полагается интернет, показывает, насколько велика угроза прорыва квантовых вычислений. TLS зависит от квантововосприимчивой инфраструктуры открытых ключей (public key infrastructure, PKI), цифровых сертификатов, цифровых подписей, асимметричных шифров, симметричных ключей и хешей. TLS использует асимметричные шифры и цифровые сертификаты, позволяющие компьютеру-хосту и пользователям аутентификацию. Это также дает возможность участникам общаться, безопасно генерируя общие симметричные ключи сеанса, чтобы уполномоченные стороны могли шифровать трафик (используя независимые генерируемые общие сеансовые симметричные ключи). В 2019 году более 70 % интернет-сайтов используют HTTPS, полагаясь на TLS (https://etherealmind.com/percentage-of-https-tls-encrypted-traffic-on-the internet/). TLS также внедряется с головокружительной скоростью практически в каждую виртуальную частную сеть (VPN) как часть безопасности VPN. В течение десятилетий для большинства сетей VPN составлялись собственные алгоритмы и методы обеспечения безопасности, но сейчас большинство из них, в том числе самые крупные и популярные VPN

(Cisco, Palo Alto, Microsoft и т. д.), полагаются на TLS, по крайней мере в части базовой безопасности.

Существует несколько разных версий TLS (версия 1.3 является самой последней версией на момент написания статьи), и хотя TLS может быть обновлена для использования в квантовоустойчивой криптографии, почти каждая текущая реализация использует квантововосприимчивую версию. Если история нас чему-нибудь да учит, то с момента, когда миру станет ясно, что пора обновить TLS реализации квантовоустойчивой формой, пройдет много лет, прежде чем это будет сделано и большая часть интернета будет обновлена. TLS перенесла много прошлых критических уязвимостей, и обычно большинству разработчиков TLS требовалось от трех до пяти лет, чтобы перейти к менее уязвимым версиям. Будем надеяться, что это не займет столько времени, когда произойдет квантовый прорыв. Или давайте надеяться даже на большее – что разработчики смогут перейти на квантовоустойчивые версии TLS еще раньше.

PKI и приложения для цифровых сертификатов

Как и в случае с TLS, популярность приложений, использующих инфраструктуру открытых ключей (PKI) и цифровые сертификаты, за последнее десятилетие возросла. PKI была популярна в течение десятилетий, хотя обычно реализовывалась, оставаясь незаметной. Большинство конечных пользователей не понимают, насколько серьезно они полагаются на PKI изо дня в день. В последние 10 лет наблюдается быстрый рост числа внутренних приложений в организациях, использующих PKI. Почти невозможно найти организацию, которая не полагалась бы на PKI при осуществлении ежедневных важных для бизнеса функций.

Как только квантовые компьютеры смогут использовать пару открытый/закрытый ключ размером 4096 бит или меньше, большинство текущих реализаций PKI в мире будут полностью нарушены – от корневой сертификации полномочий (certification authority, CA) до каждого цифрового сертификата, который CA и ему подчиненные, зависимые CA когда-либо выдавали. Большинство выпущенных в настоящее время цифровых сертификатов используют только 2048 бит защиты, и значительный процент всех цифровых сертификатов все еще используют только 1024 бита. 4096-битный криптопрорыв взломает их все, хотя 1024- и 2048-битные сертификаты сдадутся первыми. Центры сертификации PKI и многие приложения с поддержкой PKI могут быть обновлены, используя менее восприимчивые формы криптографии. Но, как и в случае с TLS, почти каждое из этих приложений в настоящее время использует квантововосприимчивую форму, и перемещение их в квантовоустойчивые формы, вероятно, займет годы. Эти приложения с поддержкой PKI включают следующее:

- решения идентификации и аутентификации хоста с использованием цифровых сертификатов;
- решения для паролей и аутентификации с использованием криптографии с открытым ключом;
- TLS-защищенные версии протокола защищенного копирования (SCP), почтового протокола (POP3), сеть протокола передачи новостей

(NNTP), простой протокол передачи почты (SMTP), протокол доступа интернет-сообщений (IMAP), протокол передачи файлов (FTP), Telnet, протокол передачи гипертекста (HTTP), протокол защищенной интернет-конференции Live (SILC) и т. д.;
- смарт-карты / виртуальные смарт-карты;
- многофакторную аутентификацию (MFA), использующую асимметричные шифры;
- Secure Shell (SSH);
- Pretty Good Privacy (PGP);
- безопасные/многоцелевые интернет-почтовые расширения (S/MIME);
- Unified Extensible Firmware Interface (UEFI), который является протоколом загрузки вычислительного устройства и используется большинством компьютеров;
- расширения безопасности системы доменных имен (DNSSEC), используемые для защиты транзакций DNS;
- DomainKeys Identifi-Mail (DKIM), используется для предотвращения подделки почтового домена;
- модули безопасности оборудования (HSM);
- безопасность порта 802.1X (при использовании цифровых сертификатов);
- криптосистемы Paillier (и их исторических предшественников);
- YAK (протокол согласования ключей с аутентифицированным открытым ключом);
- автомобильные компьютерные системы, которые используют асимметричные шифры (большинство из них);
- почти любое другое приложение, использующее PKI и цифровые сертификаты.

Достаточно сказать, что квантовые вычисления, скорее всего, взломают большую часть того, на что опирается безопасность интернета. Легче найти то, что не будет взломано, чем то, что будет взломано.

Цифровые подписи

Цифровая подпись аутентифицирует содержание контента (документы, программы, данные, идентификационные данные и т. д.), использующие PKI, асимметричные шифры и хеширование. Все текущие популярные реализации, включая алгоритм цифровой подписи (Digital Signature Algorithm, DSA) и алгоритм цифровой подписи эллиптической кривой (EDSA), используют квантововосприимчивую криптографию. Одним из самых распространенных применений цифровых подписей является подпись контента и загрузок из открытых источников и от коммерческих поставщиков. Квантовый криптовзлом может позволить противникам генерировать идентичные пары открытый/закрытый ключ, а затем разрешить им подписывать новые или подписанный вредоносный контент и отправлять его ничего не подозревающим потребителям.

Историческая реальная асимметричная атака Атака произошла в 2012 году с использованием открытой криптографии с сертификатом цифровой

подписи, которые со временем были значительно ослаблены. Продвинутая вредоносная программа, известная как Flame (https://en.wikipedia.org/wiki/Flame_(malware)), создала поддельный сертификат цифровой подписи Microsoft (см. рис. 5.2) для подписи вредоносной программы. Подделка удалась из-за нескольких недостатков, в том числе:

- длина задействованного асимметричного ключа составляла всего 512 бит;
- он был хеширован уязвимым хешем MD-5;
- родительский центр сертификации (CA) разрешил дочерним сертификатам включать цель цифровой подписи, хотя не было никаких оснований для того, чтобы эта конкретная цель была разрешена для любого сертификата, выданного CA. Это позволило злоумышленникам создавать новые цифровые сертификаты подписи, как только оригинал пары асимметричных ключей был взломан.

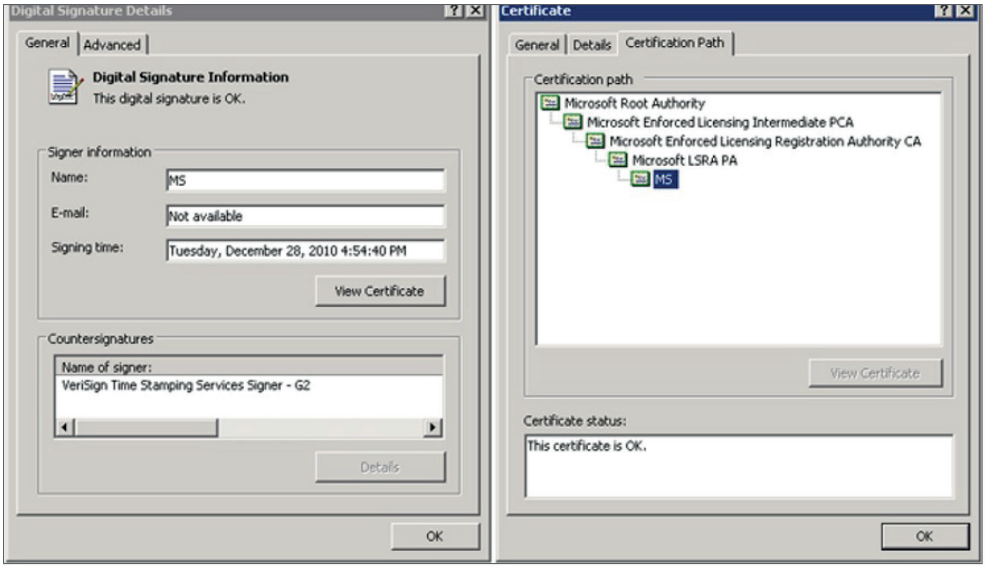


Рис. 5.2. Поддельный цифровой сертификат, имитирующий сертификат от компании Microsoft и использующий фальшивую подпись

Все эти криптографические недостатки позволили злоумышленнику воссоздать законную пару открытый/закрытый ключ, используемую реальным CA Microsoft для подписи дополнительных (мошеннических) цифровых сертификатов. Злоумышленник создал новый сертификат цифровой подписи, а затем использовал его для подписи своих подделок.

Затем вредоносное программное обеспечение может быть отправлено возможным жертвам, которые легко обманутся, поверив, что соответствующая программа является законной программой от Microsoft. В некоторых случаях цифровая подпись позволяла устанавливать вредоносное программное обеспечение без согласия пользователя на установку.

Это был первый известный случай, когда пара открытых и закрытых ключей CA популярного поставщика была взломана злоумышленником и позволила злонамеренно подписать несанкционированный контент. Создатели вредоносного программного обеспечения ранее похитили пары открытых и закрытых ключей от законных поставщиков, а затем использовали украденный сертификат для создания своих вредоносных программ (как это было сделано во вредоносной программе Stuxnet). Но это был первый раз, когда криптографический взлом использовался для создания совершенно нового (мошеннического) сертификата цифровой подписи. Смотрите https://arstechnica.com/information-technology/2012/06/flame-malware-hijacks-windowsupdate-to-propogate/ – отличное обсуждение вредоносной программы Flame и посетите веб-сайт https://blogs.technet.microsoft.com/msrc/2012/06/03/microsoft-releases-security-advisory-2718704/, если хотите прочитать официальное предупреждение Microsoft об этой проблеме.

Microsoft разными способами аннулировала мошеннический цифровой сертификат и провела полную проверку всех своих открытых цифровых сертификатов, срок которых либо не истек, либо они ранее не были аннулированы. Было найдено несколько других слабых цифровых сертификатов, которые были удалены или отозваны, прежде чем могли быть злонамеренно использованы. Компания Microsoft также обновила систему Microsoft Windows и соответствующее программное обеспечение, с тем чтобы они больше не принимали цифровые сертификаты с асимметричными ключами размером менее 1024 бит. Урок заключается в том, что ослабленный или взломанный асимметричный шифр может быть легко использован злоумышленником.

Безопасность сети Wi-Fi

Большинство беспроводных сетей Wi-Fi защищены с помощью беспроводного протокола безопасности, известного как Wi-Fi Protected Access (WPA). В настоящее время существует три версии: WPA, WPA2 и WPA3. Большинство сетей Wi-Fi в настоящее время используют WPA2. Версия WPA3, впервые примененная в 2018 году, до сих пор не получила широкого распространения.

Во многих корпоративных сценариях беспроводная безопасность WPA2 использует цифровые сертификаты, безопасность портов 802.1X и симметричное шифрование. В большинстве реализаций (дома или на предприятии), даже если асимметричные шифры не используются, есть симметричные шифры. И в большинстве случаев симметричным шифром является AES с размером ключа 128 бит. В некоторых более новых реализациях (с использованием WPA3) используются 192-битные симметричные ключи шифрования, которые все еще намного ниже минимального размера симметричного ключа 256 бит, рекомендуемого для долговременной квантовой устойчивости. Многие маршрутизаторы Wi-Fi используют предварительный общий ключ (pre-shared key, PSK) в качестве значения инициализации, чтобы позволить новым узлам присоединиться к сети. Это «пароль Wi-Fi», который большинство людей дают гостям, чтобы они могли присоединиться к сети Wi-Fi. Сегодня PSK должны генерироваться случайным образом и содержать

не менее 16–20 символов или больше, хотя на практике немногие реализации Wi-Fi следуют этому совету по безопасности. Традиционным инструментом взлома сети Wi-Fi часто предлагают PSK и пытаются снова и снова подсоединяться к сети, пока не получают правильный ключ PSK.

Примечание Большинство беспроводных концентраторов Wi-Fi позволяют использовать PSK длиной до 63 символов.

После того как клиент предоставит правильный PSK (или цифровой сертификат 802.1X), WPA2 создает общий сеансовый секретный ключ, называемый *парным главным ключом* (pairwise master key, PMK), и хеширует его с помощью алгоритма хеширования PBKDF2-SHA1 с квантововосприимчивыми размерами ключей. Квантовое ускорение компьютера может позволить квантовому компьютеру быстрее взломать хеш и угадать PMK.

Итак, путем атаки на PSK, PMK, хеши или симметричные/асимметричные алгоритмы и ключи современные традиционные сети Wi-Fi предоставляют квантовым компьютерам много возможностей для получения неавторизованного доступа к сети или подслушивания защищенной с помощью криптографии информации.

Примечание Мотивированные противники уже могут записывать защищенный в настоящее время трафик сети Wi-Fi своих противников, ожидая того дня, когда они смогут расшифровать этот трафик, используя квантовые вычисления. Угроза квантового криптовзлома против беспроводных сетей и других видов подслушивания – это уже риск.

Microsoft Windows

Как и большинство популярных современных операционных систем, Microsoft Windows включает множество восприимчивой криптографии, в том числе хеши, симметричные шифры, асимметричные шифры и RNG. Основные протоколы аутентификации Windows (Kerberos и NT [New Technology (Новая технология)] LAN Manager [NTLM]) являются квантововосприимчивыми. Оба используют 128-битное значение MD-5 хеша NT. Хеши NT используются не только в сетевых и локальных сценариях аутентификации, но и для хеширования памяти паролей, как локально, так и на контроллерах домена Active Directory. Локально кешированные пароли используют хеш PBKDF2, который более устойчив, но все же восприимчив.

Новый протокол аутентификации Microsoft Windows Hello for Business использует аппаратное или программное обеспечение, зашифрованное шифром с открытым ключом и/или цифровыми сертификатами для поддержки разрешенных механизмов аутентификации. Windows 10 (и другие версии) поддерживает стандарт FIDO (Fast ID Online) 2.0 (https://fidoalliance.org/fido2/), основанный на цифровых сертификатах и шифрах с открытым ключом.

Microsoft использует SHA-2 (128-бит) для хеширования, хотя многие файлы также (или только) используют хеш SHA-1 для целей обратной совмес-

тимости. В настоящее время Windows применяет 128-битные шифры AES для симметричного шифрования и 2048-битные ключи RSA по умолчанию для асимметричного шифрования, хотя и бóльшие размеры ключа поддерживаются и могут быть легко включены.

Большинство приложений Microsoft, включая флагманский продукт PKI, сертификат Active Directory Services (ADCS), используют квантововосприимчивые шифры по умолчанию. Microsoft уже успешно протестировала ADCS с использованием квантовоустойчивых шифров, чтобы убедиться, что ADCS может применять их при необходимости.

Поскольку Windows по умолчанию не включает квантовоустойчивые асимметричные шифры, любое приложение Microsoft с использованием асимметричного шифра также можно считать квантововосприимчивым. Любая функция или приложение Microsoft, использующее меньшие симметричные ключи и хеши (особенно если не применяются большие размеры ключа, такие как 192 или более), также восприимчиво в течение длительного времени. Как описано в главе 2 «Введение в квантовые компьютеры», компания Microsoft – главный квантовый исследователь и уже в значительной степени исследовала и инвестировала в изучение того, как при необходимости перевести все свои продукты в квантовоустойчивые формы, больше, чем любой другой популярный поставщик операционных систем. Обратите внимание на то, что Microsoft говорит о своих рекомендациях по шифрованию. Когда Microsoft говорит, что пришло время двигаться, двигайтесь!

Криптовалюты

Общий вопрос в квантовых кругах: являются ли криптовалюты квантововосприимчивыми. В некоторой степени да; большинство из них, включая биткойны и все самые популярные реализации. Лежащая в их основе криптография, по крайней мере, в некоторой степени квантововосприимчива, и многие из наиболее важных компонентов криптовалют абсолютно чувствительны к квантовым воздействиям. Большинство криптовалют испытывают проблемы как минимум в четырех основных областях: блокчейн, открытые и закрытые ключи каждого пользователя, безопасность сети и криптовалютный кошелек отдельного пользователя.

Восприимчивость блокчейна Давайте начнем с блокчейна, который, вероятно, наименее восприимчив по сравнению со всеми задействованными компонентами. Блокчейн – это распределенная децентрализованная бухгалтерская книга (т. е. база данных) для отслеживания и проверки отдельных транзакций. Каждый участник, осуществляющий транзакцию, может быть сохранен в отдельном «блоке» транзакции, или может быть сохранено несколько транзакций в одном блоке. Количество транзакций, хранимых в блоке, зависит от реализации. Отдельный блок содержит информацию о транзакции (это может быть любая информация, определяемая приложением, включая просто хеш требуемой информации о транзакции), и, по крайней мере, один криптографический хеш вместе с любой другой необходимой информацией.

Общий формат блока блокчейна представлен на рис. 5.3.

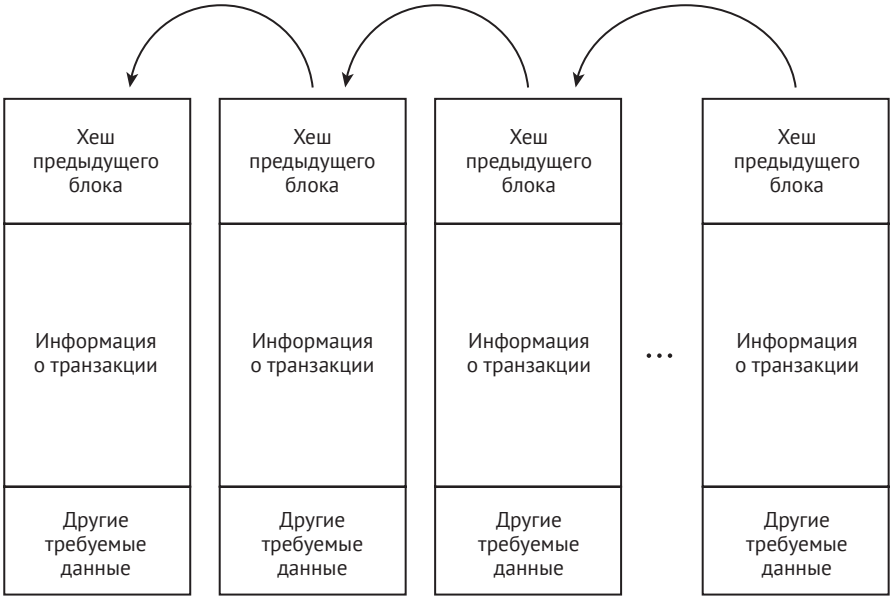


Рис. 5.3. Формат блока в блокчейне

«Цепочка» блокчейна отражает тот факт, что хеш предыдущего блока сохраняется в следующем блоке, который затем хешируется и сохраняется в следующем блоке, и т. д. Это делает каждый последующий блок «сцепленным» путем хеширования с предыдущим блоком таким образом, что все блоки в блокчейне криптографически связаны друг с другом. Вы не можете легко вмешаться в любой блок без изменения каждого последующего блока (потому что хеш из поврежденного блока будет изменен). Это очень сильная защита хешей. Хеш в большинстве блокчейнов является квантовоустойчивым и использует 256-битную защиту хеш-дайджеста. Хотя 512 бит были бы более квантовобезопасными и надежнее в долгосрочной перспективе, но уже хорошо, что большинство хешей не 128-битные. Есть также другие варианты.

Во-первых, как описано выше, для того чтобы злонамеренно манипулировать любым блоком в блокчейне, вам нужно будет изменить информацию, хеши всех последующих блоков и сделать это так, чтобы это не было обнаружено и восстановлено всеми основными участниками (или как минимум половиной). Это очень сильная внутренняя защита. Поэтому блокчейны становятся настолько популярными для транзакций, нуждающихся в долгосрочной защите целостности.

Примечание Так называемые «атаки 51 %» были совершены в реальном мире против менее популярных криптовалют. Смотрите в качестве примера https://www.ccn.com/ethereum-classic-51-attack-blockchain-securityresearchers-reveal-full-implications/.

Во-вторых, хотя хеш-дайджест может иметь длину всего 256 бит, он часто один и тот же используется несколько раз и/или в сочетании с дополнительными хешами. Например, биткойн применяет SHA-256 и RIPEMD-160. RIPEMD-160 в отдельности, безусловно, считается квантововосприимчивым, но в сочетании с SHA-256 и особенно с несколькими доработками SHA-256 он оказывается таковым в меньшей степени.

Другие криптовалютные восприимчивости Криптовалюты становятся более квантововосприимчивыми в условиях, где и когда они используют квантововосприимчивые открытые шифры. Интернет-соединения между отдельными участниками и блокчейном криптовалюты защищены TLS, и каждый отдельный пользователь использует квантововосприимчивую криптографию с открытым ключом, чтобы модифицировать блокчейн и защитить свои индивидуальные кошельки. Любой, кто изучает пару открытый/закрытый ключ пользователя, может украсть пользовательский кошелек или злонамеренно манипулировать пользовательской транзакцией на пути к блокчейну.

Кошельки отдельных пользователей снова и снова подвергались жесткому взлому, так как биткойн мгновенно сделал многих людей миллионерами. Сотни миллионов долларов и, вероятно, миллиарды долларов были украдены еще до того, как квантовый криптографический взлом считался частью картины потенциального риска. Блокчейны и криптовалюты подвергаются атакам не только отдельных хакеров и групп, но также и национальных государств. Некоторые страны-изгои, такие как Северная Корея, известны тем, что пополняют свой бюджет, крадя сотни миллионов долларов в криптовалютах.

Есть два больших опасения, связанных с квантовым взломом криптовалют. Во-первых, когда случится квантовый прорыв, денежная система всего мира также будет атакована (ее большая часть защищенна TLS и другими квантововосприимчивыми шифрами), поэтому криптовалюты будут только одной из наших многочисленных забот. Во-вторых, большинство криптовалют могут «раскошелить» (т. е. разделить) свои реализации на более квантовоустойчивые наборы требований. Этот подход создает отдельные проблемы, но он много раз применялся для решения других проблем и вопросов безопасности.

Есть также несколько уже существующих квантовоустойчивых криптовалют, но они находятся в меньшинстве. Большинство существующих руководящих органов организаций, связанных с криптовалютой, считают, что криптографические издержки преждевременного перехода на квантовоустойчивые шифры не оправданы. Многие популярные криптовалюты планируется перевести на менее квантововосприимчивую криптографию, когда станет очевидным скорый квантовый криптографический прорыв. Если вы хотите больше узнать о криптовалютах и их квантовой восприимчивости, обратитесь к многочисленным ресурсам, в том числе:

- https://en.bitcoin.it/wiki/Quantum_computing_and_Bitcoin;
- www.youtube.com/watch?v=Uy5zHAwo43o;
- http://diyhpl.us/~bryan/papers2/bitcoin/On%20Bitcoin%20security%20in%20the%20presence%20of%20broken%20crypto%20primitives%20-%202016.pdf.

Bluetooth и NFC

Bluetooth – это очень распространенный стандарт беспроводной связи на УВЧ-радиочастотах на короткие расстояния (обычно 4,5 метра или менее), часто используемый между двумя устройствами для передачи информации и для подключения беспроводных наушников и колонок. *Связь ближнего поля* (near field communication, NFC) используется для передачи информации на очень короткие расстояния, обычно измеряемые несколькими дюймами. NFC часто применяется для беспроводных платежных систем, бесконтактной аутентификации и передачи информации между двумя устройствами, такими как сотовые телефоны. И Bluetooth, и большинство протоколов NFC основаны на квантововосприимчивых шифрах. Например, существуют различные уровни и режимы безопасности Bluetooth в зависимости от версии используемого протокола. Но даже самые лучшие и самые высокие уровни безопасности являются квантововосприимчивыми. Уровень безопасности Bluetooth 2 поддерживает 128-битный ключ AES. Уровень 4, самый высокий уровень безопасности, поддерживает эллиптическая кривая Диффи–Хеллмана P-256. К сожалению, большинство пользователей Bluetooth понятия не имеют, какие версии или функции безопасности используются в их продуктах, применяющих Bluetooth. Для получения дополнительной информации о безопасности Bluetooth прочитайте https://en.wikipedia.org/wiki/Bluetooth#Security_concerns и https://duo.com/decipher/understanding-bluetooth-security.

С точки зрения безопасности NFC намного хуже. Ее создатели предполагали, что определяющей защитой NFC будет ее использование на коротких расстояниях. И это так. Но, как с любой беспроводной технологией, хакеры, вероятно, научатся взаимодействовать со своими беспроводными транзакциями на много порядков дальше, чем предполагали создатели. Большинство реализаций NFC не имеют безопасности за пределами расстояний, которые встроены в качестве средства беспроводной передачи в используемые NFC приложения. Те, в которых приняты некоторые меры для защиты передачи, часто используют шифры, расположенные в слабом конце шкалы безопасности, такие как AES-128 или квантововосприимчивые реализации криптографии с открытым ключом. Таким образом, NFC является квантововосприимчивой.

Примечание Радиочастотная идентификация (radio-frequency identification, RFID) является типом NFC. Хотя RFID часто используется в кредитных картах для беспроводных транзакций, она не имеет встроенной безопасности передачи. Любой, кто оказался на подходящем расстоянии от читателя, может прочитать то, что передается между двумя узлами. Вы можете легко найти видео по RFID-прослушиванию в интернете. Имея это в виду, тем не менее надо сказать, что риск RFID-преступности очень низок и постоянно снижается. Для получения дополнительной информации читайте мою статью на эту тему: www.csoonline.com/article/3243089/cyber-attacks-espionage/the-truthabout-rfid-credit-card-fraud.html.

IoT и аппаратные устройства

Большинство компонентов *интернета вещей* (Internet of Things, IoT) и другие вычислительные устройства (такие как телефоны, телевизоры, камеры и приборы) содержат квантововосприимчивые формы криптографии. Это создает для многих компонентов интернета и других основных аппаратных устройств риск выше среднего. Большинство потребителей не знают, в какой степени безопасны устройства, которые они используют, и им часто сложно обновить технику. Итак, когда-то криптопрорыв произойдет, и появятся, вероятно, миллиарды квантововосприимчивых IoT и аппаратных устройств, многие из которых будут находиться в наших домах.

Владельцы многих аппаратных устройств (например, проигрывателей Blu-ray, стереосистем и динамиков) не имеют возможности их обновить. А они, вероятно, уже сегодня имеют недостатки в части безопасности и многие уязвимости, которые проявятся в будущем и в принципе не могут быть устранены. Некоторые устройства содержат встроенные способы обновления, но по множеству причин многие владельцы устройств не обновят их. Многие владельцы просто не знают, что их устройствам может потребоваться обновление безопасности. Большинство потребителей никогда не заходят в консоль управления устройством после начальной установки, чтобы проверить, нужно ли применять патчи. Их устройства будут ждать проверки и применения новых патчей, но владельцы никогда не увидят соответствующих подсказок. Немало потребителей знают, что устройства, которые они покупают, впоследствии будут нуждаться в обновлении безопасности, но эти риски игнорируются и устройства не обновляются. Увы, такова печальная реальность.

Примечание Процент устройств, которые допускают возможность обновления и будут обновлены владельцами, значительно различается в зависимости от типа устройств. Вычислительные устройства и телефоны в этом плане занимают верхнюю строчку (предположительно обновятся 70 % и выше). Почти все прочие типы устройств довольно серьезно отстают по данному показателю. Для Wi-Fi роутеров и подключенных к интернету камер охранных устройств он составляет менее 10 %. Всего в 1 % существующих устройств проведены необходимые обновления. Мир был бы безопаснее, если бы каждое аппаратное устройство регулярно обновлялось автоматически без взаимодействия с владельцем.

Остерегайтесь пустых обещаний

Остерегайтесь заявлений от организаций, которые сообщают вам, что обновить текущие квантововосприимчивые стандарты и приложения в случае необходимости будет нетрудно. Я часто слышу такого рода заявления на форумах по криптовалюте и от поставщиков IoT. Несомненно, большинство сотрудников этих организаций никогда не участвовали в проведении крупных обновлений. И они заявляют подобное по неопытности. Они думают, что процесс обновления будет таким же простым, как предложение обнов-

ленного кода и массовый переход к нему. Они не совсем понимают, какие проблемы возникнут на практике:

- сколько пользователей даже не услышат о необходимости обновления;
- сколько пользователей используют старые, неподдерживаемые формы своего продукта;
- какова вероятность того, что их «тщательно протестированный» патч не будет корректно устанавливаться в некоторых пострадавших устройствах, даже когда пользователи пытаются делать правильные вещи;
- сколько владельцев их продуктов не могут сразу применить обновление, даже если это необходимо;
- насколько сложными будут обновления, а также какие препятствия возникнут просто в силу человеческой психологии.

Никто из тех, кто участвовал в предыдущем массовом обновлении, никогда не станет утверждать, что следующее пройдет гладко. Остерегайтесь тех, кто утверждает, что процесс обновления программного обеспечения до квантовой устойчивости будет легким. Одного такого заявления достаточно, чтобы понять, чего стоит «опыт» говорящего. Любой, кто прошел через масштабный проект модернизации, становится гораздо более осторожным и не ждет слишком многого. Обновление всегда сложнее, чем мы себе это представляем.

Большая часть нашего вычислительного мира и большинство наших интеллектуальных устройств содержат квантововосприимчивую криптографию. Становится все больше вычислительных устройств и сервисов, подверженных будущим квантовым атакам, по сравнению с теми, которые являются квантовоустойчивыми. Многие из них могут быть обновлены до квантовоустойчивых алгоритмов, когда придет время. Другие останутся навсегда квантововосприимчивыми. Глава 9 покажет вам, как вы и ваша организация должны подготовиться и спланировать свои действия в этом отношении.

Квантовые вычисления

Я не хочу, чтобы эта книга была пессимистичной. Хотя в центре внимания данной книги находятся создаваемые квантовыми вычислениями угрозы нашей компьютерной безопасности, квантовые вычисления дают нам гораздо больше возможностей, чем мы можем себе представить или чем были рассмотрены в главе 2. Вот некоторые более подробные прогнозы.

Квантовые компьютеры

У нас уже есть много десятков, если не более ста, квантовых компьютеров (по состоянию на 2019 год). Это число неуклонно растет даже притом, что квантовое превосходство пока не достигнуто. Когда же оно будет достигнуто, количество квантовых компьютеров возрастет в геометрической прогрессии. Каждая большая компания, которая сегодня зорко следит за событиями в ожидании квантового превосходства, купит такой компьютер. Нет ни од-

ной крупной компании, которая хочет, чтобы конкуренты превзошли ее по вычислительной мощности. Далеко не все хотят оставить у себя в распоряжении более медленные, «старые» компьютерные технологии. Даже компании и поставщики, которые не совсем понимают, что такое квант и какие выгоды он приносит, будут мечтать заполучить его. Это будет «модное словечко», которое будет с успехом использоваться в маркетинговых целях – точно так же, как в прежние времена облачные вычисления и искусственный интеллект.

Как описано в главе 2, существует более десятка основных типов квантовых компьютеров. Можно ожидать, что количество типов с течением времени будет уменьшаться, так как индустрия будет отбирать по преимуществу наиболее эффективные типы компьютеров. В начале эпохи бинарных персональных компьютеров (ПК) существовали десятки различных поставщиков ПК (среди них Apple, IBM, Altair, Micral, Wang, Tandy, Sinclair, Nippon Electric Company [NEC], Digital Equipment Corporation [DEC], Commodore и Sun), многие из которых включали персонализированные чипы самих поставщиков. В конце концов, компьютеры Apple, IBM-стиля и Linux стали доминирующими моделями (Sun Microsystems была также основным игроком на протяжении десятилетий). Такая же консолидация, вероятно, произойдет и с квантовыми компьютерами, когда они «повзрослеют».

Какие бы типы и поставщики ни выиграли, квантовые компьютеры, вероятно, станут через некоторое время и меньше, и дешевле. Средний ПК в 1980-х годах стоил несколько тысяч долларов, и покупатели отдавали их за монохромный экран, две дискеты, очень маленький жесткий диск (от 10 до 20 мегабайт) и менее 1 мегабайта оперативной памяти. Такие компьютеры часто весили от 15 до 30 фунтов, и рабочий стол, на котором они размещались, занимал большую часть комнаты. Ранние внешние жесткие диски весили более ста фунтов и были размером с картотеку. Сегодня вы можете найти десятки компьютеров за несколько сот долларов весом менее 2 фунтов с параметрами производительности, которые были бы приравнены к суперкомпьютерам в 1980-х гг.

Такое же изменение физических параметров и производительности произойдет, вероятно, в квантовом вычислительном поле. Люди преуспевают в том, чтобы делать вещи все более компактными. Ожидайте, что квантовые компьютеры станут быстрее, дешевле и в меньших форм-факторах. Одним из самых больших ограничений форм-фактора является необходимость охлаждать большинство квантовых компьютеров почти до 0 К. Следует ожидать уменьшения размеров даже такого переохлажденного квантового компьютера, хотя уже есть, по крайней мере, несколько конструкций квантовых компьютеров (таких как захваченные ионы), которые не нуждаются в столь низких температурах. Возможно, одна из этих моделей победит, позволяя форм-фактору квантовых компьютеров сразу резко уменьшиться. Еще неизвестно, могут ли квантовые компьютеры быть сокращены до используемых сегодня нами форм-факторов устройств (настольных компьютеров, ноутбуков, планшетных устройств и смартфонов). Но мы резко уменьшили размер и затраты почти на все вычислительные устройства, в то же время значительно снизив стоимость. Почему квантовые вычисления должны стать исключением?

Квантовые процессоры

У нас уже есть десятки различных типов квантовых процессоров. Количество типов, доступность по использованию и стоимости со временем будут увеличиваться. Многие модели прогнозирования указывают на идею квантового сопроцессора. Еще в первые годы существования ПК большинство компьютеров можно было обновить, добавив отдельный математический «сопроцессор», чип в слот на материнской плате. Математический сопроцессор был специально создан, чтобы делать сложные математические расчеты быстрее, чем обычный процессор ПК. Можно возложить на сопроцессор программы, требующие использования плавающей точки, сложные расчеты, «отделив» такую математику, а затем передать результат на главный процессор, чтобы программа могла завершиться быстрее, чем это было бы без использования математического сопроцессора.

Тесты производительности обычно показывают, что компьютеры, использующие математические сопроцессоры, значительно превосходят компьютеры без таковых. Довольно скоро потребители стали настаивать на том, чтобы на любой компьютер, который они покупают, можно было по выбору установить «дополнительный» математический сопроцессор. Маркетинговые перспективы быстро вывели его из разряда «дополнений». Спрос на математические сопроцессоры был настолько велик, что со временем основные производители процессоров ПК просто добавили сложные математические процедуры в обычные процессоры. Примерно в то же время компания Intel представила свою линейку 486-х процессоров, и идея необходимости отдельного математического сопроцессора умерла естественной смертью. Сегодня каждый, кто покупает компьютер, получает его со встроенными компонентами для математических расчетов.

Многие специалисты по квантовым компьютерам ожидают, что то же самое произойдет с квантовыми компьютерами. В будущем, скорее всего, большинство компьютерных приложений не потребуют квантовых вычислений для выполнения всей работы. Квантовые эксперты ожидают, что какое-то время квантовые сопроцессоры будут иметь спрос. Наши компьютеры будут выполнять обычные (например, двоичные) вычисления, необходимые для большинства функций, и загрузят сложные квантовые вычисления в квантовый сопроцессор. Квантовый сопроцессор будет принимать входные данные от основного процессора компьютера, выполнять свое квантовое волшебство, а затем расшифрует результат и передаст его главному процессору компьютера. Потом закончится время концепции отдельного квантового сопроцессора, и он может исчезнуть, как это когда-то произошло с математическими сопроцессорами бинарных компьютеров. Многие квантовые эксперты уже видят тот день, когда на каждом рабочем столе и в каждом устройстве будет квантовый компьютер, хотя это случится, вероятно, через десять лет или много десятилетий.

Квантовые облачные вычисления

Уже существует около десятка квантовых облаков, ряд которых доступен для публичного (бесплатного) использования. Ожидается, что когда наступит квантовое превосходство, количество свободных и коммерческих квантовых облаков будет увеличиваться в геометрической прогрессии. Квантовое облако, вероятно, будет использоваться как «виртуальный квантовый сопроцессор», когда любые трудные квантовые вычисления отключены от процессора основного компьютера, и получает кванты после завершения вычислений в облаке. Эта модель имеет большой смысл, особенно на ранней стадии, когда квантовые компьютеры дороги и требуют существенного контроля окружающей среды (скажем, поддержки температуры около 0 К).

Возможно, среднесрочной моделью для квантовых вычислений является большинство традиционных компьютеров, связанных (программно) с облачными квантовыми компьютерами, благодаря чему квантовые вычисления станут экономически более эффективными для тех, кто не может позволить себе собственные квантовые компьютеры. Даже организации, нуждающиеся в большом количестве квантовых компьютеров, могут, по мере необходимости, пользоваться облаками, когда им не хватает своих собственных квантовых ресурсов. В любом случае и квантовые компьютеры, и облака останутся с нами и будут доступны каждому долгое время.

Будет использоваться квантовая криптография

Широкомасштабная реализация квантовых компьютеров принесет много новых квантовостойких криптографических алгоритмов, а также криптографических алгоритмов, основанных на квантовых свойствах. Организации перейдут на квантовостойкие и квантовоориентированные алгоритмы в течение следующей половины десятилетия. Квантовоустойчивые алгоритмы будут подробно рассмотрены в главе 6, а квантовые шифры и устройства – в главах 7 и 8.

Квантовая идеальная конфиденциальность

Одна из особенностей квантовой криптографии состоит в том, что квантовая криптография позволяет создавать системы с более полным гомоморфным шифрованием (fully homomorphic encryption, FHE) (https://en.wikipedia.org/wiki/Homomorphic_encryption), которые обещают идеальную конфиденциальность. Суть идеи FHE в том, что организация может отправить зашифрованный контент третьей стороне и позволить сторонним системам целенаправленно манипулировать зашифрованным контентом каким-либо разрешенным и предполагаемым образом, без дешифровки текста третьей стороной.

В качестве простого примера предположим, что компания хочет отправить большой набор отчетов о продажах в центр очистки данных для поиска

и удаления дубликатов и других типов недействительных записей. Это то, что регулярно делают многие организации с десятками тысяч продаж. Сегодня, даже если исходная организация отвечает всем требованиям по безопасности и все записи были зашифрованы, ей может потребоваться на каком-то этапе расшифровать их (или совместно использовать ключ дешифрования), чтобы процессор мог осуществить поиск данных и удаление соответствующих записей.

В идеальной системе конфиденциальности записи могут оставаться зашифрованными и успешно обрабатываться основным процессором очистки без раскрытия текста или передачи оригинального шифра ключей. Еще один хороший пример использования в будущем гомоморфных криптосистем – предоставление медицинских данных, возможно в глобальном масштабе, всем, кто проводит исследования (например, Google занимается краудсорсингом медицинской информации для решения проблем лечения существующих сложных болезней), без предоставления исследователям какой-либо информации о личных данных.

Большинство гомоморфных криптосистем включают дополнительный алгоритм оценки, криптографически связанный с оригинальным шифром, который может использоваться процессором третьей стороны. Гомоморфные криптосистемы позволят совершать необходимые транзакции, не раскрывая личной информации. Это будет лучше защищать оригинальную хост-компанию, компанию обработки данных и клиентов от несанкционированных утечек данных.

Гомоморфные криптосистемы были постулированы и стали создаваться сразу после изобретения открытого криптоключа в конце 1970-х годов с разными результатами. Большинство попыток привели к получению промежуточных решений, которые не могут быть использованы во всех ситуациях и известны как *частично гомоморфные* (partially homomorphic). Существует около десятка систем FHE, предложенных в доквантовом мире, но они были больше теоретическими, чем практическими. Квантовые вычисления и особенно квантовое свойство запутанности обещает дать больше, лучше практически реализуемых решений. Квантовая запутанность является ключевым компонентом, которого ждал FHE. Насчитывается достаточно много квантовых криптографов во всем мире, которые сосредоточены исключительно на этой проблеме, используя то, что они называют *квантовым гомоморфным шифрованием* (quantum homomorphic encryption, QHE). Главным результатом QHE, вероятно, будет меньшее количество искажений данных. Трудно предположить, что произойдет утечка ваших данных, если они принципиально не могут быть расшифрованы.

Появляется квантовая сеть

Прямо сейчас зарождается индустрия квантовых сетей. Продавцы тестируют и успешно производят устройства первого поколения. Квантовая сеть имеет большой потенциал из-за ее способности использоваться на больших расстояниях с высокой степенью конфиденциальности. Квантовые свойства

осложняют попытки со стороны неавторизованного субъекта подслушивать защищенный сетевой поток данных без предупреждения уполномоченных заинтересованных сторон. Ожидайте увидеть квантовые сети, используемые в сетях с высоким уровнем безопасности и последующим более общим применением в обычных условиях конфиденциальности. Квантовая сеть подробно обсуждается в главе 8 «Квантовые сети».

Широкая доступность квантовых вычислений и криптографии угрожает существующей квантововосприимчивой криптографии или разрушает ее и означает начало новой эры квантовой защиты, которая обеспечивает большую безопасность.

Квантовые приложения

Помимо квантовой криптографии, квантовые компьютеры готовы к созданию совершенно новых отраслей индустрии и радикальной трансформации существующих технологий. Приложения, которые могут извлечь пользу при использовании квантовых свойств и алгоритмов, таких как алгоритм Гровера, запутывание и суперпозиция, будут усилены квантовыми вычислениями. Есть тысячи компьютерных проблем, которые сегодня не имеют ответа или не могут быть оптимизированы, потому что классические компьютеры не имеют необходимой производительности для ответа на них. Приведу некоторые из тех приложений, которые будут улучшены квантовыми вычислениями.

Улучшение химикатов и лекарств

Первое место в списке квантовых достижений занимает улучшение химических веществ и лекарств. И это одна из основных причин разработки квантовых компьютеров. Мы знаем, что атомы состоят из электронов, протонов и нейтронов. И протоны, и нейтроны состоят из других элементарных частиц, называемых кварками. Все работает и реагирует на квантовом уровне. Отдельные элементарные атомы часто химически связаны с другими атомами того же типа или разных типов и формируют молекулы. Например, два атома водорода соединяются с одним атомом кислорода, образуя H_2O, или воду.

Почти вся материя, с которой мы ежедневно взаимодействуем каждую секунду, состоит из молекул. Часто эти молекулы насчитывают от сотен до сотен миллиардов атомов и химических связей. Каждая связь может взаимодействовать с другими атомами и молекулами множеством способов. Понимание и прогнозирование взаимодействия атомов и молекул являются краеугольным камнем химических и медицинских исследований. Чем лучше химия и медицина могут предсказать реакции на молекулярном уровне, тем лучше могут стать результирующие химические вещества и лекарственные соединения.

Традиционные классические компьютеры могут правильно отслеживать лишь небольшое количество молекулярных связей, прежде чем начнут терять

информацию и соответствующие возможности прогнозирования. Поскольку большинство молекул, которые делают нашу жизнь лучше, содержат большое количество связей, наше текущее понимание и способность улучшать свойства химических веществ и лекарств ограничены. Квантовые вычисления позволят нам не только отслеживать, понимать и прогнозировать значительно больше молекулярных взаимодействий, но и делать это на квантовом уровне (что гораздо проще, когда мы используем квантовое моделирование, а не классические компьютеры) и в другом временном масштабе. Это приведет к улучшению химических веществ и лекарств. Вполне вероятно, что квантовые компьютеры позволят нам иметь лучшие лекарства, которые имеют меньше побочных эффектов и настроены для работы с нашей конкретной медицинской структурой или структурой ДНК (то есть биомедицинские препараты).

Квантовые эффекты уже используются в некоторых лучших диагностических медицинских устройствах, таких как получение изображений методом ядерного магнитного резонанса (magnetic resonance imaging, MRI), и это, вероятно, позволит нам раньше диагностировать плохие генетические признаки и лучше выявлять заболевания. Существует большая вероятность, что мы сможем лучше понять, как работают человеческая память и сознание, как они ослабевают и как смягчить связанные с этим проблемы. Прикладные методы лечения, такие как лучевая терапия, могут стать более целенаправленными и менее продолжительными. Также можно станет точнее предсказывать вредные побочные эффекты лекарственного взаимодействия. В целом квантовые вычисления, вероятно, приведут к значительному улучшению используемых химикатов и лекарств, что принесет пользу человечеству. Если вы слышали избитую сентенцию «Химия позволяет лучше жить», не сомневайтесь: квантовые вычисления и в этом сыграют свою роль.

Лучшие аккумуляторы электроэнергии

Наука об энергии, хранящейся в батареях, не демонстрирует особого прогресса в течение десятилетий. Время автономной работы вашего ноутбука и мобильного телефона все еще довольно быстро уменьшается. Некоторые улучшения в этом плане порой наблюдаются, но они скорее обусловлены снижением энергопотребления устройства, чем совершенствованием аккумуляторных батарей. При этом использование батарей дорого обходится человечеству – они вызывают пожары и содержат опасные химические вещества. В электромобилях батарея является самым тяжелым и самым дорогим компонентом и тем самым существенно снижает преимущества электромобиля. Сотни компаний работают над тем, чтобы повысить эффективность и время работы батарей и уменьшить их вес.

Для этой цели многие автомобильные компании и производители аккумуляторов уже используют квантовые компьютеры, чтобы лучше понять механизм работы батарей на молекулярном уровне, в частности как работают и истощаются литий-водородные и углеродные молекулярные цепи (см. примеры в статье: https://insideevs.com/news/338440/volkswagen-turns-to-quantum-computing-for-electric-car-batteries/). Другие исследователи используют

квантовую запутанность, чтобы создать батареи с более быстрой зарядкой (www.extremetech.com/extreme/211580-quantum-batteries-could-allow-for-super-fast-chargingthanks-to-entanglement). Вполне вероятно, что квантовые вычисления будут играть ключевую роль в поиске новых химических взаимодействий молекул, которые будут хранить больше энергии в меньших пространствах, что принесет ощутимую пользу при применении электробатарей на практике.

Настоящий искусственный интеллект

Одно из наиболее часто используемых в компьютерном мире понятий – искусственный интеллект (и связанная с ним область машинного обучения). Концепция искусственного интеллекта (AI) заключается в таком программировании компьютеров, при котором они смогут, подобно человеку, стать самообучающимися, не утратив при этом своего главного преимущества – решать проблемы со скоростью, на которую люди не способны. Искусственный интеллект – это святой Грааль компьютеров. Существует много споров о том, является ли сверхсложная мысль человека процессом, который может когда-либо быть смоделирован на компьютере.

Сегодня мы не близки к настоящему искусственному интеллекту, хотя это не тысячи поставщиков компьютеров берутся утверждать, что получили его на некотором уровне. Квантовые вычисления, которые более точно предсказывают поведение всей материи на квантовом уровне, возможно, смогут сказать свое слово, приблизив нас к подлинному AI. Предполагается, что более совершенный искусственный интеллект улучшит наш мир во многих отношениях, как это сделает и квантовый мир (без AI). Правда, искусственный интеллект, при котором компьютер переймет всю сложность человеческого мозга, должно быть, полностью изменит правила игры. Предположительно почти все, что мы делаем, будет улучшено и оптимизировано. Один из наиболее часто упоминаемых примеров – автономное вождение транспортных средств. Автомобили уже смогут управлять сами собой. Вероятно, уже менее 10 лет отделяет нас от того момента, когда автономных транспортных средств станет больше, чем управляемых человеком. Наши дети и уж наверняка внуки не будут иметь водительских прав или собственных автомобилей. Людям будет достаточно брать напрокат автомобили, когда они им нужны, чтобы ехать на работу, выполнять поручения и путешествовать.

Квантовые вычисления, вероятно, помогут улучшить управление движением автономных автомобилей. Квантовые компьютеры смогут учитывать все задействованные автономные автомобили, их позиции, скорость и определять, как изменить их скорости и повороты, чтобы оптимизировать скорость и направление движения всех автомобилей вместе взятых. Цель состоит в том, чтобы ни одно автономное транспортное средство в принципе не останавливалось на перекрестке. Компьютеры будут изменять скорость и траекторию движения транспорта так, что он сможет просто продолжать движение через перекрестки, не останавливаясь на светофорах, которые в связи с этим уйдут в прошлое. Это сэкономит энергию, уменьшит загрязнение атмосферы и сэкономит время тем, кто в пути.

Искусственный интеллект также сильно повлияет на кибербезопасность. Уже появились ранние реализации машинного обучения, используемые, чтобы учесть новые ходы злоумышленников и выработать соответствующие методы защиты. Будущее компьютерной безопасности, скорее всего, будет зависеть от автономной безопасности обучения с помощью AI и атак ботов, которые атакуют и от которых защищаются на основе продвинутых алгоритмов. Я не уверен, что мы когда-нибудь увидим Скайнета, главного антагониста человечества из фильма «Терминатор», киборга, который нападает на своих создателей-людей, но многие незаурядные исследователи обеспокоены этим сценарием, в их числе Илон Маск (www.theguardian.com/technology/2014/oct/27/elon-musk-artificial-intelligence-ai-biggest-existential-threat). Чем бы ни обернулся искусственный интеллект, квант, скорее всего, будет идти с ним рука об руку.

Управление цепочками поставок

Компании давно хотели оптимизировать цепочки поставок и получать товары именно тогда, когда они нужны – не раньше и, конечно, не позже, чем того требует бизнес. Затаривание – это просто потраченные впустую деньги, пространство и другие ресурсы. Сегодня у нас есть много компаний, которые, кажется, приближаются к идеальному управлению цепочками поставок, в том числе Amazon, FedEx и United States Postal Service (Государственная почтовая служба США). Каждый ритейлер следует за своим лидером, пытаясь оптимизировать и обезопасить свои цепочки поставок. Даже те, кто не торгует в розницу, стараются отладить сбор и дистрибуцию. Например, управление энергосетями следующего поколения является ключевым фактором, влияющим на сокращение энергопотерь, снижение затрат, предотвращение сбоев и рост удовлетворенности потребителей. Многие из крупнейших в мире ритейлеров и энергетических компаний инвестируют в квантовые вычисления именно для этой цели.

Квантовые финансы

Само собой разумеется, если кто-то сможет добиться успеха в квантовых вычислениях, он это сделает. Предполагается, что квантовые вычисления позволят инвесторам лучше управлять своими инвестиционными портфелями и лучше понять множество факторов, которые влияют на финансирование. Это затронет торговлю акциями, создаст новые производные торговые мощности, улучшит рыночные прогнозы, торговлю сырьевыми товарами и всем прочим, чем сегодня торгуют в мире. Как и прогнозирование кибербезопасности, многое из этого будет сделано с помощью автоматизированных алгоритмических ботов, пытающихся найти пути получения технического преимущества, которое ботами другой компании еще не найдено. У нас есть предвестники такой автоматизированной *высокочастотной торговли*, которая составляет до 40 % от всей торговли акциями. Квантовые вычисления только ускорят эти тенденции. Уже существует ориентированный на кванты финансовый веб-сайт под названием Quantum for Quants (http://www.quantumforquants.org/).

Улучшенное управление рисками

Финансовые инвестиции – это управление рисками портфеля, во что и когда инвестировать. Квантовые компьютеры улучшат расчеты управления рисками для всех отраслей. Они помогут отрасли страхования лучше определять страховые шансы, выявлять больше случаев мошенничества и снизят количество фальшивых сделок. Защитникам компьютерной безопасности новые технологии позволят лучше определить, на чем следует сосредоточиться. Решение проблем управления рисками похоже на перемещение фигур на шахматной доске, и квантовые компьютеры хороши в решении сложных проблем со множеством факторов.

Квантовый маркетинг

Многие из лучших технологических изобретений нашего времени были в значительной степени стимулированы и финансировались за счет рекламы и маркетинга. Радио, телевидение и кабельное телевидение были созданы рекламой. Интернет повысил ставки рекламной игры и позволяет рекламодателям выходить с продажами на группы людей, которые с большей вероятностью купят конкретный продукт. Давно уже шутят, что Google знает о вас больше, чем ваш(а) супруг(а), и даже в курсе того, что вы сами хотели бы знать о себе. Интернет знает все. Квантовые вычисления обеспечат направленный маркетинг даже с небольшими подгруппами людей и позволят лучше понять сложную логику, казалось бы, несвязанного выбора потребителей. Вот, например: говорят, что любители собак покупают больше спагетти, и поэтому тому, кто покупает продукты для собак, может быть предложен купон на новый соус для спагетти. Так же, как квантовые вычисления помогут нам получить лучшее представление о взаимодействии молекул, квантовые вычислительные мощности будут использоваться для улучшения качества маркетинга. Я не уверен в том, как оценивать подобное влияние – как полезное или как вредное.

Более точный прогноз погоды

Инновации в метеорологии – еще одна причина для раннего финансирования квантовых вычислений, поскольку они дают возможность более точно прогнозировать влияющую на все в этом мире погоду. Это не только поможет защитить людей от суровых погодных условий, но и улучшит предсказания ее критичности, повысит вероятность прогноза, в том числе долгосрочного. Это поможет фермерам определить, что сажать и когда. Можно будет контролировать и смягчать последствия изменения климата за счет лучшего представления о глобальной климатической среде, ее изменении и влиянии на людей.

Квантовые деньги

Квантовые деньги – это, по сути, криптовалюта с основанной на квантах защитой и функцией антиподделки, которые делают необычными традиционные блокчейны. Было несколько предложений системы квантовых денег, в

том числе давних (примерно 40-летней давности), в которых показывалось, что защитные квантовые свойства могут быть использованы для создания универсальной, не поддающейся обработке, не подлежащей краже криптовалюты. Было предложено несколько типов квантовой валюты, использующих различные теоретические обоснования, но большинство из них основывается на концепции уникального серийного номера, имеющего встроенные неразделенные квантовые свойства, которые знал бы только центральный банк. Таким образом, преступники могут создать новую дубликатную версию валюты, используя те же серийные номера, но поскольку они не будут знать состояния дополнительных встроенных квантовых свойств, они не смогут создать идеально дублированную валюту, которая прошла бы процесс банковской проверки. Для получения дополнительной информации посетите https://futurism.com/the-byte/virtual-money-quantum-galactic-commercehttps://en.wikipedia.org/wiki/Quantum_moneywww.scottaaronson.com/papers/noclone-ccc.pdf. Конечно, современные криптовалютные системы могли бы использовать квантовоустойчивые шифры вместо квантововосприимчивых шифров и также считаться «квантовыми деньгами». Использование криптовалюты на квантовой основе, которая применяет распределенный (а иногда и анонимный) блокчейн вместо централизованного верификатора, считается многими пользователями криптовалюты ключевым требованием. С квантом можно выбрать любую из систем, которая лучше всего подходит для вас и ваших целей.

Квантовое моделирование

Использование компьютеров на основе квантовых свойств позволит нам намного лучше исследовать нашу среду обитания. Мы не только сможем определить «как» и «почему» квантовой механики, но будем в состоянии выяснить все квантовые взаимодействия всех вещей, которые не обязательно связываем с квантовой механикой, однако полагаемся на них. Квантовые компьютеры, скорее всего, помогут нам ответить на многие трудные вопросы физики, стоящие сегодня перед нами, например: сколько измерений имеет физическая Вселенная и что такое темная материя. Квантовые вычисления позволят нам понять окружающий мир (или даже многие миры), что невозможно сделать с помощью классических компьютеров.

Более совершенное вооружение и точное оружие

Само собой разумеется, что многое из того, что мы изобретем и улучшим, используя квантовые компьютеры, окажется востребовано вооруженными силами разных стран. Такова судьба многих технологий. Именно из военной отрасли пришел к нам, кстати, интернет. И даже такие простые и безобидные вещи, как повышение точности прогноза погоды, будут использоваться при планировании боевых действий. Увы, это просто данность.

Квантовая телепортация

Вероятно, одним из наиболее обсуждаемых и интересных квантовых изобретений является квантовая телепортация. Используя квантовую теле-

портацию, можно точно воссоздать объект (или его состояние (состояния)) в другом (получаемом) месте, независимо от того, как далеко друг от друга они находятся.

Многие люди, включая автора, начали дискуссию о квантовой телепортации, бесхитростно ссылаясь на научно-фантастический телесериал и киносериал Star Trek и его идею «транспортера» (https://en.wikipedia.org/wiki/Transporter_%28Star_Trek%29). Эта аналогия просто позволяет быстро объяснить общую концепцию телепортации, хотя квантовая телепортация больше сродни копированию или факсу, чем собственно телепортации. Многих физиков удручало использование слова *телепортация*, потому что люди под ним часто понимают нечто совершенно другое.

Существует несколько ключевых различий между вымышленным «телепортером» из Star Trek и квантовой телепортацией. Во-первых, телепортер Star Trek сам отправляет частицы объекта между двумя точками, тогда как квантовая телепортация посылает только информацию о частицах объекта (чтобы им можно было подражать), а не сами частицы. Во-вторых, и это самое главное, квантовая телепортация на самом деле работает, хотя пока она не перемещала объекты крупнее макромолекулы.

Примечание Способность телепортера Star Trek беспрепятственно перемещать в пространстве человека – это нечто, что, вероятно, еще долго будет за пределами наших реальных возможностей. Чтобы телепортировать человека, используя либо функциональный транспортер, либо реальную квантовую телепортацию, потребуется понимание, выявление и кодирование каждой йоты того, что означает быть человеком, – не только каждой клетки, свойств атома и кварка, но всего, что включает представление об активной памяти и сознании (и о подсознании, и о поведении). Мы даже не уверены, что это можно сделать, используя любое известное физическое представление. Количество частиц и состояний, которые должны быть переданы, превысит количество всех звезд в известной Вселенной.

Протокол телепортации

Теория квантовой телепортации была разработана еще в начале 1990-х, а в последнее время была успешно продемонстрирована в десятках экспериментов (с использованием фотонов, атомов и молекул) в лабораториях и между Землей и космосом (с использованием квантовых спутников). Есть много практических трудностей в создании простого устройства передачи частиц, такого как вымышленный телепортер Star Trek, в том числе теорема об отсутствии клонирования, которая препятствует прямому копированию квантовых частиц. Из-за этого квантовые телепортеры для достижения реального мира телепортации используют метод косвенной логики, представленный проверенным протоколом. Но важно полностью понять, как работает квантовая телепортация, потому что это следствие многих грядущих квантовых разработок и устройств и того, как будет работать квантовая сеть устройства. Они у нас уже есть сегодня, о чем мы подробнее поговорим в главе 8. Так что все это не только для любителей научной фантастики, и это будет ра-

ботать в не слишком отдаленном будущем. Квантовая телепортация требует как минимум пяти вещей: телепортируемый объект, два запутанных кубита, два двоичных бита для каждого кубита информации об объекте, который вы хотите телепортировать. Упрощенная версия протокола телепортации выглядит следующим образом (в графическом представлении см. рис. 5.4):

1. Создайте два спутанных кубита (A и B) для каждого кубита информации об объекте, необходимой для телепортирования (X1). Спутанность имеет решающее значение, потому что нам нужны оба кубита, чтобы оставаться в состоянии синхронизации до окончательного изменения состояния.
2. Транспортируйте одну сторону запутанных кубитов в место, куда должен быть телепортирован объект (то есть отправляющая станция).
3. Переместите другую сторону запутанных кубитов в место получения (так, как вы хотите достичь этого).
4. На отправляющей станции разрешите состоянию кубита (кубитов) объекта и передающей стороны запутанного кубита взаимодействовать друг с другом, наблюдайте и записывайте разницу между состояниями свойств объекта кубита и текущим состоянием запутанного кубита. Разница может быть точно представлена одним из четырех возможных ответов (с учетом двух кубитов, сравниваемых друг с другом), скажем 1, 2, 3 или 4.
5. Используйте две двоичные цифры (т. е. $2^2 = 4$), чтобы представить ответ о разнице при сравнении.
6. Передайте разностный ответ, представленный двоичными цифрами, используя любые классические средства, к месту назначения. Вы можете применить любой способ связи, чтобы сообщить разницу ответов, в том числе написание или вызов, но самым быстрым способом, скорее всего, будет передача цифрового бита некоторого типа.
7. Используйте полученную двоичную ответную информацию о разнице ответов, чтобы изменить целевой кубит так, чтобы это точно отражало кубит (состояние) исходного объекта, измеренного на шаге 4.
8. Повторите при необходимости, чтобы правильно воссоздать объект (X2) кубитом в целевом кубите.

Теперь о негативе. Акт телепортации разрушает изначальную запутанность и оригинальный объект (или он может даже быть уничтожен по этическим причинам). Например, предположим, вы телепортируете живого человека. Теперь у вас есть идентичная копия человека, с теми же мыслями и воспоминаниями, в двух разных местах. Каждый из них думает, что он настоящая, «оригинальная» личность. Одна из этих копий должна быть уничтожена, иначе могут начаться проблемы самого разного рода. Например, обе копии будут думать, что у них один и тот же партнер, одни и те же родители, одно и то же рабочее место и т. д. Хотели бы вы испытать на себе квантовую телепортацию, не исключая того, что вы будете уничтожены, в то время как ваш двойник заживет полной жизнью (во всяком случае до следующей телепортации)? К счастью, такого рода этические проблемы нас не мучат, когда мы пытаемся просто телепортировать обычные цифровые данные, для чего

квантовая телепортация и будет использоваться в подавляющем большинстве случаев.

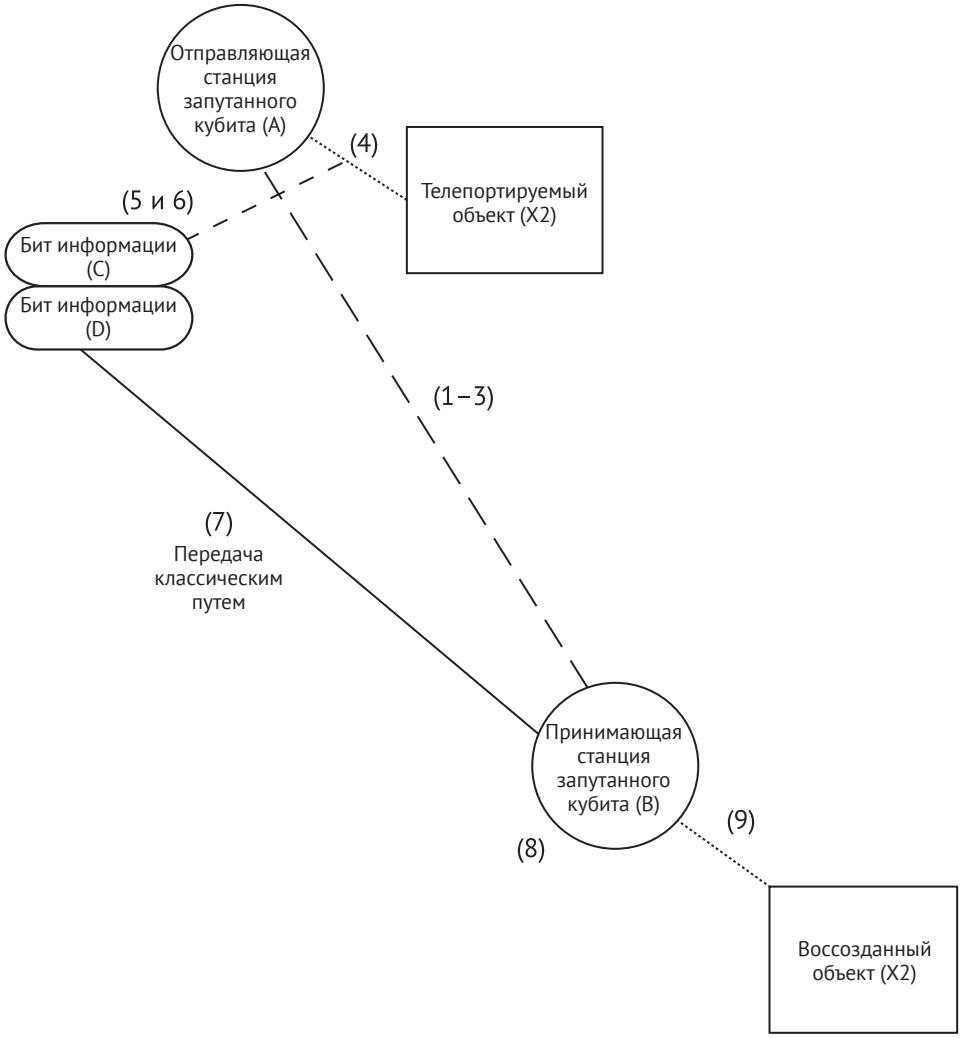


Рис. 5.4. Базовые объекты и этапы квантовой телепортации

Примечание Телепортации в кино- и телеверсии Star Trek показаны как медленное рассеяние мельчайших частиц на месте только что телепортированного человека. Что здесь не показано, так это процесс уничтожения «оригинальной копии». Убийство представлено этаким приятным и красочным действием.

Если вы хотите узнать больше о квантовой телепортации, посетите веб-сайты:

- https://en.wikipedia.org/wiki/Quantum_teleportation;
- www.youtube.com/watch?v=Czi5elPLfvA;
- www.youtube.com/watch?v=hTe2PYwnEpc;
- www.scottaaronson.com/qclec/10.pdf.

Следует отметить, что квантовая телепортация не является каким-то абсолютно уникальным методом телепортации объектов. Мы уже делаем нечто подобное, используя традиционные технологии. Мы часто кодируем информацию об объектах, а затем отправляем эту информацию по месту назначения, где оригинал объекта воссоздается. Передача по факсу, копирование, сканирование, отправка файлов по интернету – классические примеры. Квантовая телепортация – это способ обеспечить правильное получение битов информации на квантовом уровне, корректно передаваемая и/или сверхбезопасная передача битов. Неквантовая телепортация будет испытывать трудности при передаче информации на квантовом уровне.

Еще одно важное предупреждение о квантовой телепортации. В связи с тем, что люди часто опираются в своих ложных представлениях на научную фантастику, они воображают, что перемещение предметов и людей на большие расстояния, даже в галактики, возможно в мгновение ока. Этап № 6 квантовой телепортации (см. рис. 5.4) требует классической передачи информации, и это означает, что телепортация со скоростью быстрее скорости света невозможна. Это не должно удивлять. Ничего нельзя передать со скоростью, превышающей скорость света (хотя нам еще предстоит выяснить, как выглядит квантовая запутанность, чтобы сделать это), но транспортировка разностной информации должна быть выполнена классическим способом. Это не страшно. Многие классические методы, даже те, которые использует простое электричество, приближаются к скорости света, поэтому их привлечение означает, что все это можно сделать очень быстро. Просто не быстрее скорости света.

Если все эти разговоры о квантовых изобретениях и усовершенствованиях кажутся вам в некоторой степени «пустыми посулами» и вы относитесь к ним скептически, подумайте о том, как бинарные компьютеры и запоминающие устройства изменили наш мир в течение нескольких десятилетий. Прежде компьютеры были огромными и занимали целые этажи. Доступ к таким машинам имели военные, а также крупнейшие корпорации. Компьютер в наши дни стал вездесущим, довольно дешевым и очень маленьким. Сегодня мы носим электронные устройства на запястье и имеем больше вычислительной мощности в наших смартфонах, чем суперкомпьютер Cray имел всего несколько десятилетий назад. Устройство размером с кончик пальца может сохранить в памяти все созданные нами документы вместе со всей нашей музыкальной коллекцией. Вы можете доказать какой-либо факт или узнать о чем-либо в течение нескольких секунд. Вы можете посмотреть видео о том, как выполнить ту или иную работу почти на профессиональном уровне. Новости облетают мир за секунды. Квантовые компьютеры готовы показать, что принесет нам следующее поколение фантастических изобретений и усовершенствований. И это, несомненно, будет поразительным.

Резюме

Квантовые компьютеры и свойства ослабят или сломают большинство традиционных криптокодов, включая хеши, симметричные ключи и асимметричные шифры. В некоторых случаях использование более длинных ключей может стать квантовоустойчивым ответом. В других случаях будет приемлемой только полная замена квантововосприимчивого шифра на квантовоустойчивые или квантовобезопасные шифры. В ближайшие несколько лет мы все перейдем на более квантовоустойчивую криптографию. Квантовые вычисления также принесут новую, лучшую криптографию, создание сетей, идеальную конфиденциальность и много новых или улучшенных приложений. У нас будут более совершенные химикаты, лекарства, батареи, прогнозы погоды и вооружение. Каждый квантовый скачок в технологии принесет как хорошее, так и плохое. В этом квантовые вычисления ничем не отличаются от прочих изобретений. Добро пожаловать в постквантовый мир! В главе 6 «Квантовоустойчивая криптография» обсуждаются десятки квантовоустойчивых шифров; некоторые из них вы должны будете скоро использовать в приложениях вашей организации.

II Подготовка к квантовому взрыву

6 Квантовоустойчивая криптография

Криптография, которую мы будем использовать в постквантовом мире, представляет собой комбинацию квантовоустойчивой, основанной на квантах криптографии. Квантовоустойчивая криптография представляет собой традиционные, бинарные криптографические алгоритмы, устойчивые к известным квантовым атакам. Квантовый криптографический алгоритм – это криптография, которая использует квантовые вычисления и квантовые свойства для защиты информации. Эта глава посвящена квантовоустойчивой криптографии, а глава 7 – квантовой криптографии.

Данная глава полна криптографического технического и продвинутого математического жаргона. Постоянные читатели текстов по компьютерной безопасности могут задаться вопросом, почему им должны быть интересны конкретные алгоритмы во всех технических деталях. Они могут полагать, что все, что им действительно нужно знать, чтобы выполнять свою работу, – это названия постквантовых алгоритмов... и не исключено, что это правда.

Но для любого, кто связан с реализацией криптографии, основы криптографии, видимо, чрезвычайно полезны. В этой главе дается общий обзор более двух десятков квантовоустойчивых алгоритмов – вы можете понять их так же, как вы, вероятно, уже поняли, почему большие простые числа дают шифрам RSA и Диффи–Хеллмана присущую им защиту и как эта зависимость от простых чисел делает их восприимчивыми к квантовым атакам. Большее знание, чем название криптографического алгоритма, может помочь тогда, когда кто-то, конечный пользователь или начальник, задает конкретные вопросы о ваших планах создать конкретную постквантовую реализацию. Кроме того, вы будете более уверены в себе, обсуждая постквантовый план со своими коллегами. Вам не нужно разбираться в каждой детали конкретного алгоритма, но это помогает понять идею того, как это работает.

Постквантовый конкурс NIST

Существует несколько десятков квантовоустойчивых шифров и цифровых подписей, большинство из которых на протяжении многих лет получило оценку различных криптографических экспертов и групп по всему миру. В 2015 году Европейский институт телекоммуникационных стандартов (European Telecommunications Standards Institute, ETSI) вместе с учеными и исследователями во всем мире был первым крупным публичным сообществом, которое стало серьезно исследовать квантовоустойчивые шифры.

Затем последовали многие другие группы в других странах, включая Соединенные Штаты.

Национальный институт стандартов и технологий США (The U. S. National Institute of Standards and Technology, NIST; см. www.nist.gov) в течение многих лет проводил публичные «соревновательные» конкурсы для оценки способности различной предлагаемой криптографии заменить слабеющую существующую криптографию. Алгоритмы победителей становились в США новыми криптографическими стандартами, и их создатели соглашались разрешить их использование без роялти.

На предыдущем конкурсе NIST при активном участии Агентства национальной безопасности США (NSA) были выбраны SHA-3 в качестве нового стандарта хеширования и AES в качестве нового симметричного ключа стандартного шифрования. В целом эти предыдущие публичные криптографические конкурсы расценивались как огромный успех. Кроме того что многие квалифицированные кандидаты получили публичную оценку, большинство людей считали конкурсы полезными и победы в конкурсах заслуженными (хотя это имело место не с каждой криптографической оценкой NIST/NSA; см. врезку «Сомнительные конкурсы NIST/NSA»).

СОМНИТЕЛЬНЫЕ КОНКУРСЫ NIST/NSA

Несмотря на то что конкурсы NIST/NSA сегодня являются относительно доверительными для большинства заинтересованных сторон, известны по меньшей мере два случая в прошлом, когда NSA, по-видимому, активно ослабляло стандарты криптографии, с тем чтобы облегчить себе их нарушение. Впервые это было проделано десятилетия назад при выборе симметричного шифра стандарта шифрования данных (Data Encryption Standard, DES) в 1977 году. NSA убедило компанию IBM (создателя DES, тогда известного как шифр Люцифера) сократить предлагаемую длину защитного ключа от 64 до 56 бит, были попытки сократить его до 48 бит. IBM пошла на компромисс, сделав DES использующим 64-битный ключ, но большая часть защиты реально была в первых 56 битах. В 2006 году NSA вновь вызвало критику, когда потребовало от всех производителей компьютеров (которые продаются правительству США, обычно крупнейшему покупателю компьютеров) включить новый, ультрауязвимый генератор случайных чисел (RNG), известный как Dual_EC_DRBG. Он содержал математический поток, который создавал секретный вариант проникновения в любой криптокод. Конечно, NIST и NSA не афишировали, что у них есть этот черный ход (backdoor), и никто никогда не смог доказать, что этот поток был создан преднамеренно. Но даже после того, как вирус был найден, NIST заявил, что задействованный RNG должен быть включен в любой компьютер, продаваемый правительству США, как часть криптографической коллекции под названием Suite B, а также входить в качестве расширения в каждый компьютер, продаваемый неправительственным клиентам, потому что проще сделать только одну версию компьютера. Хотя производители и включили RNG в свои компьютеры, большая часть пользователей его не применяла.

Не остановившись на этом, NSA тайно заплатило очень популярным поставщикам компьютерных устройств за включение глючного RNG, и любой клиент, использующий его (вероятно, неосознанно), получал очень ослабленную защиту. Это был криптографический кошмар. Одна из великих загадок в мире прикладной криптографии – почему производители, получившие взятки от правительства США за то, что установили на компьютеры своих клиентов глючный RNG, не получили общественного осуждения. Когда производителей поймали с поличным, и об этом стало известно в 2007 году, Брюс Шнайер (Bruce Schneier) прекрасно обозначил суть проблемы: www.schneier.com/blog/archives/2007/11/the_strange_sto.html. В 2013 году все имевшие место подозрения о намеренно глючном RNG и заговоре NSA по активному давлению на общество были подтверждены сотрудником ЦРУ Эдвардом Сноуденом (Edward Snowden).
Оба инцидента, что совершенно справедливо, серьезно подорвали веру многих потребителей в то, что правительство США выберет действительно надежные стандарты криптографии. Это показало, что государственные структуры, преследуя двойную цель: и защиты, и слежки за своими гражданами, – часто допускают ослабление криптографии, не позволяя получить лучшую защиту. Несмотря на то что этот двойной подход вызвал серьезное недоверие, большинство наблюдателей считают, что выбору конкурсом NIST/NSA последних новых стандартов криптографии (то есть SHA-2, SHA-3, AES и постквантовой криптографии) можно доверять.

В начале февраля 2016 года NIST начал новый конкурс под названием «Процесс постквантовой стандартизации криптографии NIST» (https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/Documents/call-for-предложения-final-dec-2016.pdf) для выбора постквантового (квантовоустойчивого, квантовобезопасного) криптографического стандарта для обмена открытыми ключами и цифровыми подписями. В первом туре к ноябрю 2017 года кандидаты должны были представить на рассмотрение предложения. NIST получил 82 уникальных предложения и позволил 69 из них остаться в качестве официальных кандидатов «первого тура». Из них в январе 2019 года для участия во втором туре были выбраны 17 асимметричных шифров и 9 схем цифровой подписи (https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8240.pdf). Ожидается, что участники третьего тура будут официально объявлены в 2020 или 2021 году и что окончательно новые постквантовые стандарты криптографии будут объявлены между 2022 и 2024 годом. В этой главе будет дан обзор предложений всех официальных кандидатов второго тура.

Победившие предложения конкурса NIST/NSA обычно становятся официальными стандартами федерального правительства США и публикуются под общим названием «Федеральные документы по стандартам обработки информации» (Federal Information Processing Standards, FIPS). Этим стандартам должны отвечать все правительственные компьютеры и устройства, купленные и используемые правительством США, а также всеми государственными субподрядчиками. Фактически это означает, что все устройства и компьютеры, продаваемые в Соединенных Штатах, будут содержать и использовать эти стандарты, потому что правительство США является крупнейшим поку-

пателем вычислительных устройств. Поставщикам вычислительных устройств и программного обеспечения легче и экономически более выгодно включить федеральные стандарты США во все устройства, которые они производят, чем делать правительственные и неправительственные версии. В силу экономического доминирования США американские стандарты часто де-факто становятся международными (хотя некоторые более крупные страны, в частности Россия и Китай, создают и используют собственные стандарты). По этой причине такое большое значение придается криптографическим стандартам NIST/NSA. Они применяются в большинстве компьютеров и программном обеспечении в мире.

Если вас заинтересуют детали криптографических представлений на конкурс NIST, я настоятельно рекомендую загрузить алгоритм представления документов для отправки в NIST, расположенный по адресу https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-2-Submissions. Большинство подробностей вы найдете в PDF-документе в папке *Supporting_Documentation* с zip-файлом представления документов. NIST требует, чтобы каждое криптографическое представление включало обширную сопроводительную информацию, в том числе описание работы алгоритма, сведения о его слабых и сильных сторонах и об устойчивости к атакам, статистику производительности, примеры кода, рекомендации NIST по уровню безопасности (более подробно об этом далее) и многое другое. Чтобы получить общее представление о том, как работает алгоритм, вы можете почитать обзорные комментарии сторонников и критиков на веб-сайте конкурса NIST.

Классификация уровня безопасности

В конкурсе NIST Post-Quantum все представленные алгоритмы должны были включать конкретные реализации с конкретными уровнями защиты, представленными существующими в настоящее время квантовостойкими симметричными шифрами и хешами, как показано в табл. 6.1. Увеличение степени защиты возрастает с увеличением номера уровня безопасности NIST (например, уровень безопасности NIST 4 обеспечивает большую защиту, чем уровень безопасности 3).

NIST рассматривает все пять классификаций как квантовоустойчивые, хотя уровень безопасности 1 означает «предположительно безопасный в обозримом будущем, если только квантовые компьютеры не усовершенствуются быстрее, чем ожидается», иными словами – «довольно слабый». Это потому, что квантовые компьютеры, использующие алгоритм Гровера, могут эффективно снизить защиту AES-128 до 64 бит.

Таблица 6.1. Классификация NIST уровня безопасности и эквивалентной защиты

Уровень безопасности	Эквивалентная безопасность	Квантовая устойчивость
1	AES-128	Слабая
2	SHA-256/SHA3-256	Сильная
3	AES-192	Более сильная
4	SHA-384/SHA3-384	Очень сильная
5	AES-256	Самая сильная

В настоящее время неизвестны атаки, которые могут взломать AES с 64 битами, но будущие атаки, которые смогут это сделать, уже не за горами. Соответственно, многие криптографические эксперты не рассматривают криптографические реализации, достигающие лишь уровня безопасности NIST 1, как действительно квантовоустойчивые в долгосрочной перспективе. Однако NIST считает их в настоящее время приемлемыми и рассматривает их как переход к использованию более устойчивой криптографии, когда это позволят время и ресурсы.

Уровни безопасности 2 и 3, по определению NIST, означают «предположительно безопасный в обозримом будущем», а уровни 4 и 5 – «предположительно сверхбезопасный». Криптоспециалисты доверяют «предположительно сверхбезопасной» устойчивой криптографии, но соображения по производительности и реализации могут помешать их развертыванию в настоящее время. Например, многие текущие программы и устройства используют AES-128 по умолчанию и не могут использовать AES-256 или больше (пока).

Большинство конкурсантов NIST представили реализации своих алгоритмов для обеспечения безопасности с NIST уровнями 1, 3 и 5 и, в меньшем количестве, с уровнями 2 и 4. Были исключения. Компания NTRU Prime не стала представлять NIST шифры уровня безопасности 1 и 5. Компания Three-Bears не представила NIST шифры уровня безопасности 1 и 3, но отправила уровни 2 и 4. Компания SIKE представила NIST образцы шифров уровня безопасности 2. Компания NTRU Prime представила соответственно шифры уровня 2 и 4. Компании CRYSTALS-Dilithium и MQDSS не представили образцы уровня 5. Компания FALCON не представила реализации уровней 2, 3 или 4. Компания LUOV не представила образцы 1-го или 3-го уровня.

Для получения дополнительной информации и подробностей о классах безопасности NIST см. раздел 4.A.5 «Категории степени безопасности» следующего документа NIST: https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-forproposals-final-dec-2016.pdf.

Отличные итоговые обсуждения каждого алгоритма приводятся на сайтах NIST (https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions), Privacy News Online (www.privateinternetaccess.com/blog/2019/02/nist-round-2-and-post-quantumcryptography-the-new-asymmetric-algorithms-part-2/) и во многих других источниках (https://en.wikipedia.org/wiki/Post-quantum_cryptography).

В разделах ниже приведен обзор участников второго тура конкурса NIST. Описан каждый криптографический алгоритм, что он делает, какие основные принципы использует; иногда дается историческая справка, если это информация из достоверных источников, и указывается национальный состав каждой команды, подавшей заявку. Последнее призвано подчеркнуть: команды зачастую насчитывают участников из разных стран. Перед обсуждением шифров и схем определена связанная терминология и перечислены типы.

Примечание Многие алгоритмы, описанные в этой главе, также являются частью проекта Open Quantum Safe («Открытая квантовая безопасность») – https://openquantumsafe.org/. Это хранилище кода и организация, помогающая нашей подготовке к постквантовому миру. Когда криптографическая

реализация определяется как участвующая в проекте, а это означает, что организация, возможно, уже сегодня реализовала этот конкретный постквантовый алгоритм в тестовых и реальных сценариях, используйте опыт и информацию предыдущих исполнителей, а также делитесь проблемами и полученными вами уроками.

PKE против KEM

Традиционная криптография с открытым ключом, также известная как *шифрование с открытым ключом* (public key encryption, PKE), часто используется для передачи симметричных ключей шифрования, которые затем применяются для шифрования первоначально предназначенного открытого текста контента, нуждающегося в защите. Симметричные ключи быстрее и сильнее (для небольших размеров ключей), чем асимметричное шифрование, и поэтому PKE часто используются просто в качестве безопасного транспортного средства для симметричных ключей, которые выполняют всю работу прямого шифрования. Шифрование PKE отлично справлялось с этой работой десятилетиями, но у него есть по крайней мере одна большая проблема. Когда открытый ключ длиннее, чем зашифрованный контент (как это обычно бывает с симметричным ключом при обмене ключами), это позволяет злоумышленникам очень легко получить исходный закрытый ключ. Чтобы предотвратить сценарий, при котором содержимое сообщения, которое должно быть зашифровано (например, симметричный ключ), короче, чем асимметричный закрытый ключ, используемый для шифрования, эту уязвимость устраняют, вставляя в PKE «дополнение», так называемый паддинг. К сожалению, случайная генерация паддинга часто является самым слабым звеном в системе PKE. Злоумышленники, атакуя PKE, нередко сосредоточиваются на недостатках логики в паддинге и находят уязвимости. Симметричные ключи, вероятно, со временем будут только увеличиваться, особенно в противостоянии улучшенным квантовым атакам, что представляет постоянный риск.

Методы, или *схемы*, *инкапсуляции ключей* (key encapsulation methods, KEM) являются асимметричным типом метода шифрования, предназначенным для улучшения безопасной передачи (или генерации) симметричного ключа. Чтобы оставаться в безопасности, они не нуждаются в случайном заполнении, добавлении паддинга к коротким сообщениям. Многие постквантовые криптографические алгоритмы особенно предрасположены к применению KEM и потому, что постквантовые алгоритмы часто имеют даже более длинные асимметричные ключи и многие команды предлагают квантовоустойчивые KEM вместо PKE. Иногда его наличие в алгоритме обозначается включением KEM в название алгоритма, например FrodoKEM и NTS-KEM. Некоторые постквантовые криптографические алгоритмы будут предлагать и PKE-, и KEM-версии.

Формальные гарантии неразличимости

В некоторых именах и описаниях шифров вы увидите аббревиатуры CPA и CCA, которые относятся к высокоценимому криптографическому свойству,

известному как *неразличимость зашифрованного текста* (ciphertext indistinguishability). Этот термин подразумевает, что полученный зашифрованный текст устроен так, что злоумышленник не может использовать зашифрованный текст для поиска более простых атак на задействованные ключи шифрования. Обозначение CPA означает, что злоумышленник может даже знать выбранные представления открытого текста (то есть *атаковать выбранный открытый текст*), но, получив зашифрованный текст, так и не получит подсказку о задействованном секретном ключе шифрования. CCA обозначает атаку выбранного зашифрованного текста, при которой злоумышленник может получить определенный зашифрованный текст, расшифровать его и все равно не получить подсказки о задействованных секретных ключах шифрования. Для получения дополнительной информации смотрите https://en.wikipedia.org/wiki/Ciphertext_indistinguishability.

Безопасность цифровых систем безопасности иногда описывается как EUF-CMA и/или SUF-CMA, что в известной степени сродни дескрипторам CPA и CCA, используемым как обобщение базовых шифров асимметричных систем безопасности. Обозначение EUF-CMA расшифровывается как *экзистенциальная нераскрываемость при атаке по выбранному сообщению* (Existential Unforgeability under Chosen Message Attack), а SUF-CMA – *сильная экзистенциальная нераскрываемость при атаке по выбранному сообщению* (Strong Existential Unforgeability under Chosen Message Attack). При атаке в соответствии с обоими обозначениями злоумышленник может попросить подписать любой контент и получить подпись, но все равно не сможет определить закрытый ключ, используемый для подписи контента. При применении немного более сильного SUF-CMA безопасность повышается, поскольку злоумышленник не может создать другую цифровую подпись, которая все еще проверяется на соответствие первоначальной схеме цифровой подписи как исходящей из того же контента и закрытого ключа (было бы плохо генерировать две разные действительные подписи для одного того же уникального контента, используя ту же схему цифровой подписи). Имея эти свойства и доказывая, что алгоритм в полной мере обладает ими, надо учитывать, что есть разница между возможностью претендовать на один или на оба дескриптора (описания). Для получения дополнительной информации о EUF-CMA и SUF-CMA смотрите https://blog.cryptographyengineering.com/euf-cma-and-suf-cma/.

Все хорошие методы PKE и KEM обычно соответствуют требованиям безопасности CPA и CCA, и цифровые подписи, как правило, пытаются обеспечить безопасность EUF-CMA. Чтобы использовать эти обозначения, криптографический алгоритм должен сначала теоретически доказать свое соответствие безопасности и со временем выдержать реальные настойчивые атаки. NIST требует, чтобы успешные криптографические кандидаты были CPA- и CCA-безопасными или EUF-CMA-безопасными в зависимости от типа криптографического алгоритма. В документации к большинству представленных алгоритмов четко заявлено о достижении этих целей обеспечения безопасности, за исключением NTRU Prime и NTS-KEM, в отношении которых явно не упоминается о достижении целей CPA.

Размеры ключа и шифрованного текста

Все асимметричные шифры имеют два типа связанных криптографических ключей: секретный и открытый. *Секретный*, или *закрытый*, *ключ* используется для подписи контента, и он должен быть известен только держателям пары ключей. В некоторых постквантовых алгоритмах (таких как CRYSTALS-Dilithium, SPHINCS+ и LUOV) секретный ключ – это просто затравочное значение, используемое для генерации других ключей, выполняющих реальную работу. В таких реализациях секретные ключи обычно невелики (от 16 до 64 байт) и имеют постоянный размер для реализации любого уровня безопасности. В этих случаях обычно связанный открытый ключ также очень мал. Квантовоустойчивые алгоритмы могут иметь ключи переменной длины для разных уровней безопасности, так же как и различные ключи для разных версий цели реализации (например, более быстрая, но менее безопасная реализация).

Открытый ключ используется для шифрования содержимого и проверки содержимого, подписанного соответствующим закрытым ключом. Открытый ключ теоретически может быть известен и использован всеми, и все же защищенный секрет останется секретом. Так работает система с асимметричными шифрами. При асимметричном шифровании генерируется соответствующий открытый ключ, связанный с закрытым ключом.

Зашифрованным текстом, как правило, считается любой зашифрованный контент, хотя в контексте сравнения различных представленных шифров играет роль, насколько большим станет самый маленький зашифрованный открытый текст после шифрования. Например, если вы зашифровали одну только букву A современным шифром, результирующий зашифрованный текст обычно будет включать в себя намного больше символов.

Цифровая подпись является уникальным результатом хешированного контента. В схемах цифровой подписи открытый ключ и размеры цифровой подписи математически связаны между собой в обратной пропорции. Если вы уменьшите размер первого, вторая растет, и наоборот. Таким образом, для постквантовой цифровой подписи чаще всего сохраняется соотношение: если открытый ключ небольшой, цифровая подпись большая, и наоборот.

NIST требует, чтобы все создатели криптографических алгоритмов объявляли размеры каждой из этих переменных для каждого объявления уровня безопасности NIST. Также требовалось представить размер минимального зашифрованного текста для асимметричных шифров. Схемы цифровой подписи должны были быть представлены размером результирующей цифровой подписи. Эти размеры важны, потому что очень большие размеры часто имеют проблемы с производительностью и памятью (по сравнению с меньшими размерами цифровой подписи) и обычно требуют больше памяти для хранения и большей пропускной способности сети. Вычислительная сложность конкретного алгоритма, впрочем, часто оказывает гораздо большее влияние на общую производительность реализуемой криптографии.

Многие из алгоритмов с бóльшими переменными размерами ключа предполагают более широкую сферу потенциального применения, чем те, что были представлены в соответствии с уровнем безопасности, определенным

NIST. Некоторые алгоритмы позволяют применять любой размер ключа (в заданных пределах), в зависимости от желаемого уровня защиты относительно требований применения.

Типы постквантовых алгоритмов

При обсуждении различных постквантовых алгоритмов важно знать основные типы алгоритмов и применяемые ими методы защиты от квантовых атак.

Криптография на основе кода

Криптография на основе кода (также известная как *алгебраическое кодирование* или *коды с исправлением ошибок* (algebraic coding или error correcting codes, ECC)) – давно известный и устойчивый к атакам набор шифров и подписей на основе математических алгоритмов, в которых преднамеренно создаются «ошибки» (то есть коды) в содержании открытого текста таким образом, что они скрывают/шифруют исходный контент. Соответствующий «исправляющий ошибки» код/алгоритм можно использовать для удаления «ошибок» и возврата зашифрованного содержимого в исходный текст (то есть дешифрование).

В качестве простого примера давайте предположим, что отправитель шифрует открытый текст 1111. В контент будут преднамеренно введены «ошибки», скажем текст 011101, который затем будет передаваться получателю. Процесс «исправления ошибок» на стороне получателя удалит «ошибки» и надежно воспроизведет исходный контент 1111.

Криптография на основе кода основана на ECC-подобных методах, которые настолько сложны, что найти решение для «ошибки», не зная вовлеченного ключа, очень трудно (нетривиально). В 1970-х и 1980-х годах советский математик Валерий Денисович Гоппа связал с ECC геометрические фигуры и комбинации. Сегодня эти коды широко известны как *коды Гоппы* и приняты шифровальщиками. Один из самых успешных шифров на основе кода McEliece (рассматривается далее в этой главе), основанный на двоичных кодах Гоппы, как и большинство шифров на основе кода в целом, был вторым по распространенности типом шифров с асимметричным шифрованием, представленных в NIST. Представленные шифры на основе кода включают BIKE, Classic McEliece, HQC, LEDAcrypt, NTS-KEM, ROLLO и RQC.

Существует две большие технические проблемы в криптографии на основе кода. Во-первых, в криптографии ECC для шифрования данных требуется значительно больше битов ключа, чем обычно (по сравнению с другими типами шифров). Ключи шифрования на основе кода, особенно открытые ключи, могут легко превышать 300 000 бит. Раньше, в 1970-х и 1980-х годах, когда McEliece был представлен впервые, это было огромной проблемой, но сегодня уже не такое непреодолимое вычислительное препятствие. Кроме того, многие шифры на основе кода должны предоставить возможность значительно уменьшить размер своего ключа (например, многие используют

40-байтовые секретные ключи). Если вы видите огромный ключ, связанный с асимметричным шифровальным шифром, скорее всего, он основан на коде.

Во-вторых, поскольку ECC исправляет предполагаемые «ошибки», при отсутствии корректного дизайна всегда есть шанс, что «ошибки» будут обнаружены, то есть законное дешифрование даже с правильным ключом дешифрования может потерпеть неудачу. Это наводит на мысль, что дешифрование может быть выполнено дополнительно один или несколько раз, и при этом существует вероятность того, что конкретный экземпляр расшифровки ECC может не сработать или застрять во временно́м самопроизвольном циклическом отказе в обслуживании. Большинство шифров ECC пытаются предотвратить такого рода блокировки, и подобные блокировки крайне редки – близки к нулю. Но если вы читаете о ECC-шифрах, имеющих «ненулевую» частоту сбоев дешифрования (например, HQC), то должны знать, по крайней мере, о теоретической возможности.

Большой обзор дискуссий о кодах ECC и Гоппы можно найти здесь: https://surface.syr.edu/cgi/viewcontent.cgi?article=1846&context=honors_capstone.

Криптография на основе хеша

Криптография на основе хеша, как явствует из названия, строится с использованием хешей и обычно применяется к схемам цифровой подписи (в противоположность шифрованию). Как описано в предыдущих главах, хеш является односторонней функцией, которая преобразует хешированный контент в репрезентативный набор битов (называемый хеш, результат хеширования, подпись или дайджест сообщения), который уникален для контента. Схемы подписей XMSS (Extented Mercle Signature Scheme, расширенная схема подписи Меркла), подпись Leighton–Micali Signature (LMS), постквантовые подписи с блокчейном (Blockchained Post-Quantum Signatures, BPQS) и схемы цифровой подписи SPHINCS и SPHINCS+ основаны на криптографии на основе хешей. Единственной цифровой подписью на основе хеша, представленной и принятой NIST во 2-м туре конкурса, была схема SPHINCS+.

Ральф Меркл (Ralph Merkle) изобрел, по сути, целое поле криптографических хешей. Он также участвовал в первой общеизвестной реализации шифрования с открытым ключом (наряду с Уитфилдом Диффи (Whitfield Diffie) и Мартином Хеллманом (Martin Hellman)) в конце 1970-х гг. По этой причине при обсуждении криптографии на основе хеша вы часто будете слышать о деревьях Меркла (т. е. хеш-деревьях), коробках и головоломках Меркла. Деревья Меркла – это иерархическая серия хешей, которая хеширует другие хеши, хеширующие исходное содержимое. Если интересно, посмотрите https://en.wikipedia.org/wiki/Merkle_tree для более подробной информации.

Криптография на основе хеша считается квантовоустойчивой, поскольку хеши не подвержены дешифровке алгоритмом Шора, хотя чувствительны к алгоритму Гровера. Алгоритм Гровера на квантовых компьютерах при решении определенных типов задач, таких как взлом хешей, по сравнению с бинарными компьютерами дает улучшение, как квадратный корень. Это фактически вдвое уменьшает силу любой криптографии на основе хеша.

Это также означает, что удвоение размера ключа хеша компенсирует преимущества атаки, полученные алгоритмом Гровера при квантовом вычислении.

Примечание Крайне важно, чтобы базовый хеш соответствовал всем рассмотренным ранее атрибутам хорошего, безопасного хеша. Если хеш со временем перестает быть «хорошим», то любая криптография на основе этого хеша становится восприимчивой не только к квантовым, но и к бинарным вычислениям, на уровнях значительно ниже заявленной восприимчивости ключа.

Все хеши ограничены количеством сообщений, которые они могут защитить, прежде чем результаты хеша станут (преждевременно) избыточными для всех возможных уникальных входных данных, которые они могут хешировать. Например, все пароли для входа в Microsoft Windows преобразуются в хеши NT. Вы можете создать много миллиардов уникальных возможных паролей в Windows (около 2^{65535} различных комбинаций), но один и тот же NT-хеш в конечном итоге будет идентичен многим другим паролям (в теории хеш-атак это известно как пример коллизии второго прообраза) из-за присущих хешу ограничений и его ключевого пространства (т. е. всех возможных вариантов).

Если криптография на основе хеша «случайно» повторяет один и тот же одноразовый ключ для двух разных входов, то это дает злоумышленникам четкое представление о закрытом ключе. По этой причине разработчики криптографии на основе хеша делают все возможное, чтобы предотвратить одноразовые повторения ключей. Есть несколько разных методов уменьшения риска.

Одним из способов устранения этого риска является повышение точности алгоритма хеширования для различения уникальности контента. Если хеш всегда дает уникальные хеш-результаты, то проблема повторения исчезает. Это бывает трудно сделать, потому что пространство ключей хеша всегда ограничено в большей степени, чем потенциальные контенты, которые он пытается хешировать. Чтобы компенсировать этот риск, разработчики хешей также могут увеличить размер результирующей цифровой подписи (чтобы оставить больше места для ключа). Чем длиннее цифровая подпись, тем больше возможные хешированные результаты. Таким образом, хеш с результатом 128-битного хеша, вероятно, будет более точным, чем один хеш, ограниченный 64-битным результатом. Очень большие цифровые подписи могут стать слишком большими и громоздкими, вызывая проблемы с производительностью и хранением. Большинство криптографических экспертов считают, что хороший хеш, использующий присущую алгоритмическую точность, не должен приводить к очень большим цифровым подписям. Другие полагают, что большие цифровые подписи – единственный способ гарантировать точное хеширование без встроенной избыточности результата хеширования. В любом случае обработка очень маленьких и очень больших цифровых подписей требует специального рассмотрения.

Еще один распространенный способ предотвращения повторов ключей – сделать хеш меняющим состояние (а не неизменным). Меняющий свое состояние хеш сохраняет каждый использованный им секретный ключ и следит за тем, чтобы он не использовался снова. Большинство традиционных хешей подписей меняют свое состояние. Если повторный ключ обнаружен, алгоритм выполняется снова или выбирает другую часть более длинного потока ключей для создания иного уникального одноразового ключа.

Хеши с состоянием и без состояния имеют свои преимущества и недостатки. Хеши без состояния не могут гарантировать уникальные ключи, но в целом имеют бóльшие размеры ключей. Хеши с состоянием имеют меньшие размеры ключей в общем, но поскольку они должны хранить «таблицу состояний», то громоздки для ресурсов, хранилищ и перспектив безопасности. Хеши с сохранением состояния также могут создавать серьезную проблему при восстановлении данных. Если обработка проведена с недостаточной тщательностью, восстановленная реализация хеша с сохранением состояния может перезаписать свою предыдущую таблицу состояний, стирая свидетельство ранее использованного ключа, а затем хеш может случайно использовать повторно тот же ключ с будущим криптографическим действием. Злоумышленник, зная, что таблица состояний имеет перезаписанный хеш, может искать признаки повторного ключа и получить преимущество для использования в криптографической атаке. Это маловероятное событие с довольно низким риском, но когда криптографы видят какие-либо теоретические слабости, они считают это большой слабостью. Таким образом, NIST не разрешает представлять на рассмотрение криптографическую проверку на основе хеша с сохранением состояния алгоритма, исключая участие некоторых претендентов, сильных в другом отношении.

Решетчатая криптография

Решетка – это размерное, распределенное, повторяющееся геометрическое расположение/структура чего-либо – например, объектов или точек – в пространстве. Решетки встречаются во всей природе, например в молекулах или кристаллах, и часто используются людьми для создания других гораздо более крупных объектов, в том числе сетей, заборов или узоров на тканях. Многие математические формулы и алгоритмы создают решетки. Были получены формулы и результаты, которые принципиально трудно разложить на множители (это свойство называется «вычислительные проблемы решетки»). Наиболее распространенные задачи решетки, используемые в криптографии, известны как *обучение с ошибками* (learnings with errors, LWE), *кольцевое обучение с ошибками* (ring learning with errors, RLWE), *модульное обучение с ошибками* (module learning with errors, MLWE), *обучение с округлением* (learning with rounding, LWR) и десятки вариантов. Каждый тип задач решетки имеет свои преимущества и недостатки. В целом LWE с участием колец имеет тенденцию быть быстрее и иметь меньшие размеры ключей, чем классическая LWE, но также содержит новые математические конструкции, которые пока еще не были полностью протестированы.

Примечание Вы узнаете много нового о «кольцах» при изучении криптографии, особенно постквантовой. Кольца относятся к фундаментальной и сложной математической структуре, используемой в абстрактной алгебре. Посмотрите для получения более подробной информации https://en.wikipedia.org/wiki/Ring_(mathematics).

Эти очень трудно решаемые проблемы решетки, устойчивой применительно как к двоичным, так и к квантовым компьютерам, были использованы для шифрования с открытым ключом и схем цифровой подписи. В криптографии на основе решетки сложная функция решетки создается как закрытый ключ. Открытый ключ создается как модифицированная версия оригинальной решетки. Контент зашифрован с использованием модифицированной версии (открытый ключ), и только владелец оригинальной версии решетки (закрытый ключ) может легко восстановить зашифрованное сообщение, возвращая его в исходное состояние открытого текста.

По сути, решеточная криптография создала математическую проблему рабочей нагрузки для злоумышленника, которая почти эквивалентна нагрузке, необходимой для вычисления больших простых чисел (или превышает ее), но не полагается на большие простые числа для их защиты. Следовательно, криптография на основе решетки не считается восприимчивой к алгоритму Шора или любому квантовому алгоритму с простыми числами.

Теоретически недостатком криптографии на основе решетки может оказаться требование относительно больших размеров ключа по сравнению с другими типами шифров, хотя очень важно заметить, что это не относится к большинству шифров на основе решетки, представленных на рассмотрение NIST, включая CRYSTAL-Kyber, LAC, NewHope, NTRU, NTRU Prime, Round5, SABER и ThreeBears. Только FrodoKEM имеет относительно большой размер ключа, хотя несколько основанных на коде алгоритмов намного больше.

Первым шифром на основе решетки был шифр NTRU, представленный в 1998 году, за которым следовало несколько шифров на основе математических проблем LWE и RLWE. Сегодня шифры на основе решетки являются наиболее популярным типом постквантовой криптографии, представленной в NIST. Кроме того, в 2009 году Крейг Джентри (Creig Gentry) в своей диссертации (https://dl.acm.org/citation.cfm?id=1834954) использовал решеточную криптографию для создания первой в мире полностью гомоморфной системы шифрования, которая, как обсуждалось в предыдущей главе, позволяет третьей стороне правильно манипулировать зашифрованными данными без предварительного их дешифрования.

Примечание Большинство решеточных шифров и связанных с ними задач основаны на задачах кратчайших векторов (shortest vector problems, SVP), которые требуют для решения, по крайней мере, большого экспоненциального порядка времени. К сожалению, общая безопасность, обеспечиваемая SVP, не понята в полной мере, и некоторые теоретические атаки существенно ослабили их защиту. По этой причине вся криптография на основе решетки (и особенно та, которая основана на SVP без компенсации

ослабления) не является полностью устойчивой и может оказаться в будущем слабее, чем предполагалось. Это может создавать проблемы, учитывая тот факт, что большинство постквантовых шифров (представленных в NIST) были шифрами на основе решетки.

Многомерная криптография

«Многомерная» в данном случае означает «со множеством переменных или параметров». Многомерная криптография относится к асимметричным схемам шифрования и подписей, формирования криптографических примитивов с помощью многомерных полиномиальных математических уравнений, таких как $x + y + z = n$. Вы также можете встретиться с криптографией, основанной на многомерной полиномиальной математике, называемой *криптографией с многомерным квадратичным (MQ) полиномиальным уравнением* (multivariate quadratic (MQ) polynomial equation cryptography). Это название подчеркивает тот факт, что по крайней мере одна из переменных возведена во вторую степень (например, $x^2 + y + z = n$). Корректно созданная для защиты многомерная криптография не может быть решена за полиномиальное время и не опирается на большие простые числа и потому считается квантовоустойчивой. Характеристики, присущие такой криптографии, делают ее в связи с ее производительностью хорошим кандидатом для аппаратных реализаций, таких как специальные интегральные микросхемы (specific integrated circuit, ASIC) и программируемые пользователем вентильные матрицы (field-programmable gate arrays, FPGA).

Многомерная криптография включает HFE, Gui, Balanced Oil & Vinegar («масло и уксус в оптимальной пропорции»), Unbalanced Oil & Vinegar («масло и уксус в неоптимальной пропорции») и Tame Transformation Signature («послушно передаваемая подпись») (для некоторых алгоритмов намеренно выдуманы смешные названия). Схемы многомерной цифровой подписи включают GeMSS, LUOV, MQDSS и Rainbow (Радуга). Rainbow – многослойная реализация Unbalanced Oil & Vinegar.

Криптография изогенной сверхсингулярной эллиптической кривой

Изогенная криптография с надсингулярной эллиптической кривой (или кратко: *изогенная криптография*) опирается на математические уравнения и алгоритмы, которые для защиты шифрования создают сверхсингулярные эллиптические кривые и графы изогении. Эллиптические кривые описываются математическими формулами, которые представляют собой алгебраические непересекающиеся кривые (также известные как *несингулярные*). Все сверхсингулярные кривые являются несингулярными, и «сверх-» относится к необычно большим кольцам. Изогены являются отдельными алгебраическими группами, которые разделяют пересечение связанных между собой значений. В качестве простого примера представьте себе, что у вас есть числа 1, 2, 3 и 4 в одной группе и буквы A, B, C и D в другой группе и каждое число

было связано с соответствующей буквой. Изогенными кривыми будут две кривые (представленные, конечно, математически), которые можно сопоставить друг с другом.

В мире криптографии с изогенией два разных алгоритмических уравнения создают изогенную связь, которая может быть использована для шифрования и дешифрования. Открытый ключ представляет собой пару эллиптических кривых, а закрытый ключ является изогенией между ними. Нахождение этой изогении дается только сингулярной парой эллиптических кривых, и, как полагают, это очень трудная для решения задача. Если это звучит сложно, знайте, что решение уравнений изогении сверхсингулярных эллиптических кривых является одной из самых сложных математических задач, когда-либо создававшихся; тем не менее эти кривые изучены достаточно хорошо, чтобы можно было оценить их сильные и слабые стороны.

В 2012 году китайские исследователи создали первые квантовозащищенные цифровые подписи на основе изогении сингулярных эллиптических кривых и многомерную криптографию (https://pdfs.semanticscholar.org/527a/4abe13ee6ce7858e040ceaa7cd0b983969d8.pdf). Изогенная криптография имеет тенденцию к использованию ключей очень малых размеров и наряду с этим позволяет легко и идеально скрыть секреты. *Совершенная секретность передачи* (perfect forward secrecy) – это криптографическая защита, включающая часто меняющиеся сеансовые ключи, так что будущий компромисс ключа не может быть использован для взлома предыдущих сессий, потому что они использовали разные ключи. Совершенная секретность передачи обычно является весьма желательным свойством криптографии, хотя его часто невозможно достичь. Изогения хорошо сочетается с идеальной секретностью. С другой стороны, криптография изогении относительно нова, поэтому она не была протестирована и атакована в той же степени, что и другие постквантовые типы криптографии. Хотя ранние изогенные реализации были скомпрометированы, такие изменения, как использование сверхсингулярной изогении вместо просто несингулярных кривых, выдержали известные атаки. Единственным представленным изогенным шифром, принятым NIST для оценки во 2-м туре, был SIKE.

Доказательство нулевого знания

Доказательство нулевого знания (zero-knowledge proof, ZKP) (известное также как *протокол с нулевым знанием*) является методом, с помощью которого одна сторона (называется *прувер*, prover) может доказать другой стороне (называется *проверяющий*, или *верификатор*, verifier), что она знает величину x, без необходимости реально передавать или принимать какую бы то ни было еще информацию. Иными словами, прувер, удостоверяя, что он действительно знает значение x, при этом не предоставляет этого значения, равно как и дополнительной, несущественной информации.

В качестве примера обычной системы ZKP можно привести пароль для входа в систему, используемый в современной системе аутентификации «вы-

зов–ответ». Предположим, что пользователь хочет войти на сервер, используя действительный пароль, но в то же время не позволяет серверу знать или хранить незашифрованный пароль (так что он не может быть украденным или скомпрометированным). Как пользователь может доказать серверу, что он имеет (и может использовать) правильный пароль, не вводя самого пароля?

Одним из ответов ZKP является использование криптографических хешей вызова–ответа на основе пароля, но без использования фактического пароля. Например, предположим, что открытый текстовый пароль пользователя – frog («лягушка»). Давайте представим себе, что когда пользователь создает пароль в первый раз, открытый текст frog сразу хешируется, и результат хеширования составляет 1234. Хешированный результат – единственная версия пароля, отправленная и хранящаяся на сервере. Сервер не может знать исходный текстовый пароль.

Когда пользователь хочет войти на сервер, он инициирует соединение с сервером. Сервер создает случайное значение, скажем 9876, и отправляет его пользователю (это вызов). Пользователь вычитает хеш пароля 1234 из 9876, чтобы получить результат 8642, и отправляет его обратно на сервер (это ответ). Сервер использует сохраненный хеш пароля пользователя 1234 для выполнения того же вычитания случайно сгенерированного числа, получает тот же результат (8642) и сравнивает с результатом, который пользователь отправил обратно. Только пользователь с правильным исходным паролем frog будет иметь правильный хеш 1234 и сможет получить правильный результат при вычитании его из случайно сгенерированного значения 9876. Таким образом, пользователь может успешно доказать проверяющему серверу, что у него был правильный оригинальный пароль, не раскрывая сам пароль. Самые современные системы связи, включая пароли Microsoft Windows, используют аналогичные (хотя более сложные) схемы.

Реализации ZKP востребованы многими производителями компьютеров. Подобно тому как раньше в сфере компьютерной безопасности на каждом шагу употреблялись модные специальные термины вроде «искусственный интеллект» (AI) или «блокчейн», ZKP используется очень часто. Многие поставщики неправомерно включают эту аббревиатуру в описание своей продукции, чтобы придать ей больше ценности.

Итак, воспринимайте скептически уверения поставщика, использующего абревиатуру ZKP. Кстати, криптографы – довольно серьезное и правдивое сообщество. Заявляя о том, что его алгоритм применяет ZKP, криптограф обычно имеет на это все основания. Криптография ZKP чаще включает в себя проверку знаний чего-то криптографического, такого как, например, функция дискретного логарифма, без раскрытия самой функции. В криптографических кругах вы можете услышать слова «доказано и проверено», что подразумевает проверку криптоустойчивости сигма-протоколами или доказательством «в три этапа или три сообщения». Единственный представленный NIST квантовоустойчивый алгоритм, который использует ZKP, – схема цифровой подписи Picnic.

Квантовая устойчивость симметричного ключа

Под квантовой устойчивостью понимается присущая традиционному алгоритму шифрования и аутентификации с симметричным ключом способность противостоять квантовым атакам. Как уже говорилось ранее, симметричные шифры не восприимчивы к алгоритму Шора, а алгоритм Гровера уменьшает защиту вдвое. Таким образом, в некотором смысле симметричные ключи шифрования уже квантовоустойчивы, если размеры ключа достаточны для того, чтобы справиться с алгоритмом атак Гровера. Сегодня это означает: использование симметричных шифров с размером ключа 256 бит и более приемлемо для долгосрочной защиты. NIST и другие полагают симметричные шифры с 128-битными ключами слабо квантовоустойчивыми, 192-битные симметричные ключи считаются умеренно квантовоустойчивыми. Соответственно, симметричные шифры явно участвуют не в последнем постквантовом конкурсе NIST.

Все представленные алгоритмы используют традиционные симметричные шифры ключей и хеши как часть их реализации. Наиболее распространенный симметричный шифр, используемый в современном мире, – усовершенствованный стандарт AES (Advanced Encryption Standard), и это относится и к квантовоустойчивым шифрам. Наиболее квантовоустойчивые шифры используют AES.

Следует также упомянуть квантовоустойчивый симметричный шифр SNOW 3G, хотя он гораздо менее популярен и не используется ни в одном из представленных предложений шифра. SNOW – это синхронный потоковый шифр на основе слов, разработанный шведами Томасом Йоханссоном (Thomas Johansson) и Патриком Экдалом (Patrik Ekdahl) в Лундском университете (Lund University). SNOW (версия 1), SNOW 2.0 и SNOW 3G (адаптированные для использования в сотовых сетях) реализованы в нескольких продуктах и приложениях. Вы можете получить более подробную информацию о шифре SNOW и SNOW 3G здесь: www.gsma.com/aboutus/wp-content/uploads/2014/12/uea2designevaluation.pdf.

Все представленные шифры также используют традиционные хеши, которые, как и шифрование с симметричным ключом, не восприимчивы к алгоритму Шора. Большинство используют SHA-3 (еще один стандарт NIST), хотя многие также используют шифр SHAKE, потоковый шифр, который тоже применяется SHA-3. Квантовоустойчивые шифры должны применять соответствующие традиционные длины ключей, чтобы остаться квантовоустойчивыми, и размер ключа, используемый конкурсантом, часто менялся относительно уровня безопасности NIST, пытаясь удовлетворить конкретную реализацию.

В табл. 6.2 показаны все имена алгоритмов второго тура конкурса NIST и их типы криптографии.

Все эти типы алгоритмов были использованы для создания квантовоустойчивой криптографии, и каждый из них будет описан в следующем разделе.

Таблица 6.2. Криптографические типы второго тура конкурса NIST

Асимметричные шифры / KEM	Тип	Подписи	Тип
CRYSTAL-Kyber	Lattice	CRYSTALS-Dilithium	Lattice
FrodoKEM	Lattice	FALCON	Lattice
LAC	Lattice	qTESLA	Lattice
NewHope	Lattice	SPHINCS+	Hash
Three Bears	Lattice	GeMSS	Multivariate
NTRU	Lattice	LUOV	Multivariate
NTRU Prime	Lattice	MQDSS	Multivariate
SABER	Lattice	Rainbow	Multivariate
Classic McEliece	Code	Picnic	Zero-knowledge proof
NTS-KEM	Code		
BIKE	Code		
HQC	Code		
LEDAcrypt	Code		
ROLLO	Code		
RQC	Code		
SIKE	Isogeny		

Примечание. Lattice – на основе решетки. Code – на основе кода. Isogeny – изогенная. Hash – на основе хеша. Multivariate – многомерная. Zero-knowledge proof – с использованием доказательства нулевого знания.

Квантовоустойчивые асимметричные шифры

Квантовоустойчивые шифры – это криптографические шифры, которые не слишком восприимчивы к квантовым вычислениям с использованием квантовых алгоритмов и, в частности, алгоритма Шора (или любого квантового алгоритма, который может очень быстро вычислять уравнения с простыми числами). Они не используют квантовые свойства, чтобы защититься от атак. Существуют десятки квантовоустойчивых шифров, хотя один или несколько из 17 кандидатов конкурса NIST второго тура асимметричного шифрования, вероятно, станут одним из возможных федеральных стандартов NIST. Асимметричные кандидаты с инфраструктурой PKE и инкапсуляцией KEM второго тура NIST следующие (в алфавитном порядке):

- BIKE;
- Classic McEliece;
- CRYSTALS-Kyber;
- FrodoKEM;
- HQC;
- LAC;
- LEDAcrypt;
- NewHope;
- NTRU;

- NTRU Prime;
- NTS-KEM;
- ROLLO;
- Round5;
- RQC;
- SABER;
- SIKE;
- ThreeBears.

Некоторые из этих 17 шифров представляют собой сочетания нескольких шифров, представленных отдельно в первом туре конкурса, которые были объединены в одно семейство шифров с похожими характеристиками. Например, HILA5 и Round2 в конечном итоге стали Round5.

Примечание Строчные и прописные буквы в вышеприведенных названиях алгоритмов используются в строгом соответствии с авторской версией. Если все название состоит из прописных букв, оно чаще всего представляет собой аббревиатуру.

Примечание Этот список, разумеется, включает далеко не все возможные сильные постквантовые асимметричные алгоритмы. Многие существующие постквантовые криптографические алгоритмы (асимметричные и цифровые подписи) не были представлены по целому ряду причин, в том числе из-за того, что создатели не хотели отказываться от своих алгоритмов бесплатного публичного использования; многие (если точнее, 22) были атакованы и разбиты после представления. У многих были недостатки в представленных документах, или они не соответствовали критериям приема на конкурс NIST (например, XMSS, LMS и BPQS). Алгоритмы, которые изначально были представлены на рассмотрение в первом туре, но не участвовали во втором, следующие: BIG QUAKE, CFPKM, Compact LWE, DAGS, DME, DRS, DualModeMS, Edon-K, EMBLEM/R.EMBLEM, Giophantus, Guess Again, Gui, HiM-3, HK17, KCL, KINDI, Lepton, LIMA, Lizard, LOTUS, McNie, Mersenne-756839, pqNTRUSign, Odd Manhattan, Post-quantum RSA-Encryption, Post-quantum RSA-Signature, QC-MDPC KEM, RaCOSS, Ramstake, RankSign, RLCE-KEM, RVB, SRTPI, Titanium и WalnutDSA. Кроме того, десятки квантовоустойчивых алгоритмов не были представлены; среди них GGH, XMSS и UOWHF. Эти криптографические алгоритмы были приняты или могут быть приняты другими органами стандартизации и странами.

BIKE

Инкапсуляция битовых ключей (BIKE) – это набор методов инкапсуляции KEM на основе кода. Создан многонациональной командой (в основном французскими авторами в партнерстве с участниками из Германии, Израиля и США), у него есть три разных варианта под названиями BIKE-1, BIKE-2 и BIKE-3. Он основан на McEliece-шифровании, QC-MDPC (Quasi-Cyclic Moderate Density Parity Check, квазициклическая проверка на четность умеренной плотности), CAKE, Ouroboros (отдельно заявлен на 1-й тур конкурса

NIST, но не прошел во 2-й тур). *Эфемерные ключи* – это криптографические ключи, которые генерируются для каждого процесса выполнения установки ключа вместо генерации одного статичного ключа. Эфемерные ключи позволяют шифру использовать совершенную секретность передачи.

BIKE имеет производительность и размеры ключей, аналогичные решетчатым криптосистемам. Для 2-го тура конкурса NIST требуется следующая реализация безопасности: секретные ключи варьируются в размере от 1988 до 4110 байт, открытые ключи имеют размер от 20 326 до 65 498 байт, а шифротексты – от 20 326 до 65 498 байт. BIKE имеет одни из самых больших открытых ключей и шифротекстов среди всех представленных кандидатов, хотя у размера его закрытого ключа средний рейтинг. Довольно интересная его характеристика, которую имеют немногие другие постквантовые шифры, – зашифрованные с помощью BIKE данные имеют узнаваемую «подпись», которая может быть использована злоумышленниками и средствами безопасности для распознавания и манипулирования ею. Обычно в большинстве шифрований нельзя сказать, какой шифр использовался, что усложняет атаки любого рода. С BIKE дело обстоит иначе. BIKE является частью проекта Open Quantum Safe.

Для получения дополнительной информации о BIKE посетите https://bikesuite.org.

Classic McEliece

В 1978 году Роберт Дж. Макэлис (Robert J. McEliece) создал шифр с открытым ключом, который выдерживал атаки на протяжении более чем 40 лет. Это шифр на основе кода Гоппа. Статью Макэлиса 1978 года, представившую открытый ключ шифрования McEliece, можно найти здесь: https://ipnpr.jpl.nasa.gov/progress_report2/42-44/44N.PDF.

Примечание Часто рядом с упоминанием системы McEliece можно встретить и название криптосистемы Niederreiter. Последняя намного быстрее и может использоваться для цифровых подписей.

Оригинальный шифр McEliece является быстрым (по сравнению с RSA) и квантовоустойчивым, но требует больших размеров ключа (300 КБ и более, часто свыше 1 МБ). За эти годы несколько разных команд пытались изменить его так, чтобы уменьшить требуемый размер ключа, но в конечном итоге почти все новые реализации оказались гораздо менее безопасными, чем оригинал.

Команде, в которую входит высококвалифицированный криптограф и разработчик программ безопасного кодирования Даниэль Дж. Бернстайн (Daniel J. Bernstein) и которая представила NIST этот ключ, удалось изменить шифр McEliece так, что при меньших размерах он сохраняет квантовую устойчивость с нулевыми ошибками дешифрования. Для 2-го тура конкурса NIST требуется следующая реализация безопасности: размеры закрытых ключей – от 6452 до 13 892 байт, открытых ключей – от 261 120 до 1 044 992 байт, а шифротекстов – от 128 до 240 байт.

Ключ Classic McEliece имел второй по величине размер открытого ключа, превзойденный только ключом NTS-KEM. Оба имели наименьший результи-

рующий шифротекст. Хотя они все еще были значительно больше, чем традиционные шифры с открытым ключом и большая часть их постквантовых конкурентов, они были очень управляемы при использовании современных компьютеров и сетей. Шифр Classic McEliece имеет дополнительное преимущество – очень малый размер зашифрованного текста, оставаясь довольно быстрым в основанных на аппаратуре реализациях.

Для получения дополнительной информации о Classic McEliece посетите https://classic.mceliece.org.

Примечание Если вы заинтересованы в криптографии или написании безопасного кода, учтите: все, что пишет или разрабатывает Даниэль Бернстайн (Daniel J. Bernstein), заслуживает большого уважения. Он сотни раз выступал с докладами, написал почти столько же статей и разработал много разных, очень безопасных, с низким количеством ошибок программ. Бернстайн изобрел термин *постквантовая криптография* и был одним из первых лидеров отрасли, которые взялись поведать миру, что нас ждет в связи с развитием этого направления. Читателям предлагается посетить персональный сайт Даниэля Бернстайна: https://cr.yp.to.

CRYSTALS-Kyber

CRYSTALS («КРИСТАЛЛЫ») (Cryptographic Suite for Algebraic Lattices, криптографический набор для алгебраических решеток) – хорошо защищенный EUF-CMA алгоритм цифровой подписи, который включает две решетки на основе криптографии примитива: Kyber, защищенный CCA KEM, и Dilithium. CRYSTALS-Kyber основан на более ранних задачах шифрования MLWE, но использует в качестве открытого ключа квадратные и прямоугольные матрицы вместе с кольцами многочленов (https://en.wikipedia.org/wiki/Polynomial_ring), а не целые числа. Он имеет хорошую производительность и может быть легко масштабирован, когда требуются ключи большего размера. По словам многонациональной команды разработчиков, Kyber-512 имеет защиту безопасности, примерно эквивалентную AES-128 (классификация уровня безопасности NIST 1), Kyber-768 имеет безопасность, примерно эквивалентную AES-192 (классификация уровня безопасности NIST 3), а Kyber-1024 – защиту, примерно соответствующую AES-256 (классификация уровня безопасности NIST 5). Для 2-го тура конкурса NIST требуется следующая реализация безопасности: размеры закрытых ключей – от 1632 до 3168 байт, открытых ключей – от 800 до 1568 байт, а зашифрованных – от 736 до 1568 байт. CRYSTALS-Kyber последовательно ранжируется со средним и меньшим размерами ключей. Это часть открытого проекта Open Quantum Safe.

Для получения дополнительной информации о CRYSTALS см. https://pq-crystals.org/ и https://pq-crystal.org/kyber/index.shtml.

FrodoKEM

FrodoKEM – это CCA-безопасная и CPA-безопасная криптосистема на основе решетки с решением задачи LWE для ее защиты. Она имеет несколько бóль-

шие размеры ключей и меньшую производительность по сравнению с другими решетчатыми моделями (с кольцами LWE). Поставляется в трех ключевых размерах:

- FrodoKEM-640, которая претендует на безопасность, эквивалентную AES-128;
- FrodoKEM-976, претендующая на безопасность, эквивалентную AES-192;
- FrodoKEM-1344, которая претендует на безопасность, эквивалентную AES-256.

Для 2-го тура конкурса NIST требуется следующая реализация безопасности: размер закрытых ключей – от 19 888 до 43 088 байт, открытых ключей – от 9616 до 21 520 байт, а размер шифротекстов – от 9720 до 21 632 байт. FrodoKEM имеет один из самых больших открытых ключей и размеров текста.

В команде FrodoKEM много сотрудников Microsoft и Google. Команда взяла предыдущую версию FrodoCCS, которая является схемой обмена эфемерными ключами, и усовершенствовала ее, чтобы сделать IND-CCA-KEM. FrodoKEM – более простая версия, в которой меньше кода. Это делает ее, вероятно, более надежной и устойчивой к атакам, а при нахождении ошибки ее легче устранить. Это часть проекта Open Quantum Safe.

Построение представленного FrodoKEM также является «постоянным во времени». Не нужно повторно оптимизировать безопасность, чтобы предотвратить определенные типы «подслушивающих» атак. *Постоянное время* – криптографическое свойство защиты, разработанное, чтобы сделать менее опасными многие типы атак синхронизации побочного канала. Проще говоря, по разнообразным причинам многие шифры и многие ранние реализации шифров вводят задержки непосредственно в центральный процессор (CPU) в зависимости от того, с чем связан шифр (скажем, оценкой ключа шифра). Любой процесс шифрования, который изменяет время обработки в зависимости от длины некоторой исследуемой переменной, создает ощутимую и предсказуемую разницу во времени, позволяющую злоумышленнику лучше оценить закрытую информацию. Эта информация может позволить злоумышленникам сделать предположения, чтобы ускорить атаку. В мире криптографии эти типы получаемой информации называются *кормушками* (cribs). Отличную базовую дискуссию о времени атак по побочным каналам можно найти здесь: www.chosenplaintext.ca/articles/beginners-guide-constant-time-cryptography.html. Для получения дополнительной информации о FrodoKEM см. https://frodokem.org/.

Примечание Джопп В. Бос (Joppe W. Bos), криптографический исследователь компании NXP Semiconductors (Лёвен, Бельгия), является автором трех постквантовых шифров: FrodoKEM, CRYSTALS-Kyber и NewHope.

HQC

HQC (Hamming Quasi-Cyclic, квазициклический код Хемминга) – это схема шифрования с открытым ключом, основанная на сложности декодирования случайных квазициклических кодов, использующих коды Боуза–Чоуд-

хури–Оккенгема (Bose–Chaudhuri–Hocquenghem, BCH) с кодом повторения. Коды BCH были изобретены в 1959 и 1960 годах и рассматривались как коды исправления «ошибок», что облегчает декодирование при наличии корректных ключей. Коды BCH широко используются в компакт-дисках, DVD-дисках, штрих-кодах и компьютерных устройствах хранения в течение десятилетий. Несмотря на то что HQC применяет «легко декодируемые» коды BCH, он подвержен «ненулевым» (но все же очень редким) сбоям расшифровки.

HQC имеет вероятность 2^{-128}, что любой конкретный раунд дешифрования не приведет к исходному текстовому содержанию. Компьютеры, как правило, допускают много других гораздо более распространенных ошибок, которые имеют намного более высокую вероятность того, что это произойдет, но мы принимаем это и широко используем компьютеры. Отказ означал бы, что для успеха могут потребоваться дополнительные раунды расшифровки, но эти дополнительные раунды пройдут очень быстро и почти незаметно. Однако малая вероятность все же отлична от нулевой, и потому это следует отметить. Криптографы придерживаются строгих стандартов отчетности. Криптография HQC использует секретный ключ размером 40 байт для всех необходимых реализаций безопасности NIST (который привязан ко второму, маленькому, с тремя другими представлениями). Для 2-го тура конкурса NIST требуется следующая реализация безопасности: размеры открытых ключей HQC – от 3125 до 8897 байт, с шифрованием текста размером от 6234 до 17 777 байт. Как и BIKE, HQC имеет маркеры, которые можно использовать для идентификации HQC-зашифрованного трафика, и он использует эфемерные ключи, чтобы обеспечить идеальную секретность пересылки. Команда HQC по своему составу является многонациональной, и многие из членов команды представили другие алгоритмы на конкурс NIST (например, француз Филипп Габори (Philippe Gaborit)) также работал над BIKE, HQC, RQC и ROLLO).

Для получения дополнительной информации об HQC см. https://pqc-hqc.org.

LAC

Шифр LAC (LAttice-based Cryptosystems, криптосистемы на основе решетки), защищенный CPA и CCA, включает четыре различных LAC-связанных примитива, основанных на полиномиальном обучении с ошибками (poly-LWE) задачи над кольцом. Примитивы шифра LAC:

- LAC.CPA: безопасная схема шифрования с открытым ключом, которая является также основой трех других реализаций;
- LAC.KE: безопасный протокол обмена ключами, который напрямую конвертируется из LAC.CPA;
- LAC.CCA: механизм инкапсуляции защищенного ключа, связанный с LAC.CPA;
- LAC.AKE: протокол обмена ключами с аутентификацией.

LAC может работать на процессорах Intel и ARM (как и большинство кодов, заявленных на конкурс), использует относительно меньшие размеры ключа

и имеет хорошую производительность. Для 2-го тура конкурса NIST требуется следующая реализация безопасности: размеры секретного ключа от 512 до 1204 байт, размеры открытого ключа – от 544 до 1056 байт, а размеры шифротекстов – от 712 до 1424 байт. Это дает LAC четвертые самые маленькие комбинированные размеры ключа и зашифрованного текста среди конкурентов в NIST.

Похоже, что у рецензентов, оценивающих участников конкурса NIST, к безопасности LAC возникает больше вопросов, чем обычно, о чем свидетельствует, например, этот комментарий: https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-1/official-comments/LAC-official-comment.pdf. Однако никто из них пока не решился сказать брейк.

Команда LAC состоит из китайских криптографов. Китайские криптографы участвуют в создании многих квантовоустойчивых алгоритмов и материалов для NIST. Это понятно, потому что Китай является лидером в исследованиях квантовых компьютеров и устройств, квантовой криптографии и защиты.

Для получения дополнительной информации о LAC загрузите https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-1/submissions/LAC.zip.

У команды LAC нет общедоступного веб-сайта, но этот zip-файл содержит много актуальной информации.

LEDAcrypt

LEDAcrypt (Low-dEnsity parity-check coDe-bAsed cryptographic systems, криптографические системы с кодовым контролем с низкой четностью) представляет собой асимметричный шифр, основывающийся на квазициклических кодах с проверкой четности низкой плотности (Quasi-Cyclic Low Density Parity Check, QC-LDPC) и эфемерных ключах. Он был создан в результате слияния LEDAkem/LEDApkc, первого тура и многих улучшений по результатам рассмотрения NIST. LEDAcrypt является модифицированной версией криптосистемы Niederreiter. Коды QC-LDPC позволяют высокоскоростное декодирование и меньшие по размеру пары ключей. Для 2-го тура конкурса NIST требуется следующая реализация безопасности: размеры закрытых ключей – от 452 до 1092 байт, размеры открытых ключей – от 1872 до 8520 байт, а шифротекстов – от 1872 до 4616 байт. LEDAcrypt может обеспечить совершенную секретность передачи и использует SHA-3 (от 256 до 512 бит) для функций хеширования, но, как и многие другие схемы, основанные на коде, подвержен сбоям дешифрования. Команда LEDAcrypt из Италии.

Для получения дополнительной информации о LEDAcrypt смотрите www.ledacrypt.org.

NewHope

NewHope («Новая надежда») – это метод обмена решетчатыми ключами на CCA и CPA, основанными на кольцевом обучении задач с ошибками (ring-LWE). Он имеет четыре версии:

- NewHope512-CPA-KEM;
- NewHope1024-CPA-KEM;

- NewHope512-CCA-KEM;
- NewHope1024-CCA-KEM.

Предполагается, что версия с размерами кольца 512 равна или превышает AES-128, а версия с размером колец 1024 равна или превышает AES-256. Для 2-го тура конкурса NIST требуется следующая реализация безопасности: диапазон размеров секретных ключей версий CCA – от 1888 до 3680 байт, размеры открытых ключей варьируются от 928 до 1824 байт, а диапазон шифротекстов – от 1120 до 2208 байт. NewHope имеет относительно хорошую производительность и подвергся небольшим исследованиям в Google. Это часть проекта Open Quantum Safe.

Для получения дополнительной информации о NewHope смотрите https://newhopecrypto.org.

NTRU

NTRU (N-th degree Truncated Polynomial Ring, «Усеченное полиномиальное кольцо N-й степени») – это быстрое решетчатое KEM, основанное на шифровании по NTRU-схеме (которая существует примерно с 1996 года и хорошо изучена). NTRU была одной из первых ключевых криптосистем, не основанной на факторизации или дискретных логарифмических задачах (после McEliece), и первым асимметричным шифром, который был определен как не подверженный алгоритму Шора. NTRU во 2-м туре NIST – это объединение NTRUEncrypt (шифрование) и NTRU-HRSS-KEM, которые в 1-м туре проходили как отдельные участники. Основные шифры NTRU были запатентованы, но позже, в 2013 году, переданы в общественное пользование.

В терминах практической криптографии NTRU использует решетки с большей, чем средняя решетка, «структурой», что позволяет шифровать и генерировать защищенные ключи значительно быстрее, чем в традиционных системах с открытым ключом, таких как RSA и ECC, и работает быстрее, чем большинство предложений в 1-м туре (хотя и не обгоняет всех конкурентов). Для 2-го тура конкурса NIST требуется следующая реализация безопасности: размер секретного ключа – от 935 до 1590 байт; размеры открытого ключа и зашифрованного текста варьируются от 699 до 1230 байт. NTRU был представлен на конкурс NIST многонациональной командой. Это часть проекта Open Quantum Safe.

Для получения дополнительной информации об NTRU загрузите https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-2/submissions/NTRU-Round2.zip.

NTRU Prime

NTRU Prime – криптосистема с открытым ключом; была создана как экспертная версия NTRU, «подправленная» с целью добавить больше защиты тому, что команда NTRU Prime называет NTRU Classic. Команда NTRU Prime обсудила все возможные проблемы безопасности с решеточной криптографией и NTRU Classic, а затем использовала разные типы колец (https://ntruprime.cr.yp.to/ntruprime-20170816.pdf). Команда NTRU Prime описывает свой шифр

как «эффективную реализацию высоконадежной криптографии на идеальной решетке с инертным модулем группы Галуа» (efficient implementation of high-security prime-degree large-Galois-group inert-modulus ideal-lattice-based cryptography), другие же используют определения вроде «неприводимые, нециклотомические полиномы» (irreducible, non-cyclotomic polynomials) – для объяснения потребовалось бы слишком серьезно углубляться в тему, что не входит в задачу данной книги. Для 2-го тура конкурса NIST требуется следующая реализация безопасности: размеры секретного ключа – от 1518 до 1999 байт, размеры открытых ключей – от 994 до 1322 байт, а шифротекстов – от 897 до 1312 байт.

NTRU Prime устраняет некоторые из наиболее очевидных недостатков NTRU Classic, убирает сбой дешифрования и делает это в постоянное время, чтобы смягчить некоторые атаки побочного канала синхронизации. Хотя команда NTRU Classic представила «улучшенную версию» NTRU Classic, создатели NTRU Prime до сих пор предупреждают о том, что не стоит всецело доверять криптографии на основе решетки, включая их собственную. NTRU Prime представлена в NIST многонациональной командой, куда в числе прочих входит и Даниэль Бернстайн.

Для получения дополнительной информации об NTRU Prime смотрите Https://ntruprime.cr.yp.to.

NTS-KEM

NTS-KEM – это шифр, основанный на варианте кода шифрования KEM с открытым ключом схем McEliece и Niederreiter. Как и многие шифры на основе кода, он требует больших размеров открытого ключа, но, в отличие от предшествующих шифров, способен достичь неразличимости, гарантированной CCA. NTS-KEM использует SHA3-256. Для 2-го тура конкурса NIST требуется следующая реализация безопасности: секретные ключи варьируются в размере от 9248 до 19 922 байт, открытые ключи – от 319 488 до 1419 704 байт, а шифротексты – от 128 до 253 байт. У NTS-KEM самый большой открытый ключ и самый маленький размер зашифрованного текста среди всех конкурентов. К этим значениям приближается только Classic McEliece.

Команда из Великобритании подала заявку на патенты в Великобритании и США, а затем отказалась от них для участия в конкурсе. Текущая версия не является постоянной во времени. Команда под руководством Даниэля Бернстайна утверждала, что Classic McEliece лучше, чем NTS-KEM, однако разработчики NTS-KEM выдвинули опровержение: https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-1/official-comments/Classic-McEliece-official-comment.pdf.

Для получения дополнительной информации об NTS-KEM смотрите https://nts-kem.io.

ROLLO

ROLLO (Rank-Ouroboros, LAKE и LOCKER) – это группа шифров с базовым кодом с проверкой четности низкого ранга (low-rank parity check, LRPC), основанная на слиянии трех других шифров на основе кода из NIST первого

тура: LAKE, LOCKER и Ouroboros-R. LAKE (сейчас называется ROLLO-I) – это защищенный CPA KEM, LOCKER (ROLLO-II) – это CCA-безопасный PKE (шифрование с открытым ключом), и Rank-Ouroboros (ROLLO-III) – это KEM.

LRPC – относительно новый тип кодирования, основанный на метрике ранга, который предлагает высокую производительность и меньшие размеры ключей. Чтобы узнать больше о LRPC, см. https://pdfs.semanticscholar.org/d791/016d78.b1054ce6c756a55ac78909ede25fdb.pdf. Шифры ROLLO – быстрые, с меньшим размером ключа. Для 2-го тура конкурса NIST требуется следующая реализация безопасности: секретные ключи всегда 40 байт, а открытые ключи и зашифрованный текст варьируются в пределах от 465 до 947 байт. ROLLO так же, как и SIKE, по сравнению с конкурентами имеет самые маленькие размеры ключа и шифротекста. Минус в том, что шифры на основе кодов LRPC не были хорошо изучены и не так надежны, как другие. ROLLO представлен французской командой.

Для получения дополнительной информации о ROLLO смотрите https://pqc-rollo.org/.

Round5

Round5 – группа шифров на основе решетки, с общим обучением и округлением (general-learning-with-rounding, GLWR), объединение хорошо изученного обучения с округлением (learning-with-rounding, LWR) и кольцевого обучения с округлением (ring-learning-with-rounding, RLWR) – задач решетки для их защиты. Это слияние двух отдельных кандидатов NIST первого тура: Round2 и Hila5. R5_CPA_KEM – это защищенный CPA KEM, а R5_CCA_PKE – открытый CCA безопасный ключ шифрования. Сам шифр и заявление о его неразличимости довольно-таки удивили некоторых рецензентов, потому что большинство представленных постквантовых KEM обычно CCA-безопасны (т. е. выбраны устойчивые к атакам шифры) и CPA-небезопасны (выбран метод защиты открытого текста).

По сравнению с другими LWR- и RLWR-шифрами, Round5 имеет хорошую производительность с узкой полосой пропускания. Размеры ключа и шифротекста небольшие. Для начала второго тура конкурса NIST требуется следующая реализация безопасности: секретные ключи размером от 16 до 32 байт, открытые ключи – от 634 до 1117 байт, шифротексты варьируются от 682 до 1274 байт. Round5 имеет четвертый наименьший комбинированный размер (после ROLLO, LAC и SIKE). Команду Round5 в основном составляют участники из Нидерландов и сотрудники компании Philips; кроме них туда входит один участник из Великобритании и один из США.

Для получения дополнительной информации о Round5 смотрите https://round5.org.

RQC

RQC (Rank Quasi-Cycle, ранжированный квазицикл) – это шифрованный постквантовый шифр с открытым ключом на основе кода, использующий сложность решения задач декодирования синдрома квазициклического ранга, который работает со случайным рангом кода. RQC применяет коды Га-

бидулина (Gabidulin), обобщение хорошо известных (в кругах криптографов и математиков) кодов Рида–Соломона (Reed–Solomon) для декодирования. Декодирование синдрома считается хорошо понятным, высокоэффективным способом декодирования ошибок, обнаруженных в шумовом канале, или, для непрофессионала, хорошим способом кодирования и декодирования в криптографии, основанной на кодах. Для 2-го тура конкурса NIST требуется следующая реализация безопасности: закрытый ключ всегда 40 байт, открытый ключ – от 853 до 2284 байт, размер шифротекста – от 1690 до 4552 байт. Он имеет низкий, до нулевого, рейтинг ошибки.

Команда RQC в основном из Франции, и шифр частично спонсировался Французским комитетом поставок вооружения (the French Government Defense procurement office).

Больше информации можно получить на сайте https://pqc-rc.org.

SABER

SABER – это решетчатое CPA-безопасное шифрование и CCA-безопасный KEM-пакет, защита которого зависит от сложности решения задач модульного обучения с округлением (module-learning-with-rounding, MLWR). Он предлагает три уровня безопасности:

- LightSABER: постквантовый уровень безопасности, подобный AES-128;
- SABER: постквантовый уровень безопасности, подобный AES-192;
- FireSABER: постквантовый уровень безопасности, подобный AES-256.

Для 2-го тура конкурса NIST требуется следующая реализация безопасности: размеры секретного ключа – в диапазоне от 832 до 1664 бит, размеры открытых ключей – от 672 до 1312 байт, шифротекстов – от 736 до 1472 байт. Он имеет хорошую производительность, гибкость и небольшую полосу пропускания, с меньшим количеством случайностей при обеспечении безопасности. Шифр SABK нельзя использовать для цифровой подписи. Команда, представившая SABER, базируется в Бельгии.

Для получения дополнительной информации о SABER смотрите www.esat.kuleuven.be/cosic/pqcrypto/saber/.

SIKE

Инкапсуляция сверхсингулярного изогенного ключа (Supersingular Isogeny Key Encapsulation, SIKE) – единственный шифр (набор) на конкурсе NIST, основанный на изогении. SIKE PKE – это CCA-безопасная схема шифрования с открытым ключом, а SIKE.KEM – это CPA-безопасный KEM. SIKE основан на изогенной конструкции обмена ключами, известной как *сверхсингулярная изогения Диффи–Хеллмана* (supersingular isogeny Diffie–Hellman, SIDH). Для 2-го тура конкурса NIST требуется следующая реализация безопасности: размер закрытого ключа – от 44 до 80 байт, открытого ключа – от 330 до 564 байт, размер шифротекста – в диапазоне от 346 до 596 байт. SIKE имеет наименьший размер открытого ключа и наименьший размер закрытого ключа. Если рассматривать все три размера вместе взятых, SIKE имеет наименьшие показатели в целом среди всех конкурентов.

Изогенные шифры являются относительно новыми и менее изученными, чем другие типы шифров, хотя авторы SIKE указывают, что исследования изогенных вычислений между эллиптическими кривыми (над конечными полями) велись с 1990-х годов. Вообще, изогенные шифры обладают большим потенциалом, имея сравнительно небольшие размеры ключей, но безопасность и особенно производительность до сих пор выступают предметом жарких дискуссий. Вы можете оценить атмосферу этих споров по поводу SIKE и других изогенных шифров, прочитав комментарии рецензента NIST (https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-1/official-comments/SIKE-official-comment.pdf) в отношении SIKE.

Если сверхсингулярно изогенная криптография выдержит устойчивые методы атаки, то с течением времени она имеет большой шанс стать одним из наиболее популярных квантовоустойчивых шифров. Команда проекта насчитывает участников из разных стран. SIKE является частью проекта Open Quantum Safe.

Для получения дополнительной информации о SIKE смотрите https://sike.org.

ThreeBears

ThreeBears («Три медведя») – это асимметричный шифр обмена открытыми ключами на основе решетки, построенный с использованием варианта MLWE. ThreeBears предоставляет один режим, защищенный только от CPA, и другой режим, защищенный от обоих – и CPA, и CCA. Основное математическое кольцо применяет так называемое псевдомерсенновское простое число. *Мерсенновское простое число* (Mersenne prime), названное в честь французского математика Мерсенна, – это простое число x, для которого $(2^x - 1)$ также является простым числом. Они также часто используются в традиционной криптографии с эллиптическими кривыми. Для получения дополнительной информации о простых числах Мерсенна смотрите https://en.wikipedia.org/wiki/Mersenne_prime. *Простые псевдомерсенновские числа* – это числа Мерсенна с некоторой особенностью: вычитаемый компонент в формуле может быть любым небольшим числом больше 0 (а не только 1). По уверению его создателей, ThreeBears был назван так потому, что его псевдомерсенновское простое число имеет ту же математическую структуру, что и предыдущий шифр, известный как Златовласка (Goldlocks), а также три различных набора параметров с именами BabyBear, MamaBear и PapaBear.

ThreeBears, кроме прочего, использует коды с исправлением ошибок, работает довольно быстро и имеет один из самых низких показателей ожидаемых сбоев обмена ключами по сравнению с конкурентами. Для 2-го тура конкурса NIST требуется следующая реализация безопасности: секретные ключи всегда 40 байт (вторые по наименьшему размеру наряду с тремя другими шифрами) и используемые в качестве начальных (затравочных) значений. Размеры открытых ключей варьируются от 804 до 1584 байт, шифротекста – от 917 до 1697 байт.

Самый большой вопрос в отношении ThreeBears – это являются ли решетки на основе простых чисел Мерсенна более или менее устойчивыми к атакам на шифры, чем у других шифров на основе решетки. Этот факт

признает и создатель шифра Майк Гамбург (Mike Hamburg) из Стэнфордского и Гарвардского университетов. ThreeBears поддерживается компанией Rambus, Inc.

Для получения дополнительной информации о ThreeBears смотрите https://shiftleft.org/papers/threebears/ и www.shiftleft.org/papers/threebears/threebears-spec.pdf.

Один или несколько из этих официальных кандидатов NIST 2-го тура, скорее всего, в ближайшие несколько лет станут стандартами США квантового асимметричного шифрования. В табл. 6.3 сведена информация о постквантовом асимметричном обмене открытыми ключами и KEM, а также размерах ключа и шифротекста для наиболее популярных представлений классификации по уровню безопасности NIST (т. е. уровни 1, 3 и 5). Указанные значения взяты из документа NIST по представленным шифрам и/или подтверждены членом команды, представившей шифр. Они могут относиться только к одной или нескольким версиям шифров, даже если сообщается о большем количестве версий. Представленные данные не всегда отражают самые большие или самые маленькие значения конкретного параметра для конкретной версии шифра, – в таблицу включены наиболее показательные величины из числа возможных. Экстремальные значения некоторых версий не могут быть адекватно представлены. В некоторых случаях размеры секретного ключа могут включать размеры открытых ключей – другими словами, они могут не указываться в документации явно.

Общие замечания по размерам ключей PKE, KEM и шифротекста

Вот некоторые общие сравнительные наблюдения о размерах различных PKE- и KEM-ключей и шифротекстов, которые указаны в табл. 6.3.

- Нет конкретного типа алгоритма шифра (код, решетка, многомерный), доказавшего как класс, что имеет самые большие или самые маленькие размеры. Почти всегда были представлены классы с наименьшим и наибольшим размерами, причем большинство оказывается посередине. Это идет вразрез с тем, что предсказывали многие теоретические дискуссии, с различными типами шифров, имеющих постоянно большие или меньшие размеры ключей. Появились определенные модели, которые в целом поддерживают эту аргументацию, но и исключений достаточно много для того, чтобы можно было говорить о четкой зависимости.
- Наименьшие закрытые и открытые ключи (и вторые по размеру наименьшие шифротексты) имеют SIKE, а за ним ROLLO.
- Самые большие секретные ключи у Classic McEliece, FrodoKEM и NTS-KEM.
- У четырех шифров (BIKE, Classic McEliece, FrodoKEM и NTS-KEM) самые большие размеры открытых ключей (приведены в порядке убывания).
- Размеры ключа Classic McEliece и NTS-KEM выпадают из общей шкалы по сравнению с другими 15 шифрами, но они также имеют самые маленькие шифротексты (следуют сразу за SIKE и ROLLO).

Таблица 6.3. Второй тур конкурса NIST. Размеры PKE и KME, ключей и шифротекстов уровней 1, 3 и 5 по классификации безопасности NIST

Eq. AES-128 NIST 1				Eq. AES-192 NIST 3			Eq. AES-256 NIST 5		
Алгоритм	**SK**	**PK**	**CT**	**SK**	**PK**	**CT**	**SK**	**PK**	**CT**
BIKE	1988	20 326	20 326	3090	39 706	39 706	4110	65 498	65 498
Classic McEliece	6452	261 120	128	13 568	524 160	188	13 892	1 044 992	240
CRYSTAL-Kyber	1632	800	736	2400	1184	1088	3168	1568	1568
FrodoKEM	19 888	9616	9720	31 296	15 632	15 744	43 088	21 520	21 632
HQC	40	3125	6234	40	5884	11 749	40	7989	16 984
LAC	512	544	712	1024	1056	1188	1024	1056	1424
LEDAcrypt	452	1872	1872	644	3216	3216	764	4616	4616
NewHope	1888	928	1120	–	–	–	3680	1824	2208
NTRU	935	699	699	1234	930	930	1590	1230	1230
NTRU Prime	–	–	–	1763	1158	1039	–	–	–
NTS-KEM	9248	319 488	128	17 556	929 760	162	19 992	1 419 704	253
ROLLO	40	465	465	40	590	590	40	947	947
Round5	16	634	682	24	909	98	32	1178	1274
RQC	40	853	1690	40	139	2766	40	2284	4552
SABER	832	672	736	1248	992	1088	1664	1312	1472
SIKE	44	330	346	62	462	486	80	564	596
ThreeBears	–	–	–	–	–	–	40	1584	1697

Обозначения: SK – размер закрытого ключа, PK – размер открытого ключа, CT – размер шифротекста. Все величины в байтах.
Примечание: цифры представляют реализации отдельных шифров в наборе шифров.

- Самые большие шифротексты были у BIKE, FrodoKEM и HQC.
- Наименьшие размеры комбинированного ключа и зашифрованного текста у SIKE, затем следуют ROLLO и Round5.

Отличная онлайновая веб-страница сравнения постквантовых ключей NIST: https://pqc-wiki.fau.edu/w/Special:DatabaseHome.

Каждый алгоритм также оценивается по ряду других характеристик, кроме размеров ключа и шифротекста. В том числе учитываются:

- производительность (как в программном, так и в аппаратном исполнении);
- размеры хранилища (время выполнения и на носителе);
- генерация ключей;
- скорость шифрования;
- скорость расшифровки;
- сложность;
- простота реализации;
- процент отказов;
- возможность обеспечить охрану.

Все эти и другие факторы каждого представленного шифра рассматриваются заинтересованными сторонами. Шифры, которые лучше всего справляются с этими факторами, наряду с устойчивой безопасностью перейдут в 3-й тур и/или, в конце концов, будут рассмотрены как возможность для выбора постквантового стандартного шифра NIST.

Квантовоустойчивые схемы цифровой подписи

Квантовоустойчивые схемы цифровой подписи – это криптографические цифровые подписи, которые не являются чрезмерно чувствительными к квантовым компьютерам, использующим квантовые алгоритмы. Они не используют основанные на квантах свойства, чтобы отразить атаки. Существует более десятка квантовоустойчивых схем цифровой подписи, хотя только один или несколько из девяти кандидатов второго тура NIST, вероятно, будут признаны NIST федеральным стандартом. Вот участники второго тура конкурса NIST в алфавитном порядке:

- CRYSTALS-Dilithium;
- FALCON;
- GeMSS;
- LUOV;
- MQDSS;
- Picnic;
- qTESLA;
- Rainbow;
- SPHINCS+.

Примечание Существует как минимум три другие основные схемы квантовоустойчивой цифровой подписи, которые не соответствуют критериям представления на конкурс NIST: подписи Leighton-Micali (LMS), расширенная подпись Merkle Signature Scheme-MT (eXtended Merkle Signature Scheme-MT, XMSS), а также блок-цепочечные постквантовые подписи (Blockchained Post-Quantum Signatures, BPQS). По крайней мере, первые две сохраняют текущее состояние, что может вызвать проблемы, если их неправильно обработать во время операций восстановления данных, а схема BPQS использует относительно непроверенный гибридный подход, который называют мостом между сохранением и несохранением текущих состояний. Вы можете прочитать больше о XMSS и LMS на https://eprint.iacr.org/2017/349.pdf и BPQS на https://eprint.iacr.org/2018/658.pdf.

CRYSTALS-Dilithium

CRYSTALS (Cryptographic Suite for Algebraic Lattices, криптографический набор для алгебраических решеток) включает в себя две решетки на основе криптографических примитивов: Kyber, CCA-безопасный KEM и Dilithium (рассмотренный ранее), EUF-CMA – строго безопасный алгоритм цифровой подписи и CRYSTALS-Dilithium.

Схема CRYSTALS-Dilithium основана на MLWE, которую, как утверждают авторы, можно рассматривать в качестве решетки между неструктурированным LWE и структурированным RLWE. Она также использует интерактивную идею доказательства знания, известную как *Fiat-Shamir with Aborts* (https://www.iacr.org/archive/asiacrypt2009/59120596/59120596.pdf), которая похожа на системы ZPK, упоминавшиеся выше, но все же имеет некоторые отличия. В системе *интерактивного доказательства знания* (interactive proof-of-knowledge system) прувер не доказывает верификатору, что он знает значение *x*. Третий процесс, известный как *экстрактор знаний* (knowledge extractor), проверяет верификатор. Смотрите https://en.wikipedia.org/wiki/Proof_of_knowledge для получения более подробной информации об интерактивных теориях и системах доказательства знаний.

Dilithium создает относительно небольшие цифровые подписи и открытые ключи, обеспечивая уровень AES-128 или бóльшую безопасность. Для 2-го тура конкурса NIST требуется следующая реализация безопасности: размеры закрытого ключа – 64 байта для всех реализаций (NIST Security Levels 1, 2 и 3), размеры открытого ключа – от 1184 до 1760 байт, а размеры сигнатур – от 2044 до 3366 байт. Как и другие квантовоустойчивые цифровые подписи, Dilithium начинается с небольшого закрытого ключа, в данном случае 64-битного, который является просто начальным значением, псевдослучайно переходящим в другое значение, которое алгоритм затем использует для генерации открытого ключа и цифровой подписи.

Если оценивать размер квантовоустойчивых цифровых подписей, а не какую-либо другую характеристику, то размеры, которые для целей сравнения значат больше всего, – это открытый ключ и полученная цифровая подпись (и их общие комбинированные размеры). «Закрытый ключ» часто может быть увеличен или уменьшен. Увеличение размера закрытого ключа

исходной версии начального значения или вычисление большего значения, фактически используемого для реальной работы, обычно, по крайней мере хотя бы немного, снижает производительность, и наоборот. Применяющие ключ того или иного размера чаще могут выбирать оптимальное соотношение безопасности и производительности, увеличивая или уменьшая ключ и получая в результате соответствующую ценность подписи.

NIST предложил отправителям выбирать конкретные значения для соответствия требованиям NIST к разным уровням безопасности. Команды иногда немного модифицировали свой алгоритм или значения, чтобы получить улучшенное соотношение размер / эксплуатационная характеристика. Это часть того, что NIST делает «конкурсом». Конкуренция улучшает многие алгоритмы, или, по крайней мере, конкурсанты более вдумчиво относятся к своим конкретным предложениям.

Интересно, что после того, как реализация CRYSTALS-Dilithium была представлена NIST в 1-м туре, рецензенты обнаружили слабость, которая оказалась простой двухстрочной ошибкой переноса кодирования в CRYSTALS-Dilithium RNG – ошибкой, которую разработчики признали и исправили быстрым обновлением. Дается шанс и другим командам при желании рассмотреть все иные представленные алгоритмы, и это может помочь улучшить их. Хорошие криптографические алгоритмы поддерживаются и улучшаются в открытом доступе. Не следует доверять создателям криптографии, которые держат свои алгоритмы в секрете и не позволяют просматривать и тестировать их. Это никогда не являлось хорошим признаком безопасности. Команда Dilithium многонациональна; в нее входят сотрудники IBM и Google. Это часть проекта Open Quantum Safe.

Для получения дополнительной информации о CRYSTALS смотрите https://pq-crystals.org/ и https://pq-crystal.org/dilithium/index.shtml.

FALCON

FALCON (FAst fourier Lattice-based COmpact signatures over NTRU) – это NTRU-решетчатый алгоритм цифровой подписи, основанный на решении задач с коротким целым числом (short integer solution, SIS) (как и qTESLA). SIS-задачи очень трудны для решения, хотя большинство криптографий на основе решетки все же используют кратчайшие векторные задачи (shortest vector problems, SVP). Алгоритм FALCON основан на работе 2008 года, которая привела к созданию общего фреймворка, называемого Gentry, Peikert и Vaikuntanathan (GPV) – защищенного хеш-кода схемы подписи на основе решетки. В ней также используется арифметика с плавающей точкой с точностью 53 бита.

Dilithium и qTESLA опираются на парадигму Fiat-Shamir, тогда как FALCON использует конкурирующую парадигму hash-then-sign (хеш-затем-подпись). Алгоритмы, основанные на первом, опираются на системы доказательства знаний и могут иметь проблемы с безопасностью подписания длинных сообщений. Алгоритмы hash-then-sign сначала хешируют сообщение (и получают намного более короткий результат хеширования) и вместо сообщения подписывают хеш-результат.

Примечание CRYSTALS-Dilithium основан на Module-SIS, который похож на Ring-SIS, однако есть и отличия. По существу, это очень сложные для решения математические задачи, одни сложнее других. Если вас интересуют математические нюансы и различия в работе, можете прочитать https://eprint.iacr.org/2012/090.

FALCON разрабатывался специально для обеспечения хорошей производительности, особенно в условиях ограниченного объема памяти. Создатели FALCON намеренно позиционировали свой алгоритм как сильного соперника алгоритмам с наименьшим открытым ключом и размером подписи, однако он использует математику с плавающей запятой (что уменьшает общую производительность на платформах, которые не поддерживают этот тип математики).

Для 2-го тура конкурса NIST требуется следующая реализация безопасности (FALCON представлен только для уровней NIST 1 и 5): размеры закрытых ключей FALCON – от 1280 до 2304 байт, открытые ключи – в диапазоне от 897 до 1793 байт, а размер цифровой подписи – от 617 до 1233 байт. По утверждениям его создателей, FALCON-512 с открытым ключом размером 897 байт и цифровой подписью 617 байт имеет безопасность, эквивалентную RSA 2048 бит (которая имеет открытые ключи и подписи 256 байт). Команда разработчиков FALCON многонациональна. Основным разработчиком является Томас Порнин (Thomas Pornin).

Для получения дополнительной информации о FALCON смотрите https://falcon-sign.info.

GeMSS

GeMSS (Great Multivariate Signature Scheme, большая схема многомерной подписи) является многопараметрической подписью, защищенной схемой EUF-CMA, обеспечивающей довольно маленькие постквантовые подписи (длиной от 258 до 576 бит, не байт). Для 2-го тура конкурса NIST безопасности: ключи от средних до больших (открытые ключи размером от 352 до 3041 килобайта и закрытые ключи от 13 до 76 килобайт). Это дает GeMSS наименьшую подпись и один из двух самых больших размеров открытого ключа среди всех конкурентов (сходные характеристики имеет Rainbow).

Процесс создания подписи довольно медленный, но проверка подписей быстрая. Схема GeMSS была построена на основе более старой схемы многомерной подписи, известной как QUARTZ, и использует уравнения vHidden Field Equations (-vHFE) с применением модификаторов minus и vinegar. Вы можете прочитать больше о HFE и его модификаторах здесь: https://en.wikipedia.org/wiki/Hidden_Field_Equations. Схема GeMSS была создана французской командой в рамках французского национального проекта.

Для получения дополнительной информации о GeMSS см. www-polsys.lip6.fr/Links/NIST/GeMSS.html.

LUOV

LUOV (Lifted Unbalanced Oil & Vinegar) – это многомерная открытая схема цифровой подписи, которая строится на основе Unbalanced Oil & Vinegar (UOV). UOV создает ключи больших размеров и использует неуникальные ключи. Это может озадачить любого, кто изучал традиционную криптографию. В традиционной асимметричной криптографии каждая пара открытый/закрытый ключ уникальна. В схеме UOV и других многомерных алгоритмах один открытый ключ может иметь миллионы различных закрытых ключей. Здесь не соблюдается отношение 1:1.

LUOV использует модифицированную версию UOV с эффективным закрытым ключом (длиной 32 байта), чтобы позволить иметь меньшие открытые ключи и улучшенную производительность. Закрытые ключи LUOV находятся внизу шкалы. Для 2-го тура конкурса NIST требуется следующая реализация безопасности: размеры открытых ключей от 12 до 76 килобит и цифровые подписи в диапазоне от 311 до 494 байт. LUOV использует псевдослучайный генератор чисел (PRNG). Однако команда разработчиков была единственной командой, не представившей реализации для уровней безопасности NIST 1, 3 или 5. Новый, «поднятый», используемый для защиты метод не был широко оценен и проверен на безопасность, хотя базовый UOV широко изучался ранее (по крайней мере, с 1996 года). LUOV поддерживается бельгийской командой.

Для получения дополнительной информации о LUOV смотрите www.esat.kuleuven.be/cosic/pqcrypto/luov/.

MQDSS

MQDSS (Multivariate Quadratic Digital Signature Scheme, многомерная квадратичная схема цифровой подписи) – это многомерная схема цифровой подписи, которая, как и CRYSTAL-Dilithium, использует обобщенное преобразование Фиата–Шамира (Fiat–Shamir transform) и схему идентификации 5-Pass Saku-moto, Shirai, and Hiwatari (SSH). Это первая многомерная цифровая подпись, которая *вероятно безопасна*, опираясь для защиты только на сложность решения многомерных квадратных уравнений.

Для удовлетворения требованиям безопасности 2-го тура конкурса NIST (уровни с 1 по 4) она имеет чрезвычайно малые размеры открытых и закрытых ключей, от 46 до 64 байт и от 16 до 24 байт соответственно (экземпляр уровня 5 не был представлен). Это очень мало и является соответственно первым или вторым наименьшим размером среди всех конкурентов. К сожалению, MQDSS создает огромные цифровые подписи размером от 20 до 43 килобайт. Это очень много – второе место по величине среди конкурентов, и это даже после изменений, выполненных между 1-м и 2-м турами, удвоивших производительность и вдвое уменьшивших размеры подписи. Это, по сути, постоянное время. MQDSS – многообещающий алгоритм, но требует дополнительных исследований, тестирования и оптимизации. MQDSS имеет многонациональный состав команды.

Для получения дополнительной информации о MQDSS см. http://mqdss.org.

Picnic

Семейство алгоритмов цифровой подписи Picnic является единственным представлением на конкурс NIST, где используется доказательство нулевого знания, которое обеспечивает доказательство единственным сообщением. Согласно команде создателей, оно «не полагается на теоретико-числовые или алгебраические твердые предположения». Как MQDSS и CRYSTALS-Dilithium, Picnic использует модель преобразования Фиата–Шамира для двух своих вариантов (Picnic-FS и Picnic2) и преобразование Unruh в третьем (Picnic-UR). Picnic применяет SHAKE. Для 2-го тура конкурса NIST NIST требуется следующая реализация безопасности: небольшие размеры открытого и закрытого ключей (от 32 до 64 байт и от 16 до 32 байт соответственно), наряду с гораздо бóльшими цифровыми подписями (от 32 до 125 килобайт) и малой производительностью.

Алгоритмы Picnic были протестированы с цифровыми сертификатами TLS и x.509. Это часть проекта Open Quantum Safe. Команда модифицировала OpenSSL (самая популярная в мире криптографическая программа с открытым исходным кодом) с целью использовать Picnic совместно с цифровыми сертификатами на основе Picnic (используя ключи и подписи на основе Picnic). Она использовала Picnic для соединения TLS 1.2 с веб-серверами Apache, возможно, впервые публично объявив о применении этого постквантового алгоритма. OpenSSL пришлось изменить, чтобы принять и использовать бóльшие размеры ключей Picnic. Команда учла, что стандарт TLS поддерживает размеры ключей всего 65 535 байт, поэтому его надо обновить, чтобы упростить поддержку постквантовых алгоритмов. Команда также провела тестирование Picnic, работающего с подключенными устройствами аппаратного модуля безопасности (hardware security module, HSM) приложения PKI, и это было сделано успешно и доказало, что постквантовая криптография может использоваться сегодня в реальных сценариях, требуя лишь незначительных изменений. Picnic был разработан многонациональной командой, включающей исследователей Microsoft.

Для получения дополнительной информации о Picnic смотрите https://microsoft.github.io/Picnic/.

qTESLA

Схема qTESLA основана на ряде предыдущих схем семейства TESLA, включая BG-схему, TESLA, кольцо-TESLA и TESLA#. Это защищенная EUF-CMA схема цифровой подписи на основе решетки RLWE с двумя основными вариантами примитивов: защищенная доказательством (для высоких требований безопасности) и эвристики (для лучшей производительности). Как и другая постквантовая криптография, она опирается на Fiat–Shamir с преобразованием Aborts (с 2012 года), а также на более эффективный вариант схемы (изначально анонсированной в 2014 году) подписи Бай–Гэлбрейта (Bai–Galbraith). Это постоянное время и имеет относительно средние размеры ключей и подписи. Для 2-го тура конкурса NIST требуется следующая реализация безопасности: размеры открытых ключей от 1504 до 6432 байт, закрытые

ключи – от 1216 до 4672 байт, а цифровые подписи – от 1376 до 5920 байт. qTESLA является частью проекта Open Quantum Safe.

В процессе проверки в NIST была выявлена слабость, которую в следующей версии исправили (см. https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-2/official-comments/qTESLA-round2-official-comment.pdf), хотя все еще продолжаются споры на тему, действительно ли проблема устранена. Такого рода жесткие дебаты «прорыва сквозь огонь критики» хорошо влияют на криптографию и выявление возможного победителя, кем бы он ни оказался. Команда создателей qTESLA многонациональна и включает исследователей Microsoft (www.microsoft.com/en-us/research/project/qtesla/).

Для получения дополнительной информации о qTESLA смотрите www.qtesla.org.

Rainbow

Rainbow – это многомерный алгоритм цифровой подписи, защищенной EUF-CMA, использующей многослойную реализацию Unbalanced Oil & Vinegar. Предложенный алгоритм содержит несколько вариантов, максимизированных по производительности, размеру или безопасности. Он использует алгоритм хеширования SHA-2 от 256 до 512 бит в зависимости от соответствия классификации безопасности. Генерация подписи очень быстрая, а размеры подписи короткие. Для 2-го тура конкурса NIST требуется следующая реализация безопасности: закрытые ключи – от 93 до 1227 килобайт, открытые ключи – от 149 до 1705 килобайт, а подписи – от 512 до 1632 бит (не байт). Как и GeMSS, Rainbow в числе самых маленьких подписей среди конкурентов, но при этом размер закрытых и открытых ключей один из самых больших. Размеры ключей можно уменьшить, но это приведет к снижению общей производительности.

С точки зрения безопасности Rainbow является одним из наиболее проверенных постквантовых алгоритмов. Он был создан в 2005 году, а последняя успешная атака, которая потребовала изменения кода, была выполнена в 2008 году. И вот уже более 10 лет случаи успешных атак не отмечались. Несмотря на это, исследователи продолжают поиск слабых мест алгоритма, как о том свидетельствует статья 2018 года: www.hindawi.com/journals/scn/2018/2369507/. Rainbow был создан и представлен многонациональной командой.

Для получения дополнительной информации загрузите https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-2/submissions/Rainbow-Round2.zip.

SPHINCS+

SPHINCS+ представляет собой схему цифровой подписи на основе хеша без сохранения состояния с тремя вариантами. Она основана на улучшенной версии SPHINCS, представленной в 2015 году. Улучшения были сосредоточены на снижении размеров цифровой подписи. Это гибкая структура с более чем 36 комбинациями вариантов, включая:

- SPHINCS+-SHAKE256;
- SPHINCS+-SHA-256;
- SPHINCS+-Haraka.

В основе SPHINCS+ лежат давно известные и используемые цифровые подписи на основе хеш-функции, впервые созданные в конце 1970-х годов (наряду с первыми асимметричными шифрами). SPHINCS+ – это квантовоустойчивое улучшение представленной в 2017 году в качестве первой квантовоустойчивой схемы цифровой подписи. Схема SPHINCS + не сохраняет состояния, что важно.

Создатели SPHINCS+ сделали это, имея для подписи на верхнем уровне открытую/закрытую пару ключей (на основе неизмененной XMSS), которая подписывает и проверяет другие, нижние пары псевдослучайных ключей, выполняющих саму подпись. Авторы называют это *гипердеревом* (по сравнению со стандартным деревом Меркла), основанным на использовании метода нескольких подписей в нижней части гипердерева (именно это отличает схему от хеш-подписи). В корневом узле гипердерева один многократно используемый закрытый ключ в качестве начального значения, которое затем изменяется псевдослучайной функцией для генерации пар ключей нижнего узла.

Схема SPHINCS+ использует SHA256, SHAKE256 или Haraka и представлена с небольшой подписью и более быстрыми версиями. Более быстрые версии имеют большие сигнатуры для ключей тех же размеров. Для 2-го тура конкурса NIST требуется следующая реализация безопасности: открытые ключи – от 16 до 32 байт, закрытые ключи – 64 байта и размер цифровых подписей – от 8080 до 49 216 байт. Таким образом, схема SPHINCS+ имеет одну из самых длинных подписей на конкурсе.

SPHINCS+ была специально разработана консервативной. Поскольку она основана на хеше, она не восприимчив к алгоритму Шора и в основном вызывает беспокойство относительно алгоритма Гровера. Единственная главная угроза – криптографическая атака на саму хеш-функцию (что верно для любого метода подписи, который использует начальный хеш сообщения). К сожалению, SPHINCS+ основана на хеш-подходе, что также означает, что она относительно медленная по сравнению с большинством конкурентов и генерирует более длинные цифровые подписи.

Создание SPHINCS+ финансировалось Европейской комиссией посредством включения ее в программы «Информационные и коммуникационных технологии» (ICT) и гранта Национального научного фонда США. Схема SPHINCS+ была создана многонациональной командой, в которую вошли ведущие исследователи Андреас Хюльсинг (Andreas Hülsing) и Даниэль Дж. Бернстайн (Daniel J. Bernstein). Для получения дополнительной информации о SPHINCS+ смотрите https://sphincs.org.

Как можно было видеть, создано много квантовоустойчивых алгоритмов, которые прошли во 2-й тур NIST и находятся на этапе оценки. В табл. 6.4 приведены различные схемы цифровой подписи с указанием размеров их ключей и подписей.

Таблица 6.4. Второй тур конкурса NIST. NIST-классификация безопасности размеров ключей алгоритмов цифровой подписи

Eq.AES-128 NIST 1				**Eq.AES-192 NIST 3**			**Eq. AES-256 NIST 5**		
Алгоритм	**SK**	**PK**	**Sig**	**SK**	**PK**	**Sig**	**SK**	**PK**	**Sig**
CRYSTALS-Dilithlum	64	1184	2044	64	1760	3366	–	–	–
FALCON	1280	897	617	–	–	–	2304	1793	1233
GeMSS	13K	352K	258b	34K	1238K	411b	76K	3041K	576b
LUOV	–	–	–	–	–	–	32	75K	494
MQDSS	16	46	20854	24	64	43728	–	–	–
Picnic	16	32	32 838	16	48	74 134	32	64	128 176
qTESLA (Heuristic)	126	1504	1376	2368	3104	2848	4672	6432	5920
Rainbow (cyclical)	93K	14K	512b	51K	711K	1248b	1227K	170K	1632b
SPHINCS+ (small)	64	16	8080	64	24	17 064	64	32	29 792

Обозначения: SK – размер закрытого ключа, PK – размер открытого ключа, Sig – размер подписи.
Примечание 1: размеры в байтах, если не указано иное. K – килобайты, b – биты.
Примечание 2: цифры точны только для конкретных алгоритмов реализации в каждом криптографическом наборе.

Представленные значения взяты из документов команд, участвующих в конкурсе NIST, и могут отражать одну или несколько версий алгоритма, даже если сообщается о большем количестве версий. Для конкретной схемы не всегда указываются самые большие или самые маленькие величины – иногда приведены самые показательные. Экстремальные значения некоторых версий могут быть представлены неадекватно.

Общие замечания о ключе и размерах подписи

Вот некоторые общие сравнительные наблюдения о различных ключах цифровой подписи и размерах подписи, указанных в табл. 6.4.

- Не существует определенного типа схемы алгоритма (хеш, решетка, многомерный или ZKP) как класса, который твердо доказывает наличие самых больших или самых маленьких размеров. Были почти всегда представлены размеры каждого класса в наименьших и наибольших величинах, причем большинство находится между ними.
- Самые маленькие закрытые ключи у LUOV и Picnic, за которыми следует SPHINCS+. У Picnic и SPHINCS+ также наименьшие размеры открытых ключей.
- Самые большие закрытые и открытые ключи, безусловно, принадлежат GeMSS и Rainbow, но они же имеют самые маленькие подписи (единственные, измеренные в битах, а не в байтах).
- Самые большие подписи у Picnic, за которым следуют SPHINCS+ и MQDSS.

Каждый алгоритм также рассматривается по многим другим характеристикам, включая:

- производительность (как в программной, так и в аппаратной реализации);
- размеры памяти (время выполнения и носитель);
- генерацию ключей;
- скорость шифрования;
- скорость расшифровки;
- сложность;
- простоту реализации;
- процент отказов;
- возможность обеспечить охрану.

Каждый представленный алгоритм криптографии рассматривается заинтересованными сторонами с точки зрения соответствия его этим и другим факторам. Те алгоритмы, которые получили наивысшую оценку, будут представлены в третьем туре и/или в конечном итоге предложены NIST в качестве стандарта постквантовой цифровой подписи.

Рекомендуемые предостережения

Постквантовая криптография необходима в мире, в котором большая часть нашей традиционной криптографии может быть взломана. Защита будет до-

стигнута за счет увеличения размера ключа традиционных шифров и реализации как квантовоустойчивой, так и квантовой криптографии. Мы будем сначала пользоваться квантовоустойчивой криптографией, а за ней последует квантовая.

Это будет сражение за безопасность. У нас не будет распространенной, дешевой и доступной квантовой криптографии, пока не будет достаточно дешевых квантовых компьютеров и соответствующих процедур обработки, которые производители могли бы создавать, а массовый клиент мог бы себе позволить покупать. Но когда это случится, мы все, вероятно, будем использовать квантовую криптографию.

Однако до того, как это произойдет, квантовых компьютеров и процессоров будет достаточно, чтобы обладающие необходимыми финансами противники атаковали нашу традиционную квантововосприимчивую криптографию. Использование квантовоустойчивой криптографии – наш мост от настоящего к будущему. Мы будем вынуждены использовать квантовоустойчивую криптографию как промежуточный вариант защиты.

Существует, однако, несколько весомых причин, по которым люди не должны необдуманно торопиться и преждевременно переходить к квантовоустойчивой (или квантовой) криптографии. Есть, по крайней мере, три основных препятствия: отсутствие стандартов, проблемы с производительностью и отсутствие проверенной защиты.

Недостаток стандартов

В этой главе основное внимание уделяется NIST и попыткам выбрать постквантовый криптографический стандарт. В настоящее время на рассмотрении находится 26 предложений по криптографии для стандарта США, и только два (или еще несколько) станут победителями. Если вы сейчас решите реализовать определенный квантовоустойчивый алгоритм, есть большая доля вероятности, что вы не выберете тот, который со временем станет новым стандартом.

В таком случае вы всегда сможете переключиться на новые стандарты, как только они станут известны, или оставаться с выбранной вами (нестандартной) реализацией. История показывает, что последний вариант очень неэффективен и значительно подорвет вашу безопасность и/или явится операционным риском. Продвигаться вперед с нестандартным алгоритмом может быть рискованно, потому что часто есть веские причины, по которым конкретный алгоритм не был выбран в качестве возможного стандарта (например, его предполагаемая защита безопасности или проблемы с производительностью).

Переход от преждевременно выбранного постквантового алгоритма к новым стандартам, безусловно, более приемлем для продвижения вперед, но, вероятно, увеличит общие затраты. Вам следует начать экспериментировать с реализацией квантовоустойчивой криптографии, но будьте осторожны с полным развертыванием производства. Вы, по-видимому, не захотите тратить слишком много денег, встав на путь, который может оказаться неправильным. Лучший выбор – начать проводить ограниченные эксперименты и развертывание производства с несколькими надежными квантовоустой-

чивыми алгоритмами и убедиться, что продукты, которые вы сейчас приобретаете, являются *криптоперестраиваемыми*. Криптоперестраиваемость означает, что любой существующий криптографический алгоритм, который используется сейчас, по мере необходимости легко заменить на другой. Подробнее об этом – в главе 9 «Готовимся сейчас».

Проблемы производительности

Даже если квантовоустойчивый криптографический стандарт имеет меньшие размеры ключей, для создания и проверки ключей часто требуются усилия, намного бóльшие, чем при традиционной криптографии. Вот почему конкурс NIST требует много тестов производительности, и авторы изо всех сил стараются оптимизировать скорость работы их алгоритма. Вероятно, NIST выберет тот постквантовый стандарт, который обеспечит хороший компромисс между производительностью и безопасностью, но при переходе к постквантовому алгоритму производительность даже самых быстрых компьютеров и устройств, вероятно, уменьшится. Для глобального перехода на квантовоустойчивый алгоритм в производственной сфере или применительно к конкретному продукту нужно внимательно взвесить все за и против.

Отсутствие проверенной защиты

Что важнее всего, большинство квантовоусточивых криптографических алгоритмов являются относительно новыми и не подверглись проверке в течение необходимого, достаточно длительного периода времени. Есть несколько исключений, но даже создатели большинства квантовоустойчивых алгоритмов не всегда уверены в надежности защитных свойств их алгоритмов. Большинство алгоритмов строятся на основе новой сложной математики, которая нетривиальна, а в ряде случаев почти непостижима. Однако все, что нужно, для того чтобы обеспечить безопасность защиты, – это новый тип атаки или, соответственно, новый предлагаемый квантовоустойчивый алгоритм.

Это особенно верно, если вы проследите историю современной криптографии и используете ее в качестве руководства. Шифрование симметричным ключом с использованием 128-битных ключей считалось очень надежным всего несколько лет назад, но сейчас квантовые компьютеры в сочетании с алгоритмом Гровера наполовину снижают их защиту. Алгоритм Шора готов разрушить большую часть современного шифрования с открытым ключом. Есть много более новых алгоритмов, созданных с момента публикации Шора, разработчики которых утверждают, что он лучше при взломе, чем Шор. Это эволюция. Это прогресс. Единственный трюизм в отношении криптоатак заключается в том, что со временем они становятся все лучше, и криптография, которую они атакуют, только ослабевает. У нас нет никакого способа выяснить в обозримом будущем, является ли квантовоустойчивая криптография безотказной. Мы не узнаем этого, пока не пройдут десятилетия, на протяжении которых каждый из алгоритмов будет выдерживать атаку за атакой и продолжит выживать.

У нас нет никакой возможности узнать, когда появится следующий Шор или произойдет алгоритмический прорыв Гровера, но, скорее всего, даль-

нейшие прорывы будут. И однажды наши квантовоустойчивые алгоритмы ослабеют и рухнут так же, как SHA1, MD5, DES и множество другой криптографии до них. Вероятно, гораздо больше рисков и уязвимостей будет обнаружено во многих реальных реализациях в остальном сильных алгоритмов. Это в порядке вещей: мы редко пишем код без ошибок. Когда кто-то говорит вам, что чего-то нельзя взломать, это неправда.

С учетом сказанного, у нас нет другой, лучшей альтернативы, кроме как верить в то, что квантовоустойчивая криптография даст нам больше защиты, чем традиционная, и будет достаточно долго и надежно защищать нас, пока мы не осуществим полный долгосрочный переход к полностью квантовой криптографии. Просто помните: ничто, даже квантовоустойчивую криптографию, нельзя на 100 % уберечь от взлома или защитить от ошибок. Это риск, который мы все должны принять, пока на смену этой технологии придет нечто лучшее, – как было со всей современной традиционной криптографией, на которую мы опираемся сегодня.

Для дополнительной информации

Вот отличная статья Даниэля Бернстайна 2009 года о постквантовой криптографии: https://pqcrypto.org/www.springer.com/cda/content/document/cda_downloaddocument/9783540887010-c1.pdf.

Для серьезного обсуждения постквантовой криптографии и PKI посетите www.primekey.com/wp-con-tent/uploads/2017/08/post-quantum-algorithms-for-pki.pdf.

Резюме

В этой главе описана квантовоустойчивая криптография и обобщены 26 криптографических алгоритмов, которые были допущены к участию во 2-м туре конкурса NIST по постквантовой криптографии. Мы рассмотрели различные типы квантовоустойчивых алгоритмов, а также их сильные и слабые стороны, а еще обсудили размеры ключей. Как минимум два или более из этих алгоритмов (один для шифрования с открытым ключом и один для цифровой подписи), вероятно, станут новым постквантовым криптографическим стандартом США на следующие несколько лет. Глава 7 будет посвящена квантовой криптографии.

7 Квантовая криптография

Глава 6 посвящена традиционной бинарной криптографии, устойчивой к известным квантовым атакам. Теперь же мы поведем речь о квантовой криптографии, криптографии, которая существует и работает на квантовых устройствах, использующих квантовые свойства. Квантовая криптография устойчива как к известным квантовым атакам, так и к атакам традиционных бинарных компьютеров. Бинарная криптография является приемлемой защитой в постквантовом мире, когда недостаточно широко доступны дешевые квантовые вычисления и сетевые устройства. Но квантовая криптография теоретически намного безопаснее для всех известных атак и, вероятно, станет криптографическим выбором для долгосрочной безопасности. В этой главе мы рассмотрим основные типы квантовой криптографии, в том числе генераторы случайных чисел (RNG), хеши, распределение ключей и цифровые подписи. В главе 8 будут исследоваться квантовые сети.

Этим квантовым криптографическим реализациям присущи все известные квантово-механические свойства, однако четыре конкретных квантовых свойства – суперпозиция, запутанность, эффект наблюдателя и теорема об отсутствии клонирования – являются центральными в том, как квантовая криптография проявляет свою суперзащитную силу. Суперпозиция дает больше возможностей выбора, чем может предложить двоичная цифра. Запутанность защищает обмен криптографическими секретами между уполномоченными сторонами. Эффект наблюдателя и теорема об отсутствии клонирования усложняют возможность скрытого подслушивания. Вы узнаете больше об этих свойствах, когда мы будем обсуждать различные квантовые криптографические реализации.

Важно отметить, что поскольку работающие квантовые компьютеры и устройства все еще относительно молоды, таких систем отнюдь не сотни тысяч. Это не значит, что их вообще нет или что некоторые типы не увеличиваются в количестве день ото дня. На самом деле существует много квантовых устройств (например, квантовые RNG и системы распределения ключей, надо полагать, исчисляются многими тысячами), которые присутствовали в нашей жизни в течение почти двух десятилетий. Но никто не ожидает увидеть квантовую криптографию в том же масштабе, что и ее цифровых двоюродных братьев, по прошествии многих, многих лет. Квантовая криптоустойчивость безусловно одержит верх и будет достаточно безопасной, чтобы объединять нас, когда мы сможем использовать только квантовую криптографию. С учетом этого в данной главе исследуется текущее состояние квантовой криптографии. Некоторые типы квантовой криптографии и устройств

достаточно развиты и могут быть широко использованы уже сегодня, в то время как другие все еще настолько молоды и сложны, что варианты их применения сегодня редки и до́роги. Начнем с обсуждения генераторов случайных чисел, которые криптография использует независимо от типа.

Квантовые RNG

Как показано в главе 5 «Каким будет постквантовый мир?», большинство криптографических функций требуют в качестве критической начальной компоненты своих алгоритмов строго случайных чисел. В традиционном бинарном мире без строго случайных чисел любой алгоритм или функция намного менее безопасны. Существует неудобная правда, которую большинство пользователей компьютеров не знают: традиционный двоичный компьютер не может генерировать действительно случайное число. Мы можем получить только то, что лишь кажется по-настоящему рандомизированным.

Случайное не всегда случайное

Я усвоил этот урок – «случайный не всегда случайный» – более двух десятилетий назад, когда был руководителем информационных технологий крупной конгломератной компании, которая имела небольшой бизнес по тестированию на наркотики профессиональных спортсменов, участвующих в соревнованиях. Среди этих спортсменов были профессиональные теннисисты и гонщики. Победители соревнований всегда проверяются, и все остальные проверяются случайным образом в течение года. Чтобы случайным образом выбрать спортсменов для пробы мочи, каждый месяц спортивная ассоциация или организатор соревнования отправляют компании файл с именами всех спортсменов и другую идентифицирующую информацию под номерами участников. Я загружал файл в программу и запускал функцию создания случайной выборки. Программа случайным образом выводила из входного файла текущего месяца фамилии спортсменов, и мы передавали представительной организации результаты.

Однажды меня позвали на экстренное совещание, потому что ведущий участник гонки был «случайно» выбран два месяца подряд. Я был вызван на совещание высшим руководством, которое отвечало на жалобу гонщика о несправедливой атаке. Я просмотрел код программы (написанной на dBASE III+), не обнаружил ошибок кодирования и сообщил об этом. Менеджмент решил, что высшие должностные лица гоночной организации и представители спортсмена должны напрямую услышать от меня, главного компьютерного эксперта, что двойной выбор в принципе допускается при рандомизации. Каждый человек теоретически может быть выбран два раза подряд, и последовательный выбор гонщика был просто случайностью. Всем было интересно узнать, как работает настоящая случайность, гонщик прошел свой второй тест на наркотик. Тест не выявил никаких проблем, и все, казалось, были рады, дело уладилось… Затем тот же гонщик был выбран в следующем месяце.

Ни он, ни гоночная организация так и не узнали об этом третьем выборе. Мы поняли, что у нас настоящая проблема. Я пересмотрел код и не нашел ошибок. В отчаянии, стремясь выяснить, что происходит, я создал новую программу, которая содержала ту же самую процедуру кодирования рандомизации (тоже написанную в dBASE III+). Ни больше ни меньше. Я использовал числа от 1 до 100, запустил программу 10 000 раз, чтобы узнать, как часто будет выбрано какое-либо конкретное число. В действительно случайном процессе выбора все числа должны были появляться примерно в 1 % результатов с небольшим отклонением. Но когда я запустил программу, несколько чисел появились 15 % раз, одно даже имело более 20 % популярности, а десятки чисел мелькнули лишь эпизодически. Я был ошеломлен. Случайная функция программы не была даже близка к тому, чтобы быть действительно случайной.

Я решил написать программу, не основанную на случайной функции dBASE III+, которая явно имела проблемы. На этот раз я использовал функцию RNG в Microsoft Windows. Я повторил тот же тест, на сей раз с тысячью чисел и десятками тысяч тестовых раундов. И снова был удивлен. Хотя Windows RNG был лучше, перебор и недостаточный выбор все еще проявлялись. Поэтому я написал программу на ассемблере (я научился деассемблировать компьютерные вирусы в конце 1980-х), который использовал характеристики генератора RNG, встроенного в компьютер. Я перезапустил тест. И хотя это было лучше, чем Windows RNG для аппроксимации случайности, она тоже не была полностью случайной. Я обнаружил наличие определенных чисел-фаворитов и исключений, хотя дисбаланс проявлялся в значительно меньшей степени, чем в предыдущих тестах. Именно тогда я понял, что такой вещи, как истинная случайность, в компьютерном мире не существует, а существует лишь *псевдослучайность*. На это указывают многие криптографы и криптографические процедуры, используя термин *псевдо-RNG* (также известный как PRNG). Он лишний раз подчеркивает: на двоичном компьютере никакой случайности не существует.

За три десятилетия, прошедших с момента моего открытия, все задействованные RNG, встроенные в компьютер Microsoft Windows и многие другие пользовательские RNG, включенные в различные программы, были кодированы так, чтобы быть как можно ближе к истинной случайности. Но если бы вы проделали тест, похожий на тот, который проделал я в те давние дни, вы тоже отметили бы наличие чисел-фаворитов и исключений, пусть и в самой малой степени.

Это происходит потому, что традиционные бинарные компьютеры не могут создавать истинно случайные числа. Все бинарные компьютеры имеют один или несколько кристаллов кварца, расположенных на материнской плате и на другом оборудовании для проведения операций в определенное время. Эти кварцевые «часы» вибрируют (создают так называемые осцилляции) постоянное число раз в секунду (каждый отдельный период времени называется *тактом*, или *временны́м циклом*). Все на материнской плате компьютера запускается по сигналу синхронизации, посылаемому ее кварцевыми часами. Современные центральные процессоры (ЦП) имеют свои собственные внутренние временные осцилляции, которые контролируют, когда процес-

сор может сделать что-то (например, переместить такой-то бит в такой-то регистр ЦП, сложить такое-то и такое-то числа, стереть некоторое значение в таком-то регистре и т. д.). Каждое ядро в ЦП может выполнять только одно действие в цикле (если не выполняются параллельные операции), и это действие может происходить строго при каждом такте процессора. Тактовая частота процессора намного выше, чем частота тактов материнской платы, но обычно имеет точное соответствие тактовой частоте материнской платы (например, для каждого такта материнской платы процессор может выполнить в 100 раз больше операций, каждая из которых равномерно распределена по времени). Могут быть и другие таймеры, но часы материнской платы и процессора являются наиболее важными.

Лучшие аппаратные и программные процедуры обеспечивают то, что с виду очень приближено к истинной случайности, но эти результаты не являются действительно случайными. Лучшее, что мы можем сделать, – подобраться как можно ближе к истинной случайности, так что любые возникающие ошибки будут ничтожными для зависимых приложений.

Это не означает, что нет хороших и плохих PRNG или что некоторые не лучше других. NIST создал серию тестов, которые может применить любой поставщик или заказчик RNG, чтобы увидеть, насколько хорош или плох их RNG по сравнению с теоретически идеальным генератором случайных чисел. Тесты и требования задокументированы в специальной публикации NIST 800-22: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-22r1a.pdf.

Примечание Официальное определение RNG требует, чтобы приближение случайности формируемых им чисел было *недетерминированным* (то есть не могло быть определено заранее), а PRNG является *детерминированным*. Что интересно, PRNG являются детерминированными, потому что должны начинаться с начального значения из RNG, которое, как мы знаем, на двоичном компьютере никогда не может быть действительно случайным. Как ни странно, хороший PRNG на двоичном компьютере может вернуть больше случайных чисел, чем поступающее ему начальное значение RNG.

Почему истинная случайность так важна?

Большинство криптографических алгоритмов требуют действительно случайное число при запуске (часто называемое *вектором инициализации* (initialization vector), *начальным значением* (seed value) или *данным временем* (nonce)). Затем используется сложная математика для получения результата, который действительно трудно оценить или угадать. Например, RSA требует двух больших, случайно выбранных простых чисел, являющихся частью алгоритма (обычно они представлены математически как p и q). После того как выбор этих случайных чисел сделан, они участвуют в сложных математических преобразованиях, которые дают результат, трудный для обратного разложения на множители.

Но предположим, что простые числа, какими бы большими они ни были, не были бы случайными вообще. Предположим, что по какой-то ошибке

простые числа, выбраемые каждый раз, были одинаковыми. Это станет похожим на алгебраическую формулу типа $X + 23 = Z$, но вы знаете, что X всегда 5. Имея эту информацию, вы будете знать, что раз Z составляет 28, то X было 5 независимо от того, сколько раз вы запускали «алгоритм». В этом случае результат RSA всегда оставался бы неизменным, если простые числа всегда были бы одними и теми же. Любой злоумышленник, узнав об этой ошибке и увидев тот же ожидаемый результат, немедленно выяснит, какие простые числа использовались, и может сразу разложить результат обратно к исходным компонентам X и Z. Шифр будет иметь нулевую защиту.

И хотя такой сценарий нулевой случайности звучит немного надуманно, это происходило в компьютерном мире много раз. Люди, полагающиеся на то, что, как им сказали, является хорошо проверенными, надежными шифрами для защиты их конфиденциальных данных, позже узнавали, что в программе, реализующей шифр, была ошибка в его RNG, которая полностью нарушила предполагаемую защиту шифра. Это происходило не раз в широко используемых программах, защищающих миллионы сайтов и компьютеров.

Ошибка в RNG программы Debian OpenSSL

Одним из наиболее известных примеров небезопасных ошибок RNG является разгром Debian OpenSSL RNG в 2006 году. Debian Linux является очень популярной версией Linux, включая «дистрибутив», известный как Ubuntu, который часто выбирают пользователи, пытающиеся впервые перейти с Microsoft Windows на Linux. OpenSSL – самая популярная библиотека криптографии с открытым исходным кодом и являющаяся программой, используемой компьютерами с операционной системой (ОС) с открытым исходным кодом. Когда в 2006 году обновленная версия OpenSSL была «разветвлена» для Debian, один из разработчиков ОС Debian неправильно интерпретировал предупреждение о коде компилятора, удалил несколько строк задействованного кода и, не подозревая того, убрал почти всю случайность.

Ошибка была замечена лишь в 2008 году, и были выпущены многие миллионы неслучайных ключей. Удаление случайности привело к тому, что возможное количество ключей от многих триллионов возможных комбинаций упало до не более чем 1 в 32 767 комбинациях. И во многих случаях десятки тысяч реализаций стали использовать одни и те же пары ключей. Спустя годы десятки тысяч веб-сайтов по-прежнему содержат хорошо известные и широко документированные пары ключей, и тысячи все еще существуют по сей день (хотя большинство из тех, что используются в интернете, уже устарели). Хакеры даже создали инструменты, которые проверяют и перебирают цифровые сертификаты и пары ключей, основанные на этой ошибке: смотрите www.madirish.net/309.

Вы можете прочитать больше об ошибке Debian RNG на сайтах:

- www.schneier.com/blog/archives/2008/05/random_number_b.html;
- https://hdm.io/tools/debian-openssl/;
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0166;
- https://security.stackexchange.com/questions/143133/all-weak-debian-openssl-dsa-keys.

Я не хочу, чтобы вы думали, что только один разработчик допустил такую ошибку. Есть еще много примеров глючных RNG, показанных здесь: https://en.wikipedia.org/wiki/Random_number_generator_attack. И это не считая того времени, когда правительства и компании могли преднамеренно создавать такие RNG, как было описано в главе 6 «Квантовоустойчивая криптография». Подтверждение случайности не просто желательно, оно необходимо.

Но есть еще бóльшая проблема. Даже если RNG не содержат грубой ошибки кодирования, они все еще не являются действительно случайными. По своей сути, все они похожи на RNG в примере с dBASEIII+. Такой RNG может выглядеть случайным, но когда он проанализирован и изучен компетентными людьми с большими ресурсами, прорехи в случайности будут раскрыты. Первичным источником на двоичном компьютере являются кварцевые часы, и тот тактовый цикл, которым начинается в компьютере каждый процесс, не является случайным. Это отсутствие реальной случайности дает криптографическим злоумышленникам ту «колыбель», которая позволяет легко взломать криптокоды и другие механизмы, требующие действительно случайных чисел для их защиты.

Что еще хуже, большинство квантовоустойчивых шифров полагаются на двоичные RNG или PRNG. Устойчивость защиты их шифров все еще невероятно высока, но, по сути, они полагаются изначально на слабые RNG. Эта дилемма часто рассматривается создателями различных квантовоустойчивых шифров как риск дизайна, который полностью контролировать невозможно. Из-за этих проблем с RNG, непреднамеренных или преднамеренных, важно, чтобы случайно сгенерированные числа были действительно случайными или почти случайными. Ни то, ни другое невозможно получить на традиционных компьютерах без привлечения квантовых устройств.

Квантовые RNG

Введем понятие *квантовых RNG* (QRNG). QRNG – это квантовые устройства, которые могут генерировать доказуемо действительно случайные числа. По крайней мере, после 2001 года уже существовало несколько реальных QRNG, а статьи о том, как создать их, публиковались еще раньше. Есть десятки серийных примеров. Это наиболее доступные производимые квантовые устройства. Генераторы QRNG создаются различными способами и используют разные материалы и механизмы для генерации действительно случайных чисел.

Основой большинства QRNG являются квантовые свойства суперпозиции, запутанности и неопределенности. Квантовым свойством могут быть все возможные состояния до начала измерения, и вы не можете предсказать заранее основные свойства RNG, необходимые для генерации истинной случайности. Все эти свойства необходимы для генерации истинной случайности. Большинство устройств QRNG тем или иным способом используют в качестве основного источника квантовые свойства фотонов.

Теорема Белла о неравенстве

С момента открытия квантовой физики не утихает беспокойство физиков и криптографов по поводу того, является ли наблюдаемое ими поведение

квантов именно квантовыми свойствами, а не чем-то еще (каким-то классическим объяснением, которое они упустили). В 1930-х годах Эйнштейн и другие физики выдвигали гипотезы о том, что, возможно, неизвестные и необъяснимые тогда (классические) локальные скрытые переменные, связанные с объектом, были причиной предполагаемого квантового поведения, которое наблюдали все ученые. Фактически Эйнштейн совсем не был убежден, что то, что ученые видят и объясняют как квантовое поведение, действительно является таковым. Он (и другие ученые) задавался вопросом, не могло ли это быть чем-то другим, что вписывается в стандартную классическую модель физики. Такое предположение известно как теория *локальных скрытых переменных* (local hidden variables).

Слово «локальные» в названии локальных скрытых переменных означает, что переменные или их свойства, влияющие на объект и определяющие его поведение, находятся на объекте, в объекте, рядом с ним или иным образом непосредственно связаны с объектом. «Скрытая» означает, что локальные переменные в настоящее время не наблюдаемы и не объяснены.

Чтобы объяснить на примере, что такое локальные скрытые переменные, представим себе фантастическую ситуацию. У некоей группы людей, проживающих в очень холодном климате, руки по какой-то неведомой причине всегда теплее по сравнению с окружающей средой и с остальными частями тела. Независимо от того, какова температура воздуха, руки у этих людей ровно на два градуса теплее.

Допустим, этим вопросом занялись ученые и выяснили, что температура воздуха вокруг рук испытуемых всегда выше, чем везде. Никакого объяснения этому факту нет, во всех наблюдениях это именно так, однако он прекрасно объясняет, почему руки людей всегда теплее. Ученые даже дали странному явлению название «микропогода», и этим объяснением пользовалось все больше ученых в течение многих лет после десятилетних наблюдений.

Позже, когда эти воображаемые ученые присмотрелись более внимательно, они увидели, что люди вынимали из карманов перчатки, чтобы держать руки в тепле. Это было вовсе не нечто фантастически новое и прекрасное – все было куда проще и прозаичнее. Этот пример дает понять, почему физики боятся некорректно объяснить в рамках существующей понимаемой ими классической теории то, что они наблюдают, и, возможно, преждевременно назвать какое-то иное необъяснимое поведение *квантовым поведением*. Квантовая физика очевидно противоречит тому, что ученым доводилось наблюдать прежде.

Эйнштейн также предложил убедительный способ доказать или опровергнуть существование локальных скрытых переменных. Если бы локальные скрытые переменные могли быть опровергнуты, это было бы бóльшим доказательством того, что квантовая механика действительно существует. Такого доказательства не появилось за время жизни Эйнштейна (он умер в 1955 году), но он открыл миру физики экспериментальный путь исключения одной из последних возможностей опровержения, позволяющий выяснить, является квантовая физика чем-то новым и удивительным или это просто упущенный аспект классической физики.

В 1964 году ирландский физик Джон Стюарт Белл (John Stewart Bell) в своей основополагающей статье под названием On the Einstein–Podolsky–Rosen Paradox («О парадоксе Эйнштейна–Подольского–Розена») математически доказал, что локальные скрытые переменные не могут объяснить наблюдаемое квантовое поведение, и предложил эксперименты, которые можно провести, чтобы доказать это. Не вдаваясь в теоретическое объяснение того, что предложил Белл (эти эксперименты включают углы, спины и измеренные отличия квантовых частиц и их свойств), отметим, что он опирался на небольшую разницу в ожидаемых измерениях между свойствами объекта и тем, что наблюдалось бы, если бы существовало только классическое поведение (и локальные скрытые переменные). Графически в классическом мире различия будут представлены прямой линией, но в квантовом мире измерения будут больше похожи на кривую колокольчика (в качестве примера см. рис. 7.1). Оказывается, что экспериментальные наблюдения всегда имели форму, напоминающую кривую колокольчика, что доказывает существование квантовых свойств. Разница между ожидаемыми классическими измерениями и реальными квантовыми измерениями известна как нарушение неравенства Белла.

Рис. 7.1. Неравенство Белла, представленное графически

Проще говоря, Белл создал экспериментальную структуру, где ответ может быть только ложным, если все, что у нас есть, – это лишь классическая физика, но ответ всегда верен, и потому кроме классической физики есть что-то еще. По сути, Белл наконец «доказал» квантовую физику, продемонстрировав, что локальные скрытые переменные не могут существовать. Вспомним, что физикам не нужно ждать реальных подтверждений, чтобы в чем-то убедиться. Экспериментов и вспомогательной математики достаточно.

Начиная с 1970-х годов несколько физиков проводили эксперименты, которые дали результаты, ожидаемые в соответствии с *теоремой Белла о неравенстве*. Некоторые наблюдатели все же полагали, что эксперименты были плохо спланированы и что возможно существование какого-то пути, при котором скрытые локальные переменные все же могут работать (известны как *лазейки Белла* (Bell's loopholes)). Однако после сотен экспериментов, которые

никогда не нарушали теорему Белла, в 2015 году был проведен эксперимент, окончательно, без тени сомнения доказывающий теорему Белла (www.physicsforums.com/threads/another-loophole-free-test-ofbells-теорема.842620/). Довольно хорошее объяснение теоремы Белла находится здесь: https://en.wikipedia.org/wiki/Bell%27s_theorem.

Примечание Хотя это может показаться нелогичным, «нарушение» теоремы Белла о неравенстве является хорошим ожидаемым результатом и означает, что эксперимент или устройство правильно указывает на квантовые свойства. «Нарушение» – это результаты измерений, отличающиеся от результатов, которые вы получили бы при существовании только классической физики.

Все квантовые устройства, использующие запутывание, включая QRNG, всегда должны быть проверены, чтобы мы могли убедиться, что они проходят тест Белла. Разработчики хотят убедить, что результаты, которые они предоставляют, являются чисто квантовыми и что в результатах не допускается какая-то классическая, неквантовая ошибка. Это может быть сделано во время создания, тестирования и сертификации. Это особенно важно для QRNG, истинная случайность которого должна быть подтверждена, чтобы гарантировать максимально возможную безопасность в течение всего времени зависимой реализации.

Существует также теоретическая опасность, что QRNG, использующий запутывание, может быть сертифицирован как проходящий тест Белла, а затем злонамеренно модифицирован для вывода неслучайных чисел. Например, возможно, вражеское государство создает компонент QRNG, на который опирается популярный бренд QRNG и который потому кажется безопасным. В действительности же длинный поток якобы «случайных» чисел, которые он производит, тайно документирован, что означает, что государство знает, каков он и каким будет. Генератор QRNG должен быть проверен кем-либо, кто подтвердит, что он соответствует теореме Белла о неравенстве и является действительно случайным. Самые лучшие QRNG разработаны таким образом, что они самостоятельно тестируются во время операций, чтобы можно было убедиться, что они нарушают неравенство Белла. Вы найдете хорошую статью об этой концепции здесь: www.nature.com/articles/npjqi201621.

Кроме того, QRNG, желающие доказать, что они соответствуют концепции случайности, могут подвергнуться тестам NIST 800-22, созданным для измерения случайности любого RNG (квантового или нет), и опубликовать их результаты. Потребители должны получить возможность запускать такие же тесты и получать схожие результаты. Вы можете найти пример результатов тестирования одного из поставщиков QRNG здесь: http://marketing.idquantique.com/acton/attachment/11868/f-004c/1/-/-/-/-/Randomness%20Test%20Report.pdf.

Но абсолютно лучший тест для QRNG (использущего запутывание), чтобы доказать, что он генерирует действительно случайные числа, – это тест, показывающий, что они были получены при нарушении неравенства Белла. Доказательство предоставляется на квантовом уровне. Пока единственны-

ми работающими коммерческими QRNG, которые следуют этому, являются QRNG компании Cambridge Quantum Computing под названием IronBridge (https://cambridgequantum.com/cqcunveils-the-worlds-first-commercially-ready-certifiable-quantum-cryptographic-device/) и QRNG NIST (рассматривается ниже).

Работающие QRNG

Вначале QRNG заполняли длинные лаборатории и работали, стреляя лазерами между двумя устройствами, разделенными многими футбольными полями лазерного оптического кабеля. Но QRNG все чаще создаются как компьютерные устройства размером с коробку для пиццы или даже в виде небольших интерфейсных карт, которые, имея размер автономной сетевой карты, могут быть вставлены в компьютер.

Вы можете купить рабочие QRNG любого форм-фактора стоимостью менее тысячи долларов у разных поставщиков, от производителей чипов небольшого оригинального оборудования до поставщиков серверов. Они сертифицированы для работы со многими операционными системами, включая Windows, Linux, BSD, Солярис и Apple. У них есть библиотеки кода, API и интерфейсы для нескольких языков программирования. Компании, нуждающиеся в QRNG, уже давно покупают и используют их. Генераторы QRNG используются в банковском деле, науке, лотереях, телекоммуникациях, финансовой сфере и вооруженных силах.

Швейцарская компания ID Quantique (www.idquantique.com/random-number-generation/overview/) была первой компанией, которая создала реальный рабочий QRNG еще в 2001 году. С тех пор она продолжает производить эти изделия. На рис. 7.2 показаны три различных продукта ID Quantique QRNG, предназначенных для подключения к внутреннему слоту компьютерного интерфейса. Среди других компаний, выпускающих QRNG на продажу, – австралийская Quintessence Labs (www.quintessencelabs.com/), базирующаяся в США ComScire (https://comscire.com) и канадская Quantum Numbers Corp (www.quantumnumberscorp.com). Вы найдете хорошую обзорную статью об этих компаниях и их продуктах здесь: www.nanalyze.com/2017/02/quantum-random-number-generator-qrng/. Вы даже можете бесплатно генерировать и использовать свои собственные квантовые случайные числа по интернету, в том числе посетив страницу https://qrng.anu.edu.au.

Генератор QRNG Public Beacon NIST

В 2018 году NIST создал QRNG (www.nist.gov/news-events/news/2018/04/nists-new-quantummethod-generates-really-random-numbers), генерирующий действительно случайные числа. Чтобы создать запутанные фотоны, кристалл облучается высокоинтенсивным лазером. Доказано, что случайность его чисел лежит в пределах «одной триллионной от 1 %», что примерно так и есть. Целью проекта NIST являлось создание QRNG – публичного маяка (beacon) случайности, которым может пользоваться любой в любой программе (https://csrc.nist.gov/projects/interoperable-randomnessbeacons). Первоначально NIST собирался создать частный сервис, но затем решил, что наличие общедоступного QRNG – достоверного источника истинно случайных чисел будет полезно всему компьютерному миру.

Рис. 7.2. Пример генераторов QRNG фирмы ID Quantique.
С разрешения фирмы ID Quantique

Недостатки генераторов QRNG

Недостатки QRNG – стоимость и совместимость. Вы можете купить относительно дешевые (от нескольких сотен долларов) генераторы QRNG, но генераторы псевдо-RNG бесплатны или почти бесплатны. Каждый компьютер уже имеет один или несколько встроенных генераторов. Чтобы использовать QRNG, вы должны купить, установить и согласовать его. В настоящее время очень немногие приложения работают с QRNG, и по умолчанию с QRNG не работает ни одно популярное стандартное программное обеспечение. Поставщики QRNG создали программное обеспечение и драйверы, чтобы позволить существующим приложениям подключать их продукты, но большинство приложений не имеют необходимых изменений интерфейса. Разработчикам довольно легко их добавить, но пока для подавляющего большинства RNG-зависимых приложений они просто не существуют, по сравнению с применением традиционных RNG, используемых в настоящее время всеми нуждающимися в них существующими устройствами и приложениями.

Генераторы QRNG желательны даже для доквантового мира, потому что они дают доказуемо случайные числа и могут улучшить все зависимые криптографические операции, как классические, так и квантовые.

Квантовые хеши и подписи

В этом разделе обсуждаются квантовые хеши и цифровые подписи.

Квантовые хеши

Как уже говорилось ранее, хеши – это односторонние криптографические функции, которые создают уникальный представительский набор символов или битов (известный как *хеш*, *результат хеширования*, *цифровая подпись* или *дайджест сообщения*) рассматриваемого уникального контента. Хеши необходимы и используются во многих других криптографических процессах, таких как шифрование и цифровая подпись. Традиционные хеши являются квантововосприимчивыми к атакам на прообразы (но не конфликтам согласно https://cr.yp.to/hash/collisioncost-20090517.pdf). Поэтому нужны квантовые хеши.

Квантовые хеши могут принимать либо традиционные двоичные входы, либо квантовые входы и возвращать хеш на основе квантовых состояний. Квантовые хеши, которые принимают двоичный контент и возвращают квантовый хеш, известны как *классические квантовые* (classical-quantum). Как и любой другой хеш, традиционный или квантовый, он должен быть устойчивым к атакам на прообразы, атакам на повторные прообразы и конфликты. Квантовые хеши естественным образом распространяются на квантовые цифровые подписи.

Некоторые квантовые хеши отвечают этим требованиям, но большинство не были в достаточной степени проверены временем. Хотя некоторые квантовые хеши были реализованы в реальных рабочих устройствах, большинство из них являются просто мысленными экспериментами, доказывающими,

что квантовое хеширование возможно и может быть реализовано в нужных масштабах, когда это будет необходимо. Доступны многие научные исследования относительно квантовых хешей. Например, в 2013 году россияне Фарид Аблаев и Александр Васильев предложили теоретический классический квантовый хеш (https://arxiv.org/pdf/1310.4922v1.pdf). Их алгоритм квантового хеша (см. рис. 7.3) содержит достаточно сложную математику, и это, вероятно, отталкивает большинство криптографов с нематематическим мышлением. Упрощая, можно сказать, что эти авторы предложили математические доказательства всех требуемых свойств хешей, представляемых квантовыми свойствами.

Для сообщения $M \in \{0, 1\}^n$ мы используем

$$|h_K(M)\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |i\rangle \left(\cos \frac{2\pi k_i M}{N} |0\rangle + \sin \frac{2\pi k_i M}{N} |1\rangle \right)$$

Рис. 7.3. Математическое представление алгоритма квантового хеша Аладьева и Васильева

Ключевой аргумент состоит в том, что их алгоритм позволяет кубитам точно и однозначно представлять любое сообщение длиной n бит не более чем $O(\log n)$ кубитами. Не вдаваясь в подробности, отметим: $O(\log n)$ по существу означает существенно меньшее число, чем n кубитов, необходимых для каждого бита хешированного сообщения, откуда теоретически следует, что исходное сообщение не может быть получено из меньшего результирующего хеша.

Примечание Если вы хотите узнать больше о том, что математически представляет выражение $O(\log n)$, смотрите www.quora.com/How-can-we-check-for-the-complexity-log-n-and-n-log-n-for-an-algorithm, и www.quora.com/How-would-you-explain-O-log-n-in-algorithms-to-1st-year-undergrad-student-Can-any-one-explain-it-with-mathematical-proof-for-log-n-complexity-by-taking-a-simpleexample-like-Binary-search-and-simple-to-understand.

Ограничение Holevo

Алгоритм Аблаева и Васильева опирается на другую квантовую теорему, известную как *ограничение Холево* (Holevo's bound) (https://en.wikipedia.org/wiki/Holevo%27s_theorem). Эта теорема говорит, что кубит может находиться в одном из двух состояний, но когда он измеряется (декодируется), то должен разбиваться на измерение, представленное только одним из двух состояний, поскольку информация об одном состоянии теряется при каждом измерении кубита (т. е. бит, имеющий только два состояния, не может точно измерить свойство с тремя возможными состояниями). Чтобы точно представлять один кубит (который может иметь три возможных состояния), потребуется, по крайней мере, два двоичных бита (2 бита = 2^2 = 4, т. е. могут представлять 4 возможных состояния).

Авторы заканчивают свою работу созданием квантового алгоритма цифровых отпечатков пальцев на основе их хеша. Статья и исследование финансировались грантом Российского фонда фундаментальных исследований. Создатели хешей пошли дальше и создали большее количество квантовых хешей, и даже рассмотрели и доказали, что применение еще более сложной математики может быть основой любого квантового хеша. Для получения дополнительной информации о квантовых хешах смотрите www.bjmc.lu.lv/fileadmin/user_upload/lu_portal/projekti/bjmc/Contents/4_4_17_Ablayev.pdf.

Квантовые цифровые подписи

Разница между хешем и подписью заключается в аутентификации личности. Хеш является уникальным отпечатком уникального контента. Цифровая подпись связывает хеш с личностью субъекта. Например, скажем, вы хешируете файл, и хеш возвращается как 1234. Затем вы используете закрытый ключ вашей асимметричной пары ключей для цифровой подписи хеша. Пара асимметричных ключей привязана к вашей личности. Цифровая подпись является предметом блокировки в конкретном хеше в конкретный момент времени конкретной идентичности.

Чтобы получить цифровую подпись, вам нужен хеш, который соответствует паре асимметричных ключей и алгоритму цифровой подписи. Для проверки любой предполагаемой цифровой подписи заинтересованному лицу понадобится соответствующий проверенный открытый ключ, который будет использован для «разблокировки» хеша, а это возможно, только если документ был подписан соответствующим закрытым ключом. Если открытый ключ не раскроет действительный, ранее «зашифрованный» хеш, правильно представляющий предполагаемое содержимое хеша, то целостность файла или цифровая подпись должна быть проверена. В любом случае заинтересованная сторона не будет доверять такому файлу или цифровой подписи.

Традиционная пара асимметричных ключей и цифровая подпись могут передаваться с использованием квантового обмена, но в этой главе мы рассматриваем лишь истинность квантовой цифровой подписи, основанной на квантовых свойствах. Квантовая цифровая подпись требует квантового хеша, квантовой пары асимметричных ключей и квантового цифрового алгоритма подписи, которые представлены квантовыми свойствами. Квантовые свойства в настоящее время нестабильны в течение достаточно длительного времени, поэтому они не создают фантастически хороших пар асимметричных ключей. Есть многие другие дополнительные проблемы масштабирования (они будут обсуждаться ниже), которые не позволяют получить хорошую квантовую цифровую подпись, особенно по сравнению с гораздо менее строгими (но до сих пор очень надежными) доступными квантовоустойчивыми цифровыми подписями. Однако для ограниченных случаев применения в течение коротких промежутков времени реализация на квантовой основе позволяла бы создавать уникально защищенные цифровые подписи.

Один из приемов, который позволял бы делать цифровую подпись на квантовой основе ультрабезопасной, – использование квантового хеша цифровой подписи. Как обсуждалось ранее, квантовые хеши очень трудно атако-

вать. Они основаны на теореме Холево, и невозможно (даже с использованием квантовых компьютеров) обратить их в исходное сообщение. Сложность решения этой проблемы заключается в том, что из-за теоремы о неклонировании подписывающее лицо не может просто создать набор идентичных квантовых открытых ключей и отправить их получателям. Все становится намного сложнее.

Первый квантовый алгоритм цифровой подписи

Первый практический алгоритм квантовой цифровой подписи был создан в 2001 году Даниэлем Готтесманом (Daniel Gottesman) и Айзеком Чуангом (Isaac Chuang) (https://arxiv.org/pdf/quant-ph/0105032.pdf). Этот алгоритм не очень эффективен, но работает. Во-первых, отправитель / подписывающая сторона, Алиса, должна отдельно подписывать каждый кубит/бит сообщения. Она не может просто хешировать контент и подписать хеш за одну операцию, как это было бы возможно с классическими алгоритмами подписания. Хеш (или сообщение) должен быть подписан по одному кубиту/биту за раз. Алиса должна создать для использования один или несколько закрытых ключей, которые будут, если часть своего сообщения она подписывает, = 1, и отдельный набор закрытых ключей, если бит ее сообщения = 0. Затем, используя алгоритм асимметричного шифра, Алиса генерирует соответствующий открытый ключ для каждого созданного закрытого ключа и отправляет все открытые ключи всем получателям, Бобу и Чарли. Получателей не может быть слишком много, потому что каждая дополнительная скопированная пара ключей начинает создавать повышенный риск компрометации ключа.

Теперь для каждого 0-го бита в подписанном сообщении Алиса отправляет Бобу и Чарли все закрытые 0-битные ключи вместе с 0-битным подписанным сообщением. Алиса также отправляет Бобу и Чарли все 1-битные закрытые ключи вместе с 1-битным подписанным сообщением. Затем Боб и Чарли используют ранее отправленные открытые ключи для проверки закрытых ключей. Если у Боба и Чарли частота ошибок сравнения низкая, то подписанный бит проверяется. Если у Боба и Чарли частота ошибок сравнения большая, то можно предположить, что где-то в системе произошел сбой. Процесс должен повторяться для каждого бита подписанного сообщения/хеша.

Это не очень эффективный способ создавать цифровую подпись, даже если вам нужна сверхвысокая безопасность, хотя были предложены протоколы для повышения эффективности всех битов сообщения (https://www.researchgate.net/publication/312062995_The_postprocessing_of_quantum_digital_signatures). Тем не менее это была первая, хотя и неэффективная, квантовая цифровая подпись, показывающая, что она может быть создана.

Цифровые подписи с фазовым кодированием

Затем в 2012 году другой, несколько более эффективный, но очень похожий алгоритм квантовой цифровой подписи был опубликован в журнале Nature, в котором использовались «фазово-кодированные когерентные состояния света» (www.nature.com/articles/ncomms2172). С помощью этого метода Алиса выбирает случайный набор квантовых состояний (который приравнивается к закрытому ключу), что может быть представлено различными фазами

света. Каждый бит сообщения все еще подписывается отдельно Алисой. Для каждого 0-битного или 1-битного сообщения Алиса генерирует пару, закодированную по фазе, и отправляет одну копию пары Бобу, а другую копию пары Чарли. Боб и Чарли декодируют фазы и проверяют подписанный бит.

В 2013 году цифровые подписи на квантовой основе были снова несколько улучшены (https://journals.aps.org/prl/pdf/10.1103/PhysRevLett.112.040502), а затем последовало множество успешных экспериментов с цифровыми подписями, включая www.nature.com/articles/s41598-017-03401-9 и http://cnqo.phys.strath.ac.uk/research/quantum-theory-of-light/quantum-digital-signatures/. В этих последних экспериментах использовалась улучшенная, фазово-кодированная вариация подписи.

Цифровые подписи на квантовой основе прогрессировали настолько, что криптографы теперь ищут способы, с помощью которых такие подписи могут быть успешно атакованы. Посмотрите следующие две статьи: https://link.springer.com/article/10.1007/s11128-019-2365-8 и www.sciencedirect.com/science/article/pii/S0030402617308069. Всякий раз, когда криптографический алгоритм или продукт подвергается проверке атакой, это хороший знак и улучшает протокол. С учетом сказанного, потребность в квантовой цифровой подписи, особенно с повышенной сложностью и множеством хороших квантовоустойчивых цифровых подписей, скорее всего, в обозримом будущем останется небольшой.

Для получения дополнительной информации о квантовых цифровых подписях смотрите https://arxiv.org/pdf/quantph/0105032.pdf, https://journals.aps.org/prl/pdf/10.1103/PhysRevLett.113.040502 и https://en.wikipedia.org/wiki/Quantum_digital_signature.

Квантовые шифры

Квантовое шифрование обеспечивает защиту сохраненных данных или защиту при их передаче с использованием квантовых устройств, программного обеспечения и квантовых свойств. Как и в традиционном двоичном мире, квантовые шифры могут быть симметричными или асимметричными. Трудно и даже невозможно просматривать, копировать данные, защищенные или находящиеся в квантовом состоянии, или управлять ими. Если кто-то несанкционированно пытается напрямую просмотреть данные или вмешаться в поток данных или область хранения с квантовой кодировкой, квантовое состояние будет изменено. Это гарантировано эффектом наблюдателя и теоремой об отсутствии клонирования. Наблюдатели могут манипулировать закодированными данными, но нет способа, который не был бы легко обнаружен вовлеченными в обмен уполномоченными сторонами. Это весьма желательная характеристика для криптографов и пользователей криптографии. Данный раздел будет охватывать асимметричные квантовые шифры в целом, но более широкое обсуждение квантовых сетей оставим для главы 8.

Примечание Читателям может быть интересно, почему мы не рассматриваем квантовые симметричные шифры. Причина в том, что эта область шиф-

рования мало изучена, освещена лишь в небольшом количестве источников и доступных материалов исследований. Традиционное двоичное симметричное шифрование в настоящее время считается устойчивым к известным квантовым атакам, и они мало обсуждались в дискуссиях. Возможно, в будущем по квантовым симметричным шифрам будет проводиться больше исследований и выделяться больше ресурсов для их анализа, но в настоящее время эта область шифрования в основном плохо изучена.

Асимметричная криптография существует с 1970-х годов. Мы знаем, что этот тип шифрования обычно используется для безопасной передачи симметричных ключей шифрования от источника получателю, а также для цифровой подписи и аутентификации. Традиционная асимметричная криптография уже хорошо работает более полувека.

Как подчеркивается в этой книге, квантовые компьютеры, скорее всего, довольно скоро взломают многие традиционные популярные шифры квантововосприимчивой криптографии с открытым ключом, такие как RSA и Diffie-Hellman. Как показано в главе 6, существует более двух десятков конкурирующих квантовоустойчивых криптографических алгоритмов, стремящихся стать новым постквантовым стандартом NIST. Все эти квантовоустойчивые алгоритмы, охватывающие как криптографию с открытым ключом, так и обмен ключами, основаны на двоичных вычислениях с двоичными ключами, используя двоичные устройства.

Квантовые асимметричные шифры основаны на квантовых устройствах и свойствах. Один тип, самый популярный в настоящее время, использует квантовые свойства для безопасного секретного традиционного симметричного обмена между авторизованным источником и пунктом назначения. Это известно как *распределение квантовых ключей* (quantum key distribution, QKD). Другой метод использует квантовые свойства для безопасной передачи ключа, и сам ключ также основан на квантовых свойствах. Некоторые исследователи (включая этот документ: https://arxiv.org/pdf/0810.2859.pdf) называют их *квантовой криптографией с открытым ключом* (Quantum Public Key Cryptography, QPKC), соответственно класс 1 и класс 2. QPKC Class 1 является QKD, где ключ все еще состоит из двоичных битов. QPKC Class 2 – это QKD с ключом, состоящим из квантовых кубитов. QPKC Class 2 сложнее осуществить из-за отсутствия квантовых сетевых устройств и присущих сложностей сохранения стабильного секретного ключа на квантовой основе в течение длительных периодов времени. Таким образом, большинство алгоритмов и реализаций QPKC относятся к классу 1. Даже те, которые оказались сложными для реализации в настоящее время в реальном мире, все же существуют как успешные реализации.

Распределение квантовых ключей

Существует много алгоритмов и систем распределения ключей класса 1 QPKC, и хотя они не широко распространены, начиная с 2000 года было много частных и коммерческих сетей, использующих QKD. Сети на основе QKD впервые были использованы в Европе в 2007 году и используются в Соеди-

ненных Штатах с 2010 года. Сегодня многие страны, особенно Китай, используют и улучшают их. Больше об этих квантовых сетях – в главе 8.

BB84

Первый алгоритм QKD был создан американцем Чарльзом Беннеттом (Charles Bennett) и канадцем Жилем Брассаром (Gilles Brassard) в 1984 году и часто упоминается просто как аббревиатура BB84. Беннетт и Брассар считаются двумя отцами квантовой криптографии. Беннетт, сотрудник IBM, в свои 70 лет продолжал исследования и активно публиковался в 2016 году в блоге на сайте под названием *The Quantum Pontiff* (https://dabahttps://dabacon.org/pontiff/author/chb/con.org/pontiff/автор/chb/). Брассар помог создать *протокол исправления ошибок* (cascade error correction protocol), который позволяет обнаруживать и исправлять шум, вызванный прослушиванием каналов передачи с квантовой криптографической защитой (Беннетт также проводил здесь много исследований), и работал в области квантовой телепортации и новой теории игр, известной как *квантовая псевдотелепатия* (quantum pseudo-telepathy).

Алгоритм BB84 был не только первой схемой QKD, но по определению первым алгоритмом, математически показавшим, что использование квантовых состояний надежно защищено от прослушивания. Если опустить математические подробности, основные идеи, связанные с BB84, заключаются в следующем. Алиса хочет отправить сообщение Бобу через ненадежный канал. Алисе нужно получить общий симметричный ключ для Боба, чтобы они могли начать шифрование секретных сообщений друг к другу. Вот основные шаги в BB84:

1. Алиса создает две случайные двоичные строки, скажем a и b, а затем кодирует их, используя кубиты и математический алгоритм BB84, в единый результат, скажем математически n. a и b связаны друг с другом, но никто не знает, что такое b, не зная, что такое a.
2. Алиса отправляет n Бобу как кубиты, через квантовый канал, и это последний раз, когда используется квантовый канал. Остальные коммуникации происходят по открытому классическому каналу.
3. Боб измеряет все полученные n кубитов, которые декодируют кубиты в биты. Боб измеряет половину кубитов в одну сторону (скажем, метод 1) и половину кубитов в другую сторону (скажем, метод 2). Только один из методов является правильным методом для того, что послала Алиса. Метод 1 и метод 2 дают разные ответы во время измерения в зависимости от того, представлял кубит 0 или 1. Правильный метод, который совпадает с тем, что отправила Алиса, будет правильно измерять все 100 % ее половины кубитов (то есть 50 % от общего числа), а неправильный метод в конечном итоге будет правильно измерять только 50 % его половины кубитов (то есть другие 25 % от общего числа). Если Боб получил и измерил все кубиты от Алисы правильно, благодаря способу их измерения, используя как правильный, так и неправильный методы, только 75 % битов будут точно представлять кубиты, отправленные Алисой. Это ожидаемый результат.
4. Боб сообщает Алисе, какой метод, 1 или 2, он использовал для измерения каждого кубита.

5. Алиса, зная теперь, какой метод использовал Боб для каждого кубита и каков был результат, говорит Бобу, какие кубиты, которые он измерил, были измерены правильно, а какие неправильно.
6. Алиса и Боб отбрасывают неправильно преобразованные биты, а оставшиеся 75 % становятся их общим секретным ключом.
7. Непосредственно перед использованием нового общего секретного ключа для будущих доверительных связей в качестве теста Алиса и Боб поделятся друг с другом короткими сериями ключевых битов через ненадежный канал. Если тестовое сравнение соответствует 100 %, они начнут безопасно общаться, используя оставшуюся часть общего ключа. Если нет, они получат шум или прослушивание и не будут доверять текущему общему ключу.

Протокол BB84 имеет больше шагов, чем приведено здесь, и является более сложным, но эта серия шагов показывает общую суть протокола. Хорошее видеопредставление BB84 здесь: www.youtube.com/watch?v=UVzRbU6y7K. Почти все схемы QKD являются улучшенными версиями BB84 и обеспечивают даже лучшую защиту, чем BB84.

Если бы Ева при подслушивании смогла перехватить исходные кубиты между Алисой и Бобом, измерение Евой кубитов было бы декогерентировано только в 75 % правильных битов (как это получилось бы у любого оригинального, законного измеряющего). Но Алиса не знает, какие биты были правильно измерены, а какие не были, и поэтому она должна была бы отправить Бобу то, что она измерила (в том числе 25 % неправильных битов). Повторная отправка Бобу этих измеренных битов как кубитов приведет к тому, что Боб получит только 75 % первоначальных правильных кубитов, предназначенных ему для отправки. Когда он декогерирует их путем подачи в два его метода, он получает менее 75 % правильных кубитов вместо положенных 75 %. Когда Боб и Алиса сообщают друг другу о том, какие биты были получены и какие методы использовал Боб для их чтения, то, если Боб получил точность менее 75 %, Алиса и Боб узнают, что на канале был шум или они были подслушаны.

Методы QKD, такие как BB84, где квантовое состояние одного фотона передается между отправителем и детектором, как правило, называются *дискретно-переменными QKD* (*discrete-variable QKD*). Были разработаны многие другие улучшенные системы QKD на основе BB84, в том числе B92 (www.semanticscholar.org/paper/Quantum-cryptographyusing-any-two-nonorthogonal-Bennett/e99dc04d91409a4668ad0368ef7017e27a034008), созданный одним из авторов BB84 Беннеттом, SARG04 (https://en.wikipedia.org/wiki/SARG04) и Протокол шести состояний (Six-State Protocol): https://en.wikipedia.org/wiki/Six-State_Protocol.

Запутанное QKD

В 1991 году британско-польский профессор Артур Экер (Artur Eker) предложил принципиально иной подход к QKD, использующий запутанность, в своей статье Quantum Cryptography Based on Bell's Theorem («Квантовая криптография на основе теоремы Белла») (http://cqi.inf.usi.ch/qic/91_Ekert.pdf).

Метод Экера выглядит примерно следующим образом:

1. Алиса создает секретный ключ, используя разделенный запутанный кубит для каждого бита ключа.
2. Алиса держит одну сторону запутанной пары и посылает другую сторону Бобу через квантовый канал.
3. Алиса и Боб измеряют свои кубиты (разбивая их на биты), используя свои собственные детекторы с различными комбинациями ориентации для каждого кубита.
4. После измерения всех кубитов Алиса и Боб объявляют ориентацию своих отдельных детекторов для каждого измеренного кубита.
5. Кубиты, которые были измерены одной и той же ориентацией детектора, отбрасываются.
6. И Боб, и Алиса, теперь зная, каковы были ориентации детекторов друг друга, могут конвертировать остальные биты в их результирующие двоичные представления.
7. Наконец, и Боб, и Алиса используют тест неравенства Белла для проверки запутанности. Если запутанность была нарушена, можно предположить, что кто-то подслушивал или наблюдался сильный шум. В любом случае полученный секретный ключ не будет доверенным.

Подход Экера к QKD (также известный как E91) привел к созданию множества новых алгоритмов QKD и других связанных с ним схем.

Атака расщепления фотонов

Теоретически системы QKD устойчивы к прослушиванию из-за эффекта наблюдателя квантовой физики и теоремы о неклонировании. Пока один кубит используется для представления одного бита во время передачи, Еве трудно подслушивать так, чтобы ее не обнаружили. Но на практике большинство систем QKD не могут отправить только один фотон для каждого передаваемого бита. Фотон быстро теряет свою силу при движении вдоль волоконно-оптического кабеля, и считывающие детекторы с трудом обнаруживают один фотон. Из-за этого большинство систем QKD отправляют несколько фотонов для каждого переданного кубита/бита. В многофотонных системах Ева может отбирать один или несколько дублированных фотонов, позволяя остальным пока оставаться между Алисой и Бобом. Протоколы QKD (например, SARG04) созданы, и большинство реальных систем QKD включают дополнительные механизмы защиты и исправления ошибок, чтобы уменьшить риск атак расщепления числа фотонов.

Непрерывно-переменное QKD

Второй основной, более новый тип QKD известен как QKD *с непрерывной переменной* (continuous-variable, CV-QKD). В CV-QKD квантовые свойства закодированы в модуляции амплитуд и фаз потока лазерного луча, который затем может быть декодирован детектором, известным как *гомодинный детектор* (homodyne detector). Эти методы более устойчивы к атакам с расщеплением фотонов. Системы CV-QKD могут отправлять больше ключей за один период (по сравнению с системами QKD с дискретными переменными) и дешевле в реализации, но они не могут работать на многокилометро-

вых расстояниях, которые могут преодолевать системы с дискретными переменными. Примеры схем CV-QKD можно найти здесь: https://arxiv.org/ftp/arxiv/papers/0705/0705.0515.pdf и https://arxiv.org/pdf/1703.09278.pdf. Вы будете часто читать о квантовых сетевых устройствах, поддерживающих алгоритмы с дискретными или непрерывными переменными.

Проблемы с повторителем

Системы QKD в связи с теоремой об отсутствии клонирования устойчивы к необнаружимому подслушиванию. В криптографических кругах это считается очень важным. На практике при попытке использовать QKD в больших сетях это становится большой проблемой. Системы QKD по существу созданы, чтобы быть двухточечными. Вы не можете просто вставить ретранслятор или маршрутизатор традиционного типа между двумя конечными точками QKD для повторения сообщения. Повторяющее устройство будет рассматриваться как подслушивающее. При удаленной связи точка–точка можно отправить квантовый световой сигнал лишь на несколько миль, затем он потеряет свою силу и должен быть повторен.

Примечание Проводятся исследования с целью увеличения расстояния, на которое квантовый сигнал может быть отправлен и после которого его необходимо повторить. В частности, смотрите www.nature.com/articles/s41586-018-0066-6.

Таким образом, сети QKD должны быть единой непрерывной системой точка–точка, или кубиты должны измеряться, расшифровываться в двоичный файл, а затем ретранслироваться с использованием квантовых повторителей. Каждое из этих двоичных местоположений является слабым звеном в цепи, где подслушивающий злоумышленник может включиться и безнаказанно получить зашифрованную информацию.

Вспомните, сколько точек ретрансляции в вашей простой домашней сети. Ваши мобильные устройства, вероятно, подключаются к маршрутизатору Wi-Fi, который затем подключается к кабельному модему, который подключается к устройству за пределами вашего дома, которое подключается к точке агрегации окрестности, которая затем соединяется с десятками и сотнями других ретрансляторов на пути к вашему провайдеру интернет-услуг (internet service provider, ISP). Потом ваш провайдер подключается к одному–трем дюжинам узлов, чтобы обойти интернет (каждый из которых может иметь любое количество ретрансляторов к ним и от них), и, наконец, переходит в конечный компьютер назначения или устройство – и этот путь меняется на обратный для каждого сетевого пакета, который необходимо отправить обратно. Типичный пакет сети интернет легко проходит через десятки ретрансляторов. Если мы когда-нибудь захотим иметь квантовый интернет, это создаст огромную проблему. Эта проблема и ее решение более подробно будут рассматриваться в главе 9.

Другие проблемы QKD

Системы QKD имеют много критиков, включая Брюса Шнайера (Bruce Schneier), www.schneier.com/blog/archives/2018/08/gchq_on_quantum.html) и Нацио-

нальный центр кибербезопасности Великобритании (the U. K. National Cyber Security Centre, www.ncsc.gov.uk/whitepaper/quantum-key-distribution). Многие задаются вопросом, оправдывает ли затраты разработка чисто квантовой сети. То, что нам сегодня известно, позволяет говорить, что это можно сделать, особенно с учетом квантовоустойчивой криптографии, и, вероятно, она будет отвечать самым высоким требованиям безопасности в течение долгого времени.

Еще одной практической проблемой является отсутствие текущей совместимости между существующими реализациями QKD, даже когда они предположительно используют одни и те же алгоритмы; но некоторые проекты уже начинают доказывать свою способность взаимодействовать. В целом многие критики находят, что проблемы, требующие решения, предполагают существенные затраты, и это не то, что можно реализовать на практике в больших масштабах в ближайшее время. В официальном документе Великобритании – Белой книге утверждается, что еще долгое время будет нецелесообразно рассчитывать на QKD-шифры как шифры, которые могут использоваться в массовых масштабах, таких, в каких сегодня используются шифры в миллиардах устройств, например, интернета вещей (Internet of Things, IoT). Вместо этого критики рекомендуют придерживаться проверенных квантовоустойчивых шифров.

Другая серьезная проблема – общая безопасность реальных систем QKD. Они существуют недостаточно долго, чтобы можно было понять, какова их реальная безопасность. Помимо слабых звеньев, создаваемых каждым узлом-ретранслятором, системы QKD еще открыты для множества хакерских атак и на двоичном, и на квантовом уровнях. Криптографы не любят использовать системы, которые не прошли испытания временем, подвергаясь атакам злоумышленников и испытаниям исследователей.

Это правильные оценки на текущий период времени, но это аргументы примерно того же рода, что использовались в спорах о том, почему автомобили никогда не смогут заменить лошадей, или как непрактично считать, что электрические двигатели когда-либо заменят бензиновые. Я уверен, что нашим ИТ-предкам было трудно представить себе мощь компьютера, которую мы сегодня имеем в наших крошечных, портативных мобильных телефонах. Проблемы стоимости, безопасности и распространения обычно так или иначе преодолеваются, особенно в компьютерном мире.

Протокол Субхаша Кака

QKD по своей природе использует много классических систем и каналов. Если применяются квантовые ключи, QKD является предпочтительным, потому что чисто квантовой криптографии в такой системе не так много. В будущем, вероятно, будут использоваться полностью квантовые системы QPKC класса 2. В таком случае эти системы, скорее всего, будут основаны на так называемом *трехэтапном протоколе Кака* (Kak's three-stage protocol).

До появления асимметричных шифров одним из наиболее распространенных предлагаемых решений был многоступенчатый, многоключевой (трехступенчатый) обмен ключами. В традиционном примере, где Алиса и Боб, пытаясь безопасно общаться через ненадежный канал, используют

трехступенчатый обмен симметричными ключами, Алиса зашифровывает предполагаемый секрет закрытым ключом, который знает только она, и затем отправляет его Бобу. Боб зашифрует то, что было ему отправлено, с помощью своего личного ключа, который знал только он, а затем отправит его обратно Алисе. Затем Алиса уберет свое шифрование, и оно останется зашифрованным секретным ключом Боба, а потом отправит его Бобу. Боб удаляет свое шифрование и читает открытое сообщение Алисы. Существенной для этого типа трехступенчатого шифрования является способность обеих сторон удалить собственное шифрование, особенно способность Алисы точно удалить ее шифрование после применения шифрования Боба (см. рис. 7.4).

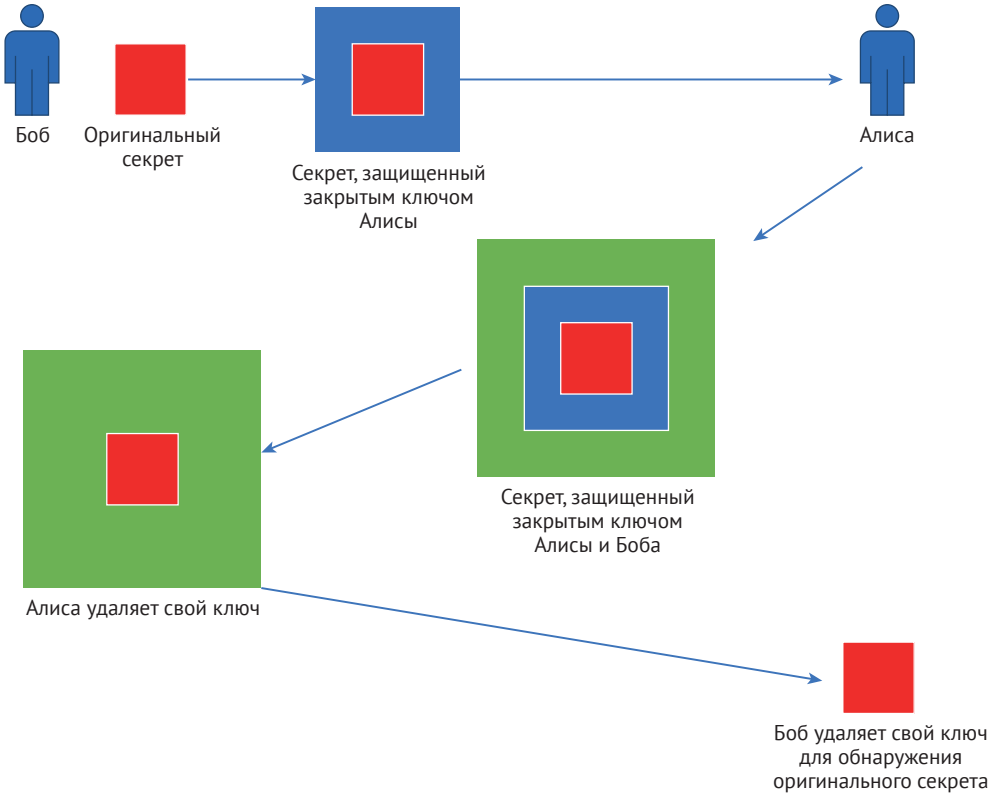


Рис. 7.4. Три этапа симметричного шифрования

В 2005 году инженер штата Луизиана Субхаш Как (Subhash Kak) опубликовал статью (https://arxiv.org/pdf/quantph/).0503027.pdf), в которой показал, как выполнить симметричный трехэтапный обмен ключами с использованием квантовых свойств. В настоящее время он известен как *трехступенчатый квантовый протокол*, или *трехступенчатый протокол Как*а. Он был реализован в реальных квантовых устройствах с использованием одно- и многофотонных методов. Однофотонный метод трудно или невозможно подслу-

шать без ведома уполномоченных сторон. Злоумышленник в середине может нарушить процесс, но нарушение может быть компенсировано механизмом коррекции ошибок.

С тех пор как была опубликована статья Кака, были разработаны дополнительные улучшенные версии с использованием нескольких фотонов и исправлением ошибок. Многофотонные реализации позволяют использовать больше потенциальных приложений, но увеличивают риск успешного подслушивания. Разработчики многофотонных реализаций включают другие средства защиты, чтобы компенсировать повышенный риск. Квантовый протокол Кака широко приветствовался, потому что он является чисто квантовым и, в отличие от других протоколов квантового обмена ключами, не использует классические компоненты.

Компании QKD

Есть много компаний, которые делают системы QKD, в том числе:

- ID Quantique (www.idquantique.com);
- MagiQ Technologies (www.magiqtech.com);
- Quintessence Labs (www.quintessencelabs.com).

ID Quantique производит три системы QKD (www.idquantique.com/quantum-safe-security/products/#quantum_key_distribution), включая более крупный сервер с оптическими блейдами. С другой стороны, каждый блейд может представлять в коммуникационном потоке QKD Алису или Боба. Их QKD-системы могут иметь протяженность до 100 км (62 миль) до того, как потребуется ретранслятор, и автоматически отправят оповещение и сигнал тревоги, если будет обнаружен подслушивающий злоумышленник. Компания MagiQ Technologies делает устройство QKD, известное как QPN, которое работает с использованием метода BB84 (www.idquantique.com/quantum-safe-security/products/#quantum_key_distribution).

Для получения дополнительной информации о QKD см. https://arxiv.org/pdf/1504.05471.pdf и https://ieeexplore.ieee.org/abstract/document/6459842.

Резюме

В этой главе мы исследовали квантовую криптографию. Квантовая криптография включает в себя генераторы случайных чисел, хеши, цифровые подписи и распределение ключей. Были рассмотрены квантовые генераторы случайных чисел и схемы распределения ключей, создававшиеся на протяжении почти двух десятилетий. Многие компании предлагают несколько современных моделей обоих типов. Размеры варьируются от большой комнаты размером с футбольное поле до маленьких компьютерных интерфейсных карт и чипов. Цены варьируются от нескольких сотен долларов до десятков тысяч. Эти типы устройств квантовой криптографии продолжают совершенствоваться. Их сложность и цены снижаются, их срок эксплуатации и допустимые расстояния увеличиваются, и их способность к взаимодействию с существующими системами с каждым днем становится лучше. Разрабаты-

ваются и тестируются новые протоколы и атаки. К сожалению, в настоящее время потребность в квантовых асимметричных шифрах, цифровых подписях или симметричных шифрах не слишком велика, и, возможно, так будет в течение многих лет. Множество квантовоустойчивых шифров, вероятно, уменьшит спрос на всю квантовую криптографию, по крайней мере до тех пор, пока не появятся достаточно дешевые квантовые устройства, чтобы стать конкурентоспособными.

Следующая глава расскажет, как эта криптография используется и совершенствуется для создания сетей, основанных на квантах.

8 Квантовые сети

Эта глава посвящена тому, как осуществляется сетевое взаимодействие квантовых устройств с использованием квантовых свойств. Квантово-устойчивая криптография, описанная в главе 7, безусловно, может использоваться и часто используется, но не является обязательной для квантовой сети. Квантовые сети имеют свои собственные проблемы и исследуются различными компаниями и государственными учреждениями уже более десяти лет. Теперь, когда приближающееся квантовое превосходство становится реальностью, стремление найти устойчивую квантовую сетевую модель набирает обороты. В этой главе будут рассмотрены специфика компонентов квантовой сети, проблемы и возможные приложения.

Сеть использует согласованный протокол связи для перемещения информации и контента от источника к месту назначения по какой-либо среде передачи, будь то беспроводная, проводная или другая (например, человеческие сети). Квантовая сеть использует квантовые устройства, свойства, алгоритмы и протоколы для передачи (квантовой) информации по сети. Как и любая другая квантовая технология, квантовые сети используют полный спектр квантовых свойств, хотя наиболее широко обсуждаются суперпозиции, запутанность и теоремы о неклонировании. Квантовая сеть может создаваться для связи квантовых устройств, физически отдаленных друг от друга, превращения их в более мощные объединения, облегчая передачу информации и контента (включая квантовую телепортацию). Если все будет сделано правильно, квантовая сеть обещает быть гораздо более безопасной и более непроницаемой к несанкционированному подслушиванию, чем сегодняшние неквантовые сети.

Компоненты квантовой сети

Как и любая сеть, квантовая сеть состоит из среды передачи, протоколов и сетевых устройств. Квантовые сети могут состоять из классических и квантовых компонентов или создаваться на чисто квантовой основе.

Среда передачи

Среда передачи включает в себя как физические кабели, так и свободную среду пространства.

Волоконно-оптические кабели

Физическая квантовая сеть в основном использует фотоны, и свет обычно передается через оптоволоконный кабель. В некоторых вариантах реализаций, основанных на свете в классических сетях, уже используется высококачественный оптоволоконный кабель, и он может быть применен для квантовых сетей. Для этого нужно заменить все приборы устройства, используемые для отправки и получения сигналов. Вместо отправки световых волн, которые кодируются и декодируются в двоичные представления, используются отдельные фотоны, и кодирование выполняется по отдельным квантовым свойствам каждого задействованного фотона. В других случаях создаются и используются специально создаваемые ультравысококачественные оптоволоконные кабели. Сетевые квантовые оптоволоконные кабели в большей степени защищены от внешних воздействий и внутренне более чувствительны к изменениям, которые необходимы квантовой сети. Кабельные квантовые передачи обычно имеют протяженность менее 100 км, хотя были созданы более длинные сети.

Теоретически для отправки каждого кубита используется только один фотон света, и это самый легкий метод обеспечения безопасности. Но однофотонные кубиты тем легче блокируются, теряются и расшифровываются, чем дальше они перемещаются по сети в реальном мире. Во многих квантовых сетях создаются, кодируются и передаются несколько фотонов, представляя один и тот же кубит информации для увеличения шансов представленного единственного кубита успешно доставить его от источника до места назначения. Это, однако, вызывает проблемы безопасности. Подробнее об этом – в разделе «Очистка запутывания» далее.

В зависимости от типа устройств, работающих в квантовой сети, используются различные длины волн света. Часто для создания различных длин волн и цвета используются алмазы, кристаллы и другие драгоценные камни и материалы. Они могут быть намеренно легированы дефектами или выбраны с естественными дефектами, чтобы создать желаемый признак, который может быть использован в квантовой сети.

Примечание Один из самых распространенных дефектов, обнаруженных в алмазах и используемых не только для квантовых сетей, называется *нитроген-вакантным центром* (*nitrogen-vacancy center*). Алмазы обычно состоят полностью из атомов углерода, но иногда в центр углеродной решетки алмаза вписывается атом азота. Углерод и азот находятся рядом друг с другом в периодической таблице элементов, и атом азота имеет на один электрон больше, чем атом углерода. Это создает «дополнительный», очень полезный, свободно плавающий электрон, который может использоваться в квантовых вычислениях и коммуникациях (помимо многого прочего). Слишком большое количество дефектов углерода в алмазах, с точки зрения любителей ювелирных изделий, снижает ценность камня, но такие алмазы отлично подходят для создания дополнительных используемых цветов и длин волн и манипулирования субатомными квантовыми свойствами. Для получения дополнительной информации смотрите https://en.wikipedia.org/wiki/Nitrogen-vacancy_center.

Среда свободного пространства

Среда свободного пространства включает в себя любую среду передачи, не связанную с физическим объектом. Самой распространенной квантовой средой передачи в свободном пространстве являются электромагнитные волны некоторого типа, в том числе микроволны, лазерные лучи и звуковые волны. Квантовые передачи могут отправляться из точки в точку от наземных отправляющих к принимающим станциям, от наземной станции к спутникам и обратно, или в некоторых других гибридных применениях. Передача в свободном пространстве гораздо более подвержена влиянию внешних воздействий.

Квантовый эксперимент со спутником продемонстрировал отправку запутанных фотонов на расстояние более 1200 км, а одиночные фотоны были отправлены со спутника на расстояние более 20 000 км. Как это происходит с сегодняшними традиционными сетями, спутниковые квантовые сети чаще всего рассматриваются как способ подключения распределенных наземных сетей и мобильных систем, хотя квантовые сети имеют специальные приложения для некоторых видов спутников (описано далее в разделе «Приложения квантовых сетей»). Трудно и дорого передать квантовый фотон на высокоорбитальный спутник на расстоянии 20 000 км. Если попытка передать один кубит по защищенному оптоволоконному кабелю затруднительна, то представьте себе попытку успешно передать тот же кубит через незащищенное пространство со всеми триллионами других квантовых частиц, которые он может встретить каждую секунду на этом пути. Проделать это удалось, но с трудом.

Китайские специалисты успешно провели эксперимент с использованием относительно недорогого (на низкой орбите) полета беспилотного аппарата для отправки и получения квантовой информации между двумя наземными узлами. Этот метод может быть использован для подключения наземных станций в нескольких сотнях километров. Пока прорабатываются соответствующие вопросы передачи в средах свободного пространства, на практике, скорее всего, будут широко применяться физические квантовые сети.

Расстояние против скорости

Все сети, их материалы и устройства подчиняются физическим законам природы, которые определяют, как далеко и быстро можно передавать информацию даже при использовании самого лучшего и эффективного оборудования. Квантовые сети в этом ничем не отличаются, хотя квантовые законы физики могут казаться более странными. Эти законы определяют, насколько длинной и быстрой может быть квантовая сеть, по крайней мере без устройства с повторителем (если не появится нечто принципиально новое, меняющее всю картину). В общем, чем длиннее квантовая сеть, тем медленнее передача информации, и наоборот. Есть теоретические максимумы для обоих параметров, в зависимости от используемой среды передачи.

Предел PLOB

Закон квантовой физики, известный как предел Пирандолы–Лоренцы–Оттавиани–Банчи (Pirandola–Laurenza–Ottaviani–Banchi, PLOB, https://arxiv.org/

pdf/1510.08863.pdf), говорит, что максимальная скорость, с которой кубиты могут передаваться через любой известный двухточечный, односторонний сегмент сети без дополнительных повторителей, равен $-\log_2(1 - x)$, где x – *коэффициент пропускания канала передачи сети* (transmissivity). Этот коэффициент определяет (максимальные) степень/скорость/длину, до которой любая среда позволит чему-либо проходить сквозь нее. Каждая среда передачи может физически разрешить чему-то (например, электричеству, свету, электромагнитному излучению и т. д.) передаваться через нее с определенной скоростью на определенном расстоянии до того, как передаваемая субстанция начнет разрушаться или вообще остановится.

Предел PLOB в зависимости от среды передачи устанавливает максимальную теоретическую скорость и расстояние для одного квантового сегмента сети из точки в точку без ретранслятора и, следовательно, максимальное расстояние для одного квантового ретранслятора или сегмента сети, по которому может передать информацию. Он устанавливает верхнюю границу того, насколько протяженной и/или быстрой может быть любая квантовая сеть (без ретранслятора) для квантовой передачи, в том числе для оптоволоконных кабелей и спутниковых линий. Он включает квантовую запутанность и рассматривает, как естественная энтропия ограничивает запутанность. Вряд ли когда-либо удастся получить максимальные скорости и расстояния, теоретически определенные PLOB для реальных сетей, что связано с экологическими и физическими проблемами.

Но поставщики квантовых сетей работают над тем, чтобы увеличить максимальное расстояние, и оценивают возможность работы своего оборудования в одном сегменте. Большинство поставщиков квантовых сетевых устройств тестируют свое оборудование на различных расстояниях и скоростях, и многие публикуют эти цифры, чтобы клиенты могли видеть, что они покупают с точки зрения производительности, а также с целью сравнения либо разных моделей оборудования в пределах своей линейки, либо с продукцией конкурентов. Обычно поставщик коммерческого оборудования для квантовой сети сообщает, как минимум, следующие данные: максимальные допустимые потери при передаче (в децибелах), максимальное расстояние канала передачи (в километрах), а также различные значения скорости, например 1,4 килобита генерируемых ключей на 50 километров. Оценки скорости всегда будут понижаться с увеличением расстояния. Хорошую статью о квантовом сетевом расстоянии и скорости обмена можно найти здесь: https://www.nature.com/articles/s42005-019-0147-3.pdf.

В каждой квантовой сети необходимо иметь дополнительные устройства и механизмы для преобразования кубитов, передаваемых по сети на все возможные устройства назначения. В классическом мире эти устройства часто называют сетевыми картами. В квантовом мире ими являются оптические переключатели, светоделители, детекторы или повторители (более подробно будут рассмотрены ниже).

Точка – точка

Почти все современные типы передачи в квантовых сетях являются двухточечными, т. е. от одного местоположения непосредственно к другому, источ-

ник – место назначения. Среда передачи по сети не поделена и не распределена. По сути, просто изображается линией, которая проходит от исходного узла к месту узла назначения. Чтобы расширить квантовую сеть на большее количество узлов, добавляются дополнительные соединения точка–точка.

Это связано с несколькими причинами, не последняя из которых заключается в том, что кубиты не хотят делиться (например, ввиду теоремы об отсутствии клонирования, сложности сохранения квантовых сигналов изолированными от внешнего мира, стоимости (двухточечные связи дешевле) и значительной сложности подключения сетевых точек). Общая облачная сетевая схема – святой Грааль квантовой сети и является очень востребованной. Наверняка однажды она войдет в обиход, но сейчас соединения точка–точка составляют большинство квантовых сетей. Меньшее, но растущее число квантовых сетей имеет большее количество двухточечных сегментов, которые в конечном итоге перерастут в большие сети и когда-нибудь даже сети общегородского масштаба.

Эту модель распространения сетей по принципу «сначала научись ходить, а потом бегать» можно сравнить с ранними днями классических сетей. Первые классические сети были двухточечными аналоговыми телефонными соединениями. В конце концов, традиционные сети созрели до такой степени, что стал использоваться либо общий «эстафетный токен» (например, Token Ring и другие), либо среда совместно с несколькими узлами с частыми повторными передачами (например, Ethernet). Интернет-соединения раньше были двухточечными и требовали внешнего телефонного набора (например, аналоговый RJ-11, ISDN, Frame Relay и т. д.), но в конечном итоге стала использоваться модель, которую мы имеем сегодня, где все, что нужно сделать узлу, – это подключиться к одной из многочисленных близлежащих точек агрегации (сервиса интернет-провайдера) или спутниковому каналу связи, что часто называют «последняя миля». Соседние соединения подключаются к более крупным глобальным сетям, которые затем подключаются к глобальной интернет-сети. Теперь практически любой желающий может отправить сетевой пакет данных по всему миру за несколько секунд. Нет сомнений, что однажды квантовые сети будут распространены до модели дом/узел, к которой мы привыкли сегодня. Но сейчас мы находимся в самом начале создания квантовых сетей. В настоящее время большинство квантовых сетей являются частными экспериментальными сетями «точка–точка» и содержат много повторителей для увеличения расстояний передачи. Существует два основных типа квантовых повторителей.

Доверенные повторители

В классическом сетевом мире все, что нужно сделать ретранслятору, – это захват, повторное усиление и повторная передача всех захваченных битов. Это можно сделать на физическом уровне, по существу, просто обнаруживая и повторно передавая электроэнергию почти со скоростью света. Однако теорема об отсутствии клонирования говорит, что дублирование сигнала и его реализация не могут быть выполнены в квантовой сети. Квантовая информация всегда может быть прочитана (декодирована в классический дво-

ичный файл), а затем перекодирована и отправлена в следующий квантовый сегмент сети, как новые кубиты. И это самый распространенный квантовый метод повторения, используемый сегодня.

Ключевая проблема при использовании этого метода в том, что нельзя быть полностью уверенным, что чтение ретранслятора и перекодирование информации осуществляются правильно и без непреднамеренного или преднамеренного вредоносного вмешательства. В чистом квантовом мире квантовая механика обеспечивает доверие. Вам не нужно передоверять операции каким-либо посредническим устройствам, потому что если кто-то вмешивается в них или подслушивает, то помехи могут быть немедленно обнаружены. Но если не все повторяющиеся устройства являются полностью квантовыми, как это часто бывает в современных квантовых сетях, безопасная передача информации должна быть обеспечена другим способом.

Ответ заключается в создании так называемого доверенного повторителя, в котором информация защищена использованием квантового кодирования, отправляемого одним или несколькими безопасными повторителями, которым все участники доверяют, с несколькими наборами квантовых ключей шифрования. Например, предположим, что у нас есть квантовая сеть, пытающаяся передать квантовую информацию из точки отправления A в точку назначения Z, с доверенным повторителем R между ними (как показано на рис. 8.1). Чтобы безопасность была обеспечена, обе стороны должны доверять R.

Рис. 8.1. Квантовая сеть, использующая доверенный повторитель

И A, и Z будут по отдельности создавать квантовые ключи (используя распределение квантовых ключей, как в главе 7), которые будут применяться для шифрования и безопасной передачи других ключей, которые создадут фактическое шифрование данных. Давайте назовем их ключами AR и ZR. Они будут делиться AR и ZR только с доверенным повторителем R. Затем узел A создаст ключ шифрования данных, который будет использовать между ним и Z (назовем его AZ-ключ). Узел A зашифрует ключ AZ ключом AR и отправит доверенному повторителю R. R расшифрует ключ, отправленный A, повторно зашифрует его ключом ZR, а затем отправит узлу Z. Z-узел расшифрует и теперь безопасно получит ключ AZ, созданный A. Когда A и Z захотят отправить данные друг другу, они будут шифровать эти данные с помощью ключа AZ, а затем отправлять в R. R прочитает/декодирует зашифрованные здесь квантовые данные (оставив их в зашифрованном состоянии), перекодирует и отправит другой стороне. Ясно, что R должен быть безопасным и доверенным во время первоначального обмена ключами AZ, чтобы все оставалось в безопасности. Трехступенчатый обмен ключами Kak (смотрите

главу 7) также будет работать без необходимости явно доверять повторителю, но модель доверенного повторителя является основной моделью повторения, используемой сегодня в большинстве расширенных квантовых сетей.

Квантовые повторители

Лучшая идея для поддержания чистой квантовости на протяжении всей передачи по сети заключается в использовании квантовой запутанности и телепортации (как описано в главе 5). Зачем беспокоиться о чтении/декогерировании квантовых данных и перекодировании их снова, если квантовое состояние может быть просто передано от источника к месту назначения в его первоначальном квантовом состоянии? Нам все еще нужны повторители, потому что еще есть максимальное расстояние, которое может быть одним сегментом сети точка–точка, но, по крайней мере, когда повторитель используется, он может сохранить данные в своем первоначальном квантовом состоянии, не декогерируя данные. Использование чисто квантового ретранслятора также означает, что присущие ему квантовые свойства обеспечивают защиту от нежелательного подслушивания. С чисто квантовым ретранслятором вы получаете и точность, и безопасность, которые может обеспечить доверенный повторитель в квантовой сети.

Чисто квантовые повторители используют телепортацию для передачи квантовой информации между сегментами. Как описано в главе 5, квантовая телепортация является косвенным способом использования одного или нескольких запутанных кубитов для передачи квантовых состояний. Напомним, что для квантовой телепортации сначала должны быть созданы и доставлены в исходные и конечные области запутанные квантовые частицы. Тогда дополнительные квантовые частицы добавляются к исходным квантовым частицам, и проводятся измерения, с тем чтобы получить различия. Эти различия затем передаются (любым из множества различных классических методов) в область назначения для восстановления искомых кубитов с использованием запутанных частиц пункта назначения. Как только целевые кубиты измерены, запутанность разрушается.

Примечание Как описано в главе 5, телепортация (по крайней мере, в настоящее время, если не всегда) не позволяет передачу быстрее скорости света, потому что ничто не может ее опередить, даже квантовая телепортация. Кроме того, квантовая телепортация всегда требует классического метода для передачи по назначению изменений на стороне источника, что означает, что квантовая телепортация по определению никогда не будет быстрее классических методов.

Квантовые повторители, использующие запутывание, были успешно созданы, и, вероятно, это лучший выбор для будущих зрелых квантовых сетей. Конечно, есть много вопросов, и не самый маленький из них состоит в том, что искусственные запутанные фотоны чрезвычайно легко разрушаются. Раньше мы не могли запутать кубиты на расстоянии большем, нежели несколько миллиметров друг от друга, хотя в реальном мире мы уверенно за-

путывали фотоны, находящиеся на расстоянии световых лет друг от друга. На сегодняшний день успешно продемонстрировано использование квантовой запутанности и повторителей квантовых сетей, по крайней мере, до 50 километров.

Это нелегко. Типы запутанных фотонов, которые в настоящее время создаются в лабораториях и на компьютерах, часто теряются при декогеренции, особенно чем дольше они отправляются по сетям. Они с большей вероятностью исчезнут среди шума окружающей среды, когда сеть удлиняется. Есть целый подраздел квантовой информатики, которая изучает *верность запутанности* (entanglement fidelity) и *оптимизацию запутывания* (entanglement optimization). Одно из решений – принять запутанный фотон, поступающий из квантового компьютера с запертыми ионами, который обычно при отправке по оптоволоконному кабелю долго не существует, и отправить его через специально разработанный кристалл, который преобразует длину волны запутанного фотона в нечто гораздо более удобное для успешной передачи. Оказалось, что кубиты, созданные внутри квантовых компьютеров, не самое лучшее для передачи по сети. Этот метод преобразует кубиты в другое состояние, которое более приемлемо для передачи по сети без необходимости декогеренции кубита из его начального квантового состояния.

Обмен запутанностью

Другая обычно исследуемая технология квантовых ретрансляторов известна как *обмен запутанностью* (entanglement swapping). По сути, это следующее решение: «Если А доверяет В и В доверяет С, то А доверяет С». Давайте предположим, что у нас есть узлы А и Z, представляющие источник и пункт назначения, как показано на рис. 8.2. Узел А имеет квантовую запутанность с квантовым повторителем, который мы будем называть R1. Узел Z также имеет квантовое запутывание с другим фотоном в квантовом повторителе, который мы будем называть R2. Узел А телепортирует квантовую информацию для квантового повторителя R с помощью запутывания R1. Квантовый ретранслятор принимает ту же разностную информацию, которая необходима для телепортации между ним и узлом А, и повторяет ее передачу между ним и узлом Z. Узел Z, используя запутывание R2 и переданную разностную информацию, может реконструировать информацию, передаваемую узлом А.

Рис. 8.2. Представление обмена запутанностью

Были успешные эксперименты по обмену запутанностью, и это, вероятно, станет методом квантового ретранслятора в будущем. В настоящее время был продемонстрирован полезный обмен запутанностью между узлами на расстоянии до 1,3 км. С достаточным количеством квантовых ретранслято-

ров и квантовым обменом мы могли бы создать что-то, очень похожее на наш интернет, но в чисто квантовом состоянии.

Квантовые сетевые протоколы

Каждая сеть нуждается в протоколах. Сетевые протоколы являются предварительно согласованными методами и форматами для передачи данных между двумя или более участвующими узлами. Никто пока не знает, как будут выглядеть окончательные квантовые сетевые протоколы, хотя начинают предлагаться и проверяться некоторые стандарты. Группа квантовых исследователей создала официальный интернет-проект (https://tools.ietf.org/pdf/draft-dahlberg-ll-quantum-02.pdf) по определению канальных уровней сети, что может в дальнейшем привести к созданию квантового интернета.

Примечание Канальный уровень (данных) – это модель низкого уровня общих абстрактных уровней сетевого протокола. В наиболее распространенной модели Open Systems Interconnect (OSI) все связи в сети могут быть определены как существующие на одном из семи объединенных, взаимозависимых уровней: физический, канал передачи данных, сеть, транспорт, сеанс, презентация и приложение. Канальный уровень помогает получить данные (в форме дейтаграмм) двум напрямую соединенным узлам. Он обрабатывает и исправляет ошибки (это связано с физическим уровнем), а также устанавливает и разрывает каналы связи. На этом уровне в традиционной сети функционируют мосты Ethernet и коммутаторы.

В квантовых сетях протоколы связи будут помогать общаться двум квантовым узлам, включая использование запутывания и, в частности, обмен запутываниями (как рассматривалось ранее). Разработчики протокола хотят, чтобы любые три участвующих узла могли легче инициировать обмен запутываниями с целью облегчения в дальнейшем обмена запутываниями множеству междугородных сетей, создавая полностью связанные, распределенные квантовые сети, аналогичные тем, которые мы имеем сегодня, но с большей защитой от подслушивания.

Одна из основных задач квантового канального уровня – помочь узлам передавать предназначенные им запутанные кубиты, обеспечивая общение. Как вы помните из главы 1, создание/измерение квантовых свойств является вероятностным, то есть вы никогда не сможете полностью предсказать результат какой-либо квантовой операции. Вы можете предсказать только процент вероятности конкретных результатов по серии попыток. Скажем, вам нужно отправить по сети «1» в качестве квантовой информации. Вы не можете просто детерминистически создать кубит, представляющий «1» (как определено протоколом), с первой попытки, как вы могли бы легко сделать в классической сети. Вы не можете сказать «мне нужен кубит, представляющий “1”», и первый созданный вами кубит волшебным образом будет гарантированно равен «1». Вы можете, однако, создать один или несколько кубитов, пока не получите кубит, который представляет «1». Помните, что сделать это намного сложнее в связи с тем фактом, что если вы непосредственно

измеряете кубит, то переводите его в неквантовое состояние. Точно так же вы не всегда можете гарантировать, что с первой попытки сразу создаете запутанные кубиты и правильно запутанные кубиты. Квант является вероятностным, а не детерминированным.

Протокол квантового канального уровня был разработан специально для решения этой проблемы. Физический уровень все равно должен будет изначально создавать правильные запутанные кубиты (это может занять одну или несколько попыток). Канальный уровень гарантирует, что кубиты являются «правильными» и что они запутаны. Канальный уровень позволит узлам отбрасывать «неправильно» запутанные кубиты, заново создавать и повторно передавать «правильно» запутанные кубиты и сообщать узлам о различии «правильных» кубитов и шума.

В этих целях канальный уровень делает несколько вещей, включая создание и использование сигнала-предвестника (heralding signal), который указывает, что запутанная пара кубитов была создана, и назначает логический «идентификатор запутанности» каждому запутанному набору кубитов. Это позволяет различным узлам отслеживать «правильно» запутанную пару кубитов при обмене между узлами. Более высокие уровни квантовой сети могут запросить запутывание пар, отправив сообщение *CREATE* (Создать). Канальный уровень затем работает с физическим уровнем, чтобы создать спроектированные запутанные пары. Канальный уровень отвечает верхним уровням с помощью *ACK* (т. е. acknowledgment, подтверждение) или *OK*. Ответ ACK сообщает верхнему уровню, что канальный уровень принял его запрос и запланировал пару запутывания для генерации. Он также включает в себя *CREATE ID* (Создать идентификатор), так что каждый может отслеживать точно запрошенную пару запутывания. OK означает, что запрошенные запутанные кубиты были созданы.

Присутствуют даже величины *доброкачественности и временно́й доброкачественности* (goodness and time of goodness values), которые я не встречал в других стандартах сетевых протоколов (хотя, если честно, я не трачу все свое свободное время на чтение сетевых протоколов). Величина доброкачественности указывает, насколько сильна запутанная пара (значение, которое протокол и теория квантовой запутанности также называет *верность* (fidelity)). Временна́я доброкачественность – это оценка того, как долго запутанность должна держаться перед декогерированием. Важно, чтобы задействованные узлы понимали, как долго они должны передавать/обмениваться запутыванием с другим узлом, прежде чем связи запутанности станут ненадежными. Есть много других полей и типов информации, передаваемой туда и обратно между канальными верхними уровнями. На рис. 8.3 показаны структура и обозначения сообщения OK канального уровня типа K, как в настоящее время определено в предложенном проекте «Протокол квантового канального уровня», который финансировался организацией Европейского союза (EU Flagshipon Quantum Technologies) и является частью квантового интернет-альянса (the Quantum Internet Alliance).

Канальный уровень управляет легкостью и надежностью квантового запутывания и обмена. Сетевой уровень гарантирует, что переданные запутанные кубиты надежно передаются от источника к месту назначения по всей

сети. Транспортный уровень обрабатывает кубиты, перемещаемые через сеть, отделенные от запутывания или сетевого уровня, и передает результаты в прикладной уровень. Предложенные нижние уровни стека квантовой сети выглядят примерно как на рис. 8.4.

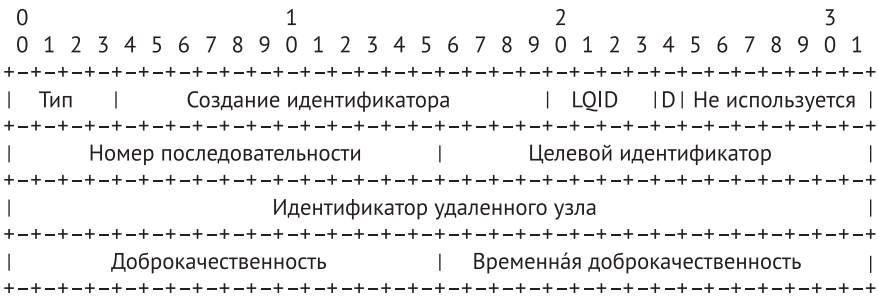


Рис 8.3. Структура и обозначения сообщения OK квантового канального уровня типа K

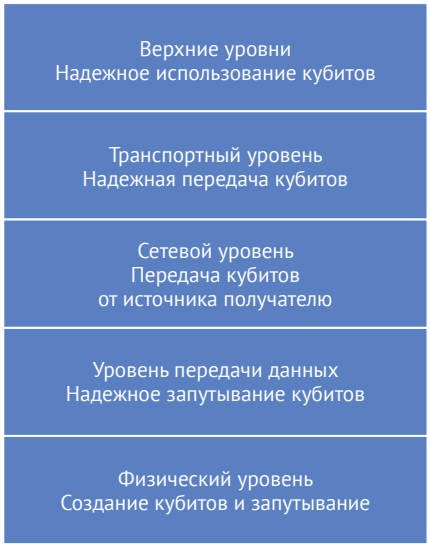


Рис. 8.4. Представление предлагаемых нижних уровней стека квантовой сети

Верхние уровни модели, по сути, являются уровнями приложений, и если нижние уровни уже выполнили свою работу, верхние не должны беспокоиться о надежности передачи кубита. Они необходимы, и они появляются. Устройства назначения и приложения просто берут их. Все просто.

Конечно, ни один из квантовых сетевых стеков еще не выходит за рамки предложенной теории и индивидуальных экспериментов. Но были продемонстрированы сетевые коммуникации с использованием предложенного протокола сообщения при обмене информацией между различными типами квантовых устройств.

В целом мысль о том, что многие исследователи уже сегодня пытаются выяснить, как создать квантовую сетевую связь, включая запутывание и обмен,

процедуры и надежность, весьма вдохновляет. Ведь это свидетельство того, что квантовые информационные науки в целом становятся более зрелыми и к тому же технологически более надежными. Для получения дополнительной информации о протоколах квантовой сети смотрите https://arxiv.org/pdf/1904.08605.pdf и https://tools.ietf.org/pdf/draft-vanmeter-qirg-quantum-connection-setup-00.pdf.

Очистка запутывания

В настоящее время квантовая запутанность и обмен являются нелегким делом. Вы начинаете с вероятностных квантов и пытаетесь создать запутанные пары, которые могут затем быть отправлены по сети с использованием QKD, доверенных повторителей или квантовых повторителей. Почти все на этом пути (то есть во внешней среде) пытается ослабить передачу квантовой информации. Любые ошибки, которые не обнаруживаются на физическом или канальном уровнях, будут распространяться вдоль всей остальной части сети и сетевого стека. Один из способов уменьшить количество ошибок – использовать канальный уровень, который обрабатывает обнаружение ошибок на физическом уровне и использует повторную передачу, чтобы помочь создать надежные квантовые запутывания и перестановки по всей цепочке сети.

Другой метод заключается в создании с самого начала нескольких идентичных квантовых пар запутывания, поскольку, создавая больше пар, по крайней мере одну из них мы получим в месте назначения с большей вероятностью. Допустим, например, что начальный узел создает 20 идентичных пар запутывания, каждая из которых представляет один и тот же кубит информации. В конечном итоге пусть 10 из начальных 20 пар окажутся в месте назначения, но три из «одинаковых» пар разные. Большинство наблюдателей логично предположили бы, что 7 идентичных пар с большей вероятностью будут правильно представлять значение исходного свойства кубита, по сравнению с 3 парами, которые в меньшинстве. Процесс использования нескольких идентичных запутанных пар кубитов для создания более точной передачи в сети известен как *очистка запутывания* (entanglement purification). Долгосрочная цель состоит в том, чтобы «уменьшить» количество необходимых дубликатов копий, но иметь лучшую *верность* (т. е. точность). Есть много ученых, работающих над очисткой запутанности и верностью, как и квантовых ученых, пытающихся уменьшить ошибки вычислений квантовых кубитов, используя коррекцию квантовых ошибок, что в конечном счете должно привести к увеличению длины и повышению надежности квантовых сетей.

Квантовые сетевые приложения

Так зачем нам нужны квантовые сети? Каковы их приложения?

Примечание Этот раздел посвящен сильным сторонам квантовой сети, и не в связи с квантовыми компьютерами и приложениями, которые работают на них (об этом говорилось в главе 5).

Более безопасные сети

Во-первых, и главным образом, квантовые сети имеют встроенную присущую им защиту от прослушивания, которую классические сети просто не могут иметь. Это не значит, что квантовые сети могут стопроцентно застраховать от подслушивания (взломать можно все), но по умолчанию они намного больше защищены по сравнению с классическими сетями. Нет сомнений, что у людей возникнет желание попытаться преодолеть эту защиту, и квантовые сети имеют еще много существенных уязвимостей, которые хакеры найдут и будут использовать. Но когда эти уязвимости будут устранены, состояние квантовых сетей по умолчанию будет значительно сложнее взломать, и это огромный бонус.

Примечание Все правительства мира и правоохранительные органы стран ведут борьбу с любым дефолтом каналов шифрования, который может затруднить (юридически) сбор доказательств неправомерных действий при проведении расследований. В большинстве стран сетевые провайдеры *обязаны* создать условия для выполнения закона принудительного прослушивания любого сетевого потока связи под контролем провайдера. Будет интересно посмотреть на эти требования подслушивания, когда технология по умолчанию предотвращает подслушивание. Существует вероятность того, что для сетевых провайдеров или правоохранительных органов станет невозможным шпионить за кем-либо, и с этим потенциально невозможно будет что-либо сделать технически, не избавившись в какой-то момент от квантовой сети. Это будет интересное время, когда придется искать компромиссы между квантовой безопасностью и насущными потребностями государственных структур.

Облако квантовых вычислений

Квантовые вычисления обещают решить многие проблемы, и в том числе те, над которыми человечество работало на протяжении тысячелетий. Это даст нам возможность лучше понять природу нашей Вселенной, предсказывать будущее и создавать продукты и услуги, которые мы сегодня не можем себе представить. Представьте, как это было бы замечательно – собрать как можно больше квантовых компьютеров и заставить их работать одновременно над одной и той же проблемой! Это было бы похоже на совместную работу целой команды Эйнштейнов вместо одного. Облако квантовых вычислений представляет собой совокупность квантовых суперкомпьютеров, объединенных в сеть и синергетически работающих вместе, что позволяет им выполнять свои задачи быстрее и эффективнее. Облако квантовых вычислений – это совместная более быстрая работа.

Лучшая временна́я синхронизация

Есть много приложений, которые требуют очень точного времени. У нас уже есть часы, показывающие сверхточное время. Они известны под названи-

ем «атомные часы» и уже настолько точны, что теряют меньше секунды за миллиард лет (https://en.wikipedia.org/wiki/Atomic_clock). При этом сохраняется вопрос: как получить максимально точное время для автономного устройства, находящегося очень далеко, или синхронизировать каждое зависимое устройство в конкретном сервисе или сети с другими устройствами, чтобы все они показывали одно и то же время? На то, чтобы передать время, требуется немало времени!

Квантовые сети не предлагают более быструю передачу времени (вспомним, что события в классическом мире уже идут почти со скоростью света, и квантовая механика, скорее всего, не нарушит ограничения, заданного скоростью света, если наши фундаментальные знания не претерпят изменений). Но квантовые сети могут предложить лучшую синхронизацию времени между зависимыми устройствами. Причина в том, что квантовые устройства и сети могут учитывать больше факторов временно́й синхронизации при выполнении коррекции ошибок времени / синхронизации. Спад временно́й синхронизации в любой большой сети будет меньше.

Например, система глобального позиционирования (GPS) работает с использованием серии спутников на орбите, которые могут применяться приемниками GPS для определения своего географического положения. Для того чтобы правильно определить, где находится приемник GPS, и спутники GPS, и приемники должны синхронизироваться по времени. Чем точнее время на всех устройствах и чем более точно оно синхронизируется у всех участников, тем более точно GPS-приемник определяет свое местоположение. У спутников GPS есть на борту атомные часы, и они очень точны, но без синхронизации они могут терять до 10 наносекунд каждые 24 часа (https://www.insidescience.org/news/quantum-way-synchronize-atomic-clocks), а наносекунда соответствует разнице в расстоянии примерно в фут. Из-за этого время GPS-часов обновляется, так что оно не теряет ни одной наносекунды в течение года. Служба синхронизации времени GPS постоянно обновляется, чтобы время на спутниках оставалось как можно более точным. Еще в 2000 году приемник GPS мог иметь точность до 5 метров / 16 футов. Сегодня из-за улучшений в технологии GPS, включая синхронизацию времени, приемники GPS могут отслеживать свое положение с точностью до 30 сантиметров / 11,5 дюйма. Квантовая синхронизация времени сделает систему GPS еще более точной.

Хотя все атомные часы в конечном итоге работают на квантовой механике, синхронизация времени сети, которую используют спутники GPS, является классической. Это означает, что квантовые свойства, которые на самом деле выполняют реальную работу, должны быть декодированы в наш классический мир, а затем переданы классическим путем. Но квантовая синхронизация времени пропускает шаг преобразования, остается квантовой и позволяет синхронизации времени быть еще более точной. Это означает, что определение местоположения GPS будущего можно будет измерять в миллиметрах вместо сантиметров или, по крайней мере, всего в нескольких сантиметрах вместо 30. Это означает не только то, что вы во время вождения не пропустите поворот налево, но и то, что квантовые системы в течение ближайших одного-двух десятилетий будут более точно отслежи-

вать нахождение сотен миллионов автомобилей с автоматическим управлением, которыми мы будем пользоваться. Это означает, что люди в городах с небоскребами смогут более точно определить дверь, в которую им надо войти. Инженеры смогут более точно провести измерения и т. д. Квантовая синхронизация времени сделает каждый зависимый от времени сервис более точным и более успешным.

Примечание Интересно, что на протяжении многих лет квантовые часы считались наиболее точными атомными часами, но теперь при точных измерениях их вытеснили решетчатые оптические часы. Однако даже устройства синхронизации, основанные на решетчатых оптических часах, могут извлечь выгоду из квантовой синхронизации времени.

Предотвращение помех

Задолго до 1940-х годов, когда австрийско-американская актриса Хеди Ламарр (Hedy Lamarr) и ее соавтор Джордж Антейл (George Antheil) предложили новый способ предотвращения глушения военных беспроводных торпед (они изобрели в качестве защиты от помех *скачкообразную перестройку частоты*), военные во всем мире пытались подавить беспроводные сигналы противника, сделав собственную связь помехоустойчивой. В общем, защита от помех может включать инструкции управления серией модулированных изменений частоты/сигнала, которые противник не может распознать, имитировать или блокировать.

Постановщики помех делают все возможное, чтобы выяснить, как сигнал передается на управляемое устройство. Если они могут выяснить, как изменяются частоты, то могут восстановить инструкции управления, понять, как действует устройство, и даже, возможно, перепрограммировать его, чтобы воспользоваться им в своих целях. На войне знающий это противник может послать вражескую ракету или торпеду назад к отправителю. Это не фантазия. На Второй мировой войне это происходило все время.

Постановщик помех может и не выяснять, как работает управляющий сигнал противника. Все, что ему нужно сделать, – заблокировать все возможные задействованные частоты и препятствовать получению беспроводным устройством новых или обновленных инструкций. В большинстве случаев «ослепшее» устройство, такое как ракета или дрон, в каком-то режиме, например по умолчанию, продолжает лететь по последнему указанию курса или полетит обратно. Сегодня в военной отрасли используется масса технологий создания помех и противопомех.

Разработчики оружия стараются сделать свое оружие более устойчивым к помехам, а постановщики помех продолжают придумывать новые способы глушить их системы управления. Примерно та же ситуация наблюдается и в мире компьютерных технологий: хакер изобретает способ выяснить секретный код, а криптограф пытается улучшить шифр для предотвращения успешных атак.

Квантовые сети, имеющие присущие им свойства суперпозиции, запутанности и отсутствия клонирования, идеально подходят для создания помехо-

устойчивых сигналов. У устройства с квантовой поддержкой, использующего квантовую сеть, будет гораздо больше шансов создать более изощренное, устойчивое к помехам управление сигналами и игнорировать фоновый сигнал противника. Так что даже если враг посылает миллион изменений частоты на тысячах возможных частот, снова и снова пытаясь создать помеху, то квантовое устройство, скорее всего, сможет выяснить, какие команды являются нужными, а какие следует просто игнорировать как фоновый шум.

Предотвращение подавления управления не является прерогативой военных. Таким же способом могут пресекаться попытки злоумышленников прослушать разговоры по сотовому телефону и нарушить сетевой трафик Wi-Fi, а также отправить ошибочные инструкции автономному автомобилю. Предотвращение помех делает нашу жизнь лучше, и квантовая сеть может помочь нам в этом.

Квантовый интернет

Святой Грааль квантовой сети – это полная замена существующего классического интернета. И подобно классическому интернету, квантовый, скорее всего, на заре своего существования будет представлять собой разнородную массу отдельных сетей, начиная с хорошо финансируемых военных, правительственных и университетских, которые затем будут расширяться и охватывать все больше пользователей. Миллионы подключенных к интернету квантовых устройств в конечном итоге сформируют огромное глобальное вычислительное облако. Будет сложнее совершать вредоносные действия и вмешиваться в работу сети, что позволит нашему миру наслаждаться всеми квантовыми улучшениями, подобно тому как мы освоились с современным интернетом.

Примечание Программа под названием SimulQron (http://www.simulaqron.org/) – это симулятор, помогающий разработке квантового программного обеспечения для интернета (https://arxiv.org/pdf/1712.08032.pdf).

Над квантовым интернетом работает несколько команд и консорциумов, в том числе the European Union's Quantum Internet Alliance (https://twitter.com/eu_qia), начинающий демонстрационный проект в четырех городах Нидерландов – Амстердаме, Лейдене, Гааге и Делфте. Проект включает в себя все компоненты, необходимые для создания большой квантовой глобальной сети, которая должна быть введена в эксплуатацию к 2020 году. Затем планируется расширить его для всего Европейского союза.

Другие квантовые сети

В настоящее время все существующие квантовые сети имеют довольно ограниченное применение и носят экспериментальный характер, даже притом что каждый день их появляется все больше. В 2018 году QKD на основе оптоволокна была успешно продемонстрирована на расстоянии 421 км (261 ми-

ля). Большинство существующих систем QKD для коммерческой продажи имеют максимальную передачу на расстояние 100 км (62 мили), так что эта экспериментальная сеть в четыре раза больше. Ожидается, что расстояние, на которое квантовые системы QKD смогут передавать, продолжит расти.

Особенно большое внимание сетевым аспектам квантовой информации уделяет Китай. В 2016 году Китай запустил первый квантовый спутник связи Micius (https://www.bbc.com/news/world-asia-china-37091833). Спутник безопасно отправлял раздельно, используя QKD, индивидуальные секретные ключи на наземные станции в Пекине и Вене, находящиеся на расстоянии 7500 км (4700 миль) друг от друга. Затем он создал третий ключ для совместного использования всеми участниками. Он шифровал третий ключ с каждым из ранее переданных индивидуальных секретных ключей наземной станции. Каждая наземная станция может затем третьим ключом расшифровать общий секрет и начинать шифровать сообщения друг с другом. Это был знаковый эксперимент.

Спутник Micius может работать только при наличии прямой видимости и не может работать при солнечном свете. Тем не менее он был использован для успешной демонстрации на созванной 75-минутной видеоконференции, что является более чем адекватной демонстрацией первого поколения, первого в своем роде квантового спутника. Вы можете прочитать больше о системе Micius здесь: https://www.wired.com/story/why-this-intercontinental-quantum-encrypted-videohangout-is-a-big-deal/, https://cosmosmagazine.com/technology/the-quantum-internet-is-already-being-built и https://en.wikipedia.org/wiki/Quantum_Experiments_at_Space_Scale. Китай также создает основную коммуникационную квантовую магистраль между Шанхаем и Пекином, расстояние между которыми составляет 2000 км (1200 миль). Она соединяет 4 города и имеет 32 узла.

Примечание Некоторые ученые, работающие в области квантовой информации, скептически относятся к заявлениям Китая о квантовых сетях или сомневаются, что они на 100 % являются квантовыми.

Япония продемонстрировала квантовую сеть с использованием квантовых повторителей (https://qiqb.otri.osakau.ac.jp/wp-content/uploads/2019/01/AllPhotonicQR-QIQBen.pdf). В качестве квантовых ретрансляторов (известных как фотоника) были использованы оптические устройства, которые позволили отправлять квантовую информацию без классических компонентов и использования квантовой памяти.

Команда из США работает над созданием квантовой сети 48 км (30 миль), используя квантовую запутанность и телепортацию (https://spectrum.ieee.org/tech-talk/telecom/security/us-national-labs-join-forces-on-a-quantum-network). Большинство исследователей квантовых сетей в США применяют QKD, и данный проект Национальной лаборатории США, расположенной недалеко от Чикаго, будет одним из первых, использующих телепортацию. Министерство энергетики США предоставило для этого проекта несколько миллионов долларов. Национальные лаборатории (Аргоннская национальная лаборатория и Национальная ускорительная лаборатория Ферми) вместе с Чикагским университетом создали официальную организацию Chicago Quantum

Exchange (Чикагская квантовая биржа) (https://quantum.uchicago.edu/). В ней участвует более 100 исследователей квантовой информации.

Квантовые сети уже существуют и работают на стадиях эксперимента в нескольких реальных проектах и устройствах и будут доступны через несколько лет.

Где получить больше информации

Quantum Network, Rodney Van Meter, Wiley, 2017, https://www.worldcat.org/title/quantumnetworking/oclc/879947342.

The Quantum Internet Is Emerging, One Experiment at a Time, Anil Ananthaswamy, Scientific American magazine, June 19, 2019, https://www.scientificamerican.com/article/the-quantum-internet-is-emerging-one-experiment-at-a-time/.

The Quantum Internet, H. J. Kimble, June 25, 2008, white paper, https://arxiv.org/pdf/0806.4195.pdf.

A Poisson Model for Entanglement Optimization in the Quantum Internet, Laszlo Gyongyosi and Sandor Imre, Quantum Information Processing, June 5, 2019, https://link.springer.com/content/pdf/10.1007%2Fs11128-019-2335-1.pdf.

The quantum internet has arrived (and it hasn't), Davide Castelvecchi, Nature Magazine, February 14, 2019, https://www.nature.com/articles/d41586-018-01835-3.

Internet Research Task Force (IRTF) research group on quantum Internet called QIRG. Qirg mailing list submissions to qirg@irtf.org. Чтобы подписаться или отписаться, посетите https://www.irtf.org/mailman/listinfo/qirg.

Резюме

Квантовые сети как основное технологическое средство будут расти и расширяться, так же, как и остальная часть квантовой информации. Квантовые сети начнутся с классических составляющих (например, доверенных повторителей) и будут использовать QKD для обмена безопасными ключами, а затем перейдут к полному стеку, основанному на квантовой сети с использованием истинных квантовых повторителей, квантовой запутанности, телепортации и квантового обмена. Ограниченные экспериментальные сети скоро будут заменены реальными, рабочими, квантовыми сетями. В конечном итоге многие, если не все, сети нашего классического интернета будут заменены квантовыми сетями по множеству причин, и не последней в их ряду является более высокая их надежность, обеспечиваемая квантовой механикой.

Все предыдущие главы были посвящены квантовой механике, вычислительной технике, криптографии и причинам, по которым квантовые компьютеры, скорее всего, скоро взломают криптокоды с открытым ключом. Часть II началась с описания квантовоустойчивой и квантовой криптографии. Эта глава была посвящена квантовым сетям и их компонентам, проблемам и вероятным приложениям. Глава 9 расскажет, как всем заинтересованным сторонам надо готовиться к грядущему квантовому прорыву и революции.

9 Готовимся сейчас

Грядет квантовый криптографический прорыв. Вопрос только, когда. Когда этот прорыв случится, это лишит законной силы большую часть мировой криптографии с открытым ключом и, как минимум, на 50 % ослабит другую существующую криптографию. И это не самый худший сценарий, не включающий многие другие квантовые успехи, которые могут сделать еще проще раскрытие симметричных шифров и хешей.

В предыдущих главах мы обсуждали квантовую механику, квантовые компьютеры, сети и грядущие изменения, в том числе вероятные криптографические взломы. В этой главе обсуждается то, как вы и ваша организация можете начать подготовку сегодня, до того, как произошел этот прорыв. Скорее всего, именно ради этой информации многие из вас купили данную книгу. Сначала мы рассмотрим четыре основных этапа любого проекта смягчения последствий постквантового прорыва, а затем сосредоточимся на последовательности шагов осуществления проекта.

Четыре основных этапа смягчения последствий постквантового прорыва

Постквантовые проекты по смягчению последствий в большинстве организаций будут включать следующие четыре основных этапа:

- этап 1: укрепление существующих решений;
- этап 2: переход к квантовоустойчивым решениям;
- этап 3: внедрение квантово-гибридных решений;
- этап 4: внедрение полностью квантовых решений.

На рис. 9.1 графически представлен каждый этап. Каждый этап проекта будет обсуждаться более подробно в следующих разделах.

Этап 1. Укрепление существующих решений

Каждая организация должна по возможности скорее обновить любую слабую квантовоустойчивую криптографию, использовать современную квантовоустойчивую криптографию и увеличить размеры ключей. Квантовые вычисления с использованием алгоритма Гровера вдвое уменьшают защитную силу существующих симметричных шифров и хешей, поэтому имеет смысл удваивать размер ключей и хешей, особенно там, где это нетрудно сделать. Например, любые системы, использующие AES-128, должны быть переве-

дены на AES-256 или выше. Если у вас есть критические данные, которые должны быть защищены на протяжении 10 лет, даже если они используют AES-256, возможно, вам следует усилить их до AES-512 и т. д.

Размеры ключей асимметричных шифров должны быть обновлены как минимум до 4096 бит. Большинство открытых ключей сейчас 2048- и 1024-битные. Когда квантовые компьютеры получат кубиты и приобретут соответствующие способности, они в первую очередь будут взламывать меньшие размеры ключа. Переходя к большему размеру ключей в вашей существующей криптографии, вы снижаете риск, хотя и не так сильно, как если бы вы имели возможность немедленного перехода к истинно квантовой устойчивой криптографии. Измените политику определения минимально допустимых размеров ключей в вашей организации.

Рис. 9.1. Четыре основных этапа проектов смягчения последствий постквантового прорыва

При всем этом не всегда будет возможно перейти к ключам большего размера для существующей криптографии. Многие приложения жестко запрограммированы, а многие другие могут принимать только определенные размеры ключей (и не все размеры ключей, приведенные в стандарте). Например, SHA2 поставляется в 224-, 256-, 384- и 512-битных размерах. В течение многих лет Microsoft Windows могла безупречно использовать SHA2-256 (размер ключа SHA2 по умолчанию), но у вас будут проблемы с работой на сайтах, защищенных TLS, если вы перейдете на SHA2-512 (эта «ошибка» была исправлена несколько лет назад). Windows по-прежнему по умолчанию не предлагает SHA2-224 (хотя это часть официального стандарта), когда вы используете его встроенное программное обеспечение. Многие приложения

принимают только один размер ключа или, может быть, два. Некоторые из них могут принять более крупные размеры ключей, и у них возникнут непредвиденные проблемы в работе. Поэтому увеличивать размер ключей всегда необходимо после тщательного тестирования, чтобы убедиться, что это не вызовет проблем.

Вы также должны помнить, что переход к максимально возможному размеру ключа может снизить производительность устройства. Каждый бит, добавляемый вами в криптографический ключ, увеличивает количество вычислений, необходимых для использования криптографии. Во многих случаях, например при переходе с RSA 2048 бит на 4096 бит, снижение производительности происходит, но почти незаметно для большинства пользователей и в большинстве сценариев. Однако в некоторых сценариях с высокой транзакцией, таких как популярные веб-сайты или базы данных, изменение может стать заметным и оказывать неблагоприятное влияние при увеличении трафика.

В некоторых сценариях снижение производительности может быть неприемлемым даже для одного пользователя и низкого трафика. Например, несколько лет назад один из моих клиентов перенес сертификацию инфраструктуры открытых ключей (public key infrastructure, PKI) цифрового сертификата авторизованного сервера с 2048 до 16 384 бит лишь по той причине, что хотел обеспечить максимальную безопасность. Увеличение битов было настолько значительным, что большинству его компьютеров потребовалась минута, чтобы открыть любое зашифрованное сообщение, которое в итоге было привязано к корневой сертификации 16 КБ цифрового сертификата. Сравните это с 1–1,5 секунды, необходимыми, чтобы открыть то же сообщение, используя 2048-битный ключ. Цифровой сертификат большего размера был безопасным, но, вероятно, чрезмерно безопасным и определенно слишком медленным для используемого оборудования и приложений, в то время как при применении 4096-битных ключей была бы обеспечена и достаточная безопасность, и скорость.

Следует ли увеличивать размеры асимметричных ключей?

Некоторым читателям, возможно, интересно узнать, имеют ли какой-либо практический смысл обновление размеров асимметричных ключей и попытка опередить ожидаемое продолжающееся увеличение возможностей квантового компьютера. Ответ на этот вопрос – не просто «да» или «нет», хотя увеличение размера асимметричного ключа как минимум до 4096 бит не может повредить, и вы можете сделать это легко и естественно, когда срок действия старых ключей истекает.

Но есть хорошие аргументы не только «за», но и «против» увеличения размера асимметричных ключей для борьбы с грядущим квантовым прорывом. Например, используя алгоритм Шора, квантовому компьютеру необходимо не менее $(2 \times n) + 3$ стабильных кубитов, где n – количество битов ключа для взлома. Итак, чтобы взломать 2048-битный RSA-ключ, квантовому компьютеру нужно 4099 стабильных кубитов, а для взлома 4096-битного ключа RSA ему нужно 8195 стабильных кубитов. Таким образом, если вы увеличите асимметричные шифры с 2048 до 4096 битов, эта стратегия будет защищать

вас, пока квантовые компьютеры не будут иметь, по крайней мере, 8195 стабильных кубитов (при условии использования меньшего количества кубитов квантовый компьютер не будет достаточно быстрым).

В настоящее время мы не знаем, сколько потребуется времени, прежде чем квантовые компьютеры будут иметь 4099 стабильных кубитов, и сколько времени потребуется, чтобы добраться до 8195. Но увеличение от 100 кубитов до 4099, вероятно, не займет столько времени, сколько его потребовалось, чтобы добраться до первых 100 кубитов. Когда общество научится создавать кубиты в больших масштабах, увеличение будет расти довольно быстро.

Однако существуют соображения, добавляющие сложность. Если верить некоторым оценкам исправления ошибок, каждый стабильный кубит в настоящее время занимает от сотен до более миллиона исправляющих ошибки кубитов, так что можно говорить о разнице в кубитах в количестве многих миллиардов, необходимых для взлома 2048-битного ключа по сравнению с 4096-битным ключом. Если оценки исправления ошибок верны, то, скорее всего, увеличение количества вспомогательных кубитов для более длительного периода защиты стоит того.

В то же время многие разработчики новых алгоритмов квантового факторинга утверждают, что они могут составлять уравнения для подсчета простых чисел с гораздо меньшим числом кубитов, чем того требует Шор. А если еще и индивидуальные кубиты становятся более стабильными, или требуется гораздо меньше кубитов для исправления ошибок, чем дают их оценки более высокого уровня, то это дает результат в обратном направлении. Я не разделяю никакую из этих точек зрения и, чтобы не сбивать вас с толку, хочу только добавить, что увеличение количества битов симметричного ключа не так просто, как увеличение симметричного ключа и размера хеша. Но вообще, если вы хотите уменьшить риск вашей традиционной квантововосприимчивой асимметричной криптографии, то, пока вы не можете смягчить последствия за счет квантовоустойчивой криптографии, будет небесполезно увеличить размер ключей, если это не вызывает больших затруднений.

Криптогибкость

Криптогибкость (crypto-agility) – это способность устройства, программного обеспечения или системы применять криптографию с другим шифрованием, схемой или размером ключей без чрезмерных затруднений. В конечном итоге все рабочие системы должны быть спроектированы так, чтобы вы могли, насколько возможно, переключать задействованную криптографию с минимальными усилиями. К сожалению, это то, что должен предусмотреть именно разработчик данных систем. Это трудно осуществить клиентам и конечным пользователям без усилий разработчика и в первую очередь без его усилий при создании необходимой для этого базовой структуры.

Некоторые известные разработчики уже сделали это. Например, Microsoft Windows в большинстве своих продуктов отделяет криптографию от программных и аппаратных систем, которые используют ее. Microsoft делает это, рекомендуя, чтобы криптографические шифры и схемы были представлены в цифровых модулях отдельных поставщиков хранилищ ключей (key storage provider, KSP) (их раньше, в более ранних версиях Windows, называ-

ли криптографическими поставщиками услуг (cryptographic service providers, CSP)), и их можно было устанавливать и удалять из приложений, которые их используют, порознь.

Windows поставляется со многими встроенными KSP, которые содержат все популярные стандарты шифрования и схем. Третьи лица и клиенты могут создавать свои собственные схемы шифрования и заменять один KSP на другой или просто установить новый (который обычно довольно маленький и быстрый при установке), выбрав его из выпадающего меню KSP. Флагманский продукт Центра сертификации Microsoft (Active Directory Certificate Services) позволяет устанавливать разные KSP для поддержки разных типов криптографии.

В мире Linux с открытым исходным кодом многие из самых популярных приложений и утилит, таких как OpenSSL и SSH, позволяют взаимно заменять различные типы криптографии. Часть команды разработчиков квантовоустойчивой схемы подписи Picnic использовали Picnic, LWE-FRODO и SIDH с OpenSSL и Apache Web Server для создания устойчивых соединений TLS 1.2 HTTPS (см. раздел 8.2 документа разработки Picnic: https://github.com/Microsoft/Picnic/blob/master/spec/design-v1.0.pdf). OpenSSL и Apache не требуют значительных изменений, хотя для OpenSSL нужны незначительные изменения, позволяющие TLS применять ключи больших размеров, генерируемых Picnic.

Сравните эту простую универсальность (то есть криптогибкость) с жестко закодированной криптографией большинства приложений, которые не могут быть заменены без обновления шифровального кода в программе, перекомпиляции и переустановки всей программы.

Старайтесь, чтобы все ваши поставщики (и ваше собственное разработанное программное обеспечение) были криптогибкими. Тогда при очередном необходимом смягчении последствий развития криптографии переход будет проще. Начните этот этап вашего проекта квантовой криптомиграции сейчас. Сделайте так, чтобы каждый в ИТ-команде знал, что такое криптогибкость, понимал, как она работает, и требовал ее наличия.

Этап 2. Переход к квантовоустойчивым решениям

Как уже говорилось ранее, большинство организаций не могут перейти к новой квантовоустойчивой криптографии до тех пор, пока их национальный орган по стандартизации (такой как Национальный институт стандартов и технологий (NIST) или Агентство Европейского союза по сетям и информационной безопасности) не объявляет постквантовые криптографические стандарты. Но многим организациям, особенно тем, которые являются разработчиками собственных внутренних приложений, использующих криптографию, имеет смысл начать эксперименты. Доступно много библиотек квантового кодирования, API, симуляторов и наборов для разработки программного обеспечения (SDK), которые могут помочь переходу организации на квантовоустойчивую криптографию. Во многих организациях есть программное обеспечение, инструменты, ресурсы и знающие специалисты, которые помогут вам перейти к квантовоустойчивой криптографии. Такие

команды могут предоставить все, что нужно вашей организации, чтобы начать квантовую криптографическую «миграцию», включая опытных квантовых разработчиков и испытателей. Посмотрите эти страницы:

- открытый проект Quantum Safe (https://openquantumsafe.org/);
- проекты с открытым исходным кодом Quantum Software на GitHub (https://github.com/qosf/os_quantum_software);
- открытые исходные и коммерческие проекты квантового программного обеспечения и квантовые онлайн-порталы (https://github.com/qosf/os_quantum_software).

И конечно же, у таких поставщиков квантового оборудования, как Microsoft, IBM и Cambridge Quantum Computing, есть много ресурсов и инструментов. Работайте с вашими сегодняшними поставщиками. Даже если все, что вы сделаете, – осуществите один небольшой демонстрационный проект, это окажет вам помощь в конкурентной среде. Если квантовый криптопрорыв произойдет раньше, чем вы планировали, время, усилия и ресурсы, вложенные в любые тестовые проекты, будут на вес золота. Тестовые проекты становятся тем автобусом, который (как и люди в этом автобусе) движется в правильном направлении.

Когда национальные государственные органы утвердят официальные стандарты квантовой устойчивости, вы должны как можно скорее начать двигаться к квантовоустойчивой криптографии. Любой выбранный стандарт, вероятно, будет хорошей комбинацией производительности и удобства использования и будет предусматривать те же оперативные и предупредительные меры, как обновление размеров ключа вашей традиционной криптографии (включая производительность и вопросы эксплуатации). Обычно к тому времени, когда стандарт будет утвержден, много реальных ресурсов и библиотек программного обеспечения будут готовы помочь разработчикам и потребителям. Как только стандарты будут объявлены, все государства (или даже мир в целом) начнут двигаться в том же самом направлении. Убедитесь, что вы будете частью этого движения. Вам не нужно быть на переднем крае, но даже если вы где-то поблизости – это отличное место.

Эта стадия вашего миграционного проекта, вероятно, продлится не менее двух лет с момента выбора квантовоустойчивых стандартов. NIST утверждает, что национальный стандарт США будет выбран где-то между 2022 и 2024 годом, что означает, что этот этап большинства проектов в США, вероятно, займет 3–7 лет до завершения. Конечно, эта стадия проекта может быть приближена, если кто-то вдруг объявит квантовый криптопрорыв раньше сегодняшних ожиданий.

Примечание С завершением этапа 2 переход к квантовоустойчивым решениям приведет к значительному снижению риска, по крайней мере до тех пор, пока не произойдет очередной технологический прорыв, который уменьшит обеспеченную устойчивость квантовоустойчивой криптографии. Следующие два этапа будут продолжать снижать риск, но сокращение, скорее всего, не будет таким резким. Завершение этапа 2, вероятно, станет кульминацией проекта.

Защита PKI

PKI (public-key infrastructure, архитектура открытых ключей) обеспечивает бóльшую часть интернета и бизнеса. Предстоящий квантовый криптопрорыв взломает все существующие PKI, потому что они работают на квантововосприимчивой криптографии (Rivest–Shamir–Adleman, Diffie–Hellman, Digital Signature Algorithm, Elliptic Curve Digital Signature Algorithm и т. д.). Как уже говорилось ранее, Microsoft и другие исследователи смогли показать, что, по крайней мере, некоторые из существующих PKI, цифровые подписи и аппаратные модули безопасности (hardware security modules, HSM) могут работать как квантовоустойчивые шифры. С небольшой настройкой эти цифровые сертификаты могут быть использованы в интернете с TLS. Есть много других программ и поставщиков PKI, но когда наступит время перехода на квантовоустойчивые шифры, большинство, вероятно, сделает это.

Любой из кандидатов схем цифровой подписи, представленных на втором туре конкурса NIST и описанных в главе 6 (CRYSTALS-Dilithium, FALCON, GeMSS, LUOV, MQDSS, Picnic, qTESLA, Rainbow и SPHINCS+), серьезно рассматривает вопрос о замене постквантовой цифровой подписи PKI. Вы найдете хорошую белую книгу криптогибкости PKI здесь: www.isara.com/wp-content/uploads/2018/05/ISARA_Corp_PKI_Migration_WhitePaper_FINAL.pdf.

Варианты Leighton–Micali Signatures (LMS) и eXtended Merkle Signature Scheme (XMSS) также обсуждаются, но поскольку они являются государственными, то не вошли в число официальных кандидатов NIST. Они предположительно рассматриваются NIST в качестве субпроектов. Вариант со многими деревьями XMSS известен как XMSS-MT или XMSS-MTS (Merkle Tree Signature), а вариант со многими деревьями LMS известен как HSS. Оба были представлены в качестве предложений для комментариев (requests for comments, RFC), что является последним шагом в процессе утверждения инженерной рабочей группой по интернету (the Internet Engineering Task Force, IETF). В случае заинтересованности вы можете прочитать больше о XMSS и LMS на https://eprint.iacr.org/2017/349.pdf. Узнать последние новости о XMSS и LMS можно на https://www.isara.com/standards/, а хороший официальный документ по XMSS вы можете найти здесь: https://tools.ietf.org/html/draft-irtf-cfrg-xmss-hash-basedsignatures-11.

Обратите самое пристальное внимание на постквантовую PKI в объявлениях форума CA/Browser Forum (https://cabforum.org/) и, в частности, на их стандарты PKI, известные как базовые требования (https://cabforum.org/baseline-requirements/). Эта группа состоит из нескольких крупных PKI-поставщиков и исполнителей. Их требования обычно выполняются всеми «публичными» поставщиками CA и косвенно большинством частных компаний. С помощью общедоступных центров сертификации эта организация следит за использованием публичными компаниями CA криптографии, а также за большинством факторов, связанных с операциями PKI и лучшей практикой их применения. Группа успешно вынудила большинство CA перейти с SHA1 на SHA2. Этот шаг привлек внимание и других компаний, и они провели криптографический переход этим вдумчивым и успешным способом.

В марте 2019 года в CA/Browser Forum прошли слушания, на которых обсуждались грядущие квантовые изменения (https://cabforum.org/2019/05/03/minutes-for-ca-browser-forum-f2f-meeting-46-cupertino-12-14-march-2019/#Quantum-Cryptography-problem-need-solutions-and-timeframe---assign-ForumSCWG-liaisons). Если у вас есть PKI, следуйте обновлениям и требованиям CA/Browser Forum.

Для получения дополнительной информации о цифровых сертификатах PKI и X.509 в постквантовом мире ознакомьтесь с https://eprint.iacr.org/2018/063.pdf и https://eprint.iacr.org/2017/349.pdf.

Получите другие квантовые устройства и услуги

Сейчас настало время поразмышлять о возможности получения квантовых (сертифицируемых) генераторов случайных чисел (RNG) и устройств распределения квантовых ключей (как описано в главе 7). Оба этих устройства относительно недороги, используются в течение почти двух десятилетий и могут применяться для улучшения вашей криптографии за счет какой-либо другой квантовой криптографии или без нее, а также с помощью задействованных устройств.

Примечание Генераторы случайных чисел на основе квантовых чисел существуют уже долгое время, но сертифицированные RNG начали появляться только в 2019 году. Первая коммерческая версия доступна на сайте https://cambridgequantum.com/cqc-unveils-the-worlds-first-commercially-ready-certifiablequantum-cryptographic-device/.

Сейчас в целях информационно-технологической безопасности также предстоит решить, когда нужно получить эти типы систем, чтобы к моменту, когда наступит время реализации квантовоустойчивой криптографии, они у вас были. Если у вас нет необходимости в каком-либо типе системы или вы просто не хотите ее иметь, имеет смысл хотя бы обеспечить себе доступ к ней. Подумайте о возможности покупки квантовых компьютеров или квантовых услуг, когда это станет доступным. Не останьтесь в чисто бинарном мире, когда мир начнет становиться квантовым.

Этап 3. Применение квантово-гибридных решений

Большинство ранних квантовых сетей и систем будут использовать комбинацию квантовых и классических бинарных вычислительных устройств. Например, квантовые устройства распределения ключей (QKD) обычно передают квантовые ключи по классическому двоичному сетевому каналу. Большинство квантовых генераторов RNG создают чисто случайные числа, которые затем используются в классических двоичных системах. Доверенные повторители, которые надежно разделяют квантовые ключи шифрования, делают это в классических сетях. Все существующие квантовоустойчивые шифры работают в двоичном мире и используют классические двоичные файлы хешей. Многие из ранних квантовозадействованных систем и устройств, которые вы будете использовать, будут обладать смесью квантовых и классических черт.

Этого следует ожидать, особенно перед тем, как мы в долгосрочной перспективе перейдем на полностью квантовые сети и устройства.

Один из важных моментов – выяснить, когда имеет смысл с точки зрения безопасности и бюджета перейти от классической бинарной модели к квантово-гибридной. Переход к квантово-гибридной модели, когда это доступно, не всегда экономически эффективное решение. Основная причина перехода на квантовые решения состоит в том, чтобы получить встроенную защиту от квантовой механики. Когда это сочетается с классическим подходом, как это происходит в гибридных моделях, максимальная защита ограничивается самой простой технологией взлома (т. е. классической). Классический подход может существенно снизить безопасность перехода к квантово-гибридной модели и, как правило, со значительно бóльшими затратами.

Некоторое время чисто классическое решение будет обеспечивать необходимую безопасность. Каждая команда, осуществляющая проект, должна решить, когда надо осуществить переход и на какой тип технологии. Ожидается, что переход к квантово-гибридным системам займет больше времени, чем переход к полностью квантовоустойчивой криптографии, и, возможно, продлится до 10 лет с момента запуска вашего проекта.

Этап 4. Применение полностью квантовых решений

Конечная цель, которой предстоит достичь через много лет, состоит в том, чтобы полностью перейти на квантовую криптографию и сетевые устройства. Возможно, требования безопасности вашей организации вынудят как можно скорее перейти на полностью квантовые системы. Квантовая механика по своей сути создает для квантовой криптографии все условия, чтобы она была более безопасной. Квантовоустойчивая криптография устранит большую часть риска от квантовых криптографических атак, но полностью квантовая криптография и устройства являются самой надежной защитой.

Например, начните сегодня с ваших сетевых устройств и убедитесь, что все ваши сетевые устройства используют квантовоустойчивые размеры ключей существующей традиционной криптографии. Когда национальные стандарты будут утверждены, замените их размеры на соответствующие квантовоустойчивой криптографии. Затем перейдите к классическим/квантовым решениям, таким как доверенные повторители, а потом и полностью на квантовые решения, такие как квантовые повторители. И сделайте это для всех ваших систем защиты данных. Этап 4 может длиться до 20 лет с начала вашего постквантового «проекта миграции».

Эти четыре этапа не обязательно должны следовать друг за другом. В разное время может существовать несколько параллельных путей с участием разных систем. Например, вы можете остаться на этапе 1, с более широкими реализациями существующих криптографических стандартов для многих систем в обозримом будущем, в то же время изучая другие этапы для других систем. Вы можете решить купить квантовый RNG для некоторых проектов и использовать его в гибридном решении. Вы все еще можете быть связаны с переводом многих проектов на квантовоустойчивую криптографию, когда какой-то поставщик предложит полностью квантовое решение по разумной

цене. За исключением этапа 1, остальные, скорее всего, будут в одних случаях следовать в заданном порядке, а в других – параллельно, в зависимости от сценария. Будьте к этому готовы.

Шесть основных шагов проекта смягчения последствий постквантового прорыва

С приходом квантового криптографического взлома каждая организация, которая хочет защитить свои цифровые секреты, должна иметь план действий. В этом разделе книги как раз и предлагается такой план. Основные общие этапы проекта таковы:

1) обучение;
2) создание плана;
3) сбор данных;
4) анализ;
5) действия/исправления;
6) обзор и улучшение при необходимости.

На рис. 9.2 представлены общие этапы жизненного цикла проекта постквантового перехода.

Рис. 9.2. Этапы жизненного цикла проекта постквантового перехода

Примечание Представленный в этой главе план был проверен и использовался много раз, хотя и в отношении криптографического перехода другого типа. Я помог многим десяткам, если не сотне с лишним, компаний перейти от SHA1 к SHA2 в период с 2014 по 2017 год. Хотя цели были разные, план и этапы очень похожи.

В завершение главы мы в подробностях обсудим каждый этап плана.

Шаг 1. Обучение

Поскольку вы читаете эту книгу, то уже сделали первый шаг к составлению плана. Вы должны учиться сами и информировать вашу команду, руководство и всех конечных пользователей о том, что сулит предстоящий прорыв квантовой криптографии, а также о том, что ваша организация планирует делать в связи с этим. В особенности необходимо обучить разработчиков и заинтересованные стороны, участвующие в принятии решений по изготовлению и покупке программного и аппаратного обеспечения.

Используйте эту книгу и все дополнительные ссылки и рекомендации, чтобы продолжить обучение в области квантовых вычислений. Ключевая задача для вас – быть в курсе последних изменений и достижений квантовых вычислений и того, как они повлияют на ваш план подготовки к квантовым вычислениям. Просто обращайте больше внимания на общие новостные статьи, в которых упоминается слово «квант». Это поможет вам. Подписка на конкретные почтовые рассылки и блоги по квантовым вычислениям – также хороший способ оставаться в курсе событий.

Списки рассылки и блоги по теме квантовых вычислений

Ниже приводится ряд рассылок и блогов по теме квантовых вычислений. Вы можете посетить эти ресурсы и подписаться на них:

- https://quantiki.org;
- www.scottaaronson.com/blog/;
- www.quantiki.org/wiki/mailing-lists;
- https://golem.ph.utexas.edu/category/2010/12/quantum_foundations_mailing_li.html;
- https://accounts.eclipse.org/mailing-list/quantum-computing-wg;
- https://hepsoftwarefoundation.org/workinggroups/quantumcomputing.html;
- https://dabacon.org/pontiff/;
- https://quantumcomputingreport.com/news/;
- https://quantumcomputing.stackexchange.com (отлично подходит для проработки технических вопросов);
- https://geekforge.io;
- не повредит следить и за моими статьями (www.csoonline.com/author/Roger-A.-Grimes/), Твиттером (@rogeragrimes) или LinkedIn (www.linkedin.com/in/rogeragrimes/), хотя я освещаю широкий круг тем компьютерной безопасности, а не только квантовые.

В приложении, которое вы найдете в конце книги, представлено еще больше полезных ссылок. Я прошу прощения, если пропустил ваш любимый список рассылки, блог или сайт по данной теме.

Попытайтесь понять квантовую механику и квантовые вычисления как можно лучше. Будучи защитником подготовки к предстоящему квантовому

криптопрорыву, вы должны хорошо представлять себе, что такое квант. Надеюсь, эта книга дала вам хорошее общее представление обо всех проблемах, связанных с квантами и квантовыми вычислениями, но если вы захотите познакомиться с дополнительными источниками, это только приветствуется. Автор данной книги более двух десятилетий накапливал опыт и изучал сотни самых разных трудов и статей по квантовой механике и компьютерам, чтобы дойти до нынешнего понимания предмета. Вот список онлайн-курсов по квантовой теории и квантовым вычислениям: https://Quantcomputingreport.com/resources/education/ – и другой похожий сайт: https://hackernoon.com/16-best-resources-to-learn-quantum-computing-in-2019-e5d8b797aeb6.

Презентация слайдов

Все ИТ-специалисты должны быть знакомы с основными технологическими подходами и проблемами. Вовлекайте всех конечных пользователей, если предстоящие перемены (например, обновление программного обеспечения и изменение стандарта защиты данных) будут влиять на их жизнь.

Хороший способ познакомить других с квантовой механикой, вычислениями и грядущим криптографическим прорывом – показ электронной презентации. Я с успехом давал подобную часовую презентацию в течение многих лет и призываю читателей загрузить и использовать мои слайды. На рис. 9.3 показан пример слайда. Электронная презентация охватывает квантовую механику, квантовые компьютеры, криптографию, квантовое превосходство, квантовый прорыв и показывает, как к ним подготовиться. Чтобы ваши слушатели извлекли максимум пользы из сказанного вами, им понадобятся хотя бы базовые знания из области криптографии.

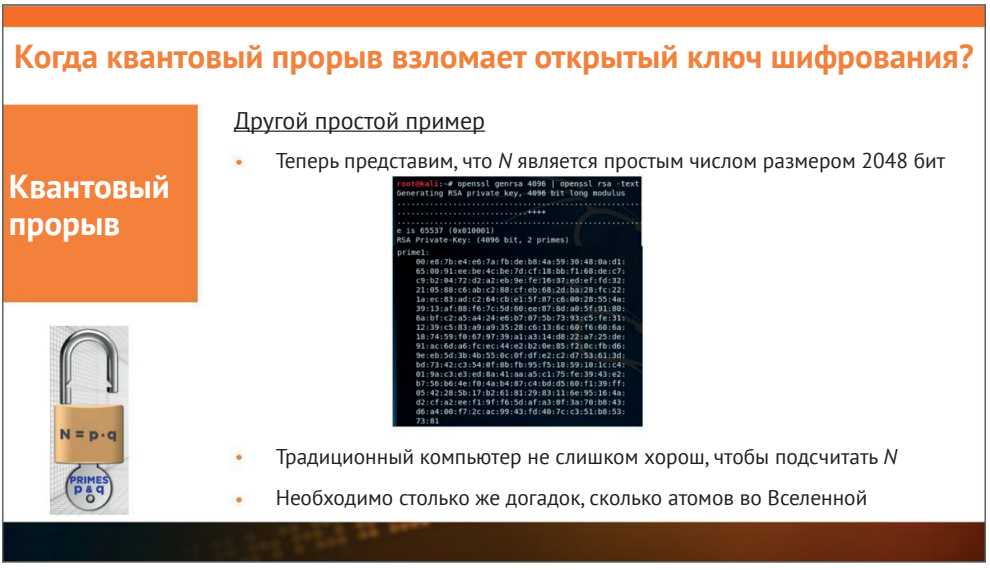


Рис. 9.3. Пример слайда презентации

Общая презентация в форматах Microsoft PowerPoint и Adobe PDF доступна по адресу www.wiley.com/go/cryptographyapocalypse. Вы вправе менять ее по своему усмотрению, учитывая специфику вашей аудитории.

Краткая справка для менеджмента

Старшее руководство всегда занято. Вполне вероятно, что ваши начальники совсем не слышали или слышали крайне мало о грядущих квантовых криптографических вызовах. Вы должны информировать свое руководство о проблеме и ее важности. Возможно, имеет смысл создать одно-двухстраничный краткий документ, который вы можете передать начальству вместе с небольшой (5–10 слайдов) презентацией, охватывающей основы. Одно-двухстраничный документ обычно представляет собой краткое введение, за которым следуют некоторые часто задаваемые вопросы (FAQ) и ответы на них. Вы можете скачать пример на www.wiley.com/go/cryptographyapocalypse и/или воспользоваться нижеследующим шаблоном:

Кому: По месту требования

От: <ваше имя>

Дата: <дата>

Тема: Подготовка к грядущему квантовому криптографическому прорыву

Настоящий документ ставит целью помочь менеджменту ознакомиться с новым, развивающимся проектом под названием «Квантовая защита данных» и поделиться общими деталями и графиком этого проекта.

Компьютеры, основанные на квантовой механике, получают такое развитие, что начинают серьезно угрожать большей части существующей сегодня традиционной криптографии, включая HTTPS, Wi-Fi, проверку подлинности при входе в систему, смарт-карты, многофакторную проверку подлинности и инфраструктуры открытых ключей (PKI). Никто не может предсказать, когда квантовые компьютеры усовершенствуются настолько, что станут реальной угрозой для большинства организаций; по оценкам экспертов, это произойдет в ближайшие годы (менее чем через десятилетие). В 2016 году Национальный институт стандартов и технологий (NIST) и Агентство национальной безопасности (NSA) рекомендовали всем организациям начать подготовку к грядущему криптографическому взлому. Мы на [X] лет опоздали с началом нашей подготовки.

В рамках выполнения этих рекомендаций и в связи с постоянно растущей скоростью квантовых вычислений мы подготовим нашу организацию для решения этих проблем, создав специальную команду. Мы проведем оценку защиты данных (чтобы определить, какие из наших критически важных цифровых активов нуждаются в долгосрочной защите от несанкционированного доступа) и создадим план, обеспечивающий к критической дате их защиту посредством соответствующей квантовоустойчивой криптографии, а также проведем другие мероприятия для смягчения нежелательных последствий. Первый важный этап проекта и работа нашей недавно сформированной проектной команды начнется в ближайшие несколько недель и, как ожида-

ется, продлится несколько лет, пока угроза не будет полностью устранена. Наша цель – до того, как произойдет прорыв квантовой криптографии, обновить квантововосприимчивую криптографию до квантовоустойчивой. Это может повлиять на многие из наших существующих реализаций защиты данных, и причиной запуска данного проекта сейчас является необходимость минимизировать будущие сбои в работе и затраты. Стоимость проекта, ресурсы и сроки трудно рассчитать адекватно до проведения анализа и оценки защиты, которые, как ожидается, будут выполнены в течение следующих 12–24 месяцев. Мы будем следовать руководящим принципам и методологии, принятым в отрасли, и использовать их везде, где это возможно. Буду рад ответить на любые ваши вопросы и/или предоставить вам более подробную информацию и обучение.

С уважением,

<Ваше имя и должность>

Страница 2. Часто задаваемые вопросы (FAQ)

Что такое квантовая механика?

Квантовая механика/физика – давно подтвердившие свою состоятельность разделы физики, которые описывают свойства и поведение микрочастиц. Все во Вселенной подчиняется принципам квантовой механики и зависит от нее. Так устроен мир. Создаются компьютеры и программное обеспечение, которые используют свойства квантовых частиц. В течение ближайших нескольких лет, если не раньше, мы будем иметь квантовые компьютеры, способные делать то, что не могут сделать компьютеры, не являющиеся квантовыми, в связи с чем многие формы традиционной криптографии окажутся ненадежными и будут созданы новые, устойчивые формы криптографии.

Как долго существуют квантовые компьютеры?

Первый работающий квантовый компьютер был создан в 1998 году. Сегодня существует более сотни квантовых компьютеров и десятки различных типов квантовых устройств. Известно, что квантовые компьютеры все еще относительно малоэффективны, находятся в лабораторной и экспериментальной стадии развития, но ожидается, что к концу 2019 года или вскоре после этого они превзойдут возможности традиционных компьютеров. Правительства и корпорации мира тратят десятки миллиардов долларов в год, чтобы построить квантовые суперкомпьютеры и сети. В число поставщиков квантовых компьютеров входят крупнейшие в мире компании, такие как Google, IBM, Intel, Microsoft и Alibaba.

Как квантовые вычисления могут угрожать традиционной криптографии?

Отдельные типы квантовых компьютеров, вооруженные математическим алгоритмом, известным как алгоритм Шора, могут быстро решать математические уравнения с большими простыми числами. Уравнения с большими простыми числами – это то, что дает традиционной криптографии с открытым ключом защитные возможности. Традиционные двоичные компьютеры не могут легко делать такие вычисления. Квантовые компьютеры

с достаточным количеством кубитов способны решать уравнения с большим числом простых чисел за очень короткий промежуток времени, от нескольких минут до нескольких часов.

Когда квантовые компьютеры сломают традиционные криптокоды с открытым ключом?

Никто не знает наверняка, хотя считается, что как только квантовые компьютеры получат четыре тысячи или около того «стабильных» кубитов, традиционные открытые ключи длиной 2048 бит или меньше будут легко и быстро взломаны. Большая часть существующей в мире публичной криптографии полагается именно на такие ключи. Квантовые компьютеры способны наполовину снизить защитную силу других типов криптографии. По общим оценкам, до момента, когда квантовые компьютеры смогут взломать традиционную публичную криптографию, осталось несколько лет (не более десяти). В любом случае, большинство экспертов утверждают, что начинать подготовку надо уже сейчас. Если прорыв случится раньше, чем ожидается, то у нас будет больше шансов соответствующим образом ответить на этот вызов.

Что мы делаем?

Мы формируем новую проектную команду, которая называется «Группа квантовой защиты данных», чтобы определить те места, где наша критическая защита данных может быть затронута и риск необходимо уменьшить. Ближайшие меры по снижению риска, вероятно, будут включать увеличение существующих размеров криптографических ключей, выделение критических данных и переход к квантовоустойчивой криптографии. Долгосрочные меры по смягчению последствий криптографического квантового прорыва на многие годы включают в себя переход на квантовые шифры и устройства.

Как вы можете помочь

Нам необходимы одобрение и поддержка этого проекта со стороны одного или нескольких представителей высшего руководства. Эти заинтересованные лица должны присутствовать на первом заседании по обсуждению проекта, а возможно и на дальнейших обсуждениях, чтобы иметь возможность отвечать на вопросы других старших менеджеров.

Вы вправе использовать этот документ в качестве образца и при необходимости менять его по своему усмотрению. Онлайн-версия данного документа (www.wiley.com/go/cryptographyapocalypse) может обновляться и исправляться в дальнейшем.

Шаг 2. Создание плана

Создание плана проекта включает в себя множество подкомпонентов, в том числе создание команды проекта, плана и графика проекта.

Создание команды проекта

Для смягчения последствий угрозы со стороны квантовых компьютеров, вероятно, потребуются многие годы. Если можно выделить ИТ-проект, для

которого особенно важно создание команды, это именно данный. Если у вас нет управленческих навыков для создания солидного проекта, пригласите в свою команду хорошего менеджера проекта или получите необходимые навыки сами. В команду должны входить:

- спонсор из старшего руководства;
- руководитель проекта, знакомый с квантовыми вычислениями и другими смежными темами (вероятно, это будете вы);
- менеджер по информационной безопасности;
- другие ИТ-сотрудники по мере необходимости;
- эксперт по криптографии;
- представитель конечного пользователя;
- специалист по связи;
- бухгалтер / представитель финансовой службы / поставщик;
- менеджер / специалист по инвентаризации.

В небольших компаниях многие из этих ролей может взять на себя один человек. В очень маленькой компании даже допускается исполнитель, который «един во всех лицах».

Хотя это не требуется на ранних этапах, на более поздних этапах работа с поставщиками уязвимых систем будет решающей. Они должны быть в курсе ваших проблем и иметь возможность поддерживать с вами обратную связь, чтобы вы знали, что делает их компания для решения ваших проблем с квантовым прорывом. В идеале вы должны хотеть, чтобы они помогали вам с решениями перехода на другие технологии. Возможно, вам потребуется привлечь поставщика на этапе или сразу после этапа сбора данных проекта.

Специалист по коммуникациям играет важную роль. Если все идет по плану и все меры принимаются до того, как произойдет квантовый криптографический взлом, специалист по коммуникациям сможет помочь вам донести эту информацию о проекте до поставщика. Если же квантовый криптографический взлом произойдет до того, как все возможные последствия будут смягчены, должен быть принят экстренный ускоренный план и график. Критически затронутые активы, возможно, понадобится отключить. Вероятно, даже следует временно приостановить бизнес. Вам понадобится план реагирования на инциденты. Пусть менеджмент и специалист по коммуникациям знают, что хотя вероятность сценария работы по ускоренному графику невелика, в случае необходимости вы должны быть готовыми к этому.

Также было бы целесообразно инициировать дискуссии с другими торговыми организациями в вашей отрасли и даже конкурентами. Каждая организация будет заниматься проектом квантовой устойчивости какого-либо типа, хотя и с разными сроками и целями. Тем не менее подобные цели (переход на квантовоустойчивую криптографию) будут преследовать все, и кто-то может поделиться с вами, что было сделано в этом процессе, а от чего отказались. Звоните по телефону, проводите встречи и поднимайте тему на отраслевых встречах и конференциях. Это проект самых больших масштабов. И в данной ситуации все мы в одной лодке. Мы нужны друг другу. Это не вопрос создания конкурентного преимущества, а вопрос выживания.

Создание плана проекта

Каждый руководитель проекта должен создать подробный план проекта, вероятно, с использованием какого-либо программного обеспечения, такого как Microsoft Project (https://products.office.com/en-us/project/project-and-portfoliomanagement-software) или любой другой конкурирующий продукт (предложения смотрите на сайте www.pcmag.com/roundup/260751/the-best-project-management-software). Очень важно выяснить и задокументировать ключевые задачи и критические пути. Чем больше деталей и приблизительных сроков, тем лучше. В целом любой план управления проектом должен охватывать четыре основных этапа постквантового перехода, перечисленных ранее, и шесть шагов проекта, описанных в этом разделе.

Создание графика

Конечная цель – заменить всю квантововосприимчивую криптографию и системы, защищающие критически важные данные для квантовоустойчивой криптографии, прежде чем квантовый прорыв явит реальную угрозу вашей организации. Не все организации и отрасли будут сразу же атакованы при квантовом криптопрорыве. На раннем этапе большинство целевых атак, вероятно, будут проводиться национальными государствами, и под ударом в первую очередь окажутся военные и правительственные объекты, а затем – очень крупные организации. Любые организации в цепочке поставок этих объектов также будут одними из первых мишеней. Но как только прорыв произойдет, уже нельзя будет предугадать, когда квантовые компьютерные ресурсы будут использованы против вашей организации.

Чтобы подготовиться, вам нужно примерно оценить, сколько времени пройдет до квантового криптографического взлома (для этого обратитесь к материалу главы 4 «Когда случится криптопрорыв?»), и разработать график, в котором будет расписано, сколько времени понадобится вашей организации для защиты всех важных конфиденциальных данных методами квантовоустойчивой криптографии.

Пусть неравенство Моски будет вашим руководством Ориентируйтесь на неравенство Моски при составлении графика работ. В главе 4 говорится, что если мы хотим сохранить наши данные в безопасности, надо обеспокоиться квантовыми атаками заблаговременно. Точнее говоря, время, которое потребуется вашим компьютерным системам для перехода от классического к постквантовому состоянию для обеспечения безопасности данных, должно опережать то время, которое понадобится квантовым компьютерам, чтобы начать разрушать существующие протоколы шифрования (см. рис. 9.4). Когда этот момент наступит, у вас уже не будет возможности адекватно защитить ваши данные, прежде чем квантовые компьютеры сломают текущую квантововосприимчивую защиту. Например, если вы хотите, чтобы ваши критически важные данные были в безопасности в течение 10 будущих лет, и на переход к новой технологии уйдет 5 лет, вам нужно начать переходить на постквантовые системы за 15 лет до постквантового прорыва.

Рис. 9.4. Неравенство Моски

Ваши расчеты и оценки существенно осложняет тот факт, что никто не знает точно, когда этот прорыв случится. Большинство экспертов считают, что до него осталось менее 10 лет, и отдельные специалисты, в числе которых автор этой книги, полагают, что это может произойти уже через 2–3 года. Относительно безопасным можно было бы считать срок до 5 лет. Большинство людей хотят защитить свои наиболее важные конфиденциальные данные от прослушивания в течение 5–10 лет, поэтому возьмите 7 лет в качестве безопасного среднего значения. Теорема Моски о неравенстве гласит, что вы должны начать работать над постквантовым переходом за 12 лет до квантового криптографического взлома, если хотите обеспечить надежную защиту своих данных в течение 7 лет, включая 5 лет миграции. По сути, если вы еще не начали подготовку и не отвели достаточно времени на реализацию, есть основания полагать, что вы уже опаздываете с началом проекта квантовой защиты.

Не спешите выбирать нестандартную постквантовую криптографию У большинства организаций на пути к квантовоустойчивой криптографии появится необходимость принять соответствующие национальные официальные стандарты постквантовой криптографии. Немногие организации выиграют от того, что, не дожидаясь появления официального национального стандарта, внедрят нестандартную криптографию в своей производственной среде. Организация вправе выбрать нестандартный шифр или схему для работы, но это обычно требует серьезного обоснования. Нестандартные шифры и схемы обычно менее проверены и заслуживают меньше доверия, даже если они кажутся или на самом деле сильнее и безопаснее. Выбор криптографии, отвечающей стандарту, безопаснее, а потому есть смысл подождать, когда этот стандарт будет определен.

Примечание Поначалу в течение нескольких лет считалось, что применение криптографии с изогенной эллиптической кривой означает высокую квантовую устойчивость. Однако через некоторое время кто-то нашел способ быстро подвергнуть факторизации вовлеченные изогенные кривые. «Доработка», использующая только сверхсингулярные эллиптические кривые, победила этот конкретный тип атаки, и теперь криптография изогенной эллиптической кривой известна как криптография с изогенной сверхсингулярной эллиптической кривой. Но кто-то может придумать новую атаку, которая разлагает даже сверхсингулярные изогенные эллиптические кри-

вые. Бóльшая часть квантовоустойчивой криптографии очень нова. Шифры и схемы все еще подвергаются атакам и проверке. Если вы примете решение слишком рано, то увеличите риск выбора неработающего криптографического решения и необходимость переделок.

В Соединенных Штатах и в большинстве стран мира это означает необходимость ждать объявления постквантовых криптографических стандартов NIST, которые, как утверждается, появятся между 2022 и 2024 годом. NIST также заявил, что стандарт может быть объявлен раньше, если новая информация потребует ускорения выбора. Это означает, что большинству организаций для начала масштабного перехода к квантовоустойчивой криптографии придется подождать до 2022–2024 года. И весь процесс, скорее всего, займет один-два года (в лучшем случае) после того, как постквантовые криптографические стандарты будут выбраны, когда все участвующие поставщики начнут предлагать свое аппаратное и программное обеспечение. Это будет естественной отсрочкой в период между выбором криптографических стандартов и их широким распространением.

Вы можете, и должны, начать экспериментировать, тестировать и развивать любой метод, который претендует на то, чтобы стать постквантовым криптографическим стандартом. Это принесет пользу вашей организации, когда наступит время полного развертывания производства. Но хотелось бы предостеречь любую нормальную организацию от развертывания на полную мощность производства с какой бы то ни было нестандартной постквантовой криптографией до появления официального стандарта. В то же время ничего не делать, прежде чем не появится стандарт, тоже не оптимальный вариант. Каждая компания должна начать исследование, планирование и защиту критически важных данных сейчас, а некоторым организациям следует уже приступить к разработке тестов, чтобы подготовиться надлежащим образом.

Создание сценария с ускоренной временной шкалой Важно, чтобы вы создали резервное копирование и составили экстренный план действий на случай, если квантовый прорыв нагрянет внезапно, до того, как вы полностью переместите активы своей организации в квантовоустойчивую криптографию. Представьте, что завтра вы просыпаетесь, и Агентство национальной безопасности объявляет, что некое государство получило возможность взломать традиционную криптографию с открытым ключом, и более того, ряд атак уже проведен. Вместо того чтобы годами переходить на квантовоустойчивую криптографию, вам нужно сделать это прямо сейчас! Как это меняет ваши планы? Что вы оставите на потом? Что сейчас, а что нет? Можете ли вы получить больше ресурсов для ускорения работы по проекту? Должны ли вы предупредить клиентов и совет директоров о новой неизбежной угрозе? Кто будет финансировать проект? Создайте заблаговременно два графика: один на случай, если все будет развиваться предсказуемо, и другой – экстренный. Для каждого варианта разработайте отдельный план.

Создайте оценки сроков фаз проекта Сколько времени вам потребуется, чтобы завершить проект перехода к квантовой защите? Оцените, сколько времени понадобится вашей организации, чтобы переместить все задействован-

ные системы защиты данных для постквантовых реализаций после запуска проекта квантовой устойчивости, чтобы старшее руководство и участники проекта могли видеть вероятные ожидания. Ответ уникален для каждой организации и зависит от того, что вы должны переместить, как и когда вы способны это сделать. У каждой организации будет свой план, но руководители проектов должны начать с некоторых основных предположений по каждому этапу проекта. Для примера обратитесь к табл. 9.1.

Таблица 9.1. Примерный перечень задач в плане квантовоустойчивого проекта и расписание работ

Этапы проекта	Оценка времени завершения
Обучение	1 месяц
Формирование команды проекта и планирование	1 месяц
Создание графика	1 месяц
Создание списка защищаемых данных	3 месяца
Анализ плана квантизации и разработка рекомендаций	6 месяцев
Предупреждение утечки данных в будущем	3 месяца
Усиление существующей традиционной криптографии	12 месяцев
Переход к квантовоустойчивой криптографии	60 месяцев
Переход к квантово-гибридной технологии	60 месяцев
Полностью квантовая технология	В настоящее время не определено

В общих чертах обозначив задачи и сроки, вы можете получить приблизительную оценку времени, которое придется затратить на проект постквантовой миграции, и ознакомить с этим предварительным планом все заинтересованные стороны. Некоторые задачи, такие как обучение, формирование команды проекта и планирование, а также создание графика, могут выполняться одновременно. Если брать за основу табл. 9.1, фактическая реализация такого проекта займет шесть-семь лет, и большая часть этого времени придется на этап «Переход к квантовоустойчивой криптографии». Конечно, переход к квантовоустойчивой и в конечном итоге квантовой криптографии определяется не зависящими от вас факторами. Благодаря надлежащему планированию всех этапов, включая собственно обновление технологий, даже если потребуется более быстрый, ускоренный переход к квантовоустойчивой криптографии, чем тот, который вы изначально планировали, ваша организация может лучше подготовиться к переходу в квантовый мир. Правильное планирование экономит время. Над этим законом не властна даже квантовая механика.

Шаг 3. Сбор данных

Решающее значение для любого проекта квантовоустойчивой криптографической миграции имеет полная инвентаризация защищаемых данных. Она должна включать пять компонентов:

- обнаружение всех конфиденциальных данных и устройств;
- определение данных и заинтересованных сторон;
- выполнение рейтинга конфиденциальности;

- определение времени, в течение которого данные или устройства должны быть защищены от несанкционированного доступа и подслушивания;
- выявление современных систем защиты данных, связанных с защитой устройств, использующих криптографию, в частности определение вовлеченной криптографии и размеров ключей.

Инвентаризация должна включать тщательный учет всех конфиденциальных данных и устройств, которые вам необходимо скрыть от несанкционированного разглашения. У специалистов по компьютерной безопасности есть поговорка: «Если ты думаешь, что знаешь, где находятся все твои данные, ты или ошибаешься, или обманываешь себя». С учетом сказанного вам нужно как можно лучше разобраться в том, где находятся все конфиденциальные данные и устройства всех заинтересованных сторон, владеющих данными и устройствами, хранящих их и полагающихся на них. Заинтересованные стороны должны выяснить всю другую необходимую информацию.

Все устройства, хранящие конфиденциальную информацию или связанные с хранением таковой, должны быть учтены и исследованы. К ним относятся компьютеры, ноутбуки, планшеты, смартфоны, сетевое оборудование, устройства аутентификации, устройства физической безопасности и многое другое. Инвентаризация должна включать критические данные и устройства интернета вещей (IoT), такие как камеры видеонаблюдения, системы пропуска и контроля доступа к зданиям. Если эти устройства записывают конфиденциальную информацию или находятся в помещениях с ограниченным доступом, они должны быть включены в список. Если устройство использует криптографию и защищает что-то не предназначенное для общего пользования, оно тоже должно находиться в списке.

Все данные и устройства должны быть ранжированы в соответствии с чувствительностью данных и необходимостью их защиты. Некоторые организации используют маркировку, характерную для военной отрасли: «совершенно секретно», «секретно», «конфиденциально» и «для служебного пользования». Другие предпочитают корпоративные эквиваленты: «высокая ценность для бизнеса», «средняя ценность для бизнеса», «низкая ценность для бизнеса». Некоторые организации просто делят сведения на конфиденциальные и общие. Какую бы систему классификации данных, вы ни использовали, все данные и устройства должны быть ранжированы по критичности и значению для организации.

Далее, заинтересованные стороны должны определить, как долго идентифицированные данные и устройства должны сохраняться в безопасности, указав сроки (в годах) или критичные периоды (например: долгосрочные, среднесрочные, краткосрочные; или: 10 лет и более, 5–10 лет, менее 5 лет).

Затем определите даты систем защиты данных и устройств, участвующих в защите этих данных и этих устройств, если они используют криптографию. Не все системы защиты данных напрямую используют криптографию, но большинство использует ее хотя бы косвенно. Например, многие системы контроля доступа применяют только разрешения операционной системы, которые напрямую не связаны с криптографией, но общий успех разрешения

контроля доступа зависит от безопасности операционной системы, и все операционные системы используют криптографию (обычно много шифров, схем и систем). Вам следует поставить на учет всю криптографию, содержащуюся в секретной памяти, передаваемых секретных данных и приборах. Критические системы данных также будут включать всю вашу жизненно важную ИТ-инфраструктуру, такую как системы аутентификации и инфраструктурные услуги. Для каждой системы защиты данных определите используемую криптографию (симметричная, асимметричная, хеши, цифровые подписи и т. д.) и размеры ключей.

В отношении многих систем не получится определить, что представляют собой шифры, схемы и размеры ключей. Поставщики или разработчики могли уйти от вас, практически не оставив доступной документации, касающейся реализации криптографии. Команда проекта должна будет рассмотреть каждого найденного «неизвестного» и определить, является ли риск настолько незначительным, что его можно игнорировать для целей модернизации, или он должен считаться главным приоритетом (просто для снижения потенциального риска). Включайте эти неизвестные в план.

Шаг 4. Анализ

Компьютерная безопасность – это в основном оценка рисков. На этом наиболее важном шаге проекта вы определяете данные и системы, подверженные наибольшему риску, и указываете шаги, которые необходимо предпринять для снижения риска грядущего квантового криптовзлома. Анализ и рекомендации будут включать следующие задачи:

- определение квантовочувствительных систем безопасности данных, защищающих критически важные данные и устройства;
- ранжирование факторов риска для систем, находящихся под угрозой, включая то, какие системы нуждаются в приоритетном исправлении;
- определение исправлений;
- определение необходимых ресурсов, затрат и сроков.

Получив результаты инвентаризации защиты данных, определите квантовую восприимчивость используемой криптографии и, в частности, защиты критически важных конфиденциальных данных и устройств. Сравните то, что вы найдете, с перечнем криптокодов и размерами ключей, о которых известно, что они являются квантововосприимчивыми, как показано в табл. 5.1 главы 5. В главе 5 также рассматриваются квантововосприимчивые асимметричные шифры (например, RSA, DH, ECC, ElGamal и др.).

Любая система защиты важных критических данных или устройств, использующая устойчивую криптографию, должна быть выделена, и наиболее критическим системам должно уделяться особое внимание. Это даст общее представление с высоты птичьего полета о том, насколько велика проблема перехода в постквантовый мир. Не исключено, что масштабы проблемы вас расстроят, но возможен и другой вариант: вы будете удивлены, узнав, что многие ваши системы используют менее восприимчивые криптографические формы, такие как AES-256 или AES-512. Тщательная оценка риска может

привести вас к выводу, что проблема не так сложна, как вам представлялось. К сожалению, такое положение дел будет нехарактерным для большинства организаций, особенно тех, где используются асимметричные шифры.

Восстановление должно включать все возможные решения, необходимые для исправления квантововосприимчивой системы, начиная с обучения для всех заинтересованных сторон системы. Восстановление должно также определить, какие решения сводятся к простому обновлению размера ключа (например, с AES-128 до AES-256) и какие требуют полной замены шифров. Что можно обновить, а что просто заменить? Насколько будут велики ожидаемые усилия для каждой системы? Каковы ожидаемая стоимость и сроки для каждого решения по восстановлению? Вам надо будет поговорить и с заинтересованными сторонами, и с поставщиками.

Многие системы могут в конечном итоге использовать гибридные подходы. Например, возможно, основные цифровые ключи сертифицирующей организации (certification authority, CA), которые, как можно ожидать, будут иметь долгий срок службы, обновляются с помощью квантовоустойчивой криптографии, но отдельные ключи конечного пользователя с гораздо более коротким сроком службы обновляются для использования традиционной криптографии с большими размерами ключей.

Важно как можно скорее привлечь поставщиков, чтобы они поняли вашу озабоченность и, может быть, сообщили вам, как их компания планирует помочь. Во многих случаях поставщики не в полной мере знают о проблеме, или они знают о предстоящем квантовом прорыве, но практически не готовятся к нему, потому что думают, что у них впереди 10–20 лет. Обсуждение с ними ваших проблем может стать началом серьезного обсуждения в их компании. Вы даже можете узнать, что они не планируют переходить к постквантовой реализации или что для этого требуется обновление программного обеспечения до последней версии. Многие поставщики использовали миграцию SHA2, чтобы заставить клиентов перейти на последнюю версию программного обеспечения.

Многие компании могут иметь приложения, разработанные внутри компании, и им необходимо выяснить, кто их использует и как их можно модернизировать. Часто находят приложения, разработанные внутри компании, по которым не может быть найдено никакой информации и для анализа и обновления которой некого нанять. Ваша проектная группа должна будет решить, как поступать с такими приложениями, или, возможно, рассматривать каждый конкретный случай.

Даже системы, которые в настоящее время не считаются квантововосприимчивыми, понадобится обновить. Например, у вас могут быть критически важные данные, которые в настоящее время защищены системой AES-256, что не считается квантововосприимчивым решением. Но если вы планируете хранить данные в течение 10 лет или дольше, то можете перевести систему в AES-512. Этот переход от слабо квантововосприимчивой криптографии к гораздо менее квантововосприимчивой криптографии может не быть вашим основным приоритетом, но в перспективе он должен быть сделан.

Затем, после тщательного изучения всех задействованных систем, критичности, сроков и затрат, заинтересованные стороны должны решить, какие

меры по исправлению ситуации необходимо предпринять и когда. Следует документировать решения и представить их старшему руководству для утверждения и составления бюджета. Если вы провели анализ и сделали обзор правильно и тщательно, запланированные шаги облегчат принятие большинства окончательных решений.

Защита некоторых или всех данных

Вы можете решить, имеет ли смысл защищать только самые важные данные или защитить все. Иногда защита всех данных экономит деньги и время. Например, это приемлемое решение для многих компаний, ведущих бизнес в Европейском союзе (ЕС) или с клиентами из ЕС, при попытке согласовать требования Общего регламента защиты данных ЕС (General Data Protection Regulation, GDPR). Многие интернациональные компании решили, что дешевле применять требования GDPR ко всем данным и клиентам, расположенным в любом регионе, даже за пределами ЕС, чем раздельно применять требования ЕС только для специфических данных ЕС. Они также обеспокоены юридическими и финансовыми затратами, в случае если некоторые данные, к которым был бы применен регламент GDPR, попали в их менее защищенные хранилища данных. Чтобы не рисковать, эти компании просто применяли более строгий контроль ко всем данным. И наоборот, некоторые компании решили поместить конфиденциальные данные в изолированное хранилище данных, которое затем защищали более дорогими компонентами управления. Многие американские фирмы приняли это решение для PCI- и HIPAA-регулируемых данных. Эта стратегия может иметь смысл, когда количество данных составляет небольшой процент от того, с чем организация имеет дело, и если защищаемым данным можно доверить оставаться в изолированной области данных. Каждая организация должна решить, будет ли она защищать все или только некоторые данные. Компромиссное решение – защита только самых важных данных, но делать это нужно для всего предприятия, сосредоточив внимание на системах, которые их защищают.

Организации должны решить, какие данные должны быть защищены от квантовых атак, а какую криптографию необходимо обновить и когда.

Шаг 5. Принять меры / исправить

Настало время начать действовать. Обновите шифры, схемы и размеры ключей. Переходите на квантовоустойчивую криптографию и выполняйте другие постквантовые действия. Каждый шаг должен быть тщательно проверен в ограниченных пилотных проектах перед переходом к полномасштабным производственным мероприятиям. Каждый план действий должен включать план аварийного «возврата» на случай, если криптографический шаг миграции что-то сломает. Шаги возврата должны быть задокументированы и тщательно проверены перед выполнением шагов защиты.

Примечание Я с гордостью говорил, что за мои 30 лет реализации криптографических проектов и обновлений я ни разу не вызвал ни одного крупного непреднамеренного перерыва в работе – вплоть до нескольких лет

тому назад. И это было круто. Команда клиентов и я обновляли цифровые сертификаты на критически важные сетевые медицинские устройства в рамках более крупного глобального проекта по обновлению. Нами была создана процедура, позволяющая удаленно заменять, если необходимо, любой из недавно выпущенных сертификатов оригинальным, более старым действующим сертификатом, запустив единственную, хорошо проверенную команду. Если бы что-то с производственным обновлением пошло не так, мы могли бы запустить всего одну команду и сидеть сложа руки, пока она восстановит все затронутые устройства.

Несколько тестов процесса обновления сертификата прошли так хорошо, что я рекомендовал развернуть все остальные десятки тысяч сертификатов немедленно и по всему миру. Я выполнил подобное глобальное обновление десятки раз до этого и считал, что обновление сертификата не может вызвать проблем. Ни при каких условиях. К сожалению, когда были установлены новые сертификаты, один клиент без моего ведома внес пользовательские изменения в половину своих устройств, что привело к отключению недавно обновленных устройств (критического медицинского оборудования) от сети. Отказали в работе и остальные устройства, и поскольку они также отключились от сети, наша отказоустойчивая процедура возврата с помощью одной команды не могла быть запущена. Работа глобальной сети больницы была прервана на несколько дней, и необученным бригадам работников медицинского учреждения пришлось самим выполнять онлайн десятки практических шагов по установке специфицированных данных ЕС. В моей профессиональной карьере это была самая большая (и, к счастью, единственная) катастрофа для моих клиентов. Урок выучен. Протестируйте и попробуйте снова. Не спешите с производственными развертываниями без достаточного тестирования. Проверьте свои процедуры возврата и убедитесь, что они не зависят от работы сети подключения.

Обновите существующие политики и стандарты

Не вызывает сомнений, что вы должны убедиться прямо сейчас, что знаете обо всех организационных политиках и стандартах, требующих строго квантовоустойчивой криптографии. Вам нужно избежать серьезных потерь. Вы не хотите, чтобы новые, поступающие в вашу организацию системы имели слабую квантовоустойчивую криптографию, и не хотите просто добавить это к своим проблемам в будущем. Обновите вашу политику и стандарты, что автоматически потребует отказа от слабых криптографических систем. Обновляя политику, вы должны заявить, что все системы должны использовать общепринятые криптографические стандарты, если такое требование еще отсутствует. И если вы хотите добиться успеха, требуйте, чтобы все недавно купленные криптографические системы были криптогибкими.

Предотвратите утечку имеющихся данных в будущем

Существует риск, что сторонние организации с текущим или ближайшим будущим доступом к технологиям квантового взлома смогут подслушивать ваши «защищенные» сегодня данные, сохранять их и ждать возможности

взломать эти данные, когда получат соответствующие средства для этого. Мы можем предположить, что это происходит уже сегодня на уровне государств. Было бы глупо и безответственно с их стороны не делать этого. Это могут делать и крупные аморальные, коррумпированные корпорации, которые участвуют в корпоративном шпионаже против конкурентов. Например, возможно, ваши сетевые маршрутизаторы Wi-Fi используют AES-128. Все, что защищено AES-128, скоро станет квантововосприимчивым. Ваши противники могут прослушивать поток данных Wi-Fi и сохранять их для будущего взлома. Если это возможно в отношении вашей организации, рассмотрите все методы, которые необходимо использовать для предотвращения прослушивания ваших текущих защищенных данных. Эти методы включают:

- удаление важных данных из любого онлайн-хранилища или сетевой передачи (прежде всего для того, чтобы их нельзя было прослушать или украсть);
- использование квантовоустойчивой криптографии уже сегодня;
- изоляция физической области данных (там, где ее нельзя перехватить или украсть);
- использование оборудования изоляции сети, которое не подвержено квантовому взлому (это не то же самое, что использование квантовоустойчивой криптографии).

Что касается последнего пункта, то существуют поставщики, производящие высоконадежные сетевые карты армейского уровня и оборудование, которое нельзя легко подслушать. Они не используют традиционную криптографию, но вместо этого применяют методы экранирования и сигнализации, которые не позволят злоумышленнику подслушать или считать зашифрованную или защищенную информацию.

Шаг 6. Обзор и улучшение

Любой план проекта должен заканчиваться этапом проверки и улучшения. Как в процессе выполнения любого сложного проекта, вас будут ждать уроки – как положительные, так и отрицательные. Каждый план проекта должен иметь несколько контрольных точек, по достижении которых можно оценить план, провести корректирующие действия и получить рекомендации, что и где следует улучшить, если это необходимо.

Резюме

В этой главе мы обсудили, как уже сегодня вы и ваша организация можете начать готовиться к предстоящему квантовому прорыву до того, как он произойдет. Эта стратегия включает вовлечение высшего руководства, формирование долгосрочной команды проекта, обеспечение обучения и переход системы вашей организации от традиционной классической системы криптографической защиты. Чтобы сделать это последовательно, вам нужно провести полную и тщательную инвентаризацию защиты данных и опреде-

лить системы, которые необходимо заменить. Затем следует принять решение о правильном смягчении последствий, которые включают в себя увеличение размера существующих ключей и хешей, использующих в настоящее время традиционную криптографию, с последующим переходом на квантовоустойчивую криптографию и, в дальнейшем, на полностью квантовые криптографию и устройства. Планирование и вдумчивый процесс экономит время и деньги любой организации и, что более важно, эффективно сокращает компьютерный риск безопасности.

Я хочу поблагодарить читателей за то, что они позволили мне взять их в путешествие, начиная с изучения того, что такое квантовая механика и как она позволит взломать многие формы традиционных криптокодов. Эта книга рассказывает о квантовоустойчивой и квантовой криптографии и устройствах, а также ресурсах, имеющихся сегодня на рынке, и заканчивается сводным планом того, как сегодня ваша организация может начать подготовку к постквантовому миру. Если у вас есть какие-либо вопросы, предложения или возражения, напишите мне на roger@banneretcs.com. Я постараюсь ответить на вопросы в течение 24 часов.

Завершает книгу приложение, в котором перечисляются многие онлайн-ресурсы по квантам и квантовым вычислениям; они могут быть использованы в качестве справочного материала для обучения и получения новостей.

Приложение
Дополнительные источники по квантам

В этом приложении перечислены десятки ресурсов, которые вы можете использовать для улучшения и расширения вашего понимания квантовой механики, квантовых компьютеров и криптографии.

Полное понимание предмета – это то, к чему стремятся все специалисты в области квантовой механики. Это не только сложный вопрос, который бросает вызов нашему традиционному подходу к естествознанию, но и самое начало развития нового подхода с большим количеством пробелов. Поэтому неполное понимание вами квантовой механики, компьютеров или криптографии простительно. Каждая связанная с квантом статья и ресурс, которые вы изучите, улучшат ваше понимание. С учетом этого в приложении приводится перечень, в котором указаны как ресурсы, уже упоминавшиеся в книге, так и новые ресурсы. Приводятся ссылки на разные источники, в том числе книги, видео, онлайн-курсы, веб-сайты, блоги, правительственные программы, веб-сайты поставщиков и т. д. В отдельных случаях после названия ресурса я привожу в скобках свои комментарии, что, как мне кажется, поможет вам понять, подходит ли вам этот ресурс.

Книги

Aaronson Scott (2013). Quantum Computing Since Democritus. Cambridge: Cambridge University Press. (Отличная книга с сильным акцентом на компьютерную логику для прочтения активным исследователем квантовой механики и квантовых компьютеров. Особенно хорошо объясняет запутанность и квантовую телепортацию.)

Bell Philip (2018). Beyond Weird: Why Everything You Knew About Quantum Physics Is Different. Chicago. University of Chicago Press. (Отличная книга. Подробно обсуждает различные квантовые интерпретации; объясняет некоторые понятия квантовой механики различными замечательными и необычными способами (объяснение декогеренции и запутанности – лучшее из тех, что я когда-либо читал). Не должна быть вашей первой или единственной книгой по квантовой физике; эта книга для всех, кто проявляет интерес к пониманию квантовой механики.)

Bernhardt Chris (2019). Quantum Computing for Everyone. Cambridge, MA: MIT Press Carroll, Sean (2019). Something Deeply Hidden. United States: Dutton. (Вдохновенная логическая защита толкования концепции «Много миров».)
Johnston Eric R., Nic Harrigan, and Mercedes Gimeno-Segovia (2019). Programming Quantum Computers: Essential Algorithms and Code Elements. Sebastopol, CA: O'Reilly. (Насколько я знаю, новейшая книга по квантам.)
Kumar Manjit (2009). Quantum. New Delhi: Hachette India. (Рекомендуется Филипом Беллом как великолепное введение в квантовую механику.)
Kumar Manjit (2011). Quantum: Einstein, Bohr, and the Great Debate about the Nature of Reality. New Delhi: Hachette India.
Orzel Chad (2009). How to Teach [Quantum] Physics to Your Dog. New York: Scribner. (Отличная книга; идеально подходит для начинающих изучать квантовую физику.)
Orzel Chad (2018). Breakfast with Einstein: The Exotic Physics of Everyday Objects. Dallas, TX: BenBella Books, Inc. (Отличная книга; идеально подходит для тех, кто впервые изучает квантовую физику.)
Rhodes Richard (2012). Hedy's Folly: The Life and Breakthrough Inventions of Hedy Lamarr, the Most Beautiful Woman in the World. New York: Doubleday. (Отличная книга; вы узнаете, как Хеди Ламарр в соавторстве создала шифрование, которое является основой того, что даже сегодня защищает большинство беспроводных коммуникаций.)

Видео

Анионы и квантовые топологические компьютеры:

- www.youtube.com/watch?v=igPXzKjqrNg;
- www.youtube.com/watch?v=RW44rIrAZHY;
- www.youtube.com/watch?v=qj-w6ISQL5Y;
- www.youtube.com/watch?v=Xyfsr-coriQ.

BB84: www.youtube.com/watch?v=UVzRbU6y7Ks.

Процесс D-Wave/annealing:

- www.youtube.com/watch?v=UV_RlCAc5Zs;
- www.youtube.com/watch?v=kq9VqR0ZGNc;
- www.youtube.com/watch?v=Yy93LMGQbpo.

Анимация эксперимента с двумя щелями? (см. выше описание эксперимента): www.youtube.com/watch?v=fwXQjRBLwsQ.

Квантовые компьютеры с ионной ловушкой:

- www.youtube.com/watch?v=9aOLwjUZLm0;
- www.youtube.com/watch?v=WOQ_jWe62EA.

Канал Quanta Magazine YouTube: www.youtube.com/c/QuantamagazineOrgNews.

Квантовая физика для семилеток: www.youtube.com/watch?v=ARWBdfWpDyc.

Квантовая телепортация:

- www.youtube.com/watch?v=Czi5elPLfvA;
- www.youtube.com/watch?v=hTe2PYwnEpc.

Quantum Theory–Full Documentary HD: www.youtube.com/watch?v=CBrsWPCp_rs.

Нейл де Грассе Тисон (Neil deGrasse Tyson) объясняет квантовое запутывание: www.youtube.com/watch?v=q8CQAOwi2RI.

Онлайновые курсы

Scott Aaronson (2006). Quantum Computing Since Democritus («Квантовые вычисления со времен Демокрита»): www.scottaaronson.com/democritus/.

Quantum Computing Report's list of online educational resources («Перечень онлайновых лекций по квантовым вычислениям») // https://quantumcomputingreport.com/resources/education/.

Kirill Shilov. 16 Best Resources to Learn Quantum Computing in 2019 («16 лучших курсов по обучению квантовым вычислениям в 2019 году») // https://hackernoon.com/16-best-resources-to-learn-quantum-computing-in-2019-e5d8b797aeb6.

Leonard Susskind (2011), профессор Стэнфордского университета: The Theoretical Minimum («Квантовая механика. Теоретический минимум») // http://theoreticalminimum.com/courses/quantum-mechanics/2012/winter.

Веб-сайты

Daniel J. Bernstein, персональный сайт: https://cr.yp.to.

Caltec's Institute for Quantum Information and Matter: https://quantumfrontiers.com/.

GeekForge: https://geekforge.io/.

High Energy Physics Foundation Quantum Computing working group: https://hepsoftwarefoundation.org/workinggroups/quantumcomputing.html.

IFLScience!: www.iflscience.com/physics/.

Inside Science quantum-related articles: www.insidescience.org/search/node/quantum.

ISARA: www.isara.com/standards/ (перечень ведущихся работ по постквантовой криптографии).

Quantiki: www.quantiki.org.

Quantum Algorithm Zoo: https://quantumalgorithmzoo.org/.

Quantum Computing Reporting: https://quantumcomputingreport.com.

Quantum Computing Stackexchange: https://quantumcomputing.stackexchange.com/ (интересна с точки зрения решения технических вопросов).

Quantum for Quants: www.quantumforquants.org/ (сайт о финансировании).

Phys.org – Новости квантовой физики: https://phys.org/physics-news/quantum-physics/.

Physics Forum: www.physicsforums.com/forums/quantum-physics.62/.

Post-Quantum Cryptography wiki: https://pqc-wiki.fau.edu/w/Special:DatabaseHome.

PQCrypto: http://pqcrypto.eu/.

Sam Mugel's website for quantum technology in simple words: www.qwise.org.
Science Daily: www.sciencedaily.com/news/matter_energy/quantum_physics/.
CienceDirect's quantum-related articles: www.sciencedirect.com/search/advanced?qs=quantum.
The Quantum Pontiff: https://dabacon.org/pontiff/.
UK's National Quantum Technologies Hub for Networked Quantum Information Technology: www.nqit.ox.ac.uk.

Блоги

Scott Aaronson's blog: www.scottaaronson.com.
Quantum Physics blog: www.techbubble.info/blog/quantum-physics.
Top 25 Quantum Computing Blogs: https://blog.feedspot.com/quantum_computing_blogs/.

Подкаст

Stupid Qubit: https://stupidqubit.com/ (забавный, острый подкаст по квантам).

Журналы по квантам/информационные бюллетени

Quanta Magazine, Facebook: www.facebook.com/QuantaNewsQuanta.
Magazine newsletters: https://us1.campaign-archive.com/home/?u=0d6ddf7dc1a0b7297c8e06618&id=f0cb61321c.
Nature Magazine, quantum-related articles: www.nature.com/search?q=quantum.
Wired Magazine's quantum-related articles: www.wired.com/search/?q=quantum.

Перечень почтовых рассылок по квантам

Quantiki list of mailing groups: www.quantiki.org/wiki/mailing-lists.
Eclipse Foundation's Quantum Computing Working Group: https://accounts.eclipse.org/mailing-list/quantum-computing-wg.
Quantum Foundations mailing list: https://golem.ph.utexas.edu/category/2010/12/quantum_foundations_mailing_li.html.
Quantum Internet: www.irtf.org/mailman/listinfo/qirg.

Разные статьи по квантам

Philip Ball, Quanta Magazine articles: www.quantamagazine.org/authors/philip-ball/.
Mark G. Jackson's articles for popular audiences: http://physicsjackson.com/articles/.

Поставщики

Accenture: www.accenture.com/us-en/insight-quantum-computing.
Alibaba: https://us.alibabacloud.com/.
Atos: https://atos.net/en/insights-and-innovation/quantum-computing/atos-quantum.
Baidu: http://research.baidu.com/Research_Areas/index-view?id=75.
Cambridge Quantum Computing: https://cambridgequantum.com/.
ComScire: https://comscire.com.
D-Wave: www.dwavesys.com.
Google: https://ai.google/research/teams/applied-science/quantum-ai/.
Honeywell: www.honeywell.com/en-us/company/quantum.
Huawei: www.huaweicloud.com/en-us.
IBM: www.research.ibm.com/ibm-q/.
ID Quantique: www.idquantique.com.
Intel: https://newsroom.intel.com/press-kits/quantum-computing/#quantumcomputing-news.
IonQ: https://ionq.co/.
MagiQ Technologies: www.magiqtech.com.
Microsoft: www.microsoft.com/en-us/research/research-area/quantum/.
Quantum Computing, Inc.: https://quantumcomputinginc.com/.
Quantum Numbers Corp.: www.quantumnumberscorp.com.
Quintessence Labs: www.quintessencelabs.com.
Raytheon: www.raytheon.com/capabilities/products/quantum.
Rigetti: www.rigetti.com/qcs.
Toshiba: www.toshiba.eu/eu/Cambridge-Research-Laboratory/Quantum-Information/.

Твиттер

Caltech: https://twitter.com/IQIM_Caltech.
European Union's Quantum Internet Alliance: https://twitter.com/eu_qia.
Qiskit: https://twitter.com/qiskit.
Quanta Magazine: https://twitter.com/QuantaMagazine.
Quantiki: https://twitter.com/quantiki.
UK's National Quantum Technologies Hub for Networked Quantum Information Technology: https://twitter.com/NQIT_QTHub.

Ресурсы, относящиеся к программному обеспечению

Перечень квантовых алгоритмов: http://quantumalgorithmzoo.org/.
Перечень имитаторов квантовых вычислений: www.quantiki.org/wiki/list-qc-simulators.
Перечень открытых квантовых проектов: https://arxiv.org/pdf/1812.09167.pdf.
Перечень квантового программного обеспечения: https://github.com/qosf/os_quantum_software.

IBM Quantum Q Experience: https://quantumexperience.ng.bluemix.net/qx/editor.
Microsoft Quantum Software Development Kit: https://marketplace.visualstudio.com/items?itemName=quantum.DevKit.
Open Quantum Safe Project: https://openquantumsafe.org/.
Open-source and commercial quantum software projects and online quantum portals: https://github.com/qosf/os_quantum_software.
Python quantum open-source library: https://github.com/rigetti/pyquil.
Quantum Open Source Foundation: https://qosf.org/.
Quirk, drag-and-drop quantum simulator: https://algassert.com/quirk.

Различные квантовые консорциумы

Alliance for Quantum Technologies: http://inqnet.caltech.edu/index.html.
Quantum Worldwide Association: http://quantumwa.org/.

Спонсируемые правительством и некоммерческие программы

Australia, Australian Research Council's Centre of Excellence for Engineered Quantum Systems: https://equs.org/.
Australia, Center for Quantum Computation & Communication Technology: www.cqc2t.org.
Barcelona, Catalonia, Spain, Institute of Photonic Sciences: http://quantumtech.icfo.eu/.
Barcelonaqbit: www.barcelonaqbit.com/.
Beijing Academy of Quantum Information Science: www.baqis.ac.cn/en/.
Berkeley Quantum: https://berkeleyquantum.org/.
Brookhaven National Laboratories: www.bnl.gov/compsci/quantum/.
China, CAS Key Laboratory of Quantum Information: http://lqcc.ustc.edu.cn/.
Entanglement Institute, Newport, Rhode Island: www.entanglement.institute/.
Fermilab Quantum Information Science Program: https://qis.fnal.gov/.
France, Grenoble Quantum Silicon: www.quantumsilicon-grenoble.eu/.
German Research Foundation's Matter and Light for Quantum Computing: https://ml4q.de/.
IARPA's Coherent Superconducting Qubits: www.iarpa.gov/index.php/research-programs/csq.
IARPA's Logical Qubits: www.iarpa.gov/index.php/research-programs/logiq.
IARPA's Multi-Qubit Coherent Operations: www.iarpa.gov/index.php/research-programs/mqco.
IARPA's Quantum Enhancement Optimization: www.iarpa.gov/index.php/research-programs/qeo.
India, Light and Matter Physics: www.rri.res.in/light-matter-physics.html.
Korea, Center for Quantum Information: http://quantum.kist.re.kr/.
Leti, France: www.leti-cea.com/cea-tech/leti/english/Pages/Applied-Research/Strategic-Axes/Quantum-leti-initiative.aspx.

Los Alamos Quantum Institute: https://quantum.lanl.gov/about.shtml.
NASA Quantum Artificial Intelligence Laboratory: https://ti.arc.nasa.gov/tech/dash/groups/quail/.
National Science Foundation's Enabling Practical-Scale Quantum Computing: www.epiqc.cs.uchicago.edu/.
National Science Foundation's Quantum Information Science: www.nsf.gov/funding/pgm_summ.jsp?pims_id=505207.
Netherlands, QuSoft Research Center for Quantum Software: www.qusoft.org.
Netherlands, QuTech Academy: http://qutech.nl/.
NIST Joint Center for Quantum Information and Computer Science: http://quics.umd.edu/.
NIST Joint Quantum Institute: https://jqi.umd.edu/.
NIST Post-Quantum Cryptography contest: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography.
NIST Quantum Information Science: www.nist.gov/topics/quantum-information-science.
Oak Ridge National Laboratory Quantum Computing Institute: https://quantum.ornl.gov/.
Oak Ridge National Laboratory Quantum Information Science Group: https://web.ornl.gov/sci/qis/index.shtm.
Paris Centre for Quantum Computing: www.pcqc.fr.
Perimeter Institute for Theoretical Physics Quantum Information Research Group: http://perimeterinstitute.ca/research/research-areas/quantum-information.
Russian Quantum Center: https://rqc.ru/.
Singapore, Centre for Quantum Technologies: www.quantumlah.org.
Singapore, Quantum Technologies for Engineering Programme: www.a-star.edu.sg/imre/.
Research/Programmes-Centres/Quantum-Technologies-for-Engineering-ProgrammeSpanish National Research Council: https://qst.csic.es/.
Swiss National Science Foundation's Quantum Science and Technology: https://nccr-qsit.ethz.ch/.
United Kingdom's National Quantum Technology Programme: www.nqit.ox.ac.uk/.
Universities Space Research Association: www.usra.edu/quantum-computing.
U. S. National Science & Technology Council, National Strategic Overview for Quantum InformationScience: www.whitehouse.gov/wp-content/uploads/2018/09/National-Strategic-Overview-for-Quantum-Information-Science.pdf.

Примечание Много источников информации в этом перечне заимствовано из: https://quantumcomputingreport.com/players/governmentnon-profit/.

Именной указатель

Предметный указатель

Книги издательства «ДМК ПРЕСС»
можно купить оптом и в розницу
в книготорговой компании «Галактика»
(представляет интересы издательств
«ДМК ПРЕСС», «СОЛОН ПРЕСС», «КТК Галактика»).
Адрес: г. Москва, пр. Андропова, 38;
тел.: **(499) 782-38-89**, электронная почта: **books@alians-kniga.ru**.
При оформлении заказа следует указать адрес (полностью),
по которому должны быть высланы книги;
фамилию, имя и отчество получателя.
Желательно также указать свой телефон и электронный адрес.
Эти книги вы можете заказать и в интернет-магазине: **www.a-planeta.ru**.

Роджер А. Граймс

Апокалипсис криптографии

Главный редактор *Мовчан Д. А.*
dmkpress@gmail.com
Перевод *Яроцкий В. А.*
Корректор *Синяева Г. И.*
Верстка *Чаннова А. А.*
Дизайн обложки *Мовчан А. Г.*

Формат 70×100 1/16.
Гарнитура PT Serif. Печать офсетная.
Усл. печ. л. 23,56. Тираж 200 экз.

Отпечатано в ООО «Принт-М»
142300, Московская обл., Чехов, ул. Полиграфистов, 1

Веб-сайт издательства: **www.dmkpress.com**

Защитите себя от взлома с приходом квантовых вычислений

Еще в 2016 году Национальные институты стандартов и технологий (NIST) заявили, что организациям надлежит готовиться к квантовому криптографическому прорыву. Специалисты по безопасности должны прислушаться к этому совету и уже сегодня учитывать угрозы безопасности, возникающие с появлением квантовых вычислений.

В настоящее время уже созданы постквантовые алгоритмы шифрования, но их реализация требует времени и большой вычислительной мощности. Эта книга дает прогноз по поводу того, когда произойдет квантовый криптопрорыв, позволяющий обойти современные методы шифрования, какие приложения могут быть взломаны в ближайшее время и как обеспечить защиту от этих угроз при помощи имеющихся технологий.

Прочитав книгу, вы:

- познакомитесь с основными понятиями квантовой механики, а также с новейшими криптографическими методами;
- изучите основы цифрового шифрования, аутентификации и целостности хеширования;
- узнаете о новых изобретениях и усовершенствованиях, выходящих за рамки криптоквантовых вычислений;
- научитесь внедрять новую постквантовую криптографию для обеспечения безопасности пользователей, данных и инфраструктуры;
- поймете, как квантовые вычисления изменят нашу жизнь в ближайшем будущем.

Роджер А. Граймс проработал в области компьютерной безопасности более 30 лет, специализируясь на защите хостов и сетей, в том числе систем криптографии, и оценивая уровень защиты компаний от взломов. С 2005 г. Р. Граймс сотрудничает с журналами InfoWorld и CSOOnline, публикуя материалы по защите информации. Как представитель компании KnowBe4, крупнейшего в мире поставщика учебных материалов по вопросам безопасности, Роджер выступает на важнейших тематических мероприятиях по всему миру.

Интернет-магазин:
www.dmkpress.com

Оптовая продажа:
КТК «Галактика»
books@alians-kniga.ru

WILEY

ДМК ПРЕСС
ИЗДАТЕЛЬСТВО
www.дмк.рф

ISBN 978-5-97060-837-1