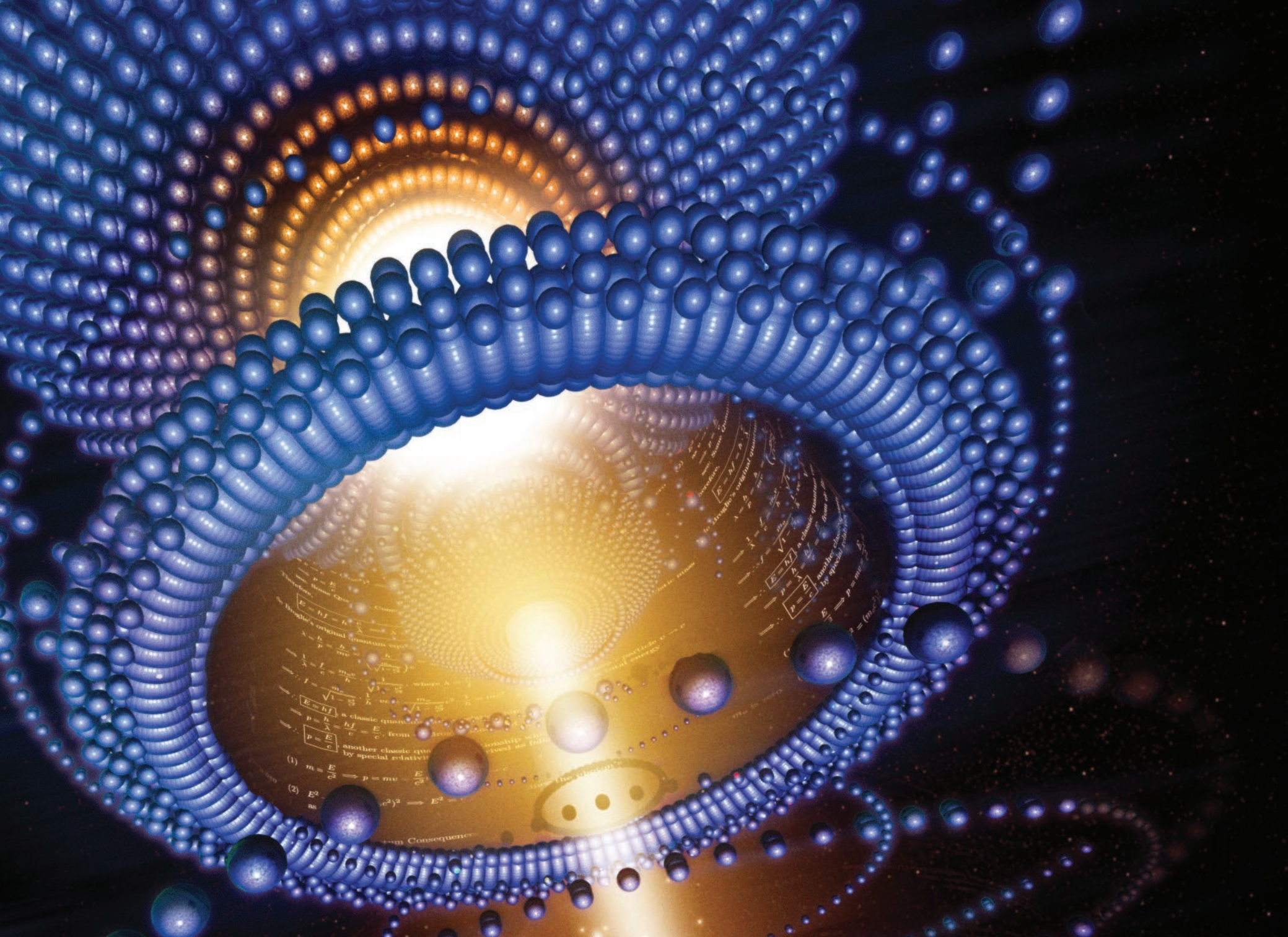


Illustration by Kenn Brown, Mondolithic Studios

ТЕХНОЛОГИИ

Квантовый взлом

Квантовые компьютеры сделают современные методы криптографии безнадежно устаревшими. И что тогда будет?

Тим Фолджер

ОБ АВТОРЕ

Тим Фолджер (Tim Folger) пишет для журналов *National Geographic*, *Discover* и других общенациональных изданий. Помимо этого, он редактор серии ежегодной антологии «Лучшая американская публикация в области естественных наук и наук о природе», выпускаемой издательским домом *Houghton Mifflin Harcourt*.

В один из солнечных октябрьских дней на пляже в Сан-Хуане, Пуэрто-Рико, два ученых нашли решение задачи, которая в то время еще даже не существовала. Шел 1979 г. Жиль Брассар (Gilles Brassard), незадолго до того получивший докторскую степень в Корнеллском университете, погрузился в теплые карибские воды, когда кто-то поплыл ему навстречу. Темноволосый незнакомец с жаром принялся рассуждать о том, как изготовить купюры, которые невозможно будет подделать. Метод, изобретенный несколькими годами ранее выпускником Колумбийского университета по имени Стивен Визнер (Stephen Wiesner), заключался во включении в банкноты фотонов — частиц света. Согласно законам квантовой механики, любая попытка измерить или скопировать фотоны мгновенно изменит их свойства. Каждая купюра имела бы свою собственную цепочку фотонов, квантовый регистрационный номер, который никоим образом нельзя скопировать.

«Я, конечно, был удивлен, — говорит Брассар, ныне профессор информатики Монреальского университета, — но вежливо выслушал». Его новым знакомым был Чарлз Беннетт (Charles Bennett), физик-исследователь из компании *IBM*. Как выглядит Брассар, Беннетт узнал на конференции, в которой оба принимали участие. Хотя они были заинтригованы идеей квантовой банкноты, им было ясно, что технически это невозможно. Даже сегодня никто не знает, как захватить, остановить и сохранить фотоны в куске бумаги. Частицы света, помимо всего прочего, обычно очень быстро движутся.

«Сегодня мы лучше разбираемся в проблеме, но так ни на йоту и не приблизились к тому, что хотя бы отдаленно имело практическое значение для квантовых банкнот, — продолжает Брассар. — Однако это стало исходной точкой мысленного эксперимента. Это прекрасный пример идеи, которая абсолютно безумна с практической точки зрения, но одновременно оказалась чрезвычайно плодотворной, поскольку именно оттуда у Беннетта и у меня родилась идея того, что ныне называется квантовым распределением ключа».

Квантовое распределение ключа (КРК) — это метод кодирования и передачи данных с помощью фотонов. В принципе, это дает нам в руки абсолютно не поддающуюся расшифровке форму криптографии. После той встречи на пляже Беннетт и Брассар начали пятилетнее сотрудничество, в ходе которого родился первый в истории криптографический метод, основанный не на сложности

ОСНОВНЫЕ ПОЛОЖЕНИЯ

- Традиционные компьютеры были плохо приспособлены для взлома схем шифрования (часто базирующихся на простых числах большой длины), которые лежат в основе повседневных интернет-коммерции и коммуникаций.
- Квантовые компьютеры, однако, смогут взломать сегодняшние схемы шифрования, эксплуатируя странные законы субатомного мира и испытав все варианты кода одновременно.
- Еще никто не построил полномасштабный квантовый компьютер, но ученые из университетов, государственных и частных компаний пытаются это сделать, и некоторые эксперты говорят, что смогут преуспеть в этом уже через десять лет.
- Именно поэтому ученые гоняются за совершенством и развертывают технику квантового шифрования, которая использует квантовую неопределенность для формирования практически неуязвимых кодов.

математических вычислений, а на законах физики. Когда в 1986 г. Беннетт и Брассар наконец опубликовали свою работу, мало кто из ученых заметил ее. Брассар вспоминает: «Те, кто уделил ей хотя бы какое-то внимание, сочли чем-то из разряда "физики шутят". Мы сами не воспринимали ее всерьез».

Теперь все изменилось. Тридцать лет назад едва ли кто-нибудь кроме сотрудников правительственных разведывательных агентств использовал криптографию. Сегодня она стала важной составной частью повседневных финансовых операций в Интернете. Всякий раз, когда кто-нибудь в режиме онлайн вводит пароль или номер кредитной карточки, сложные программы, встроенные во все интернет-браузеры, проводят невидимую работу, чтобы защитить эту информацию от кибервзломщиков. «Это технология, которая нужна всем, но никто не знает, что это такое, — утверждает Вадим Макаров, ученый из Института квантовых вычислений Университета Уотерлу в провинции Онтарио. — Она просто работает, и все!»

Но возможно, уже в недалеком будущем она перестанет работать. Почти каждая используемая сегодня схема шифрования скорее всего безнадежно устареет с приходом квантовых компьютеров — машин, способных взломать самые замысловатые шифры, защищающие сегодня все: от покупок на *Amazon.com* до электрораспределительных сетей. Хотя никто пока еще не построил полноценный квантовый компьютер, ученые в университетских, частных и правительственных лабораториях во всем мире пытаются это сделать. Среди документов, которые увидели свет благодаря разоблачителю Эдварду Сноудену, было описание секретного проекта Агентства национальной безопасности, называемого «Проникновение в хорошо защищенные укрытия», — программы создания квантового компьютера стоимостью $ 79,7 млн. «Трудно утверждать с какой-либо долей уверенности, что он не появится через 10–15 лет», — считает Рэй Ньюэлл (Ray Newell), физик из Лос-Аламосской национальной лаборатории.

Если (или, вернее, когда) загрузится этот первый квантовый компьютер, самым эффективным способом противостоять его способности быстро раскалывать самые трудные шифры скорее всего окажется другой вид квантового волшебства: методика криптографических сетей, базирующаяся на теории, которую Беннетт и Брассар придумали 32 года назад. Квантовое шифрование — метод кодирования сообщений, использующий странные

СЕГОДНЯ

Как работает схема шифрования сейчас

Каждый раз, когда вы покупаете что-нибудь в Интернете, ваш браузер и веб-сайт продавца обмениваются секретным кодом — ключом для шифрования информации, которой они собираются обменяться. Поскольку обе стороны используют один и тот же ключ, этот процесс называется симметричным шифрованием. Однако, чтобы безопасно переслать этот ключ, обе стороны используют второй вид шифрования — асимметричное шифрование. Эта двухступенчатая система работает отлично, но она в одно мгновение устареет, если появятся квантовые компьютеры.

Симметричное шифрование

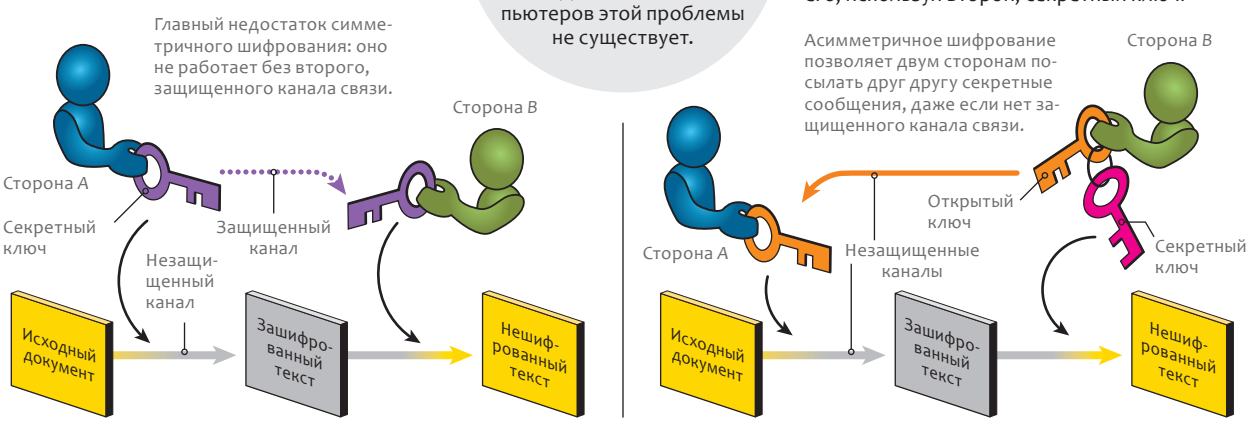
Столкнувшись с незащищенным каналом связи, сторона *A* зашифровывает сообщение, прежде чем отослать его стороне *B* по незащищенному каналу. Однако сторона *B* может прочесть это сообщение, поскольку сторона *A* отослала стороне *B* секретный ключ по защищенному обратному каналу.

Уязвимости

Асимметричное шифрование работает, поскольку классическому компьютеру чрезвычайно трудно находить простые множители очень больших чисел. Для квантовых компьютеров этой проблемы не существует.

Асимметричное шифрование

Сторона *B*, получатель, выбирает пару ключей: один, объясняющий, как закодировать сообщение, и другой, поясняющий, как его расшифровать. Это открытый ключ. Сторона *A* шифрует свое послание с помощью открытого ключа. Когда сторона *B* получает зашифрованное сообщение, она декодирует его, используя второй, секретный ключ.



Illustrations by Jen Christiansen

свойства одиночной частицы света, — более простая, как оказалось, задача, чем постройка квантового компьютера. И действительно, несколько небольших проектов по квантовому шифрованию уже в состоянии готовности к работе. «Если вы полагаете, что эта проблема через 10–15 лет все еще не будет решена, нам следовало бы заняться ею еще вчера, — говорит Ньюэлл. — Но, возможно, мы уже опоздали».

Очень большие числа

За не требующими усилий ударами по клавишам мыши или нажатиями пальцем на экран планшета со страницей электронной коммерции прячется элегантный и сложный математический каркас из двух различных форм криптографии: симметричное шифрование, при котором один и тот же секретный ключ используется для того, чтобы зашифровать и расшифровать данные; и асимметричное шифрование, при котором один ключ используется для шифрования сообщения и совсем другой для дешифровки. Каждый обмен секретной информации по Интернету требует использования обоих методов.

Типичная сессия между компьютером у вас дома и сервером интернет-продавца начинается с формирования симметричного ключа, который одинаков у покупателя и продавца и будет использоваться для шифрования номеров кредитной карты и другой персональной информации. Секретный ключ — это, по сути, набор инструкций, каким образом кодировать информацию. Самый простой до нелепости ключ мог бы, например, указывать, что каждую цифру в номере кредитной карты следует умножить на три. В реальном мире, конечно, ключи математически гораздо более сложны. Всякий раз, когда кто-нибудь покупает что-нибудь в Сети, браузер домашнего компьютера обменивается ключом с сервером интернет-продавца. Но каким образом сам ключ остается секретным во время первоначального обмена данными? Второй инструмент обеспечения безопасности, асимметричный ключ, шифрует симметричный.

Изобретенное в 1970-х гг. независимо Британской секретной службой и университетскими учеными асимметричное шифрование использует два различных ключа: открытый и секретный ключ. Оба необходимы для шифрованной передачи данных финансовой операции. Во время совершения онлайн-покупки сервер продавца посылает свой открытый ключ компьютеру покупателя. Тот, в свою очередь, использует открытый ключ продавца, который доступен всем клиентам, — чтобы зашифровать общий симметричный ключ. После получения зашифрованного симметричного ключа от покупателя сервер продавца расшифровывает его с помощью секретного ключа, которого больше ни у кого нет. После того как симметричный ключ безопасно передан, с его помощью шифруются остальные данные финансовой операции.

Открытый и секретный ключи, используемые при асимметричном шифровании, получают с использованием множителей очень больших чисел, вернее, очень больших простых чисел — целых, делящихся только на самих себя и единицу. Открытый ключ состоит из числа, полученного умножением двух больших простых чисел; закрытый ключ состоит из двух простых множителей,

ЗАВТРА

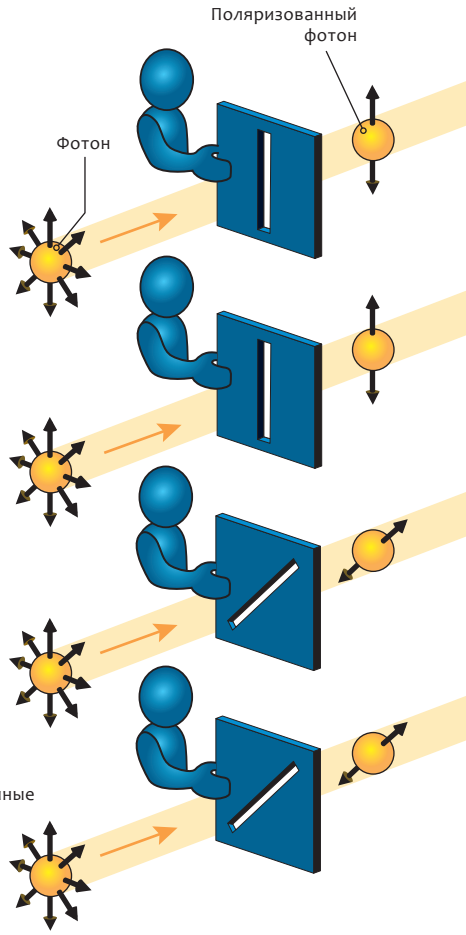
Квантовое будущее криптографии

Распределение квантового ключа — это способ секретной пересылки общего криптоключа с помощью потока поляризованных световых частиц — фотонов. Если устройство для перехвата информации определяет поляризацию этих фотонов, когда они пролетают мимо, сам акт измерения изменит поляризацию некоторых из этих фотонов, и оба, отправитель и получатель, будут знать, что их сообщение было перехвачено.

Отправка и получение поляризованных фотонов

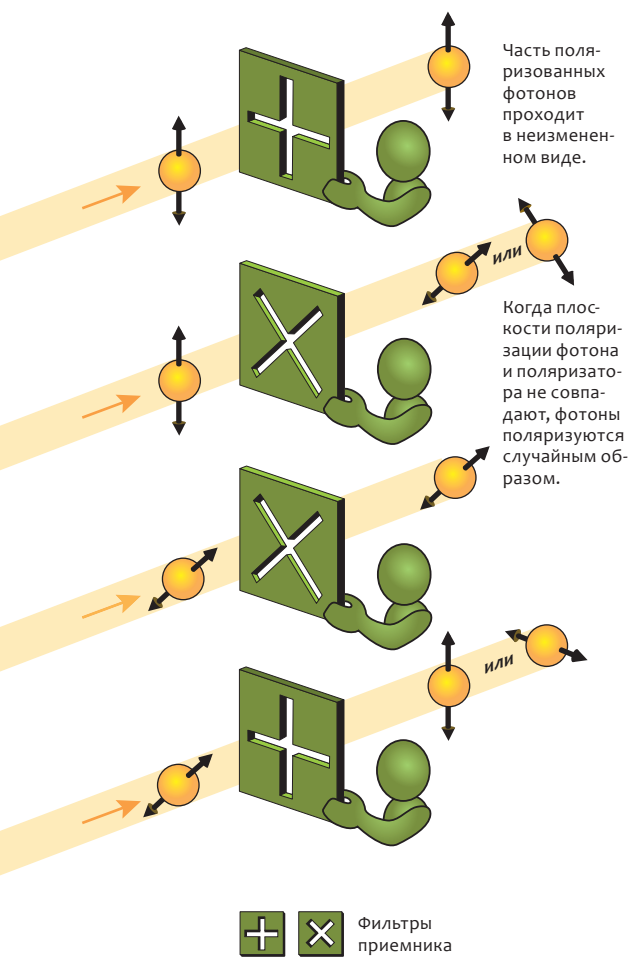
Отправитель *(синий)* испускает последовательность фотонов, каждый из которых проходит через один из четырех поляризационных фильтров. Каждому фильтру, а следовательно и направлению поляризации, соответствует значение «0» или «1» бита информации *(внизу)*. Отправитель записывает значение бита каждого фотона. Получатель *(зеленый)* может определить значение бита каждого фотона только после того, как он прошел через фильтр приемника.

В передатчик встроены четыре поляризационных фильтра. Последовательность битов (бит кодируется ориентацией плоскости поляризации фотона) при передаче.



но обратная операция — факторизация, или разложение на простые множители, большого числа — непосильная задача даже для самых мощных компьютеров. Числа, используемые для асимметричного шифрования, в типичном случае состоят из сотен цифр. Найти простые делители таких больших чисел — все равно что пытаться выделить исходные цвета в смеси двух красок. «Проще простого смешать две краски. А вы попробуйте их разделить!», — говорит Ньюэлл.

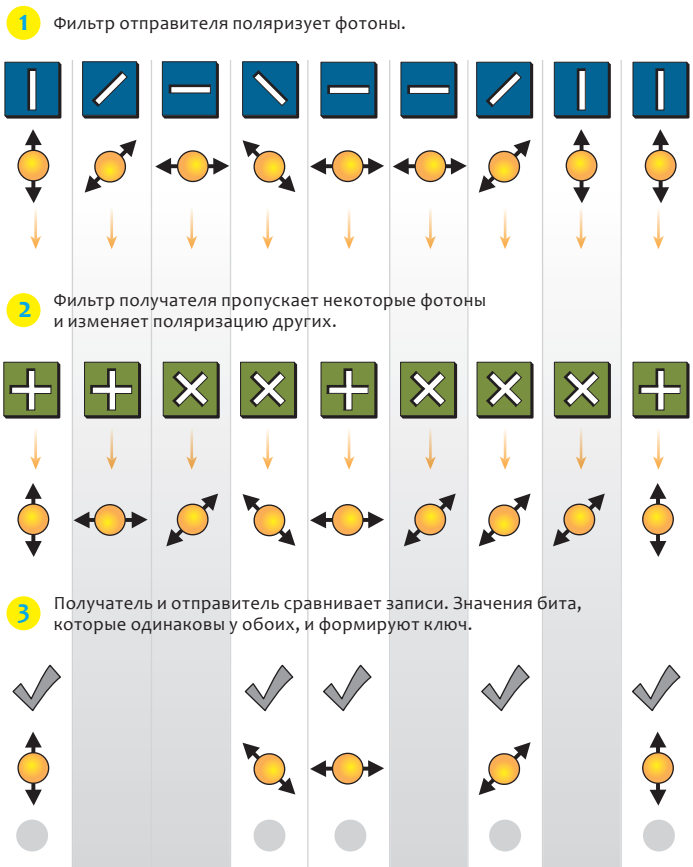
Самый распространенный способ асимметричного шифрования называется *RSA* в честь его изобретателей — Рона Ривеста (Ron Rivest), Ади Шамира (Adi Shamir) и Леонарда Адлемана (Leonard Adleman), которые предложили идею в конце 1970-х гг. в Массачусетском технологическом институте. Длина ключа постоянно увеличивалась для того, чтобы уберечь его от хакеров с все более мощными компьютерами, использующих все более эффективные алгоритмы: более длинные ключи требуют для расшифровки больше вычислительной мощности. Типичный асимметричный ключ сегодня имеет длину 1024 бит, но даже если оставить в стороне перспективы создания квантовых компьютеров, этого, возможно, окажется недостаточным, чтобы отразить кибератаки в будущем. «Американский Национальный институт стандартов и технологий активно рекомендует увеличить длину ключей *RSA*-шифрования до 2048 бит, — рассказывает Ричард Хьюз (Richard Hughes), физик из Лос-Аламоса. — Но платой за удлинение ключа становится производительность. Раздражающая всех задержка, когда вы кликаете "Купить" и все на секунду-две зависает, — это работа открытого ключа. И чем больше его длина, тем дольше задержка». Проблема в том, что процессоры

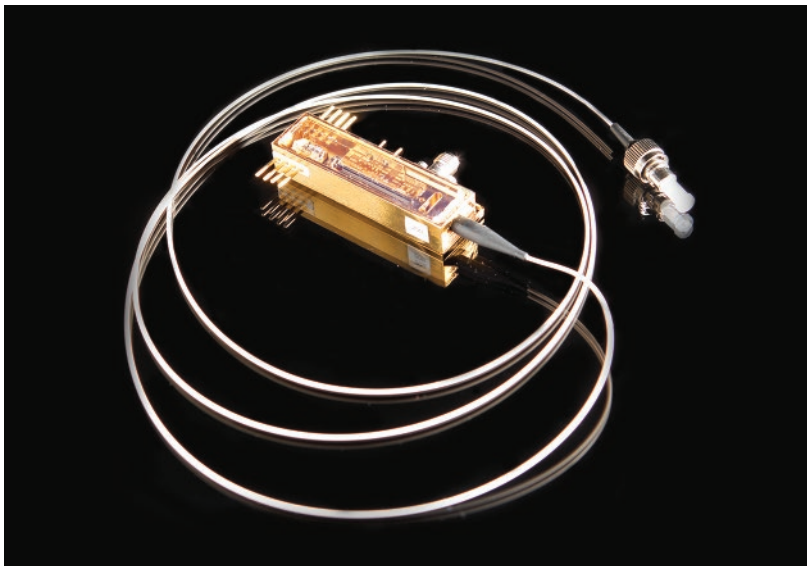


Приемник выбирает случайным образом один из двух фильтров для каждого фотона.

Восстановление ключа

Получатель записывает значения битов фотонов, проходящих через фильтр приемника, затем сравнивает записи с отправителем, который показывает, когда получатель правильно выбрал фильтр. Последовательность значений битов, которые одинаковы и у отправителя, и у получателя, и есть квантовый ключ.





Квантовый маршрутизатор: *плата QKarD, разработанная учеными Лос-Аламосской национальной лаборатории, позволит любому количеству компьютеров, мобильных телефонов и других устройств обмениваться квантовыми ключами через защищенный центральный сервер*

в наших компьютерах совершенствуются недостаточно быстро, чтобы успеть за совершенствованием алгоритмов декодирования, которые заставляют увеличивать длину ключей. «Это становится проблемой по многим причинам, — продолжает Хьюз. — Если вы имеете дело с облачной системой, выполняющей множество сессий с открытыми ключами одновременно, или если вы управляете чем-то вроде электрической распределительной сети, вы не можете позволить системе задержки такой продолжительности».

Но даже рекомендованное Национальным институтом стандартов и технологий усовершенствование безнадежно устареет, если на сцену выйдут квантовые компьютеры. «Мне думается, с вероятностью один к двум квантовый компьютер сможет находить ключи стандарта *RSA*-2048 к 2030 г.», — утверждает Мишель Моска (Michele Mosca), сооснователь Института квантовых вычислений, комментируя предстоящее введение стандарта на 2048-битные *RSA*-ключи. «В прошедшие пять лет мы определенно наблюдали большой прогресс, что приводит нас к мысли о необходимости быть готовым к встрече с квантовыми компьютерами, — считает Донна Додсон (Donna Dodson), главный советник в области кибербезопасности Национального института стандартов и технологий. — Мы склонны полагать, что их появление весьма вероятно».

О кодах и кубитах

Почему квантовый компьютер обещает стать таким мощным? В традиционном компьютере любой отдельный бит информации может принимать только одно из двух значений: «0» или «1». А вот в квантовом компьютере используется странное свойство субатомного мира, в котором отдельная частица может находиться одновременно во множестве состояний. Как шредингеровский кот в ящике одновременно жив и мертв до тех пор, пока кто-нибудь не откроет ящик и не заглянет внутрь, так квантовый бит, или кубит, информации может быть одновременно и «0», и «1». (Физически кубит может быть, например, единственным электроном, находящимся в двух спиновых состояниях одновременно.) Квантовый компьютер с тысячей кубитов обладал бы 2^{1000} различных возможных квантовых состояний, что намного превышает число всех частиц во Вселенной. Это не означает, что квантовый компьютер мог бы хранить неограниченное количество данных: любая попытка увидеть кубиты мгновенно заставила бы их принять единственное 1000-битное значение. Однако с помощью хитроумных инструментов гигантским числом возможных кубитных состояний можно было бы манипулировать еще до акта наблюдения, выполняя тем самым вычисления, которые невозможны с помощью обычных компьютеров.

В 1994 г. математик Питер Шор (Peter Shor), в то время работавший в компании *AT&T Bell Laboratories*, доказал, что квантовый компьютер сможет легко разложить на простые множители большие числа, которые используются в *RSA*-шифровании — схеме асимметричного шифрования, защищающей обмен симметричными ключами во время передачи данных по Интернету. Фактически Шор написал первую программу для квантового компьютера. В отличие от традиционного компьютера, где вычисления ведутся последовательно, один шаг за такт, квантовый компьютер выполняет все операции одновременно, и именно этим свойством и воспользовался Шор. «Алгоритм Шора низвергнет *RSA*-шифрование», — утверждает Моска. Но методы симметричного шифрования, самый распространенный из которых — так называемый «Улучшенный стандарт шифрования» *(Advanced Encryption Standard, AES)*, одобренный Национальным институтом стандартов и технологий в 2001 году, — по-прежнему будут безопасными даже с появлением квантовых компьютеров. Это происходит потому, что в программах симметричного шифрования, таких как *AES*, для кодирования ключей простые числа не используются. Вместо этого симметричные ключи состоят из случайных последовательностей «0» и «1»,

COURTESY OF LOS ALAMOS NATIONAL LABORATORY

обычно длиной 128 бит. Это дает 2^{128} различных вариантов комбинаций ключа, а значит, хакер в поисках ключа должен будет отсортировать одну из миллиарда миллиардов миллиардов миллиардов комбинаций. Самому быстродействующему на сегодняшний день суперкомпьютеру — китайскому «Тяньхэ-2» *(«Тяньхэ» переводится с китайского как «Млечный Путь». — Примеч. пер.)*, который способен перемалывать данные со скоростью 33,8 квадриллионов ($33{,}8 \times 10^{15}$) операций в секунду, потребовалось бы более триллиона лет, чтобы проверить все возможности в поисках ключа. Даже квантовый компьютер не смог бы помочь хакерам в лоб расколоть такие гигантские числа. Но эти огромные симметричные ключи во время проведения платежей по Интернету шифруются с помощью асимметричных программ, таких как *RSA*, которые уязвимы для метода факторизации Шора.

Однако прежде чем программа Шора сможет свалить с пьедестала *RSA*-кодирование, нужно создать квантовый компьютер достаточной мощности, который мог бы ее выполнить. Моска предсказывает, что в течение следующего года несколько лабораторий во всем мире разработают рудиментарные системы, состоящие из нескольких десятков кубитов. «Если вы попытаетесь разложить на множители 2048-битный ключ с *RSA*-шифрованием, — говорит он, — вам, возможно, потребуется не менее 2 тыс. кубитов». Скачок с десятков до тысяч кубитов, вероятно, займет лет десять, но он не видит на пути к этому каких-либо непреодолимых препятствий. «Уже сейчас мы достигли большинства рабочих характеристик, позволяющих построить полномасштабный квантовый компьютер, — продолжает Моска, — не обязательно все они получены в одном месте, в одно и то же время и в системе, которая подается масштабированию».

В отличие от обычного секретного ключа фотонный ключ почти полностью защищен от злонамеренного считывания. Любой, кто попытается перехватить фотоны, внесет изменения в их состояние, изменив их величины

Квантовые сети

Хорошая новость — то, что до сих пор прогресс в технике квантового шифрования опережал попытки создать работающий квантовый компьютер. Квантовое шифрование получило первый толчок в 1991 г., когда Артур Экерт (Artur Ekert), физик из Оксфордского университета, опубликовал статью по квантовой криптографии в престижном журнале *Physical Review Letters*. Экерт, который в то время не слышал о более ранней работе Беннетта и Брассара, описал альтернативный метод использования квантовой механики для шифрования информации. Его работа в конечном итоге вызвала новый интерес и признание идеи Беннетта и Брассара, которая оказалась более практичной, нежели собственная схема Экерта.

Однако только в 2000-е гг. техника квантового шифрования начала продвигаться из лаборатории в мир коммерции. К тому времени физики нашли способ охлаждать детекторы фотонов — существенный и самый дорогой компонент любого устройства квантового шифрования — не жидким азотом, а с помощью электрического тока. «Когда в 1997 г. я начинал работу над свой диссертацией, их охлаждали, погружая детекторы в сосуд Дьюара с жидким азотом, что вполне приемлемо в лаборатории, но не очень практично, если вы хотите использовать их в центре обработки данных», — рассказывает Грегуар Риборди (Grégoire Ribordy), председатель правления швейцарской компании *ID Quantique*, в 2007 г. разработавшая одну из первых коммерческих систем квантовой криптографии, которую правительство Швейцарии закупило для защиты центров обработки и хранения информации. Эта компания с тех пор продала свое оборудование швейцарским банкам и сегодня совместно с Баттельским мемориальным институтом в Колумбусе, штат Огайо, занимается созданием сети, которая должна соединить офисы компании в Огайо с ее отделением в Вашингтоне.

В один из хмурых летних дней Нино Валента (Nino Walenta), физик из Баттельского института, показывает мне одно из устройств шифрования. «Все, что нам требуется, находится здесь, на этой полке, — рассказывает он. — Вся квантовая оптика и все, что нам необходимо для генерирования ключей и их отсылки, вы видите здесь». Валента стоит рядом с двухметровым шкафом в подвале лаборатории комплекса института. На одной полке шкафа стоит металлический ящик размером с большой портфель. Внутри него находится физическое воплощение схемы квантового шифрования, которую первыми предложили Беннетт и Брассар более 30 лет назад.

Установка состоит из небольшого лазерного диода, похожего на те, что используются в *DVD*-проигрывателях и сканерах штрихкодов, который направляет импульсы света на стеклянный фильтр. Фильтр поглощает почти все фотоны,

пропуская в среднем лишь один фотон за раз. Эти отдельные фотоны затем поляризуются в одном из двух направлений, каждое направление соответствует значению бита «1» или «0». Будучи отфильтрованными и поляризованными, фотоны становятся основой для секретного ключа, который затем передается по оптико-волоконному кабелю адресату, чья установка декодирует ключ, измеряя поляризацию фотонов.

В отличие от обычного секретного ключа фотонный ключ почти полностью защищен от злонамеренного считывания. (Более подробно о «почти полностью» чуть позже.) Любой, кто попытается перехватить фотоны, внесет изменения в их состояние, изменив их величины. Сравнив части ключа, законные отправитель и получатель могут проверить, совпадают ли переданные фотоны с исходными. Если будут замечены следы взлома, они могут дискредитировать ключ и повторить операцию. «Сегодня ключи часто не меняют годами, — говорит Валента. — Но в случае распределения квантового ключа мы можем менять ключ каждую секунду или минуту, и именно поэтому он так надежен».

Баттельский институт уже построил квантовую сеть для того, чтобы обмениваться финансовыми отчетами и другими секретными документами между своей штаб-квартирой в Колумбусе и одним из своих производственных предприятий в Дублине, штат Огайо, по соединяющей их 110-километровой линии оптоволокна. Такое расстояние, как оказалось, приближается к верхнему пределу, позволяющему передавать сообщения с квантовым шифрованием. При бóльших расстояниях сигнал деградирует из-за поглощения фотонов волоконно-оптическим кабелем.

Чтобы обойти это ограничение и расширить свою сеть, покрыв другие районы Колумбуса, а в недалеком будущем и всю столицу — Вашингтон, ученые Баттельского мемориального института совместно с фирмой *ID Quantique* ведут работы по развертыванию так называемых защищенных узлов, которые будут получать квантовые послания и транслировать их далее. Эти узлы будут помещены в герметичные изолированные контейнеры, чтобы защитить чувствительные датчики фотонов, охлаждаемые до -40° С. Если кто-нибудь попытается проникнуть в один из таких узлов, находящееся внутри устройство сотрет всю информацию и отключится. «Генерация ключей прекратится», — объясняет Дон Хэйфорд (Don Hayford), физик, руководящий исследованиями в области квантового шифрования в институте.

Если цепь защищенных узлов будет работать без сбоев, говорит Хэйфорд, эту технологию можно будет развернуть в более широком масштабе. Он вручил мне брошюру с картой, иллюстрирующей перспективную квантовую сеть, охватывающую большие территории страны. «Это наша концепция квантовой сети, которая защитит всю Федеральную резервную банковскую систему, — продолжает он. — Если тебе доверили соединить все банки Федеральной резервной системы, это наилучшим образом характеризует твою работу. Чтобы проложить линию квантовой сети через всю страну, потребуется примерно 75 узлов. Возможно, покажется, что это слишком много, но, прокладывая обычную волоконно-оптическую линию, повторители нужно ставить на таких же расстояниях».

Многие ученые, работающие в области криптографии, считают, что американское Агентство национальной безопасности (АНБ) и другие разведывательные агентства во всем мире накопили огромное количество зашифрованных данных из Интернета, которые не поддаются расшифровке современными средствами

Китайское правительство выбрало ту же технологию. Уже началось строительство 2000-километрового участка квантовой сети между Шанхаем и Пекином, которая будет использоваться правительством и финансовыми институтами. Но хотя проекты, представленные Хэйфордом и уже осуществляемые в Китае, вероятно, будут использоваться для обеспечения безопасности банков и других организаций, имеющих частные сети, для Интернета они не годятся. Защищенные узлы соединяют один компьютер со следующим в линейной цепи и не подходят для разветвленной сети, в которой любая машина может легко общаться с любой другой. У физика Бет Нордхольт (Beth Nordholt), которая недавно уволилась из Лос-Аламосской национальной лаборатории, такие двухточечные соединения вызывают ассоциации с хаотическим становлением телефонной связи в конце XIX столетия, когда темные связки кабелей нависали над городскими улицами. «В то время нужно было прокладывать отдельную линию к каждому, с кем вы хотели перезваниваться, — говорит она. — Такая структура плохо поддается масштабированию».

Нордхольт и ее муж Ричард Хьюз, а также их коллеги по Лос-Аламосу Ньюэлл и Глен Питерсон (Glen Peterson) в настоящее время работают над тем, чтобы сделать квантовое шифрование легко масштабируемым. С этой целью они построили прибор размером с карту памяти, который позволит подключать любое количество сетевых устройств — сотовые телефоны, домашние компьютеры и даже телевизоры, — чтобы обмениваться квантовыми ключами посредством соединения с защищенным центральным сервером. Они назвали свое изобретение *QKarD*, обыгрывая термин *Quantum-Key Distribution* — распределение квантового ключа.

«Самые дорогостоящие компоненты техники квантового шифрования — это однофотонные фотоприемники и все, что требуется для их охлаждения и приведения в чувство», — рассказывает Нордхольт. Затем вместе с коллегами она устанавливает сложные дорогостоящие компоненты в один из компьютеров сетевого концентратора. Клиентские компьютеры, каждый из которых оборудован платой *QKarD*, соединяются с концентратором (но не непосредственно друг с другом) оптоволоконными кабелями. Плата *QKarD* сама по себе — это передатчик с небольшим лазером, который посылает фотоны в концентратор.

Работа *QKarD* чем-то напоминает работу АТС. Каждый компьютер сети загружает свои собственные симметричные ключи, представляющие собой поток фотонов к концентратору. Такое квантовое шифрование заменяет собой *RSA*-кодирование, которое обычно используется для защиты при передаче симметричного ключа. После того как все клиентские компьютеры и концентратор обменялись квантовыми ключами, концентратор использует эти ключи и *AES*-шифрование для передачи обычных, неквантовых сообщений между любыми двумя клиентами сети, которым требуется обменяться секретной информацией.

Группа Нордхольт работала с опытными платами *QKarD*. Несмотря на то что вся их система расположена в единственной небольшой лаборатории в Лос-Аламосе, волоконно-оптический кабель 50-километровой длины, смотанный в бухту под лабораторным столом, соединяет компоненты системы и моделирует связь на больших расстояниях. Лицензия на технологию *QKarD* была продана компании *Whitewood Encryption Systems* для коммерческого продвижения. Если прибору удастся успешно выйти на рынок, то, по расчетам Хьюза, центральный концентратор, способный объединить 1 тыс. клиентских машин, оборудованных платами *QKarD*, вероятно, будет стоить $10 тыс. При массовом производстве сама плата *QKarD* будет стоить всего $50.

«Я хотела бы увидеть устройства *QKarD*, встроенные в телефоны или планшетные компьютеры, чтобы можно было безопасно соединяться с сервером, — добавляет Нордхольт. — Или, например, вы кладете телефон или планшет на базовую станцию в своем офисе и загружаете ключи [к серверу]. Можно было бы органичным способом строить сеть».

Квантовое будущее?

Совершенствование всемирной инфраструктуры шифрования, возможно, займет более десятка лет. «Чем шире развернута какая-либо система, тем труднее исправлять ее недостатки, — говорит Моска. — Даже если мы могли бы устранить их на технологическом уровне, все должны будут прийти к соглашению, каким образом это сделать, кроме того, необходимо понять, сохранится ли работоспособность всех компонентов глобальной коммуникационной системы. Ведь в мире нет даже единой электрической системы — мы должны приспосабливаться всякий раз, когда путешествуем».

Сама по себе трудность поставленной задачи заставляет только ускорить ее выполнение. «Дело не просто в защите номеров кредитных карт. Проблема становится действительно серьезной», — говорит Нордхольт. По ее словам, Айдахская национальная лаборатория провела исследование, показавшее, что хакеры могут взорвать генераторы, запустив вредоносные данные в компьютерную сеть, управляющую работой электрораспределительной сети. «Я не хочу нагнетать атмосферу рассказами о сценариях конца света, — говорит она, — но это действительно сильно изменит жизнь людей».

Однако первоочередной задачей квантового компьютера, вероятно, будут не электрораспределительные сети. Многие ученые, работающие в области криптографии, считают, что американское Агентство национальной безопасности (АНБ) и другие разведывательные агентства во всем мире накопили огромное количество зашифрованных данных из Интернета, которые не поддаются расшифровке современными средствами. Эти данные сохраняются и пополняются, и резонно будет предположить, что в АНБ смогут расшифровать их, когда получат в свое распоряжение квантовый компьютер. При таком сценарии риску окажется подвергнутой не только личная переписка граждан несколько десятилетий назад, под угрозой будет наша сегодняшняя корреспонденция, которую мы по наивности считаем надежно защищенной.

«Было бы абсолютным сумасшествием полагать, что где-то там нет кого-нибудь, а может быть и множества тех, кто записывает весь сетевой трафик и просто ожидает, когда появится техника, способная взломать все старые шифры, — считает Брассар. — Поэтому, хотя квантового компьютера еще не существует, и даже если его не разработают

в течение следующих 20 лет, как только он появится, вся ваша корреспонденция, которую вы отправили с первого дня, используя эти классические методы [шифрования], окажется скомпрометирована, т.е. доступна тому, кому она не предназначалась».

Но даже когда квантовое шифрование получит широкое распространение, игра в кошки-мышки в криптографии продолжится. Если история традиционной криптографии может служить проводником, неизбежно существует пропасть между теоретическим совершенством и его реальным воплощением. Когда *RSA*-шифрование было впервые реализовано, оно считалось абсолютно надежным, рассказывает Зульфикар Рамзан (Zulfikar Ramzan), ответственный за технологию в компании *RSA*, которую Ривест, Шамир и Адлеман создали, чтобы коммерциализировать свое изобретение. Но в 1995 г. Пол Кошер (Paul Kocher), в то время студент Стэнфордского университета, обнаружил, что может взломать *RSA*-код, просто наблюдая, сколько времени компьютеру требуется, чтобы закодировать небольшой объем данных.

Оказалось, что если ключ имеет больше «1», чем «0», то требуется немного больше времени, чтобы выполнить *RSA*-шифрование. Используя эту особенность можно взломать *RSA*-код, просто наблюдая, измеряя временные характеристики и засекая время, которое требуется компьютеру для вычисления

«Оказалось, что если ключ имеет больше "1", чем "0", то требуется немного больше времени, чтобы выполнить *RSA*-шифрование, — рассказывает Рамзан. — А затем, повторяя это наблюдение снова и снова и измеряя временные характеристики, можно, как это ни удивительно, получить весь *RSA*-шифр, исключительно засекая время, которое требуется для вычисления». Заплатка была достаточно простой: инженерам удалось закамуфлировать время вычисления, добавив немного случайности в процедуру. «Но, опять же, эта атака была такого типа, какой никто не ожидал, пока кто-то не объявился и не совершил ее, — продолжает Рамзан. — Так что возможны аналогичные атаки в контексте квантовых вычислений».

Более того, первая квантовая атака уже была проведена. Пять лет назад группа, возглавляемая Макаровым, в то время работавшим в Норвежском технологическом университете, подсоединила чемодан, набитый оптическим оборудованием, к волоконно-оптической линии связи, соединенной с системой квантового шифрования компании *ID Quantique*. Используя лазерные импульсы, чтобы на время ослепить фотоприемник шифровального устройства, группа Макарова смогла расшифровать считавшийся защищенным сеанс квантовой передачи данных.

По словам Макарова, такая атака скорее всего не под силу обычному хакеру. «Тинейджеру с этой задачей не справиться, — говорит он. — И вам потребуется доступ к инструментам оптической лаборатории. В подпольной мастерской вы таких инструментов не найдете, по крайней мере пока». Хотя с тех пор компания *ID Quantique* устранила дыру в системе защиты информации своего устройства и она стала непроницаемой для такого типа атак, успешный взлом Макарова развеял ореол неуязвимости, окружавший квантовую криптографию. «Взломать проще, чем построить», — добавляет он.

У Брассара нет никакого сомнения, что сумасшедшая идея, которая в общих чертах родилась у него и Беннетта на пляже много лет назад, даже если она несовершенна, станет в будущем критическим звеном в обеспечении безопасности множества сетей во всем мире. «Чтобы сделать это, потребуется сильное желание, — убежден Брассар. — Это будет недешево, влетит в копеечку так же, как борьба с изменениями климата. Но все затраты мизерны по сравнению с тем, что мы потеряем, если не будем этим заниматься — и в том и в другом случаях». ■

Перевод: А.П. Кузнецов

ДОПОЛНИТЕЛЬНЫЕ ИСТОЧНИКИ

■ Беннетт Ч., Брассар Ж., Экерт А. Квантовая криптография // ВМН, № 11–12, 1992.

■ Стикс Г. Совершенно секретно // ВМН, № 4, 2005.

■ The Cost of the "S" in HTTPS. David Naylor et al. in Proceedings of the 10th ACM International on Conference on Emerging Networking Experiments and Technologies, pages 133–140; 2014.

■ NSA Seeks to Build Quantum Computer That Could Crack Most Types of Encryption. Steven Rich and Barton Gellman in Washington Post; January 2, 2014.