надо скрыть сообщение. Это Ева (Eavesdropper, «соглядатай» или «перехватчик») — она собирается перехватить сигнал и расшифровать его.

И вот Алиса формирует поток приготовленных фотонов, каждый из которых обладает заданным Алисой базисом и направлением колебаний. Боб их улавливает и оценивает. Просто наугад: вот у этого такой базис, а у того — такой. Затем Боб сообщает Алисе, какие базисы он использовал для каждого фотона, и Алиса подтверждает, какие из них были правильными, а какие — нет. Тогда Боб может отбросить данные по неправильным базисам и узнать, что ему прислали. Собственно сообщение будет состоять из нулей и единиц, которым соответствует направление колебаний по каждому базису: нулю соответствует 0 градусов на линейном базисе и 45 — на диагональном (вертикаль плюса или правая диагональ креста), а 90 и 135 градусов (перекладина плюса или левая диагональ креста) — единице.

Самое главное свойство фотона — то, что он меняется при попытке оценить его состояние. Поэтому если Ева-перехватчик подключилась к линии и попыталась считать сигнал, фотоны к Бобу придут другими. Причем неизвестно какими. Так что Боб в этом случае увидит вместо сигнала шум, о чем узнает от Алисы. Тогда это сообщение просто выбрасывается, и начинается новый цикл. Усилия Евы были напрасны.

«Математически получается, что 25% измененных битов — это свидетельство перехвата сигнала. На практике принято считать, что уже при 11% ключ скомпрометирован»,— рассказывает Юрий. И тогда все начинается заново. Сама передача занимает доли секунды, ведь фотоны движутся со скоростью света. Самое главное, что так передается не само закодированное сообщение, а ключи для его расшифровки. Секретная информация идет по открытому каналу, как когда-то Центр передавал Штирлицу шифровки по радио. Но только наличие ключа позволяет превратить набор сигналов в осмысленное сообщение. И именно этот ключ и передается с помощью квантового шифрования. Если ключ слишком короткий, то закодированное сообщение под угрозой. Так как квантовая криптография является постоянным источником ключа, становится возможно сделать ключ, равный по длине передаваемому сообщению. В этом случае, как доказали математики, сообщение невозможно взломать даже с помощью сколь угодно быстрого квантового компьютера.

Но если Ева оказалась упорной и перехватывает все передаваемые ключи? Боб просто узнает об этом, но не получит правильный код. То есть он никогда не расшифрует сообщение? Послушаем Юрия Курочкина: «Сообщение передается только после получения правильного ключа. Если все ключи перехватываются, то они, во-первых, тут же становятся недействительными, во-вторых, сообщение не передается. А значит, сам факт перехвата просто теряет смысл».

Так свойство фотона помогает выполнить не просто передачу зашифрованной информации, но и обеспечить контроль за ее защищенностью: скопированный ключ становится непригодным. Как плохая копия денежной купюры, сделанная на цветном принтере: вроде бы все на ней как на настоящей, только все видят, что это копия.

БЫСТРО И ЕЩЕ БЫСТРЕЕ Получают фотоны с помощью лазера — собственно, лазерный луч это и есть поток фотонов, удобный для обработки. Только лазер выдает целый пучок фотонов, а надо выбрать отдельный фотон и работать с каждым из них. Это и делает лабораторная установка, на которой отрабатываются технологии. Здесь испытывают детекторы, схемы управления, которые создают в соседней лаборатории. Поэтому она такая большая: надо иметь возможность оперативно менять расположение устройств. Здесь можно вспомнить

ЮРИЙ МАРТЬЯНОВ

МОДУЛИ КВАНТОВОГО ШИФРОВАНИЯ УМЕЩАЮТСЯ В СТАНДАРТНУЮ 19-ДЮЙМОВУЮ СТОЙКУ, ИСПОЛЬЗУЕМУЮ ДЛЯ КОМПЬЮТЕРНОГО ОБОРУДОВАНИЯ

про настольные компьютеры и смартфоны: они могут иметь сопоставимую производительность, но размеры и масса настольного компьютера компенсируются возможностью менять его конструкцию. Модули квантового шифрования, которые используются на практике, гораздо меньше: они умещаются в стандартную 19-дюймовую стойку. Да, квантовая криптография уже реализуется на практике. Но не в России.

«Эта технология уже не фантастика. Швейцарская компания ID Quantique уже предлагает коммерческие решения в области квантовой криптографии. Есть наработки в КНР и, конечно, в США,— рассказывает Юрий Курочкин о конкурентах.— Мы начали работать в феврале. России нужны собственные технологии, потому что все связанное с секретностью должно проходить под контролем государства». Кстати, ID Quantique в 2013 году получила $4,5 млн (по другим данным — $5,6 млн) от фонда QWave Capital. В числе основателей этого фонда — Сергей Белоусов, создатель и глава известной российской компании Parallels. Фонд гордится своими связями со многими выходцами из СССР и участием в развитии советской научной школы.

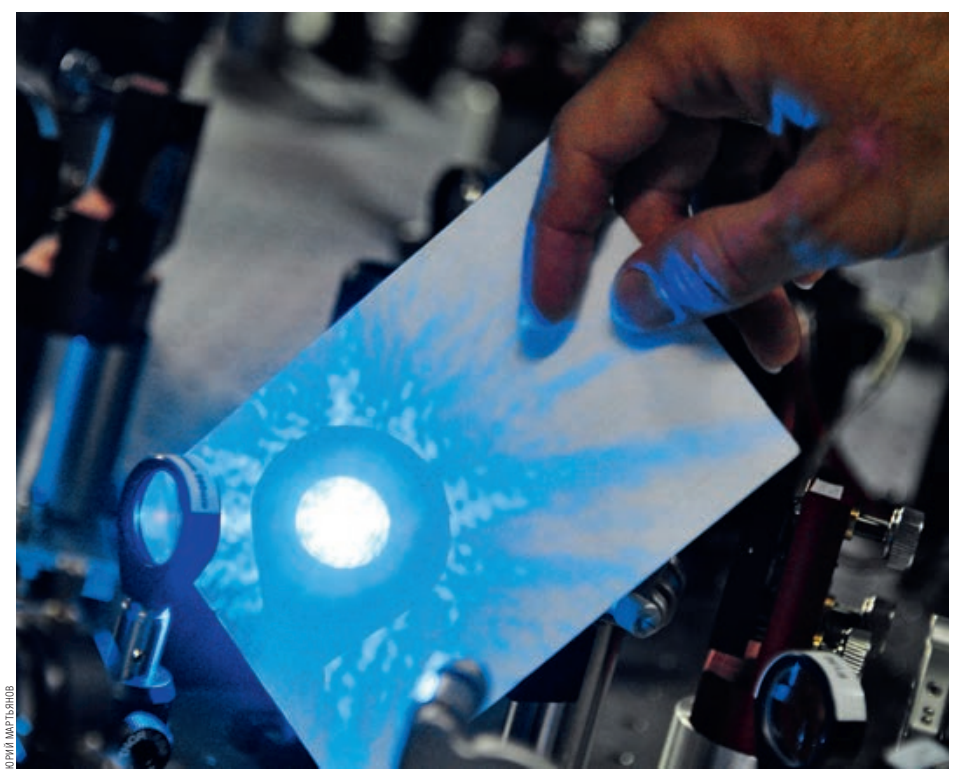
Группа, которой руководит Юрий Курочкин, должна в течение двух лет пройти путь от появления первых лабораторных образцов до их прикладного применения. Общая задача всех разработчиков в области квантовой криптографии — повышение скорости генерации ключа. Чем она выше, тем более длинные ключи и в большем количестве можно производить в единицу времени и тем надежнее будет передача. Сейчас это единицы килобайтов, цель — довести до сотен и выйти на передовые позиции в мире.

СВЕТ СО СПУТНИКА Другая критически важная проблема — дистанция, на которую можно передавать ключ. Оптико-волоконные линии давно уже реальность, и лазеры в коммуникациях уже используются. Но здесь речь об отдельных фотонах, каждый из которых должен от передатчика Алисы добраться до детектора Боба, а в оптико-волоконных линиях тоже есть потери. «Сейчас можно обеспечить передачу одиночных фотонов на 50–100 км. На больших дистанциях для нормальной работы надо уже охлаждать детекторы, чтобы добиться эффекта сверхпроводимости,— говорит Юрий.— В обычных линиях стоят усилители, но усиление тоже вмешательство, оно скомпрометирует код». Так что дальняя связь с квантовым шифрованием будет как дальние поездки в былые времена с ямщиками, когда на каждой станции меняли лошадей — только здесь на каждом пункте надо заново формировать ключ и снова передавать его.

Можно использовать «однофотонную связь» и на дальних расстояниях, например через спутник. Однофотонный сигнал со спутника удалось зарегистрировать на Земле еще в 2008 году. А теперь Китай наметил на 2016 год первые сеансы космической связи с квантовым шифрованием.

На первых порах все это, конечно, будет использоваться прежде всего для государственных нужд. Однако любая технология в конечном итоге находит коммерческое использование, и в надежной передаче конфиденциальной информации заинтересованы многие организации. В первую очередь банки и другие финансовые учреждения. «Лет через 15–20 какие-то зачатки искусственного интеллекта будут у многих бытовых приборов,— рассуждает Юрий.— И все они будут обмениваться информацией, значительная часть которой будет конфиденциальной. Наличные деньги довольно скоро могут почти исчезнуть из повседневной жизни». Все это будет генерировать огромные объемы обмена данных. Причем их перехват, а тем более подмена создадут огромные проблемы. И сохранить стабильность работы наших систем информации смогут неподкупные фотоны. ■

РОССИИ НУЖНЫ СОБСТВЕННЫЕ ТЕХНОЛОГИИ, ПОТОМУ ЧТО ВСЕ СВЯЗАННОЕ С СЕКРЕТНОСТЬЮ ДОЛЖНО ПРОХОДИТЬ ПОД КОНТРОЛЕМ ГОСУДАРСТВА



ЮРИЙ МАРТЬЯНОВ

ИСТОЧНИК ФОТОНОВ — ЛАЗЕР. НО ОН ЯВЛЯЕТСЯ ПУЧКОМ ФОТОНОВ, А ДЛЯ КРИПТОГРАФИЧЕСКИХ ЗАДАЧ НУЖНО БРАТЬ ЭТИ ЧАСТИЦЫ ПО ОДНОЙ