ЧТО СКРЫВАЕТ СВЕТ

КВАНТОВЫЕ КОМПЬЮТЕРЫ — ЭТО НЕДАЛЕКОЕ БУДУЩЕЕ: ИХ ПОЯВЛЕНИЕ ПРОИЗВЕДЕТ РЕВОЛЮЦИЮ В ОБЛАСТИ ШИФРОВАНИЯ ДАННЫХ, ВЕДЬ КВАНТОВЫЙ КОМПЬЮТЕР МОЖЕТ ВЗЛОМАТЬ ПРАКТИЧЕСКИ ЛЮБОЙ ИСПОЛЬЗУЕМЫЙ СЕЙЧАС АЛГОРИТМ КОДИРОВАНИЯ. НО В РОССИЙСКОМ КВАНТОВОМ ЦЕНТРЕ УЖЕ РАБОТАЮТ НАД НОВОЙ КРИПТОГРАФИЧЕСКОЙ ТЕХНОЛОГИЕЙ, КОТОРАЯ УСТОЙЧИВА ДАЖЕ ПЕРЕД КВАНТОВЫМИ КОМПЬЮТЕРАМИ, ЕЩЕ НЕ ПОЯВИВШИМИСЯ НА СВЕТ. ВАЛЕРИЙ ЧУСОВ

ЩИТ ПРОТИВ БУДУЩЕГО МЕЧА

В темной комнате на большом столе расставлены линзы, линзочки, зеркала, которые занимают почти весь стол. Это лабораторная модель квантового криптографического устройства. Через все эти оптические устройства идет лазерный луч, по пути преобразуясь и перенося информацию. Юрий Курочкин, руководитель группы квантовых коммуникаций Российского квантового центра, показывает нам, что установка работает, подставляя в некоторых местах лист бумаги, на котором появляется светящаяся точка — это и есть лазерный луч. Он очень слабый и не может прожечь бумагу. Но пытается. Когда Юрий увлекается разговором, на листе появляется темная точка. Квантовая криптография, как и множество других высоких технологий, такой же луч: пока ее воздействие на жизнь незаметно, но надо только немного подождать.

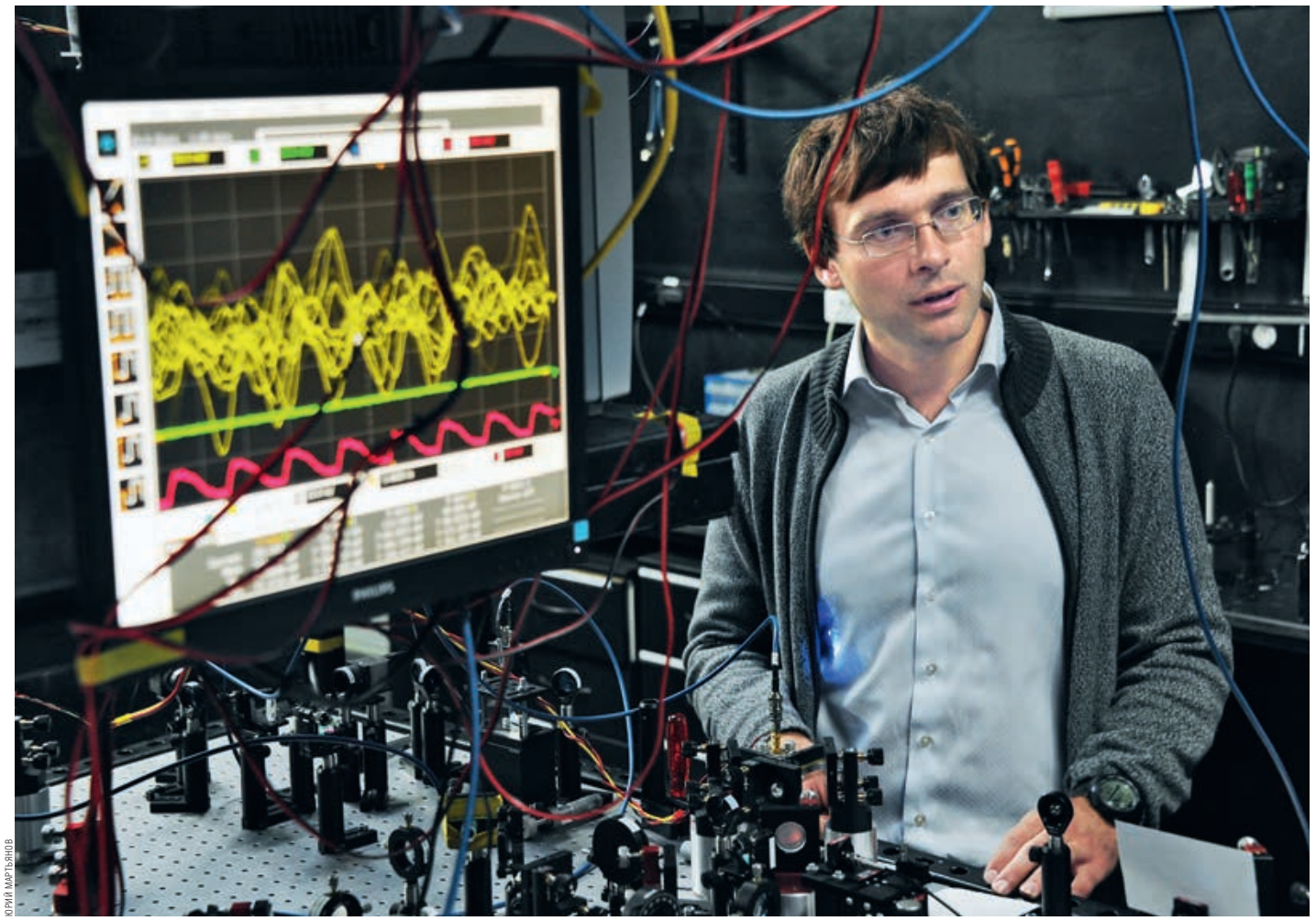
Мир вокруг нас переполнен тайнами. Речь не о тех, которые раскрыли Эдвард Сноуден или Мордехай Вануну, и даже не о местонахождении заначки Петра Петровича, которую он скрывает от своей жены Екатерины Семеновны. В современном мире любой из нас постоянно имеет дело с защищенной информацией: шифруются данные о банковских счетах, стоят пароли к почтовым ящикам и аккаунтам в социальных сетях, кодируются передаваемые в разнообразных системах связи сообщения. Криптография давно уже занимается не только перепиской государственных деятелей и передачей армейских приказов — тайны и секреты есть у всех. Безопасность не бывает лишней, убеждены специалисты, так что спрос на средства шифрования есть всегда, как и на средства дешифровки. Вечное противостояние щита и меча совершенствует и щит, и меч.

В большинстве случаев сегодня шифрование данных обеспечивает вычислительная техника, то есть компьютерные технологии. Чем сложнее шифрование, тем более защищенной считается информация. Теоретически взломать можно любой код, но для этого потребуются либо большие вычислительные мощности, либо много времени. Например, чтобы получить доступ к банковскому счету при существующих алгоритмах вычислений и отсутствии вспомогательных данных, потребуется время, превышающее возраст Вселенной. Но уже разработана теория квантового компьютера, который за счет принципиальных отличий от классического компьютера способен решать такие задачи гораздо быстрее. Правда, самих квантовых компьютеров пока нет — их создание считается фундаментальной задачей физики XXI века, которая еще не решена. Зато уже есть средства для создания шифра, который не может быть взломан квантовым компьютером. Это и есть квантовая криптография.

ВСЕ МЕНЬШЕ И МЕНЬШЕ

«Впечатляющие отличия жизни сегодняшнего обывателя от жизни его предка 100 лет назад связаны с квантовыми технологиями, например полупроводниками,— так начал рассказ о своей работе Юрий Курочкин, руководитель группы квантовых коммуникаций Российского квантового центра.—

ТЕОРЕТИЧЕСКИ ВЗЛОМАТЬ МОЖНО ЛЮБОЙ КОД, НО ДЛЯ ЭТОГО ПОТРЕБУЮТСЯ ЛИБО БОЛЬШИЕ ВЫЧИСЛИТЕЛЬНЫЕ МОЩНОСТИ, ЛИБО МНОГО ВРЕМЕНИ



ЮРИЙ МАРТЬЯНОВ

ЮРИЙ КУРОЧКИН, РУКОВОДИТЕЛЬ ГРУППЫ КВАНТОВЫХ КОММУНИКАЦИЙ РОССИЙСКОГО КВАНТОВОГО ЦЕНТРА, СЧИТАЕТ, ЧТО МИР СТОИТ НА ПОРОГЕ НОВОЙ КВАНТОВОЙ РЕВОЛЮЦИИ. И ГОТОВ В ЭТОЙ РЕВОЛЮЦИИ ПРИНЯТЬ НЕПОСРЕДСТВЕННОЕ УЧАСТИЕ

Первая квантовая революция произошла, когда человечество научилось использовать квантовые свойства макроскопических объектов и появился транзистор». Вот как — оказывается, жить в эпоху революций бывает вполне спокойно и комфортно. Мы встретились в Сколково, где работает Российский квантовый центр. Антураж совсем не напоминает лаборатории из классических фильмов «Весна» или «Девять дней одного года», да и в современном кино ученые работают в гораздо более впечатляющей обстановке. Здесь же для теории доска с маркерами, для экспериментов — темная комната с большим лабораторным столом и лазером, для создания экспериментальных образцов — скромная лаборатория, где самое заметное оборудование — лампа с огромной линзой.

«Сейчас ожидается появление технологий, которые позволят человеку научиться управлять квантовыми свойствами отдельных частиц»,— продолжает Юрий. Квантовая механика изучает взаимодействие на уровне молекул, атомов, ионов и фотонов. Миниатюризация техники все же подразумевает объекты, которые состоят из большого количества частиц или их потоков. Например, вся микроэлектроника работает с током, то есть движением электронов, и что происходит с отдельным электроном — совсем не важно. Можно сравнить с водопроводом: напор воды в кране возникает потому, что где-то работают насосы или давит столб в водонапорной башне. При этом когда «наша» вода прошла через те насосы, совершенно не важно — достаточно существующего давления. Квантовые технологии основаны на использовании отдельных фотонов, которые одновременно являются и частицей, и волной. Это и есть квант света.

ВМЕСТО ПРОЧТЕНИЯ СЖЕЧЬ

Сегодня в оптико-волоконных линиях также используются потоки фотонов. Но из потока можно незаметно «изъять» некоторое количество фотонов и таким образом получить доступ к информации. И получатель об этом не узнает. А вот с отдельным фотоном этот номер не пройдет.

Фотону можно придать различные состояния. Всем знакомы поляризационные очки в 3D-кинотеатре — их действие основано на том, что световые волны могут колебаться в разных направлениях. У фотона, который одновременно и частица, и волна, тоже может быть поляризация. Для простоты принято выделять два варианта поляризации, или базиса,— линейный и диагональный. Их обозначают плюсом и косым крестом. И в рамках каждого базиса два направления колебаний — угол поляризации 0 и 90 градусов для линейного и 45 или 135 градусов для диагонального. Оптические устройства могут отфильтровать фотоны с нужными характеристиками.

Для объяснения физик Курочкин рисует на доске схему: точку передачи называют Алисой, приемник — Бобом, как в обычной школьной задаче, здесь сигнал передается из точки «А» в точку «Б». Поскольку мы говорим о криптографии, у нас есть и третий участник, от которого нам