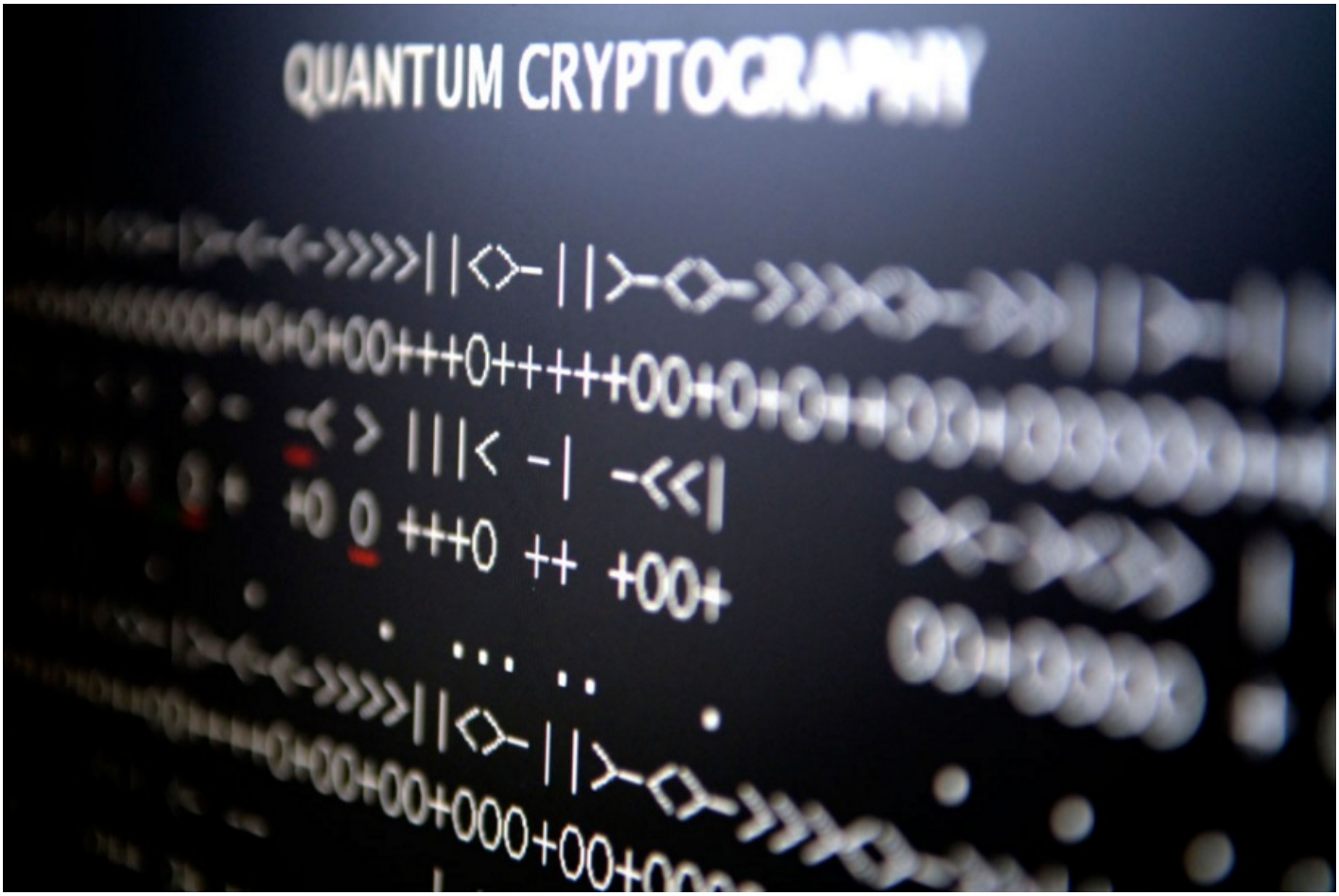
Шифрованный фотон



Развитие квантовых технологий, а также появление первых квантовых компьютеров, возможности которых в недалеком будущем будут в разы выше, чем возможности современных вычислительных машин, может кардинально изменить положение вещей в IT-отрасли и телекоммуникациях. Как отмечают специалисты, от квантовых вычислений исходит угроза безопасности при передаче и хранении данных. Поскольку скорость вычисления квантовых компьютеров значительно выше, чем у современных вычислительных устройств, то им не составит труда преодолеть все современные алгоритмы шифрования. В таком случае жизненно важной становится разработка новых методов защиты данных. Единственным вариантом становятся методы шифрования, основанные на квантовых технологиях, а именно - квантовая криптография.



Например, в Google решили не сидеть в ожидании создания квантового компьютера такой мощности, что он сможет с легкостью взламывать все современные средства шифрования, а опередить события и начать уже сейчас работать с методами пост-квантового шифрования. Приятно, что такая прозорливость характерна не только для иностранных корпораций. В России также запустили первую городскую линию связи с квантовой криптографией. Создателем проекта выступил Российский квантовый центр (РКЦ), а экспериментировать с новым видом связи вызвался "Газпромбанк". Длина оптоволокна по которому будут передавать данные, составит около 30 километров.

[Шифрованный фотон]

Современные достижения на ниве квантовой связи пока не позволяют передавать большие объемы информации на большие расстояния, поэтому по экспериментальной линии будут передаваться лишь ключи шифрования, необходимые для расшифровки сообщений, передаваемых между отделами банка. Несмотря на большие минусы, у передачи данных методом квантового шифрования есть существенное преимущество перед остальными: это самый надежный метод шифрования на сегодняшний день.

Проект "Газпромбанка".

К развитию квантовой криптографии подталкивают громкие скандалы последних лет, связанные с хищением данных, "прослушкой" и взломом конфиденциальных переписок, в том числе и первых лиц государства. Несмотря на то, что методы шифрования применяются повсеместно (едва ли не каждый мессенджер применяет алгоритмы шифрования сообщений), гарантий надежной защиты данных, передаваемых по каналам связи, предоставить не может никто.

Как отмечают эксперты РКЦ, есть множество факторов, опираясь на которые можно с уверенностью утверждать, что современные методы криптографии уже не дают стопроцентной защиты. К примеру, купить прибор для взлома оптоволоконной линии - не проблема. Его цена в сети крутится возле отметки в 200$. Также, в сети много инструкций, которые тщательно разъясняют, как найти волокно под землей и как его взломать.

Видео о том, как найти линию связи, информацию с которой нужно считать.

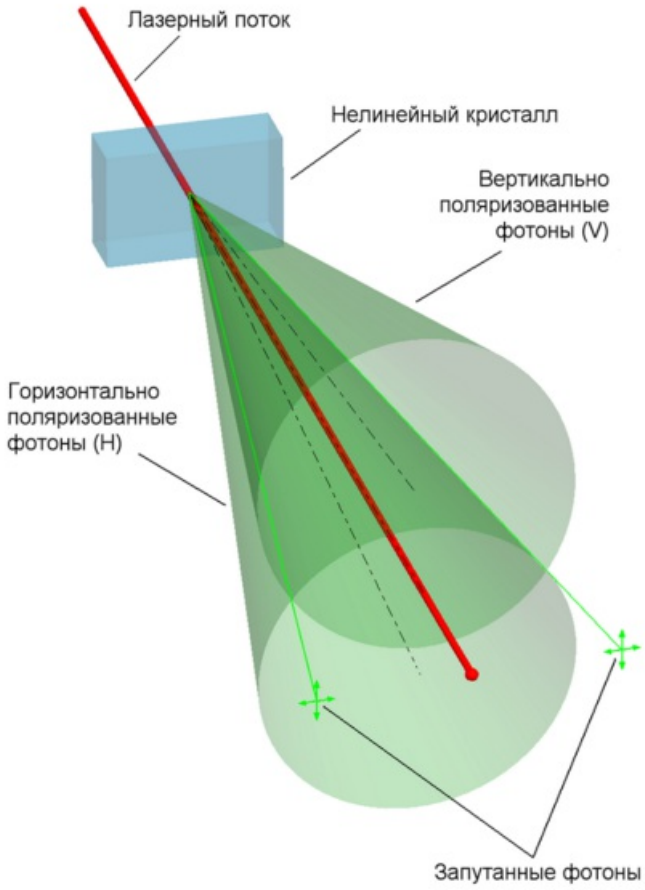
Видео как "взломать" оптоволокно.

Плюс ко всему, появление и усовершенствование квантового компьютера, в ближайшей перспективе может привести к обесцениванию современных алгоритмов шифрования. Именно этого, кстати,

опасается "Гугл".

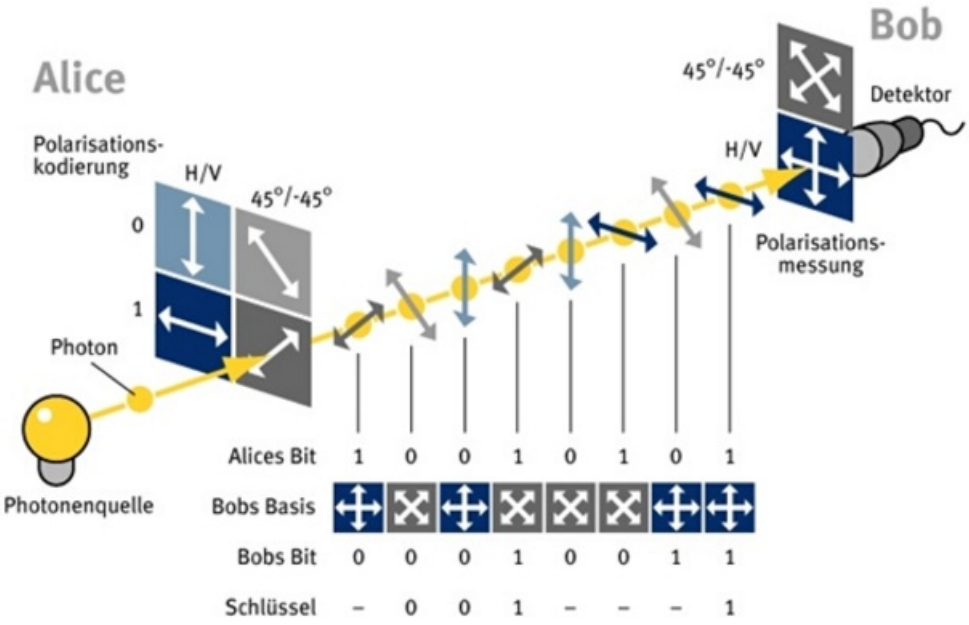
Немного истории

Современная система криптографии основана на математических методах шифрования. Квантовая же криптография предлагает обратиться к законам физики. В основу метода легла, так называемая, теория "квантовой запутанности". Согласно ей невозможно измерить какой-либо из параметров фотона, не исказив другой. Практическое применение этого физического явления позволяет смоделировать систему связи, прослушивание которой можно будет легко обнаружить, поскольку любая попытка перехватить сигнал приведет к его изменению, которое легко обнаруживается.



Генерация квантового состояния

Впервые о возможности защиты передаваемой информации с помощью постулатов квантовой физики, заговорили почти пятьдесят лет назад. Идея была предложена Стивеном Визнером, а спустя десятилетие её подхватили Чарльз Беннет из IBM и Жиль Брассар из Монреальского университета. Эти предприимчивые ребята предложили передавать секретный ключ, используя квантовые объекты. В 1984 ими была предложена схема создания канала передачи данных с помощью квантовых состояний.



На схеме пользователи Алиса и Боб обмениваются информацией в виде фотонов, а злоумышленник Ева пытается эти данные перехватить. Однако сделать это без искажения передаваемых данных у нее не получается. То есть, легальные пользователи проверяют и сравнивают сигналы, устанавливая не было ли попытки перехвата. В этом случае Боб сверял сигнал, отправленный Алисой, после чего переводил его в биты. Если ошибки не выявлялись, то информацию можно было считать случайно распределенной - то есть, случайной и секретной.



Сохранность передаваемой информации напрямую зависит от интенсивности вспышек света, которые применяют для передачи сигнала. Слабые вспышки приводят к массе ошибок у принимающей стороны. Высокая интенсивность световых вспышек наоборот позволяет избежать погрешностей принимающей стороне, но и облегчает задачу перехватчику сигнала. При этом, легальные пользователи путем анализа ошибок могут узнать какая часть информации попала к злоумышленнику.

Впервые же передать информацию с помощью квантовой криптографии попробовали пять лет спустя. Все те же Беннет и Брассар разработали квантовый канал, с передающим аппаратом Алисы и принимающим аппаратом Боба. Оборудование располагалось на оптической скамье длиной всего лишь один метр - в светонепроницаемом полутораметровом кожухе размером 0,5 × 0,5 м.



Так выглядит оптическая скамья

Собственно, квантовый канал представлял собой свободный воздушный канал длиной около 32 см. Макет управлялся от персонального компьютера, который содержал программное представление пользователей Алисы и Боба, а также злоумышленника. В том же году передача сообщения посредством потока фотонов через воздушную среду на расстояние 32 см с компьютера на компьютер завершилась успешно. Основная проблема при увеличении расстояния между приёмником и передатчиком — сохранение поляризации фотонов. Решение именно этой проблемы сможет стать качественным скачком в развитии квантовой связи в целом.

Проблемы и минусы

Главный минус, тормозящий широкое распространение квантовой криптографии, это невозможность распространения сигнала на дальние дистанции без его существенных изменений. Классическая передача сигнала по оптоволокну происходит с помощью лазерного света, который затухает с прохождением больших расстояний. В квантовой передаче данных используется минимальное количество фотонов, но чтобы избежать затухания при дальних расстояниях, на участках линии используют усилители сигнала, которые заряжают его дополнительными фотонами. Для квантовой связи важны именно отдельные фотоны и их квантовые состояния, поэтому умножение числа фотонов неблагоприятно скажется на сигнале. Максимальная дальность передачи данных по оптоволокну с помощью квантовой криптографии, которую пока что смогли достичь ученые, составила около 150 километров. Такие дальние расстояния позволяют передавать информацию лишь со скоростью около 10 бит в секунду, а на дистанции порядка пятидесяти километров, скорость составляет примерно 10 кбит в секунду, что, безусловно, слишком мало при нынешних массивах данных, передаваемых по сетям.

Реализация на практике

Как пояснили корреспонденту NAG.ru в Российском квантовом центре, в настоящее время уже доступны несколько способов реализации квантовой передачи данных. Наибольшее распространение получила передача по волоконно-оптическим линиям. Это характеризуется тем, что в мире проложено достаточно большое количество оптического кабеля, который долгое время не используется и вряд ли будет применяться в ближайшие годы. Такие оптические волокна называют "темным волокном" - они отлично подходят для тестирования метода передачи данных квантовым шифрованием.

Впервые коммерческая система квантовой криптографии была презентована в Швейцарии в 2002 году. Инженеры из швейцарской компании GAP-Optique создали компактное устройство, которое подключалось к персональному компьютеру. В результате эксперимента была установлена связь по оптоволокну между Женевой и Лузанной. Сигнал создавался лазером, а скорость передачи составила не более 117,6 кбит/с.



Несмотря на то, что в настоящее время технология квантовой криптографии по большей части применяется в экспериментальных проектах с прицелом на будущее, и это скорее технология на перспективу - квантовое шифрование уже было опробовано в ряде серьезных проектов. Например, информационное обслуживание Чемпионата мира по футболу в 2010 году.

В 2011 году в Токио прошла демонстрация проекта "Tokyo QKD Network", в ходе которого тестировалось квантовое шифрование телекоммуникационных сетей. Была проведена пробная телеконференция на расстоянии в 45 км. Связь в системе обеспечивалась обычными оптоволоконными линиями.

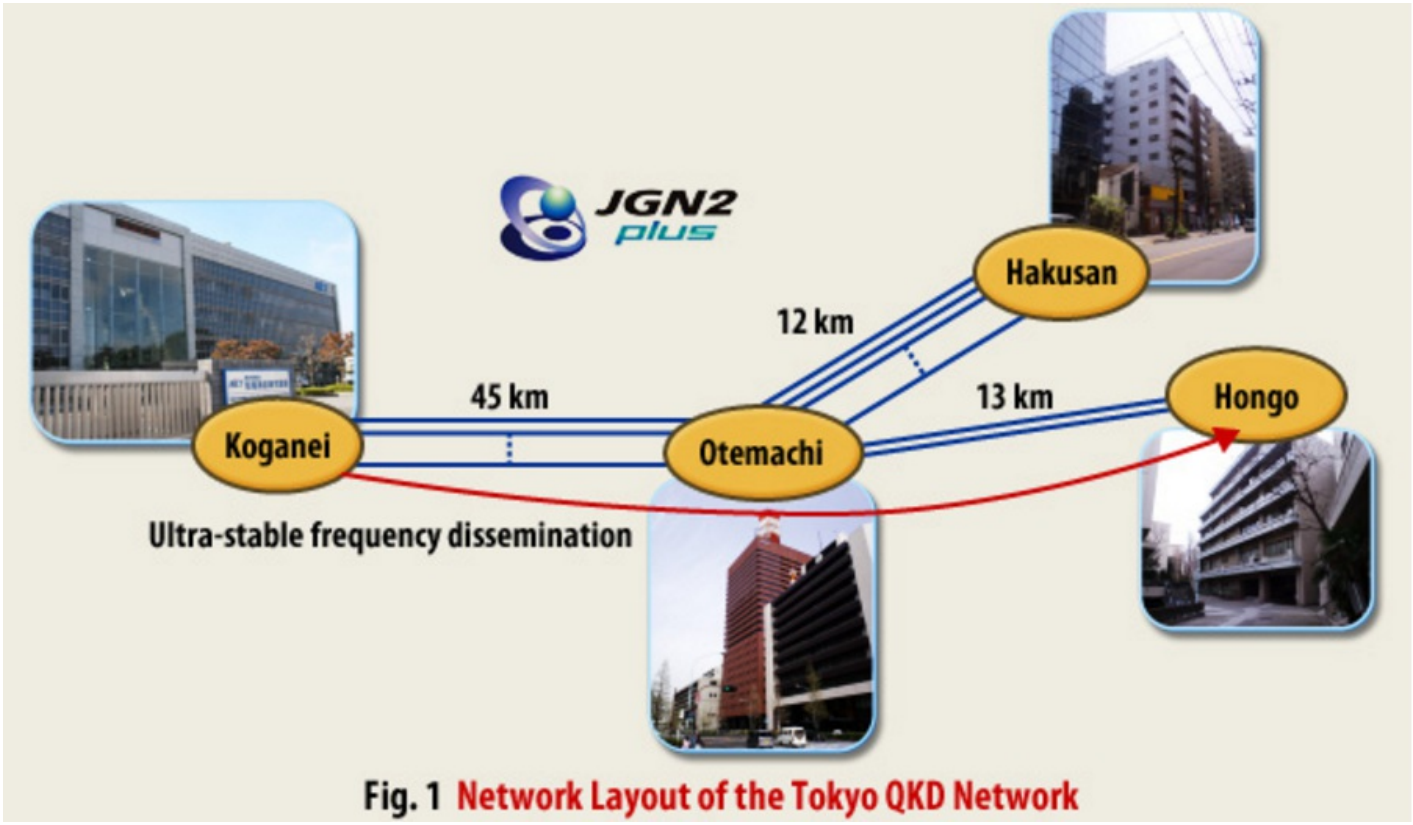
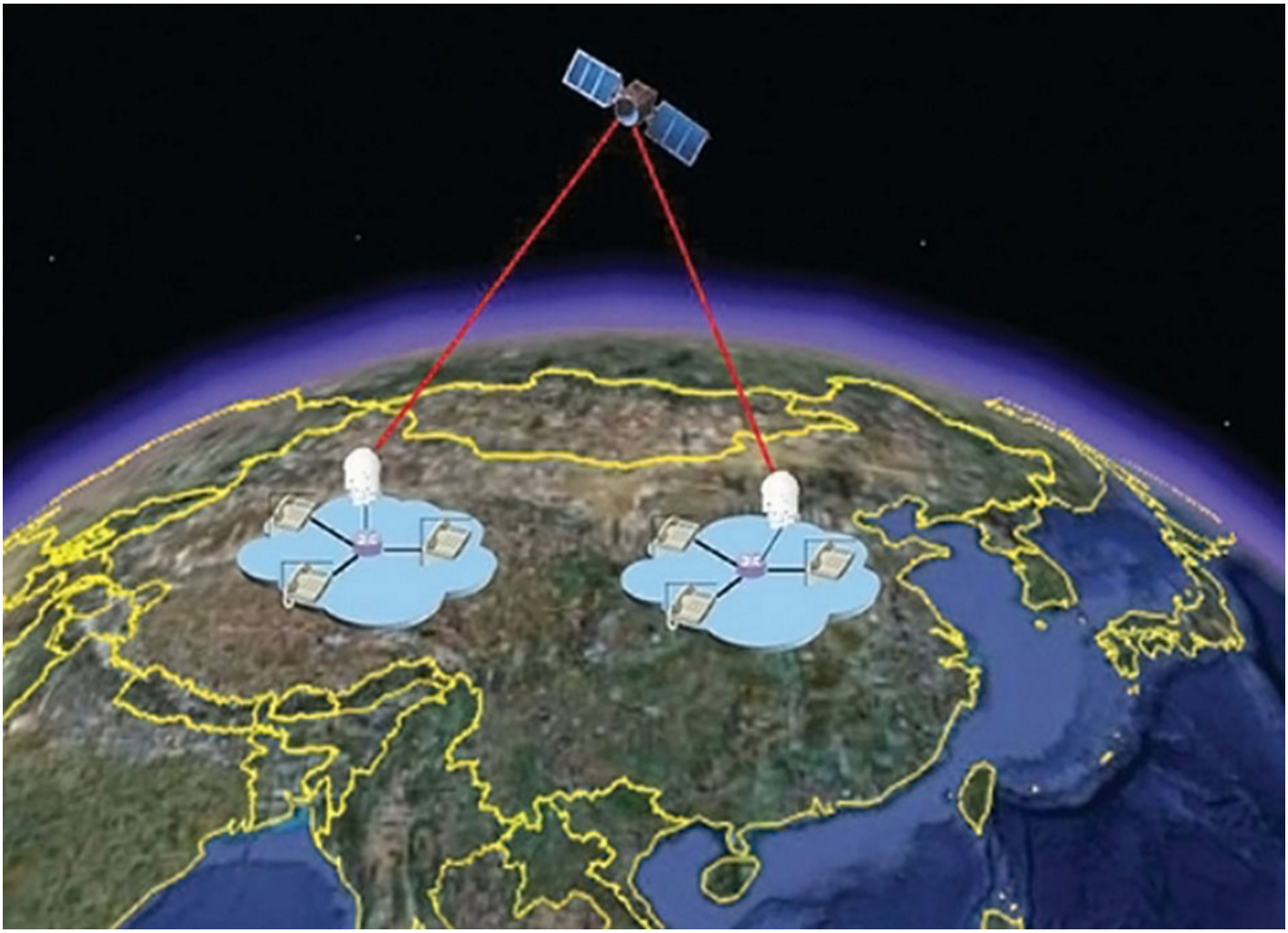


Fig. 1 Network Layout of the Tokyo QKD Network

Сейчас самые масштабные проекты по построении мощных квантовых сетей реализуются в США и Китае. Причем, в Поднебесной похоже увидели реальную перспективу квантовой криптографии, потому как именно там в последние месяцы появляется большая часть разработок в этой области. Например, сеть квантовых коммуникаций, которая должна соединить между собой Пекин и Шанхай протянется на 1000 километров. Кроме того в Поднебесной уже готовятся запустить в небо спутник

квантовой связи, который станет своего рода началом для построения "квантового космического интернета".



В этом случае речь идет уже не только о квантовой криптографии, а еще и о возможности достигнуть значительно больших скоростей передачи данных с помощью квантовой телепортации. Планируется, что на спутнике будет располагаться кристалл, который будет генерировать и запускать пары "запутанных" фотонов и отправлять их на принимающие станции в Китае и Австрии. Таким образом, ученые смогут узнать, получится ли оставить связь между запутанными фотонами при их передаче на 1200 километров. Если эксперимент удастся, то эта технология станет мощным толчком к развитию квантового интернета.

Коммерческий сектор

Масштабные эксперименты, проводимые учеными с государственной поддержкой это, безусловно, хорошо, но настоящим толчком для развития той или иной технологии является её коммерческий успех. За прошедшие годы к разработкам в квантовой криптографии подключились такие гиганты, как Toshiba, NEC, IBM, Hewlett Packard, Mitsubishi, NTT . Но наряду с ними стали появляться на рынке и маленькие, но высокотехнологичные компании: MagiQ , Id Quantique , Smart Quantum. Разработки этих компаний имеют полноценную коммерческую составляющую. Например, Id Quantique предлагает массу решений для коммерческого сектора. На сайте компании довольно широкий список различного оборудования для генерации ключей шифрования и созданий состояния квантовой запутанности фотонов. Именно эта швейцарская компания была создателем первого генератора случайных чисел для ключей, с помощью которых осуществляется квантовое шифрование.



Генератор ключей шифрования

Швейцарцы предлагают потенциальным покупателям целую линейку разнообразного оборудования как для построения новых сетей квантового шифрования, так и для встраивания шифровального оборудования в собственные сети.

В России разработки в квантовой криптографии пока не так успешны, как за границей, однако и отечественные ученые уделяют этому вопросу немало времени. О линии квантовой передачи данных, построенной для "Газпромбанка" Российским квантовым центром мы уже упоминали выше. В РКЦ отмечают, что их собственные разработки в течение нескольких лет уже должны выйти на массовый рынок.

Перспективы

Как отмечают в РКЦ, рынок квантового шифрования показывает стабильный рост и к 2018 году будет опережать по этому показателю рынок аппаратного шифрования более чем на 10%.



По словам специалистов, в перспективе создание квантовых каналов с уплотнением по длине волны; повышение скорости формирования ключей. В скором времени протяженность квантовых каналов связи достигнет устойчивых 100 километров, а расширение областей практического внедрения значительно увеличится. Причем, уже в ближайшие пять лет квантовой криптографии предсказывают интеграцию с существующими телекоммуникационными сетями, а также с сетями 5G. Близится появление спутниковых квантовых сетей, а также облачных технологий на основе кванта. Квантовой криптографии не страшно появление полноценного квантового компьютера, а наоборот его появление лишь даст огромный толчок для развития технологии. А постоянно растущее количество потенциальных киберугроз, делает технологию квантовой передачи данных как никогда востребованной во всем мире.