Безопасность квантовой криптографии.

В теории, так называемая квантовая криптография обеспечивает полностью безопасный способ передачи информации. На практике, возможно нет. Но теперь физики продемонстрировали, как закрыть технологические лазейки, которые могут оставить секреты открытыми для наблюдателей.

Предположим, Алиса хочет послать Бобу секретное сообщение. В обычной криптографии, она может преобразовывать сообщение в двоичные числа, то есть строку из 0 и 1, а затем объединить математически с другой случайной строкой из 0 и 1, которая служит в качестве ключа. Затем Боб использует этот ключ, чтобы отменить скремблирование и прочитать сообщение. Конечно, чтобы сделать схему работающей, Алиса должна передать ключ Бобу, не давая ему возможности быть перехваченным оператором перехвата сообщений, Евой.

Квантовая криптография представляет переворот в буквальном смысле. Алиса передает Бобу ключ кодирования его одиночных фотонов, которые могут быть поляризованы горизонтально, чтобы сигнализировать 0 или вертикально, чтобы сигнализировать 1.Если бы это было все, что было с ним, то потом Ева перехватчик также может считать ключ, а затем передать Бобу фотоны. Но Алиса может также случайно вращать ее передатчик для отправки фотонов поляризованного по диагонали на плюс или минус 45 ° какого-то времени. Когда ее передатчик не совпадает с приемником Боба, ключ передачи становится неоднозначным: Например, если Алиса посылает фотон, поляризованный под углом 45 °, а у Боба есть свой детектор, который установлен в горизонтальной или вертикальной ориентации. Тогда, в соответствии с правилами квантовой механики, Боб будет регистрировать горизонтальную или вертикальную с вероятностью 50%. Это не проблема, так как после передачи потока фотонов, Алиса и Боб могут сказать друг другу, для каких фотонов их устройства были приведены в соответствие, и использовать только фотоны определяющие ключ.

Все это скручивание закрывает доступ к информации Еве. Ева не знает, какие ориентации Алиса и Боб используют, и, если она угадает неверно, она будет нарушать фотоны путем измерения. Например, предположим, что для конкретного фотона Алиса и Боб установили свои аппараты в горизонтально - вертикальной ориентации. Но Ева имеет аппарат с ориентацией 45 °. Тогда, согласно квантовой механике, ее измерение фотона будет изменять его состояние и оставит его поляризованным плюс или минус 45 °. Это будет

разрушить абсолютное совпадение, что Алиса и Боб должны увидеть. Позже, когда они сверят часы, они заметят ошибки и осознают, что кто-то вмешался в передачу.

Тем не менее, в 2010 году, международная команда исследователей показала, что Ева могла взломать систему, используя слабости в так называемых лавинных фотодиодах (ЛФД), которые используются для обнаружения отдельных фотонов. Проблема в том, что ЛФД не одинаково реагируют на интенсивные импульсы света и на одиночные фотоны, так что энергия импульса должна превышать порог для регистрации. В результате, все что должна сделать Ева, это перехватить одиночные фотоны, сделать наиболее предполагаемые измерения их поляризации, и отправить ее ответы от Боба как новые, более яркие импульсы. Если она угадала и с ее аппарата фотоны измеряли в той же ориентации, что и у Алисы и Боба, то аппарат Боба будет интерпретировать яркий импульс как один фотон. Но, если она не угадала, и послала Бобу яркий импульс, но поляризация не соответствовала ориентации его аппарата, то аппарат Боба будет разбивать его на два тусклых импульса. Ни один из них не будет достаточно сильным, чтобы сработали детекторы Боба. Так Боб никогда не заметил бы, что Ева испортила поляризации фотонов. И, так или иначе, он не заметит потери импульсов от Алисы к Бобу из-за неэффективности детектора.

В прошлом году физик Хой-Квонг Lo в Университете Торонто и коллеги утверждали, что нашли способ обойти эту проблему. В новом протоколе Алиса и Боб начнут создание квантового ключа, отправив случайно поляризованные сигналы Чарли, третьей стороне. Чарли будет измерять сигналы, чтобы определить, не их фактические поляризации, но только сдвиг фаз. Были ли сигналы поляризованы под прямым углом. Например, если Алиса послала сигнал вертикальной поляризации, и Боб также послал сигнал вертикальной, Чарли ответит отрицательно. Но если Алиса послала сигнал вертикальной поляризации, и Боб послал сигнал горизонтальной поляризации, Чарли ответит "да". Как только Боб услышал "да", он просто покрутит сигнал на 90 °, чтобы сделать его таким же, как и у Алисы. Так формируется квантовый ключ. Хитрость тут в том, что Чарли просто сравнивает поляризации фотонов, не определяя, какие они есть. Так что не может быть никакого расщепления фотонов и сигналов вполсилы. В результате, подделка Евы не могла бы пройти незамеченной. Даже если бы она заглянула через плечо Чарли, она бы знала только не были ли соотнесены сигналы Алисы и Боба, и никогда бы не знала их фактических значений.

Ло и его коллеги только что представили свою идею. Теперь, в статьях опубликованных в *журнале* Physical Review Letters, две независимые группы физиков показали, что новый протокол работает. Вольфганг Титтель и его коллеги из Университета Калгари в Канаде размещали детектор Чарли в Калгари в главном кампусе, а генератор сигнала Боба в лаборатории в 6 километрах, и генератор сигнала Алисы - в другой лаборатории в 12 километрах. Хотя исследователи не имели генерации случайных сигналов у Алисы и Боба, как требуется в по-настоящему безопасной криптографии, они показывают, что синхронизация сигнала и измерений может быть выполнена на таких и больших расстояниях. Между тем, Цзянь-Вэй Пан в Университете науки и технологии Китая в Хэфэй и коллеги продемонстрировали протокол квантовой криптографии со случайными сигналами , хотя и только в лаборатории.

Означает ли это, что квантовая криптография является безопасной? Грегуар Ribordy, генеральный директор швейцарской компании Quantique ID, создающей коммерческую квантовую криптографию, говорит, что практические системы уже в значительной степени получили возможность непрерывного управления детекторами, чтобы они всегда по-разному взаимодействовали со входящими фотонами. Такие контрмеры затрудняют попытки Евы помешать безопасности, поскольку она должна была бы непрерывно посылать сильной световой сигнал. Но Ribordy добавляет, что демонстрацию нового протокола Титтелем и другими можно только приветствовать при разработке будущих систем. Короткий ответ гласит, что это очень интересно, хотя еще не созрело для реализации, с практической точки зрения. http://news.sciencemag.org/physics/2013/08/quantum-cryptography-safe-again