КВАНТОВЫЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Жукевич А.Ф., Колесова Т.Р.

Бойправ О.В. – м.т.н., ассистент

Письма по электронной почте, конфиденциальная информация, персональные данные – секреты, которые нужно знать только некоторым лицам, особенно в политике, экономике или банковской сфере. Но, если их узнал посторонний, это может стать роковой ошибкой. Риск есть всегда, даже если информация зашифрована. Однако скоро это может остаться в прошлом. Все спецслужбы, политики и просто важные люди будут в восторге и в тоже время в полном разочаровании. Во-первых, будет невозможно украсть передаваемые секретные данные, во-вторых, это преимущество будет доступно и другим спецслужбам, что полностью исключает возможность кражи данных.

В квантовом мире ключ не может быть украден не замечено и никому не под силу взломать квантовый ключ, т.к. он был сгенерирован не математическим алгоритмом, а самой настоящей случайностью.

Носителями информации в квантовой криптографии являются фотоны, поляризованные под углами 0, 45, 90, 135 градусов. В соответствии с законами квантовой физики, с помощью измерения можно различить лишь два ортогональных состояния: если известно, что фотон поляризован либо вертикально, либо горизонтально, то путем измерения, можно установить — как именно; то же самое можно утверждать относительно поляризации под углами 45 и 135 градусов. Однако с достоверностью отличить вертикально поляризованный фотон от фотона, поляризованного под углом 45 градусов, невозможно.

Эти особенности поведения квантовых объектов легли в основу протокола квантового распространения ключа. Чтобы обменяться ключом, отправитель и получатель предпринимают следующие действия:

Отправитель посылает получателю фотон в одном из поляризованных состояний (0, 45, 90, 135 градусов) и записывает угол поляризации. Отсчет углов ведется от направления "вертикально вверх" по часовой стрелке. Получатель располагает двумя анализаторами: один распознает вертикально-горизонтальную поляризацию, другой — диагональную. Для каждого фотона получатель случайно выбирает один из анализаторов и записывает тип анализатора и результат измерений. По общедоступному каналу связи получатель сообщает отправителю, какие анализаторы использовались, но не сообщает, какие результаты были получены. Отправитель по общедоступному каналу связи сообщает получателю, какие анализаторы он выбрал правильно. Те фотоны, для которых получатель неверно выбрал анализатор, отбрасываются.

Последовательность фотонов Алисы	|	/	/	—	\	|	|	—	—
Последовательность анализаторов Боба	+	x	+	+	x	x	x	+	x
Результаты измерений Боба	0	0	1	1	1	0	1	1	0
Анализаторы выбраны верно	+	+		+	+			+	
Ключ	0	0		1	1			1	

Условные обозначения:

Поляризация фотонов: *| - вертикальная, — - горизонтальная, / - под угром 45, \ - под углом 135.*

Анализаторы: *+ - прямоугольный, x - диагональный*

Значения разрядов ключа получаются следующим образом: в случае вертикально-горизонтальной ("прямоугольной") поляризации вертикально-поляризованный фотон означает 0, горизонтально-поляризованный — 1; в случае диагональной поляризации фотон, поляризованный под углом 45 градусов -- 0, 135 градусов -- 1.

Рисунок 1 – Пример шифрования по протоколу BB84

Злоумышленник может попытаться перехватить ключ в ходе передачи потока квантов, но тогда они делятся надвое и уже не передают существенно важной информации. При подобном перехвате данных сразу станет заметным, что кто-то пытается их украсть. И даже если хакер попытается украсть само письмо в бинарном коде, у него все равно ничего не выйдет, ведь сам ключ был сгенерирован настоящей случайностью.

А это означает, что ученые нашли способ сгенерировать не взламываемый код, с которым можно быть на 100 процентов уверенными, что ваше письмо точно не будет украдено. Однако, чтобы использовать такую передачу данным по всему миру, понадобиться создать полноценную инфраструктуру.

Квантовые ключи могут быть переданы через оптоволокно на расстояние до 200 км, и сейчас некоторые банки уже используют эту функцию, а если расстояние слишком большое, то сигнал будет слабее и этот метод уже бездейственен. Для передачи данных на большие расстояния, эта система может работать исключительно через систему спутников.

Сделать специальное оборудование для спутника не самая сложная задача, но до них квантовым состояниям придется преодолеть очень большое расстояние. Главными проблемами на пути передачи фотонов являются два фактора: солнечный свет и турбулентность.

Ученым удалось передать квантовые состояния по воздуху в дневное время суток, с помощью лазерных вспышек. Сигнальные лазерные вспышки и их световые волны являются носителями сигналов, они крепко держатся против дневного света, таким образом ученые сохраняют требуемый квантовый сигнал.

Остается только одна проблема: турбулентность. Передаче квантовых состояний по воздуху могут мешать деревья, здания, горячие дроги.

Ученые открыли, что для поляризации турбулентность не играет никакой роли, это направление вибрации электрического поля электромагнитной волны. Когда свет распространяется в одну сторону, то он может это делать по горизонтальным направлениям или вертикальным, эти два вида движения света не искривляются при встрече с турбулентностью. Благодаря этому, ученым удалось передать лазерную вспышку на расстояние 1,6 км.

Проводятся эксперименты с геостационарными спутниками, если эти эксперименты пройдут успешно, то квантовая коммуникация станет для нас повседневностью, а хакерам придется из-за этого очень нелегко.

Список использованных источников:

Е. А. Павельева, А. С. Крылов, Поиск и анализ ключевых точек радужной оболочки глаза методом преобразования Эрмита, Информ. и ее примен., 2010, том 4, выпуск 1, 79–82

Е.А. Павельева, А.С. Крылов, Алгоритм сравнения изображений радужной оболочки глаза на основе ключевых точек, Информатика и ее применения, 2011. Т.5. Вып. 1 С. 68-72 -