Квантовая криптография. Идея квантового повторителя.

Козлов Роман Николаевич
Офицер ГШ ВС РФ, Россия, г, Москва

Аннотация

В данной статье проанализирован классический способ квантовой криптографии с помощью поляризации фотона, обозначены фундаментальные законы квантовой механики в части касающейся защиты информации в пределах изучения задачи. Дано направление решения проблемы потери данных в квантовых сетях.

Введение

Криптографические методы издавна и до сегодняшнего дня считаются надежным способом защиты информации при ее передачи по незащищенным каналам связи. В последнее время актуальным стало новое направление в криптографии – квантовая криптография. Квантовая криптография – метод защиты коммуникаций, основанный на определенных явлениях квантовой физики. В отличие от традиционной криптографии, которая использует математические методы, чтобы обеспечить секретность информации, квантовая криптография сосредоточена на физике информации, так как рассматривает случаи, когда информация переносится с помощью квантов. Процесс отправки и приема информации всегда выполняется физическими средствами, например, при помощи электронов в электрическом ток, или фотонов в линиях волоконно-оптической связи. А подслушивание может рассматриваться, как измерение определенных параметров физических обьектов – в нашем случае, переносчиков информации. Технология квантовой криптографии опирается на принципиальную неопределенность поведения квантовой системы – невозможно одновременно получить координаты и импульс частицы, невозможно измерить один параметр фотона, не исказив другой. Это фундаментальное свойство природы в физике стало известно как принцип неопределенности Гейзенберга, сформулированный в 1927 г.

Постановка и решение задачи

Простейшим алгоритмом генерации секретного ключа является алгоритм BB84, схема его работает следующим образом:

Вначале отправитель (А) производит генерацию фотонов со случайной поляризацией, выбранной из 0, 45, 90 и 135°. Получатель (Б) принимает эти фотоны, затем для каждого выбирает случайным образом способ измерения поляризации, диагональный или перпендикулярный. Затем по открытому каналу сообщает о том, какой способ он выбрал для каждого фотона, не раскрывая при этом самих результатов измерения. После этого А по тому же открытому каналу сообщает, правильный ли был выбран вид измерений для каждого фотона. Далее А и Б отбрасывают те случаи, когда измерения Ба были неверны. Если не было перехвата квантового канала, то секретной информацией или ключом и будут оставшиеся виды поляризации. На выходе будет последовательность битов: фотоны с горизонтальной или 45°-й поляризацией принимаются за двоичный «0», а с вертикальной или 135°-й поляризацией — за двоичную «1». Этот этап работы квантово-криптографической системы называется первичной квантовой передачей.

Следующим этапом очень важно оценить попытки перехватить информацию в квантово-криптографическом канале связи. Это производится по открытому каналу А и Б путем сравнения и отбрасывания подмножеств полученных данных случайно ими выбранных. Если после такого сравнения будет выявлен перехват, то А и Б должны будут отбросить все свои данные и начать повторное выполнение первичной квантовой передачи. В противном случае они оставляют прежнюю поляризацию. Согласно принципу неопределённости, криптоаналитик (Е) не может измерить как

диагональную, так и прямоугольную поляризацию одного и того же фотона. Даже если им будет произведено измерение для какого-либо фотона и затем этот же фотон будет переслан Б, то в итоге количество ошибок намного увеличится, и это станет заметно А. Это приведет к тому, что А и Б будут полностью уверены в состоявшемся перехвате фотонов. Если расхождений нет, то биты, использованные для сравнения, отбрасываются, ключ принимается. С вероятностью $1 — 2^{-k}$ (где k — число сравненных битов) канал не прослушивался.

Квантовый повторитель

Одной из основных проблем повсеместного использования данной системы криптографии состоит в крайне малых расстояниях возможных для передачи фотонов без их критических потерь в волоконно-оптических сетях, по которым и передаются фотоны, к сожалению данные сети не идеальны и какое-то количество света теряется (фотон – квант света), что естественным образом ведет к потере информации. При этом если в других сетях мы имеем возможность использовать усилители сигнала, то в сетях где передаются фотоны у нас такой возможности нет, потому что такой усилитель никак нельзя отличить от шпиона, то есть отсутствует возможность определить данный усилитель как установленный нами или шпионом. Перспективным способом передачи фотона без его потери является идея квантового повторителя суть которого основана на квантовой телепортации, то есть вместо того, чтобы посылать фотон от одного партнера другому приготавливается переплетенное состояние между двумя партнерами и далее фотон приводится во взаимодействие с одним из элементов данного переплетенного состояния и по средствам явления квантовой нелокальности второй элемент переплетенного состояния переходит в состояние равное первоначальному состоянию фотона.

Заключение

Тем самым используя квантовые явления, можно спроектировать и создать такую систему связи, которая всегда может обнаружить подслушивание. Это обеспечивается тем, что попытка измерения взаимосвязанных параметров в квантовой системе вносит в нее нарушения, разрушая исходные сигналы, а значит, по уровню шума в канале легитимные пользователи могут распознать степень активности перехватчика.

Литература

1. Семенов Ю.А. «Телекоммуникационные технологии»;
2. Килин С.Я. «Квантовая информация/Успехи Физических Наук.» - 1999 г.;
3. Robert Malaney . «Технологии, основанные на принципе ULV (unconditional location verification)»;