УДК 621.391.7

ЗАЩИТА ПРОТОКОЛА КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧА ШИФРОВАНИЯ BB84 ОТ АТАК РАЗДЕЛЕНИЯ ЧИСЛА ФОТОНОВ

Толстов И. К. (Университет ИТМО)
Научный руководитель – к.т.н., доцент Кузнецов А. Ю.
(Университет ИТМО)

В докладе будут представлены результаты аналитического обзора уязвимостей протокола квантового распределения ключа шифрования BB84. А также будет предложна математически и физически обоснованная методика противодействия выявленным угрозам.

Квантовое распределение ключа в теории позволяет реализовать симметричный алгоритм шифрования с абсолютной криптографической стойкостью. Классический протокол квантовой криптографии BB84 наиболее прост и дешев в реализации, а также технологически его внедрение возможно уже сегодня в системы, где необходимо сверхнадежное, быстрое симметричное шифрование потоковых пакетных данных, например, в канале видеосвязи. Однако применение многофотонных импульсов, вследствие невозможности реализации однофотонного источника, приводит к уязвимости протокола — возможности разделения числа фотонов в импульсе. На сегодняшний день однофотонные источники реализованы только в лабораторных условиях, а опыт зарубежных компаний показывает, что разработки, с одной стороны, ведутся с упором на протокол E91, использующий в своей основе свойства запутанных квантовых частиц, однако технология генерации таких частиц дорогостоящая, а область малоизученная. С другой стороны, компании, к примеру Toshiba, фокусируются на увеличении расстояния беспроводного распределения ключа, не занимаясь вопросом о безопасности передаваемых сигналов. Российские опытные разработки используют модификации протокола BB84, закрывая уязвимости повышением контроля за целостностью квантового канала связи.

Таким образом, цель работы повысить защищенность протокола квантового распределения ключа шифрования. Основная задача состоит в разработке методики защиты протокола BB84.

Решение позволяет защитить протокол квантового распределения ключа BB84 (и его модификации) от атак, нацеленных на разделение числа фотонов в импульсе. Суть метода заключается в регистрации плотности потока энергии излученных импульсов отправителем и получателем, что позволяет удостовериться, действительно ли принятый импульс излучен отправителем. Реализация при этом предполагает использование для формирования и измерения квантовых состояний фотонов поляризаторы, основанные на эффекте двулучепреломления в кристалле. А также появляется необходимость использования сверхчувствительных лавинных фотодиодов и системы, перенаправляющей импульсы.

В алгоритм протокола вносятся следующие изменения. После прохождения через двулучепреломляющий поляризатор отправителя случайно выбранный луч кодирует логический бит и направляется получателю, а второй луч отражается отправителем на фотодиод для расчета плотности энергетического потока исходного импульса. При получении импульса принимающая сторона, пропустив импульс через поляризатор случайного базиса, также перенаправляет луч на фотодиод. На этапе отправки последовательности использованных базисов также прилагаются данные о измеренных на фотодиоде параметрах. Отправитель, основываясь на физические законы изменения плотности потока энергии при поляризации и с учетом потерь в квантовом канале, вычисляет исходную плотность энергетического потока импульсов, полученных и измеренных получателем. Из плотности энергетического потока возможно вычислить количество излученных в импульсе фотонов с заданной точностью. Так как количество фотонов в импульсе является случайной величиной,

то она способна однозначно идентифицировать принадлежность импульса к источнику света и временному промежутку. Таким образом, возможно определить был ли импульс разделен или ретранслирован.

Решение позволяет внедрять классический протокол квантовой криптографии BB84 с защитой от уязвимости разделения числа фотонов. Внедрение этого протокола оправдано, так как его реализация технически возможна, экспериментально проверена и экономически выгодна для систем, требующих абсолютной криптографической стойкости, быстродействия алгоритма шифрования и передачи потоковых пакетных данных. Примером может быть распределенная киберфизическая система видеонаблюдения с интерфейсом компьютерного зрения для банкоматов или режимных объектов.