процента. Это подтверждает правомерность использования предлагаемого алгоритма генерации случайных чисел по закону Пуассона.

В качестве параметра фотоприемного модуля использовалась его квантовая эффективность, характеризующая вероятность преобразования оптического сигнала в электрический. Данный параметр, наряду с шумовыми свойствами фотоприемной аппаратуры, является одним из определяющих эффективность всей системы связи.

При моделировании квантового канала связи учитывались потери оптического излучения связанные с поглощением и рассеянием излучения. Так же, моделировалась ситуация наличия в канале перехватывающего агента. При этом исследовались две ситуации:

1) Перехват и генерация злоумышленником всех фотонов за длительность оптического импульса. Данная ситуация позволяет моделировать реальные системы связи.

2) Отбор только одного фотона за длительность импульса. Эта ситуация позволяет оценивать эффективность протокола квантовой криптографии при наличии злоумышленника с идеальной аппаратурой, позволяющей осуществлять несанкционированный съем.

Таким образом, проведенные исследования позволили оценить эффективность протокола квантовой криптографии BB84 при использовании поляризационной модуляции.

Список литературы

1. Радиоэлектронные технологии информационной безопасности: Сборник научных статей / Под. ред. К.Е. Румянцева. – Таганрог: ТРТУ, 2002. – С. 145-155.

АНАЛИЗ МЕТОДОВ ФОРМИРОВАНИЯ КЛЮЧЕВОЙ ПОСЛЕДОВАТЕЛЬНОСТИ В МНОГОПОЛЬЗОВАТЕЛЬСКИХ КВАНТОВЫХ КОМПЬЮТЕРНЫХ СЕТЯХ

Хайров И.Е., Румянцев К.Е.,
Новиков В.В., Троцюк Е.В.
Таганрогский государственный радиотехнический университет, Таганрог

Бурное развитие в последние годы квантовых компьютеров и связанных с ними технологий привело к появлению ряда революционных достижений, способных значительно ускорить научно-технический прогресс. К таким достижениям относится квантовая криптография.

Генерация ключа методами квантовой криптографии осуществляется непосредственно в процессе передачи единичных фотонов по каналу связи. Надежность этих методов базируется на незыблемости фундаментальных законов квантовой физики.

Квантово-криптографические системы первоначально использовались для связи отдельных пар пользователей. Однако актуальным является разработка и исследование подобных методов для связи большого количества пользователей. Работа в данном направлении активно ведется как зарубежными, так и отечественными научными центрами.

Как показали исследования известные методы распределения секретного ключа используют либо древовидную топологию сети, либо кольцевую с необходимостью использования дополнительных каналов обмена информацией. В частности методы квантовой криптографии могут использоваться при построении пассивной оптической сети, содержащей центральный сетевой контроллер, связанный посредством пассивного оптического светоделителя с множеством сетевых пользователей. В этой схеме используется квантовое поведение оптического светоделителя. Соответственно каждый пользователь будет обеспечен уникальным произвольно выбранным подмножеством битов.

Другая квантово-криптографическая система содержит квантовый канал связи с множеством узлов, включающих передающий и приемный модули, связанные с квантовым каналом связи. Передающий модуль генерирует световой сигнал, представляющий собой последовательность фотонов, для распределения через квантовый канал. Получатель сообщения принимает световой сигнал, посланный передатчиком и измеряет квантовые состояния этого сигнала. Данный метод организации оптической сети использует кольцевую топологию, однако основным ее достоинством является то, что каждый из пользователей может быть инициатором обмена данными.

В связи с этим, актуальной является проблема разработки метода распределения секретного ключа между большим количеством последовательно расположенных пользователей без дополнительных каналов обмена информацией. В работе предложен новый метод организации оптической сети, в которой происходит распределение секретного ключа с использованием квантовой криптографии. Данный метод основан на принципе измерение–повторная отправка и применим в системах с модуляцией по поляризации.

Исследования так же показали, что при непосредственном использовании данного метода, процесс обмена характеризуется большим процентом ошибок. Однако, с введением в рассматриваемую сеть подсистемы синхронизации между поляризационными анализаторами пользователей, данный метод будет соответствовать протоколам, применяющимся для обмена данными между несколькими пользователями.

Данная оптическая сеть распределения секретного ключа методами квантовой криптографии может быть также отнесена к сети связи с кольцевой топологией.

Основной проблемой практической реализации подобной оптической сети, является обеспечение точной синхронизации поворотов поляризационных анализаторов большого количества последовательно расположенных пользователей. Так как вероятность прохождения поляризованного фотона через анализатор пропорциональна косинусу угла между направлением поляризации и осью анализатора, то неточность синхронизации может составлять единицы градусов.