И.Е. ХАЙРОВ (к.т.н., доцент), **К.Е. РУМЯНЦЕВ** (д.т.н., профессор), **А.А. ДЗЕЙКАЛО** (студент), **М.А. ЖУКОВ** (студент), **В.В. ПОЛЫВЯНАЯ** (студентка)
(Таганрогский государственный радиотехнический университет)

ОБЗОР ОСНОВНЫХ МЕТОДОВ ФОРМИРОВАНИЯ КВАНТОВО-КРИПТОГРАФИЧЕСКОГО КЛЮЧА, С КОДИРОВАНИЕМ ОДНОФОТОННЫХ ИМПУЛЬСОВ ПО ОТНОСИТЕЛЬНОЙ ФАЗЕ

В настоящее время для шифрования секретной информации широкое распространение получили криптографические методы, основанные на специальных секретных ключах.

Все современные криптографические системы делятся на симметричные и несимметричные. Симметричные или системы с секретным ключом представляют собой такие системы, в которых Алиса и Боб (принятые в научной литературе условные имена для передающей и принимающей сторон соответственно) владеют конфиденциальной информацией (например, ключом), которая не известна Еве (условное имя для обозначения подслушивающей стороны). Ключ применяется каждый раз для кодирования и декодирования передаваемой информации. В несимметричных системах или системах с открытым ключом используется два ключа. Один из них (публичный ключ) используется для шифрования, в то время как другой (секретный ключ), используется для дешифрования сообщений.

Бурное развитие квантовых технологий привело к появлению нового направления в криптографии - квантовой криптографии. 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.

Первоначально квантово-криптографические системы были предназначены для отдельных пар пользователей, но затем стали рассматривать и для большого количества людей. Для генерации секретного ключа было предложено достаточно большое количество протоколов. Однако наиболее распространенным является BB84.

В этом протоколе для передачи ключевой информации однофотонные импульсы кодируются по поляризации, либо по относительной фазе. Эти методы кодирования имеют как преимущества, так и недостатки.

Рассмотрим основные системы с фазовым кодированием.

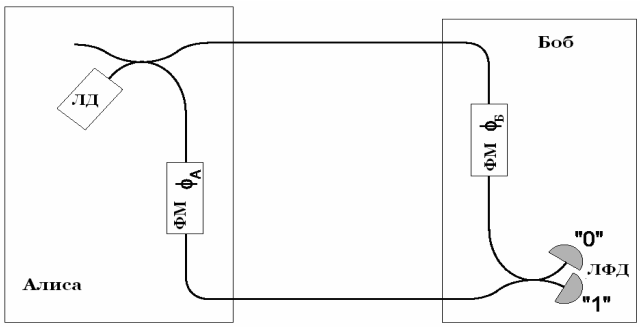

Рис. 1. Интерферометр Маха-Цендера (ЛД - лазерный диод, ФМ - фазовый модулятор, ЛФД - лавинный фотодиод).

Эти системы преимущественно используются для передачи информации по волоконно-оптическим линиям связи, где основным недостатком поляризационного кодирования является случайная деполяризация сигнала.

Главным звеном в системе с кодированием по фазе является интерферометр Маха-Цендера (рис.1), который выполнен из двух волоконно-оптических разветвителей, соединённых между собой, и двух фазовых модуляторов – по одному в каждом плече. В такую систему можно ввести свет, используя классический непрерывный источник, и

наблюдать наличие или отсутствие интерференционной картины на выходе. Данное устройство работает как оптический переключатель. Необходимо отметить, что крайне важным является сохранение постоянной и малой разности длин плеч для получения устойчивой интерференции.

Описанное выше поведение интерферометра справедливо и для одиночных фотонов. Вероятность зарегистрировать фотон на одном из выходов будет изменяться с изменением фазы.

В квантовой криптографии интерферометр используется вместе с однофотонным источником и детекторами, подсчитывающими фотоны. Установка Алисы содержит источник, первый разветвитель и первый фазовый модулятор, а установка Боба состоит из второго модулятора, разветвителя и детекторов (см. рис. 1.).

Данная схема прекрасно работает в лабораторных условиях на оптическом столе, но в случае, когда Алиса и Боб отделены друг от друга более чем на несколько метров из-за нестабильности плеч интерферометра приводит к дрейфу фазы, в результате чего возникают ошибки в передаваемом ключе. Для устранения этой проблемы в [1] предложено использовать два несбалансированных интерферометра Маха-Цендера, соединённых последовательно оптическим волокном (см. рис. 2).

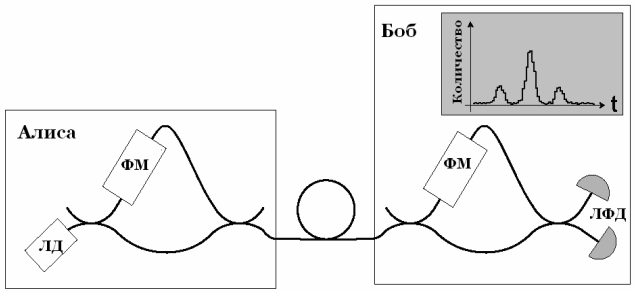

Рис. 2. Система для квантовой криптографии с двумя интерферометрами Маха-Цендера (ЛД - лазерный диод, ФМ - фазовый модулятор, ЛФД - лавинный фотодиод).

Данная система работает следующим образом. Регистрируя количество отсчётов во времени, Боб получает три пика. Первый пик соответствует случаям, когда фотоны прошли по коротким плечам в интерферометрах Алисы и Боба, третий – случаям, когда они прошли по длинным плечам. Наконец, центральный пик соответствует фотонам, прошедшим через короткое плечо у Алисы и через длинное у Боба и наоборот. Такие фотоны интерферируют между собой. Для того чтобы отделить проинтерферировавшие фотоны (то есть центральный пик) от остальных, используется временное "окно". Результат интерференции будет зависеть от состояния фазовых модуляторов Алисы и Боба.

Преимущество этой установки заключается в том, что обе "половинки" фотона проходят по одному и тому же волокну [2]. Следовательно, они проходят пути равной длины в той части системы, которая является наиболее чувствительной к изменениям состояния окружающей среды.

Помимо описанных выше систем, существует так же система Plug&Play. Благодаря этой системе существует возможность автоматически и в пассивном режиме компенсировать все поляризационные флуктуации в оптическом волокне [3]. В данной схеме импульсы, которые излучаются Бобом, могут проходить через короткое плечо у Боба, отражаться от зеркала Фарадея у Алисы и возвращаться уже через длинное плечо у Боба, либо наоборот – проходить через длинное плечо, отражаться и проходить через короткое на обратном пути. Эти два типа импульсов интерферируют на разветвителе. Лавинный же фотодиод расположен только в приемном модуле. Главным недостатком систем "Plug&Play" является уязвимость по отношению к атакам типа "Троянский конь".

Таким образом, в результате проведённой работы были проанализированы основные способы кодирования однофотонных импульсов, применяемые в квантово-

криптографических системах, рассмотрены их достоинства и недостатки. Выявлено, что для передачи информации по волоконно-оптическим линиям связи наиболее предпочтительным является кодирование по относительной фазе.

1. Charles H. Bennett et al. Experimental Quantum Cryptography, Journal of Cryptology, no. 5, 1992.

2. Wolfgang Tittel, Gregoire Ribordy and Nicolas Gisin. Quantum Cryptography, Physics World, March 1998.

3. Martinelli M., A universal compensator for polarization changes induced by birefringence on a retracting beam. Opt. Commun., 1989, vol. 72, pp. 341-344.