СИСТЕМА КВАНТОВОЙ КРИПТОГРАФИИ С ПОЛЯРИЗАЦИОННЫМ КОДИРОВАНИЕМ

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

Зеленин А.С.

Урядов В.Н. – к-т. техн. наук, доцент

В волоконно-оптических системах передачи под поляризацией понимают ориентацию световой волны, которая сразу же нарушается, как только свет входит в оптоволокно. В настоящее время применение новых типов оптоволокна, сохраняющего состояние поляризации, определяет перспективы дальнейшего развития ВОСП.

В существующих системах квантовой криптографии дисперсия поляризационных мод деполяризует фотоны. По этой причине практическая реализация подобных систем затруднялась, а поляризационное кодирование не представлялось лучшим выбором при построении волоконно-оптических систем квантовой криптографии.

Таким образом, нестабильные во времени изменения поляризации требуют создания механизма активной компенсации поляризационных изменений, что уже накладывает на систему криптографии серьёзные ограничения (рисунок 1).

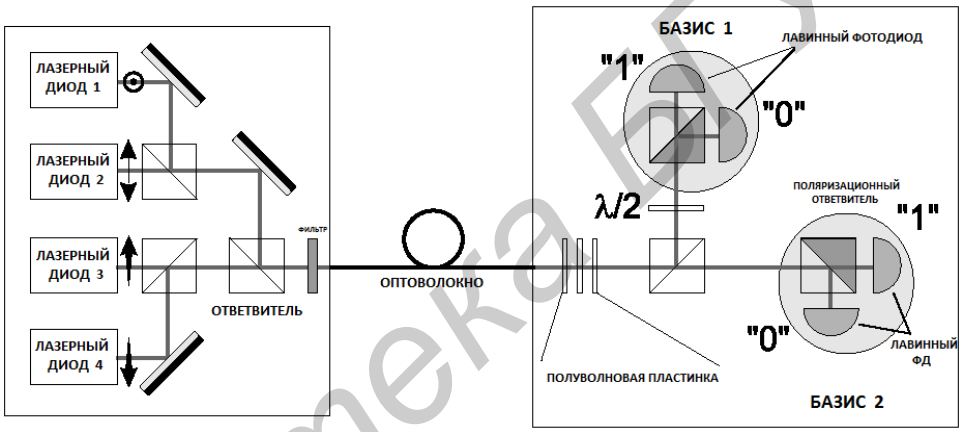

Рис. 1 – Структурная схема системы квантовой криптографии с механизмом компенсации поляризационных изменений

Импульсы при извлечении из волокна проходят через набор волновых пластинок, используемых для восстановления исходных поляризационных состояний путём компенсации трансформаций, внесённых волокном. Затем импульсы достигают ответвителя, осуществляющего выбор базиса. Переданные фотоны анализируются в базисе вертикальной/горизонтальной поляризации при помощи поляризационного ответвителя и двух счётчиков фотонов, далее фотоны анализируются вторым набором из поляризационного ответвителя и счётчиков фотонов.

Новое решение задачи о поляризационной балансировке лежит в области применения новых типов волокон с сохранением состояния поляризации и внедрения нового механизма компенсации (рисунок 2).

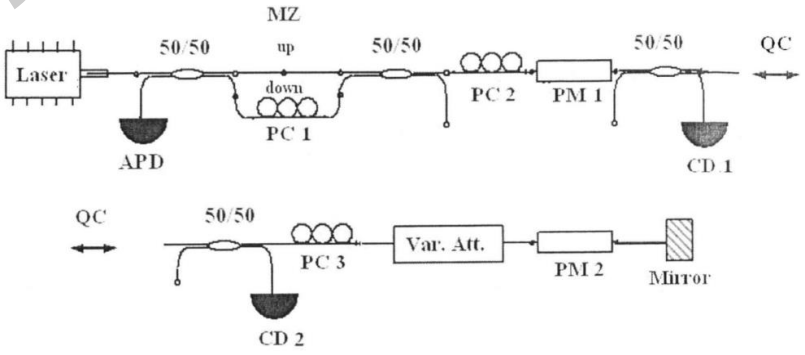

Рис. 2 – Структурная схема технического решения задачи о поляризационной балансировке

Сущность способа состоит в том, что для серии классических синхронизирующих лазерных импульсов на передающей-принимающей станции создают поляризационные состояния при помощи поляризационного контроллера в одном из плеч интерферометра и поляризационного контроллера на выходе интерферометра.

Они обеспечивают интерференционную балансировку интерферометра, серию однофотонных состояний после отражения от зеркала в преобразующей станции детектируют на передающей-принимающей станции и по полученной статистике фотоотсчетов вычисляют допустимую ошибку, которую затем сравнивают с определенным пороговым значением ошибки для получения известного только на передающей-принимающей и преобразующей станциях криптографического ключа.

В результате применения новых типов волокон с сохранением состояния поляризации, а также представленного механизма поляризационной балансировки расширяется диапазон возможных искажений поляризации лазерных и однофотонных импульсов при передаче ключей между передающей-принимающей и преобразующими станциями. Данное техническое решение, в свою очередь, даёт импульс к появлению нового поколения криптографических систем, призванного обеспечить конфиденциальность передаваемой информации, недостижимую для классических криптосистем.

Список использованных источников:

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

2. Nicolas Gisin, Gregoire Ribordy, Wolfgang Tittel, Hugo Zbinden. Quantum Cryptography, submitted to Reviews of Modern Physics, January 19, 2001.

3. Федеральный институт промышленной собственности: способ квантового кодирования и передачи криптографических ключей. [Электронный ресурс]. – Режим доступа: http://www1.fips.ru. – Дата доступа: 11.02.2016.