

УДК 535.8

РЕАЛИЗАЦИЯ АЛГОРИТМА КОМПЕНСАЦИИ ДРЕЙФА ПОЛЯРИЗАЦИИ В СИСТЕМЕ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧА НА НЕПРЕРЫВНЫХ ПЕРЕМЕННЫХ

Сулимов Д.В. (Университет ИМТО),
Геллерт М.Е. (Университет ИМТО)
Научный руководитель – Наседкин Б.А.
(Университет ИТМО)

Введение. Системы квантового распределения ключа (КРК) – это системы рассылки криптографического ключа между двумя пользователями, с помощью кодирования этого самого ключа в квантовых объектах. Изначальной версией КРК является квантовое распределение ключа на дискретных переменных, которое использует одиночные фотоны как основу для передачи информации (ключа). Другим подходом в реализации систем КРК является квантовое распределение ключа на непрерывных переменных, использующее гомодинные или гетеродинные детекторы, которые в свою очередь измеряют квадратуру сигнала, а не фотоны по отдельности.

Одной из существующих проблем систем КРК НП является необходимость компенсации поляризационного дрейфа, возникающего при распространении передаваемых сигналов по стандартному (не сохраняющему поляризацию) волоконно-оптическому каналу связи [1]. При передаче данных в системах КРК НП для восстановления исходного сигнала излучение разделяется на сигнальные импульсы, в которых содержится передаваемая информация и импульсы локального осциллятора, которые используются для гомодинного или гетеродинного детектирования. Поскольку интенсивности сигнальных импульсов и импульсов локального осциллятора отличаются на несколько порядков, возникает необходимость во временном и поляризационном мультиплексировании и демultipлексировании [2].

Основная часть. В работе рассмотрено устройство динамического контроля поляризации, а также алгоритм стохастического параллельного градиентного спуска [3]. На основе данного алгоритма реализован алгоритм компенсации дрейфа поляризации для системы КРК НП.

Выводы. Реализованный алгоритм позволяет компенсировать дрейф поляризации, который может негативно влиять на параметры системы КРК НП при поляризационном мультиплексировании и демultipлексировании внутри системы. Проведенный анализ влияния самого алгоритма на систему КРК НП, показал, что вносимый алгоритмом шум является незначительным и слабо влияет на параметры системы.

Список использованных источников.

1. Weedbrook C. et al. Quantum cryptography without switching //Physical review letters. – 2004. – Т. 93. – №. 17. – С. 170504. DOI: 10.1103/PhysRevLett.93.170504
2. Laudenbach F. et al. Continuous-variable quantum key distribution with Gaussian modulation—the theory of practical implementations //Advanced Quantum Technologies. – 2018. – Т. 1. – №. 1. – С. 1800011. DOI: 10.1002/qute.201800011
3. Grosshans F. et al. Quantum key distribution using gaussian-modulated coherent states //Nature. – 2003. – Т. 421. – №. 6920. – С. 238-241.