УДК 535.8

ПОЛЯРИЗАЦИОННАЯ МОДЕЛЬ СИСТЕМЫ КВАНТОВОГО РАСПРЕДЕНИЯ КЛЮЧА НА НЕПРЕРЫВНЫХ ПЕРЕМЕННЫХ

Сулимов Д.В. (Университет ИМТО)
Научный руководитель – Наседкин Б.А.
(Университет ИТМО)

В настоящем докладе представлена модель системы квантового распределения ключа на непрерывных переменных на основе матриц Мюллера, при помощи которых учитываются поляризационные искажения при распространении излучения. Описывается алгоритм поляризационного демультиплексирования для системы квантового распределения ключа на непрерывных переменных.

Введение. Системы квантового распределения ключа (КРК) – это системы распределения криптографического ключа между двумя пользователями, посредством кодирования информации в квантовых объектах. Более ранней версией КРК является квантовое распределение ключа на дискретных переменных, использующих одиночные фотоны как основу передачи ключа. Другой подход в реализации систем КРК стало квантовое распределение ключа на непрерывных переменных, использующее гомодинные или гетеродинные детекторы, которые в свою очередь измеряют квадратуру сигнала, а не конкретно единичные фотоны.
Одной из существующих проблем систем КРК на непрерывных переменных (НП) является необходимость компенсации поляризационных искажений, возникающих при распространении передаваемых сигналов по волоконно-оптическому каналу связи. 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 (ЛО), которые используются для реализации схемы гомодинного или гетеродинного детектирования. Поскольку интенсивности сигнальных импульсов и импульсов ЛО отличаются на несколько порядков, возникает необходимость во временном и поляризационном мультиплексировании и демультиплексировании.

Основная часть. В работе рассмотрена модель распространения излучения на основе матриц Мюллера, которые позволяют учитывать изменения поляризации излучения при распространении в канале связи. На основе полученной модели, были определены состояния поляризации, при которых будет обеспечиваться работоспособность системы КРК НП учитывая возможные потери при реализации поляризационного демультиплексирования. Это, в свою очередь, позволяет предъявить требования к алгоритму поляризационного демультиплексирования.

Выводы. Модель на основе матриц Мюллера позволяет сформулировать требования к алгоритму поляризационного демультиплексирования, который в дальнейшем будет реализован при помощи контроллера поляризации с обратной связью.

Исследование выполнено при финансовой поддержке гранта НИРМА ФТ МФ Университета ИТМО

Сулимов Д.В. (автор) Подпись

Наседкин Б.А. (научный руководитель) Подпись