

УДК 535.8, 535.015

ТЕОРЕТИЧЕСКИЙ АНАЛИЗ СИСТЕМ РАСПРЕДЕЛЕНИЯ КВАНТОВЫХ КЛЮЧЕЙ, НЕ ЗАВИСЯЩАЯ ОТ ИЗМЕРИТЕЛЬНЫХ УСТРОЙСТВ, ПРИ ИХ ИНТЕГРАЦИИ В ВОЛОКОННО-ОПТИЧЕСКИЕ ЛИНИИ СВЯЗИ С ПРИМЕНЕНИЕМ ТЕХНОЛОГИИ DWDM

Воронцова И.О. (Университет ИТМО), **Гончаров Р.К.** (Университет ИТМО), **Болычев Е.А.** (Университет ИТМО)

Научный руководитель – кандидат физико-математических наук, Киселев Ф.Д. (Университет ИТМО)

Методами численного моделирования проведено теоретическое исследование влияния шумов, вызванных спонтанным комбинационным рассеянием, четырехволновым смешением и линейными перекрестными помехами в канале на производительность систем КРК, не зависящих от измерительных устройств (MDI КРК) в случае их симметричной и асимметричных схем. Приведены математические модели системы MDI КРК, а также рассматриваемых канальных шумов. Для всех случаев определена скорость генерации секретного ключа для оценки и последующего анализа производительности систем, по результатам чего выявлены и изложены особенности работы системы MDI QKD в случае интеграции с существующими системами DWDM.

Введение. Направление квантовых коммуникаций, а в частности квантовое распределение ключей (КРК), показали и зарекомендовали себя как одну из наиболее активно развивающихся областей квантовых технологий. Технологии КРК делают возможным рассылать криптографически стойкий ключ между двумя и большим количеством аутентифицированных пользователей, которые соединены между собой квантовым и информационными каналами. Теоретически стойкость КРК к атакам со стороны злоумышленника продиктована принципами квантовой механики.

Тот факт, что сигнал, передаваемый по квантовому каналу, обладает значительно более низкими характерными значениями мощностей, долгое время был фактором, сдерживающим широкое применение технологий КРК. Использование так называемых темных волокон, то есть волокон, подразумевающих распространение только одного (в текущем контексте --- квантового) сигнала, нецелесообразно как с практической, так и с экономической точек зрения. Таким образом, необходима интеграция технологий мультиплексирования каналов, в частности плотного мультиплексирования с разделением по длине волны (DWDM), в системы КРК. Однако проявления нелинейных эффектов, которые возникают в оптическом волокне в присутствии мощного излучения, приводят к появлению канальных шумов, к основным из которых относят спонтанное комбинационное рассеяние (СКР), четырехволновое смешение (ЧВС), а также линейные перекрестные помехи (ЛПМ) классических информационных каналов.

В данной работе проведено численное моделирование влияния шумов, вызванных эффектами СПР, ЧВС и ЛПМ на производительность систем MDI КРК при их интеграции в ВОЛС DWDM. Произведен расчет скорости генерации стойкого ключа для упомянутых систем для различных схем расположения каналов (конфигураций). В результате обнаружены и сформулированы особенности и закономерности, характерные MDI КРК.

Основная часть. В работе предлагается производить расчет мощностей шумов, являющихся следствием СКР, ЧВС и ЛПМ, которые затем могут быть преобразованы в вероятности обнаружения фотона для использования в дальнейших расчетах скорости генерации секретного ключа MDI КРК. В работе описывается подход к выбору оптимальных конфигураций расположения квантового и информационных каналов на DWDM сетке, заключающийся в поиске ситуаций, характеризующихся наименьшим значением суммарных шумов, а следовательно – наибольшей дальностью функционирования системы. Для

полученных конфигураций проведено численное моделирование одновременного распространения квантового и информационных сигналов в одном оптическом волокне и дальнейший анализ полученных зависимостей для системы MDI КРК в ее симметричном и асимметричных случаях.

Выводы. С помощью методов численного моделирования исследовано влияние шумов СКР, ЧВС и ЛПМ на MDI КРК при интеграции с ВОЛС DWDM для оптимальных конфигураций – схем расположения квантового и информационных каналов на сетке DWDM. Подтвержден вывод о том, что оптимальным для систем MDI КРК является случай равенства плеч отправителя и получателя (симметричный), с последующим ухудшением результата по мере увеличения параметра асимметричности. В случае расположения квантового канала в С-диапазоне превосходство симметричного случая минимально, в то время как для квантового канала на 1310 нм (О-диапазон) разница существенна. Кроме того, выделение для квантового канала длины волны 1310 нм позволяет достичь наибольшего расстояния функционирования. Полученные результаты позволяют сделать выводы о практической реализации систем MDI КРК с целью получения оптимальных результатов.

Воронцова И.О. (автор)

Гончаров Р.К. (автор)

Болычев Е.А. (автор)

Киселев Ф.Д. (научный руководитель)
