УДК 535.8

КВАНТОВАЯ КОММУНИКАЦИЯ НА НЕПРЕРЫВНЫХ ПЕРЕМЕННЫХ В СИСТЕМЕ НА БОКОВЫХ ЧАСТОТАХ С ДИСКРЕТНОЙ МОДУЛЯЦИЕЙ

Гончаров Р.К. , Сантьев А.А., Первушин Б.Е.
Научный руководитель – Самсонов Э.О.
Национальный исследовательский университет ИТМО

В настоящем докладе описывается протокол квантовой рассылки ключа на непрерывных переменных с использованием многомодовых когерентных состояний, сгенерированных на поднесущих частотах модулированного оптического излучения. Для регистрации квадратурных компонент предложена схема когерентного приёма, аналогичная классической, описанной в научной литературе.

Введение. Квантовая рассылка ключа (КРК) – это метод распределения симметричных криптографических ключей между двумя легитимными пользователями, основанный на кодировании информации в состояниях квантовых объектов и последующей её обработки при помощи классических каналов связи.

Основная проблема реализации первых протоколов КРК, которые принято называть протоколами на дискретных переменных, заключается в необходимом наличии в схеме высокогабаритных детекторов одиночных фотонов.

В свою очередь, схемы КРК на непрерывных переменных, которые были предложены позже, опираются на методы когерентного приёма: гомодинный или гетеродинный, для получения информации о квадратурных распределениях. Другими словами, однофотонное обнаружение заменяется типичными классическими методами.

В докладе предлагается реализация протокола КРК на непрерывных переменных, использующего сигнал на поднесущих частот модулированного излучения как переносчик информации и сигнал на несущей частоте – как локальный осциллятор в системе когерентного приёма.

Основная часть. Цель данной работы – продемонстрировать универсальность описываемого протокола. Поэтому была построена математическая модель протокола КРК на непрерывных переменных с использованием поднесущих частот и показана возможность выполнения анализа секретности для рассматриваемого случая многомодовых когерентных состояний. Полное доказательство секретности выходит за рамки доклада и будет предметом отдельного исследования. Здесь же проведён анализ секретности с ключом конечной длины с использованием методики асимптотических свойств распределения, и рассчитана нижняя граница скорости генерации секретного ключа. Значения скорости генерации секретного ключа получены для схемы прямого согласования с последующей выборкой в случае коллективных атак.

Выводы. Предложена реализация протокола квантовой рассылки ключа на непрерывных переменных с использованием многомодовых когерентных состояний, сгенерированных на поднесущих частотах модулированного оптического излучения, построена математическая модель предложенной схемы и продемонстрирован метод доказательства секретности.

Рассчитана скорость генерации секретного ключа с выборкой в асимптотическом и в режиме конечной длины в предположении, что шум квантового канала незначителен по сравнению с шумом детектора, а нарушитель ограничен коллективными атаками.

Расчёты показывают, что система позволяет обеспечить секретный ключ для потерь в канале до 9 дБ в реалистичной реализации. Важно отметить, что предложенная схема также позволяет реализовать протокол с т.н. гауссововым типом модуляциии, и представленный анализ секретности может быть принят там.

Сантьев А.А. (автор) Подпись

Самсонов Э.О. (научный руководитель) Подпись