УДК 535.8, 535.015

КВАНТОВОЕ РАСПРЕДЕЛЕНИЕ КЛЮЧЕЙ НА НЕПРЕРЫВНЫХ ПЕРЕМЕННЫХ С НЕДОВЕРЕННЫМ УЗЛОМ НА БОКОВЫХ ЧАСТОТАХ

Болычев Е.А. (Университет ИТМО), **Гончаров Р.К.** (Университет ИТМО), **Воронцова И.О.** (Университет ИТМО),
Научный руководитель – кандидат физико-математических наук, Киселев Ф.Д. (Университет ИТМО)

В работе описан подход к реализации системы квантового распределения ключей (КРК), не зависящей от измерительных устройств, где будет использоваться не дискретный набор квантовых состояний, а непрерывный – MDI (от англ. measurement-devise-independent) КРК на непрерывных переменных (КРКНП). В работе продемонстрирована схема системы, рассмотрены процессы генерации секретного ключа и детектирования, обоснована стойкость протокола против коллективных атак.

Введение. В настоящее время безопасный обмен информацией играет все более значимую роль. И современные разработки в области квантовых коммуникаций помогают решить большой объем соответствующих задач. Квантовое распределение ключей (КРК) — один из методов квантовых коммуникаций, способ передачи ключа, который использует квантовые явления для гарантии безопасной и стойкой связи.

Помимо популярных и хорошо изученных протоколов на дискретных переменных (КРКДП), описывающих генерацию и передачу однофотонных состояний, существуют протоколы на непрерывных переменных (КРКНП), использующие когерентные состояния в качестве носителей информации. Их отличительной чертой является удобство реализации и лучшая совместимость с современными телекоммуникационными системами. Такие протоколы не требуют использования однофотонных источников и детекторов, а используют гомодинное и гетеродинное детектирование.

Не так давно в системах КРКНП также было предложено несколько стратегий атак на реальные детекторы. Например, атака калибровки и атака флуктуаций ЛО используют ЛО для манипулирования результатами измерения, что провоцирует Алису и Боба переоценить секретность ключа. Самым логичным вариантом устранения этих атак в системе КРКНП было охарактеризовать каждую конкретную лазейку и найти меры противодействия. Однако довольно сложно полностью охарактеризовать реальные детекторы и учесть все возможности для атак на систему. Учитывая все проблемы в области детектирования, был предложен MDI КРКНП протокол, который решает большой объём задач, связанных с детектированием.

В докладе предлагается реализация протокола MDI КРКНП на боковых частотах модулированного излучения. От аналогов, рассматриваемы подход отличается отсутствием необходимости в опорном сигнале и дополнительными возможностями, которые могут быть доступны в перспективе, например, мультиплексирование по боковым компонентам различных порядков.

Основная часть. Основная идея MDI КРКНП, как и в стандартном MDI КРК, состоит в том, что и Алиса, и Боб являются отправителями, а для проведения измерения вводится ненадежная третья сторона (Чарли). Результаты измерений на реле Чарли будут использоваться Алисой и Бобом на этапе постобработки для генерации секретных ключей. Алиса и Боб готовят по когерентному состоянию, плотность распределения комплексный амплитуды которого подчиняется гауссовскому закону с нулевым средним и заданной дисперсией и отправляют их по квантовому каналу на недоверенное реле Чарли. Моды Алисы и Боба интерферируют на

светоделителе и измеряются Чарли на схеме, аналогичной типичному гомодинному детектированию, построенной специально для подхода боковых частот. Полученное третье состояние Чарли оглашает публично. В итоге Боб изменяет свое изначально сгенерированное состояние используя состояние, полученное на реле, Алиса же оставляет своё состояние неизмененным. После стандартных процедур по оценке параметров, согласованию информации и усилению стойкости Алиса и Боб получают коррелированные состояния.

Для анализа безопасности против произвольных коллективных атак вводится эквивалентная схему, основанной на запутанности (ОЗ). ОЗ-схема MDI эквивалентна схеме «приготовление-детектирование» (ПД) КРКНП с когерентными состояниями и гетеродинным детектированием. Более того, эффективность такого протокола против коллективных атак с клонирующими устройствами будет представлена с помощью методов численного моделирования.

Выводы. В работе был рассмотрен независимый от измерительных устройства протокол MDI КРКНП на боковых частотах, который остается стойким против коллективных атак на детекторы. Данная модель будет учитывает падение эффективности и шум, вызванные использованием обозначенного подхода. Кроме того, этот КРК протокол требует лишь незначительных изменений существующих систем КРКНП и, таким образом, может быть легко реализован на практике.

Болычев Е.А. (автор) _____

Гончаров Р.К. (автор) _____

Воронцова И.О. (автор) _____

Киселев Ф.Д. (научный руководитель) _____