УДК 535.8, 535.015

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

Гончаров Р.К. (Университет ИТМО), **Самсонов Э.О.** (Университет ИТМО), **Киселев Ф.Д.** (Университет ИТМО)
Научный руководитель – доктор физико-математических наук, доцент Киселев А.Д. (Университет ИТМО)

Описан подход к реализации системы квантовой коммуникации на боковых частотах, суть которого заключается в использовании не дискретного набора квантовых состояний, а непрерывного набора, распределённого по Гауссу с нулевым средним и заданной дисперсией. В работе продемонстрирована схема системы, рассмотрены процессы гауссовской модуляции многомодовых когерентных состояний и детектирования, обоснована стойкость протокола против коллективных атак.

Введение. Квантовая рассылка ключа (КРК) представляет собой достаточно интересную альтернативу устоявшимся классическим криптографическим методам, подверженным взлому в обозримом будущем. Суть КРК заключается не в передачи зашифрованной информации, но передачи ключей шифрования, генерируемых случайным образом в сеансе рассылки между двумя (или более) легитимными пользователями.

Наиболее популярные протоколы описывают генерацию и передачу однофотонных состояний, в фазе или поляризации которых может быть закодирована информация о ключе. Однако очевидно, что в реальности их аналогами служат ослабленные когерентные импульсы. Для их регистрации, в любом случае, требуются однофотонные детекторы, работающие в режиме счёта.

Тем не менее, в начале века начали появляться протоколы КРК, в которых не только используются когерентные состояния в качестве носителей информации, но также применяются методы когерентного детектирования (гомодинного или гетеродинного), популярные в приложениях квантовой оптики. Таким образом, выделен целый класс протоколов КРК, называемый КРК на непрерывных переменных (НПКРК).

В докладе предлагается реализация протокола КРК на непрерывных переменных с гауссовским типом модуляции. От известных схем, предлагаемая к рассмотрению отличается тем, что в ней используется сигнал на боковых частотах модулированного излучения как переносчик информации и сигнал на несущей частоте – как локальный осциллятор в системе когерентного приёма. Следует отметить, что аналогичная схема, но с дискретной фазовой модуляцией была продемонстрирована ранее.

Основная часть. Суть предлагаемого решения заключается в использовании электрооптических модуляторов для генерации когерентного состояния, плотность распределения комплексный амплитуды которого подчиняется гауссовскому закону с нулевым средним и заданной отправителем дисперсией. Это достигается тем, что действительная амплитуда состояния распределяется согласно распределению Рэлея, а фаза — согласно однородному распределению. После генерации состояние передаётся по квантовому каналу и детектируется получателем системой когерентного приёма, в которую входят фазовый модулятор, спектральный фильтр и балансный детектор. После процесса детектирования и последующей обработки отправитель и получатель имеют коррелированные битовые строки. Нарушитель же ограничен коллективными атаками. Предполагается также, что канал защищён от наличия побочных каналов утечки информации. Из приведённых соображений обосновывается стойкость протокола против коллективных атак.

Выводы. Предложена реализация схемы квантовой коммуникации на боковых частотах с гауссовским типом модуляции. Гауссовская модуляция позволяет существенно повысить

скорость генерации секретного ключа по причине того, что отправитель и получатель обмениваются не двоичными последовательностями, а действительными, которые далее подвергаются дополнительной обработке. Схема может быть реализована из стандартных телекоммуникационных компонент. Потенциал схемы заключается в возможности распределения информации на боковых полосах разных порядков одновременно. Также следует отметить, что предлагаемая схема может найти своё применение в компактных криптографических приложениях и в «интернете вещей».

Гончаров Р.К. (автор) _____
Самсонов Э.О. (автор) _____
Киселев Ф.Д. (автор) _____

Киселев А.Д. (научный руководитель) _____