УДК 535.8

СИСТЕМА КВАНТОВОЙ КОММУНИКАЦИИ НА НЕПРЕРЫВНЫХ ПЕРЕМЕННЫХ С НЕДОВЕРЕННЫМ ПРИЕМНЫМ УЗЛОМ

Фадеев М.А. (Университет ИТМО), **Гончаров Р.К.** (Университет ИТМО)
Научный руководитель – доцент, кандидат технических наук, Чистяков В.В.
(Университет ИТМО)

Введение. Квантовое распределение ключа (КРК) — разновидность квантовой связи, в которой задача создания и распределения случайного симметричного криптографического ключа между двумя пользователями решается с помощью кодирования классической информации в квантовых объектах. Большинство этих систем основано на концепции «точка-точка», где отправитель (Алиса) кодирует и отправляет сигнал получателю (Бобу). Важно, что в данном случае в теоретических доказательствах стойкости для протоколов предполагается, что оборудование Алисы и Боба защищено от потенциальных угроз со стороны нарушителя (Евы), обладающего бесконечным вычислительным ресурсом. Это несоответствие между теорией и практикой приводит к тому, что Ева в конечной системе КРК может проводить физические атаки на оборудование (например, повреждение лазером). В связи с этим была разработана концепция независимости от устройств (DI), подразумевающая, что все оборудование в системе не является доверенным. Из основных разновидностей выделяется - независимое от устройств измерения (MDI) КРК [1], где используется недоверенный детектирующий узел.

Основная часть. В качестве решения для передачи секретного ключа в данной работе предлагается использование аппаратно-независимой системы КРК на непрерывных переменных [2] с использованием боковых частот [3]. В системе такого типа используются два доверенных узла – Алиса и Боб, между которыми происходит сеанс обмена информацией, и один недоверенный - Чарли, где происходит регистрация излучения. Алиса и Боб модулируют лазерное излучение переменным высокочастотным сигналом, в который кодируется информация. В результате такой модуляции в спектре появляются боковые гармоники. Полученный таким образом сигнал ослабляется до энергий менее 1 фотона в импульсе в среднеми отправляется по оптическому волокну. В недоверенном детектирующем узле сигналы от Алисы и Боба интерферируют на светоделителе с 2 входами и 2 выходами, выходы которого подключены к балансному детектору. В результате этой интерференции поле перераспределяется между плечами балансного детектора, на выходе которого формируется положительное или отрицательное напряжение, в зависимости от разности фаз между сигналами Алисы и Боба. После этого Чарли по открытому каналу раскрывает информацию о детектировании, зная которую Алиса и Боб могут формировать секретный ключ.

Выводы. В рамках данной работы проведен эксперимент по реализации системы КРК с недоверенным приемным узлом. Обоснована работоспособность данного подхода.

Список использованных источников:

1. Lo H. K., Curty M., Qi B. Measurement-device-independent quantum key distribution // Physical Review Letters. – 2012. – Т. 108. – №. 13. – С. 130503.
2. Li Z. et al. Continuous-variable measurement-device-independent quantum key distribution // Physical Review A. – 2014. – Т. 89. – №. 5. – С. 052301
3. Mazurenko Y. T., Merolla J. M., Godgebur J. P. Quantum transmission of information with the help of subcarrier frequency. Application to quantum cryptography // Optics and Spectroscopy. – 1999. – Т. 86. – №. 2. – С. 145-147.