УДК 535.8

ИССЛЕДОВАНИЕ АТАКИ С ВРЕМЕННЫМ СДВИГОМ НА СИСТЕМУ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ НА БОКОВЫХ ЧАСТОТАХ

Геллерт М. Е. (ИТМО)

Научный руководитель – кандидат физико-математических наук Наседкин Б. А. (ИТМО)

Введение. Наиболее безопасным способом передачи информации на данный момент являются системы квантового распределения ключей (КРК). В таких системах безопасность гарантируется фундаментальными законами квантовой механики [1], а не ограниченностью вычислительных мощностей злоумышленника. Хотя теоретически ряд протоколов КРК являются безопасными [2-4], практические реализации данных систем могут иметь уязвимости, которыми может воспользоваться злоумышленник для извлечения информации о ключе [5-6]. Одной из таких уязвимостей является временное окно чувствительности детектора одиночных фотонов (ДОФ). В настоящее время многие практические системы используют оптические волокна в качестве квантовых каналов и работают на телекоммуникационных длинах волн 1550 или 1310 нм. Обнаружение одиночных фотонов в таких системах часто осуществляется с помощью лавинных фотодиодов InGaAs. Чтобы минимизировать темновые отсчеты, данный тип детекторов обычно работает в режиме стробирования. Таким образом, изменив время попадания импульса на детектор получателя, можно управлять информацией, регистрируемой получателем. В данной работе производились исследования возможности проведения атаки с временным сдвигом на систему квантового распределения ключей на боковых частотах (КРК БЧ).

Основная часть.

В данном исследовании изучается работа системы КРК БЧ и внедряющегося в данную систему нарушителя. Основным аспектом данной атаки является возможность нарушителя влиять на состояния, измеряемые получателем, поэтому для проверки возможности проведения атаки с временным смещением необходимо удостовериться, что нарушитель может по желанию вызывать как отсутствие срабатывания ДОФ, так и срабатывания ДОФ. Для навязывания отсутствия срабатывания злоумышленнику необходимо увеличить оптический путь, проходимый излучением так, что оптические импульсы будут попадать на детектор в тот момент, когда вероятность детектирования будет минимальной.

В случае же с навязыванием срабатывания детектора злоумышленник может воспользоваться своим источникам излучения, центральная длине волны которого отличается от центральной длины волны источника отправителя. Это связано с тем, что зачастую в системах КРК БЧ в оптической схеме присутствует брегговская решетка [7], отделяющая боковые частоты от центральной.

Для повышения вероятности провоцирования срабатывания детектора злоумышленник использует не однофотонные импульсы. Поэтому в данной работе проведена экспериментальная и теоретическая оценка вероятности срабатывания ДОФ в зависимости от количества фотонов.

Выводы. В ходе данной работы была исследована вероятность детектирования импульса в зависимости от временного сдвига, вносимого злоумышленником. Также была проведена оценка мощности излучения злоумышленника, необходимой для наиболее вероятной реализации срабатывания детектора.

Список использованных источников:

1. Bennett C. H., Brassard G.zQuantum cryptography: Public key distribution and coin tossing //Theoretical computer science. – 2014. – Т. 560. – С. 7-11.

2. Lo H. K., Chau H. F. Unconditional security of quantum key distribution over arbitrarily long distances //science. – 1999. – Т. 283. – №. 5410. – С. 2050-2056.
3. Shor P. W., Preskill J. Simple proof of security of the BB84 quantum key distribution protocol //Physical review letters. – 2000. – Т. 85. – №. 2. – С. 441.
4. Gottesman D. et al. Security of quantum key distribution with imperfect devices //International Symposium onInformation Theory, 2004. ISIT 2004. Proceedings. – IEEE, 2004. – С. 136.
5. Brassard G. et al. Limitations on practical quantum cryptography //Physical review letters. – 2000. – Т. 85. – №. 6. – С. 1330.
6. Sun S., Huang A. A review of security evaluation of practical quantum key distribution system //Entropy. – 2022. – Т. 24. – №. 2. – С. 260.
7. Sajeed S. et al. An approach for security evaluation and certification of a complete quantum communication system //Scientific Reports. – 2021. – Т. 11. – №. 1. – С. 5110.