УДК 535.015

ИССЛЕДОВАНИЕ АТАКИ С ОСЛЕПЛЕНИЕМ БАЛАНСНОГО ДЕТЕКТОРА НА РАЗЛИЧНЫХ ДЛИНАХ ВОЛН

Морозова П.А. (Университет ИТМО)
Научный руководитель – научный сотрудник Наседкин Б.А.
(Университет ИТМО)

Введение. Наиболее перспективным способом безопасной передачи данных являются системы квантового распределения ключей (КРК). Эти системы позволяют двум удаленным сторонам передавать ключ шифрования по открытому каналу с помощью классической связи [1]. Однако квантовые сети всё ещё могут быть подвержены потенциальным атакам, которые ставят под угрозу передачу ключа шифрования. Системы КРК, основанные на непрерывных переменных (КРК НП), полагаются на когерентное обнаружение, используя такое устройство, как балансный детектор.

Основная часть. Основное внимание в данной работе уделено исследованию балансного детектора (БД), необходимого компонента в системах квантового распределения ключей. Атака с ослеплением направлена на насыщение фотодиодов БД путём подачи мощного излучения на сигнальный порт или локальный осциллятор [2]. Возникает вопрос о длине волны излучения, используемого в сети и для проведения атаки. Распространённой для телекоммуникационных сетей является длина волны 1550 нм, при этом интерес также представляет влияние атакующего излучения на длинах волн, отличных от используемой в данной системе КРК НП. Так, исследование было проведено также для длин волн 1440 нм и 1590 нм.

В ходе эксперимента была измерена зависимость средних значений интенсивности в каналах БД и величины дисперсии (избыточного шума) от мощности. При мощности около 7 мкВт балансный детектор переходит из линейного режима работы в нелинейный вследствие превышения допустимого уровня фототока и насыщения электроники [3]. Данный переход свидетельствует об ослеплении балансного детектора, что влечёт нарушение безопасности сети, поскольку легитимные пользователи примут скомпрометированный ключ, основываясь на допустимости измеренного значения дисперсии.

Выводы. Экспериментально были определены зависимости средних значений интенсивности от мощности излучения для каждого канала балансного детектора, на основании чего определяется порог насыщения балансного детектора, а также зависимость дисперсии от мощности. Полученные результаты могут помочь в выявлении потенциальной атаки с ослеплением балансного детектора и в разработке стратегии защиты.

Список использованных источников:

1. Nitin J., Chin H., Mani H., Lupo C., Nikolic D.S., Kordts A., Pirandola S., Pedersen T.B., Kolb M., Omer B., Pacher C., Gehring T., Andersen U.L. Practical continuous-variable quantum key distribution // Nature communications. – 2022. – № 13(1).
2. Qin H., Kumar R., Makarov V., Alléaume R. Homodyne-detector-blinding attack in continuous-variable quantum key distribution // Physical Review A. – 2018. – №. 98(1). – С. 012312.
3. Tang X., Kumar R., Ren S., Wonfor A., Penty R. V., White I. H. Performance of continuous variable quantum key distribution system at different detector bandwidth // Optics Communications. – 2020. – № 471. – С. 126034.