УДК 530.145

МОДЕЛИРОВАНИЕ ЭФФЕКТОВ АСИММЕТРИИ НЕИДЕАЛЬНЫХ ИЗМЕРЕНИЙ В АНАЛИЗЕ СТОЙКОСТИ ПРОТОКОЛОВ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧА НА НЕПРЕРЫВНЫХ ПЕРЕМЕННЫХ

Наумчик А.С. [1], **Гончаров Р.К.** [1]
Научный руководитель – д. ф.-м. н., доцент Киселев А.Д. [1]
[1]Университет ИТМО
C0wl0ver@yandex.ru

Работа выполнена при поддержке Российского научного фонда (проект № 24-11-00398).

Введение

При практической реализации протоколов квантового распределения ключа с непрерывными переменными (КРКНП) учет неидеальности когерентных измерений является исключительно важным фактором, влияющим на их стойкость. Для моделирования измерительных шумов и построения положительных операторнозначных вероятностных мер (ПОВМ) используются гауссовские квантовые каналы, такие как канал аддитивного шума (аддитивный шум) и релаксационный канал (аттеньюатор) [1,2]. Целью работы является исследование влияния модели канала измерительного шума на асимптотическую стойкость протокола КРКНП GG02 [3] в сценарии недоверенного шума, предполагающего, что параметры всех каналов, описывающих шумы и потери, доступны перехватчику [4].

Основная часть

Эффекты асимметрии, рассматриваемые в работе, включают в себя разбалансировку светоделителей и неравную квантовую эффективность детектирования. Для моделирования асимметричных схем гомодинирования и двойного гомодинирования в гауссовском приближении были построены ПОВМ и использованы две модели измерительных каналов: аддитивный шум и аттенюатор, параметры которых определяются ковариационными матрицами ПОВМ. При этом ПОВМ и каналы двойного гомодинирования дополнительно зависят от параметра сжатия состояний измерительного базиса идеальных измерений [2]. Показано, что информация Холево зависит от параметров ПОВМ и модели канала: модель аддитивного шума соответствует увеличению эффективного шума коммуникационного канала, а аттенюатор – уменьшению пропускания и шума канала передачи. В случае аддитивного шума, для параметра сжатия существует оптимальное значение, обеспечивающее максимум информации Холево. В результате, по сравнению с аттеньюатором, аддитивный шум значительно сильнее уменьшает максимальную длину коммуникационного канала даже при малой асимметрии.

Выводы

Показано, что в модели аддитивного шума увеличение эффективного шума канала передачи существенно снижает скорость генерации ключа и длину передачи, тогда как, для модели аттеньюатора, негативный эффект слабее. Исследовано влияние параметра сжатия на скорость генерации ключа в схеме двойного гомодинирования. В отсутствии эффектов асимметрии, полученные результаты согласуются с известными [4].

Литература

1. Serafini A. Quantum continuous variables: a primer of theoretical methods. – CRC press, 2024.
2. Naumchik A.S., Goncharov R.K., Kiselev A.D. [Электронный ресурс]. – 2025. – Режим доступа: https://arxiv.org/abs/2512.22591 (дата обращения: 18.02.2026).
3. Grosshans F. et al. Quantum key distribution using Gaussian-modulated coherent states //Nature. – 2003. – Т. 421. – №. 6920. – С. 238-241.
4. Laudenbach F. et al. Continuous-variable quantum key distribution with Gaussian modulation—the theory of practical implementations //Advanced Quantum Technologies. – 2018. – Т. 1. – №. 1. – С. 1800011.