УДК 535.8 535.015

РЕШЕНИЕ ЗАДАЧИ ВЫПУКЛОЙ ОПТИМИЗАЦИИ ДЛЯ ПРОТОКОЛА КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧА НА БОКОВЫХ ЧАСТОТАХ

Иванков Н.А. (Университет ИТМО), **Гончаров Р.К.** (Университет ИТМО),
Болычев Е.А. (Университет ИТМО), **Сеник К.А.** (Университет ИТМО)
Научный руководитель – Зиновьев А.В.
(Университет ИТМО, НГУ)

Введение. Квантовое распределение ключей (КРК) — это метод обмена симметричными криптографическими ключами между двумя сторонами, основанный на кодировании информации при помощи состояний квантовых объектов и последующей передачи по классическому каналу связи. На данный момент системы КРК, как правило, используют стандартный набор известных решений для постобработки сырой последовательности, исправления ошибок и усиления стойкости. Однако, в последнее время наблюдается рост интереса к разработке и адаптации программных методов, которые могут значительно повысить производительность систем КРК. Одним из таких является полуопределенное программирование.

В докладе рассматривается система КРК на боковых частотах (КРКБЧ), которая использует в качестве информационных квантовых состояний ослабленные многомодовые когерентные состояния, получаемые посредством фазовой модуляции несущей волны, то есть кодирование информации осуществляется на боковых частотах модулированного излучения. У такого подхода можно выявить ряд преимуществ, среди них: высокая спектральная эффективность в квантовом канале, возможность распределения различной информации на отдельных боковых модах различных порядков вокруг одной оптической несущей моды.

Основная часть. Многие практические задачи исследования операций и комбинаторной оптимизации могут быть смоделированы или аппроксимированы как задачи полуопределенного программирования. В контексте КРК, средствами полуопределенного программирования может быть осуществлена оптимизация ключевых параметров системы, как следствие, уточнена длина конечного ключа для заданной реализации. Стратегия состоит в выражении длины секретного ключа (или приведённой скорости генерации) в виде задачи выпуклой оптимизации, которая может быть решена численно [1,2].

Выводы. Решение вышеописанной задачи позволяет увеличить число сгенерированных ключей в единицу времени при том же числе задействованных волоконно-оптических линий связи при интеграции систем КРК в реальную инфрастуктуру благодаря программной оптимизации существующих аппаратных реализаций.

Список использованных источников:

1. George I., Lin J., Lütkenhaus N. // Phys. Rev. Res. – 2021. – Т. 3. – №. 1. – С. 013274
2. Bunandar D. et al. // npj Quantum Inf. – 2020. – Т. 6. – No. 1. – С. 1-12