УДК 004.722.2

ПРОБЛЕМА ПОСТРОЕНИЯ ДИНАМИЧЕСКОГО МАРШРУТА В КВАНТОВОЙ СЕТИ

Лихтенберг А.М. (Университет ИТМО)
Научный руководитель – д.т.н., доцент Беззатеев С.В.
(Университет ИТМО)

Введение. Квантовая криптография – наука, которая начала развиваться в прошлом столетии благодаря открытиям физиков и попыткам создать квантовые деньги. На текущий момент квантовую криптографию разделяют на квантовые коммуникационные технологии, технологии квантовой обработки информации и технологии квантовых вычислений [1]. К квантовым коммуникационным технологиям относятся такие вопросы, как квантовое распределение ключей и построение квантовых сетей для передачи данных. Построение таких сетей имеет множество ограничений, вызванных особенностями передачи фотона по каналу.

Основная часть. Основная сложность при построении квантовой сети для формирования ключей – ограниченная дальность канала и возможность связи исключительно между двумя участниками обмена [2], в связи с чем многие классические способы построения сетей не могут быть применены к вопросу квантовой связи.

Современные методические рекомендации описывают протокол ISTOQ, который использует как квантовые, так и классические каналы для формирования квантовозащищённого ключа (далее – КЗК) между доверенными промежуточными узлами (далее – ДПУ) [3]. Однако, в данном протоколе не описаны способы построения маршрута для передачи квантовой компоненты ключа: согласно рекомендациям, выбор маршрута может быть произведён разработчиком при построении сети.

При построении маршрута для передачи квантовой компоненты может быть использован как статический, так и динамический маршрут. Использование статического маршрута для передачи квантовой компоненты проще в реализации, однако при активном использовании квантовой сети могут возникнуть следующие сложности:

- часть сети может быть перегружена, в то время как на другом сегменте может быть простой;
- ДПУ может выйти из строя, и за неимением альтернативного маршрута для передачи квантовой компоненты выработка КЗК остановится до восстановления работоспособности элемента сети.

Из вышесказанного можно сделать вывод, что построение динамического маршрута между ДПУ может повысить работоспособность сети и уменьшить скорость выработки КЗК. Для исследования предлагается [4] построить модель сети в виде графа, в котором вершинами будут являться ДПУ, а рёбрами – квантовые каналы между ДПУ. Сложность задачи заключается в присвоении веса каждому ребру, так как необходимо учитывать множество условий, некоторые из которых также изменяются со временем, например: количество запросов на КЗК от каждого узла, количество выработанных КЗК, буфер компонент, нагрузка на ДПУ и прочие.

Выводы. Для успешного построения динамического маршрута между узлами квантовой сети необходимо исследование модели сети с помощью теории графов. Для корректного построения модели необходимо определить:

- критерии, по которым будет присваиваться тот или иной вес ребру графа;
- способы измерения присваиваемых весов;
- степень влияния каждого критерия на общий вес ребра;
- используемый алгоритм для поиска кратчайшего маршрута между двумя вершинами в построенном графе.

В результате проведённого исследования будут рассмотрены проблемы построения динамического маршрута в квантовых сетях связи, а также предлагаемые способы их решения.

Список использованных источников:

1. Корольков А. О современном этапе развития прикладной квантовой криптографии. [Электронный ресурс]. – Режим доступа: http://lib.itsec.ru/articles2/crypto/o-sovremennometape-razvitiya-prikladnoy-kvantovoy-kriptografii (дата обращения: 12.02.2023).
2. Лихтенберг А.М. Квантовое распределение ключей: обзор решаемых задач // Альманах научных работ молодых ученых Университета ИТМО -2022. - Т. 2. - С. 79-82
3. АО «ИнфоТеКС» // Криптографическая защита информации // Ключевая система полносвязной многоарендаторной сети шифрованной связи на базе ККС ВРК с ДПУ. - проект изд. - Москва: Технический комитет по стандартизации «Криптографическая защита информации», 2021. - 25 с.
4. А. В. Уривский Принципы проектирования сетевых протоколов распределения ключей для квантовых сетей // Информатика и управление. - Федеральное государственное автономное образовательное учреждение высшего образования «Московский физико-технический институт (национальный исследовательский университет)», 2022. - С. 136-147.

Лихтенберг А.М. (автор) Подпись

Беззатеев С.В. (научный руководитель) Подпись