УДК 004.7

ПРОБЛЕМА РАЗРАБОТКИ ПОРОТОКОЛА РАСПРЕДЕЛЕНИЯ КЛЮЧА В КВАНТОВЫХ СЕТЯХ

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

Аннотация. Появление новых технологий передачи данных привело к формированию нового раздела науки: квантовой криптографии, для которой особое значение имеет разработка эффективных протоколов распределения ключей в квантовых каналах. В работе рассмотрены типы существующих решений по эффективному разветвлению квантовых сетей, что необходимо для расширения существующих возможностей по обмену ключом между участниками информационной системы.

Введение. Современное общество нуждается в способах быстрого обмена информацией. Эта потребность привела к созданию квантовых каналов связи: они позволяют передавать информацию быстро, с меньшими потерями и с меньшим количеством угроз со стороны злоумышленников. Однако, устройство квантовых сетей отличается от сетей из проводниковых материалов, что приводит к возможности применения новых криптографических механизмов внутри такого канала.
Созданные на данный момент протоколы квантовой криптографии для обмена ключом позволяют установить связь только между двумя узлами сети. Из-за ограниченной длины квантового канала обмен информацией между двумя удаленными узлами без взаимодействия с промежуточным узлом становится сложной комплексной задачей.

Основная часть. Передача данных по квантовым каналам основана на передаче состояний фотонов. Сохранение состояния фотона – одна из ключевых задач в протоколах распределения ключей по квантовому каналу, так как изменение состояния ведёт к потере информации и снижению скорости обмена ключом. Также необходимо учитывать среду передачи: в зависимости от использования оптоволоконных сетей, воздушного или безвоздушного пространства влияние на состояние фотона и способы его сохранения будут различными. Теорема о запрете клонирования неизвестного квантового состояния ограничивает возможности использования квантовых усилителей, что, в свою очередь, приводит к ограничениям дальности квантовых каналов. Таким образом, изучение вопроса эффективного разветвления квантовой сети нецелесообразно без учёта принципов квантовой механики и физических особенностей приборов, обеспечивающих сохранение состояния фотона (таких как фазовые модуляторы, интерферометры, контроллеры поляризации, волокна, сохраняющие поляризацию, и прочие).
На данный момент предложены несколько способов эффективного разветвления квантовых каналов с учётом существующих ограничений на передачу данных. К таким решениям относят: использование квантовозащищённых ключей, построение сетей топологии «звезда», использование доверенного узла при построении сетей. Данные решения либо частично используют квантовую сеть для передачи данных, либо слишком дороги в использовании и потому не применимы на практике, либо в них имеются существенные потери данных в результате атак злоумышленников. Таким образом, разработка нового эффективного протокола обмена ключом в квантовой сети безусловно является актуальной задачей, возможные подходы к решению которой будут представлены в данном докладе.

Выводы. В результате проведённого исследования будут рассмотрены и классифицированы существующие решения по разветвлению квантовой сети. Введённая классификация

позволит определить начальные условия экспериментов, необходимых для проектирования распределённых квантовых сетей.