Квантовая криптография: роль в современном мире, перспективы развития

И. Л. Кузнецов, Н. А. Бобырь, С. М. Гурский, И. В. Бережной

Военно-космическая академия имени А.Ф. Можайского

e-mail: vka@mil.ru

Аннотация. **Квантовая криптография – подраздел криптографии, который использует принципы квантовой механики в целях обеспечения безопасности при передаче информации. Традиционно криптографическая безопасность основывается на математике и учитывает разработанные ограниченные вычислительные мощности. Взлом криптографического кода потребовал бы разложения чрезвычайно больших чисел на два простых числа, обычно длиной более 100 цифр, что считалось невозможным за разумное время (менее миллиона лет), даже если бы все доступные сегодня компьютеры работали. Квантовая криптография, использующая фотоны и опирающаяся на законы квантовой физики вместо «чрезвычайно больших чисел», является передовым открытием, которое, кажется, гарантирует конфиденциальность даже при наличии подслушивающих устройств с неограниченными вычислительными возможностями.**

Ключевые слова: криптография, квантовая криптография, криптографическая безопасность, передовое открытие, перспективы развития

I. Введение

В основе метода квантовой криптографии лежит наблюдение квантовых состояний фотонов. Отправитель задает эти состояния, а получатель их регистрирует. Здесь используется квантовый принцип неопределенности, когда две квантовые величины не могут быть измерены одновременно с требуемой точностью. Закодированным отправляемым данным, задаются определённые квантовые состояния, после чего получатель их регистрирует, затем он (получатель) и отправитель совместно обсуждают результаты наблюдений. По итогу, со сколь угодно высокой достоверностью можно быть уверенным: переданная и принятая кодовые последовательности – тождественны. Обсуждение результатов касается ошибок, которые вносят шумы, но не отдельные биты. При передаче данных контролируется поляризация фотонов. В качестве источника света может использоваться светоизлучающий диод или лазер. Свет фильтруется, поляризуется и формируется в виде коротких импульсов малой интенсивности.

Цель доклада – исследовать понятие «квантовая криптография» и описать ее роль как в современном мире, так и в ближайшем будущем.

II. Основная часть

A. Роль квантовой криптографии в современном мире

В современном цифровом мире, где информационные технологии проникают во все сферы нашей жизни, обеспечение безопасности данных и защиты конфиденциальности становится все более актуальной проблемой. Криптография, наука о защите информации с помощью математических методов и алгоритмов, играет важную роль в обеспечении безопасности коммуникаций и хранения данных. Однако с появлением квантовых компьютеров, которые оперируют на основе законов квантовой механики, классические криптографические методы сталкиваются с угрозой быстрого взлома [2].

Квантовая криптография возникла как ответ на эту новую угрозу и представляет собой новый подход к обеспечению безопасности данных. В отличие от классической криптографии, которая использует сложные математические функции для шифрования информации, квантовая криптография использует квантовые явления, такие как квантовая запутанность и квантовая суперпозиция, для создания абсолютно защищенных ключей и обеспечения непрерывной контролируемой защиты информации [3].

Основной принцип квантовой криптографии состоит в том, что любая попытка перехватить квантовую информацию приведет к немедленному нарушению ее состояния, что сделает такую попытку обнаружимой и тем самым обеспечит абсолютную защиту от перехвата или подслушивания. Это открывает новые перспективы для безопасности информации и защиты частной жизни в эпоху растущей угрозы кибератак и развития квантовых вычислений [4].

Квантовая криптография, несмотря на свою относительную новизну, уже находит применение в различных коммерческих и государственных секторах. Ее основное преимущество – обеспечение абсолютно защищенного обмена информацией и ключами шифрования. Роль квантовой криптографии в коммерческих и государственных секторах становится все более важной в условиях быстрого развития квантовых вычислений и угрозы кибератак. Успешные квантово-криптографические системы обеспечивают надежную защиту данных и информации, делая квантовую криптографию обещающим и перспективным направлением в обеспечении безопасности в эпоху цифровых технологий [5].

В 1992 году Чарльз Беннет предложил один из первых протоколов (B92) реализации однонаправленного канала связи с квантовым шифрованием (рис. 1).

Рис. 1. Канал связи с квантовым шифрованием

В представленной схеме коллиматор необходим для получения пучков параллельных световых лучей. Ячейки Покеля служат для импульсной вариации поляризации потоков квантов передатчиком и анализа импульсной поляризации приемником. Кальцитная призма расщепляет пучок на два фотодетектора (ФЭУ), изменяющие две ортогональные составляющие поляризации. В качестве канала передачи может использоваться оптоволокно.

Технологии квантовой защиты связи активно используют крупные банки и финансовые организации, госструктуры, а также Центры обработки данных. Мировой рынок квантовой криптографии оценивается в более чем пол миллиарда долларов [5].

B. Перспективы развития квантовой криптографии

Роль квантовой криптографии в коммерческих и государственных секторах становится все более важной в условиях быстрого развития квантовых вычислений и угрозы кибератак. Успешные квантово-криптографические системы обеспечивают надежную защиту данных и информации, делая квантовую криптографию обещающим и перспективным направлением в обеспечении безопасности в эпоху цифровых технологий.

Анализ текущих исследований и достижений в области квантовой криптографии указывает на большие перспективы развития данного направления передачи информации, в том числе и по закрытым каналам связи.

Квантовая криптография представляет собой многообещающее направление в области обеспечения безопасности данных. Перспективы развития квантовой криптографии связаны с возможностью преодолеть текущие ограничения и применять ее на практике в широком масштабе. С развитием технологий и увеличением доступности квантовых систем, квантовая криптография может стать ключевым средством защиты информации в эпоху развития квантовых вычислений и кибератак. Ожидается, что квантовая криптография станет неотъемлемой частью будущей информационной инфраструктуры, обеспечивая надежную защиту данных и приватности в цифровом мире [6].

III. Заключение

Квантовая криптография, в отличие от обычной криптографии, появилась относительно недавно, но уже успела показать себя, как метод шифрования информации, который в будущем заменит остальные системы безопасности. Конечно, для этого необходимо избавиться от проблем и недостатков такого способа защиты и передачи информации. Но зная, как быстро развиваются технологии в наше время, авторы уверены, что эти проблемы будут исправлены очень скоро.

Благодарность

Авторы выражают благодарность командованию Военно-космической академии за помощь при проведении исследований, предоставленные возможности информационной поддержки, а также руководству СПбГЭТУ «ЛЭТИ» за возможность участия в работе 14 секции «Молодежная школа РЭС» 79-й научно-технической конференции Санкт-Петербургского НТО РЭС им. А.С. Попова, посвященной Дню радио.

Список литературы

[1] Пилькевич С.В., Романченко А.М., Лохвицкий В.А. Теоретико-числовые методы в криптографии: Учебное пособие. – Электрон. текстовые дан. (160 Mb). СПб.: ВКА имени А.Ф. Можайского, 2021. 1 электрон. опт. диск (CD-ROM).

[2] Квантовая криптография: идеи и практика / Под ред. С.Я. Килина, Д.Б. Хорошко, А.П. Низовцева. Минск: Беларуская навука, 2007.2007. 391 с.

[3] Холево А.С. Введение в квантовую информацию. МЦНМО. 2002. 128 с.

[4] Голубчиков Д.М. Применение квантовых усилителей для съема информации с квантовых каналов распределения ключа // Известия ТТИ ЮФУ. 2008. №1(78), С.119.

[5] Голубчиков Д.М. Анализ способов съема информации с квантового канала распределения ключа и методы их обнаружения // Современные информационные технологии - 2007: материалы докладов Всероссийской НТК с международным участием. 2007.

[6] Романченко А.М., Пилькевич С.В. Криптографические методы защиты информации: Учебное пособие. Электрон. текстовые дан. (630 Mb). СПб.: ВКА имени А.Ф. Можайского, 2022. 1 электрон. опт. диск (CD-ROM).