ПЕРСПЕКТИВА ИСПОЛЬЗОВАНИЯ КВАНТОВОЙ КРИПТОГРАФИИ КАК ОСНОВНОГО МЕТОДА ЗАЩИТЫ КОММУНИКАЦИИ

Хомельянский Д.В
Ермакович Н.В

Белорусский государственный университет информатики и радиоэлектроники
г.Минск, Республика Беларусь

Савилова Ю.И – канд. тех. наук, доцен

В данной работе рассмотрена перспектива использования квантовой криптографии, как метода защиты коммуникации, а также последние исследования, направленные на развитие и популяризацию этого метода.

Криптография – общий термин, к которому относятся методы, обеспечивающие шифрование и целостность данных. Криптография подразумевает преобразование информации в шифр, который не несёт в себе исходного смысла сообщения. Процесс кодирования сообщения называется шифрованием. Обратный метод, подразумевающий расшифровку оригинального сообщения, называется дешифрованием. Традиционная криптография представляет собой область симметричных криптосистем, в которых шифрование и расшифрование проводится с использованием одного и того же секретного ключа [1].

Квантовое распределение ключа (КРК) — это технология, позволяющая создать у двух удаленных пользователей строку случайных бит, впоследствии используемую в качестве криптографического ключа.

Квантовая криптография — метод защиты коммуникаций, основанный на принципах квантовой физики.

Принципиальное отличие квантового способа заключается в том, что КРК — это первая в истории человечества система распределения ключей, для которой есть строгое математическое доказательство того, что она не взламывается, даже со всеми неограниченными вычислительными мощностями и технологиями, которые не запрещены законом физики. Метод КРК решает одну из фундаментальных задач криптографии — распределение ключей между конечными пользователями по открытым каналам связи.

Схема практической реализации квантовой криптографии показана на рисунке 1 [2].

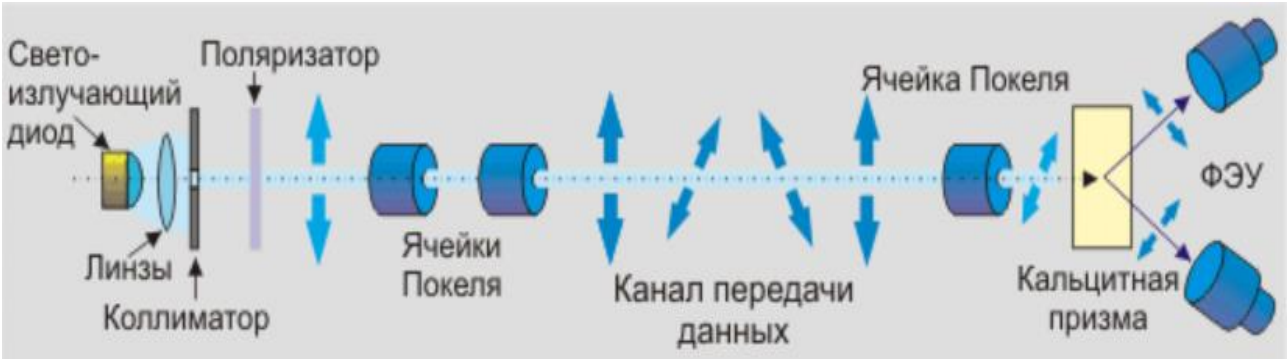

Рисунок 1 – Схема процесса квантовой криптографии

Передача информации на схеме происходит слева на право. Ячейки Покеля предназначены для импульсной вариации поляризации потока квантов передатчиком и для анализа импульсов поляризации приемником. Передатчик отправляет одну из двух поляризаций, каждая из которых имеет по 2 взаимно перпендикулярных направления. Передаваемые данные приходят в виде управляющих сигналов на принимающие ячейки Покеля. Одной из альтернативных сред передачи данных может являться оптическое волокно. В качестве источника сигнала вместо светоизлучающего диода можно использовать лазер.

На стороне приемника после ячейки Покеля установлена кальцитовая призма, которая разделяет пучок на два фотодетектора (ФЭУ), измеряющие две ортогональные составляющие поляризации.

При формировании передаваемых импульсов квантов иногда возникает проблема их интенсивности, что требует решения. Например, чем больше в импульсе содержится квантов — тем выше вероятность того, что злоумышленник сможет перехватить всю необходимую информацию в

ходе передачи. Поэтому идеальным вариантом является ситуация, когда в импульсе количество квантов стремится к одному. В таком случае, при перехвате — состояние системы изменится, провоцируя возникновение ошибок у получателя.

Целью данной работы является анализ новых достижений в области квантовой криптографии с точки зрения технологического прогресса и перспективы использования данного метода.

Одной из последних разработок в области квантовой криптографии является модификация системы квантового шифрования с компактным детектором [3].

Данная система КРК с компактным когерентным детектором работает на основе протокола квантового распределения ключа на боковых частотах, разработка ведется уже последний несколько лет Главной особенностью данного протокола является образование состояний при помощи электрооптического фазового модулятора.

Ключевым достижением этой системы является разработка когерентного приема. В его основе лежит использование несущей оптической частоты, которая не несет в себе информации, но которую используют в качестве опорной для фиксации фазы слабого сигнала с боковых частот.

В данной разработке используется дополнительный модулятор, но с повышенным уровнем модуляции, затем требуется с его помощью преобразовать сигнал. Таким способом образуются дополнительные боковые частоты, которые взаимодействуют с теми, что пришли от передатчика. При конструктивной интерференции большая часть излучения окажется на боковых частотах и, наоборот, при деструктивной, большая часть излучение окажется на центральной частоте, что может быть зарегистрировано балансным детектором.

Данное исследование поможет удешевить стоимость оборудования, используемого для создание массовых сетей КРК, что сделает их доступными для более широкого круга пользователей. В дополнение эта разработка позволит использовать для КРК инфраструктуру обычных оптоволоконных линий связи.

В начале 2021 года учеными был предложен новый, более устойчивый к внешним воздействиям алгоритм коррекции ошибок с использованием так называемых полярных кодов [4]. Полярный код — линейный корректирующий код, основанный на явлении поляризации канала. Применение полярных кодов позволяет устройствам для квантового распределения ключей стабильно работать в условиях реальной жизни под воздействием различных факторов окружающей среды. Использование полярных кодов позволит сделать систему устойчивой к влиянию ветра, осадков, повышения или снижения температуры.

Еще одним достижением является сокращение доли ключа, необходимой для аутентификации данных, передаваемых во время процесса классической постобработки. В системах квантовой криптографии часть ключа, который был распределен ранее, используется для аутентификации классических сообщений в последующих раундах генерации ключей. Чем этот расход меньше, тем эффективнее работает система в целом. В данном реализации протокола аутентификации доля ключа, затрачиваемая на подтверждение подлинности трафика, значительно уменьшилась и может составлять менее доли процента.

Результаты этих исследований увеличат эффективность работы существующих систем КРК. Значительную роль в эффективности квантовых криптографических систем играет классическая постобработка — набор манипуляций над данными, направленный на выявление и исправление ошибок в квантовых ключах, а также анализ и исключение из него информации, которая могла быть перехвачена злоумышленником.

Описанные достижения окажут значительное влияние на будущее развитие технологии квантовой криптографии. Увеличение эффективности и скорости работы устройств для квантового распределения ключей ускорит массовое внедрение и расширит сферы применения этой технологии в будущем, а модификация алгоритма корреляции ошибок повысит устойчивость данной системы.

На данный момент одной из ключевых проблем повсеместного внедрения квантовой криптографии является высокая стоимость оборудования, но эта проблема решается путём альтернативного использования оптоволоконных сетей, как среды передачи и различных разработок, направленных на удешевление детекторов.

Список использованных источников:

Бабаш А.В. Криптографические методы защиты информации [Электронный ресурс]. – Режим доступа: https://dlib.rsl.ru/02000022576 – Дата доступа: 23.03.2021.

Реализация идеи квантовой криптографии [Электронный ресурс]. – Режим доступа: https://www.tadviser.ru/index.php/Статья:Квантовая_криптография_(шифрование) – Дата доступа: 23.03.2021.

ИТМО: Приемник для передачи ключей квантового шифрования [Электронный ресурс]. – Режим доступа: https://www.tadviser.ru/index.php/Продукт:ИТМО:_Приемник_для_передачи_ключей_квантового_шифрования – Дата доступа: 23.03.2021.

Новый мировой рекорд в области квантовой криптографии [Электронный ресурс]. – Режим доступа: https://misis.ru/science/achievements/2021-02/7242/ – Дата доступа: 23.03.2021.