УДК 004.056.5

КВАНТОВАЯ КРИПТОГРАФИЯ ДЛЯ БУДУЩЕГО ИНТЕРНЕТА И АНАЛИЗА БЕЗОПАСНОСТИ

Садуова Улболсын Сериккызы
saduova@mail.ru
Магистрант кафедры «Радиотехника, электроника и телекоммуникации»
ЕНУ им. Л.Н.Гумилева, Нур-Султан, Казахстан
Научный руководитель – У.М. Кабылбекова

В работе отмечена, роль и место криптографической защиты в обеспечении безопасности передаваемой информации частного характера так и государственного значения. Приводятся основные понятия квантовой информации затем основа криптографической защиты сигналов – квантовая физика, где информация переносится с помощью объектов квантовой механики, т.е. процесс отправки и приёма информации при помощи электронов в электрическом токе или фотонов в линиях волоконно-оптической связи. Рассмотрены основные меры защиты современного интернета, а также технология квантовой связи интернета в будущем т.е. принцип использования квантовых вентилей в криптографической защите информации.

Интернет – Браузеры. VPN (виртуальная частная сеть). Электронная почта. WI-FI. Квантовая криптография. Квантовые ключи. Кубиты Квантовые вычисления. Алгоритмы и протоколы.

Киберпространство стало самым популярным средством обмена информацией во всех уголках нашей жизни, что благотворно сказывается на нашей жизни практически во всех аспектах. Следует отметить, из каждого угла за Вами следят злоумышленники разной категории, вооруженные цифровой техники. Это маркетологи, и агенты АНБ и простые воры.

И непрерывным развитием науки и техники, особенно квантового компьютера, безопасность киберпространства стала наиболее важной проблемой для интернета в ближайшем будущем.

Мы можем бороться и защищаться от злоумышленников с помощью тех же достижения цифровой технологии т.е использовать шифровку, обеспечивающие криптозащиту, в частности квантовой технологией.

Криптография и сетевая безопасность являются ключевыми технологиями для обеспечения безопасности информационной системы [6]. Квантовая криптография – важная отрасль криптографии, представляющая собой комбинацию квантовой механики и классической криптографии. Кроме того, для обеспечения безопасности следует обратить внимание на источники и который может быть в руках злоумышленника.

1 Основы квантовой информации

Самой ценной информацией в криптографии – шифровальные ключи.

Ключ – секретная информация, используемая криптографическим алгоритмом при зашифровании/расшифровании сообщений, постановке и проверке цифровой подписи, вычислении кодов аутентичности (MAC). При использовании одного и того же алгоритма результат шифрования зависит от ключа. Для современных алгоритмов сильной криптографии утрата ключа приводит к практической невозможности расшифровать информацию.

Если ключ имеет длину, равную самому сообщению или еще длиннее, то расшифровать послание, не зная ключа, в принципе невозможно. Остается организовать защищенную передачу ключей, а это как раз и обеспечивает квантовые линии связи. Однако пока дистанция передачи данных для таких линий слишком коротка: из-за тепловых шумов, потерь, дефектов в оптоволокне фотоны не «выживают» на больших расстояниях.

Следует иметь в виду, что максимальная длина канала связи, позволяющего использовать метод квантовой криптографии, составляет всего лишь чуть больше сотни километров. Поэтому ученые из Российского квантового центра разрабатывали способ значительно увеличить эту дистанцию [6,7,8].

1.2 Основы криптографической защиты сигналов

Квантовая криптография – метод защиты коммуникаций, основанный на принципах квантовой физики. В отличие от традиционной криптографии, которая использует математические методы, чтобы обеспечить секретность информации, а в квантовой криптографии информация переносится с помощью объектов квантовой механики. Процесс отправки и приёма информации всегда выполняется физическими средствами, например, при помощи электронов в электрическом токе (Рис.1) или фотонов в линиях волоконно-

оптической связи (Рис.2). Подслушивание может рассматриваться как изменение определённых параметров физических объектов – в данном случае, переносчиков информации. Например, при переходе электрона обратно в состояние с меньшей энергией излучается фотон hv (Рис.1), который квантовой системе связи является носителем информации [1.5].

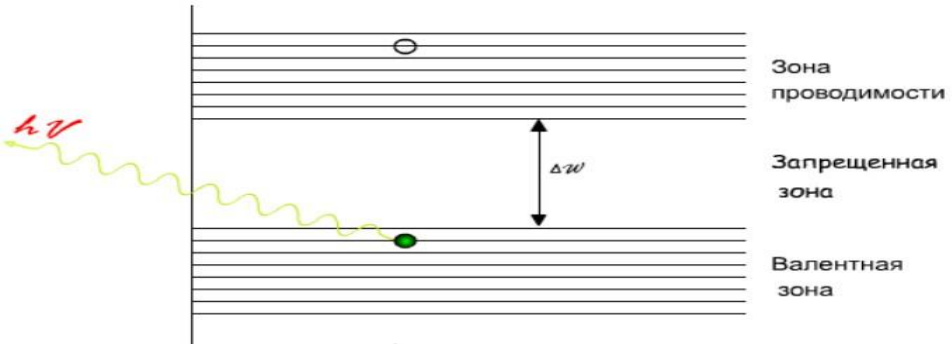

Рисунок 1 – График излучения фотона hv

Кроме того, следует учитывать существенное влияние квантомеханических эффектов на процессы переноса, так как квантовые свойства характерны для микроскопических объектов, классический пример – элементарные частицы (электрон, фотон) [5].

Рисунок 2 – Фотон в линии волоконно-оптической связи

1.3 Интернет. Меры защиты

- Браузер. Браузеры работают в двух направлениях: первое для получение полезной информации, а второе для слежки, получение личной, ценной информации. К примеру, можно привезти идентификационные файлы (куки-файлы) и браузерная дактилоскопия. Gooqle Microcoft – они работают над способами идентификации, которые используются в криптографической защите, в которых учитываются не только параметры персонального домашнего компьютера, но и Ваши данные о пользовании браузерами на планшетах и смартфонах. [3,5]

Одна из экстренных мер – это использование программы Tor Browser Bundle.

Программа объединяет ваши данные в зашифованный пакет и пересылает его через некую всемирную добровольческую сеть, состоящую из 3000 серверов. Таким образом он скрывает ваше местонахождение и затрудняет прочтение ваших зашифрованных данных.

Есть также «виртуальная частная сеть» (VPN) – это еще один уровень защиты, в котором информация передаваемые на вешние компьютеры шифруется с помощью квантового вентиля. Объединяя услуги Tor и (VPN), можно обеспечить защиту.

- Электронная почта. Включить дополнительные средства безопасности. К нему можно отнести программу Stellar Wind, накапливающий метаданные по электронной почте. Формировалась база списков контактов из почтовых аккаунтов сотен миллионов человек. Скорость наращивания этой базы составляла 250 млн пользователей e-mail в год, которое привело на разрушение двух служб, которые обеспечивали довольно высокий уровень защиты. [6], но уровень секретности будут циркулировать только среди пользователей конкретной службы. Следует иметь в виду. что эти стандартные протоколы в электронной почте, не позволяют прятать ту информацию, которая входит в метаданные.

Для защиты информации используется способ безопасного распространения секретных ключей, основанный на применении алгоритма открытого распределения ключей Диффи-Хеллмана. Алгоритм позволяет двум сторонам получить общий секретный ключ, по незащищенному каналу от прослушивания, но защищённый от подмены канал связи. Этот ключ может быт ь использован для шифрования дальнейшего обмена с помощью алгоритма симметричног о шифрования.

WI- FI. Уязвимость стандарта 802.11 является то, что третье лицо может настроиться на ваш канал и перехвотить информацию между компьютером и роутером. Для защиты используется системы WEP или WPA. Системы кодируют сообщения, проходящие между компьютером и точкой доступа [4]

К экстренным мерам для защитить своей переписки от посторонних глаз используют PGP (Pretty Good Privacy). Каждый пользователь получает пару ключей к шифровке – публичный ключ для кодирования и частный ключ для раскодирования. Публичный ключ доступен каждому, в то время как частный ключ пользователь хранит при себя. Посылающая сторона шифрует свое письмо с помощью публичного ключа принимающей стороны. Поскольку ключи имеются только у посылающей и принимающей стороны, это сообщение не может расшифровать никто из оказавшихся на пути этого письма, включая и провайдера [2,3].

1.4 Технология квантовой связи

Квантовая технология – область физики, в которой используются специфические особенности квантовой механики, прежде всего квантовая запутанность. Цель квантовой технологии состоит в том, чтобы создать системы и устройства, основанные на квантовых принципах, к которым обычно относят следующие:

- Дискретность (квантованность) уровней энергии (квантово-размерный эффект, квантовый эффект Холла);
- Принцип неопределённости Гейзенберга;
- Квантовая суперпозиция чистых состояний систем; - Квантовое туннелирование через потенциальные барьеры; - Квантовую сцепленность состояний.

К возможным практическим реализациям относят квантовые вычисления и квантовый компьютер, квантовую криптографию, квантовую телепортацию, квантовую метрологию, квантовые сенсоры, и квантовые изображения [1,4].

Технология квантовой криптографии опирается на принципиальную неопределённость поведения квантовой системы, выраженную в принципе неопределённости Гейзенберга – невозможно одновременно получить координаты и импульс частицы, невозможно измерить один параметр фотона, не исказив другой.

Из выше сказанного следует, что, используя квантовые явления можно спроектировать и создать такую систему связи, которая всегда может обнаруживать подслушивание. Это обеспечивается тем, что попытка измерения взаимосвязанных параметров в квантовой системе вносит в неё нарушения, разрушая исходные сигналы, а значит, по уровню шума в канале легитимные пользователи могут распознать степень активности перехватчика.

Кроме того, сохранность тайны передаваемых данных напрямую зависит от интенсивности вспышек света, используемых для передачи. Слабые вспышки, хоть и делают трудным перехват сообщений, все же приводят к росту числа ошибок у легального

пользователя, при измерении правильной поляризации. Повышение интенсивности вспышек значительно упрощает перехват путём расщепления начального одиночного фотона (или пучка света) на два: первого по-прежнему направленному легальному пользователю, а второго анализируемого злоумышленником. Легальные пользователи могут исправлять ошибки с помощью специальных кодов, обсуждая по открытому каналу результаты кодирования.

Следует отметить. что решение многих таких задач уже требуетна практике интернета в будущем, Например, алгоритм Шора позволяет за секунды взламывать самые современные шифры, а алгоритм Лова Гровера принципиально снижает сложность поиска в больших объемах данных [9, 10, 13, 14.]

2 Квантовые вентили (квантовые логические элементы)

2.1 Принцип использования квантовых вентилей в криптографической защите

В квантовых вычислениях используются квантовые элементы – вентили (гейты), которые выполняют основные квантовые операции. Выстраивая их композиционно, можно производить требуемые квантовые вычисления над кубитами. Квантовые вентили математически представляются унитарными матрицами, в которых число кубитов, подаваемых на вход и получаемых на выходе должно быть одинаковым.

В отличие от классических логических вентилей, на входы квантовых вентилей подаются не бинарные сигналы, а векторы состояний, которые состоят из кубитов.

Рассматривается принцип использования квантовых вентилей в системе безопасной передачи сигналов как эффективный метод криптографической защиты на основе квантовых явлении (суперпозиция и запутанность).

В некоторых вариантах, сохранение целостности данных или пресечь работу программ отслеживающих Ваших сообщении, для их обнаружения и исправления ошибок можно осуществить за счет особого расположения кубитов в пространстве: и как правило, контрольные кубиты располагается вокруг тех, которые выполняют вычисления и при этом необходимым условием являетя соблюдения когерентности [10,11].

3 Квантовая криптография для будущего интернета.

Безопасность киберпространства в будущем Интернете должна быть гарантирована, поскольку это совокупность всех информационных систем и информационная среда для выживания человека. Для решения растущей проблемы безопасности в киберпространстве квантовая криптография становится первым соображением.

Кабель и свет являются основными носителями современной интернеткоммуникации. Классическая криптосистема грубо делится на два вида: криптосистемы с симметричным ключом и криптосистемы с асимметричным ключом. Для этих двух криптосистем их безопасность в основном основана на сложности вычислений.

Однако быстрое развитие аппаратного обеспечения и предлагаемые новые усовершенствованные алгоритмы создали беспрецедентные проблемы для безопасности классических криптосистем. Более того, быстрое развитие квантовых вычислений также привело к тому, что многие сложные задачи классической математики стали разрешимыми в области квантовой физики. Например, DLP и задача целочисленной факторизации были решены в 1994 году. Таким образом, изучение квантовых криптографических протоколов станет неотъемлемой частью вопросов безопасности киберпространства для будущего Интернета [12, 13,14].

Основанная на квантовой механике и классической криптографии, квантовая криптография является новой в области криптографии. По сравнению с классической криптографией, ее основными преимуществами являются безусловная безопасность и обнаружение перехвата. Эти характеристики могут решить важнейшую проблему безопасности киберпространства для будущего интернета. В частности, квантовая криптография обеспечивает безопасность для различных приложений (например, интернета вещей и умных городов [11]) в киберпространстве для будущего интернета. Результаты нашего экспериментального анализа показывают безусловную безопасность и обнаружение квантовой криптографии, что делает ее подходящей для будущего интернета.

Список использованных источников

1. Сергеенко В.С., Баринов В.В. Сжатие данных, речи, звука и изображений в телекоммуникационных системах. Издательское предприятие Радио Софт. Москва 2014. С.35 -85

2. Бернард Скляр. Цифровая связь. Теоретические основы и практическое применение. Москва, Санкт-Петербург, Киев: -2007 С.800 - 826

3. Шитов С.Б «Популярная механика» Цифровая оборона Технологии. 2014. № 3

4. Дэвид Дарлинг Телепортация: прыжок в невозможное / Дэвид Дарлинг. - Москва: Эксмо, 2008. - С. 300

5. Килин С. Я. «Квантовая информация / Успехи Физических Наук.» - 1999. - Т. 169. - С. 507-527

6.Румянцев К.Е., Плёнкин А.П. Экспериментальные испытания телекоммуникационной сети с интегрированной системой квантового распределения ключей // Телекоммуникации. 2014. № 10. С. 11 - 16

7. Плёнкин А. П. Использование квантового ключа для защиты телекоммуникационной сети. Технические науки - от теории к практике. 2013. № 28. - С. 54-58

8. Шитов С.Б «Популярная механика». Запутать распутанное. Наука2016. № 2

9. Нильсен М., Чанг И. Квантовые вычисления и квантовая информация. - М.: Мир, 2006. – С. 824

10. Шитов С.Б «Популярная механика». Технологии. 2018. № 5

11. Валиев К. А., Кокин А. А. Квантовые компьютеры: надежды и реальность. - Ижевск: РХД, 2004. С. 320

12.Shor P. W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer // Foundations of Computer Science: Conference Publications. - 1997. - P. 1484 – 1509.

13. С Сысоев. Квантовые вычисления - СпбТУ. Курс лекци. Алгоритм Гровера. Июнь. 2021. С.15-17

УДК 004.05

РАЗРАБОТКА ЛАБОРАТОРНОЙ РАБОТЫ ПО ИЗУЧЕНИЮ ТЕХНОЛОГИИ RFID

Амангельдинов Арслан Русланович
arslan.amangeldinov98@gmail.com
Магистрант кафедры «Радиотехника, электроника и телекоммуникации»
ЕНУ им. Л.Н.Гумилева, Нур-Султан, Казахстан
Научный руководитель – Н.А. Бурамбаева

В статье представлен цикл создания лабораторной работы по изучению технологии RFID в лабораторном стенде. Процесс разработки работы включает исследование технических особенностей оборудования, ознакомление с программным обеспечением «Flowcode», моделирование и тестирование созданной работы.

1. Исследование блока технологии RFID

Разработка лабораторной работы будет осуществляться с изучения блока RFIDмодуля, который изображен на рисунке 1. Он состоит из:

1) микроконтроллера, в который будет записана программа для управления устройствами
2) RFID-модуля
3) ЖК-дисплея для вывода информации