Доклад

Квантовое шифрование. Квантовая передача информации

Шалыгин Георгий Эдуардович

Содержание

Список иллюстраций

Список таблиц

1 Введение

В современном мире информация является одним из самых ценных ресурсов. Ее защита от несанкционированного доступа является одной из важнейших задач информационной безопасности. Традиционные методы шифрования, основанные на математических алгоритмах, становятся все более уязвимыми перед развитием квантовых компьютеров.

Квантовое шифрование - это новое направление в криптографии, которое использует квантовые свойства физических систем для обеспечения абсолютной секретности передаваемой информации [1].

1.1 Цели и задачи

- Изучить принципы и алгоритмы квантовое шифрование. Познакомиться с понятием квантовой передачи информации.
- Задачи доклада:
  - Рассмотреть основные понятия квантового шифрования и квантовой передачи информации.
  - Рассмотреть основные протоколы квантового шифрования.
  - Обсудить перспективы развития квантового шифрования и квантовой передачи информации.

1.2 Краткий обзор основных понятий

Квантовая криптография - это метод защиты информации, основанный на принципах квантовой механики. Она использует квантовые свойства физических систем, такие как квантовая запутанность и квантовая телепортация, для обеспечения абсолютной секретности передаваемой информации.

Квантовая передача информации - это метод передачи информации, основанный на принципах квантовой механики. Она использует квантовые свойства физических систем, такие как квантовая запутанность и квантовая телепортация, для передачи информации с высокой скоростью и надежностью.

Основные понятия квантового шифрования и квантовой передачи информации:

- **Квантовое состояние** - это состояние квантовой системы, которое может быть описано набором вероятностей.
- **Квантовая запутанность** - это состояние двух или более квантовых систем, в котором эти системы остаются связанными друг с другом, даже если они находятся на расстоянии друг от друга.
- **Квантовая телепортация** - это процесс передачи квантового состояния от одной квантовой системы к другой без передачи самих частиц.

2 Квантовая криптография

Квантовая криптография представляет собой отрасль криптографии, которая использует принципы квантовой механики для обеспечения безопасности в обмене и защите информации. Этот раздел подробно рассмотрит основы квантовой криптографии, ключевые протоколы, преимущества и недостатки этой технологии.

2.1 Основы квантовой криптографии

Квантовая криптография основывается на основных принципах квантовой механики, таких как суперпозиция и квантовая запутанность, для обеспечения безопасности передачи информации.

В общем случае, протокол квантового шифрования включает в себя следующие этапы[4]:

1. **Генерация секретного ключа**. На этом этапе Alice и Bob генерируют секретный ключ, используя один из основных протоколов квантового шифрования.
2. **Классическая криптография**. На этом этапе Alice и Bob используют классический метод шифрования для шифрования сообщения с использованием секретного ключа.
3. **Передача сообщения**. На этом этапе сообщение передается по открытому каналу связи.

4. **Расшифровка сообщения**. На этом этапе Bob расшифровывает сообщение с использованием секретного ключа.

Существует несколько основных протоколов квантового шифрования. Наиболее известными являются следующие:

- **Протокол BB84**[2] - это протокол квантового шифрования, который использует квантовую запутанность для генерации секретного ключа.
- **Протокол Ekert-91**[1] - это протокол квантового шифрования, который использует квантовую нелокальность для генерации секретного ключа.
- **Протокол B92**[2] - это протокол квантового шифрования, который использует квантовую телепортацию для генерации секретного ключа.

2.2 Основные протоколы квантового шифрования

2.2.1 Протокол BB84

Первым и одним из наиболее известных алгоритмов квантового шифрования был протокол BB84, разработанный в 1984 году Чарльзом Беннеттом и Жильом Брассаром[1]. Протокол BB84 является одним из первых протоколов квантового шифрования и был важным шагом в развитии квантовой криптографии. Рассмотрим его на примере поляризации фотонов.

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.

Так поляризация фотонов может быть ортогональной, диагональной или циркулярной. Измерение одного вида поляризации рандомизирует другую составляющую. Таким образом, если отправитель и получатель не договорились между собой, какой вид поляризации брать за основу, получатель может разрушить посланный отправителем сигнал, не получив никакой полезной информации.

Сообщение	1	1	0	1	0	1
Базис	+	×	×	+	+	+
Поляризация	|	\	/	|	–	|

В качестве источника света может использоваться светоизлучающий диод или лазер. Свет фильтруется, поляризуется и формируется в виде коротких импульсов малой интенсивности. Поляризация каждого импульса модулируется отправителем произвольным образом в соответствии с одним из четырех перечисленных состояний.

Рассмотрим два базиса: горизонтально-вертикальный(+) и диагональный (x). В каждом их них выбираем состояния, соответствующие 0 и 1 (например поляризация 0^o и 45^o кодируют 0, а 90^o и 135^o кодируют 1).

Состояния внутри одного базиса ортогональны, но состояния из разных базисов — попарно неортогональны. Эта особенность протокола позволяет определить возможные попытки нелегитимного съёма информации.

Шаги алгоритма следующие[3]:

1. Алиса шифрует передаваемую строку битов с помощью фотонов, поляризованных согласно договорённости (описанной выше). Для каждого бита она случайно выбирает базис: + или x.

2. Боб принимает полученные импульсы и декодирует. Для каждого импульса (считаем, фотона) он выбирает случайно базис (+ или x) и измеряет состояние фотоно в данном базисе.

   Здесь работает следующий квантовый механизм. Если фотон был поляризован в базисе + и измерен в том же базисе, то получатель однозначно узнает закодированный бит. Если же для измерения был выбран базис x, то есть один из фильтров: 45^O или 135^o, свет проходит через эти фильтры с вероятностью $\frac{1}{2}$, то есть закодированный бит узнать не получится. Этот принцип отражен на fig. 2.1.

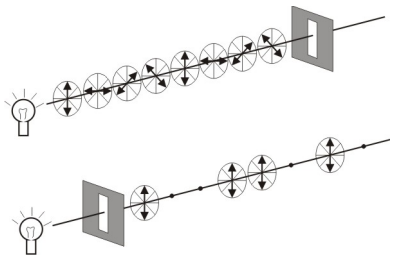

Рис. 2.1: Измерение поляризации

3. После оба участника обмениваются последовательностью выбора базисов для поляризации и измерения поляризации фотонов. Из вышесказанного следует, что биты, закодированные и прочитанные в одних базисах, будут известны обоим участникам. Эти биты и принимаются как общий секретный ключ.

Детекция ошибок

Эффективный способ обнаружения и исправления ошибок заключается в перемешивании и разбиении последовательностей Алисы и Боба на блоки.

Он был предложен 1991 году Чарльзом Беннетом[4].

Основная идея состоит в проверке чётности блоков: разбивают на блоки и проверяют на чётность в несколько итераций, уменьшая каждый размер именно тех блоков, чётность которых не совпала. Итерации производят, пока не обнаружат и не исправят ошибки. Наиболее мелкие блоки отбрасываются при обнаружении в них ошибки. В результате вероятность ошибки в полученной последовательности ничтожно мала.

2.2.2 Протокол B92

Протокол B92 основан на принципе неопределённости. Носителями информации являются 2-х уровневые системы, называемые кубитами (квантовыми битами). В отличие от своего предшественника, данный протокол может использовать неортогональные квантовые состояния. Чарльз Беннет разработал данный

протокол, чтобы показать принципиальную возможность такого разделения ключа[3].

2.2.3 Протокол Ekert-91 (E91)

Протокол Ekert-91 - это один из первых и наиболее известных протоколов квантовой криптографии, разработанный Артуром Экертом в 1991 году. Этот протокол использует свойства квантовой механики для создания безопасного ключа между двумя сторонами. Давайте рассмотрим его подробно[2].

Шаг 1: Подготовка состояний кубитов (фотонов)

1. Алиса и Боб начинают с подготовки пары фотонов, где каждый фотон может находиться в одном из двух состояний: вертикальная поляризация или горизонтальная поляризация.
2. Специально подбирая определенные углы, они создают пары фотонов, такие что, если один фотон вертикально поляризован, то другой горизонтально поляризован, и наоборот. Это создает ЭПР-пары (где ЭПР означает Эйнштейн-Подольский-Розен, которые представили в статье 1935 года одноимённый парадокс).

Шаг 2: Отправка и измерение фотонов

1. Алиса и Боб сохраняют по одному фотону из каждой пары для себя и отправляют остальные фотоны друг другу через открытый канал.
2. Алиса и Боб измеряют поляризацию фотонов в своих руках, используя фильтры, которые могут измерять поляризацию в вертикальном и горизонтальном направлениях.

Шаг 3: Создание ключа

1. Теперь, когда Алиса и Боб измерили фотоны, они сравнивают результаты. Если Алиса измерила вертикальную поляризацию, а Боб горизонтальную (и наоборот) для одного и того же фотона, они сохраняют это как бит 1.

2. Если поляризации совпали (вертикальная с вертикальной или горизонтальная с горизонтальной), они сохраняют это как бит 0.
3. Повторяя этот процесс для всех отправленных фотонов, они создают общий ключ из последовательности битов.

Протокол Экерта-91 использует свойство квантовой корреляции, позволяющее создавать безопасные ключи, так как любые попытки перехвата изменят состояние фотонов и будут замечены.

В 1964 году Джон Белл доказал, что любая теория локально скрытой переменной должна удовлетворять выведенному им неравенству Белла. Однако, эксперименты, проводимые с 1972 года убедительно показали, что теория квантовой механики данное неравенство нарушает и посему является теорией без локально скрытых параметров. Именно благодаря этому факту квантовые криптографические протоколы на ЭПР-парах способны определить вмешательство криптоаналитика в процесс передачи данных, т.к. наличие криптоаналитика в квантовомеханической системе вносит в неё скрытый параметр, что влечет за собой выполнение неравенства Белла.

2.3 Физическое воплощение технологий

2.3.1 Первая реализация

В 1989 г. все те же Беннет и Брассар в Исследовательском центре IBM построили первую работающую квантово-криптографическую систему. Она состояла из квантового канала, содержащего передатчик Алисы на одном конце и приемник Боба на другом, размещенные на оптической скамье длиной около метра в светонепроницаемом полутораметровом кожухе размером 0,5х0,5 м. Собственно квантовый канал представлял собой свободный воздушный канал длиной около 32 см. Макет управлялся от персонального компьютера, который содержал программное представление пользователей Алисы и Боба, а также злоумышленника.

В 1989 г. передача сообщения посредством потока фотонов через воздушную среду на расстояние 32 см с компьютера на компьютер завершилась успешно. Основная проблема при увеличении расстояния между приемником и передатчиком - сохранение поляризации фотонов.

2.3.2 Современные исследования

Активные исследования в области квантовой криптографии ведут IBM, GAP-Optique, Mitsubishi, Toshiba, Национальная лаборатория в Лос-Аламосе, Калифорнийский технологический институт, молодая компания MagiQ и холдинг QinetiQ, поддерживаемый британским министерством обороны.

В IBM продолжаются фундаментальные исследования в области квантовых вычислений, начатые группой Чарльза Беннетта. Ими занимается принадлежащая корпорации лаборатория Almaden Research Center. О практических достижениях IBM в квантовой криптографии известно немногое - эти работы мало рекламируются.

Исследователям из Лос-Аламоса удалось передать фотонный ключ по оптоволокну на расстояние 48 км со скоростью в несколько десятков килобитов в секунду. Этого достаточно, чтобы соединить между собой отделения банка или правительственные учреждения.

Созданная при участии Женевского университета компания GAP Optique под руководством Николаса Гисина совмещает теоретические исследования с практической деятельностью. Специалистам этой фирмы удалось передать ключ на расстояние 67 км из Женевы в Лозанну с помощью почти промышленного образца аппаратуры. Этот рекорд был побит корпорацией Mitsubishi Electric, передавшей квантовый ключ на расстояние 87 км, правда, на скорости в 1 байт/с.

Исследования в области квантовой криптографии ведутся и в европейском исследовательском центре Toshiba Research Europe Limited (TREL), расположенном в Кембридже (Великобритания). Отчасти они спонсируются английским правительством; в них участвуют сотрудники Кембриджского университета и

Империал-колледжа в Лондоне. Сейчас они могут передавать фотоны на расстояние до 100 км. Таким образом, технология может использоваться только в пределах одного города. Есть надежда, что вскоре будут выпущены коммерческие продукты.

Также ведутся исследования по производству источника отдельных фотонов.

2.4 Преимущества и недостатки квантового шифрования

Преимущества квантового шифрования:

1. **Высокая степень безопасности:** Одним из главных преимуществ квантового шифрования является его высокий уровень безопасности. Оно основано на фундаментальных принципах квантовой механики, и любые попытки перехвата информации будут изменять состояние квантовых битов (квантовых ключей) и моментально обнаруживаться.
2. **Невозможность взлома существующих ключей:** Если ключ был правильно создан и обменен с использованием квантовой криптографии, тогда даже будущие атаки с более мощными вычислительными машинами не помогут злоумышленникам взломать этот ключ.
3. **Безопасность относительно квантовых вычислений:** Квантовое шифрование предоставляет защиту от будущих квантовых вычислений, которые могли бы разгадать современные классические шифры.

К недостаткам можно отнести следующие:

1. **Требования к инфраструктуре:** Реализация квантового шифрования требует специализированных устройств, включая квантовые каналы и квантовые приборы для подготовки и измерения квантовых состояний. Это может быть дорого и сложно внедрить.
2. **Квантовая дистанция:** Квантовая связь ограничена квантовой дистанцией, то есть расстоянием, на котором квантовые состояния могут быть

надежно переданы. Это ограничение может быть преодолено с использованием ретрансляторов, но добавляет сложности.

3. **Проблемы с производительностью:** В некоторых случаях создание и измерение квантовых состояний может быть неэффективным и затратным процессом, что влияет на производительность системы.
4. **Зависимость от классической связи:** Несмотря на квантовую безопасность, для управления квантовыми каналами и передачи ключей всегда требуется классическая связь, которая подвержена классическим методам атак.
5. **Требует обеих сторон:** Для использования квантовой криптографии обе стороны должны иметь соответствующее оборудование и обладать знаниями в области квантовой механики.

3 Квантовая передачи информации

3.1 Квантовые ключи

Квантовые ключи – это одна из основных технологий квантовой передачи информации. Она позволяет двум сторонам создавать общий квантовый ключ с высокой степенью безопасности. Процесс создания квантовых ключей включает в себя следующие шаги:

- **Подготовка состояний кубитов:** Стороны подготавливают пары кубитов (квантовых битов) с использованием спиновой энтанглированности. Это означает, что изменение состояния одного кубита автоматически изменяет состояние другого кубита в паре.
- **Отправка и измерение:** Половина каждой пары кубитов передается другой стороне, которая измеряет их состояния, используя квантовые измерительные приборы.
- **Создание ключа:** После измерения кубитов стороны сравнивают результаты и используют их для создания общего ключа. Если результаты измерения совпадают, это используется как бит 0, и если они различаются, это бит 1.

3.2 Квантовые ретрансляторы (Quantum Repeaters)

Квантовые ретрансляторы используются для увеличения квантовой дистанции, то есть расстояния, на котором можно передавать квантовые состояния. Это особенно важно для долгосрочных квантовых коммуникационных систем

и сверхдлинных расстояний. Квантовые ретрансляторы работают следующим образом:

- Когда квантовое состояние приближается к пределу дальности, его состояние измеряется ретранслятором.
- Ретранслятор создает новое квантовое состояние, которое затем передается дальше. Это позволяет продлить дальность передачи без ухудшения квантовой состояния.

Основная причина, почему квантовые состояния ухудшаются с увеличением расстояния, связана с феноменом деградации сигнала.

С квантовыми состояниями (например, фотонами), передаваемыми на большие расстояния, происходит деградация сигнала по следующим причинам:

1. **Рассеяние фотонов:** Фотоны могут рассеиваться во время передачи, что приводит к их потере или размыванию. Это может происходить из-за взаимодействия фотонов с окружающей средой, такой как волоконные оптические кабели.
2. **Аттенюация:** Фотоны могут потерять энергию, когда они двигаются по оптическим волокнам или другим средам, что снижает их интенсивность.
3. **Дисперсия:** Дисперсия может привести к искажению состояния фотонов, так что они становятся менее определенными, что усложняет точное измерение и восстановление состояния.
4. **Воздействие на окружение:** Взаимодействие фотонов с окружающей средой, такое как фотоны, попадающие в атмосферу или другие объекты, также может привести к изменению их состояния.

Ретрансляторы используются для устранения или компенсации этих потерь и искажений. Они работают следующим образом:

1. Ретрансляторы перехватывают квантовое состояние, когда оно приближается к пределу дальности, на которой оно может быть надежно передано.

2. Затем ретранслятор создает новое квантовое состояние и передает его дальше. Это новое состояние имеет меньше потерь и искажений, чем исходное, так как оно создается ближе к месту назначения.
3. Процесс повторяется, пока квантовое состояние не достигнет конечной точки. Каждый ретранслятор улучшает состояние, увеличивая дальность передачи.

Таким образом, ретрансляторы позволяют значительно увеличить квантовую дистанцию и обеспечивают более надежную передачу квантовых состояний на большие расстояния.

3.3 Квантовые сети (Quantum Networks)

Квантовые сети объединяют квантовые каналы и устройства в общую инфраструктуру. Они позволяют эффективно управлять квантовыми коммуникациями и передачей данных. Квантовые сети включают следующие компоненты:

- **Квантовые репитеры:** Квантовые репитеры помогают усилить и переслать квантовые состояния через большие расстояния.
- **Квантовые коммутаторы:** Квантовые коммутаторы позволяют маршрутизировать квантовые состояния в сети, определяя путь передачи.
- **Центры обработки квантовой информации:** Центры обработки квантовой информации выполняют функции обработки и манипулирования квантовыми состояниями.
- **Защита и аутентификация:** Сети также включают механизмы защиты и аутентификации для обеспечения безопасности.

Квантовые каскадные системы позволяют бесконечно расширить дальность передачи квантовых состояний. Они предоставляют специализированные устройства и алгоритмы, которые обеспечивают непрерывную передачу квантовых состояний на длинные расстояния.

4 Выводы

В заключении нашего доклада о квантовом шифровании и квантовой передаче информации, подчеркнем следующие ключевые выводы:

1. Квантовое шифрование и квантовая передача информации представляют собой передовые подходы к обеспечению безопасности коммуникаций и защите информации.
2. Принципы квантовой механики, такие как спиновая энтанглированность и непрекращающаяся передача, обеспечивают уровень безопасности, недостижимый с использованием классических криптографических методов.
3. Технологии, такие как квантовые ключи, квантовые ретрансляторы и квантовые сети, играют ключевую роль в реализации квантовой передачи информации и обеспечении ее эффективности.
4. Квантовое шифрование защищает от будущих квантовых вычислений, что делает его перспективной областью для обеспечения безопасности в будущем.
5. Несмотря на свои преимущества, квантовое шифрование и квантовая передача информации требуют специализированных знаний и инфраструктуры для реализации.
6. Квантовая коммуникация открывает новые горизонты в области информационной безопасности и может стать основой будущих защищенных коммуникационных систем.

В целом, квантовое шифрование и квантовая передача информации представляют собой важный шаг в развитии средств защиты информации и обеспечения

надежности коммуникаций в современном мире. Эти технологии обещают революционизировать область криптографии и информационной безопасности, открывая новые возможности и вызовы.

Список литературы

1. Баженов В.В. Квантовая криптография и квантовые коммуникации. Физматлит, 2017. 324 с.
2. Скворцов О. Квантовая информация и квантовая криптография. Физматлит, 2012. 212 с.
3. Андерсен Н.А. Квантовая криптография. Наука, 2007. 324 с.
4. Бунин А.В. Протоколы квантового шифрования: обзор и перспективы. 3-е изд. Квантовая физика и квантовые технологии, 2021. 20 с.