Квантовое шифрование. Квантовая передача информации.

Common information

discipline: Основы информационной безопасности
group: НПМ6д-02-21
author: Старков Н.А.

Введение

Квантовая криптография – подраздел криптографии, который использует принципы квантовой механики для 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.

Проблемы

1. Современные методы шифрования могут быть подвержены атакам со стороны мощных компьютеров, таких как квантовые. Это вызывает необходимость в разработке более защищенных систем.
2. Классические методы криптографии, основанные на математических сложностях, могут быть нарушены с помощью квантовых алгоритмов.
3. Квантовые системы требуют высоких технологий и значительных ресурсов для их создания и поддержания, что может затруднить их внедрение в повседневную практику.
4. На данный момент не существует общепринятых стандартов для квантового шифрования и передачи информации, что затрудняет интеграцию этих технологий в существующие системы.

Цели

1. Создание новых алгоритмов для квантового шифрования, которые обеспечивают высокий уровень безопасности для передачи данных.
2. Оценка существующих криптографических систем на предмет их устойчивости к квантовым вычислениям и разработка новых подходов для повышения их защиты.
3. Создание протоколов квантовой передачи информации.

4. Анализ практической применимости: Оценка реальных сценариев использования квантового шифрования и передачи информации в различных отраслях.

Гипотезы

1. Квантовое шифрование обеспечивает более высокий уровень безопасности.
2. Квантовая передача информации может быть реализована в реальных условиях.
3. Предполагается, что более сложные квантовые алгоритмы шифрования будут более устойчивыми к атакам со стороны квантовых компьютеров.

Алгоритм работы квантовой криптографии

Квантовая криптография - это метод безопасной передачи сообщений с использованием принципов квантовой механики. Эта технология использует свойства запутанных частиц, чтобы гарантировать, что любая попытка перехвата или подслушивания сообщения будет немедленно обнаружена.

Квантовая криптография была успешно продемонстрирована в лабораторных экспериментах и в настоящее время используется в ограниченном количестве коммерческих приложений в рамках тестирования:

Безопасные банковские и финансовые операции Связь с государственными органами Оборонные предприятия Электроэнергетическая сеть

Для обеспечения безопасности передачи информации, используется протокол BB84, разработанный Чарльзом Беннетом и Жильом Брассардом в 1984 году. Протокол включает использование случайно выбранных базисов (набор состояний) для измерения состояний кубитов (основная единица квантовой информации, аналогичная классическому биту, который может принимать значения 0 или 1).

Процесс передачи информации в квантовой криптографии основан на двух основных принципах: невозможности измерения состояний квантовой системы без изменения этих состояний и невозможности создания копии квантовых состояний. Таким образом, при попытке перехвата и прослушивания информации, ее состояние изменяется, что может быть замечено.

1. Отправитель (Алиса) и получатель (Боб) имеют устройства, которые могут создавать запутанные частицы.
2. Алиса отправляет одну из запутанных частиц получателю, а другая частица остается у Боба.
3. Алиса кодирует свое сообщение, измеряя состояние вращения своей частицы и отправляя эту информацию Бобу.
4. Боб декодирует сообщение, сравнивая состояние своей частицы с состоянием отправленной частицы.
5. Если кто-то попытается перехватить сообщение (Ева), процесс измерения частицы изменит ее состояние, предупреждая Алису и Бобу о том, что сообщение было скомпрометировано.

Достоинства

Достоинства и недостатки квантового шифрования Квантовая криптография предлагает несколько преимуществ по сравнению с традиционными криптографическими методами:

1. Обеспечивает безопасность, поскольку опирается на фундаментальные принципы квантовой механики, обеспечивающие безопасность. Это гарантирует, что ни один злоумышленник не сможет перехватить или изменить зашифрованные данные, не будучи обнаруженным.
2. Позволяет безопасно распространять ключи шифрования с помощью КРК, гарантирующее безопасный обмен ключами и не может быть перехвачен третьей стороной. Это устраняет риск перехвата или угадывания ключей, существующий в традиционных методах.
3. Считается ориентированной на будущее, поскольку неуязвима перед потенциальными достижениями в области квантовых вычислений, которые могут нарушить традиционные методы шифрования. Используя принципы квантовой механики, она предлагает безопасное решение для долгосрочной защиты данных.
4. Используя квантовые ключи, гарантирует, что отправитель и получатель, а также любые посредники могут безопасно аутентифицировать друг друга. Это помогает предотвратить несанкционированный доступ и защищает от атак типа «человек посередине».

В целом, преимущества квантовой криптографии заключаются в ее способности обеспечивать надежную защиту, безопасное распределение ключей, защиту от достижений квантовых вычислений в будущем и надежные механизмы аутентификации.

Недостатки

Потенциальные недостатки и ограничения, связанные с квантовой криптографией, включают следующее:

1. Протоколы КРК ограничены максимальным расстоянием, на котором они могут быть реализованы. Это связано с потерей квантовых состояний через передающую среду. После определенного расстояния количество потерь становится слишком большим, чтобы надежно установить безошибочное распределение ключей.
2. Для реализации квантовой криптографии требуется сложное и высокочувствительное оборудование. Установка и обслуживание таких систем может быть дорогостоящим и сложным делом.
3. Стоимость систем квантовой криптографии может быть значительно выше по сравнению с традиционными криптографическими методами.
4. Квантовая криптография не защищена от всех возможных атак. Уязвимости могут существовать в реализации криптографических протоколов, а также потенциальные недостатки в используемых физических устройствах или методах измерения.
5. Квантовая криптография исходит из предположения, что инфраструктура, используемая для передачи и получения квантовых состояний, является безопасной и надежной. Любая компрометация в этой инфраструктуре, например вмешательство в среду передачи или атака на аппаратные компоненты, может подорвать гарантии безопасности, обеспечиваемые квантовой криптографией.
6. Квантовая криптография еще не совместима с существующими классическими криптографическими системами. Это создает проблемы с точки зрения интеграции квантовых криптографических протоколов в существующие сети или системы связи. Это требует значительных обновлений или отдельной инфраструктуры, предназначенной для квантовой связи.

Будущее квантовой криптографии

В будущем квантовая криптография может стать неотъемлемой частью современной криптографической инфраструктуры.

Квантовые компьютеры находятся на ранних стадиях и нуждаются в дополнительной разработке, прежде чем широкая аудитория сможет начать использовать квантовую связь.

Обычная криптография симметричных ключей может быть подвержена угрозам со стороны квантовых компьютеров. Однако исследователи работают над разработкой новых квантово-безопасных методов шифрования, устойчивых к атакам квантовых компьютеров.

Как и со всеми новыми технологиями, будущее квантовой криптографии также будет сопряжено с вызовами и преградами. Необходимо разработать и внедрить стандарты квантовой криптографии, чтобы обеспечить совместимость и безопасность систем. Также необходимо улучшить и расширить физические и технические аспекты квантовых каналов связи.

Вывод

Квантовая криптография является новым подходом к обеспечению безопасности информации, который основан на фундаментальных принципах квантовой механики. Она предлагает новые методы шифрования и передачи данных, которые потенциально более устойчивы к атакам и взлому, чем классическая криптография.

Уникальные свойства квантовой криптографии делают ее перспективной альтернативой для обеспечения безопасности информации. Однако, на данный момент, квантовая криптография все еще находится в стадии исследования и разработки. Она требует использования специальных квантовых устройств, которые являются сложными в производстве и дорогими в разработке. Кроме того, требует наличия надежных средств передачи квантовых сигналов, таких как оптические волокна.

Тем не менее, квантовая криптография предлагает новые возможности для создания безопасных систем передачи информации. Она может быть особенно полезна для защиты важных данных. В долгосрочной перспективе, с развитием технологий и уровнем их доступности, квантовая криптография может стать всемирным стандартом для обеспечения безопасности интернет-коммуникаций.

Литература

1. Квантовая криптография / шифрование [Электронный ресурс]: TAdviser. URL: https://www.tadviser.ru/index.php/Статья:Квантовая_криптография_(шифрование) (дата обращения: 01.07.2023).
2. Quantum Cryptography: An Overview of the Future of Encryption. URL: https://cybertalents.com/blog/quantum-cryptography (дата обращения: 04.07.2023).
3. BB84 [Электронный ресурс]: URL: https://ru.wikipedia.org/wiki/BB84 (дата обращения 04.07.2023).