Доклад

Квантовое шифрование. Квантовая передача информации

Шалыгин Г. Э.

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Шалыгин Георгий Эдуардович
- студент НФИ-02-20
- Российский университет дружбы народов

Вводная часть

Актуальность

- Информация является одним из самых ценных ресурсов. Ее защита от несанкционированного доступа является одной из важнейших задач информационной безопасности.
- Развитие квантовых вычислений угрожает классическим криптографическим методам, таким как RSA и ECC. Поиск новых методов шифрования становится актуальным.
- Квантовое шифрование обеспечивает более высокий уровень безопасности при передаче данных, попытка перехвата может быть обнаружена.

Цели и задачи

- Цель: изучить принципы и алгоритмы квантового шифрования.
- Задачи доклада:
  - Рассмотреть основные понятия квантового шифрования и квантовой передачи информации.
  - Познакомиться с основными протоколами квантового шифрования.
  - Обсудить перспективы развития квантового шифрования и квантовой передачи информации.

Основы квантовой криптографии

- Основана на передаче квантовых состояний и принципах квантовой механики.
- В общем случае, протокол квантового шифрования включает в себя следующие этапы:

    1. **Генерация секретного ключа**. На этом этапе Alice и Bob генерируют секретный ключ, используя один из основных протоколов квантового обмена ключами.
    2. **Шифрование сообщения**. На этом этапе Alice и Bob используют классические метод симметричного шифрования для шифрования сообщения с использованием секретного ключа.
    3. **Передача сообщения**.
    4. **Расшифровка сообщения**.

Поляризация фотонов

- Поляризация, колебание электрического поля $\vec{E}$. Пример линейно поляризованных волн показан на рисунке.
- a, b – базис +, горизонтально-вертикальный (H/V); $45^o, 135^o$ – базис $\times$, и диагонально-антидиагональный (D/A).

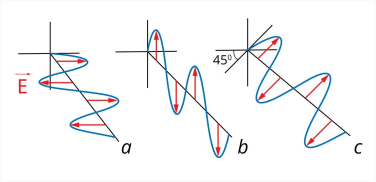

Figure 1: Поляризованные волны

Передача бита с помощью фотона

- Рассмотрим два базиса: горизонтально-вертикальный(+) и диагональный ($\times$).

  Пусть — и $\diagup$ соответствует 0, | и $\diagdown$ соответствуют 1.

- Два участника: один поляризует фотон и отправляет другому. Другой измеряет поляризацию, случайно выбирая базис.

- 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 $\times$, 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 рисунке.

Иллюстрация измерения поляризации

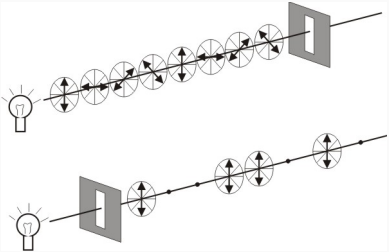

Figure 2: Измерение поляризации

Протокол BB84 (1984 г., Ч. Беннетт, Ж. Брассар)

Шаги алгоритма следующие:

1. Алиса шифрует передаваемую строку битов с помощью фотонов, поляризованных согласно договорённости. Для каждого бита она случайно выбирает базис: + или $\times$.

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

Протокол BB84 (Ч. Беннетт, Ж. Брассар, 1984 г.)

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

Протокол BB84 (Ч. Беннетт, 1992 г.)

- Может использовать неортогональные квантовые состояния.
- Показывает принципиальную возможность такого подхода.
- Использует меньше состояний.

Протокол E91 (А. Эркерт, 1991 г.)

- Основан на квантовой запутанности.
- Создаются ЭПР-пары фотонов, фотоны из которых отправляются Алисе и Бобу.
- Если базис совпал, то бит сохраняется.

Состояние	$\|0\rangle$	$\left\|\frac{3\pi}{6}\right\rangle$	$\left\|\frac{\pi}{6}\right\rangle$	$\left\|\frac{4\pi}{6}\right\rangle$	$\left\|\frac{2\pi}{6}\right\rangle$	$\left\|\frac{5\pi}{6}\right\rangle$
Бит	0	1	0	1	0	1

Figure 3: Отдельные состояния

$$|S_0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle\left|\frac{3\pi}{6}\right\rangle + \left|\frac{3\pi}{6}\right\rangle|0\rangle\right)$$
$$|S_1\rangle = \frac{1}{\sqrt{2}}\left(\left|\frac{\pi}{6}\right\rangle\left|\frac{4\pi}{6}\right\rangle + \left|\frac{4\pi}{6}\right\rangle\left|\frac{\pi}{6}\right\rangle\right)$$
$$|S_2\rangle = \frac{1}{\sqrt{2}}\left(\left|\frac{2\pi}{6}\right\rangle\left|\frac{5\pi}{6}\right\rangle + \left|\frac{5\pi}{6}\right\rangle\left|\frac{2\pi}{6}\right\rangle\right)$$

Figure 4: Запутанные состояния

Детекция ошибок

- Способ был предложен 1991 году Ч. Беннетом.
- Последовательности Алисы и Боба перемешиваются и разбиваются на блоки.
- Основная идея состоит в проверке чётности блоков: блоки проверяют на чётность в несколько итераций, уменьшая каждый размер именно тех блоков, чётность которых не совпала. Достаточно мелкие блоки отбрасываются при обнаружении в них ошибки.
- Неравенства Белла для алгоритмов на ЭПР-парах.

Реализация

- 1989 г., Беннет и Брассар, Исследовательский центр IBM. Квантовый канал длиной 32 см.
- 48 км, Национальная лаборатория в Лос-Аламосе.
- 67 км, GAP Optique.
- 87 км, Mitsubishi Electric. Скорость – 1 байт/с.
- Команда исследователей из Китая, Сингапура, Великобритании смогла с помощью спутника «Мо-Цзы» объединить города Наньшань и Дэлинха: 1120 км.

Вывод

Вывод

- Передовая, развивающаяся область, защищено от атаки с помощью квантовых вычислений.
- Другой уровень защищенности по сравнению с классическими подходами.
- Сложные в реализации технологии.
- ResearchAndMarkets: рынок квантовой криптографии оценен в $93,1 млн.