ВВЕДЕНИЕ. ОБЩИЕ ПОНЯТИЯ КВАНТОВОЙ КРИПТОГРАФИИ

ВАДИМ РОДИМИН
СТАРШИЙ НАУЧНЫЙ СОТРУДНИК ГРУППЫ КВАНТОВЫХ КОММУНИКАЦИЙ РОССИЙСКОГО КВАНТОВОГО ЦЕНТРА

ЧЕМ МЫ ЗАНИМАЕМСЯ?

Наша группа довольно успешно занимается разработкой устройства **квантовой криптографии** с 2015-го года, делая продукт, который будет готов к работе уже в существующих телекоммуникационных сетях. Кроме этого, наша группа занимается разработкой генератора случайных чисел, но в основном все крутится вокруг квантовой криптографии.

В частности, я занимаюсь устройством, предназначенным для учебных целей. С помощью этого устройства можно делать быстрое прототипирование какого-то квантового распределения ключа, а также изучать квантовую физику и квантовую криптографию.

ЧТО ТАКОЕ КВАНТОВАЯ КРИПТОГРАФИЯ?

Нам нужно передать сообщение из пункта A в пункт B (Alice и Bob). Это сообщение должно быть конфиденциальным, его никто не должен прослушать и перехватить. Для этого его нужно зашифровать. И вопрос криптографии именно в том, как же зашифровать это сообщение.

Классификация ключей:

1. Асимметричные ключи — ключи, используемые в асимметричных алгоритмах. Но их можно расшифровать
2. Шифр Вернама (одноразовый блокнот) — основан на том, что сообщение кодируется побитовым xor с одноразовым ключом, длина которого не меньше длины передаваемого сообщения

Если использовать 2-ой вариант шифрования, то остается вопрос: как сделать так, чтобы у Алисы и Боба был один и тот же ключ? Это сделать сложно, но именно квантовая криптография позволяет передавать ключ от Алисы к Бобу и быть уверенным, что его никто не перехватит.

По сути, информация, передаваемая с помощью ключа, шифруется в квантовых состояниях элементарных частиц. Эти состояния обладают фундаментальной хрупкостью, такой, что если кто-то их подслушает или подсмотрит — он разрушит эти квантовые состояния.

Таким образом, квантовая криптография позволяет передавать информацию с полной конфиденциальностью и секретностью. Если кто-то попытается подсмотреть или перехватить информацию, то мы увидим это в виде возрастающих ошибок. Квантовая криптография — генератор случайных чисел, который генерирует одинаковую случайную последовательность сразу в двух местах. Эту случайную последовательность потом можно использовать как ключ. Но сразу информацию генерировать нельзя.

ОПИСАНИЕ ПРОТОКОЛА BB84

Информация кодируется в поляризации фотона. Если мы приготовим вертикальную или горизонтальную поляризацию и будем измерять ее прибором с вертикальными или горизонтальными осями, то, скажем так, базисы фотона и прибора совпадут, и прибор покажет все правильно — либо вертикальную поляризацию, либо горизонтальную.

Но если на прибор с прямым базисом подать диагональную поляризацию, то прибор покажет 50 на 50.

На этом и основана «игра» по распределению квантового ключа:

- Алиса выбирает случайное значение: 0 или 1
- Алиса выбирает случайным образом между двумя базисами
- Алиса отправляет одиночный фотон, закодированный в выбранном базисе
- Боб измеряет полученный фотон в случайном базисе
- Боб получит верное значение, только если использует тот же базис, что и Алиса
- После завершения передачи и Алиса и Боб сообщают друг другу базисы
- Алиса и Боб выкидывают те случаи, в которых они использовали разные базисы
- У Алисы и Боба остается идентичный секретный ключ

То есть, квантовое распределение ключа — одинаковая генерация ключа в обоих пунктах A и B.