ТЕХНИЧЕСКАЯ РЕАЛИЗАЦИЯ КВАНТОВОЙ КРИПТОГРАФИИ И ОБЛАСТИ ПРИМЕНЕНИЯ

ВАДИМ РОДИМИН
СТАРШИЙ НАУЧНЫЙ СОТРУДНИК ГРУППЫ КВАНТОВЫХ КОММУНИКАЦИЙ РОССИЙСКОГО КВАНТОВОГО ЦЕНТРА

КАК ЖЕ ПРОИСХОДИТ РЕАЛИЗАЦИЯ КВАНТОВОЙ КРИПТОГРАФИИ?

Выбор объекта

Сначала нам нужно выбрать объект, который мы можем использовать для передачи информации. Как я уже говорил, это может быть поляризация фотона.

Почему фотон? Потому что у фотона много шансов дойти от Алисы к Бобу и не потеряться по пути. У других электронных частиц таких шансов практически нет.

Оптоволокно позволяет фотону долетать очень далеко и не потеряться. Однако, есть проблемы с передачей большого объема энергии. Учитывая, что угол преломления не может превышать 90°, получаем, что при достаточно большом угле падения свет должен полностью отражаться в среде с большим n:

$$\theta_c = \arcsin\left(\frac{n_2}{n_1}\right)$$

Выбор длины волны

Нужно выбрать такую длину волны, которая, опять же, с большой вероятностью дойдет из пункта А в пункт В и не потеряется.

2 механизма, обеспечивающие наш выбор:

- Рэлеевское рассеяние, когда фотон, летящий в чем-то, начинает рассеиваться на неоднородностях этого чего-то. В данном случае, чем длиннее волна, тем меньше рэлеевское рассеяние. Поэтому нам желательно уйти в область длинных волн
- Поглощение в инфракрасном спектре

Наиболее подходящая длина волны — 1,5 мкм.

Для кодирования информации необязательно использовать поляризацию. Если мы используем поляризацию, то это будет поляризационное кодирование. Но есть, например, еще фазовое кодирование (для этого нужно вспомнить, что такое интерференция).

Интерференция

Свет — это волна. Если 2 волны одной частоты и примерно одинаково распространяются, то они могут друг друга гасить или усиливать. Если 1 волна приходит с «горбом» и 2 тоже с «горбом», то они будут друг друга усиливать; если же 1 волна приходит с «горбом», а 2 — с «впадиной» в противофазе, то они будут друг друга взаимно ослаблять. Получается интерференционная картина в виде чередования ярких и темных полос, колец и т. д.

Будет ли интерференция конструктивной или ослабляющей, определяется разницей длин путей двух волн или разницей фаз этих волн.

Если волны приходят в данную точку экрана:

1. В одинаковой фазе, то они взаимно усиливают друг друга, и на экране в этом месте наблюдается светлая полоса
2. В противофазе, то они взаимно ослабляют друг друга, и на экране в этом месте наблюдается темная полоса

Интерферометр Маха-Цендера

Интерферометр — прибор для наблюдения интерференции.

Как он работает? Мы берем лазер, он испускает луч. Мы разделяем этот луч с помощью полупрозрачного зеркала на 2 части. В конце есть еще полупрозрачное зеркало, где лучи сходятся и интерферируются. Луч, пришедший из одного плеча, может пройти насквозь и проинтерферироваться лучом, отразившемся от зеркала, пришедшего из другого плеча. Так мы получаем интерференционную картину.

Если плечи будут одинаковы, оптическая разность хода между этими лучами будет равна 0, то у нас всегда будет реализовываться интерференционный максимум в первом детекторе, а во втором детекторе, соответственно, будет интерференционный минимум. А если мы будем вносить какую-то оптическую разность хода между этими лучами, то мы будем проходить через череду интерференционных максимумов и минимумов.

А что будет, если на этот интерферометр послать одиночный фотон? Он не может пойти по двум плечам сразу, потому что фотон не делится. Но, тем не менее, даже для фотона будет продемонстрирована некоторая интерференционная картина. Например, если оба плеча будут

одинаковы, то у нас всегда будет «кликать» первый детектор, а второй детектор будет молчать.

Фазовое кодирование

- Алиса при помощи фазового модулятора создает разность фаз между импульсами
- Если разность фаз между импульсами равна 0, то на детекторе D1 создается конструктивная интерференция, при этом на детекторе D2 — деструктивная интерференция (значение бита 0)
- Если Алиса создает фазовый сдвиг равный π, то на детекторе D1 будет деструктивная интерференция, а на детекторе D2 — конструктивная (значение бита 1)
- Второй базис обеспечивается введением со стороны Алисы еще двух фазовых сдвигов: π/2 и 3π/2
- Боб, в свою очередь, может решать в каком базисе проводить измерения. Боб и Алиса выбирают базис измерения и базис приготовления совершенно случайно

Таким образом, сохраняется вся последовательность действий протокола BB84.