УДК 535.513.1

Моделирование квантово-криптографических систем

Зар Ни Аун[1,2]

[1]Московский физико-технический институт (государственный университет)

В настоящее время квантовая криптография возникает для защиты информации с помощью ключей. В первой экспериментальной демонстрации установки квантового распределения ключей проведенной в 1989 в лабораторных условиях, передача осуществлялась через открытое пространство на расстоянии тридцати сантиметров. После первых экспериментов Мюллера и др. в Женеве с 1995 г. до 2006 г. расстояние передачи было увеличено с 1,1км до 184 км [1].

1. Квантовый протокол BB84

В протоколе BB84 используются 4 квантовых состояния фотонов.

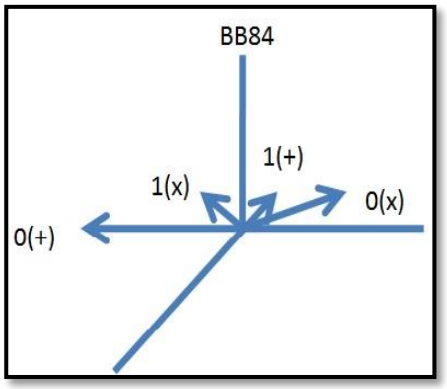

Рис.1. Состояния поляризации фотонов, используемые в протоколе BB84 .

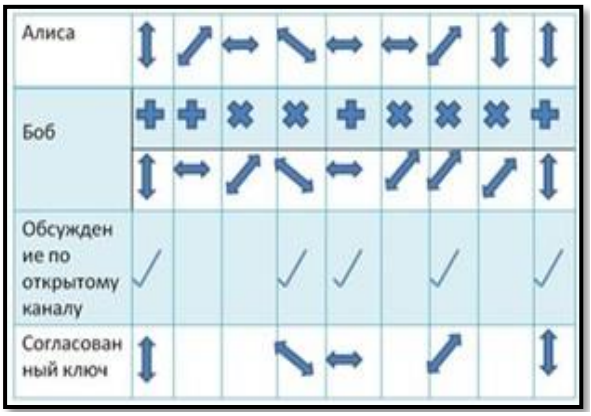

Рис. 2. Формирование квантового ключа по протоколу BB84 .

Алиса отправляет Бобу поляризованные фотоны. И Боб измеряет сообщение Алисы. После этого Боб кодирует информации с базисами поляризации ("+ "или "x") и посылает Алисе сообщение. Алиса принимает сообщение. Возможны два направления поляризаторов, вертикальный и горизонтальный. При вертикальном направлении поляризатора фотонов в 90°, его битное значение становится 1 а для поляризации фотона в 0°, его битное значение становится 0. При диагональных направлениях поляризаторов фотонов в 45°, его битное значение будет равно 0, и если поляризация фотона равна 135°, то его битное значение становится равным 1 [2]. В нашей модели первый пользователь зашифровывает информацию с помощью генератора случайных чисел реализуемом на класическом компьютере с помощью (random). Второй пользователь расшифровывает информацию с помощью этого же генератара.

Для квантовой защиты каналов будем использовать квантовый генератора случайных чисел возпроизводящий поляризации фотонов.

Литература

1. *Голубчиков Д.М., Румянцев К.Е*. Квантовая криптография принципы, протоколы, системы// Электронная библиотека МГУ. 2013.2-9с.

2. *Слепов Н.*, Квантовая криптография: передача квантового ключа. Проблемы и решения..-2006.56с.