КВАНТОВАЯ КРИПТОГРАФИЯ

Репин Степан, гр. 8307

1. ВВЕДЕНИЕ

Ключевым элементом современных компьютерных систем и средств связи является шифрование — обратимое преобразование информации, применяемое для сокрытия данных от неавторизованных лиц. Это преобразование — функция от двух переменных: собственно кодируемой информации и некоторой специальной битовой последовательности, называемой ключом. Для того, чтобы авторизованный пользователь мог расшифровать информацию, ему необходимо знать ключ.

Если для шифрования и дешифрования используется один и тот же ключ, то такая система криптографии называется симметричной. Дальнейшее развитие привело к появлению асимметричной криптографии. В этом случае ключ делится на две части: открытую и закрытую. Открытый ключ нужен для шифрования, а закрытый для дешифрования. Открытый ключ можно передавать по незащищенным канал связи, его перехват не позволит злоумышленнику расшифровать сообщение.

Но так как закрытый и открытый ключи все же имеют между собой взаимосвязь через специальную математическую функцию, то на самом деле теоретически возможно по открытому ключу восстановить закрытый. Но практически это нереально выполнить за конечное время на электронном компьютере, если ключи имеют достаточно большой размер (для алгоритма RSA ключ должен быть больше 2048 байт по последним рекомендациям NIST).

К сожалению, ситуация кардинально меняется, когда речь заходит о квантовых компьютерах. В 1994 году был представлен квантовый алгоритм Шора, на основе которого возможно выполнять взлом криптографической системы со скоростью, близкой к скорости шифрования. Оказывается, что квантовые компьютеры представляют реальную угрозу современной инфраструктуре безопасности (вся защита информации сейчас базируется на асимметричном шифровании).

Но и здесь наука криптографии смогла предложить решение проблемы. Заключается оно в использовании квантовых технологий, только уже не для взлома, а для сетевого распределения абсолютно стойких ключей. Таким образом, квантовая рассылка ключей позволит эффективно и удобно применять симметричное шифрование (неподдающееся взлому ни каким известным способом даже теоретически), не переживая за перехват ключа. Невозможность перехвата гарантируется законами квантовой физики.

Квантовая рассылка ключей принципиально строится на факте того, что одиночный фотон нельзя незаметно измерить (при измерении он изменится в соответствии с принципом неопределенности Гейзенберга), нельзя разделить и нельзя скопировать. Таким образом, в отличии от классических способов передачи данных незаметно прослушать информацию в канале связи невозможно.

2. ПРОТОКОЛ BB84

Первый и самый известный протокол квантового распределения ключей был предложен американцем Ч. Беннетом и канадцем Ж. Брассаром в 1984 году.

Пользователи Алиса и Боб взаимодействуют друг с другом по трем каналам: квантовому (для рассылки ключей), классическому (для обсуждения результатов, должен быть аутентифицированным) и синхронизации. Злоумышленник, Ева, имеет доступ ко все каналам.

Квантовый канал передает одиночные фотоны. Физическим уровнем может быть любой оптический канал: оптоволокно, атмосферный, спутниковый и т.д. Кодируется информация обычно с помощью изменения поляризации фотона (но можно применять и другие характеристики фотона). Не вдаваясь в физические детали, можно сказать, что из принципа квантово-волнового дуализма фотон можно рассматривать как электро-магнитную волну, имеющую некоторое переменное значение вектора напряженности электрического поля $\vec{E}$. Причем $\vec{E}$ является гармонической функцией и в пространстве представляет собой винтовую линию. Конкретные характеристики этой лини в плоскости, перпердикулярной направлению распространения волны, и описываются поляризацией. На рис. 2.1 показаны две волны с круговой (сверху) и плоской поляризацией (снизу).

Фотоны поляризуются линейно под углами $0°$, $45°$, $90°$ и $135°$. Так получаются 4 возможных состояния, образующих 2 базиса: вертикально-горизонтальная поляризация и диагональная поляризация.

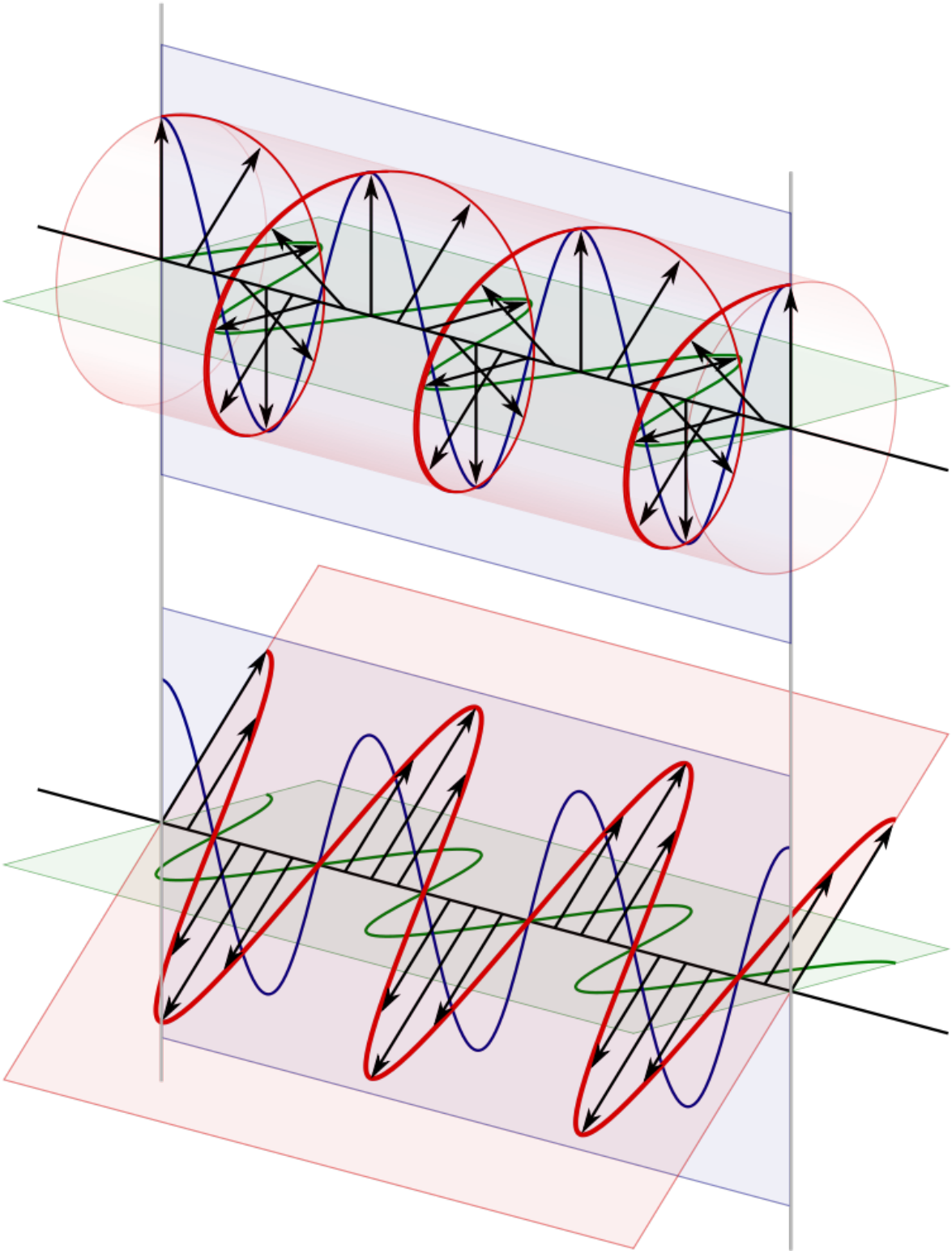

Рис. 2.1 Волны с круговой и плоской поляризацией

Алгоритм генерации ключей следующий (см. рис. 2.2:

1. Алиса и Боб договариваются, как будут интерпретировать состояния фотонов (например, 0 для вертикальной поляризации, 1 для горизонтальной в первом базисе, и аналогично во втором базисе).

2. Алиса отправляет по квантовому каналу одиночные фотоны в случайно выбранном состоянии.

3. Боб измеряет полученные фотоны, случайно выбирая базис. Так Боб получит сырой ключ, содержащий в среднем 25% ошибок.

4. Боб по открытому каналу сообщается для каждого переданного состояния, в каком базисе проводилось измерение, но не сообщает сам результат измерения.

5. Алиса по открытому каналу отвечает, в каких случаях выбранный базис верен.

6. Если базис совпал, то бит оставляют; иначе, игнорируют. У Боба появляется просеянный ключ.

7. Процесс повторяют, пока у Боба не будет ключа требуемой длины.

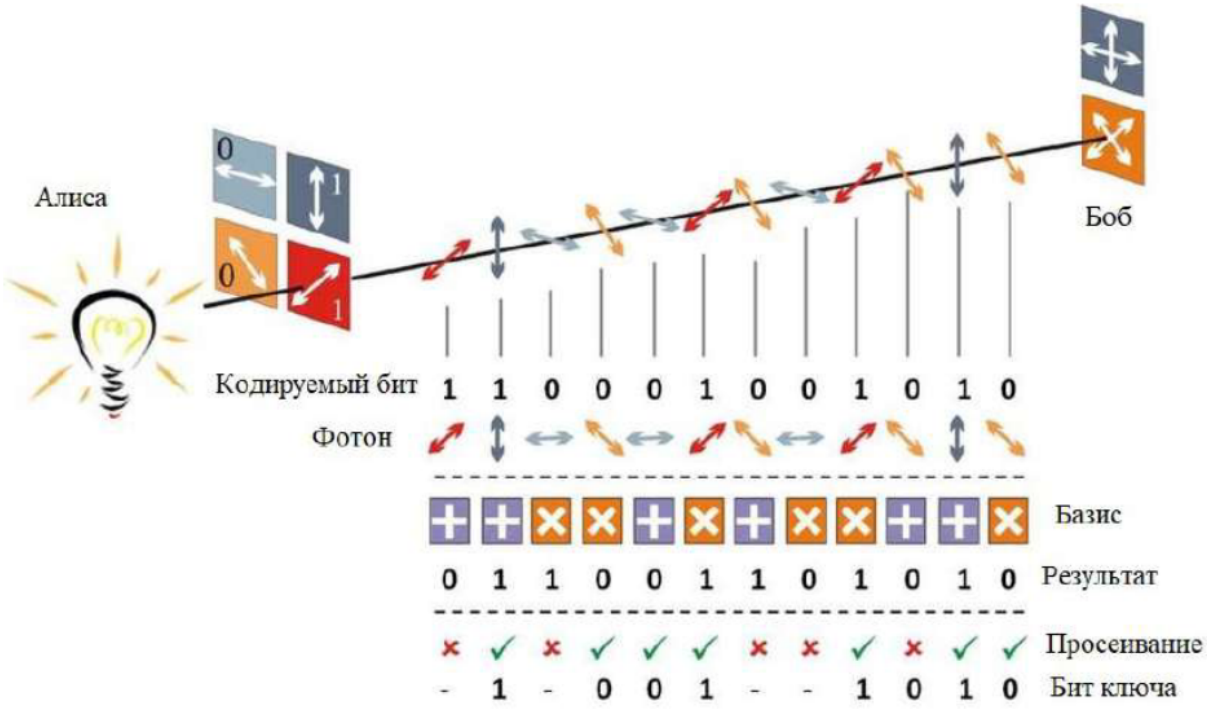

Рис. 2.2 Алгоритм генерации квантового ключа

Ошибки возникающие в канале из-за шумов могут быть исправлены специальной процедурой, если ошибок не больше 11%.

3. ПРОБЛЕМЫ ТЕХНИЧЕСКОЙ РЕАЛИЗАЦИИ

Для работы квантового распределения ключей необходимы сложные физические приборы: источник одиночный фотонов (не больше и не меньше, иначе обмен ключами будет подвержен атакам) и детектор одиночных фотонов.

В настоящее время однофотонные источники не созданы и на практике используются слабокогеретные импульсы, генерируемые многофотонными источниками. Соответственно есть вероятность того, что импульс будет содержать >1 фотона, которые несут одну и ту же информацию.

В то же время есть трудности и в создании детекторов фотонов. Они либо имеют плохую эффективность (фотон может быть пропущен), либо могут генерировать ложные срабатывания, либо неприменимы нормальных атмосферных условиях.