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. Подробнее об этих свойствах ниже. 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 (линейной) 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. Или:

1. $+$: $|x\rangle = |0\rangle, |y\rangle = |1\rangle$
2. $\times$: $|u\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |v\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

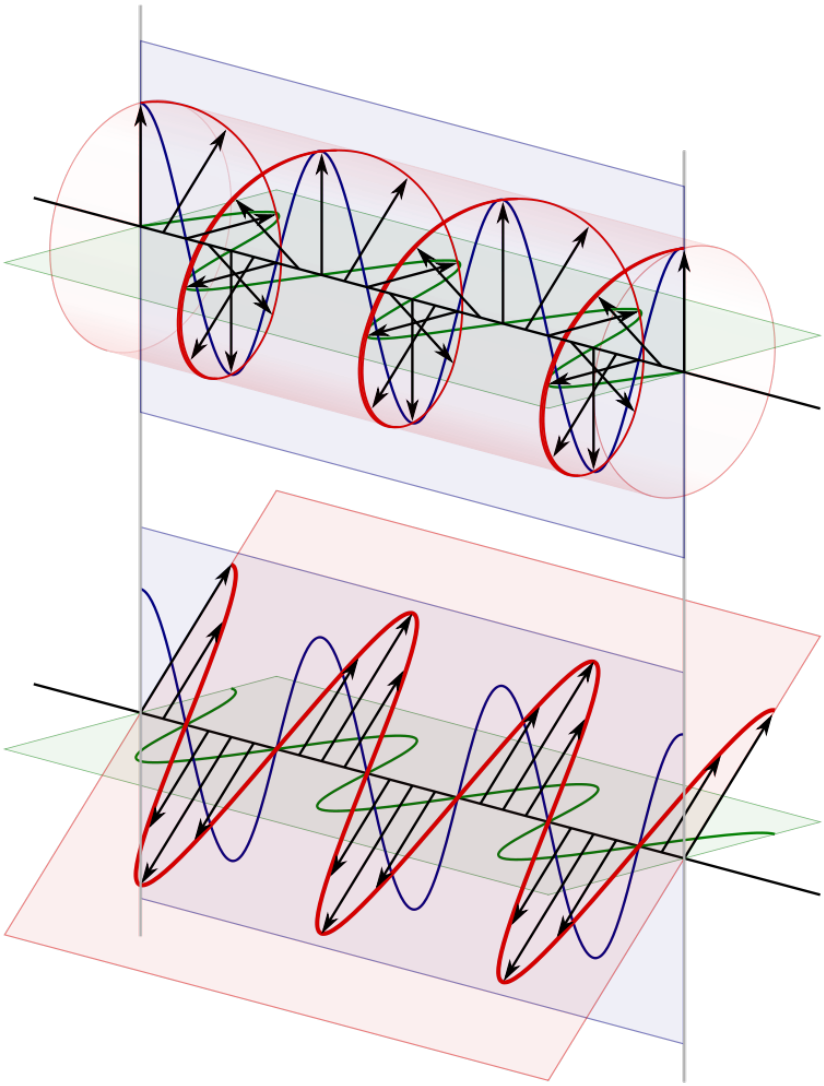

Рис. 2.1 Волны с круговой и плоской поляризацией

Алгоритм генерации ключей следующий (см. рис. 2.2):

1. Алиса и Боб договариваются, как будут интерпретировать состояния фотонов. Например,
   - $|x\rangle$, если базис $+$ и бит равен 0,
   - $|y\rangle$, если базис $+$ и бит равен 1,
   - $|u\rangle$, если базис $\times$ и бит равен 0,

– $|v\rangle$, если базис $\times$ и бит равен 1,

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

3. Боб измеряет полученные фотоны, случайно выбирая базис. Причем, каждое измерение дает достоверный результат из-за ортогональности состояний внутри каждого базиса. Так Боб получит сырой ключ, содержащий в среднем 25% ошибок (для каждого полученного фотона возможны 4 варианта состояния, из которых верный, т.е. который выбрала Алиса, только один).

4. Боб по открытому каналу сообщает 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.

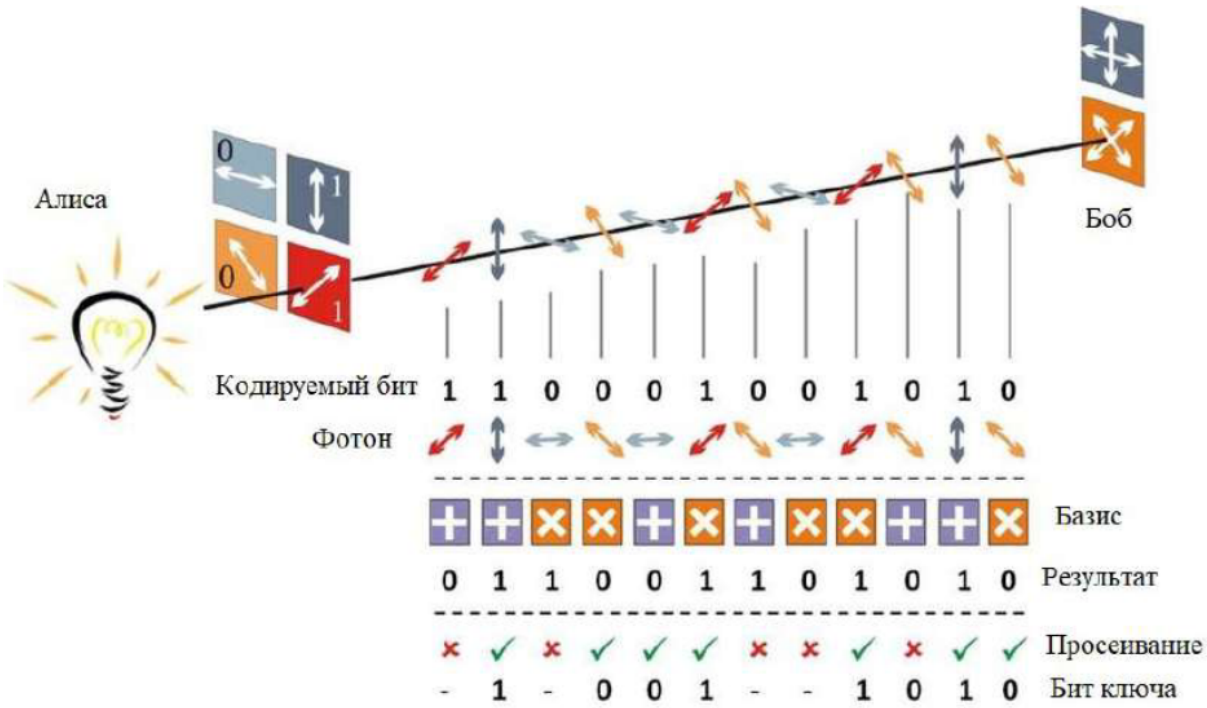

Рис. 2.2 Алгоритм генерации квантового ключа

В идеальном случае, когда в канале нет помех и отсутствуют действия со стороны перехватчика, битовые строки у Боба и Алисы будут совпадать в тех позициях, где базис, используемый Алисой, совпал с базисом, выбранным Бобом. В противном случае (были помехи или воздействие злоумышленника) Алиса и Боб должны раскрыть около половины своих битовых строк. Тогда в соответствии с центральной предельной теоремой из теории вероятностей можно получить достаточно точную оценку ошибки во всей битовой строке. Если ошибка не превысила некоторый заданный предел (обычно около 11%, что следует из доказательства стойкости BB84 при использовании границы Шеннона для коррекции ошибок), то Алисе и Бобу необходимо произвести коррекцию ошибок и усиление секретности. Иначе передача данных считается скомпрометированной и требуется повторить ее с начала.

3. КОРРЕКЦИЯ ОШИБОК И УСИЛЕНИЕ СЕКРЕТНОСТИ

Коррекция ошибок наиболее эффективно выполняется с помощью случайных кодов и эта процедура относится к классической теории информации, потому что работа производится над битовыми строками. Зная вероятность ошибки в канале Q и желаемую длину ключа n Алиса генерирует избыточный код, состоящий из

$$2^{n(C_{clas}-\delta)}$$

кодовых слов (каждый длинной n), где $C_{clas} = 1 - h(Q)$ – пропускная способность канала с ошибками, $\delta \Rightarrow 0$ при больших n, а $h(Q)$ — бинарная энтропия Шеннона. к этой последовательности Алиса присоединяет свою битовую строку и передает по открытому каналу Бобу. На основе метрики Хемминга Боб выбирает ближайшее кодовое слово. А в соответствии с теоремой Шеннона о кодировании для канала с шумом, Боб с вероятностью 1 выберет битовую строку Алисы.

Заметим, что в ходе обмена битовыми строками, часть информации о переданном ключе по квантовому канала стала известна и Еве. Эта часть представляет собой оценку значения ключа на основе числа ошибок в сыром ключе и из процесса коррекции ошибок.

Поэтому Алисе и Бобе нужно применить специальный алгоритм для общих битовых строк, установленных при коррекции, чтобы получить ключ, который будет полностью неизвестен Еве. Для этого применяется набор универсальных хеш-функций, которые отображают n-битовые строки A в m-

битовые строки B, причем для случайно выбранно из этого набора функции и любых несовпадающих строк из A вероятность совпадения их образов не превосходит $\frac{1}{|B|}$. Итоговый секретный ключ сжимается с помощью такой универсальной хэш-функции.

4. КВАНТОВЫЕ СВОЙСТВА ОДИНОЧНОГО ФОТОНА

Выше упоминалось, что квантовая криптография основывается на некоторых принципах квантовой физике, которые не дают злоумышленнику незаметно отследить передаваемую в квантовом канале информацию. Всего свойства три:

1. нельзя произвести измерение, не изменив состояния фотона;
2. нельзя различить неортогональные квантовые состояния.
3. нельзя скопировать фотон (получить новый фотон с таким же состоянием, как и оригинальный)

Рассмотрим (1). В квантовой физике этот закон называется редукцией фон Неймана или коллапсом волновой функции: после измерения (применения оператора измерения M) фотон перейдет в одно из собственных состояний оператора измерения. При измерении $\{M_i\}$ и получении результата i фотон перейдет в состояние:

$$\rho_i' = \frac{\sqrt{M_i}\rho\sqrt{M_i}}{TrM_i\rho},$$

где ρ — исходное состояние (смешанное квантовое состояние), $TrM_i\rho$ — частичный след. Таким образом, любые попытки измерения данных в канале будут вести к помехам.

Рассмотрим (2). Для чистых состояний $|\psi_0\rangle$ и $|\psi_1\rangle$, таких что $\langle\psi_0\,|\,\psi_1\rangle = \cos\alpha \neq 0$, не существует измерения $\{M_0, M_1\}$, дающего точный результат.

Рассмотрим (3). Предположим, что существует преобразование U, клонирующее произвольное чистое квантовое состояние $|\psi\rangle$. Тогда его можно записать так:

$$U|\psi\rangle \otimes |A\rangle = |\psi\rangle \otimes |\psi\rangle,$$

где $|A\rangle$ – начальное состояние некоторой вспомогательной системы, $\otimes$ – оператор умножения тензоров. Рассмотрим его действие на базисные состояния $|0\rangle$, $|1\rangle$ и состояние $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$:

$$U|0\rangle \otimes |A\rangle = |0\rangle \otimes |0\rangle,$$
$$U|1\rangle \otimes |A\rangle = |1\rangle \otimes |1\rangle,$$
$$U(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)) \otimes |A\rangle = \frac{1}{2}(|0\rangle \otimes |1\rangle) \otimes (|0\rangle \otimes |1\rangle).$$

А с другой стороны, в силу линейности оператора U и соотношений выше:

$$U(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)) \otimes |A\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle \otimes |1\rangle \otimes |1\rangle).$$

Получилось противоречие. Но заметим, что клонирование возможно из ортогональных состояний. В таком случае, можно произвести измерение и создать новый фотон с измеренным состоянием.

5. 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.