Лекция по КВАНТОВОЙ КРИПТОГРАФИИ (II). *Дубна (15-17 апреля 2006)*

О.Д.Тимофеевская

Квантовые протоколы обмена секретным ключом: EPR -протокол

Эта вариация BB84 протокола представляет особый концептуальный, исторический и практический интерес. Идея (принадлежащая Артуру Эккерту) состоит в замене квантового канала, по которому передадаются кубиты от Алисы к Бобу, каналом, в котором от одного EPR (Эйнштейн-Подольский-Розен) - источника к Алисе и Бобу направляются фотоны из пары $|\Psi-\rangle$: один фотон-1 направляется к Алисе, а второй– фотон-2 к Бобу.

Конечно, идейно этот протокол основывается на парадоксе Эйништейн-Подольский-Розен (1935) в форме переформулированной Бомом для двухкубитов в антисимметричном состоянии (двух спинов $1/2$ с сумарным значением полного спина равным 0).

Одноразовый ключ должен представлять собой абсолютно случайную последовательность нулей и единиц, и если в протоколе BB84 эта последовательность генерируется по усмотрению Алисы, то в этом случае квантовая механика выступает идеальным ренератором такой случайной последовательности. И Алиса и Боб независимо и случайно используют два базиса: с вертикальной и горизонтальной поляризациями

$$|0\rangle \quad = \quad |\updownarrow\rangle \quad |1\rangle \quad = \quad |\leftrightarrow\rangle$$

и с наклонными под углами $\pm 45°$ поляризациями

$$|0'\rangle \quad = \quad |\nearrow\rangle \quad |1'\rangle \quad = \quad |\searrow\rangle,$$

а затем согласуют свои результаты по классическому каналу.

Алиса использует следующую кодировку битов в поляризациях:

$$0 \quad \longrightarrow \quad |\uparrow\rangle \qquad 1 \quad \longrightarrow \quad |\rightarrow\rangle$$

или

$$0 \quad \longrightarrow \quad |\nwarrow\rangle \qquad 1 \quad \longrightarrow \quad |\nearrow\rangle$$

Боб наоборот:

$$1 \quad \longrightarrow \quad |\uparrow\rangle \qquad 0 \quad \longrightarrow \quad |\rightarrow\rangle$$

или

$$1 \quad \longrightarrow \quad |\nwarrow\rangle \qquad 0 \quad \longrightarrow \quad |\nearrow\rangle$$

Запишем поляризационное состояние пары фотонов в состониии с полной нулевой поляризацией в этих базисах

$$|\Psi-\rangle_{12} = \frac{1}{\sqrt{2}}(|\updownarrow>_1|\leftrightarrow>_2 - |\leftrightarrow>_1|\updownarrow>_2) = \frac{1}{\sqrt{2}}(|\nearrow>_1|\searrow>_2 - |\searrow>_1|\nearrow>_2)$$

или

$$|\Psi-\rangle_{12} = \frac{1}{\sqrt{2}}(|0>_1|1>_2 - |1>_1|0>_2) = \frac{1}{\sqrt{2}}(|0'>_1|1'>_2 - |1'>_1|0'>_2).$$

Каким бы базисом ни воспользовалась Алиса, вероятность получить 0 (или 1) при измерении поляризации фотона $=1/2$. Таким образом, генерируется случайная последовательность битов.

Как бы далеко ни были удалены друг от друга Боб и Алиса, в каком временном порядке и какими бы методами ни производили они измерения своих фотонов в тех случаях, когда фотон Алисы окажется поляризован вертикально, фотон Боба будет иметь достоверно (с вероятностью 1) горизонтальную поляризацию, так как для этих событий его матрица плотности (условная матрица плотности) равна

$$\hat{\rho}_2 = \frac{{}_1<0|\Psi-><\Psi-|0>_1}{1/2} = |1>_2<1|,$$

то есть поляризационная волновая функция фотона Боба $|1\rangle_2$. Аналогично, для других поляризаций.

Таким образом, если Алиса и Боб выбирают один и тот же базис, то они, если подслушивание отсутствует, достоверно получают те же значения– 0 или 1. Если они выбрали разные базисы, то с вероятностью 1/2 значения битов совпадают, а с вероятностью 1/2 различны. Обмениваясь информацией о выбранных базисах, Алиса и Боб сохраняют в переданном ключе только те биты, которые были измерены в одинаковых базисах.

Внедрение Ева полностью соответствует случаю протокола BB84 и приводит к очень большой ошибке в результатах Алисы и Боба $= 25\%$.

В 1991 году А.Эккерт предложил модифицировать этот протокол, используя три базиса, что позволяет использовать соотношения из неравенств Белла для проверки наличия внедрения Евы в канал связи.

Квантовые протоколы обмена секретным ключом: протокол BB92

В 1992 Беннет заметил, что двух пар ортогональных поляризаций слишком много для того чтобы передать секретный ключ по квантовому каналу: достаточно двух неортогональных поляризаций.

В B92-протоколе Алиса распоряжается фотонами с двумя неортогональными поляризациями, например, вертикальной $|\uparrow>$ и образующей положительный угол в $45°$ градусов

с осью Ox – $|\nearrow>$. Устройства Боба позволяет выделять фотоны с поляризациями, перпендикулярными этим, а именно с образующей угол в (-45°) – $|\nwarrow>$ с осью Ox и горизонтальной – $|\rightarrow>$ поляризациями. Алиса создает случайную последовательность двоичных чисел и сопоставляет с ними поляризации фотонов по следующим правилам.
Алиса:
$$0 \quad \leftrightarrow \quad |\uparrow>, \qquad 1 \quad \leftrightarrow \quad |\nearrow>.$$

Боб создает свою случайную последовательность и сопоставляет с ними ориентации фильтров, определяющих поляризацию фотонов, которые он фиксирует:

$$0 \quad \leftrightarrow \quad |\nwarrow>, \qquad 1 \quad \leftrightarrow \quad |\rightarrow>.$$

Боб регистрирует результаты наблюдений по правилам: Y – удача, если ему удалось зафиксировать фотон, и N – неудача, если фотона зафиксировать не удалось. Если биты Алисы и Боба различны, то заведомо будет зафиксирована неудача. В случае удачи бит Боба всегда совпадает с битом Алисы. Удача регистрируется для половины одинаковых битов. Приведем пример распределения битов.

$$\left(\begin{array}{cccc} 1 & 0 & 1 & 0 \\ |\nearrow> & |\uparrow> & |\nearrow> & |\uparrow> \\ 0 & 0 & 1 & 1 \\ |\nwarrow> & |\nwarrow> & |\rightarrow> & |\rightarrow> \\ N & N & Y & N \end{array}\right)$$

Первый и четвертый биты Алисы и Боба имеют различные значения, так что в каждом из этих случаях результат Боба равен N. Во втором и третьем случаях значения битов совпадают, и с вероятностью 0.5 результат Боба будет равен Y. Конечно, нельзя предсказать заранее результат каждого измерения.

Чтобы закончить протокол Боб посылает свои результаты Y или N Алисе, не сообщая значений поляризации своих анализаторов. Это сообщение посылается по открытому каналу.

После этого Алиса и Боб оставляют только те биты, для которых результаты Боба равны Y, именно эти биты соответствуют совпадению алфавитов. В приведенном примере только третий бит передает одинаковые буквы алфавита.

Таким образом, эффективность идеальной процедуры обмена, η_Q, равна 0.25.

Внедрение Евы приведет к ошибке в 25%, если она будет, например, измерять поляризации в базисе Алисы.

В реальных ситуациях происходят определенные потери при передаче фотонов. Ева скачивает только незначительную часть передаваемых кубитов.

Хотя нельзя однозначно, не возмущая состояния, различить две неортогональные поляризации, это можно сделать за счет определенных потерь. Что было продемонстрировано экспериментально. То есть, на практике протокол с двумя поляризациями менее надежен, чем BB84.

Квантовые протоколы обмена секретным ключом: Экспериментальная реализация

Впервые предложенная схема передачи сообщений **BB84** была реализована **в 1989 году** в лаборатории IBM. Продемонстрированное устройство передавало сообщения на расстояние **30 cm.**

Опишем опыт, демонстрирующий возможность **квантоых коммуникаций с помощью коррелированных фотонных пар** [4].

Порожденный аргон-ионым лазером пучок фотонов длины волны 351 nm мощностью 350 mW, падая на кристалл β-бората бария (BBO). Это приводит к появлению пар фотонов длины волны 702 nm, с нулевой полной поляризацией.

Каждый из фотонов попадает в оптический кабель, транспортирущий их к Алисе и Бобу. В эксперименте длина каждого из кабелей была равна 500 m, а расстояние между экспериментальными устройствами, принадлежащими Алисе и Бобу равнялось 360 m.

Алиса и Боб могли анализировать поляризационные состояния своих фотонов с помощью поляризационных разделителей. Перед анализаторами помещались электро-оптический модуляторы. Они быстро (rise time $<$ 15 ns, minimum switchihg interval 100 ns) ориентировали оси анализатора по двум выбранным направлениям. Работа модуляторов управлялась квантовыми генераторами случайных сигналов **[Jennewein et al. 1999]**. Время корреляции было меньше 100 ns. Фотоны детектировались кремневыми лавинными фотодиодами. Временные анализаторы, выполненные на базе локальных персональных компьютеров, регистрировали длительность всех событий измерения как временные метки, присоединяя к этим данным сведения о положении анализаторов и результат измерения. Начало измерения инициировалось импульсом отдельного лазерного диода, посылаемого от источника Алисе и Бобу по второму световому кабелю. Только после того, как измерения заканчивались, Алиса и Боб сравнивали результаты, выделяя совпадения.

Чтобы точно фиксировать события детектирования, время, основанное на показаниях анализаторов, контролировалось рубиновыми часами. Оказалось, что стабильность каждого временного промежутка была лучше, чем 1 ns для одной минуты. Максимальная продолжительность измерения ограничивалась объемом памяти персонального компьютера (оказалось, что типичное время – это одна минута). Скорость измерения совпадений оказалась равной $\approx 1700s^{-1}$, скорость выделения отдельных событий – $\approx 35000s^{-1}$. Эти значения позволяют оценить полную эффективность слежения за каждым фотонов как 0.05, а скорость рождения пары $7{\cdot}10^5\ s^{-1}$. Система оказалась весьма устойчивой к возможным заменам фотонных пар, поскольку относительная вероятность двух пар всего лишь $\approx 3{\cdot}10^{-3}$, если выбирать события рождения двух пар внутри окна совпадений в 4 ns. Ширина окна совпадений ограничивается временем разрешения детекторов и электроники, но, принципе, может быть сведена до времени когерентности фотонов, которая обычно – величина порядка пикосекунд.

Возможности системы исследовались на пробных передачах квантовых алфавитов, сначала модернизированной процедуры Экерта, а затем – реализации BB84-протокола. В первом случае Алиса и Боб обменялись 2162 битами сырого алфавита со скоростью 420 bits/sec. Ошибка в отождествлении квантовых битов составила $3.4{\cdot}10^{-2}$. Во втором случае было зарегистрировано $\approx$ 80000 квантовых битов со скоростью 850 bits/sec., а ошибка наблюдения составила $2.5{\cdot}10^{-2}$. Эта величина обеспечивает помехоустойчивость квантового канала. После этого была осуществлена обычная схема исправления ошибок, что привело к такому результату: из $\approx$ 80000 битов с квантовой ошибкой $2.5{\cdot}10^{-2}$ Алиса и Боб использвали 0.1 часть материала для проверки устойчивости, оставшшиеся 0.9 битов для приготовления 49984 исправленных битов с уровнем ошибки 0.004. После этого Алиса передала Бобу по компьютерной сети послание объемом 40000 битов, используя побитную XOR-комбинацию битов квантового алфавита, который они получичили реализуя BB84-протокол, и битов, записавших сообщение, которое нужно передать Бобу. Получив послание Алисы, Боб побитно складывает его с имеющимся у него результатом BB84-протокола и получает то сообщение, которое хотела передать Алиса. Поясним это соотвествующими формулами. Пусть послание Алисы состоит из последовательности битов $\{m_k\}$. Результат BB84-протокола – это последовательность $\{s_k\}$. Боб получает последовательность $\{r_k = m_k \oplus s_k\}$ и преобразует ее в $\{r_k \oplus s_k\}$. Но $r_k \oplus s_k = (m_k \oplus s_k) \oplus s_k = m_k$.

Послание Алисы к Бобу содержало фотографию "Вилендорфской Венеры гордости музея Вены – статуэтку, вырезанннную из известняка примерно 24000-22000 лет до Рождества Христова. Для передачи изображения была использована матрица, содержащая $60 \otimes 90$ точек, 8 битов цветной информации на точку: 432000 битов информации, кодирующей изображение. Файл содержал дополнительную информацию, включая таблицу цветов – всего 51840 битов. Боб воспроизвел только ту информацию, которая относилась к изображению. В результате получилось изображение, которое содержало лишь несколько ошибок, которые были вызваны ошибками, оставшимися в квантовом алфавите.

Результаты эксперимента привели авторов к убеждению, что несмотря на необходимость дальнейших теоретических и экспериментальных исследований, квантовая передача сообщений с помощью коррелированных фотонов вполне может стать частью завтрашней технологии.

В работе [5] эта схема реализована уже на расстоянии 1.45 км, а в работе [6] квантовая передача ключа была осуществлена на 122 км.

Классическая криптография: криптосистема с открытым (RSA) ключом

Это асимметричная криптосистема, в которой для зашифровки и расшифровки используются совсем разные ключи.

Криптосистема с публичным **(открытым) ключом или (RSA) система** была изобретена Р.Ривестом, А.Шамиром и Л.Адлеманом (Ronald Rivest, Adi Shamir, Leonard Adleman) в 1978 году. Чтобы реализовать эту систему, не требуется никаких встреч, чтобы обменяться секретными кодами. Вместо этого отправитель и получатель используют различные ключи для шифровки и дешифровки послания. Фактически, в наше время наиболее секретные коммуникации осуществляются на основе RSA криптосистемы.

Основная идея состоит в следующем. Персона, желающая получать секретные послания, используя RSA, создает пару ключей, состоящую из "publyc key"и "private key". Она публикует публичный ключ, но держит в секрете личный ключ. Когда кто-либо хочет послать ей секретное послание, он использует публичный ключ, чтобы зашифровать его.

После получения зашифрованного текста (например, по E-MAIL), получатель расшифровывает его с помощью своего личного ключа. Трюк состоит в том, как связаны публичный и личный ключи, обеспечивая работу схемы эффективно и надежно секретно.

RSA система основана на трудности факторизации больших целых чисел.

Пусть Алиса хочет получать секретные послания от других людей. Чтобы создать пару секретных *public/private* ключей, Алиса выбирает два больших целых простых числа p и q и вычисляет произведение $n = pq$.

Потом она находит два специальных целых числа d и e, которые связаны с p и q. Целое d есть какое-либо взаимно простое число с числом $(p-1)(q-1)$ (т.е. наибольший общий делитель d и $(p-1)(q-1)$ равен 1). Целое e обратно d по модулю $(p-1)(q-1)$; т.е., $ed = 1(mod)(p-1)(q-1)$. Алиса использует эти специальные целые, чтобы составить публичный ключ из пары целых $\{e, n\}$ и личный ключ из пары целых $\{d, n\}$. Алиса публикует публичный ключ $\{e, n\}$ и держит в секрете "private"$\{d, n\}$.

Пусть Боб (или кто-то еще) хочет послать Алисе секретное сообщение. Боб может послать Алисе сообщение, и только она может его прочитать. Чтобы это сделать, Боб берет публичный ключ, распространенный Алисой, и представляет свой текст M_{text} как последовательность целых от 1 до n.

Это послание из целых $M_{integers}$ Боб шифрует по правилу:

$$E_i = M^e_{i\ (mod)n},$$

где $M_i \in M_{integers}$. Этот зашифрованный текст посылается по открытому каналу. Последний шаг в схеме – это восстановление Алисой M_i по E_i.

Работа схемы представлена в таблице:

RSA Public Key Cryptography

1. Выбрать два больших целых простых числа $p, q: \quad n = pq$.

2. Найти d взаимнопростое с $(p-1)(q-1) = \Phi(n)$.

3. Вычислить e из $ed \equiv 1_{(mod)(p-1)(q-1)}$.

4. Распространить публичный ключ, т.е. пару чисел (e, n).

5. Представить текст как M_{text} как последовательность целых $\{M_i\}$ в диапозоне от 1 до n.

6. Зашифровать $\{M_i\}$, используя публичный код

$$E_i = M^e_{i\ (mod)n}.$$

7. Расшифровать послание по правилу

$$M_i = E^d_i(mod)n.$$

8. Вернуться от $\{M_i\}$ к оригинальному тексту.

1. Существует множество формул, предлагающих вычисление простых чисел (как всех так и некоторых), хотя большинство из них ошибочны. (По этому поводу существует обзор Дадли [7].)

Например, можно вопользоваться формулой Миллса [8], который показал, что существует постоянная A, что $[A^{3^n}](modn)$-(?) простое для любого n.

Проверка того, является ли данное число простым, (например, 100-значное) осуществляется компьютером очень быстро, менее чем за минуту. Конечно, без того, чтобы выдать какие-либо его множители.

2. Число $\Phi(m)$ называется эйлеровской функцией и определяется как число положительных целых чисел, меньших m и взаимнопростых к m. Если p и q – простые, то $\Phi(n) = (p-1)(q-1)$ и числа n и $\Phi(n)$ взаимнопростые.

Найти число d взаимно простое к $r = (p-1)(q-1)$. Проверка, того, являются ли числа взаимно простыми (т.е. их наибольший обший делитель равен 1) осуществляется с помощью алгоритма Эвклида для нахождения наибольшего обшего делителя.

3. Найти число e можно по теореме Эйлера:

Пусть m и b взаимно простые, тогда

$$b^{\Phi(m)} = 1_{mod(m)}.$$

Так как d и r взаимнопростые, то $e = d^{\Phi(\Phi(n))-1}$. В самом деле, по теореме Эйлера

$$ed = d^{\Phi(\Phi(n))} = 1_{mod(\Phi(n))}$$

6. Зашифрованный текст представляет собой последовательность

$$E_i = M^e_{i\ (mod)n}.$$

7. Расшифровка

$$E_i^d(mod)n = M_i^{ed}(mod)n, \quad ed = 1 + \Phi(n)s,$$

где s- целое число. Но согласно теореме Эйлера

$$M_i^{\Phi(n)}(mod)n = 1.$$

В самом деле если M_i и n взаимнопростые, то это и есть утверждение теоремы Эйлера. Если же $M_i < n$ имеет множителем, например p , то $M_i = G*p$, где G и n взаимнопростые. Так как согласно теореме Эйлера

$$p^{(q-1)s}(mod)q = 1,$$

то

$$p^{(p-1)(q-1)s}(mod)q = 1, \quad p^{(p-1)(q-1)s} = q*j+1, \quad p^{1+(p-1)(q-1)s} = n*j+p$$

и

$$M_i^{1+\Phi(n)s}(mod)n = G*p = M_i.$$

Таким образом,

$$E_i^d(mod)n = M_i.$$

Открытый ключ –это (n,e), а секретный – это (n,d). Открытый ключ можно свободно публиковать, потому что в науке неизвестны легкие методы вычисления d,p или q по паре (pq,e), а разложение pq в произведение "методом грубой силы"потребует астрономического времени. Тем не менее следует помнить, что нет строгого доказательства невозможности легкого разложения произведения или того, что это единственный способ взлома RSA.

Существуют реализации алгоритма RSA на языке Perl, которые занимают всего три строки.

Легко видеть, что e и d в алгоритме эквивалентны. Если Алиса зашифрует сообщение своим секретным ключом, то Боб может расшифровать его с помощью открытого ключа Алисы, и тем самым убедиться, что его написала именно она. На этом принципе основан механизм цифровой подписи для электронной почты и защищенных транзакций.

Литература:

1. N.Gisin, G.Ribordy, W.Tittel, H.Zbinden. Quantum Cryptography arXiv:quant-ph/0101098 **(2001)**.

2. S.J.Lomonaco. A Talk on Quantum Cryptography or How Alice Outwits Eve. arXiv:quant-ph/0102016 **(2001)**.

3. W.Dusek, N.Lutkenhaus, M.Hendrych. Quantum Cryptography. arXiv:quant-ph/0601207 **(2006)**.

4. T.Jennewein, Ch.Simon, G.Weihs. Quantum Cryptography with Entangled Photons. arXiv:quant-ph/9912117 **(2000)**.

5. A.Poppe and et. Practical Quantum Key Distribution with Polarization Entangled Photons. arXiv:quant-ph/0404115 **(2004)**.

6. C.Gobby, Z.L.Yuan and A.J.Shields. Quantum Key Distribution over 122 km of Standard Telecom Fiber. arXiv:quant-ph ... **(2004)**.

7. U.Dudley. Formulas for Primes. Math.Mag. **56**,17-72 (1983).

8. M.R.Schoeder. Number Theory in Science and Communication. *Springer, 1985*