Лекция по КВАНТОВОЙ КРИПТОГРАФИИ (I)
Дубна (15-17 апреля 2006)

О.Д.Тимофеевская

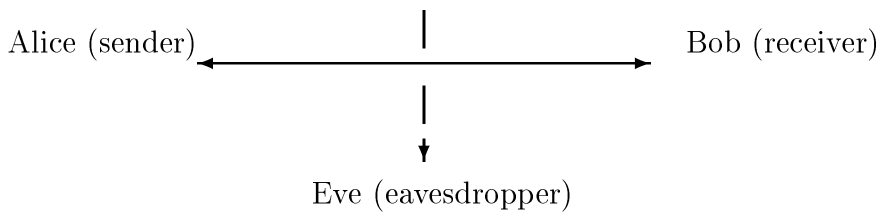
Великолепная идея

Квантовая криптография была впервые предложена как идея только в семидесятых годах прошлого столетия, хотя сама работа была опубликована только через 10 лет Виснером и Беннеттом (1985). Идея квантовой криптографии столь проста, что даже студент, первый год изучающий квантовую механику, мог бы догадаться до нее. Тем не менее только в наши дни, когда почва была подготовлена, когда фундаментальные основы квантовой механики стали рассматриваться физиками не только как странная теория с ее парадоксами, но как инструмент для инженерной науки, когда секретность информации стала чрезвычайно важной, квантовая криптография стала активно развиваться.

В квантовой механике измерение всегда возмущает систему.
(Кроме того случая, когда состояние системы совпадает с состоянием базиса, в котором производится измерение.) **Квантовая криптография** обеспечиваем новый механизм, который позволяет обменивающимся информацией сторонам **автоматически обнаружить подслушивание.** Следовательно, она дает способы обнаружения нарушения тайны коммуникации.

Введение

Две стороны – Алиса (sender) и Боб (receiver) хотят конфиденциально обмениваться информацией и быть уверенными, что "шпионка"Ева (eavesdropper) их не подслушивает. Алиса и Боб находятся на большом расстоянии друг от друга. Как они могут разговаривать и избавиться от подслушивания Евы?



В современном обществе в условиях бума электронных и телекоммуникаций с особой силой возрастают требования развития новых методов конфеденциальности связи и засекречивания информации. Вместе с тем, основная задача криптографии, которая состоит в том, чтобы обеспечить двум сторонам возможность обмениваться посланиями так, чтобы никакая третья сторона не была посвящена в тайну переписки стара как мир, о чем говорят раскопки таких древнейших цивилизаций как Месопотамия, Индия, Китай, Египет. Древние греки, например, использовли шифры, основанные на перестановке букв в тексте. Известно, что Юлий Цезарь, общаясь со своими легионами использовал, например, следующий шифр: буква A заменялась на D, буква B на E, C на F и т.д. В средние века использовались шифры, использующие одновременно и перестановки и подстановки букв.

Однако, ни один из таких шифров не является надежным, так как возможно взломать их, используя различные характеристические свойства языка, такие, например, как частота употребления различных букв и их сочетаний

Классическая криптография: симметричные криптографические схемы.

В классической схеме текст послания шифруется с помощью секретного ключа, а затем передается. Ключ должен быть надежным, чтобы расшифровка без ключа потребовала длительного времени, т.е. его было бы очень сложно взломать.

В таких схемах используется тот же самый ключ как для шифровки, так и для дешифровки. Этот ключ должны иметь только Алиса и Боб, и он распределяется по секретному каналу между ними еще до передачи секретного сообщения. Такой секретный канал может обеспечить, например, надежный курьер. Другими словам, согласно утверждению из известной 22 хитрости классической криптографии,

"Есть совершенные возможности секретных коммуникаций при том условии, что возможности секретных коммуникаций есть"

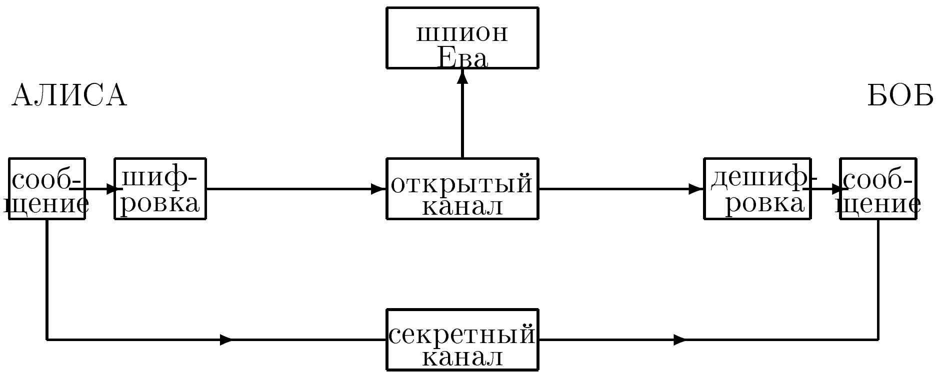


Схема классических секретных коммуникаций

Практическая надежность такой схемы при условии надежности секретного канала определяется надежностью шифровального ключа в ДАННОЕ время.

Не так давно, наиболее распространенной шифровальной системой являлась (DES) была (Date Encryption Standart) и ее разновидности, разработанная IBM. Это пример блок-шифра, когда строки фиксированной длины исходного текста трансформируются через серию операций в криптотекст той же длины. Размер блока в DES составлял 16 битов, и хотя разрабатывались ключи длиной 56-128 и даже 192 битов, в настоящее время эта система взломана и ее заменила более надежная ADS (Advanced Encrypted Standart) система, в котрой блоки имеют 128 битов и ключи могут иметь размер 128, 192 и 256 битов. (Как долго она продержится?)

Одноразовый ключ

Совершенной криптографической схемой является классическая криптографическая система, предложенная Верманом, или так как называемая схема с одноразовым ключом.

Заметим, что любое целое число в двоичной системе представляет собой последовательность 0 и 1 (двух возможных значений битов).

Рассмотрим бинарные последовательности:

011 и 111.

Первая из них представляет число 3, а вторая 7.

$$N = 2^0 x_n + 2^1 x_{n-1} + ... + 2^{n-1} x_1 = 2^{n-1} x_1 + ... + 2^0 x_n,$$

$$N = |x_1, ..., x_n\rangle$$

С помощью n битов записываются числа N от 0 до $2^n - 1$.

Если в свою очередь букву заменить числом, то любое сообщение можно рассматривать как последовательности нулей и единиц.

Итак, шифруемый текст представляет собой бинарную последовательность нулей и единиц:

$$P = P_1 P_2, P_3 ... P_n ...$$

В 1917 году Гильберт Вернам предложил невзламываемый ключ, который называется шифром Вернама или одноразовым ключом (One-time Pad). Его безусловная секретность была доказана в 1949 году Шенноном в терминах теории информации.

Секретный ключ состоит из совершенно случайной бинарной последовательности той же длины что и щифруемый текст, т.е.

$$K = K_1 K_2 K_3 ... K_n ...$$

Зашифрованный текст –это бинарная последовательность

$$C = C_1 C_2 C_3 ... C_n ...$$

где

$$C_i = P_i \oplus K_{imod2} \quad i = 1, 2, 3...$$

Например,

$$P = \quad 0110 \quad 0101 \quad 1101$$

$$K = \quad 1010 \quad 1110 \quad 0100$$

$$C = \quad 1100 \quad 1011 \quad 1001$$

Эта схема совершенна, если K - абсолютно случаен и известен только Алисе и Бобу. Но если использовать тот же самый ключ для кодировки двух различных текстов $P^{(1)}$ и $P^{(2)}$ в шифрованные тексты $^{(1)}$ и $^{(2)}$, она сразу же превращается из совершенно надежной в одну из самых легко взламываемых схем. В самом деле

$$P^{(1)} \oplus P^{(2)} = C^{(1)} \oplus C^{(2)},$$

что легко расшифровать вследствие повторяемости и закономерностей, которые всегда присутствует в незашифрованных текстах.

Эта схема использовалась во время второй мировой войны и после. Использование при переговорах германских подводных лодок многократно одного и того же ключа привело к тому, что эти переговоры легко расшифровывались в Оксфорде.

Такой одноразовый ключ абсолютно надежен, и единственная проблема, состоит в том, что секретная "одноразовая страница такой же длины как и основное сообщение, должна быть послана до того как будет использована. Это вновь приводит к проблеме 22 классической криптографии.

Квантовая криптография: квантовые протоколы обмена секретным ключом.

Мы переходим к рассмотрению основных идей и достижений квантовой криптографии, но прежде всего следует сразу же сказать, что

Замечательное и уникальное достижение квантовой криптографии состоит в том, что позволяет двум переговаривающимся сторонам

Автоматически Обнаружить Подслушивание.

Следовательно, она дает способ обнаружения нарушения секретности обмена информацией (например, при обмене секретным ключом).

В квантовой криптографии для передачи информации используются квантовые состояния – кубиты: *кубит -это вектор гильбертова пространства размерности 2.*

Если обозначить $|0\rangle$ и $|1\rangle$ базисные векторы

$$< 0|0 >=< 1|1 >= 1, \quad < 0|1 >= 0,$$

то наиболее общее нормированное состояние может быть выражено как

$$|\psi >= \alpha|0\rangle + \beta|1\rangle, \qquad (*)$$

где α и β – комплексные числа, которые удовлетворяют условию

$$|\alpha|^2 + |\beta|^2 = 1. \qquad (**)$$

Q-bit –это состояние в двумерном Гильбертовом пространстве, которое может принимать любую форму вида $(*)$.

Измерение изменяет квантовое состояние и проектирует q-бит в одно из базисных состояний $\{|0\rangle, |1\rangle\}$. Вероятность обнаружить в результате измерения состояние $\{|0\rangle$ равна $|\alpha|^2$, а состояние $|1\rangle$ равна $|\beta|^2$.

Рассмотрим, например, фотон, который распространяется в горизонтальном направлении. Выберем в качестве двух базисных поляризационных состояний вертикальную поляризацию:

$$|0\rangle \quad = \quad |\updownarrow\rangle \quad = \quad \binom{1}{0}$$

и горизонтальную поляризацию:

$$|1\rangle \quad = \quad |\leftrightarrow\rangle \quad = \quad \binom{0}{1}.$$

Можно выбрать другой поляризационный базис:

$$< 0'|0' >=< 1'|1' >= 1, \quad < 0'|1' >= 0,$$

полязизацию под углом 45° к горизонтали

$$|0'\rangle \quad = \quad |\nearrow\rangle \quad = \quad \frac{1}{\sqrt{2}}\binom{1}{1}$$

и полязизацию под углом -45°

$$|1'\rangle \quad = \quad |\searrow\rangle \quad = \quad \frac{1}{\sqrt{2}}\binom{1}{-1}.$$

Если фотон поляризован вдоль оси $+45^\circ$, то вероятность того, что его поляризация окажется вертикальной, то есть он пройдет через вертикальный фильтр, равна $|\langle 0|0'\rangle|^2 = \frac{1}{2}$, аналогично, горизонтальной $|\langle 1|0'\rangle|^2 = \frac{1}{2}$. Если фотон поляризован вдоль оси -45°, то вычисление обеих вероятностей дает также $\frac{1}{2}$.

Фотон как кубит

В теории квантовой информации в качестве кубита чаще всего используют фотон.

В квантовой механике поляризационную матрицу плотности фотона можно представить в форме

$$\hat{\rho} \quad = \quad \frac{1}{2}(\hat{E} + r\vec{n}\hat{\vec{\sigma}}),$$

где $\vec{n}\hat{\vec{\sigma}} = n_\alpha \hat{\sigma}_\alpha, n_\alpha$– составляющие единичного вектора $\vec{n}^2 = 1$, $\hat{\sigma}_\alpha$–матрицы Паули, а число r ограничено неравенствами

$$0 \leq r \leq 1.$$

Параметр r называют **степенью поляризации фотона**. Если $r < 1$, то говорят, что фотон поляризован частично, а при r=0, когда

$$\hat{\rho} \quad = \quad \frac{1}{2}\hat{E},$$

его называют **полностью неполяризованным**. Если $r = 1$, то полязизационная матрица плотности оказывается проекционной. В этом случае фотон обладает определенной поляризацией, т.е. равна нулю дисперсия величины

$$\hat{S}_n = \frac{1}{2}\vec{n}\hat{\vec{\sigma}}.$$

В оптике принято задавать поляризацию в терминах параметра Стокса, определяя их как составляющие вектора

$$\vec{\xi} = r\vec{n}.$$

Если длина вектора Стокса равна единице, его составляющие можно задать двумя параметрами:

$$\xi_1 = \sin 2\alpha \cos\beta, \quad \xi_2 = \sin 2\alpha \sin\beta, \quad \xi_3 = \cos 2\alpha.$$

Содержащиеся в этих формулах углы совпадают с представлением вектора поляризации в форме

$$\vec{\epsilon} \quad = \quad \vec{\chi}_1 \cos\alpha + \vec{\chi}_2 e^{i\beta} \sin\alpha,$$

в которой векторы $\vec{\chi}_{1,2}$ образуют базис в плоскости, перпендикулярной к направлению распространения фотона.

Два базисных состояния полязации, например, вертикальное и горизонтальное, можно обозначить как $|\updownarrow\rangle = |0\rangle$ и $|\leftrightarrow\rangle = |1\rangle$.

Теорема о невозможности клонирования произвольного квантового состояния (No Cloning Theorem)

Хорошо известно, что невозможно измерить состояние $|\psi\rangle$ единственной квантовой системы: результат единственного измерения наблюдаемой A есть одно из его собственных состояний, что дает только очень бедную информацию о состоянии $|\psi\rangle$, а именно оно должно быть неортогонально к полученному в результате измерения собственному состоянию. Востановить $|\psi\rangle$ (или в более общем случае матрицу плотности любого смешанного состояния) можно только измерив средние значения полного набора наблюдаемых, что получается только в результате статистического усреднения большого числа идентично приготовленных систем.

Например, измерив поляризацию фотона в вертикально-горизонтальном базисе, вы получите фотон или с вертикальной или с горизонтальной поляризацией, и если фотон не был первоначально поляризован именно в этом базисе, вы полностью разрушите первоначальное поляризационное состояние и никак не сможете повторить измерение первоначального состояния, скажем, в наклонном под $+45°$ базисе.

Можно было бы вообразить следующую процедуру, которая могла бы исправить это обстоятельство: возьмем систему в неизвестном состонии $|\psi\rangle$ и позволим ей взаимодействовать с N другими системами, приготовленными в некотором "чистом"состоянии $|R\rangle$ некоторого базиса, для того, чтобы получить N копий состояний исходной системы:

$$|\psi\rangle \otimes |R\rangle|... \otimes |R\rangle \to |\psi\rangle|\psi\rangle ... \otimes |\psi\rangle.$$

Такая бы процедура позволила бы нам определить состояние единственной квантовой системы, даже не возмущая ее, так как мы смогли бы измерять N копий, не трогая исходную систему. Теорема о невозможности клонирования квантовой информации содержит утверждение, что такая процедура невозможна.

Прежде, чем сформулировать и доказать эту теорему, заметим, что теорема о невозможности клонирования квантового состояния, также как и соотношение неопределенностей Гайзенберга, не является ограничением возможностей приборов наших лабораторий, а является внутренним свойством квантовой механики.

Справедлива **No-cloning Theorem**, которая утверждает, что
не существует преобразования в квантовой механике, которое может создавать точную копию произвольного квантового состоянияю

Приведем **доказательство** (оно принадлежит Wootters и Zurek(1982)), которое просто использует линейность операторов физических величин в квантовой механике.

Наиболее общее преобразование описывающее эволюцию в квантовой механике –это сохраняющее след изометрическое преобразование. И всегда можно рассматривать нашу систему как подсистему более широкой системы, эволюция которой унитарна.

Предположим, что существует $\hat{U}$ унитарное преобразование эволюции, которая возможно затрагивает дополнительную физическую систему "an ancilla"(машину), способное клонировать произвольное квантовое состояние, т.е.

$$\hat{U}|\psi\rangle \otimes |R\rangle| \otimes |M\rangle \quad = \quad |\psi\rangle \otimes |\psi\rangle| \otimes |M(\psi)\rangle.$$

Рассмотрим

$$|\psi\rangle \quad = \quad \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle).$$

По линейности

$$\begin{aligned}&\hat{U}\frac{1}{\sqrt{2}}(|0\rangle \otimes |R\rangle| \otimes |M\rangle + \frac{1}{\sqrt{2}}\hat{U}|1\rangle \otimes |R\rangle| \otimes |M\rangle)\\ = \quad &\frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle \otimes |M(0)\rangle + |1\rangle \otimes |1\rangle \otimes |M(1)\rangle).\end{aligned}$$

Но если $\hat{U}$ – преобразование клонирования, тогда

$$\begin{aligned}&\hat{U}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle\otimes) \otimes |R\rangle \otimes |M\rangle\\ = \quad &\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)|M(0+1)\rangle.\end{aligned}$$

Так как

$$(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)|M(0+1)\rangle \quad = \quad (|00\rangle + |10\rangle + |10\rangle + |11\rangle)|M(0+1)\rangle,$$

что никак не может быть равно первому результату, предположение о существовании преобразования клонирования приводит к противоречию.

Следовательно, ни один унитарный оператор не может в действительности клонировать неизвестное квантовое состояние.

Важно понимать, какое клонирование разрешено, а какое нет. Возможно клонировать известное квантовое состояние. Так как базисные состояния можно измерить не разрушая их, базисные состояния можно клонировать. Принцип невозможности клонирования утверждает, что невозможно реально клонировать неизвестное состояние. Так можно получить n частиц в перепутанном состоянии:

$$\alpha|0...0\rangle + \beta|1...1\rangle$$

из неизвестного состояния

$$\alpha|0\rangle + \beta|1\rangle,$$

но невозможно создать n-частичное состояние

$$(\alpha|0\rangle + \beta|1\rangle) \otimes ... \otimes (\alpha|0\rangle + \beta|1\rangle)$$

из неизвестного состояния

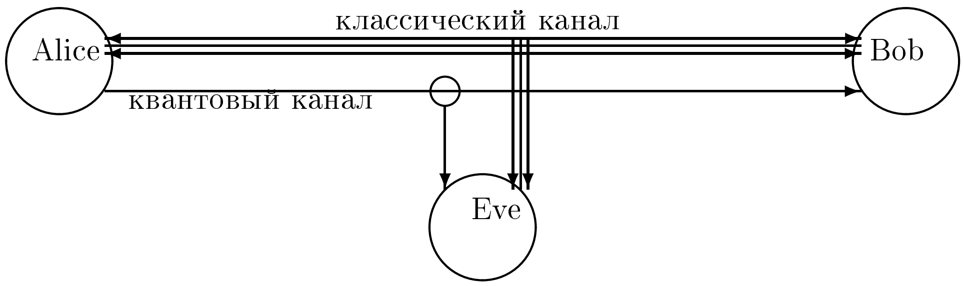
$$(\alpha|0\rangle + \beta|1\rangle).$$

Это свойство квантовых систем может быть использовано, например, в квантовой криптографии. Квантовое измерение изменяет состояние, поэтому нельзя произвести измерение сначала в одном базисе, а потом в другом. Более того, нельзя произвести измерение в двух различных базисах непрямым путем, скажем, копируя q-бит и измеряя копию, так как это запрещено "no-cloning"теоремой.

Квантовые протоколы обмена секретным ключом. Квантовый протокол BB84

Последовательности одиночных кубитов могут быть использованы для секретного обмена шифровальным ключом. Любая информация может быть извлечена из кубита только в результате измерения его квантового состояния.

Рассмотрим ситуацию, в которой Алиса и Боб хотят договориться о секретном ключе, с помощью которого впоследствии они смогут вести секретную переписку. Они используют один обычный открытый канал связи, работающий в двух направлениях, и один квантовый канал, который работает только в одном направлении. За обоими каналами наблюдает Ева, которая стремится подслушить их разговоры и завладеть секретным ключом, но так, чтобы ее вмешательство не было обнаружено.



Квантовый канал позволяет Алисе посылать индивидуальные частицы (фотоны) Бобу, который может измерять их квантовые состояния. Ева может попытаться измерить состояния фотонов и переслать их Бобу.

Беннетт и Брассар в 1984 году первыми описали квантовую схему обмена секретным ключом – **протокол BB84**.

Алиса использует две пары поляризаторов:

горизонтальную ($\leftrightarrow$) и вертикальную ($\updownarrow$) или

ортогонально ориентированных под углом в 45 градусов к первой паре ($\nwarrow$) и ($\nearrow$). Алиса сообщает об этих ориентациях Бобу, например, по классическому каналу связи.

Чтобы начать процесс установления секретного кода, Алиса посылает Бобу последовательность битов, кодируя каждый бит в квантовых состояниях фотонов, случайным образом используя ту или иную пару направлений поляризации, следующим образом:

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

или

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

Боб измеряет поляризации фотонов, которые он получает, случайным образом выбирая один из базисов. Кодировка Боба совпадает совпадает с кодировкой Алисы. Когда кубиты переданы, Алиса и Боб связываются по открытому классическому каналу, чтобы обменяться сведениями о базисах которые они использовали, чтобы закодировать и раскодировать каждый бит. С помощью этой информации они устанавливают те биты, которые были переданы заведомо правильно, т.е. те, для кодировки которых был использован тот же самый базис. Они используют эти биты для установления ключа, а остальные отбрасывают. В среднем, Алиса и Боб используют ту же поляризацию в 50% случаев.

1	1	1	1	1	0	0	1	0	1	0	0
$\times$	$+$	$\times$	$\times$	$\times$	$\times$	$\times$	$+$	$\times$	$\times$	$+$	$+$
$\nwarrow$	$-$	$\nwarrow$	$\nwarrow$	$\nwarrow$	$/$	$/$	$-$	$/$	$\nwarrow$	$\vert$	$\vert$

$\nwarrow$	$-$	$\nwarrow$	$\nwarrow$	$\nwarrow$	$/$	$/$	$-$	$/$	$\nwarrow$	$\vert$	$\vert$
$+$	$+$	$\times$	$+$	$\times$	$\times$	$+$	$\times$	$+$	$\times$	$+$	$+$
0	1	1	1	1	0	0	0	1	1	0	0

Предположим, что Ева измеряет поляризацию фотонов, посылаемых Алисой, а затем посылает Бобу фотоны с теми поляризациями, которые она определила. При таком процессе она будет использовать неправильный базис в 50% случаев, и в этих случаях будет пересылать кубиты в неправильном базисе. Поэтому Боб, измеряя поляризации пересланных Евой фотонов в базисе Алисы, с вероятностью 25% будет получать неправильную величину. Такая большая ошибка сразу же будет обнаружена и присутствие Евы выявлено, если Алиса и Боб обменяются значениями части оставленных битов через открытый канал.

Таким образом, Ева не только получит 25% неправильных значений битов, но и ее вмешательство будет обнаружено. Ключ не может быть использован, если хотя бы для одного контрольного бита значения Алисы и Боба не совпадают.

Протокол с 6 состояниями

Подобно тому как в BB84 используется две пары ортогональных состояний. В этом протоколе используют три таких пара. Эффективноть передачи при этом составит только 33%, но зато повышается надежность против внедрения посторонных слушателей. Это достигается благодаря гораздо большей симметрии в пространстве состояний кубитов. Так если распространение фотона – это ось X, то поляризационные базисы –это $(\updownarrow), (\leftrightarrow)$ (вертикальная и горизонтальная поляризации); $(\nearrow), (\nwarrow)$ (под 45°); $(+), (-)$ (право- и левокруговые поляризации). Если Ева измеряет каждый фотон, то возникающая ошибка 33%, по сравнению с 25% в BB84 протоколе.

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. V.Scarani, S.Iblisdir and N.Gisin. Quantum Cloning. arXiv:quant-ph/0511088 **(2005)**.
6. U.Dudley. Formulas for Primes. Math.Mag. **56**,17-72 (1983).
7. M.R.Schoeder. Number Theory in Science and Communication. *Springer, 1985*