С.Кулик, проф.,Физический факультет
МГУ им. М.В.Ломоносова

КВАНТОВАЯ КРИПТОГРАФИЯ

Квантовая криптография (КК) – бурно развивающееся направление науки и технологии. Несмотря на то, что сегодня уже имеются коммерчески доступные устройства КК, научная компонента в тематике КК до сих пор прогрессирует. Цель статьи – ознакомление с физическими принципами квантового распределения ключа и основными проблемами, возникающими при его реализации.

Тематике КК посвящено большое число популярных статей, оригинальных работ, монографий, прекрасных обзоров [1 – 6]. Несмотря на то, что сегодня уже имеются коммерчески доступные устройства КК, научная компонента в тематике КК до сих пор прогрессирует. С каждым годом появляются новые результаты: предлагаются новые протоколы, проводится анализ их секретности, сообщается о физической реализации и проч. Предлагаемая статья не претендует на оригинальность. Это не популярное изложение общих принципов и не полноценный обзор. Вместе с тем, список литературы включает как «классические» работы по КК, так и последние достижения в этой области. Цель статьи – ознакомление с физическими принципами квантового распределения ключа и основными проблемами, возникающими при его реализации.

Итак, квантовая криптография это интердисциплинарная область знания, технологии и техники, в которой решается задача обеспечения легитимных пользователей идентичными случайными последовательностями символов посредством передачи квантовых состояний. Такие последовательности представляют собой основу для криптографических ключей, с помощью которых шифруется закрытая информация. Поэтому иногда квантовую криптографию называют квантовым распределением ключей (Quantum Key Distribution). КК основана на соотношении неопределенностей Гейзенберга: наблюдаемые величины, которым в квантовой механике ставятся в соответствие некоммутирующие операторы, не имеют общего набора собственных векторов, не могут быть достоверно и одновременно различимы. Таким образом, в основе КК лежат законы природы, а не вычислительные или любые другие возможности легитимных пользователей или злоумышленников. КК является составной частью квантовой связи (quantum communication).

Прежде чем перейти непосредственно к основным принципам и протоколам КК, рассмотрим основы классической криптографии, которая имеет давнюю и богатую историю. Немаловажную роль в ней играет и отечественная школа.

КЛАССИЧЕСКАЯ КРИПТОГРАФИЯ

Исторически криптография, т.е. наука о создании секретной информации, возникла из потребности передачи секретной информации. Вместе с криптоанализом (наука о взламывании секретной информации) криптография составляет часть науки криптологии. Криптология в настоящее время является частью математики, кроме того, она имеет ряд важных приложений в информационных технологиях. Принято считать, что основой криптологии как науки послужила работа Шеннона «Теория связи в секретных системах» [7]. Долгое время криптография была связана только с разработкой специальных методов преобразования информации для представления ее в форме, которая окажется недоступной для потенциального подслушивателя. Появление компьютерных технологий обработки данных в корне поменяло задачи криптографии – иногда можно услышать мнение, что именно криптография стимулировала их развитие.

По сложившейся традиции, особенно в англоязычной литературе, участников процесса кодирования/декодирования называют Алисой и Бобом. Кроме того, в криптографии рассматривается некий злоумышленник или подслушиватель (eavesdropper) (Ева). Подслушиватель владеет современными вычислительными ресурсами, полностью осведомлен об используемых криптографических методах, алгоритмах, протоколах и т.д. и пытается каким-либо образом скомпрометировать их. Под компрометацией понимается несанкционированное чтение закрытой информации, ее модификация и проч. Все эти действия подслушивателя называются криптог-

рафической атакой. Специфика криптографии состоит в том, что она направлена на разработку приемов, обеспечивающих стойкость к любым атакам, хотя ясно, что на момент создания криптосистемы невозможно предусмотреть новые варианты атак. Отметим и такую социально-этическую сторону криптографии, как противоречие между желанием пользователей защитить свою информацию и желанием специальных государственных служб иметь возможность доступа к информации некоторых организаций и отдельных лиц с целью пресечения незаконной деятельности.

Классической задачей криптографии является обратимое преобразование некоторого исходного текста (открытый текст) в кажущуюся случайной последовательность знаков, называемую криптограммой. Количество знаков в открытом тексте и в криптограмме может отличаться. Секретность самого алгоритма шифрования не может, в принципе, обеспечить безусловной стойкости, поскольку предполагается, что подслушиватель обладает бесконечными вычислительными ресурсами. Поэтому в настоящее время используются так называемые открытые алгоритмы. Стойкость современных криптосистем основывается не на секретности алгоритма, а на секретности некоторой информации относительно малого размера, которая называется ключом. Ключ используется для управления процессом шифрования и должен быть легко сменяемым элементом криптосистемы. Он может быть заменен пользователями в любой момент времени. Сам алгоритм является долговременным элементом криптосистемы, его изменение требует вмешательства специалистов (разработчиков). Существует правило, сформулированное в конце XIX века голландским криптографом Керкхоффом (принцип Керкхоффа): стойкость шифра (кода) должна быть обеспечена в том случае, когда подслушивателю известен весь механизм шифрования, за исключением секретного ключа, т.е. той информации, которая управляет процессами криптографических преобразований. В более широком смысле мы приходим к важному требованию – все долговременные элементы защиты должны предполагаться известными потенциальному подслушивателю. Таким образом, в криптологии подслушиватель всегда оказывается в более выгодном положении – он не ограничен техническими возможностями, в отличие от реальных пользователей.

К.Шеннон [7] рассматривал шифрование (кодирование) как отображение исходного сообщения в криптограмму – зашифрованное сообщение:

$$C=F_i(M), \quad (1)$$

где C – криптограмма (от coding), F_i – отображение, M – исходное сообщение (от message), i – индекс, соответствующий конкретному используемому ключу. Для однозначного декодирования сообщения отображение F_i должно иметь единственное обратное отображение, такое, что

$$F_i F_i^{-1} = I, \quad (2)$$

где I – тождественное отображение:

$$M= F_i^{-1}(C). \quad (3)$$

Мы считаем, что источник ключей является статистическим процессом или устройством, которое задает отображения $F_1, F_2,...F_{N1}$ с известными вероятностями $p_1, p_2,...p_{N1}$. Число возможных сообщений N_2 конечно, а сообщения $M_1, M_2,... M_{N2}$ имеют априорные вероятности $q_1, q_2,...q_{N2}$.

Рассмотрим простейший шифр, в котором исходный алфавит сообщения совпадает с множеством знаков ключа и множеством знаков криптограммы. Пусть кодирование выполняется путем замены знаков исходного сообщения знаками криптограммы в зависимости от очередного значения символа ключа. Символ ключа из случайной последовательности чисел от 0 до 39. Тогда сообщение, ключ и криптограмма представляются в виде последовательности знаков одного и того же алфавита:

$$M = (m_1m_2m_3...m_n), \quad K = (k_1k_2k_3...k_n), \; C = (c_1c_2c_3...c_n)$$
$$(N_2=N_1). \quad (4)$$

Текущий шаг кодирования выражается следующим образом:

$$c_i = f(m_i, k_i). \quad (5)$$

Например, будем использовать простой алфавит заглавных букв русского языка, пробел и несколько знаков препинания (табл.1).

Допустим, мы хотим зашифровать сообщение “КОД ВЕРНАМА”. Запишем его в верхней строке вспомогательной таб-

Табл.1 Соответствие символов алфавита числам от 00 до 39

А	Б	В	Г	Д	...	...	...	Э	Ю	Я		.	,	!	?	;
00	01	02	03	04				31	32	33	34	35	36	37	38	39

Табл.2 Пример кодирования сообщения «КОД ВЕРНАМА»

К	О	Д		В	Е	Р	Н	А	М	А
10	14	04	34	02	05	16	13	00	12	00
15	04	13	28	11	09	38	30	02	24	05
25	18	17	22	13	14	14	03	02	36	05

лицы. Ниже укажем соответствующие численные символы из верхней таблицы. В третью строку поместим случайную выборку из сорока чисел от 00 до 39. В последней строке поместим результат суммирования символов второй и третьей строки по модулю 40 (табл.2).

Например, четвертый символ «пробел» в сообщении имеет числовой код «34». Соответствующее случайное число, выпавшее на этот символ, оказалось «28». Тогда 34 + 28 = 62 = 40 + 22. Следовательно, остаток при суммировании по модулю «40» равен 22. Таким образом, шифрование и дешифрование по рассмотренному алгоритму можно записать в виде:

$$M + k(\mathrm{mod}\ 40) = C. \qquad (6)$$

$$C - k\ (\mathrm{mod}\ 40) = M. \qquad (7)$$

Этот способ шифрования был изобретен Жильбером Вернамом [8]. Клод Шеннон строго показал, что если ключ действительно случайный, если он имеет такую же длину, как и само сообщение и если он не используется дважды, то такая одноразовая передача сообщения абсолютно защищена. Заметим, что этот вывод был получен В.А.Котельниковым в 1941 году, но не был опубликован в открытой печати [9]. Примечательно, что результат не зависит от вычислительной мощности, доступной криптоаналитику. Шифры такого рода называются безусловно стойкими. Другими словами, безусловно стойкими называются шифры, для которых криптоаналитик (даже если он обладает бесконечными вычислительными ресурсами) не может улучшить оценку исходного сообщения M на основе знания криптограммы C по сравнению с оценкой при неизвестной криптограмме. Ясно, что это возможно в случае, когда M и C являются статистически независимыми, т.е. когда выполняется условие:

$$P\ (M = M_i/C = C_i) = P\ (M = M_i) \qquad (8)$$

для всех возможных сообщений M. В нашем примере:

$$c_i = f\ (m_i, k_i) = (m_i + k_i)\ \mathrm{mod}\ L, \qquad (9)$$

где L = 40. Выбранный нами источник ключа обеспечивает равную вероятность выбора любого ключа длины n L=40. В этом случае вероятность выбора данного ключа длины n составляет

$$P\ (K = K_i) = L^{-n}. \qquad (10)$$

Отсюда следует, что для произвольных M и C выполняется условие

$$P\ (M = M_i/C = C_i) = L^{-n} \qquad (11)$$

и, таким образом, данной криптограмме длиной n с вероятностью L^{-n} может соответствовать любое исходное сообщение длины n.

Рассмотренный пример относится к криптосистемам, использующим равновероятный случайный ключ, имеющий длину, равную длине сообщения. Они называются одноразовыми блокнотами. Несмотря на обеспечение безусловной секретности, на практике такие системы получили ограниченное применение, поскольку требуют передачи ключа большого объема для каждого нового сообщения. А для длинных ключей процедура их управления, включающая их генерацию, передачу и хранение, крайне усложняется.

Другим недостатком шифра Вернама является тот факт, что ключ должен использоваться лишь один раз. Так, при повторном использовании Ева может, записывая и сравнивая отдельные части криптограммы, восстановить как фрагменты открытого текста, так и сам ключ. Пусть, например, Ева записала два сообщения, закодированных одним ключом в двоичном коде. Тогда, используя обстоятельство, что операция сложения по модулю два ⊕(XOR) коммутативна, она может сложить криптограммы и получить сумму двух открытых текстов:

$$s_1 \oplus s_1 = m_1 \oplus k \oplus m_2 \oplus k = m_1 \oplus m_2 \oplus k \oplus k \equiv m_1 \oplus m_2\ . \qquad (12)$$

Кроме того, чисто из физических соображений, классические состояния физических объектов могут быть измерены сколь угодно точно и без их возмущения. Поэтому в рамках классических физических представлений невозможно обеспечить секретное распределение ключа через открытый канал связи, так как нельзя гарантировать обнаружение попытки пассивного подслушивания. И криптограммы с одноразовыми ключами не получили широкого применения.

Итак, существующие одноключевые криптографические протоколы обеспечивают хорошую защищенность при условии решения задачи распределения ключа. Однако у этих систем существует две принципиальные проблемы:

1) как осуществить распределение ключей по защищенному каналу;
2) как осуществить аутентификацию секретного ключа (т.н. проблема первого общения). Под аутентификацией понимается процедура, позволяющая получателю удостовериться, что секретный ключ принадлежит законному отправителю. Чтобы пояснить, о чем идет речь, представим себе, что Ева перехватывает все сообщения, посылаемые Алисой, и выдает себя как Алису для Боба, а для Алисы она представляется Бобом – так называемая атака раздельных миров или «с человеком посредине» (man in the middle). Оказывается, что если у Алисы и Боба уже имеется секретный ключ (которым они обменялись, например, при встрече), то аутентификация вспомогательных ключей не представляет проблем. Однако если секретный ключ не распределен, то теоретически аутентификация невозможна, хотя и существуют методы (классические) по ее оптимизации.

Что касается проблемы распределения ключа, то существуют два способа ее решения. Первый –математический – достигается с помощью двухключевых протоколов или криптографии с открытым ключом. В нем используется алгоритм, основанный на функциях с секретом [10], когда вычисление функции в одну сторону оказывается простым, а нахождение обратной функции требует огромных вычислительных ресурсов. В частности, стойкость известных

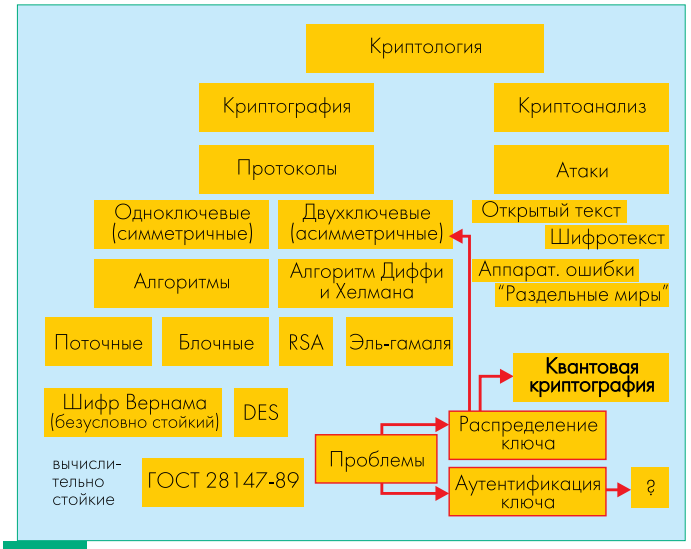

Рис.1 Упрощенная структура криптологии

криптографических систем RSA и Эль-Гамаля [11] основывается на том, что факторизация больших чисел требует экспоненциального по числу знаков факторизуемого числа N операций. Это значит, что при увеличении разряда числа на один (прибавление еще одной цифры к факторизуемому числу) умножает время, необходимое для факторизации на фиксированный множитель. При увеличении числа задача быстро становится вычислительно не решаемой. Таким образом, в настоящий момент защищенность двухключевых криптосистем основывается на ограниченности технического прогресса. Существует квантовый алгоритм, предложенный П.Шором, позволяющий решить задачу факторизации за полиномиальное время [12] (обращение дискретного логарифма), так что если квантовый компьютер будет создан, использование подобных криптосистем окажется бессмысленным.

Второй способ – физический – реализуется с помощью квантовой криптографии. К сожалению, квантовое распределение ключа не дает метода аутентификации или борьбы с атаками раздельных миров. Очень упрощенно структура и проблемы криптологии представлены на рис.1.

КВАНТОВАЯ КРИПТОГРАФИЯ (КВАНТОВОЕ РАСПРЕДЕЛЕНИЕ КЛЮЧЕЙ)

Безусловная секретность. Квантовая криптография позволяет решить одну из задач классической криптографии, а именно распределение ключей с последующим шифрованием в режиме одноразового блокнота. Это обеспечивает безусловную секретность при обмене информацией между легитимными пользователями. Но для обеспечения безусловной секретности необходимо удовлетворить трем условиям:

- сообщение шифруется ключом, который представляет собой случайную последовательность символов, например нулей и единиц;
- длина ключа должна быть не меньше длины сообщения;
- ключ используется только один раз.

Выполнение первого условия подразумевает наличие качественного генератора случайных чисел, что само по себе представляет отдельную сложную задачу. Второе условие накладывает количественное ограничение на длину сообщения (в битах) при фиксированной длине ключа. Как отмечалось, последнее требование является наиболее трудно выполнимым в классической криптографии, поскольку требует частой смены ключей и доставки их удаленным пользователям. Для решения этой проблемы разработаны классические методы, основанные на вычислительных трудностях для злоумышленника определить последовательность символов, служащую ключом. Идеальным сценарием для злоумышленника является создание копии ключа и, как следствие, получение доступа к шифрованным сообщениям так, чтобы об этом не знали легитимные пользователи. Распределение ключей посредством квантовых состояний позволяет, в принципе, гарантировать их секретность, т.е. удовлетворить перечисленным выше условиям при обмене закрытой информацией. В основе этого утверждения лежит теорема о запрете копирования произвольного квантового состояния (no-cloning theorem), которая гласит, что неизвестное квантовое состояние нельзя копировать [13]. Под копированием понимается процедура, при которой каждому входному состоянию ставится в соответствие два идентичных ему выходных состояния. Унитарность эволюции квантово-механических систем делает такой процесс возможным только при искажении

копируемого состояния. Более того, чем больше информации о состоянии извлекается в процессе копирования, тем большее искажение вносится в исходное состояние. Искажение состояния приводит к статистическим ошибкам, проявляющимся на определенном этапе выполнения протокола КК. Анализ этих ошибок позволяет легитимным пользователям сделать вывод о несанкционированном вторжении в линию связи и либо исправить их, либо прервать сеанс связи.

Кодирование информации в квантовых состояниях впервые было предложено в работах Стефана Визнера [14], а также Чарльза Беннета и Жиля Брассарда [15] . Их идея состояла в том, что пассивный подслушиватель не может достоверно различить неортогональные квантовые состояния (назовем их $|\psi\rangle$, $|\varphi\rangle$), если он не знает базиса, в котором те были приготовлены (по определению, состояния, описываемые кет-векторами $|\psi\rangle$, $|\varphi\rangle$, называются ортогональными, если их скалярное произведение обращается в нуль $\langle\psi|\varphi\rangle=0$). На этом этапе проявляется принципиальное отличие между классическими и квантовыми состояниями. Действительно, предположим, что Ева настраивает свой измеряющий прибор в неком исходном состоянии $|m\rangle$. Ее цель – отличить состояния $|\psi\rangle$, $|\varphi\rangle$, не возмущая их. Ее действия будут описываться следующими унитарными преобразованиями над входными состояниями:

$$|\psi\rangle\,|m\rangle \rightarrow |\psi\rangle\,|m_0\rangle \qquad (13)$$

$$|\psi\rangle\,|m\rangle \rightarrow |\psi\rangle\,|m_1\rangle \qquad (14)$$

Унитарность сохраняет скалярное произведение, поэтому

$$\langle\psi|\varphi\rangle\,\langle m|m\rangle = \langle\psi|\varphi\rangle\,\langle m_0|m_1\rangle \qquad (15)$$

откуда следует, что при выполнении нормировки

$$\langle\psi|\varphi\rangle\,\langle m_0|m_1\rangle=1 \qquad (16)$$

Соотношение (16) означает, что конечное состояние измерительного прибора Евы одно и то же. Ева не возмутила квантовых состояний, но она и не получила никакой информации о них в силу (4). Можно рассмотреть и более общее измерение, когда Ева возмущает исходные состояния:

$$|\psi\rangle \rightarrow |\psi'\rangle,\ |\varphi\rangle \rightarrow |\varphi'\rangle \qquad (17)$$

Тогда в результате ее действий:

$$|\psi\rangle\,|m\rangle \rightarrow |\psi'\rangle\,|m_0\rangle \qquad (18)$$

$$|\varphi\rangle\,|m\rangle \rightarrow |\varphi'\rangle\,|m_1\rangle \qquad (19)$$

И опять, в силу унитарности, получаем:

$$\langle\psi|\varphi\rangle = \langle\psi'|\varphi'\rangle\,\langle m_0|m_1\rangle \qquad (20)$$

Наилучшая ситуация, с точки зрения Евы, возникает, когда скалярное произведение $\langle m_0|m_1\rangle$ принимает минимальное значение. Это происходит при условии

$$\langle\psi'|\varphi'\rangle=1 \qquad (21)$$

(поскольку $\langle\psi|\varphi\rangle=\mathrm{const}\neq 0$). При этом она получает максимальную возможность различить два состояния своего прибора, но два исходно неортогональные состояния становятся неразличимыми (21). Здесь мы подошли к важному понятию достижимой (accessible) информации как меры того, насколько хорошо Боб может сделать вывод о том, какое состояние было ему послано Алисой. В классической теории информации это понятие не играет ключевой роли, поскольку различение пары состояний, в принципе, всегда возможно, хотя и может встретить определенные технические трудности. Теорему о запрете клонирования можно рассматривать как эквивалент утверждения о том, что в квантовой механике достижимая информация для неортогональных состояний меньше, чем энтропия исходно приготовленных состояний. В теории информации вводится специальная величина – граница Холево, которая и устанавливает достижимую информацию [16, 17].

Таким образом, КК обеспечивает возможность относительно быстрой смены ключей и определения попыток злоумышленника вторгнуться в канал связи. Подчеркнем, что наличие ошибок при передаче/приеме квантовых состояний не обязательно приводит к потере секретности. Для каждого протокола КК существует критическая ошибка, превышение которой больше не гарантирует секретности. Если уровень ошибок, обычно измеряемый в процентах, ниже критического, то для извлечения ключа используются протоколы коррекции ошибок (error correction) и последующего сжатия оставшейся строки битов (privacy amplification). После выполнения этих протоколов исходная строка битов укорачивается, однако гарантируется, что злоумышленник имеет о ней столь мало информации, сколько пожелают легитимные пользователи. На рис. 2 условно изображена схема общения между участниками протоколов квантовой криптографии и основные атрибуты таких протоколов – открытый канал связи, квантовый канал и возможное наличие подслушивателя.

Заметим, что С.Визнер [14] рассматривал так называемые «квантовые деньги», т.е. деньги, которые в принципе невозможно подделать. Кроме того, он предложил способ распределения двух или трех сообщений, при котором чтение одного из них уничтожало бы информацию, содержащуюся в других. Ч.Беннет, Ж.Брассард и др. предложили первый реалистичный протокол распределения ключа [18].

ФОТОНЫ – НОСИТЕЛИ ИНФОРМАЦИИ

Как правило, для кодирования исходной случайной последовательности символов используются степени свободы однофотонного электромагнитного поля – фаза, частота, поляризация,

Рис.2 Схема общения между участниками протоколов КК

временной интервал. Фотоны – наиболее удобные квантово-механические объекты для использования в КК, поскольку они распространяются с предельно высокой скоростью и обладают набором степеней свободы для осуществления кодирования. Кроме того имеющиеся телекоммуникационные технологии позволяют использовать ряд классических методов для генерации, преобразований и контроля однофотонных состояний.

Прежде, чем перейти к обсуждению различных протоколов криптографических атак, рассмотрим проблемы, связанные с генерацией квантовых состояний, используемых при квантовом распределении ключа. Чаще всего речь идет о протоколах на основе одно- и двухфотонных фоковских состояний света. Такие состояния практически очень трудно получить экспериментально, хотя в последнее время появились сообщения об их генерации в квантовых точках (т.н. фотонные пушки, когда система испускает только один фотон и не может испустить два – антигруппировка фотонов [19]). На сегодняшний день практическим источником однофотонных состояний служат ослабленные лазерные импульсы или коррелированные пары фотонов [20].

Автор выражает глубокую благодарность С.Н.Молоткову за плодотворные обсуждения проблем, затронутых в статье. Работа выполнена при финансовой поддержке Федерального агентства по науке и инновациям (Роснаука), Госконтракт 02.740.11.0223; гранта РФФИ 10-0290036Bel_a; и также гранта поддержки Ведущих Российских научных школ 65179.2010.2.

Продолжение обзора в следующем номере: будут рассмотрены способы кодирования по поляризации и по фазе, протоколы и системы квантового распределения ключей.

ЛИТЕРАТУРА

1. **Боумейстер Д., Экерт А., Цайлингер А.** Физика квантовой информации. – М.: Постмаркет, 2002.
2. **Нильсен М., Чанг И.** Квантовые вычисления и квантовая информация. – М.: Мир, 2006.
3. **Gisin N., Ribordy G., Tittel W., and Zbinden H.** Quantum cryptography. – Reviews of Modern Physics, 74, 145 (2002).
4. **Bennett C., Brassard G., Ekert A.** Quantum cryptography. – Scientific American, October 1992, p.50.
5. **Килин С., Хорошко Д., Низовцев А.** Квантовая криптография: идеи и практика. – Минск, Бел. наука, 2007.
6. **Молотков С.** Квантовая криптография и теоремы В.А.Котельникова об одноразовых ключах и об отсчетах. – УФН, т.176, №7, 777 (2006).
7. **Шеннон К.** Работы по теории информации и кибернетике. – М.: ИЛ, 1963.
8. **Vernam G.** Cipher printing telegraph systems for secret wire and radio telegraphic communications. – J. Am. Inst. Elect. Eng. 55 109 (1926).
9. Научная сессия Отделения физических наук Российской академии наук, посвященная памяти академика В. А. Котельникова. – УФН, 176, №7, 751 (2006).
10. **Diffie W., Hellman M.** – IEEE Trans. Inf. Theory IT-22, 644 (1977).
11. **Rivest R., Shamir A. and Adleman L.** On Digital Signatures and Public-Key Cryptosystems. – MIT Laboratory for Computer Science, Technical Report, MIT/LCS/TR-212 (January 1979).
12. **Shor P.** Proc. of the 35th Annual Symposium on the Foundations of Computer Science (IEEE Computer Society, Los Alamos, CA, 1994) p. 124.
13. **Wootters W., Zurek W.** A single quantum cannot be cloned. – Nature 299 802 (1982).
14. **Wiesner S.** – SIGACT News 15, 78 (1983), (статья подготовлена в 1970 году).
15. **Bennett C., Brassard G.** – Proc. IEEE Int. Conf.Comp., Systems and Signal Processing. – IEEE, NY (1984).
16. **Холево А.** К математической теории квантовых каналов связи. – Проблемы передачи информации. 8 (1), 62 (1972).
17. **Холево А.** Введение в квантовую теорию информации. – М.: МЦНМО, Сер. Современная математическая физика. Проблемы и методы. 2002, вып.5.
18. **Bennett C., Bessette F., Brassard G. et al.** Experimental quantum cryptography. – J. Cryptology 5, 3 (1992).
19. **All'aume R., Treussart F., Messin G. et al.** Experimental open-air quantum key distribution with a single-photon source. Issue «Focus on Single Photons on Demand». – New J. Phys. 6, 92 (2004).
20. **Fasel S., Alibart O., Tanzilli S. et al.** High-quality asynchronous heralded single-photon source at telecom wavelength. Issue «Focus on Single Photons on Demand». – New J. Phys. 6, 163 (2004).