PACS numbers: 03.67.Dd, **89.70.+c**

Квантовая криптография и теоремы В.А. Котельникова об одноразовых ключах и об отсчетах

С.Н. Молотков

Квантовая криптография представляет собой новое направление в развитии средств конфиденциальной передачи информации. Точнее, квантовые криптографические системы представляют собой системы распределения секретных ключей между пространственно разделенными (удаленными) легитимными пользователями. Обеспечение секретного распространения ключей между такими пользователями играет принципиально важную роль в криптографии. Если бы существовал способ распространения (передачи) секретных ключей от одного легитимного пользователя к другому по открытому (несекретному) каналу связи с гарантией того, что в процессе передачи ключи не станут известны подслушивателю, то в этом случае была бы возможна передача зашифрованных с помощью этих ключей сообщений, которые принципиально не могут быть дешифрованы (взломаны) третьими лицами. Такие принципиально не дешифруемые системы называют абсолютно стойкими, или системами шифрования в режиме одноразового блокнота (one time pad). Позднее такие шифры стали называть совершенными.

Сначала кратко коснемся истории вопроса.

Впервые строгое обоснование того факта, что системы шифрования с одноразовыми ключами являются абсолютно стойкими, было получено в работе Владимира Александровича Котельникова. Эта работа, законченная за несколько дней до начала Великой Отечественной войны 22 июня 1941 г., вошла в один из закрытых отчетов [1] и до сегодняшнего дня не опубликована в открытой печати.

Параллельно и независимо вопросы теоретической стойкости шифров изучались Клодом Шенноном (C.E. Shannon). Результаты его исследований были представлены в закрытом отчете "A Mathematical Theory of Cryptography", датированном 1 сентября 1946 г. После окончания войны этот отчет был рассекречен[1] и опубликован в 1949 г. в виде статьи "Communication Theory of Secrecy Systems" [2], которая стала широко известным классическим трудом по теоретической криптографии.

Идея, очень близкая идее режима шифрования с одноразовым блокнотом, была высказана еще в 1926 г. в работе Вернама (G.S. Vernam) "Cipher Printing Telegraph Systems for Secret Wire and Radio Telegraphic Communication" [3], где утверждалось, правда, без каких бы то ни было математических обоснований, что шифры с "бегущим" случайным ключом (running key) будут абсолютно не дешифруемыми: "...If, now, instead of using English words or sentences, we employ a key composed of letters selected absolutely at random, a cipher system is produced which is absolutely unbreakable"[2].

Благодаря исследованиям В.А. Котельникова и К. Шеннона возникло четкое и строгое понимание того, каким условиям должен удовлетворять абсолютно стойкий шифр.

Неформально, шифр является абсолютно стойким, если:

1) ключ секретен — известен только легитимным пользователям;

2) длина ключа в битах не меньше длины сообщения;

3) ключ случаен;

4) ключ используется только один раз.

В этом случае зашифрованное сообщение статистически независимо от исходного сообщения.

Принципиальная проблема при реализации криптосистем с одноразовыми ключами состоит в передаче (распространении) секретных ключей между удаленными легитимными пользователями.

Ключ между такими пользователями должен передаваться с помощью какого-либо физического сигнала через открытый (т.е. доступный для подслушивания) канал связи. С точки зрения классической физики в этом случае не существует запретов на измерение передаваемого сигнала без его возмущения. Поэтому принципиально невозможно гарантировать секретность ключа при его распространении.

Если же передавать ключи с помощью квантовых состояний, то возникает принципиально другая, более интересная ситуация. Квантовая криптография, основанная на фундаментальных запретах квантовой механики, открывает возможность передачи ключей с помощью квантовых состояний, секретность при этом гарантируется фундаментальными законами природы. Следовательно, квантовая криптография позволяет реализовать абсолютно стойкие системы шифрования с одноразовыми ключами, истоки которых восходят к работам Г. Вернама, В.А. Котельникова и К. Шеннона. Собственно идея квантовой криптографии как раз и направлена на решение центральной проблемы криптографии — задачи распространения секретных ключей.

Впервые идея использовать квантовую механику для защиты информации была высказана S. Wiesner в 1973 г. (идея "квантовых" денег), но была опубликована [4] лишь спустя десятилетие. Интересно отметить, что идеи использования квантовой механики для защиты информации появились раньше, чем классическая криптография с открытым ключом [5, 6].

Возникновение квантовой криптографии связано с опубликованием в 1984 г. замечательной работы Бен-

[1] Здесь имеет смысл упомянуть высказывание одного из основателей криптографии с открытым ключом У. Диффи (W. Diffie), по мнению которого работа К. Шеннона, возможно, была рассекречена ошибочно (см. предисловие к монографии B. Schneier *Applied Cryptography*, John Wiley & Sons, Inc., 1996).

[2] "...Если же, вместо использования английских слов и предложений, мы воспользуемся ключом, составленным из букв, выбранных абсолютно случайным образом, то полученная система шифрования будет абсолютно стойкой". (*Перевод ред.*)

нета и Брассара, в которой был предложен первый криптографический протокол BB84, ставший впоследствии классическим [7].

Квантовая криптография, или распространение секретных ключей, в принципе позволяет реализовать абсолютно стойкие (не дешифруемые подслушивателем даже теоретически) системы шифрования с одноразовыми ключами. Секретность ключей в квантовой криптографии основана на фундаментальных запретах квантовой механики: 1) неизвестное квантовое состояние не может быть скопировано (no-cloning-теорема [8]); 2) пара наблюдаемых, которым отвечают некоммутирующие эрмитовы операторы, не может быть одновременно достоверно различима, что является следствием соотношений неопределенности Гейзенберга [9], или, говоря более формально, некоммутирующие операторы не могут иметь общих собственных векторов. В квантовой криптографии в качестве наблюдаемых выступают матрицы плотности информационных состояний, соответствующих классическим битам 0 и 1. Для чистых состояний одновременная ненаблюдаемость (достоверная неразличимость) матриц плотности эквивалентна неортогональности информационных квантовых состояний [9]. Сказанное означает, что не существует измерений, которые с вероятностью 1 позволяют различать одно из пары неортогональных состояний и так, чтобы после измерения система осталась в исходном (невозмущенном) состоянии.

Таким образом, любое измерение, если оно дает информацию о передаваемых состояниях, неизбежно приводит к их возмущению, что позволяет детектировать любые попытки подслушивания в канале связи. Другими словами, подслушивание (соответственно возмущение передаваемых состояний) должно неизбежно изменять статистику результатов измерений на приемном конце по сравнению со статистикой результатов измерений на невозмущенных состояниях. Искажение квантовых состояний возникает в неидеальном квантовом канале, что также приводит к изменению статистики результатов измерений. В квантовой криптографии принципиально невозможно различить изменилась ли статистика результатов по сравнению с таковой в идеальном случае за счет шума в канале или вследствие действий подслушивателя, поэтому любые изменения статистики приходится относить к действиям подслушивателя.

Если бы законы квантовой механики позволяли обнаруживать только сам факт возмущения передаваемых состояний, то это было бы малоинтересным для целей криптографии, точнее, передачи ключей. *Квантовая механика позволяет не только обнаруживать возмущение состояний, но и связать изменение статистики результатов измерений с количеством информации, которое может быть получено подслушивателем при наблюдаемом изменении статистики отсчетов по сравнению со статистикой в идеальном случае*.

В квантовой криптографии кроме квантового канала связи (в реальных условиях это либо оптоволокно, либо открытое пространство), по которому передаются квантовые состояния, необходим также открытый классический канал связи. Последний требуется для выяснения легитимными пользователями изменений статистики отсчетов и коррекции ошибок в первичном ключе, переданном по квантовому каналу связи.

Единственное требование, предъявляемое к классическому каналу связи, состоит в том, что передаваемая открыто и доступная всем, включая подслушивателя, классическая информация не может быть изменена подслушивателем — она должна сохранять целостность (так называемый unjamable channel) [7]. Такой открытый классический канал является, конечно, математической идеализацией. Для сохранения целостности открыто передаваемых классических данных в реальных условиях необходимо использовать процедуры аутентификации и контроля целостности данных. Для подобных процедур, в свою очередь, требуется секретный ключ. Если в качестве открытого классического канала используется, например, Интернет, то для целей аутентификации возможна генерация ключей по схеме Хеллмана – Диффи [5]. Однако если для открытого классического канала используется та же самая оптоволоконная линия, что и для квантового, то генерация ключей для аутентификации по схеме Хеллмана – Диффи оказывается неприемлемой из-за очевидной так называемой атаки "man in the middle" (человек посредине).

В такой ситуации требуется небольшой стартовый ключ один раз при первом сеансе. При последующих сеансах этот ключ выбрасывается, и для аутентификации и сохранения целостности данных, передаваемых по классическому каналу, используется часть ключа, сгенерированного по квантовому каналу в предыдущем сеансе обмена. Остальная, бóльшая часть ключа, полученного по квантовому каналу, предназначается собственно для шифрования передаваемой информации. Если для аутентификации и сохранения целостности данных применяются процедуры на основе ГОСТ Р 34.11-94 [10], то длина стартового ключа составляет 256 бит. При этом в течение нескольких секунд обмена по квантовому каналу может быть получен новый секретный ключ, гораздо более длинный, чем исходный.

Разумеется, стартовый ключ мог бы быть использован для шифрования нового ключа и передачи его второму легитимному пользователю. Однако при этом абсолютная секретность нового ключа гарантируется, лишь когда его длина не более длины ключа, на котором он шифруется, т.е. более длинного ключа, чем исходный, получить нельзя. В квантовой криптографии стартовый ключ не используется напрямую для передачи нового ключа, который генерируется по квантовому каналу связи. При этом число бит открытой информации, переданной по открытому классическому каналу на один бит нового секретного ключа, может быть сделано меньше единицы, поэтому возможно расширение ключа.

Подход с использованием небольшого стартового ключа предпочтительнее подходов на основе алгоритмов асимметричной криптографии с открытым ключом, поскольку позволяет свести к минимуму число сеансов обмена по открытому каналу связи в процессе "чистки" и усиления секретности ключа (privacy amplification).

Основная задача теории сводится к выяснению длины секретного ключа, который может быть получен при наблюдаемых изменениях статистики результатов измерений на приемном конце по сравнению со статистикой на невозмущенных состояниях. Как правило, величиной, которая характеризует отклонение статистики измерений от идеальной, является наблюдаемая вероятность ошибки на приемном конце, точнее, вероят-

ность того, что переданный бит был 0, а зарегистрирован как 1, и наоборот. Такая ситуация имеет место в широко применяемом протоколе BB84, хотя возможны и другие критерии изменения статистики, которые используют несколько параметров. Перед выяснением вероятности ошибки через открытый канал происходит сравнение базисов на приемной и передающей стороне (для протокола BB84 [7]) или раскрытие позиций на приемной стороне, где имел место результат измерений с неопределенным исходом (для протокола B92 [9]). Вероятность ошибки оценивается путем сравнения через открытый канал части последовательности, полученной по квантовому каналу информации, с соответствующей частью исходной, в дальнейшем раскрытая часть отбрасывается.

Следующий этап любого квантового криптографического протокола распространения ключей состоит в коррекции ошибок в нераскрытой части последовательности у легитимных пользователей посредством обмена информацией через открытый канал связи. Обычно легитимных пользователей называют Alice и Bob, а подслушивателю присваивают имя Eve (от англ. eavesdropper). В результате коррекции ошибок у Alice и Bob остаются последовательности бит меньшей длины и уже одинаковые. "Одинаковые" здесь означает, что последовательности совпадают с вероятностью сколь угодно близкой к единице: $1-2^{v}$ (например $1-2^{-200}\sim 1-10^{-70}$, напомним, что число атомов в видимой части Вселенной оценивается как 10^{77}). Параметр v выбирается легитимными пользователями.

После "чистки" первичного ключа у подслушивателя имеется строка бит или регистр квантовой памяти с состояниями либо и то, и другое вместе. Последний шаг при получении финального секретного ключа состоит в усилении секретности (privacy amplification [11]) — сжатии "очищенного" ключа с помощью так называемой универсальной функции хэширования 2-го рода (two universal hash function [12]), которая сама является случайной величиной для уже одинаковых последовательностей у Alice и Bob. Случайно выбираемая функция хэширования открыто сообщается одним из легитимных пользователей через открытый канал связи и считается всем известной, включая подслушивателя. Сжатая последовательность бит является для легитимных пользователей общим секретным ключом, для которого гарантируется, что подслушиватель имеет о ключе сколь угодно малую информацию по некоторому, заданному Alice и Bob параметру секретности.

Естественным требованием к процедурам коррекции ошибок и усиления секретности ключа является сохранение как можно большего числа бит в финальном ключе. Еще одно требование состоит в минимизации числа сеансов обмена по открытому каналу связи в пересчете на один бит в финальном секретном ключе.

При коррекции ошибок в первичном ключе задача легитимных пользователей состоит не только в исправлении ошибок, но также в оценке верхней границы информации, которую может получить об оставшемся ключе подслушиватель из обменов по открытому каналу связи. Для коррекции ошибок могут быть использованы различные процедуры, включая хорошо разработанные классические коды, исправляющие ошибки.

Перейдем теперь к обсуждению экспериментальных реализаций систем квантовой криптографии.

Разработки в области квантовой криптографии и реализации различных квантовых криптосистем ведутся во многих университетах всех развитых стран и практически во всех ведущих телекоммуникационных компаниях. За последние пять лет квантовая криптография прошла путь от чисто теоретических исследований до их практической реализации и создания первых коммерческих прототипов.

Имеющиеся прототипы квантовых криптосистем используют в основном следующие принципы кодирования классической информации в состояния квантовых систем.

1. Кодирование информации о ключе в поляризационные степени свободы [13].

2. Фазовое кодирование с помощью интерферометра Маха – Цандера, в котором информация кодируется в разность фаз на приемном и передающем плечах интерферометра [14, 15].

3. Кодирование на основе частотной модуляции несущей частоты [16].

4. Квантовая криптография на когерентных состояниях с использованием гомодинного детектирования на приемном конце [17].

Наибольший прогресс достигнут в криптосистемах с фазовым кодированием и самокомпенсацией [18] с использованием фарадеевских отражателей. Первый лабораторный прототип квантовой криптосистемы, созданный в 1989 г. в Исследовательском центре компании IBM, имел длину квантового канала связи 1 м [19]. Лабораторный вариант криптосистемы на базе интерферометра Маха – Цандера с разделением времени (time division interferometer) был реализован с использованием оптоволоконной линии связи длиной 30 км в исследовательской лаборатории фирмы "British Telecom" в 1995 г. [20] и с суммарной длиной оптоволоконных линий 48 км в Лос-Аламосской лаборатории [21]. В этих схемах применялся принцип фазового кодирования. В 2003 г. в исследовательской лаборатории NEC достигнута дальность 100 км [21], а в 2004 г. — уже 150 км [22]. Данные схемы являются усложнением и развитием идеи фазового кодирования с самокомпенсацией с помощью фарадеевских отражателей. Упомянутые криптосистемы, особенно схемы с фазовым кодированием и самокомпенсацией, достаточно сложны в реализации. Результатом теоретической разработки группы в Женевском университете стала практическая реализация квантовой криптосистемы с волоконно-оптическим кабелем длиной 23 км, проложенным по дну Женевского озера между городами Нион и Женева. Линия, длина которой на сегодня доведена до 67 км, представляет собой сложный оптоволоконный интерферометр с фазовым кодированием и самокомпенсацией с использованием фарадеевских отражателей [18] (первая так называемая plug & play-система квантовой криптографии). Активные исследования ведутся в исследовательской лаборатории IBM (Almaden) [23, 24]. Апробирована первая локальная квантовая криптографическая сеть в Бостоне для распространения секретных ключей между пользователями на расстоянии в 10 км (проект выполняется по заказу DARPA — Defense Advanced Research Projects Agency) [25].

Недавно инновационной фирмой "MagiQ" был анонсирован первый коммерческий вариант квантовой волоконной криптосистемы, действующей на расстоянии

120 км, в которой используется принцип фазового кодирования. Схема реализует квантово-криптографический протокол BB84.

По мнению специалистов из "QinetiQ" и "Toshiba Research Europe" (Великобритания), широкое применение квантовых криптосистем начнется в ближайшие три года, первыми на очереди стоят правительственные учреждения и банки.

Имеются реализации прототипов квантовых криптосистем, осуществляющих передачу секретного ключа через открытое пространство [26–28]. Рекорд по дальности (по опубликованным данным [28]) составляет 23,4 км как в дневное, так и ночное время. Такие квантовые криптосистемы предназначены для генерации и передачи секретных ключей между наземными объектами и низкоорбитальными спутниками (до высот в 1000 км) или между наземными объектами через спутники. По оценкам руководителя проекта из "QinetiQ" планируются эксперименты по передаче криптографических ключей на низкоорбитальные спутники, а лет через семь с их помощью можно будет посылать секретные ключи в любую точку планеты.

На ближайшее время прогнозируются следующие параметры квантовых криптографических волоконно-оптических линий связи:

1. Количество ошибок, не превышающее нескольких процентов при эффективной скорости передачи информации по оптоволоконному квантовому каналу.

2. Длина квантового оптоволоконного канала связи $\sim 100-150$ км.

3. Число подканалов при разделении по длинам волн (мультиплексировании) — 8–16.

Несмотря на впечатляющий прогресс как в понимании криптографической стойкости (секретности) квантовых криптосистем, так и в их реализации, эти системы содержат достаточно сложные оптоволоконные, электронные и программные компоненты, работа с которыми на сегодня представляет собой, скорее, проведение тонкого научного эксперимента и демонстрацию экспериментального искусства, чем практическую деятельность с использованием общеупотребительного и стандартного оборудования. Другим важным обстоятельством, сдерживающим пока широкое распространение квантовых криптосистем на основе принципа фазового кодирования, является то, что квантовые криптосистемы пока плохо встраиваются в стандартные оптоволоконные телекоммуникационные технологии, поскольку содержат специфические компоненты (интерферометры), требующие тонкой юстировки. Наконец, последний принципиальный момент состоит в том, что каждый квантовый криптографический протокол распространения секретного ключа фактически требует "темных" оптоволоконных линий (свободных линий).

Существует три базовых протокола передачи секретного ключа, которые кратко называются BB84 [7], B92 [9] и BB84$(4+2)$ [29]. Протокол BB84 использует четыре квантовых состояния: два ортогональных состояния для 0 и 1 в одном базисе и два ортогональных для 0 и 1 в другом. Между базисами состояния попарно неортогональны, что необходимо для обеспечения секретности. В протоколе B92 используется пара любых неортогональных квантовых состояний, отвечающих 0 и 1. Протокол BB84$(4+2)$ является производным от BB84 и отличается от последнего тем, что внутри базисов состояния также делаются неортогональными. Очевидно, что разные протоколы обмена требуют различных физических устройств для формирования квантовых состояний на передающем конце и соответственно разных устройств для квантово-механических измерений на приемном конце.

Криптографическая стойкость (секретность) данных протоколов достаточно подробно исследована [29–36]. С учетом реальных параметров — нестрогой однофотонности источника, неидеальности лавинных фотодетекторов и затухания в оптоволоконном канале связи, перечисленные протоколы гарантируют секретность распространения ключа до определенной критической длины оптоволоконной линии связи [29]. Протокол B92 является самым минимальным, в смысле числа используемых состояний и измерений, однако обеспечивает секретность только до длин $\sim 15-20$ км [33]. Наиболее подробно исследованный протокол BB84, использующий четыре квантовых состояния, является более сложным в реализации и остается секретным до длин ~ 50 км [29]. Наконец, в протоколе BB84$(4+2)$ применяются четыре попарно неортогональных состояния. Данный протокол еще сложнее в реализации и настройке оптоволоконного интерферометра, однако в смысле секретности "выживает" до длин ~ 150 км [29].

Для экспериментальной реализации требуются однофотонные источники. Подчеркнем, что с точки зрения теории не обязательно использовать однофотонные квантовые состояния для передачи ключей. Однако в многофотонном случае квантово-механические измерения на приемном конце для детектирования попыток подслушивания и изменения квантовых состояний формально должны быть реализованы как проекторы на соответствующие векторы многофотонных квантовых состояний. Подобных измерительных устройств пока не существует, хотя никаких теоретических запретов на реализацию таких квантово-механических измерений нет. То есть использование именно однофотонных квантовых состояний обусловлено существующими детекторами (реально это лавинные фотодетекторы с пельтье-охлаждением, работающие в стробируемом режиме).

Отметим, что уже созданы фотодетекторы на основе сверхпроводников, которые в отличие от лавинных фотодетекторов на гетероструктурах различают состояния с разным числом фотонов.

Однофотонные квантовые состояния (точнее квазиоднофотонные) получаются путем сильного ослабления когерентного состояния — лазерного изучения, которое даже после любого ослабления содержит многофотонные компоненты.

Нестрогая однофотонность источника вместе с затуханием в квантовом канале связи приводят к тому, что секретность передаваемых ключей гарантируется, лишь когда длина канала не превосходит некоторой критической величины.

Негативная роль затухания (при нестрого однофотонном источнике) в квантовом канале связи состоит не столько в том, что затухание, очевидно, снижает скорость передачи ключа из-за того, что не все фотоны достигают приемного конца, сколько в том, и это гораздо более критично, что начиная с некоторой величины затухания уже нельзя гарантировать секретность переданного ключа. Затухание в оптоволоконных линиях связи определяется длиной канала связи. Однако

критическая длина, вплоть до которой система остается секретной, до сих пор строго неизвестна. Оценки варьируются от нескольких десятков километров до 150 км [29].

Ведутся работы по использованию в квантовой криптографии источников излучения, например на основе наночастиц алмаза, которые по своим параметрам приближаются к однофотонным [37].

Если проанализировать основные квантовые криптографические протоколы и доказательства их секретности в канале с затуханием (основными являются протоколы BB84 и B92, остальные представляют собой того или иного вида производные от них), то становится очевидным, что требуется (и используется явно или неявно) априорная информация о потоке ошибок (Quantum Bit Error Rate, QBER), обусловленных затуханием. Например, если затухание в канале связи изменяется в течение времени протокола передачи ключа, то изменяется и поток ошибок (даже в отсутствие подслушивателя). Кроме того, если протокол подразумевает постоянство QBER, то никакую секретность переданного ключа вообще невозможно гарантировать. Если в оптоволоконных квантовых криптосистемах затухание еще можно считать постоянным (последнее составляет для одномодового оптоволокна на длине волны 1550 нм 0,17–0,25 дБ км$^{-1}$), то при передаче через открытое пространство это уже явно не так, поскольку состояние атмосферы невозможно контролировать. Поэтому хотелось бы иметь протоколы распространения ключа, которые были бы устойчивыми и гарантировали секретность ключа при изменении затухания в канале связи в течение времени протокола и секретность которых не зависела бы от априорного знания величины затухания. Данная проблема, на наш взгляд, достаточно серьезна и требует решения, поскольку в противном случае могут возникнуть сомнения в безусловной секретности квантовой криптографии (секретности, которая полностью гарантируется фундаментальными запретами квантовой механики, а не техническими ограничениями подслушивателя).

Все упомянутые выше трудности связаны с тем, что секретность протоколов базируется, по сути, лишь на геометрических свойствах векторов состояний квантовой системы в гильбертовом пространстве $\mathcal{H}$. Точнее, на невозможности копирования (no-cloning-теорема [8]) неизвестного квантового состояния и принципиальной достоверной неразличимости неортогональных квантовых состояний (теорема C.H. Bennett [9]). Грубо говоря, данные протоколы формулируются в гильбертовом пространстве $\mathcal{H}$. То, что все измерения и распространение квантовых состояний происходят в пространстве-времени, никак явно не используется. При распространении квантового состояния затухание имеет место не в гильбертовом пространстве, а в пространстве-времени, поэтому для устранения проблем потери секретности вследствие затухания требуются другие дополнительные *фундаментальные* ограничения, проистекающие из свойств квантовых состояний, и получение информации о них в пространстве-времени. Ограничения, диктуемые лишь геометрическими свойствами квантовых состояний в гильбертовом пространстве, для построения квантовых криптографических протоколов, по-видимому, исчерпаны.

Такими дополнительными фундаментальными и естественными ограничениями являются ограничения, диктуемые специальной теорией относительности. Кроме того, фотоны представляют собой истинно релятивистские безмассовые частицы (состояния безмассового квантованного поля), которые распространяются с предельно допустимой скоростью, поэтому при разработке и реализации квантовой криптографии в открытом пространстве было бы неестественно не воспользоваться дополнительными возможностями, предоставляемыми природой.

Ниже кратко обсудим квантовые криптосистемы для передачи ключей через открытое пространство, которые кроме ограничений на измеримость квантовых состояний, следующих из квантовой механики, используют дополнительные запреты, диктуемые специальной теорией относительности.

Поскольку в обсуждаемых ниже квантовых криптосистемах явно учитывается факт распространения квантовых состояний (ключа) в пространстве-времени, то требуется заранее знать длину квантового канала связи между передающей и принимающей сторонами.

Релятивистские квантовые криптосистемы остаются секретными при любом затухании в канале связи. Величина затухания снижает лишь скорость передачи ключа, но не влияет на его секретность. Кроме того, гарантируется секретность ключа даже для неоднофотонных состояний. Схема остается секретной при любом среднем числе фотонов в квантовом состоянии. Как показывают расчеты (см. подробности в [38]), наибольшая эффективность достигается при небольших средних числах фотонов, $\mu = 1-3$. При таких средних числах заполнения практически отсутствуют холостые посылки (доля вакуумной компоненты в когерентном состоянии мала). Последнее означает, что скорость генерации ключа, как минимум, на порядок выше, чем в схемах, базирующихся только на геометрических свойствах квантовых состояний, где требуется ослабление лазерного излучения до $\mu = 0{,}1-0{,}3$. Дополнительное увеличение скорости возникает за счет того, что ограничения специальной теории относительности позволяют использовать даже ортогональные состояния, что не требует проверки согласования базисов измерений, как в протоколе BB84. Кроме того, поскольку все действия участников (как легитимных, так и подслушивателя) осуществляются в пространстве-времени и состояния ортогональны, то коллективные измерения подслушивателя не дают ему никаких преимуществ по сравнению с индивидуальными измерениями в каждой посылке. И последнее, система гарантирует секретность ключа даже при уровне ошибок в принятой двоичной последовательности, близком к 50 % (см. детали в [38]). Отметим, что, например, для протокола BB84 секретность гарантируется лишь до уровня ошибок в 11 % [30, 32].

Напомним, что теоретически безошибочная передача информации, фактически исправление ошибок в пределе асимптотически длинных последовательностей в классическом бинарном симметричном канале, возможна, если вероятность ошибки не превышает 50 %. *В релятивистской квантовой криптографии при уровне ошибок близком к* 50 % *возможно не только исправить ошибки, но и гарантировать секретность информации (ключей), передаваемой с помощью квантовых состояний через открытое пространство.*

Единственное дополнительное требование в релятивистских квантовых криптосистемах по сравнению с нерелятивистскими квантовыми криптосистемами на неортогональных состояниях — это знание длины квантового канала связи, что, на наш взгляд, является небольшой платой за те преимущества, которые может дать релятивистская квантовая криптография.

В квантовых криптосистемах обнаружение любых попыток подслушивания гарантируется следующими двумя фундаментальными, тесно связанными между собой запретами квантовой механики.

1. Невозможность процесса

$$|\varphi_0\rangle \otimes |A\rangle \mapsto |\varphi_0\rangle \otimes |\varphi_0\rangle \otimes |A_0\rangle\,, \qquad \langle\varphi_0|\varphi_1\rangle \neq 0\,. \quad (1)$$
$$|\varphi_1\rangle \otimes |A\rangle \mapsto |\varphi_1\rangle \otimes |\varphi_1\rangle \otimes |A_1\rangle\,,$$

Такой запрет на копирование неизвестного квантового состояния называется no-cloning-теоремой.

2. Невозможность получения информации об одном из неортогональных состояний без их возмущения, т.е. запрет на процесс

$$|\varphi_0\rangle \otimes |A\rangle \mapsto U\bigl(|\varphi_0\rangle \otimes |A\rangle\bigr) = |\varphi_0\rangle \otimes |A_0\rangle\,, \qquad |A_0\rangle \neq |A_1\rangle, \quad (2)$$
$$|\varphi_1\rangle \otimes |A\rangle \mapsto U\bigl(|\varphi_1\rangle \otimes |A\rangle\bigr) = |\varphi_1\rangle \otimes |A_1\rangle\,,$$

где $|A\rangle$ — состояние прибора наблюдателя, U — некоторый унитарный оператор, описывающий совместную эволюцию исследуемого состояния и состояния прибора. Данные запреты, по сути, являются одним из проявлений фундаментального принципа неопределенности Гейзенберга о невозможности одновременного измерения наблюдаемых, которым отвечают некоммутирующие операторы.

Для ортогональных состояний запреты на копирование и извлечение информации без их возмущения отсутствуют. В рамках нерелятивистской квантовой механики наблюдаемым $\rho_0 = |\varphi_0\rangle\langle\varphi_0|$ и $\rho_1 = |\varphi_1\rangle\langle\varphi_1|$ отвечают коммутирующие измеряющие операторы, являющиеся ортогональными проекторами $\mathcal{P}_{0,1} = |\varphi_{0,1}\rangle\langle\varphi_{0,1}|$ ($[\mathcal{P}_0, \mathcal{P}_1] = 0$). Ограничения (1), (2) являются, по сути, геометрическим свойством векторов состояний квантовой системы $|\varphi_{0,1}\rangle$ в гильбертовом пространстве состояний. Если не использовать каких-то дополнительных фундаментальных ограничений на измеримость ортогональных квантовых состояний, то последние в силу достоверной различимости не могут применяться для целей квантовой криптографии. Такими дополнительными фундаментальными ограничениями являются ограничения на измеримость квантовых состояний, налагаемые специальной теорией относительности.

Для ортогональных состояний нет запрета на достоверное различение без их возмущения [9], точнее говоря, теорема [9] об этом случае ничего не говорит. Часто произносимые при интерпретации данной теоремы слова о том, что ортогональное состояние "проходит" через вспомогательную систему $|A\rangle$, взаимодействует с ней по мере прохождения и изменяет ее состояние, не соответствуют содержанию теоремы. В теореме ничего подобного нет, в том смысле, что она носит чисто геометрический характер и утверждает, что вектор состояния вспомогательной системы $|A\rangle$ может быть унитарно повернут в зависимости от входного вектора $|\varphi_{0,1}\rangle$ и переведен в новое состояние $|A_0\rangle$ или $|A_1\rangle$ без изменения входного вектора. При этом неявно предполагается, что входной вектор $|\varphi_{0,1}\rangle$ доступен как целостный объект, т.е. для совершения унитарного преобразования U нужно иметь доступ ко всему пространству состояний $\mathcal{H}_{\varphi_{0,1}}$, в котором отличен от нуля носитель состояния, в противном случае преобразование не будет унитарным. Тот факт, что в доказательстве фигурирует лишь вектор состояния как целостный объект $|\varphi_{0,1}\rangle$ без внутренней координатной "начинки", как раз и подразумевает, что вектор состояния при унитарном преобразовании участвует "сразу целиком".

Для любой реальной физической системы гильбертово пространство $\mathcal{H}_{\varphi_{0,1}}$ неизбежно привязано к пространству-времени Минковского, в котором состояние имеет амплитуду (сглаживающую волновую функцию). Доступ к гильбертову пространству состояний, таким образом, подразумевает доступ к той области пространства-времени, в которой отлична от нуля амплитуда (волновая функция) состояния. Если же доступна лишь часть такой области, то тогда даже ортогональные состояния невозможно достоверно скопировать или различить. Последнее более или менее очевидно, поскольку никакой процесс, в том числе копирование или различение, не может иметь вероятность исхода бóльшую, чем доля нормировки состояний, которая набирается в доступной пространственно-временнóй области и тем самым автоматически в доступной части гильбертова пространства. Грубо говоря, чтобы с достоверностью скопировать или различить ортогональные состояния, они нужны сразу и целиком.

Поэтому, если амплитуда состояния отлична от нуля в некоторой конечной области пространства-времени, то слова о том, что состояние доступно целиком, означают доступ к этой области. В нерелятивистской квантовой механике, где нет ограничений на предельную скорость, доступ к любой конечной области может быть получен мгновенно. В квантовой теории поля, где существуют ограничения на предельную скорость, доступ к состоянию целиком может быть получен только в том случае, если протяженное состояние предварительно унитарно преобразовано к состоянию с амплитудой, отличной от нуля лишь в сколь угодно малой пространственной области. После этого можно пользоваться теоремой [9]. Согласно принципу релятивистской причинности [39] такое унитарное преобразование состояния, заданного в конечной пространственно-временнóй области, в состояние, локализованное в сколь угодно малой пространственной области, может быть осуществлено лишь за конечное время. Минимально необходимое время определяется из условия накрытия "прошлой" частью светового конуса исходной пространственной области, в которой была отлична от нуля амплитуда состояния (рис. 1а). Вершина этого конуса находится в сколь угодно сильно локализованной области (точке), в которую унитарно преобразуется исходная амплитуда состояния. Каждое из пары ортогональных состояний, унитарно преобразованных ("собранных") в локализованной области, может быть после этого достоверно скопировано или различено. Поскольку речь идет о безмассовых состояниях квантованного поля (фотонов), которые распространяются с предельно допустимой скоростью, то такое унитарное преобразование и дальнейшее копирование приведет к сдвигу (задержке)

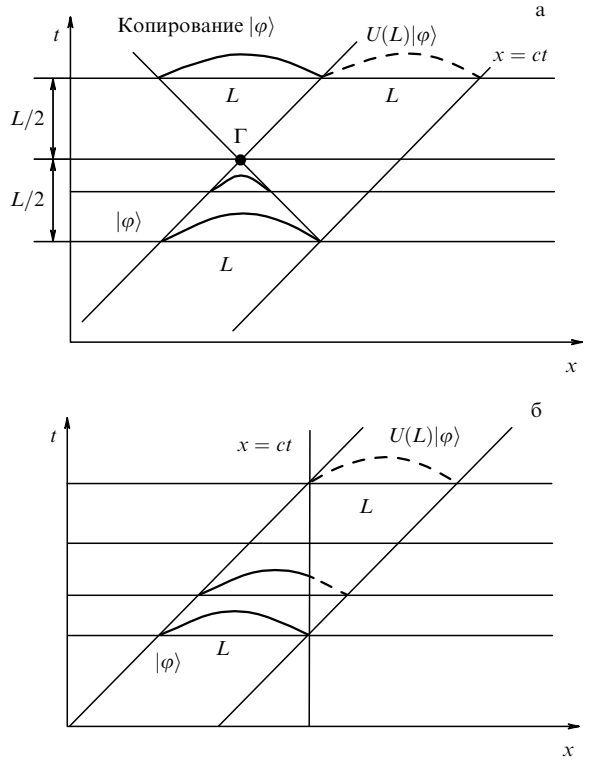

Рис. 1.

состояний в пространстве-времени по отношению к таковым в случае их свободной эволюции (распространения). Данное обстоятельство позволяет детектировать любые попытки подслушивания. Отметим, что ограничения, накладываемые на измерения в релятивистской области, исследовались впервые в работе Л.Д. Ландау и Р. Пайерлса [40], а впоследствии в работе Н. Бора и Л. Розенфельда [41][3].

Иначе говоря, для ортогональных состояний безмассового квантованного поля теорема о запрете копирования звучит следующим образом. Ортогональные состояния могут быть с вероятностью, сколь угодно близкой к единице, скопированы. В результате копирования получаются состояния с той же формой амплитуд, но сдвинутые (транслированные в пространстве-времени). То есть разрешен более слабый, чем в нерелятивистском случае, процесс в (1). Таким образом, имеем

$$|\varphi_0\rangle \mapsto \big(U_L|\varphi_0\rangle\big) \otimes \big(U_L|\varphi_0\rangle\big)\,,$$
$$|\varphi_1\rangle \mapsto \big(U_L|\varphi_1\rangle\big) \otimes \big(U_L|\varphi_1\rangle\big)\,. \qquad (3)$$

Здесь U_L — оператор трансляции в пространстве-времени вдоль ветви светового конуса, $L = \Delta(x-t)$ — размер области, в которой отлична от нуля амплитуда состояний (считаем для краткости, что оба состояния отличны от нуля в одной и той же пространственно-временно́й области, но различаются формой амплитуд $\varphi_{0,1}(x-t)$).

Аналогично модифицируется теорема [9] о различении ортогональных состояний — разрешен лишь более слабый процесс по сравнению с таковым в нерелятивистском случае (2):

$$|\varphi_0\rangle \otimes |A\rangle \mapsto \big(U_L|\varphi_0\rangle\big) \otimes |A_0\rangle\,,$$
$$|\varphi_1\rangle \otimes |A\rangle \mapsto \big(U_L|\varphi_1\rangle\big) \otimes |A_1\rangle\,, \qquad |A_0\rangle \neq |A_1\rangle\,. \qquad (4)$$

Сказанное удобно пояснить с помощью диаграмм, приведенных на рис. 1.

Поскольку амплитуда состояний безмассового квантованного поля, распространяющихся в одном направлении оси x, зависит лишь от разности $x-t$, то можно фиксировать время и считать переменной координату, либо наоборот. Рассмотрим оба случая. Этими двумя случаями исчерпываются все ситуации. Пусть задано одно из ортогональных состояний с амплитудой $\varphi(x-t)$, распространяющихся со скоростью света ($c=1$, индекс состояния 0 или 1 для краткости пока опустим). Пусть состояние сосредоточено в области L, в том смысле, что $\int_L \big|\varphi(x-t_0)\big|^2\,\mathrm{d}x \approx 1$, $\varphi_{0,1}(x-t_0)$ есть амплитуда на временно́м срезе t_0.

Чтобы иметь *сразу все значения амплитуды состояния при всех x в момент t_0* в той области, в которой она отлична от нуля, необходимо совершить унитарное преобразование сразу над всем состоянием. Пусть унитарное преобразование над амплитудой состояния — $U\varphi_{0,1}(x-t_0) = \tilde{\varphi}_{0,1}(x'-t)$ $(t > t_0)$, тогда амплитуда нового состояния $\tilde{\varphi}(x'-t)$ может быть отлична от нуля уже в меньшей пространственной области. По существу, минимальный размер области по x' к моменту t диктуется релятивистским принципом причинности, который был сформулирован в окончательной форме Н.Н. Боголюбовым [39]. Матричные элементы унитарного оператора отличны от нуля только тогда, когда точки (x,t_0) и (x',t) лежат внутри "прошлой" части светового конуса, выпущенного из точки Г, и накрывающей область, в которой отлична от нуля амплитуда состояния в момент t_0. К моменту не более раннему, чем L, амплитуда исходного состояния может быть унитарным образом преобразована в состояние со сколь угодно сильно локализованной амплитудой в окрестности Г. Принципиально важно, что это будет уже *другое* состояние, отличное от исходного $\varphi(x-t_0)$. К моменту Г доступны значения амплитуды состояния при всех x сразу (мгновенно). Теперь можно мгновенно получить исход измерения и иметь полную (с вероятностью 1) информацию о состоянии. Если пара исходных состояний ортогональна, то можно унитарным преобразованием получить также пару ортогональных состояний к моменту Г и, следовательно, достоверно отличить одно от другого (теперь уже можно воспользоваться теоремой [9] о достоверной различимости ортогональных состояний). Подчеркнем еще раз, что это будут уже *другие* ортогональные состояния, отличные от исходных. "Восстановление" или копирование состояния также может быть реализовано обратным унитарным преобразованием, "направленным" вперед во времени. Состояние с той же формой амплитуды, что и исходное, может быть получено к моменту не более раннему, чем момент, определяемый релятивистской причинностью. Амплитуда состояния с той же формой, как у исходного, находится в передней части светового конуса, выпущенного из точки Г. Полученное состояние также *другое* по сравнению с исходным, в том смысле, что оно запаздывает по времени по отношению к исходному состоянию,

[3] Важным является вопрос о локализации состояний в релятивистской области (в связи с этим см. [42–47]).

которое успело бы распространиться вперед по x к моменту L как раз на величину L, если бы не было попыток копирования или получения информации о нем (рис. 1а). Пока речь шла о получении информации о состояниях в канале с вероятностью 1. Те же самые рассуждения годятся для получения информации с вероятностью, меньшей единицы. Задержка при этом будет меньше L (см. рис. 1).

Подобные рассуждения работают и в нерелятивистском случае. Если игнорировать ограничения специальной теории относительности, то в предыдущем рассмотрении нужно отбросить ту часть, которая апеллирует к световому конусу. При этом унитарные преобразования можно делать формально мгновенно, и из рассмотрения можно исключить даже явное присутствие координаты, оставив неявно только то, что при унитарном преобразовании состояния доступны целиком (целиком мгновенно доступна вся пространственная область).

Аналогично можно провести рассуждения, когда состояние унитарным образом преобразуется в состояние вспомогательной локализованной системы. Пример такого унитарного преобразования имеет место при "остановке" света [48]. Данное унитарное преобразование переводит состояние фотонного поля в вакуумное состояние вследствие его безмассовости и невозможности иметь нулевую скорость распространения, а состояние атомной системы — в некоторое новое состояние. Преобразование, будучи унитарным, также требует доступа ко всем значениям амплитуды фотонного пакета в точке локализации атомной системы. Такой доступ достигается естественным образом по мере распространения пакета со скоростью света и достижения им локализованной атомной системы ("вхождение" пакета целиком в атомную систему). Данный процесс, если речь идет о получении результата с вероятностью 1, также требует времени L (однофотонный пакет должен целиком "войти" в атомную систему). При этом фотонное поле оказывается в *другом — вакуумном — состоянии*, а вспомогательная система оказывается в новом состоянии в зависимости от входного фотонного состояния. К моменту времени L с вероятностью 1 можно выяснить, что это за состояние и приготовить такое же, но с задержкой на L, которая неизбежна в этом случае в отличие от случая свободного распространения исходного пакета (рис. 1б).

Таким образом, любое получение информации об одном из ортогональных состояний приводит к неизбежной их модификации — трансляции в пространстве-времени (*задержке*).

Для дальнейшего также важно, что никакая эволюция безмассового квантованного поля, взаимодействующего с окружением (другими квантовыми и классическими степенями свободы в канале), не может привести к "сжатию" состояния, в том смысле, что нормировка состояния будет набираться в пространственной области, выходящей за световой конус, которая меньше, чем таковая при свободном распространении (рис. 2). Как правило, такое взаимодействие приведет к тому, что состояние будет смешанным, но носитель матрицы плотности в пространстве-времени не может быть "сжат" и выведен за световой конус (см. рис. 2). В противном случае это позволяло бы передавать информацию с помощью квантовых состояний быстрее скорости света. Действительно, пусть имеется одно из пары

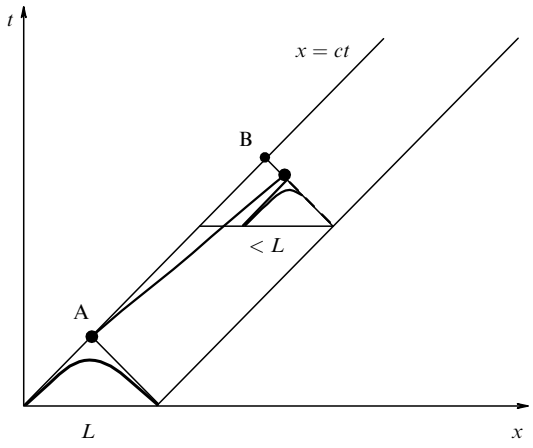

Рис. 2.

ортогональных квантовых состояний (см. рис. 2). Участник A может извлечь классическую информацию из квантового состояния не ранее, чем в момент времени, определяемый условием накрытия амплитуды состояния "прошлой" частью светового конуса. После этого он может передать уже классическую информацию участнику B. Такая передача не может быть сделана быстрее, чем со скоростью света (наблюдатели соединены ветвью светового конуса (см. рис. 2)). Если бы в результате своей эволюции квантовое состояние в канале могло "сжаться" таким образом, что при накрытии состояния "прошлой" частью светового конуса вершина конуса оказывалась в области, пространственноподобной световому конусу с вершиной в точке A, одна из ветвей которого проходит через точку B, то наблюдатель B мог бы извлечь классическую информацию из квантового состояния раньше, чем мог бы передать ее со скоростью света участник A, поскольку вершина светового конуса, накрывающего "сжатое" квантовое состояние, выходит в пространственноподобную область.

С точки зрения криптографии сказанное означает, что шум в канале не дает подслушивателю возможности ни скопировать, ни получить информацию о состоянии раньше, чем это диктуется ограничениями релятивистской причинности и квантовой механикой (*фактически квантовой теорией поля*).

Привлечение новых фундаментальных физических принципов в квантовую криптографию позволяет сформулировать новый подход к обеспечению секретности передачи ключей, который снимает трудности, имеющиеся в нерелятивистской квантовой криптографии (см. детали в [38]). Подобные квантовые криптосистемы естественно называть релятивистскими.

Рассмотрим кратко теоретическую предельно достижимую скорость генерации секретных ключей в квантовой криптографии[4] через квантовый канал связи с конечной частотной полосой пропускания W.

В классическом случае, когда сигнал описывается функцией времени $x(t)$, число бит информации, которое

[4] Сейчас скорость распространения ключей в квантовой криптографии определяется отнюдь не принципиальными ограничениями, а уровнем технологии, точнее, временем возвращения лавинных фотодетекторов в исходное состояние после регистрации фотона и эффектами афтерпалсинга (afterpulsing).

может быть передано через канал с конечной частотной полосой, согласно знаменитой теореме В.А. Котельникова об отсчетах, доказанной в 1933 г. [49] (см. приложение к докладу Н.В. Котельниковой в данном выпуске), определяется числом независимых степеней свободы сигнала, в значение которого можно кодировать передаваемую информацию. В наш цифровой век теорема об отсчетах "работает" в любом устройстве, обрабатывающем или передающем информацию в цифровом виде.

Классический сигнал с конечной частотной полосой описывается функцией времени $x(t)$. На конечном временно́м интервале $(-T, T)$ сигнал $x(t)$, как впервые было показано В.А. Котельниковым [49], определяется $2WT$ степенями свободы в том смысле, что при разложении по ортогональной системе функций,

$$x(t) = \sum_n x_n \theta_n(t)\,, \tag{5}$$

достаточно ограничиться $2WT$ слагаемыми, для которых

$$\int_{-T}^{T} \theta_n(t)\,\theta_m(t)\,\mathrm{d}t = \delta_{nm}\lambda_n(WT), \quad \lambda_n(WT) \approx 1\,. \tag{6}$$

В работе [49] в качестве базисных функций $\theta_n(t)$ использовались так называемые отсчетные функции

$$\theta_n(t) = \frac{\sin W(t - n\pi/W)}{W(t - n\pi/W)}\,. \tag{7}$$

Базис из отсчетных функций обладает замечательным свойством: значения коэффициентов разложения по этому базису x_n равны значениям самого сигнала $x(t)$ в отсчетные моменты времени. Это означает, что для описания непрерывного сигнала в любой момент времени достаточно знать его значения лишь в $2WT$ точках по времени.

Ниже нам будет удобнее использовать другие базисные функции. Число таких функций, наиболее сильно локализованных в окне $(-T, T)$, при этом остается прежним. Кроме того, данные функции возникают и в квантовом случае, где они играют роль одночастичных амплитуд (волновых функций) для фотонов, которые наиболее сильно локализованы во временно́м окне $(-T, T)$.

Ортогональность базисных функций с носителем в конечной частотной полосе W приводит к условию

$$\begin{aligned}
&\int_{-T}^{T} \theta_n(t)\,\theta_m(t)\,\mathrm{d}t = \\
&\quad = \frac{1}{\pi}\int_{k\leqslant|W|}\int_{k'\leqslant|W|} \theta_n(k)\,\frac{\sin(k-k')T}{k-k'}\,\theta_m(k')\,\mathrm{d}k\,\mathrm{d}k'\,, \\
&\theta_n(k) = \frac{1}{2\pi}\int_{-\infty}^{\infty} \theta_n(t)\exp(-\mathrm{i}kt)\,\mathrm{d}t\,.
\end{aligned} \tag{8}$$

Базисные функции ортогональны, если они удовлетворяют следующему интегральному уравнению:

$$\lambda_n(WT)\,\theta_n(k) = \frac{1}{\pi}\int_{k\leqslant|W|} \frac{\sin(k-k')T}{k-k'}\,\theta_n(k')\,\mathrm{d}k'\,. \tag{9}$$

Собственные числа зависят только от произведения WT и образуют бесконечную серию

$$1 > \lambda_1(WT) > \lambda_2(WT) > \ldots > 0\,.$$

Степень локализации квадрата n-й функции во временно́м окне $(-T, T)$ определяется собственным числом

$$\int_{-T}^{T} \theta_n^2(t)\,\mathrm{d}t = \lambda_n(WT)\,. \tag{10}$$

Интегральное уравнение (9) определяет так называемые функции вытянутого сфероида (prolate spheroidal functions) [50]. Собственные числа обладают тем замечательным свойством, что при больших WT, $WT \gg 1$, разбиваются на две группы: одна с номерами $n < 2WT$, для которых $\lambda_n(WT) \approx 1$, и другая с номерами $n > 2WT$, для которых $\lambda_n(WT) \approx 0$. Размер переходной от одного поведения к другому области по номерам составляет $\approx \ln(4\pi WT)$, т.е. для любого $\varepsilon > 0$

$$\lim_{WT\to\infty} \lambda_{2WT(1-\varepsilon)}(WT) = 1\,, \qquad \lim_{WT\to\infty} \lambda_{2WT(1+\varepsilon)}(WT) = 0\,. \tag{11}$$

Это означает, что при больших WT имеется не более $2WT(1-\varepsilon)$ ортогональных (различимых) функций, вклад которых во временно́м окне $(-T, T)$ стремится к единице. Если использовать более чем $2WT(1+\varepsilon)$ степеней свободы, то среди них будут состояния, которые дают во временно́м окне $(-T, T)$ исчезающе малый вклад. При больших WT сигнал $x(t)$ в конечной частотной полосе на конечном временно́м интервале описывается не более чем $2WT$ независимыми (ортогональными и различимыми) степенями свободы и может быть задан $2WT$ независимыми коэффициентами разложения x_n.

Если классический источник с конечной частотной полосой W генерирует сигналы, локализованные во временно́м окне $(-T, T)$ таким образом, что коэффициенты разложения задаются в соответствии с заданным распределением вероятностей $p(x_n)$ на множестве этих коэффициентов x_n (значений амплитуд сигнала), то энтропия источника определяется величиной

$$\begin{aligned}
&I\big(WT, p(x_n)\big) = 2WTH\big(p(x_n)\big)\,, \\
&H\big(p(x_n)\big) = -\sum_n p(x_n)\log p(x_n)\,.
\end{aligned} \tag{12}$$

Далее, если эти сигналы передаются через идеальный (без шума) физический канал связи, например с той же частотной полосой пропускания W, то энтропия источника (12), по существу, совпадает со взаимной информацией между входом и выходом такого канала связи. Тогда пропускная способность в единицу времени (источник + физический канал связи + приемник) определяется как

$$C = \lim_{T\to\infty}\frac{1}{2T}\max_{\{p(x_n)\}} I\big(WT, p(x_n)\big) = W\max_{\{p(x_n)\}} H\big(p(x_n)\big)\,. \tag{13}$$

Для сравнения классического и квантового случаев нам потребуются следующие качественные соображения. В рамках классической физики нет никаких формальных запретов на изменение значений коэффициентов разложения x_n (амплитуд ортогональных базисных функций $\theta_n(t)$) со сколь угодно малой дискретностью (непрерывно). Поскольку интенсивность классического сигнала x_n^2, например для электромагнитного поля, в каждой отдельной моде $\theta_n(t)$ представляет собой с

точностью до множителя $\approx \hbar W$ число фотонов в этой моде, то изменение уровня сигнала может происходить с конечной дискретностью. Для кодирования информации в значения x_n необходимы, по крайней мере, два значения ($x_n^2 \propto N_{\max}$, $N_{\max}$ — максимальное число возможных значений x_n^2). Полное число разных значений для всех мод есть $(\sqrt{N_{\max}})^{2WT}$. Если каждое значение выбирается с равной вероятностью, то энтропия источника (12) равна

$$I\bigl(WT,\, p(x_n)\bigr) = 2WT \log\bigl(\sqrt{N_{\max}}\bigr)\,. \tag{14}$$

Пропускная способность (8) в единицу времени при минимальном уровне сигнала ($N_{\max} = 2$) есть

$$C = W. \tag{15}$$

Формула (15), *являющаяся по существу другой записью теоремы В.А. Котельникова об отсчетах, определяет количество информации в битах на одну степень свободы, которое может быть передано в единицу времени.*

Строго говоря, применять формулы, когда числа заполнения мод малы, нельзя.

Далее нас будет интересовать пропускная способность в однофотонном режиме (числа заполнения мод равны единице). Именно эта величина и будет определять скорость генерации ключа в квантовой криптографии через канал с конечной частотной полосой W.

Приведенные рассуждения были нужны для качественного сравнения классического и квантового случаев. Наша задача будет фактически сводиться к подсчету для источника с конечной частотной полосой W числа возможных ортогональных многофотонных состояний, локализованных во временно́м окне $(-T, T)$. Рассмотрим сначала однофотонные состояния на выходе источника, которые затем распространяются в одном направлении ($k > 0$) и имеют носитель в конечной частотной полосе W ($k \in [0, W]$). Будем игнорировать поляризационные степени свободы при кодировании в различные формы амплитуд состояний, опять ради более близкой аналогии с классическим случаем. Для упрощения выкладок положим $c = \hbar = 1$. Имеем

$$|\varphi^e\rangle = \int_0^W \frac{\mathrm{d}k}{k}\, \varphi\bigl(k, k_0 = |k|\bigr)\, a^+(k)|0\rangle = \int_{-\infty}^{\infty} \mathrm{d}\tau\, \varphi(\tau)|\tau\rangle\,, \tag{16}$$

$\varphi(k,k)$ ($k > 0$) и $\varphi(\tau)$ — амплитуды однофотонного пакета в импульсном и пространственно-временно́м представлении соответственно,

$$\begin{aligned} &\varphi(\tau) = \frac{1}{2\pi}\int_0^W \frac{\mathrm{d}k}{\sqrt{k}}\, \exp\left(-\mathrm{i}k\tau\right) \varphi(k,k)\,,\\ &|\tau\rangle = \int_0^W \frac{\mathrm{d}k}{\sqrt{k}}\, \exp\left(\mathrm{i}k\tau\right) |k\rangle\,, \qquad |k\rangle = a^+(k)|0\rangle\,. \end{aligned} \tag{17}$$

Для безмассового поля $\tau = x - t$ зависит лишь от разности координаты и времени, следовательно, если результат измерения имел место в окрестности точки x в момент времени t, то такой же результат может быть получен в точке x' в момент $t' = t + (x' - x)$. Ниже, упоминая о временно́м окне, будем иметь в виду, что $(-T, T)$ означает $(-(x-t), (x-t))$.

Нам потребуется выбрать амплитуду (волновую функцию) однофотонного пакета с носителем в конечной частотной полосе W так, чтобы от нее набиралась максимальная нормировка в пространственно-временно́й области — окне $(-T, T)$. Формально степень локализации описывается измерением в этом окне. Любое измерение над однофотонным пакетом во временно́м окне описывается разложением единицы в одночастичном подпространстве, которое имеет вид

$$\begin{aligned} I^{(1)} &= \int_0^W \frac{\mathrm{d}k}{k}\, |k\rangle\langle k| = I^{(1)}(T) + I^{(1)}(\overline{T}) = \\ &= \int_{-T}^{T} \frac{\mathrm{d}\tau}{2\pi}\, |\tau\rangle\langle\tau| + \int_{-(\infty,\infty)/(-T,T)} \frac{\mathrm{d}\tau}{2\pi}\, |\tau\rangle\langle\tau|\,. \end{aligned} \tag{18}$$

С учетом (12), (13) оператор, соответствующий временно́му окну $(-T, T)$, представляется в виде

$$I^{(1)}(T) = \sum_{n=1}^{\infty} \lambda_n(WT)|\theta_n\rangle\langle\theta_n|\,, \qquad |\theta_n\rangle = \int_0^W \frac{\mathrm{d}k}{k}\, \theta_n(k)|k\rangle\,. \tag{19}$$

Сами функции $\theta_n(k)$ являются собственными функциями интегрального уравнения, отличающегося от (9) только тем, что интегрирование ведется по отрезку $[0, W]$. Число функций, локализованных во временно́м окне $(-T, T)$, будет равно WT. По сути, векторы $|\theta_n\rangle$ являются собственными векторами оператора $I^{(1)}(T)$ — в базисе этих векторов оператор диагонален. Любое измерение над исходным состоянием, когда доступны исходы лишь во временно́м окне, эквивалентно измерениям над следующей эффективной матрицей плотности:

$$\begin{aligned} \rho(T) = &\sum_{n,n'} \lambda_n(WT)\, \lambda_{n'}(WT)|\theta_n\rangle\langle\theta_n|\varphi\rangle\langle\varphi|\theta_{n'}\rangle\langle\theta_{n'}| + \\ &+ \mathrm{Tr}\left\{I^{(1)}(\overline{T})|\varphi\rangle\langle\varphi|\right\}|?\rangle\langle?|\,. \end{aligned} \tag{20}$$

Здесь введено формальное состояние $|?\rangle$, которое является ортогональным всем состояниям и описывает исходы вне временно́го окна. Такие исходы отвечают ситуации, в которой внутри окна вообще не было срабатывания аппаратуры. Эффективная матрица плотности с учетом таких исходов, которым должен быть приписан неопределенный (inconclusive) результат, имеет единичный след. При больших WT можно выбрать одно из WT ортогональных (различимых) однофотонных состояний, которое с вероятностью, сколь угодно близкой к единице ($\lambda_n(WT) \approx 1$), локализовано в окне $(-T, T)$ и которое имеет в этом окне эффективную матрицу плотности

$$\begin{aligned} &\rho_n(T) = \lambda_n(WT)|\theta_n\rangle\langle\theta_n| + \bigl(1 - \lambda_n(WT)\bigr)|?\rangle\langle?|\,, \qquad (21)\\ &1 \leqslant n \leqslant WT. \end{aligned}$$

Пусть источник генерирует в рабочем временно́м окне $(N = WT)$-фотонные состояния вида

$$\begin{aligned} &|\theta_{n_1}; \ldots; \theta_{n_N}\rangle = \\ &\quad = \int_0^W \ldots \int_0^W \frac{\mathrm{d}k_1}{k_1} \ldots \frac{\mathrm{d}k_N}{k_N}\, \theta_{n_1}(k_1) \ldots \theta_{n_N}(k_N)|k_1, \ldots, k_N\rangle\,,\\ &|k_1, \ldots, k_N\rangle = a^+(k_1) \ldots a^+(k_N)|0\rangle\,, \end{aligned} \tag{22}$$

где обобщенные базисные векторы полностью симметричны по перестановкам частиц:

$$|k_1, \ldots, k_N\rangle = \sqrt{\frac{k_1 k_2 \ldots k_N}{N!}} \sum_{\{j\}} \delta(k_1 - q_{j_1}) \ldots \delta(k_N - q_{j_N})\,, \tag{23}$$

символ $\{j\}$ означает, что суммирование происходит по всем перестановкам. Сконструируем теперь $(N=WT)$-фотонные матрицы плотности. Число заполнения каждой одночастичной моды при этом равно 1. Множество векторов в (17) с различными индексами образуют собственные векторы оператора $I^{(N)}(T)$ в $(N=WT)$-фотонном подпространстве, аналогично однофотонному случаю. Имеем

$$I^{(N)}=\int_0^W\dots\int_0^W\frac{\mathrm{d}k_1}{k_1}\dots\frac{\mathrm{d}k_N}{k_N}|k_1,\dots,k_N\rangle\langle k_1,\dots,k_N|= \\ =I^{(N)}(T)+I^{(N)}(\overline{T}), \tag{24}$$

$$I^{(N)}(T)=\int_{-T}^T\dots\int_{-T}^T\frac{\mathrm{d}\tau_1}{2\pi}\dots\frac{\mathrm{d}\tau_N}{2\pi}|\tau_1;\dots;\tau_N\rangle\langle\tau_1;\dots;\tau_N|= \\ =\sum_{n_1,\dots,n_N=1}^{\infty}\lambda_{n_1}(WT)\dots\lambda_{n_N}(WT)|\theta_{n_1};\dots;\theta_{n_N}\rangle\langle\theta_{n_1};\dots;\theta_{n_N}|. \tag{25}$$

Подсчитаем число ортогональных $(N=WT)$-фотонных состояний. Если бы $N=WT$ фотонов являлись бы различимыми, то число ортогональных $(N=WT)$-фотонных векторов в окне $(-T,T)$, локализованных в нем с вероятностью почти единица, равнялось бы N^N (без учета поляризационных степеней свободы). В силу принципа тождественности бозонов (фотонов) число таких векторов, которое обозначим для удобства как $2^{M(WT)}$, равно числу способов размещения $N=WT$ тождественных частиц по $N=WT$ состояниям. Таким образом, имеем [51]

$$2^{M(WT)}=\frac{(N+N-1)!}{(N-1)!N!},\qquad N=WT, \tag{26}$$

при больших N с учетом формулы Стирлинга $(N!\approx(N/e)^N\sqrt{2\pi N})$

$$\log 2^{M(WT)}=2N\log 2=2WT. \tag{27}$$

Пусть в каждом рабочем временно́м окне источник генерирует с равной вероятностью одно из $2^{M(WT)}$ ортогональных $(N=WT)$-фотонных состояний. Если источник работает достаточно долго, то статистический ансамбль, в который может быть закодирована классическая информация, описывается матрицей плотности

$$\rho\big(M(WT)\big)=\frac{1}{2^{M(WT)}}\sum_{n_1,\dots,n_N}|\theta_{n_1};\dots;\theta_{n_N}\rangle\langle\theta_{n_1};\dots;\theta_{n_N}|. \tag{28}$$

Максимальная энтропия фон Неймана ансамбля достигается при равновероятном выборе векторов. Информация в конечном временно́м окне $(-T,T)$ извлекается из эффективной матрицы плотности

$$\rho(T)=\frac{1}{2^{M(WT)}}\times \\ \times\sum_{n_1,\dots,n_N}\lambda_{n_1}(WT)\dots\lambda_{n_N}(WT)|\theta_{n_1};\dots;\theta_{n_N}\rangle\langle\theta_{n_1};\dots;\theta_{n_N}|+ \\ +\frac{1}{2^{M(WT)}}\sum_{n_1,\dots,n_N}\big(1-\lambda_{n_1}(WT)\dots\lambda_{n_N}(WT)\big)|?\rangle\langle?|. \tag{29}$$

При больших WT нельзя сконструировать статистический ансамбль, построенный из более чем $2^{M(WT)}$ ортогональных $(N=WT)$-фотонных состояний. Классическая информация, которая может быть закодирована в ансамбль $\rho\big(M(WT)\big)$ и извлечена из $\rho(T)$ (29), дается величиной $\chi\big(\rho(T)\big)$, следующей из фундаментального неравенства, полученного впервые А.С. Холево (см. подробности в [52]). Поскольку состояния $|\theta_{n_1};\dots;\theta_{n_N}\rangle$ и $|?\rangle$ являются чистыми, то $\chi\big(\rho(T)\big)$ совпадает с энтропией фон Неймана для $\rho(T)$, отсюда имеем

$$\chi\big(\rho(T)\big)=-\mathrm{Tr}\left\{\rho(T)\log\rho(T)\right\}= \\ =-\sum_{n_1,\dots,n_N}\frac{\lambda_{n_1}(WT)\dots\lambda_{n_N}(WT)}{2^{M(WT)}}\times \\ \times\log\left(\frac{\lambda_{n_1}(WT)\dots\lambda_{n_N}(WT)}{2^{M(WT)}}\right)- \\ -\sum_{n_1,\dots,n_N}\left(\frac{1-\lambda_{n_1}(WT)\dots\lambda_{n_N}(WT)}{2^{M(WT)}}\right)\times \\ \times\log\left(\frac{1-\lambda_{n_1}(WT)\dots\lambda_{n_N}(WT)}{2^{M(WT)}}\right). \tag{30}$$

Пропускная способность в единицу времени определяется пределом, который аналогичен формуле (15) для классического случая. С учетом того, что вклад второй суммы в (30) стремится к нулю, получим

$$C=\lim_{T\to\infty}C_T,\qquad C_T=\frac{\log\left(2^{M(WT)}\right)}{2T}=\frac{M(WT)}{2T}=W. \tag{31}$$

Источник генерирует во временно́м окне $(N=WT)$-фотонные состояния так, что число фотонов на выходе источника в единицу времени $\sim W$ и энергия на один фотон $\sim\hbar W$. Соответственно, число фотонов во временно́м окне $(-T,T)$ равно WT (именно число, а не среднее число фотонов, поскольку состояния $|\theta_{n_1};\dots;\theta_{n_N}\rangle$ в (22) являются собственными векторами оператора числа фотонов, отвечающих собственному числу частиц $N=WT$)[5]. Мощность на выходе источника постоянна и пропорциональна $(\hbar W)W$. Минимальность источника в квантовом случае означает, что число ортогональных одночастичных амплитуд $\theta_n(t)$, из которых строится симметричная по перестановкам частиц $(N=WT)$-фотонная амплитуда, равно WT, и число фотонов — WT, т.е. число заполнения в пересчете на отдельную одночастичную амплитуду равно 1.

Информация в классическом случае кодируется в значения амплитуд (грубо, в число фотонов) в ортогональных модах, в квантовом же случае — в различные ортогональные многофотонные состояния [53]. Последние из-за тождественности фотонов принципиально являются запутанными внутри каждого временно́го окна $2T$. Такое кодирование квантового источника можно рассматривать как квантовый аналог теоремы В.А. Котельникова об отсчетах, когда числа заполнения одночастичных мод доведены до однофотонного уровня.

Удивительным является то, что пропускная способность в единицу времени на одну степень свободы в классическом случае (15), следующая из теоремы В.А. Котельникова об отсчетах, "буквенно" совпадает с аналогичной пропускной способностью в квантовом

[5] Строго говоря, всюду под WT нужно понимать целую часть $[WT]$.

случае (31). Однако способы кодирования в классическом и квантовом случаях оказываются разными.

В заключение следует отметить, что появление новых направлений в области конфиденциальной передачи информации является естественным логическим развитием идей, возникших в работах основателей данной области.

Список литературы

1. Котельников В А, Отчет (1941)
2. Shannon C E "Communication theory of secrecy systems" *Bell Syst. Technol. J.* **28** 656 (1949)
3. Vernam G S "Cipher printing telegraph systems for secret wire and radio telegraphic communications" *J. Am. Inst. Elect. Eng.* **55** 109 (1926)
4. Wiesner S *SIGACT News* **15** (1) 78 (1983)
5. Diffie W, Hellman M "New directions in cryptography" *IEEE Trans. Inform. Theory* **IT-22** 644 (1976)
6. Rivest R L, Shamir A, Adleman L "A method for obtaining digital signatures and public-key cryptosystems" *Commun. ACM* **21** 120 (1978)
7. Bennett C H, Brassard G "Quantum cryptography: public-key distribution and coin tossing", in *Proc. of IEEE Intern. Conf. on Computers Systems, and Signal Processing, Bangalore, India, December 1984* (New York: IEEE Press, 1984) p. 175
8. Wootters W K, Zurek W H "A single quantum cannot be cloned" *Nature* **299** 802 (1982)
9. Bennett C H *Phys. Rev. Lett.* **68** 3121 (1992); Bennett C H, Brassard G, Mermin N D *Phys. Rev. Lett.* **68** 557 (1992)
10. "Информационная технология. Криптографическая защита информации. Функция хэширования", Государственный стандарт Российской Федерации, ГОСТ Р 34.11-94 (Дата введения 01.01.95)
11. Bennett C H, Brassard G, Crépeau C, Maurer U M "Generalized privacy amplification" *IEEE Trans. Inform. Theory* **41** 1915 (1995)
12. Carter J L, Wegman M N "Universal classes of hash functions" *J. Comput. Syst. Sci.* **18** 143 (1979)
13. Muller A, Breguet J, Gisin N *Europhys. Lett.* **23** 383 (1993); Muller A, Zbinden H, Gisin N *Nature* **378** 449 (1995); *Europhys. Lett.* **33** 335 (1996)
14. Marand Ch, Townsend P D *Opt. Lett.* **20** 1695 (1995); Townsend P D *Nature* **385** 47 (1997); *IEEE Photon. Technol. Lett.* **10** 1048 (1998)
15. Hughes R J et al., in *Advances in Cryptology — CRYPTO'96: 16th Annual Intern. Cryptology Conf., Santa Barbara, Calif., USA, August 1996. Proc.* (Lecture Notes in Comput. Sci., Vol. 1109, Ed. Koblitz) (Heidelberg: Springer, 1996) p. 329; Hughes R J, Morgan G L, Peterson C G *J. Mod. Opt.* **47** 533 (2000)
16. Sun P C, Mazurenko Y, Fainman Y *Opt. Lett.* **20** 1062 (1995); Mazurenko Yu T, Giust R, Goedgebuer J P *Opt. Commun.* **133** 87 (1997); Молотков С Н *ЖЭТФ* **114** 526 (1998)
17. Grosshans F et al. *Nature* **421** 238 (2003)
18. Stucki D et al. *New J. Phys.* **4** 41 (2002); quant-ph/0203118
19. Bennett C H et al. *J. Cryptology* **5** 3 (1992)
20. Hughes R J, Morgan G L, Peterson C G *J. Mod. Opt.* **47** 533 (2000)
21. Kosaka H et al. *Electron. Lett.* **39** 1199 (2003); quant-ph/0306066
22. Kimura T et al. *Jpn. J. Appl. Phys.* **43** L1217 (2004); quant-ph/0403104
23. Bethune D S, Risk W P *New J. Phys.* **4** 42 (2002)
24. Bethune D S, Navarro M, Risk W P *Appl. Opt.* **41** 1640 (2002); quant-ph/0104089
25. Elliott C, Pearson D, Troxel G, quant-ph/0307049
26. Rarity J G et al. *New J. Phys.* **4** 82 (2002)
27. Hughes R J et al. *New J. Phys.* **4** 43 (2002); quant-ph/0206092
28. Kurtsiefer C et al. *Proc. SPIE* **4917** 25 (2002)
29. Acín A, Gisin N, Scarani V *Phys. Rev. A* **69** 012309 (2004); quant-ph/0302037
30. Mayers D, Yao A, quant-ph/9802025
31. Biham E et al., quant-ph/9912053
32. Shor P W, Preskill J *Phys. Rev. Lett.* **85** 441 (2000); quant-ph/0003004
33. Tamaki K, Koashi M, Imoto N *Phys. Rev. A* **67** 032310 (2003); quant-ph/0212161
34. Lütkenhaus N *Phys. Rev. A* **61** 052304 (2000)
35. Brassard G et al. *Phys. Rev. Lett.* **85** 1330 (2000)
36. Gilbert G, Hamrick M "Practical Quantum Cryptography: A Comprehensive Analysis (Part I)", Mitre Technical Report, MTR00W0000052 (McLean, VA: Mitre Corporation, 2000); quant-ph/0009027
37. Beveratos A et al. *Phys. Rev. Lett.* **89** 187901 (2002); quant-ph/0206136
38. Молотков С Н *ЖЭТФ* **126** 771 (2004)
39. Боголюбов Н Н, Ширков Д В *Введение в теорию квантованных полей* (М.: Наука, 1973)
40. Landau L D, Peierls R *Z. Phys.* **69** 56 (1931) [Ландау Л Д, Пайерлс Р, в кн.: Ландау Л Д *Собрание трудов* Т. 1 (М.: Наука, 1969) с. 56]; Landau L D, Peierls R *Z. Phys.* **62** 188 (1930) [Ландау Л Д, Пайерлс Р, в кн.: Ландау Л Д *Собрание трудов* Т. 1 (М.: Наука, 1969) с. 33]
41. Bohr N, Rosenfeld L *Kgl. Danske Vidensk. Selskab. Math.-Fys. Medd.* **12** (8) 3 (1933) [Бор Н, Розенфельд Л *Собрание научных трудов* Т. 1 (М.: Наука, 1969) с. 39]
42. Jaffee A M *Phys. Rev.* **158** 1454 (1967)
43. Hegerfeldt G C *Phys. Rev. D* **10** 3320 (1974); Hegerfeldt G C, Ruijsenaars S N M *Phys. Rev. D* **22** 377 (1980)
44. Киржниц Д А *УФН* **90** 129 (1966)
45. Винер Н, Пэли Р *Преобразование Фурье в комплексной области* (М.: Наука, 1964)
46. Bialynicki-Birula I *Phys. Rev. Lett.* **80** 5247 (1998)
47. Newton T D, Wigner E P *Rev. Mod. Phys.* **21** 400 (1949)
48. Fleischhauer M, Lukin M D *Phys. Rev. Lett.* **84** 5094 (2000)
49. Котельников В А, в сб. *Всесоюзный энергетический комитет. Материалы к I Всесоюз. съезду по вопросам технической реконструкции дела связи и развития слаботочной промышленности* (М.: Управление связи РККА, 1933) с. 1 – 19; переизд.: *О пропускной способности "эфира" и проволоки в электросвязи* (М.: Институт радиотехники и электроники МЭИ (ТУ), 2003)
50. Slepian D, Pollak H O *Bell Syst. Tech. J.* **40** 43 (1961); Slepian D "Some asymptotic expansions for prolate spheroidal wave functions" *J. Math. Phys.* (Cambridge, Mass.: MIT) **44** 99 (1965)
51. Ландау Л Д, Лифшиц Е М *Статистическая физика* Ч. 1 (М.: Физматлит, 1995)
52. Холево А С *Проблемы передачи информации* **8** (1) 63 (1972); **15** (4) 3 (1979); *УМН* **53** (6) 193 (1998); *Введение в квантовую теорию информации* (Сер. Современная математическая физика. Проблемы и методы, Вып. 5) (М.: Изд-во МЦНМО, 2002)
53. Молотков С Н *Письма в ЖЭТФ* **78** 1087 (2003)