ЖЭТФ, 2004, том 126, вып. 4 (10), стр. 771–798

КВАНТОВАЯ КРИПТОГРАФИЯ НА МНОГОФОТОННЫХ СОСТОЯНИЯХ ДЛЯ СВОБОДНОГО ПРОСТРАНСТВА: О ПЕРЕДАЧЕ СЕКРЕТНЫХ КЛЮЧЕЙ НА СПУТНИКИ

С. Н. Молотков*

Институт физики твердого тела Российской академии наук
142432, Черноголовка, Московская обл., Россия

Московский государственный университет им. М. В. Ломоносова
119991, Москва, Россия

Поступила в редакцию 3 марта 2004 г.

В квантовой криптографии, секретность которой основана на факте достоверной неразличимости неортогональных квантовых состояний, имеются принципиальные проблемы, связанные с затуханием в квантовом канале связи и неоднофотонностью источника. Потенциально данные трудности могут перевести квантовую криптографию из безусловно секретной в условно секретную. Поскольку ограничения нерелятивистской квантовой механики, используемые для построения протоколов распространения ключей в квантовой криптографии, во многом исчерпаны, требуется привлечение новых физических принципов. Использование такого фундаментального принципа как принцип релятивистской причинности в квантовой криптографии позволяет сформулировать новый подход к обеспечению безусловной секретности квантовых криптосистем. В этом подходе снимаются упомянутые выше трудности. Подобные квантовые криптосистемы естественно называть релятивистскими. Показано, что релятивистские квантовые криптосистемы остаются безусловно секретными: во-первых, при любом затухании в квантовом канале связи затухание снижает лишь скорость генерации ключа, но не влияет на его секретность, во-вторых, не требуется строгая однофотонность источника, достаточно лишь присутствия однофотонной компоненты в состояниях лишь с некоторой вероятностью. Схема остается секретной даже при сколь угодно малой доле (вероятности) однофотонной компоненты. Формально это означает, что состояние может иметь сколь угодно большое среднее число фотонов. Доля однофотонной компоненты влияет лишь на скорость генерации ключа, но не на его секретность.

PACS: 03.65.Bz, 42.50.Dv, 89.70.+c

1. ВВЕДЕНИЕ

Квантовая криптография, точнее, распространение секретного ключа по открытым квантовым каналам связи, представляет собой, пожалуй, единственный способ реализации абсолютно стойких криптографических систем шифрования с одноразовыми ключами [1–3]. На сегодняшний день создано несколько различных прототипов квантовых криптосистем на базе оптоволоконных линий связи. По сообщениям японской группы [4], достигнутая дальность передачи секретного ключа в квантовой криптосистеме с так называемой самокомпенсацией при помощи фарадеевских оптоволоконных отражателей составляет 100 км. Предыдущий рекорд принадлежал швейцарской группе (67 км) [5]. Недавно фирмой MagiQ был анонсирован вариант коммерческой системы квантовой криптографии с длиной оптоволоконной линии связи в 120 км. Имеющиеся прототипы квантовых криптосистем используют в основном следующие принципы кодирования. 1) Информация о ключе кодируется в поляризационные степени свободы [6]. 2) Фазовое кодирование, при котором используются несбалансированный интерферометр Маха–Цандера и информация кодируется в разность фаз, которая набирается на приемном и передающем плечах интерферометра [7, 8]. 3) Квантовые криптосистемы с частотной модуляцией несу-

*E-mail: molotkov@issp.ac.ru

щей частоты [9]. 4) Квантовая криптография на когерентных состояниях с использованием гомодинного детектирования на приемном конце [10]. Наибольший прогресс достигнут в оптоволоконных криптосистемах с фазовым кодированием и самокомпенсацией с использованием фарадеевских отражателей [4, 5, 11].

Недавно 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) [12].

Создано несколько прототипов квантовых криптосистем, осуществляющих передачу секретного ключа через открытое пространство [13, 14]. Рекорд по дальности (из опубликованных данных) составляет 23.4 км как в дневное, так и ночное время. Целью использования квантовых криптосистем, работающих через открытое пространство, является генерация секретных ключей между наземными объектами и низкоорбитальными спутниками (до высот около 1000 км) или между наземными объектами через спутники. По оценкам сотрудников фирмы QinetiQ, занимающейся разработкой систем связи со спутниками, на основе анализа схем квантовой криптографии это может быть осуществлено в ближайшие годы, поскольку уже существующий технологический уровень достаточен, а планируемая цена является уже вполне приемлемой [15]. Более того, распространение ключей через спутники имеет потенциально гораздо более широкое применение. Проведение подобных экспериментов планируется в течение ближайшего года.

Все упомянутые схемы, за исключением систем на основе гомодинного детектирования, требуют принципиально однофотонного режима. Однако, из-за того что истинно однофотонные источники на сегодняшний день еще не созданы (отметим, что существует продвижение и в этом направлении на уровне лабораторных прототипов [16]), в качестве «однофотонного» источника используется лазерное излучение, ослабленное до уровня $\mu = 0.1$–0.3 фотона в импульсе. Однако, поскольку в когерентном состоянии, которым описывается излучение лазера, задано лишь среднее число фотонов, существует вероятность появления более чем одного фотона в канале связи. Реально ослабленное лазерное излучение в канале связи выглядит как статистическая смесь с разным числом фотонов. В этом случае возникают серьезные, хотя на сегодняшний день скорее потенциальные, проблемы с секретностью квантовых криптосистем относительно некоторых специфических атак на передаваемый ключ (см., например, [17, 18]). Кроме того, из-за малых средних чисел заполнения (например, при заполнении порядка 0.1 примерно 90 % посылок оказываются холостыми) существенно снижается скорость генерации секретного ключа.

Принципиальной проблемой для секретности является затухание в квантовом канале связи. Проблема с затуханием 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, а в том (и это гораздо более критично), что начиная с некоторой величины затухания нельзя гарантировать секретность переданного ключа (см. [18], а также ниже). Затухание в оптоволоконных линиях связи определяется длиной канала связи. На сегодняшний день критическая длина, до которой система остается секретной, строго не известна. Оценки варьируются от нескольких десятков до 150 км [18].

Если проанализировать основные квантовые криптографические протоколы и доказательства их секретности в канале с затуханием (основными являются протоколы BB84 и B92, остальные являются в том или ином виде производными от них), то видно, что требуется и используется, явно или неявно, априорная информация о потоке ошибок (Quantum Bit Error Rate), связанных с затуханием. Например, если затухание в канале связи изменяется в течение времени протокола передачи ключа, то изменяется и поток ошибок (даже в отсутствие подслушивателя). При этом, если протокол подразумевает постоянство QBER, никакую секретность переданного ключа вообще невозможно гарантировать. Если в оптоволоконных квантовых криптосистемах затухание еще можно считать постоянным (для одномодового оптоволокна на длине волны 1550 нм оно составляет 0.17–0.25 дБ/км), то при передаче через открытое пространство это уже не так, поскольку состояние атмосферы невозможно контролировать. Поэтому хотелось бы иметь протоколы распространения ключа, которые были бы устойчивы 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 гарантируется лишь фунда-

ментальными 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 (теорема No Cloning [19]) неизвестного квантового состояния и принципиальной достоверной неразличимости неортогональных квантовых состояний (теорема Bennett [20]). Грубо говоря, данные протоколы формулируются в гильбертовом пространстве $\mathcal{H}$. Тот факт, что все измерения и распространение квантовых состояний имеют место 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 с потерей секретности за счет затухания требуются другие дополнительные фундаментальные ограничения, вытекающие 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 являются истинно релятивистскими безмассовыми частицами (состояниями безмассового квантованного поля), которые распространяются с предельно допустимой скоростью. Поэтому было бы неестественно не использовать дополнительные возможности, предоставляемые природой.

Таким образом, неоднофотонность источника и затухание, вообще говоря, приводят к тому, что квантовые криптосистемы могут перестать быть безусловно секретными.

Ниже будут приведены несколько вариантов квантовых криптосистем 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, требуется знание длины квантового канала связи. 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 не однофотонных состояний. Формально схема остается работоспособной при любом среднем числе фотонов в квантовом состоянии. 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) происходят в пространстве-времени и состояния ортогональны, 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 более чем 40 % (при $\mu \approx 1$). Напомним, например, что для протокола BB84 секретность гарантируется лишь до уровня ошибок в 11 % [21, 22].

Единственным дополнительным требованием по сравнению с нерелятивистскими квантовыми криптосистемами на неортогональных состояниях в релятивистской квантовой криптографии требуется знание длины квантового канала связи, что, на наш взгляд, является небольшой платой за те преимущества, которые мы получаем в релятивистском случае.

Ниже мы приведем несколько примеров реализаций квантовых криптосистем.

2. ФИЗИЧЕСКИЕ ОСНОВЫ КВАНТОВОЙ КРИПТОГРАФИИ

Секретность ключа в квантовой криптографии основана не на предположениях об ограниченных технических или вычислительных ресурсах подслушивателя, как это имеет место в классических схемах шифрования, например, RSA [23, 24], а на фун-

даментальных запретах, диктуемых законами природы — квантовой механикой. В квантовых криптосистемах обнаружение любых попыток подслушивания гарантируется следующими двумя фундаментальными, тесно связанными между собой запретами квантовой механики.

1) Невозможность процесса

$$\begin{aligned} &|\varphi_0\rangle \otimes |A\rangle \longmapsto |\varphi_0\rangle \otimes |\varphi_0\rangle \otimes |A_0\rangle, \\ &|\varphi_1\rangle \otimes |A\rangle \longmapsto |\varphi_1\rangle \otimes |\varphi_1\rangle \otimes |A_1\rangle, \\ &\quad \text{если} \quad \langle\varphi_0|\varphi_1\rangle \neq 0. \end{aligned} \tag{1}$$

Такой запрет на копирование неизвестного квантового состояния называется теоремой No Cloning.

2) Невозможность получить информацию об одном из неортогональных состояний без их возмущения, т. е. запрет на процесс

$$\begin{aligned} &|\varphi_0\rangle \otimes |A\rangle \longmapsto U(|\varphi_0\rangle \otimes |A\rangle) = |\varphi_0\rangle \otimes |A_0\rangle, \\ &|\varphi_1\rangle \otimes |A\rangle \longmapsto U(|\varphi_1\rangle \otimes |A\rangle) = |\varphi_1\rangle \otimes |A_1\rangle, \\ &\quad \text{если} \quad |A_0\rangle \neq |A_1\rangle, \end{aligned} \tag{2}$$

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

Для ортогональных состояний запреты на копирование и извлечение информации без их возмущения отсутствуют. В рамках нерелятивистской квантовой механики наблюдаемым

$$\rho_0 = |\varphi_0\rangle\langle\varphi_0|, \quad \rho_1 = |\varphi_1\rangle\langle\varphi_1|$$

соответствуют коммутирующие измеряющие операторы, являющиеся ортогональными проекторами

$$\mathcal{P}_{0,1} = |\varphi_{0,1}\rangle\langle\varphi_{0,1}|, \quad [\mathcal{P}_0, \mathcal{P}_1] = 0.$$

Ограничения (1), (2) являются 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 быть использованы для целей квантовой криптографии. Такими дополнительными фундаментальными ограничениями являются ограничения на измеримость квантовых состояний, диктуемые специальной теорией относительности. Фотоны как квантовые носители информации являются принципиально релятивистскими объектами (состояниями безмассового квантованного поля). Поэтому учет дополнительных релятивистских ограничений, как будет показано ниже, приводит к принципиально новым возможностям создания квантовых криптосистем, секретность которых основывается на дополнительных ограничениях на измеримость квантовых состояний, связанных как с квантовой природой состояний, так и с запретами специальной теории относительности.

Главными и принципиальными ограничениями для практического использования схем квантовой криптографии, секретность которых основана только на достоверной неразличимости неортогональных состояний, являются неоднофотонность источника и затухание в канале связи. Почему криптосистема перестает быть секретной, проще всего можно продемонстрировать на примере так называемого протокола B92, использующего пару неортогональных состояний. При достаточном затухании подслушиватель может использовать стратегию приема–перепосыла состояний и иметь полную информацию о передаваемом ключе, оставаясь при этом незамеченным. Данная стратегия, далеко не самая оптимальная для подслушивателя, сводится к следующему. Подслушиватель в каждой посылке использует измерения, которые описываются разложением единицы

$$\begin{aligned} I = \mathcal{P}_0^{\perp} + \mathcal{P}_1^{\perp} + \mathcal{P}_?, \quad \mathcal{P}_0^{\perp} = a(I - |\varphi_0\rangle\langle\varphi_0|), \\ \mathcal{P}_1^{\perp} = a(I - |\varphi_1\rangle\langle\varphi_1|), \end{aligned} \tag{3}$$

$$\mathcal{P}_?^{\perp} = I - \mathcal{P}_0^{\perp} - \mathcal{P}_1^{\perp}, \quad a = \frac{1}{1 + |\langle\varphi_0|\varphi_1\rangle|}.$$

Пространство результатов Ω (исходов) состоит из трех событий $\Omega = \{0, 1, ?\}$. Вероятность события «0» равна

$$p_0 = \langle\varphi_0|\mathcal{P}_1^{\perp}|\varphi_0\rangle < 1,$$

отлична от нуля только на входном состоянии $|\varphi_0\rangle$ и равна нулю на втором входном состоянии $|\varphi_1\rangle$. Аналогично событие 1 будет иметь место с вероятностью

$$p_1 = \langle\varphi_1|\mathcal{P}_0^{\perp}|\varphi_1\rangle < 1,$$

отличной от нуля только на входном состоянии $|\varphi_1\rangle$. Из-за неортогональности (соответственно, достоверной неразличимости) состояний будут также иметь место исходы «?» с неопределенным исходом (inconclusive result) с вероятностью

$$p_? = \langle\varphi_0|\mathcal{P}_?|\varphi_0\rangle = \langle\varphi_1|\mathcal{P}_?|\varphi_1\rangle = |\langle\varphi_0|\varphi_1\rangle| \neq 0.$$

Поэтому, если имели место исходы «0» или «1», состояния в канале подслушиватель идентифицирует однозначно. При исходе «?» подслушиватель не может сказать, какое состояние было послано. Если в канале имеется затухание, то не все посланные состояния достигают приемного конца. В этом случае, если подслушиватель получил результат «?», он просто блокирует канал связи и ничего не перепосылает. С некоторой критической величины затухания невозможно детектировать вторжение в канал связи, при этом подслушиватель имеет полную информацию о ключе и остается незамеченным. Аналогичная стратегия имеет место для другого известного протокола BB84.

Следующим критическим обстоятельством для обеспечения секретности является требование однофотонности источника квантовых состояний. Формально, как это следует из (1), (2), может быть использована любая пара неортогональных состояний, даже многофотонных. Однако процедура измерения на приемном конце в этом случае должна уметь различать такие состояния. Грубо говоря, должно быть такое измерение, которое реализует проекции на векторы многофотонных состояний. В качестве источника используется лазер, излучение которого является когерентным состоянием, в котором задано лишь среднее число фотонов $\langle n\rangle = \mu$. Однако, из-за того что не существует фазовой привязки, в канале подслушиватель видит матрицу плотности, а не чистое когерентное состояние:

$$\rho = \int \frac{d\theta}{2\pi} |\mu e^{i\theta}\rangle\langle \mu e^{-i\theta}| = \\ = \sum_n p(\mu, n)|n\rangle\langle n|, \quad p(\mu, n) = e^{-\mu}\frac{\mu^n}{n!}. \quad (4)$$

Распределение числа фотонов в статистической смеси задается пуассоновским распределением. В реальных экспериментах используется ослабленное когерентное излучение с $\mu \approx 0.1$–0.3, в котором с вероятностями $p(\mu, n)$ встречаются фоковские состояния с различными числами заполнения $n = 0, 1, \ldots$

Это означает, что с вероятностью $p(0, \mu)$ можно обнаружить нуль фотонов, с вероятностью $p(1, \mu)$ — один фотон и т. д. Неоднофотонность источника приводит к возможности так называемой PNS-атаки (Photon Number Splitting) [17, 18] — атаки с отводом части фотонов подслушивателем. Измерение, которое позволяет невозмущающим образом определить число фотонов в канале, описывается разложением единицы вида

$$I = \bigoplus_{n=0}^{\infty} \mathcal{P}_n = \bigoplus_{n=0}^{\infty} |n\rangle\langle n|. \quad (5)$$

Формально измерение, позволяющее различать неразрушающим образом число фотонов в линии, дается измерением с двумя исходами

$$I = \mathcal{P}_{n=1} + \mathcal{P}_{n\neq 1}, \quad \mathcal{P}_{n\neq 1} = I - \mathcal{P}_{n=1}. \quad (6)$$

Поэтому, если имеется исход в $\mathcal{P}_{n=1}$ (обнаружен один фотон), посылка блокируется. В противном случае, если имеется исход в $\mathcal{P}_{n\neq 1}$ (в линии более одного фотона), подслушиватель может «отщепить» часть фотонов для измерения, а остальную послать через канал с меньшим затуханием. При наличии затухания не все посланные фотоны достигают приемного конца, поэтому подобного рода атака останется не детектируемой [18]. Здесь сразу обратим внимание на то, что использование одномодовых (монохроматических) состояний фотонов

$$|n\rangle = (a^+_{k_0})^n|0\rangle$$

(k_0 — частота, $\hbar = c = 1$) является сильной идеализацией, поскольку такое одномодовое состояние представляет собой монохроматическую волну, бесконечно протяженную в пространстве и во времени. Измерение, описывающееся формальным проектором $|n\rangle\langle n|$, подразумевает доступ к состоянию как целостному объекту, т. е. ко всей бесконечно большой области пространства, где амплитуда состояния (плоской волны) отлична от нуля, что требует бесконечного времени из-за конечной предельной скорости. Если протокол обмена использует лишь геометрические свойства состояний в гильбертовом пространстве, то он формально является протоколом вне времени, в приведенных выше рассуждениях нигде время явно или неявно не фигурирует. Тот факт, что измерение с целью выяснения того, сколько фотонов присутствует в линии связи, требует большого (формально бесконечного) времени, для таких протоколов не имеет значения. Реально любые состояния имеют некоторую конечную протяженность в пространстве (соответственно, конечную частотную полосу). В этом случае при формулировке протокола обмена в реальном времени для различения количества фотонов в линии (как и для любых других измерений) неизбежно требуется конечное время, которое приводит к задержке результатов измерений на приемном конце. Это позволяет детектировать любые попытки подслушивания.

Таким образом, если затухание таково, что подслушиватель, осуществляя неразрушающее измере-

ние числа фотонов в канале связи, может блокировать все посылки, когда в канале имеется однофотонное фоковское состояние, то протокол становится несекретным.

Для ортогональных состояний нет запрета на их достоверное различение без возмущения [20]. Точнее говоря, теорема из работы [20] в этом случае об этом 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. Эта теорема носит чисто геометрический характер. В ней утверждается, 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 $\mathcal{H}_{\varphi_{0,1}}$, где 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, где состояние имеет амплитуду (сглаживающую волновую функцию). Доступ к гильбертову пространству состояний неизбежно подразумевает доступ к той части пространства-времени, где отлична от нуля амплитуда (волновая функция) состояния. Если же доступна лишь часть пространства, где отлична от нуля амплитуда состояний, то в этом случае 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 больше, чем доля нормировки состояний, которая набирается в доступной пространственно-временной области и тем самым автоматически в доступной части гильбертова пространства. А именно, 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, тогда то, что состояние доступно целиком, означает 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 лишь 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 из [20]. Из-за принципа релятивистской причинности [25] такое унитарное преобразование состояния, заданного в конечной пространственно-временной 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, где амплитуда состояния была отлична от нуля (см. рис. 1). 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 различимо. Поскольку речь идет о безмассовых состояниях квантованного поля (фотонов), которые распространяются с предельно допустимой скоростью, такое унитарное преобразование и дальнейшее копирование приведут к сдвигу (задержке) состояний в пространстве-времени по сравнению с исходной свободной эволюцией (распространением) состояний. Данное обстоятельство позволяет детектировать любые попытки подслушивания. Отметим, что впервые ограничения, накладываемые на измерения в релятивистской области, исследовались в работе Ландау и Пайерлса [26], а затем были продолжены в работе Бора и Розенфельда [27].

Иначе говоря, для ортогональных состояний безмассового квантованного поля теорема о запрете копирования звучит следующим образом. Ортогональные состояния могут быть скопированы с вероятностью сколь угодно близкой к единице. При этом в результате копирования получаются состояния с той же формой амплитуд, но сдвинутые (транслированные) в пространстве-времени. Таким образом, разрешен более слабый по сравнению с нерелятивистским случаем (1) процесс. Имеем

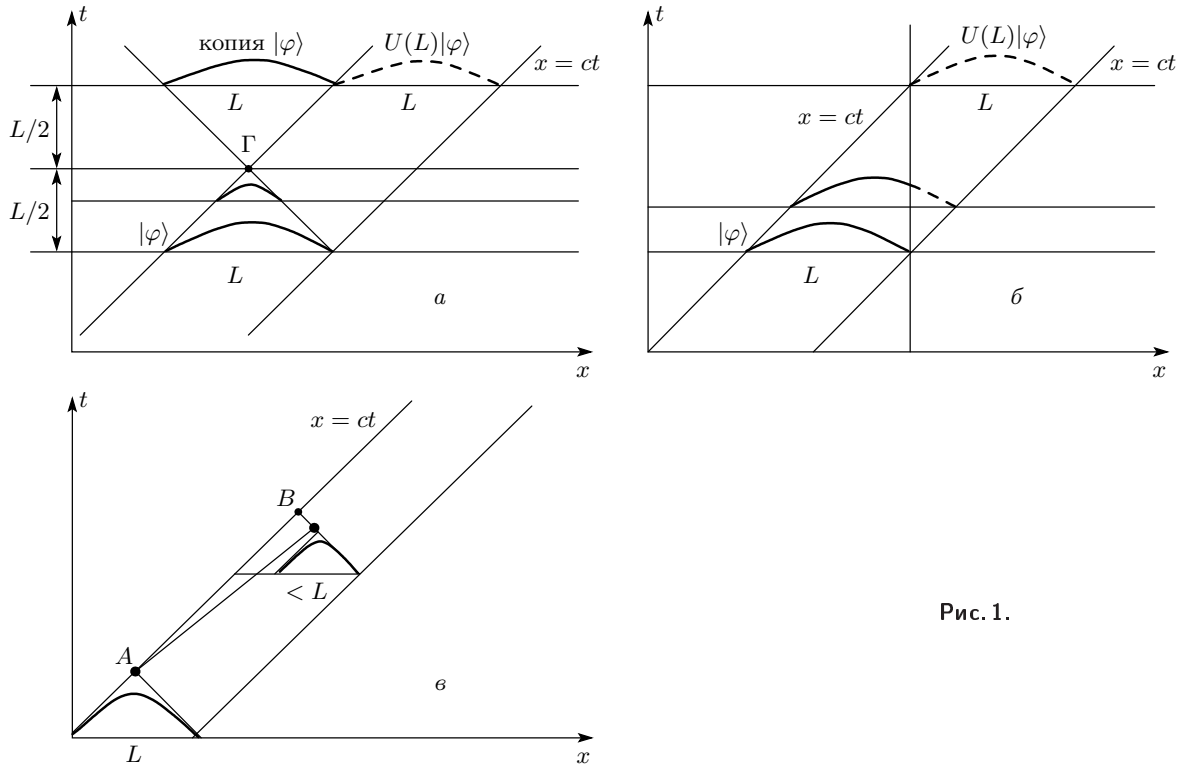

Рис. 1.

$$|\varphi_0\rangle \mapsto (U_L|\varphi_0\rangle) \otimes (U_L|\varphi_0\rangle),$$
$$|\varphi_1\rangle \mapsto (U_L|\varphi_1\rangle) \otimes (U_L|\varphi_1\rangle). \tag{7}$$

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

Аналогично модифицируется теорема [20] о различении ортогональных состояний, разрешен лишь более слабый по сравнению с нерелятивистским случаем (2) процесс. Имеем

$$|\varphi_0\rangle|A\rangle \mapsto (U_L|\varphi_0\rangle) \otimes |A_0\rangle,$$
$$|\varphi_1\rangle \otimes |A\rangle \mapsto (U_L|\varphi_1\rangle) \otimes |A_1\rangle, \quad |A_0\rangle \neq |A_1\rangle. \tag{8}$$

Сказанное удобно пояснить при помощи диаграмм, представленных на рис. 1 *а, б*.

Поскольку амплитуда состояний безмассового квантованного поля, распространяющихся в одном направлении оси x, зависит лишь от разности $x - t$, можно провести рассуждения, фиксируя время и считая переменной координату (либо наоборот). Сделаем это для обоих случаев, которыми исчерпываются все возможные 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

$$\int\limits_L |\varphi(x - t_0)|^2 dx \approx 1,$$

$\varphi_{0,1}(x - t_0)$ — амплитуда на временном срезе t_0.

Чтобы иметь сразу все значения амплитуды состояния при всех x в момент t_0 в той области, где она отлична от нуля, необходимо совершить унитарное преобразование сразу над всем состоянием. Пусть выполнено унитарное преобразование над амплитудой состояния

$$U\varphi_{0,1}(x - t_0) = \tilde{\varphi}_{0,1}(x' - t), \quad t > t_0.$$

Амплитуда нового состояния $\tilde{\varphi}(x' - t)$ может быть отлична от нуля уже в меньшей пространственной области. Минимальный размер области по x' к моменту t диктуется релятивистским принципом причинности, который был сформулирован в окончательной форме Боголюбовым [25]. 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, накрывающей область, где отлична от нуля амплитуда состояния в момент t_0. К моменту не ранее чем момент времени 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, чем исходное $\varphi(x-t_0)$. К моменту Г доступны значения амплитуды состояния при всех x сразу (мгновенно). Теперь можно мгновенно получить исход измерения и иметь полную (с вероятностью единица) информацию о состоянии. Если пара исходных состояний была ортогональна, унитарным преобразованием можно получить также пару ортогональных состояний к моменту Г и, соответственно, достоверно отличить одно состояние от другого (теперь уже можно воспользоваться теоремой [20] о достоверной различимости ортогональных состояний). Подчеркнем еще раз, что это будут уже другие ортогональные состояния, отличные от исходных. «Восстановление» или копирование состояния 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 ранее, чем это диктуется релятивистской причинностью. Амплитуда состояния с той же формой, что и 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, 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. 1*а*). Все сказанное выше относится к получению информации о состояниях в канале с вероятностью единица. Те же самые рассуждения годятся для получения информации с вероятностью меньшей единицы. Задержка при этом будет меньше L (см. рис. 1*а, б*).

Аналогичные рассуждения применимы и в нерелятивистском случае. Если игнорировать ограничения специальной теории относительности, то из предыдущего рассмотрения нужно исключить ту часть рассуждений, которые относятся к световому конусу. При этом унитарные преобразования можно делать формально мгновенно и из рассмотрения даже можно исключить явное присутствие координаты, неявно учитывая 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 [28]. 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 получения результата с вероятностью единица, также требует времени L (однофотонный пакет должен целиком «войти» в атомную систему). При этом фотонное поле оказывается в другом — вакуумном — состоянии, а вспомогательная система — в новом состоянии в зависимости от входного фотонного состояния. К моменту времени L с вероятностью единица можно выяснить, что это за состояние, и приготовить такое же, но с неизбежной задержкой на L, которая будет иметь место по сравнению со свободным распространением исходного пакета (рис. 1*б*).

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 меньшей пространственной области, выходящей за световой конус по сравнению со свободным распространением (см. рис. 1*в*). Как правило, такое взаимодействие приводит к тому, что состояние будет смешанным, но носитель матрицы плотности в пространстве-времени не может быть «сжат» и выведен за световой конус (рис. 1*в*). В противном случае это давало бы возможность передавать информацию при помощи квантовых состояний со скоростью быстрее скорости света. Действительно, пусть имеется одно из пары ортогональных квантовых состояний (рис. 1*в*). 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 на рис. 1*в*). Если бы в результате эволюции квантового состояния в канале оно могло «сжаться» таким образом, что при накрытии состояния прошлой частью светового конуса вершина этого конуса оказывалась бы в пространственно-подобной области по отношению к 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 ее мог бы передать со скоростью света участник A, поскольку вершина светового конуса, накрывающего «сжатое» квантовое состояние, выходит в пространственно-подобную область.

Для криптографии сказанное выше означает, что шум в канале не дает подслушивателю ни скопировать, ни получить информацию о состоянии раньше, чем это определяется диаграммами на рис. 1*а, б* (величина ошибки подслушивателя при условии прохождения временного теста на задержку не может быть меньше, чем величина, определяемая выражениями (31), (41), см. ниже). Это обстоятельство будет принципиально важно для секретности релятивистской квантовой криптографии, которая остается секретной при любом затухании. Поскольку в нашем случае секретность основана на релятивистском принципе причинности для эволюции квантовых состояний, затухание, каким бы оно ни было, не может отменить ограничения, диктуемые релятивистской причинностью.

3. ИНФОРМАЦИОННЫЕ СОСТОЯНИЯ И ИЗМЕРЕНИЯ

Перейдем к описанию схемы на многофотонных когерентных состояниях. В качестве информационных состояний, отвечающих «0» и «1», используется пара ортогональных состояний $\rho_{0,1}$ с конечными неперекрывающимися частотными полосами, ширину которых для простоты будем считать одинаковой. Покажем, что при данной частотной полосе существуют состояния с наиболее сильно локализованной пространственной амплитудой (с наименьшей пространственно-временной протяженностью). Фиксирование конечной частотной полосы является удобным техническим приемом, впоследствии результаты от этого не зависят. Поляризационные степени свободы будем игнорировать как несущественные. Для дальнейшего принципиально важен факт безмассовости фотонного поля.

Поскольку в каждой посылке в канал связи относительная фаза состояний не фиксируется, в канале присутствует состояние, которое описывается матрицей плотности вида

$$\rho_{0,1} = \bigoplus_{n=0}^{\infty} p(n,\mu)|\varphi_{0,1}^{(n)}\rangle\langle\varphi_{0,1}^{(n)}| = \bigoplus_{n=0}^{\infty}\rho_{0,1}, \qquad \langle\varphi_i^{(n)}|\varphi_j^{(n)}\rangle = \delta_{ij}, \tag{9}$$

где

$$|\varphi_j^{(n)}\rangle = \int\ldots\int d\hat{k}_1\ldots d\hat{k}_n\varphi_{0,1}(\hat{k}_1)\ldots \ldots\varphi_{0,1}(\hat{k}_n)\varphi^+(\hat{k}_1)\ldots\varphi^+(\hat{k}_n)|0\rangle, \tag{10}$$

$$\varphi^+(\hat{k}) = \delta(\hat{k}^2)\theta(k_0)a^+(\hat{k}), \quad \hat{k} = (k_0,k). \tag{11}$$

Далее будем рассматривать состояния, распространяющиеся в одном направлении. Именно такие состояния используются при передаче информации. Имеем с учетом (10), (11)

$$|\varphi_j^{(n)}\rangle = \int_0^\infty\ldots\int_0^\infty \frac{dk_1\ldots dk_n}{\sqrt{k_1\ldots k_n}}\,\frac{\varphi_{0,1}(k_1)\ldots\varphi_{0,1}(k_n)}{\sqrt{k_1\ldots k_n}}\times |k_1,\ldots k_n\rangle, \qquad \varphi(k)\equiv\varphi(k,k_0=|k|)\equiv\varphi(k,k_0=k), \tag{12}$$

где

$$|k_1,\ldots k_n\rangle = a^+(\hat{k}_1)\ldots a^+\hat{k}_n)|0\rangle = \sqrt{\frac{k_1\ldots k_n}{n!}}\sum_{\{i\}}\delta(k_1-q_{i_1})\ldots\delta(k_n-q_{i_n}) \tag{13}$$

— обобщенные полностью симметризованные базисные векторы, символ $\{i\}$ означает всевозможные перестановки индексов. Такая запись автоматически учитывает бозевский характер фотонов и их тождественность. Соотношение ортогональности для обобщенных базисных векторов имеет вид

$$\langle k_1\ldots k_n|q_1\ldots q_m\rangle = \delta_{nm}k_1\ldots k_n\sum_{\{i\}}\delta(k_1-q_{i_1})\ldots\delta(k_n-q_{i_n}). \tag{14}$$

Амплитуды ортогональных состояний $\varphi_{0,1}(k)$ заданы в конечных частотных полосах $\Delta k_{0,1}$, ширины которых для краткости выкладок считаем одинаковыми, при этом

$$\mathrm{supp}\varphi_{0,1}(k) \in \Delta k_{0,1}, \quad \mathrm{supp}\varphi_0(k) \bigcap \mathrm{supp}\varphi_1(k) = \emptyset.$$

Для дальнейшего важна только ширина частотных полос, а не их положение. Амплитуды состояний нормированы на единицу:

$$\int\limits_0^\infty |\varphi(k)|^2 dk = 1. \tag{15}$$

Для одномодовых монохроматических состояний

$$|\varphi(k)|^2 \to \delta(k-k_0), \quad |k_1 \dots k_n\rangle \equiv |n\rangle,$$

$$|n\rangle = (a^+(\hat{k}))^n |0\rangle.$$

В координатно-временном представлении амплитуды состояний, распространяющихся в одном направлении, из-за безмассовости фотонов зависят лишь от разности $\tau = x - t$. Имеем

$$|\varphi_{0,1}^{(n)}\rangle = \int\limits_{-\infty}^{\infty} \dots \int\limits_{-\infty}^{\infty} \frac{d\tau_1 \dots d\tau_n}{(2\pi)^n} \varphi(\tau_1) \dots \dots \varphi(\tau_n) |\tau_1 \dots \tau_n\rangle, \tag{16}$$

$$\begin{aligned} \varphi(\tau) &= \int\limits_0^\infty \frac{dk}{\sqrt{k}} e^{ik\tau} \varphi(k), \\ |\tau_1 \dots \tau_n\rangle &= \int\limits_0^\infty \dots \int\limits_0^\infty \frac{dk_1 \dots dk_n}{\sqrt{k_1 \dots k_n}} \times \\ &\times \exp\left[-i(k_1\tau_1 + \dots + k_n\tau_n)\right] |k_1 \dots k_n\rangle. \end{aligned} \tag{17}$$

Тот факт, что амплитуды зависят лишь от разности $\tau = x - t$, означает, что если результат измерений может быть получен в момент, например, t в окрестности точки x, то с той же вероятностью результат может быть получен из-за распространения амплитуды состояния со скоростью света в окрестности точки x' в момент $t' + (x' - x)$. Из-за того что состояние всегда имеет амплитуду, зависящую от пространственно-временного аргумента $x-t$, вероятность получения любого результата измерения требует доступа к той области пространства-времени, где отлична от нуля амплитуда состояния. Вероятность любого результата измерения не может быть больше, чем доля нормировки состояния, которая набирается в данной области. Поскольку амплитуда состояния безмассового поля зависит лишь от разности $x - t$, формально нет никакой разницы, как будет получен доступ к области, где отлична от нуля амплитуда. Доступ может быть получен, когда фиксирована координата (условно-локальный прибор). В этом случае состояние «собирается» за конечное время, определяемое эффективной протяженностью амплитуды в пространстве, для того чтобы оно все за счет распространения достигло и «собралось» в окрестности фиксированной точки. Последнее может быть достигнуто унитарным преобразованием, локальным в пространстве, но действующим в течение определенного времени, преобразующим состояние фотонного поля в состояние локализованной в пространстве квантовой системы. При этом из-за безмассовости фотонного поля оно само переводится в вакуумное состояние, а локализованная (например, атомная система, как это имеет в экспериментах по остановке света), переходит в некоторое новое состояние.

Измерение может формально проводиться нелокальным прибором в фиксированный момент времени из-за зависимости амплитуды лишь от разности $x - t$ (нелокальным в том смысле, что взаимодействие состояния с прибором «включается» в некоторый фиксированный момент времени в той области пространства, где в этом момент времени отлична от нуля амплитуда состояния). В этом случае унитарное преобразование нелокально в пространстве и также неизбежно требует конечного времени, поскольку из-за существования предельной скорости и принципа релятивистской причинности оно не может быть проведено быстрее, чем за то время, которое требуется для накрытия прошлой частью светового конуса пространственной области, где отлична от нуля амплитуда состояния в фиксированный момент (срез) времени. В этом случае также необходимо преобразование состояния из пространственной области в фиксированный момент в другое локализованное состояние из-за безмассовости фотонного поля, но неизбежно в более поздний момент.

В любом случае даже для получения результата с вероятностью меньшей единицы необходим доступ к части области, где отлична от нуля амплитуда. Это требует преобразования состояния в некоторое другое (из-за безмассовости) и приводит к задержке. Величина задержки формально может быть любой. Чем меньше задержка, тем к меньшей области может быть получен доступ, тем меньшая доля нормировки будет набираться в этой области. Нашей дальнейшей задачей будет выяснение вопроса о предельных (оптимальных с точки зрения подслушива-

теля) соотношениях между извлечением информации о передаваемом состоянии и производимой при этом задержкой. Далее для краткости будем называть все потенциально возможные измерения измерениями в пространственно-временном окне T, имея в виду приведенные выше пояснения.

4. СООТНОШЕНИЯ МЕЖДУ ЗАДЕРЖКОЙ СОСТОЯНИЙ И ИНФОРМАЦИЕЙ, ПОЛУЧАЕМОЙ ПОДСЛУШИВАТЕЛЕМ: ПРЯМАЯ АТАКА НА КЛЮЧ

В этом разделе после качественного обсуждения мы получим формулы, связывающие вероятность различения состояний в зависимости от различной величины вносимой задержки.

Любое измерение над квантовой системой описывается набором измеряющих операторов (операторно-значными мерами), которые дают разложение единицы. Единичный оператор представляет собой прямую сумму единичных операторов в ортогональных симметризованных n-частичных подпространствах. Поскольку используется пара состояний с носителями в частотных полосах Δk_0 и Δk_1, достаточно ограничиться разложением единицы с использованием базисных векторов в этих полосах. Имеем

$$I = \bigoplus_{n=0,i=0,1}^{\infty} I^{(n)}(\Delta k_i) =$$
$$= \bigoplus_{n=0}^{\infty} \int_{\Delta k_i} \dots \int_{\Delta k_i} \frac{dk_1 \dots dk_n}{k_1 \dots k_n} |k_1 \dots k_n\rangle\langle k_1 \dots k_n| =$$
$$= \bigoplus_{n=0,i=0,1}^{\infty} \int_{-\infty}^{\infty} \dots \int_{-\infty}^{\infty} \mathcal{M}_i^{(n)}(d\tau_1 \dots d\tau_n), \quad (18)$$

где для операторно-значной меры введено обозначение

$$\mathcal{M}_i^{(n)}(d\tau_1 \dots d\tau_n) = |\tau_1 \dots \tau_n\rangle\langle\tau_1 \dots \tau_n| = \frac{d\tau_1 \dots d\tau_n}{(2\pi)^n}, \quad (19)$$

$$|\tau_1 \dots \tau_n\rangle = \int_{\Delta k_i} \dots \int_{\Delta k_i} \frac{dk_1 \dots dk_n}{\sqrt{k_1 \dots k_n}} \times \exp\left[-i(k_1\tau_1 + \dots + k_n\tau_n)\right] |k_1 \dots k_n\rangle. \quad (20)$$

Операторно-значная мера $\mathcal{M}_i^{(n)}(d\tau_1 \dots d\tau_n)$ определяет вероятность результатов измерений в пространственно-временных окнах $(\tau_1, \tau_1 + d\tau_1 \dots \tau_1, \tau_n + d\tau_n)$ на входной матрице плотности. Для n-фотонной компоненты матрицы плотности имеем

$$\Pr^{(n)}(-\infty, \infty) = \mathrm{Tr}\{\rho_{0,1}^{(n)} I(\Delta k_{0,1})^{(n)}\} =$$
$$= \mathrm{Tr}\{\rho_{0,1}^{(n)}(\mathcal{M}_{0,1}^{(n)}(T_1, \dots T_n) + \mathcal{M}_{0,1}^{(n))}(\overline{T}_1, \dots \overline{T}_n)\} =$$
$$= \left\{ \left(\int_{T_1} + \int_{\overline{T}_1} \right) |\varphi_{0,1}(\tau_1)|^2 d\tau_1 \right\} \dots$$
$$\dots \left\{ \left(\int_{T_n} + \int_{\overline{T}_n} \right) |\varphi_{0,1}(\tau_n)|^2 d\tau_n \right\} =$$
$$= (p_{0,1}(T_1) + p_{0,1}(\overline{T}_1)) \dots (p_{0,1}(T_n) + p_{0,1}(\overline{T}_n)). \quad (21)$$

Пусть $n = 1$ (однофотонный пакет) — случай, отвечающий состоянию «0» или «1», тогда вероятность получения результата измерения во всем пространстве равна единице:

$$p_{0,1}(T_1) + p_{0,1}(\overline{T}_1) = 1.$$

Соответственно, если для измерения доступна лишь пространственно-временная область T_1, вероятность получения результата есть

$$p_{0,1}(T_1) < 1.$$

Если исход имел место, то с данной вероятностью из-за ортогональности состояний они достоверно различаются. Однако с вероятностью $p_{0,1}(\overline{T}_1) < 1$ вообще никакого исхода во временном окне T_1 не происходит (формально исход имеет место в остальной, недоступной для наблюдателя пространственно-временной области $\overline{T}_1 = (-\infty, \infty) - T_1$). Отсутствие исхода является для наблюдателя результатом с неопределенным исходом (inconclusive result). При таких исходах вероятность правильного различения одного из двух состояний равна $1/2$, что сводится к вероятности простого угадывания.

Как было отмечено выше, для безмассового фотонного поля доступ к пространственно-временной области, где отлична от нуля амплитуда состояния, неизбежно приводит к задержке (трансляции в пространстве-времени) состояния. Это означает, что получение результата с вероятностью $p_{0,1}(T_1) < 1$ в пространственно-временном окне T_1 требует доступа к области данного размера, что неизбежно приводит к задержке.

Если измерения проводятся на многофотонном входном состоянии (9), то из-за неразличимости (тождественности) фотонов вероятность регистрации во временном окне T с учетом (21) подчиняется следующему условию:

$$1 = \sum_{k=0}^{n} C_n^k p^k(T) p^{n-k}(\overline{T}),$$
$$p^k(T) + p^{n-k}(\overline{T}) = 1, \tag{22}$$

где C_n^k — биномиальный коэффициент. Индексы состояний (0,1) для краткости опущены. Смысл данного условия достаточно прост. Во временном окне T из n тождественных фотонов могут быть зарегистрированы k фотонов и не зарегистрированы $n-k$ фотонов (формально эти $n-k$ фотонов регистрируются вне доступного окна T). Из-за тождественности фотонов вероятность такого события равна

$$C_n^k p^k(T) p^{n-k}(\overline{T}).$$

После того как фиксирована частотная полоса для амплитуд состояний, нам потребуется выяснить, какое минимально возможное окно T требуется для того, чтобы в нем можно было зарегистрировать состояние с вероятностью, сколь угодно близкой к единице. Иначе говоря, какая минимальная задержка возможна, если подслушиватель пытается получить доступ ко всему состоянию. Такой доступ вызовет задержку, которая будет равна минимальному при данной частотной полосе временному окну T.

При заданной конечной частотной полосе $c\Delta k$ (далее скорость света $c = 1$) максимальная локализация (набирающаяся нормировка состояния) в данном временном окне T достигается на состояниях с такой пространственно-временной амплитудой $\varphi(k)$, которые реализуют максимум функционала $\mathcal{F}$ и имеют носители внутри частотной полосы Δk. Эти условия приводят к вариационной задаче на безусловный экстремум (максимум) функционала

$$\mathcal{F} = \frac{\dfrac{1}{2\pi}\displaystyle\int_T |\varphi(\tau)|^2 d\tau}{\displaystyle\int_0^\infty |\varphi(k)|^2 dk}. \tag{23}$$

Одночастичные амплитуды являются нормированными функциями

$$\int_0^\infty |\varphi(k)|^2 dk = 1. \tag{24}$$

Вариация функционала приводит к интегральному уравнению для амплитуды, максимальная величина локализации во временном окне T при данной частотной полосе достигается для состояний, амплитуда которых дается собственными функциями интегрального уравнения

$$\lambda_m \varphi_m(k) = \frac{1}{\pi}\int_{\Delta k} \frac{\sin(k-k')T}{k-k'}\varphi_m(k')dk',$$
$$\lambda_m(\zeta) \sim 1 - \frac{4\sqrt{\pi}8^m}{m!}\zeta^{m+1/2}e^{-2\zeta}, \quad \zeta = \Delta k \cdot T. \tag{25}$$

Наибольшее собственное число дает вероятность локализации (долю нормировки в окне T), а собственная функция этого собственного числа дает оптимальную форму состояния. Данное уравнение исследовалось ранее в работах [29, 30]. Собственные числа уравнения положительны и образуют убывающую последовательность с ростом номера m ($1 > \lambda_0 > \lambda_1 \ldots > 0$, $m = 0, 1 \ldots, \infty$). Собственные числа являются функцией параметра $\Delta k \cdot T$, несколько первых собственных чисел при разных значениях параметра $\Delta k \cdot T$ найдены численно в работе [30]. Известна асимптотика при фиксированном номере m при параметре $\Delta k \cdot T \gg 1$ [29]. Из уравнения (25) видно, что собственные числа экспоненциально близки единице при $\zeta > 1$. Таким образом, вероятность любого измерения при размере пространственной области (или временного интервала) величиной T для состояния с носителем в частотной полосе Δk не может быть больше, чем $\lambda_0(\Delta k \cdot T)$. Выбирая размер временного окна T, можно добиться того, что вероятность детектирования вне данного интервала будет сколь угодно мала.

Применительно к задачам квантовой криптографии выбор интервала необходимого размера будет гарантировать то, что подслушиватель будет иметь лишь сколь угодно малую информацию о передаваемом состоянии вне этого временного окна. Таким образом, для того чтобы зарегистрировать одно из ортогональных состояний с вероятностью, сколь угодно близкой к единице, требуется минимальное временное окно T (см. (25)).

Из-за того что амплитуда состояний задается значениями на массовой поверхности (определены значения $\varphi(k, k_0)$ как функции двух переменных не при произвольных k и k_0, а только при $k_0 = k$), она оказывается всегда отличной от нуля во всем пространстве (вне области сколь угодно большого, но конечного размера — любого компакта [31–33]). Факт нелокализуемости состояний в квантовой теории поля известен давно (см. обсуждение физической стороны данного вопроса, например, в [34]). В данном случае нелокализуемость может быть явно продемонстрирована как следствие теоремы Винера–Пэли [35]. Для функции $\varphi(k)$, нормированной как

$$\int_0^\infty dk|\varphi(k)|^2 = 1,$$

равной нулю на полуоси $k \leq 0$, но не равной нулю тождественно, допустимая степень убывания в пространстве ее фурье-образа $\varphi(\tau)$ на бесконечности определяется сходимостью интеграла

$$\int_{-\infty}^{\infty} \frac{\ln|\varphi(\tau)|}{1+\tau^2} d\tau < \infty.$$

Отсюда следует, что амплитуда $\varphi(\tau)$ не может убывать даже экспоненциально (не говоря о том, чтобы быть равной нулю вне компакта), поскольку в этом случае, если

$$\varphi(\tau)| \propto \exp(-\alpha|\tau|),$$

интеграл во втором уравнении расходится. Однако амплитуда может убывать по закону, сколь угодно близкому к экспоненциальному с любым показателем $\alpha > 0$:

$$|\varphi(\tau)| \propto \exp\left(-\alpha|\tau|/\ln(\ln...|\tau|)\right).$$

Подобной степени локализации фотонного поля можно добиться и в трехмерном случае [36], хотя долгое время после работы Ньютона и Вигнера считалось, что наиболее быстрое убывание в пространстве может быть лишь степенным со степенью $7/2$ [37]. Нелокализуемость амплитуды (отличие от нуля вне любого компакта) имеет глубокие корни, связанные с причинностью в релятивистской квантовой области. Например, как было показано Хегерфельдом [33], если бы амплитуда состояния была строго локализованной в некоторой конечной области пространства в начальный момент времени t_0, то в любой последующий момент времени $t > t_0$ в результате свободной эволюции она стала бы отличной в областях пространства, сколь угодно далеких от данной и разделенных с ней пространственно-подобным интервалом. Данное поведение вступает в противоречие с релятивистским принципом причинности, поскольку при этом можно было бы передавать информацию в пространстве со скоростью, превышающей скорость света, даже в том случае, когда вероятность исхода измерения в области, разделенной пространственно-подобным интервалом с исходным, меньше единицы.

Пусть подслушиватель пытается отличить одно из двух ортогональных когерентных состояний (9) при фиксированной задержке δT. Сама задержка δT (она же является временным окном наблюдения для подслушивателя) является параметром, которым может управлять подслушиватель. Далее индекс «0» и «1» опускаем, поскольку вероятности различения одинаковы, из-за выбора одинаковых частотных полос для состояний, отвечающих «0» и «1».

Из-за ортогональности состояний для их различения подслушивателю достаточно регистрации одного и более фотонов в выбранном им временном окне (при задержке) δT. Отметим, что вакуумная компонента в выражениях (21), (22) не дает никакой информации о передаваемых состояниях, отвечающих «0» или «1». Сумма вероятностей (за вычетом вероятности для вакуумной компоненты) должна быть нормирована на единицу, поскольку только вероятности регистрации одного и более фотонов дают информацию о передаваемых состояниях. С учетом того, что вероятность вакуумной компоненты в состоянии равна

$$p(0,\mu) = 1 - e^{-\mu},$$

для нормировки имеем

$$\frac{1}{1-e^{-\mu}} \sum_{n=1}^{\infty} p(n,\mu) = 1. \qquad (26)$$

Для вероятности различения состояний ρ_0 и ρ_1, регистрации одного и более фотонов в окне δT с учетом (26) простые комбинаторные рассуждения приводят к соотношению

$$\begin{aligned}\Pr_E(n \geq 1 \ \text{ detected}) &= \\ &= \frac{1}{1-e^{-\mu}} \sum_{n=1}^{\infty} p(n,\mu) \Pr{}^{(n)}(n \ \text{ detected}) = \\ &= \frac{1}{1-e^{-\mu}} \sum_{n=1}^{\infty} p(n,\mu)[1-(1-p(\delta T))^n] = \\ &= \frac{1-e^{-\mu p(\delta T)}}{1-e^{-\mu}}. \qquad (27)\end{aligned}$$

Данная вероятность отвечает за достоверное различение состояний (conclusive result) и формально стремится к единице лишь при $\delta T \to \infty$. Иначе говоря, эта вероятность экспоненциально близка к единице по параметру $\Delta k \cdot T$ лишь при условии, что имеется доступ к временному окну T, где состояние почти полностью локализовано.

Соответственно, вероятность отсутствия детектирования (inconclusive result) при задержке в δT равна

$$\Pr_E(\text{not detected}) = 1 - \Pr_E(n \geq 1 \text{ detected}) = \\ = \frac{e^{-\mu p(\delta T)} - e^{-\mu}}{1 - e^{-\mu}}. \quad (28)$$

Интересно проследить, как данные выражения соотносятся с классической картиной. Вероятность достоверного различения двух ортогональных состояний электромагнитного поля с неперекрывающимися частотными полосами зависит от временного окна δT (задержки) и от среднего числа фотонов μ (степени классичности). Классический случай реализуется, когда среднее число фотонов в состоянии велико, $\mu \to \infty$. В этом случае для почти достоверного различения состояний достаточно сколь угодно малого временного окна $\delta T \to 0$. Достаточно иметь доступ к сколь угодно малой пространственно-временной области, где присутствует классический сигнал. И наоборот, в ультраквантовом пределе при малом среднем числе фотонов $\mu \ll 1$ для почти достоверного различения состояний требуется временное окно и, соответственно, задержка δT, равная той области, в которой набирается почти полная нормировка квадрата амплитуды состояния.

Обсудим теперь измерения на приемном конце по обнаружению подслушивателя.

Для обеспечения секретности ключа принципиально важно следующее. На приемном конце участник B оставляет только те посылки, которые дали исход измерения в правильном временном окне. Данное временное окно на приемном конце определяется как

$$t_A + L_{ch}/c, t_A + L_{ch}/c + T, \quad c = 1.$$

Здесь t_A — момент времени, когда передний фронт состояния поступает в канал связи, L_{ch} — длина квантового канала связи, которая считается известной, T — как и ранее, временное окно, в котором состояния почти полностью локализованы. Фактически величина $(t_A + L_{ch} + T) - t_A$ есть время, необходимое для того, чтобы состояние протяженностью T, распространяясь со скоростью света, целиком достигло приемного конца участника B. Далее для сокращения обозначений будем полагать $t_A = 0$.

Поскольку величина T однозначно связана с частотной полосой, на приемном конце участник B должен проводить измерения, которые ограничены лишь частотными полосами $\Delta k_{0,1}$. Другими словами, аппаратура должна регистрировать только те состояния, которые имеют допустимые частотные полосы. На техническом уровне этого несложно достичь путем установки соответствующих фильтров перед фотодетекторами. На формальном языке установка таких фильтров означает, что измерения на приемном конце описываются разложением единицы, которое строится из операторно-значных мер с носителями в заданных неперекрывающихся частотных полосах $\Delta k_{0,1}$.

На приемном конце второй участник проводит измерения, которые описываются формальным разложение единицы в частотных полосах $\Delta k_{0,1}$:

$$I = \bigoplus_{n=0,i=0,1}^{\infty} I^{(n)}(\Delta k_i) = \\ = \bigoplus_{n=0}^{\infty} \int_{\Delta k_i} \dots \int_{\Delta k_i} \frac{dk_1 \dots dk_n}{k_1 \dots k_n} |k_1 \dots k_n\rangle\langle k_1 \dots k_n| = \\ = \bigoplus_{n=0,i=0,1}^{\infty} \left(\underbrace{\int \dots \int \mathcal{M}_i^{(n)}(d\tau_1 \dots d\tau_n)}_{\forall \tau_i \in T_{ch}} + \right. \\ \left. + \underbrace{\int \dots \int \mathcal{M}_i^{(n)}(d\tau_1 \dots d\tau_n)}_{\exists \tau_i \in \overline{T}_{ch}} \right), \quad (29)$$

где введено обозначение T_{ch} — временное окно $(L_{ch}, L_{ch} + T)$ и, соответственно, $\overline{T}_{ch} = (-\infty, \infty)/T_{ch}$ — временное окно, не содержащее T_{ch}. Смысл данного измерения сводится к следующему. У пользователя на приемном конце все исходы измерений разделяются на два подмножества. Первое слагаемое в (30) отвечает случаю, когда все отсчеты были внутри временного окна T_{ch}. Имеется в виду, что состояния приготавливаются в области, контролируемой первым участником, и в момент времени $t_A = 0$ передний фронт состояния входит в канал связи и распространяется в нем. Второе слагаемое описывает результаты, при которых имел место хотя бы один отсчет вне временного окна T_{ch}. Посылки, в которых были такие исходы, участником B отбрасываются. Такое измерение может быть реализовано с помощью двух фильтров с полосами пропускания $\Delta k_{0,1}$ и двух быстрых фотодетекторов, размещенных за ними. Фильтры нужны, чтобы обеспечить то условие, что подслушиватель не может использовать более короткие по протяженности состояния, у которых, соответственно, бóльшая, чем $\Delta k_{0,1}$ частотная полоса. Постоянная времени фотодетекторов τ_d должна подчиняться условию $\tau_d \ll T$, для того чтобы во временном окне локализации состояния можно было набрать статистику результатов. Веро-

ятность для подслушивателя узнать передаваемый участником A бит и пройти тест на приемном конце у B на задержку не превосходит величины

$$\begin{aligned}\Pr(\mathrm{bit}_E = \mathrm{bit}_A \wedge \mathrm{test}(\forall\tau_i \in T_{ch}) = \mathrm{OK}) = \\ = \Pr_E(\text{not detected}) \cdot \frac{1}{2} \cdot 1 + \\ + \Pr_E(n \geq 1 \text{ detected}) \cdot 1 \cdot (1 - p(\delta T)) = \\ = \frac{1}{2}\,\frac{e^{-\mu p(\delta T)} - e^{-\mu}}{1 - e^{-\mu}} + \\ + (1 - p(\delta T))\frac{1 - e^{-\mu p(\delta T)}}{1 - e^{-\mu}}. \quad (30)\end{aligned}$$

Первое слагаемое в выражении (30) состоит из трех сомножителей. Первый описывает вероятность отсутствия любого отсчета во временном окне δT у подслушивателя. Второй сомножитель в этом слагаемом есть вероятность различения состояний в отсутствие отсчета, которая в этом случае равна $1/2$ — вероятности простого угадывания. Третий сомножитель в первом слагаемом описывает вероятность пройти тест на временную задержу. Эта вероятность равна единице, поскольку состояние никаких отсчетов в δT у подслушивателя не вызвало.

Аналогично для второго слагаемого. Первый сомножитель есть вероятность регистрации одного и более фотонов в частотной полосе Δk_0 или Δk_1 во временном окне δT. Если срабатывание было (хотя бы один фотон дал отсчет), то вероятность различения (второй сомножитель) равна единице. Третий сомножитель есть вероятность пройти тест на задержку (дать отсчеты в окне T_{ch} на приемном конце). Поскольку

$$(1 - p(\delta T))^n < 1 - p(\delta T),$$

данная вероятность не превосходит величины $1 - p(\delta T)$. А именно, для подслушивателя максимальная вероятность пройти тест на временную задержку достигается, если он перепосылает участнику B однофотонные состояния, а не матрицу плотности (9), которая содержит многофотонные составляющие. Физически это связано с тем, что для многофотонных состояний вероятность срабатывания вне временного окна T_{ch} для задержанных состояний выше. Например, в пределе классического сигнала, задержанного по времени (факт задержки гарантируется наличием предельной скорости и тем, что временное окно «настроено» на наиболее короткие состояния в данной частотной полосе), вероятность пройти тест стремится к нулю при сколь угодно малой задержке, поскольку для классического сигнала достаточно сколь угодно малого «хвоста», не вмещающегося в тестовое временное окно T_{ch}. Далее максимальную величину вероятности в (30) будем обозначать для краткости

$$\begin{aligned}\delta_E^{OK} = \\ = \max_{\varphi(k),\delta T}\{\Pr(\mathrm{bit}_E = \mathrm{bit}_A \wedge \mathrm{test}(\forall\tau_i \in T_{ch}) = \mathrm{OK})\}. \quad (31)\end{aligned}$$

Данная величина достигается для наиболее коротких состояний (23)–(25). Иначе говоря, вид функции $p(\delta T)$ известен. Поэтому, зная $p(\delta T)$, для которой достигается максимум, подслушиватель может найти и величину δT. Следовательно, далее можно использовать $p(\delta T)$ как независимую переменную. Подчеркнем, что данная величина в канале с затуханием не превосходит величины (31), что гарантируется релятивистским принципом причинности. Кроме того, в данной схеме не нужен учет коллективных измерений, поскольку используются ортогональные состояния и протокол происходит в реальном времени в отличие от схем, где используются только геометрические свойства неортогональных состояний. В нашем случае достоверная неразличимость ортогональных состояний связана фактически с тем, что подслушивателю не хватает времени на то, чтобы получить доступ к состоянию целиком. Коллективные измерения, которые в нерелятивистском случае при различении неортогональных состояний могут дать больше информации, если измерения проводятся не над индивидуальными состояниями, а над целыми блоками, в релятивистском случае не дают подслушивателю никаких преимуществ по сравнению с индивидуальными измерениями в каждой посылке.

Если входные состояния для «0» и «1» являются чисто однофотонными,

$$\begin{aligned}|\varphi_{0,1}^{(1)}\rangle = \int_0^\infty \frac{dk}{\sqrt{k}}\frac{\varphi_{0,1}(k)}{\sqrt{k}}|k\rangle, \quad (32)\\ \varphi(k) \equiv \varphi(k, k_0 = |k|) \equiv \varphi(k, k_0 = k),\end{aligned}$$

то вероятность для подслушивателя узнать передаваемое состояние и пройти тест на приемном конце у B на задержку есть

$$\begin{aligned}\Pr(\mathrm{bit}_E = \mathrm{bit}_A \wedge \mathrm{test}(\tau \in T_{ch}) = \mathrm{OK}) = \\ = (1 - p(\delta T)) \cdot \frac{1}{2} \cdot 1 + p(\delta T) \cdot 1 \cdot (1 - p(\delta T)) \leq \\ \leq \frac{9}{16}. \quad (33)\end{aligned}$$

Максимум достигается при $p(\delta T) = 1/4$. Величина δT оптимальной задержки для подслушивателя может быть найдена из уравнения

$$\frac{9}{16} = \int\limits_{-\delta T}^{\delta T} |\varphi(\tau)|^2 d\tau. \tag{34}$$

При среднем числе фотонов $\mu = 1$ величина δ_E не оказывается очень близкой к значению $9/16 = 0.5625$, что имело бы место, если бы входные состояния были однофотонными фоковскими состояниями с амплитудами $\varphi_{0,1}$, заданными в неперекрывающихся частотных полосах шириной Δk. Еще раз напомним, что ширина полосы фактически нужна для фиксации минимальной протяженности в пространстве-времени амплитуды состояний. Кроме того, в протоколе участник A не обязан приготавливать наиболее короткие состояния при заданной частотной полосе, но участник B должен оставлять только те измерения, которые будут давать отсчеты во временном окне, отсчитанном от переднего фронта, того же размера, что и для наиболее коротких состояний.

5. PNS-АТАКА НА КЛЮЧ: АТАКА С «РАСЩЕПЛЕНИЕМ» СОСТОЯНИЯ

Выше рассматривалась прямая атака на ключ, когда подслушиватель непосредственно измеряет передаваемое состояние. Рассмотрим теперь PNS-атаку (Photon Number Splitting), когда подслушиватель из-за многофотонности состояния «отводит» часть состояния светоделителем (см. рис. 2) и проводит измерения над отведенным состоянием. Светоделитель представляет собой унитарный преобразователь с коэффициентом преобразования η (деление входного состояния в пропорции $\eta/(1-\eta)$).

Состояние на выходе светоделителя с коэффициентом преобразования η имеет вид

$$|\varphi_{E,B}^{(n)}\rangle = \sum_{k=0}^{n} (\sqrt{\eta}\,)^k \left(\sqrt{1-\eta}\right)^{n-k} \sqrt{C_n^k}\,|\varphi^{(k)}\rangle_E \otimes |\varphi^{(n-k)}\rangle_B, \tag{35}$$

$$|\varphi^{(k)}\rangle_E = \left(\underbrace{\int\limits_{-\infty}^{\infty} \dots \int\limits_{-\infty}^{\infty} \frac{d\tau_1 \dots d\tau_k}{(2\pi)^k} \varphi(\tau_1) \dots \varphi(\tau_k) |\tau_1 \dots \tau_k\rangle}_{k} \right)_E, \tag{36}$$

$$|\varphi^{(n-k)}\rangle_B = \left(\underbrace{\int\limits_{-\infty}^{\infty} \dots \int\limits_{-\infty}^{\infty} \frac{d\tau_1 \dots d\tau_{n-k}}{(2\pi)^{n-k}} \varphi(\tau_1) \dots \varphi(\tau_{n-k}) |\tau_1 \dots \tau_{n-k}\rangle}_{n-k} \right)_B. \tag{37}$$

Принципиально важно для дальнейшего, что на выходе светоделителя состояние у подслушивателя E и легитимного пользователя B является запутанным (entangled). С учетом (35)–(37), матрицу плотности такого запутанного состояния можно записать в виде

$$\rho_{E,B} = \sum_{n=0}^{\infty} p(\mu, n) |\varphi_{E,B}^{(n)}\rangle\langle\varphi_{E,B}^{(n)}|. \tag{38}$$

Из-за запутанности состояния измерения у подслушивателя E и легитимного пользователя B оказываются коррелированными, аналогично тому, как это имеет место в классическом эффекте Эйнштейна–Подольского–Розена [38]. Для нас существенна запутанность по числу фотонов в каналах E и B. Поскольку у легитимного пользователя B оставляются только те измерения, которые дали не холостые отсчеты, из-за того, что состояние является запутанным, подслушиватель получает достоверную информацию о передаваемом состоянии, когда у него также имеет место отсчет. Вероятность таких совместных событий, когда у обоих участников имеют место отсчеты, равна

$$\Pr(E \text{ detected } n \geq 1 \wedge B \text{ detected } n \geq 1) =$$

$$= \sum_{n=1}^{\infty} p(\mu, n) \mathrm{Tr}_{E,B} \left\{ \left(\bigoplus_{n=1,i=0,1}^{\infty} I^{(n)}(\Delta k_i) \right)_B \left(\bigoplus_{n'=1,i=0,1}^{\infty} I^{(n')}(\Delta k_i) \right)_E \times \right.$$

$$\times \left(\sum_{k=0}^{n} (\sqrt{\eta})^k \left(\sqrt{1-\eta} \right)^{n-k} \sqrt{C_n^k} |\varphi^{(k)}\rangle_E \otimes |\varphi^{(n-k)}\rangle_B \right) \times$$

$$\left. \times \left(\sum_{k'=0}^{n} (\sqrt{\eta})^{k'} \left(\sqrt{1-\eta} \right)^{n-k'} \sqrt{C_n^{k'}}\, {}_E\langle\varphi^{(k')}| \otimes {}_B\langle\varphi^{(n-k')}| \right) \right\}. \quad (39)$$

В операторно-значной мере оставлены только слагаемые с $n, n' \geq 1$, которые отвечают ситуации, когда регистрация одного и более фотонов имеет место одновременно у E и B. С вероятностью (39) подслушиватель идентифицирует передаваемые состояния и остается незамеченным. Отметим, что измерения с расщеплением не вызывают задержки на приемном конце у B. Операторно-значные меры (29), описывающие измерение в конечном временном окне, здесь можно заменить на единичные операторы, поскольку расщепление состояния не вносит задержку, а вне окна T имеются только экспоненциально малые хвосты состояний.

Для каждой n-фотонной компоненты матрицы плотности с вероятностью η^n будет иметь место регистрация n фотонов в канале светоделителя подслушивателя. Такие исходы на приемном конце у B не дадут отсчетов, поэтому эта составляющая вероятности не будет фигурировать в ответе. Аналогично для каждой n-фотонной компоненты матрицы плотности с вероятностью $(1-\eta)^n$ будет иметь место регистрация n фотонов в канале светоделителя у легитимного пользователя B. Такие исходы будут оставлены участником B, но у подслушивателя отсчетов в этом случае не будет. Это означает, что для таких исходов вероятность различения подслушивателем передаваемого состояния равна $1/2$ — вероятности простого угадывания.

Вакуумная компонента состояний не дает отсчетов ни у E, ни у B. Нормировка полной вероятности должна вычисляться с учетом этого обстоятельства, аналогично тому, как это было сделано в предыдущем разделе.

Окончательно для вероятности для подслушивателя узнать передаваемое состояние и остаться незамеченным в случае PNS-атаки имеем

$$\Pr(\mathrm{bit}_E = \mathrm{bit}_{A,B} \wedge n \geq 1 \text{ detected by } B) =$$

$$= \frac{1}{2} \frac{e^{-\mu\eta} - e^{-\mu}}{1 - e^{-\mu}} + \left(1 - \frac{e^{-\mu\eta} + e^{-\mu(1-\eta)} - 2e^{-\mu}}{1 - e^{-\mu}} \right). \quad (40)$$

Первое слагаемое в (40) отвечает ситуации, когда все n фотонов в каждой n-фотонной компоненте матрицы плотности дали отсчет у B. Вероятность различения состояний у E равна $1/2$ (сомножитель в первом слагаемом). Второе слагаемое описывает ситуацию, когда отсчеты были как у E, так и у B. Вероятность различения при этом равна единице.

При данной атаке максимальная величина

$$\delta_E^{OK} = \max \eta \{ \Pr(\mathrm{bit}_E = \mathrm{bit}_{A,B} \wedge n \geq 1 \text{ detected by } B) \} \quad (41)$$

зависит при заданном среднем числе фотонов μ в состояниях от коэффициента преобразования светоделителя η.

6. МАКСИМАЛЬНАЯ ВЕЛИЧИНА δ_E^{OK}

На рис. 3*а* приведены максимальные вероятности δ_E^{OK} для подслушивателя узнать передаваемый A бит и пройти тест на задержку в зависимости от величины задержки $p(\delta T)$ и среднего числа фотонов μ. Затухание в канале связи, согласно приведенным выше рассуждениям (см. рис. 1*в*), не может увеличить вероятность получения результата подслушивателем при данной задержке.

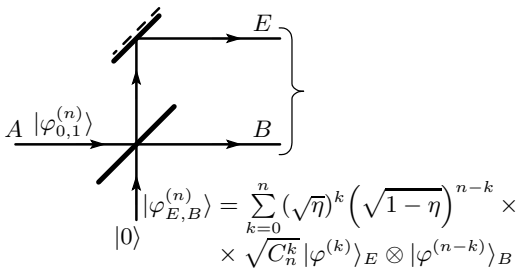

Рис. 2.

Таблица 2.

μ	η	δ_E^{OK}
0.1	0.0001	0.502
1	0.20	0.515
3.0	0.40	0.746
5.0	0.45	0.893
10.0	0.5	0.997

При малом среднем числе фотонов $\mu = 0.1$ величина δ_E^{OK}, как видно из табл. 1 (см. также рис. 3*а*), составляет $\delta_E^{OK} = 0.565$, что лишь на 0.065 превосходит вероятность простого угадывания. Для дальнейшего будет удобнее использовать минимальную вероятность ошибки для подслушивателя $\delta_E = 1 - \delta_E^{OK}$. Данная величина имеет следующий смысл. Поскольку на приемном конце участник B оставляет только те посылки, которые дали исход в нужном временном окне, для подслушивателя это означает, что вероятность ошибки, с которой он знает биты в принятых B позициях, прошедших тест, составляет δ_E. Даже при среднем числе фотонов в когерентном состоянии вплоть до $\mu = 5$ вероятность ошибки для подслушивателя равна 30 %. Это означает, что подслушиватель знает принятые легитимными пользователями биты примерно в 70 % позиций. При длинной принятой последовательности N легитимными участниками A и B может быть извлечено $0.3N$ секретных бит (см. ниже).

При большом среднем числе фотонов величина δ_E^{OK} стремится к единице (соответственно, вероятность ошибки $\delta_E \to 0$). Задержка также стремится к нулю. Хотя доля нормировки $p(\delta T)$, набирающаяся во временном окне измерения δT, стремится к нулю (при $\mu = 100$ имеем $p(\delta T) = 0.04$), эта малость компенсируется большим числом фотонов, которые могут дать отсчет в окне δT. При больших $\mu \gg 1$ имеет место классическая ситуация: два состояния электромагнитного поля с не перекрывающимися частотными полосами (с разным «цветом») могут быть достоверно идентифицированы практически мгновенно.

Тот факт, что можно использовать когерентные состояния со средним числом $\mu = 1$–3, где величина δ_E еще велика, для экспериментальных реализаций означает, что не требуется ослабления лазерного излучения до уровня $\mu = 0.1 \div 0.3$, как это обычно имеет место (доля холостых посылок при этом ≈ 90 %). При среднем числе фотонов $\mu = 3$, когда в канале присутствует лишь вакуумная компонента, холостые посылки (их доля составляет 5 %) практически отсутствуют, что позволяет увеличить скорость генерации ключа в 10 раз.

Ответ для вероятности δ_E по существу не зависит от исходной ширины частотной полосы Δk, а зависит только от безразмерного параметра $\Delta k \cdot T$. Поэтому при любой частотной полосе всегда можно выбрать требуемую величину временного окна, в которую состояние фотонного поля «помещается» целиком. Величина δ_E зависит только от структуры состояний и максимальна для чистого состояния (не статистической смеси состояний с разным числом фотонов) однофотонного пакета, распространяющегося со скоростью света. Состояние однофотонного пакета отвечает предельно квантовой релятивистской ситуации, и в этом случае величина δ_E носит универсальный характер и является, в определенном смысле, мировой константой, поскольку при ее выводе ничего, кроме нормировки амплитуды квантового состояния и факта распространения состояния со скоростью света, не использовалось.

Вероятность δ_E^{OK} для PNS-атаки в зависимости от коэффициента светоделителя η и среднего числа фотонов μ приведена на рис. 3*б*. В табл. 2 приведена максимальная величина δ_E^{OK} для оптимального η.

При малых средних числах фотонов $\mu = 0.1$ для подслушивателя вероятность узнать состояние и остаться незамеченным близка к $1/2$ ($\delta_E^{OK} = 0.502$). Данный результат качественно понятен, поскольку при $\mu = 0.1$ (за вычетом вероятности вакуумной компоненты) в канале в основном находится один фотон. Вероятности появления двух и более фотонов существенно меньше. Поэтому после светоделителя однофотонное состояние может быть зарегистрировано либо в одном плече (E), либо в другом (B), и никогда не может быть зарегистрировано сразу в обоих.

При больших числах заполнения $\mu > 10$ состояние близко к классическому, поэтому можно «отще-

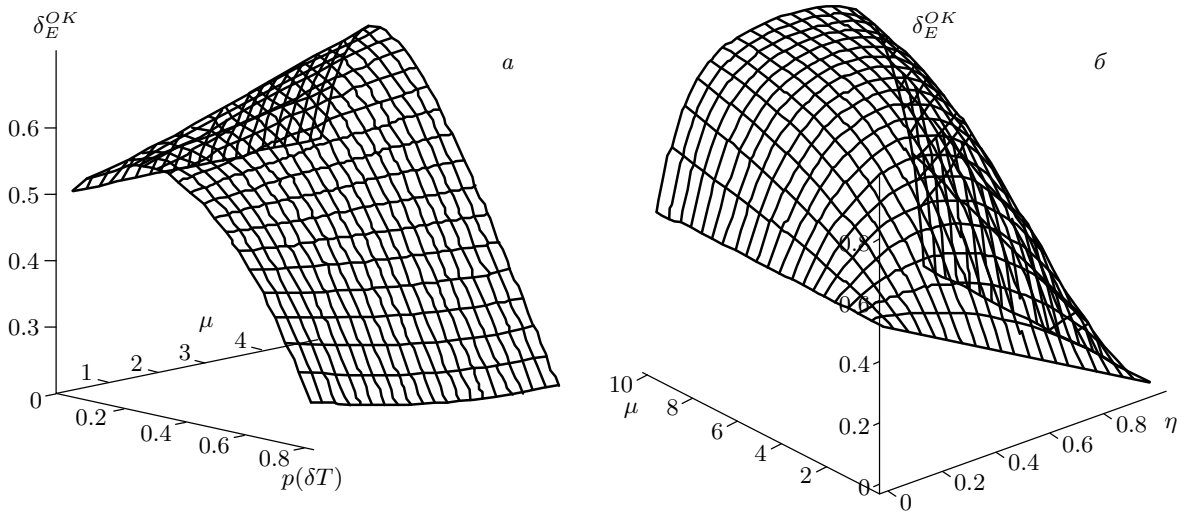

Рис. 3.

пить» половину состояния ($\eta = 1/2$), при этом вероятность одновременных отсчетов у E и B будет близка к единице.

7. СЕКРЕТНОСТЬ КЛЮЧА

Основная сложность в доказательстве безусловной секретности нерелятивистской квантовой криптографии, основанной на достоверной неразличимости неортогональных состояний, возникает из-за того, что упомянутые протоколы формулируются как протоколы «обмена» в гильбертовом пространстве состояний. Формулировка протоколов, при которой используются лишь свойства пространства состояний, неизбежно приводит к необходимости доказывать устойчивость протоколов относительно коллективных измерений, учет которых и представляет наибольшую трудность. На сегодняшний день существует несколько доказательств секретности для различных протоколов [21, 22, 39, 40].

Реально передача информации всегда подразумевает приготовление носителя информации (квантового состояния), его распространение через канал связи к пространственно удаленному пользователю с дальнейшим измерением в более поздний момент времени состояния носителя информации. В релятивистской квантовой криптографии нет необходимости учитывать коллективные измерения. Данное обстоятельство заметно упрощает доказательство секретности. Другим облегчающим обстоятельством является то, что в определенном смысле можно разделить ошибки, вносимые подслушивателем (задержку состояний), и ошибки, вызванные внешним шумом в канале (например, отсчеты от темновых фотонов). В нерелятивистском случае даже частичное разделение ошибок невозможно — ошибки из-за шума принципиально неотличимы от ошибок, вызываемых подслушивателем.

Сформулируем сначала критерий секретности ключа. Примем критерий секретности, наиболее удобный для нашего случая. Ключ должен удовлетворять двум требованиям, которые неформально сводятся к следующему. Ключ должен быть идентичен у легитимных пользователей и известен только им. Более формально, пусть строка из m бит у A и B получена в результате протокола и принята участниками A и B как секретный ключ. Тогда ключ секретен, если выполнено следующее.

1. Идентичность ключа. Вероятность того, что каждый бит в строке из m бит, уже принятых как ключ, различна для A ($b_A(i)$) и B ($b_B(i)$), должна быть экспоненциально мала для выбранных заранее параметров секретности M, ε_1, т. е.

$$\forall \varepsilon_1 > 0 \quad \exists M, \quad \Pr\{b_A(i) \neq b_B(i)\} \leq e^{-M} \leq \varepsilon_1. \quad (42)$$

Для взаимной информации между строками бит ключа A и B длиной m имеем

$$I(A;B) \geq m - 2^{-M'}. \quad (43)$$

2. Секретность ключа. Вероятность того, что подслушиватель E знает любой бит в ключе, лишь на экспоненциально малую величину превышает вероятность простого угадывания 2^{-m} (напомним, что вероятность ошибки при простом угадывании равна

1/2 и является наихудшим вариантом) результирующей строки A длиной m. А именно, вероятность того, что подслушиватель знает любой бит в строке, принятой как секретный ключ, экспоненциально мала по сравнению с 1/2:

$$\forall \varepsilon_2 > 0 \quad \exists \eta_2, \zeta, \\ \Pr\{b_A(i) = b_E(i)\} \le \frac{1}{2} + e^{-\eta_2}, \quad e^{-\eta_2} \le \varepsilon_2. \tag{44}$$

Другими словами, подслушиватель E имеет экспоненциально малую информацию о строках $b_A(m)$ и $b_B(m)$, принятых как ключ длины m легитимными пользователями:

$$I(A;E) \le e^{-\eta_2} \le \varepsilon_2, \quad I(B;E) \le e^{-\eta_2} \le \varepsilon_2. \tag{45}$$

При этом величины ε_1, η_1 и ε_2, η_2 могут выбираться независимо друг от друга. Здесь не следует понимать под строкой бит, принятых как ключ, исходные передаваемые A биты. Каждый бит в ключе является некоторой функцией множества исходных битов.

Сформулируем теперь протокол генерации секретного ключа. Напомним, что длина квантового канала связи должна быть известна. Возможны протоколы, когда требуется синхронизация общего начала отсчета времени (синхронизация часов) как на приемном, так и на передающем конце, либо такая синхронизация не требуется (см. ниже).

1. Легитимные участники протокола A и B открыто выбирают состояния. Фиксируется ширина частотного спектра состояний Δk (и, соответственно, временное окно измерения T, длина канала считается известной) и среднее число фотонов μ в состояниях. Выбор среднего числа фотонов автоматически определяет δ_E. Далее выбирается большое целое число $N \gg 1$. Протокол использует $2N$ бит.

2. Участник A генерирует случайную строку бит b_i (0 и 1) длиной $i = 1, \ldots, 2N$.

3. Участник B проводит измерения на приемном конце, которые описываются разложением единицы (21), и анонсирует через открытый канал факт регистрации состояния.

4. После посылки всех состояний участником A участник B сообщает через открытый канал номера тех посылок, в которых результаты измерений дали исходы во временных окнах $(t_i + L_{ch}, t_i + L_{ch} + T)$, т. е. без задержки. Здесь t_i — i-ый момент посылки состояния. Посылки, в которых были исходы вне временных окон, отбрасываются. Пусть число таких исходов, прошедших тест на задержку, равно $2n$.

5. Участники случайным образом выбирают n позиций из $2n$ оставленных исходов и открыто сообщают значения битов, которые у них стоят в этих позициях.

6. Через открытый канал участники A и B проводят сравнение битов в раскрытой последовательности n в каждой позиции и оценивают вероятность ошибок. Пусть число позиций, в которых биты совпадают, равно n_{OK}, а $n_{\overline{OK}}$ — число позиций, в которых биты не совпадают, причем эти величины совпадают. Оценка вероятности ошибки есть $\delta_{AB} = n_{\overline{OK}}/n$. При достаточно большом n вероятность ошибки в нераскрытой части посылок экспоненциально близка к δ_{AB}.

7. Если вероятность ошибки у легитимных пользователей $\delta_{AB} > \delta_E$, то протокол обрывается, поскольку невозможно извлечь секретный ключ. Если $\delta_{AB} < \delta_E$, то протокол продолжается.

8. Для оставшейся последовательности нераскрытых битов длиной n участники A и B исправляют ошибки. Для этого выбирается классический корректирующий код $[n, k, d]$, который исправляет $t = \delta_{AB} n$ ошибок. Это код с минимальным расстоянием по Хэммингу d и числом кодовых слов 2^k, $d > 2\delta_{AB} n + 1$ для линейного кода, либо $d > 2t + 1$ для случайного линейного кода. Для этого участник A анонсирует открыто v_i проверочных строк данного кода ($i = 1, \ldots, r$, $r = n - k$). Участник A также отрыто сообщает r проверочных битов четности

$$\mathrm{parity}_i = v_i n_A$$

(n_A — строка нераскрытых битов у A, и, соответственно, n_B — строка нераскрытых битов у B, причем n_A и n_B, вообще говоря, не совпадают, и различаются с вероятностью, сколь угодно близкой к единице примерно в $\delta_{AB} n$ позициях).

9. Участник B, зная правильную четность подстрок, исправляет ошибки в своей последовательности. На этом этапе с вероятностью, сколь угодно близкой к единице, при достаточно большом n строки битов у A и B идентичны.

10. Условие $\delta_{AB} < \delta_E$ гарантирует, что при исправлении ошибок участниками A и B через открытый канал при помощи корректирующего кода подслушиватель будет иметь экспоненциально малую информацию о ключе (см. ниже). Таким образом, коррекция ошибок автоматически обеспечивает идентичность и секретность ключа.

При достаточно большом числе $2n$ (число посылок, в которых результаты измерений у B дали исход в правильном временном окне, см. пункт 4)) оценка вероятности ошибок, возникших в раскрытой случайно выбранной части посылок длиной n

из полного числа посылок $2n$, гарантирует, что с вероятностью, сколь угодно близкой к единице, число ошибок в нераскрытых n посылках у A и B равно

$$t = n\delta_{AB}. \tag{46}$$

Это обстоятельство позволяет выбрать корректирующий ошибки линейный классический код $[n, k, d]$ с кодовым расстоянием $d \geq 2t + 1$. Длина ключа k, которая может быть получена при помощи данного кода, не более

$$k < n(1 - H(\delta_{AB})),$$

$$H(x) = -x \log x - (1 - x)\log(1 - x).$$

Данное условие является необходимым для исправления ошибок в двоичном симметричном канале, которые имеют место с вероятностью δ_{AB}. Код позволяет исправить ошибки в $(d-1)/2$ позициях с вероятностью, сколь угодно близкой к единице [41–43]. Здесь $H(x)$ — бинарная энтропийная функция. Данное утверждение следует из границы Шеннона [41] для линейных случайных кодов.

Скорость $R = k/n$ наилучших корректирующих кодов $[n, r, d]$ с $d/n \geq \delta_{AB}$ лежит не ниже достижимой границы Варшамова–Гильберта [43]:

$$k \geq n\left(1 - H\left(\frac{d}{n}\right)\right) \tag{47}$$

(предел Шеннона). Однако оценка, следующая из неравенства Варшамова–Гильберта, является более конструктивной. Существуют линейные регулярные (не случайные) коды, на которых эта граница достигается, в отличие от теоретического предела Шеннона, который достигается только на случайных кодах и не является конструктивным, а скорее представляет собой теорему существования. Таким образом, неизвестны регулярные коды, на которых граница Шеннона может быть достигнута [41, 43].

Протокол будет работать до тех пор, пока вероятность ошибки $\delta_{AB} < \delta_E$. Код, выбранный A и B, должен обладать наименьшей избыточностью в том смысле, что он должен исправлять все потоки ошибок, вероятность которых меньше δ_{AB}, но должен быть недостаточен для исправления $\delta_E n$ ошибок.

Если же $\delta_{AB} < \delta_E$, то в принципе существует случайный корректирующий код с кодовым расстоянием

$$d/n \geq \delta_{AB}, \quad \text{но} \quad d/n < \delta_E, \tag{48}$$

который с вероятностью, сколь угодно близкой к единице (почти достоверно при большом n), будет исправлять ошибки у A и B, но с вероятностью единица не будет исправлять их у подслушивателя. Число оставшихся и число уже одинаковых битов у A и B (равное nR) в результате коррекции при достаточно больших $n \gg 1$ могут быть в принципе сколь угодно близко друг к другу, но не более, чем

$$nR < nC(\delta_{AB}), \quad C(\delta_{AB}) = 1 - H(\delta_{AB}), \tag{49}$$

где $C(x)$ — пропускная способность классического симметричного бинарного канала связи, R — «скорость» (n, R) корректирующего кода.

После коррекции ошибок легитимными пользователями A и B посредством обмена через открытый канал связи достижимая вероятность

$$\Pr\{\{b_A(i)\} \neq \{b_B(i)\}\}$$

того, что строки

$$\{b_{A,B}(i)\} = (b_{A,B}(1), \ldots, b_{A,B}(n))$$

бит у них различаются, равна

$$\begin{aligned} &\Pr\{\{b_A(i)\} = \{b_B(i)\}\} > \\ &> 1 - 4\exp\left[-nE(\delta_{AB}, z)\right], \\ &E(\delta_{AB}, z) = \max_{0 \leq z \leq 1}\{zR - E_0(\delta_{AB}, z)\}, \end{aligned} \tag{50}$$

где

$$\begin{aligned} E_0(z, \delta_{AB}) = z\ln 2 - (1 + z) \times \\ \times \ln[\delta_{AB}^{1/(1+z)} + (1 - \delta_{AB})^{1/(1+z)}]. \end{aligned} \tag{51}$$

Таким образом, условие идентичности ключа (42), (43) у легитимных пользователей выполнено. Остается теперь показать, что после коррекции ключ автоматически будет секретен, т. е. строка бит после коррекции будет известна подслушивателю лишь с экспоненциально малой по параметру n вероятностью.

На самом деле при условии $\delta_{AB} < \delta_E$ подслушиватель находится в ситуации бинарного симметричного канала [42], когда скорость передачи (в смысле бит/посылку) превышает пропускную способность канала между ним и A, которая равна $C(\delta_E)$. Коррекция ошибок при помощи кодов, которые плохи для подслушивателя (т. е. при условии $\delta_{AB} < \delta_E$), выглядит для него как передача сообщений со скоростью, превышающей пропускную способность канала связи между ним и A. В то же время канал между легитимными пользователями имеет пропускную способность $C(\delta_{AB})$, которая превышает $C(\delta_E)$. Исправление ошибок легитимными пользователями при помощи корректирующих кодов выглядит для подслушивателя как ситуация по передаче

информации со скоростью, сколь угодно близкой к $R < C(\delta_{AB})$ (скорости в смысле бит на позицию), превышающей пропускную способность канала между ним и легитимными пользователями $R > C(\delta_E)$.

В этом случае при скоростях передачи $R > C(\delta_E)$ выше пропускной способности можно воспользоваться следующей теоремой о средней вероятности ошибки на символ [44].

Теорема. Для дискретного канала без памяти с пропускной способностью C для любого (n, R)-кода при $R > C$ для вероятности ошибки P_e имеет место соотношение

$$P_e \geq 1 - \frac{4A}{n(R-C)^2} - \exp\left(-\frac{n(R-C)}{2}\right), \qquad (52)$$

где A — положительная константа, которая зависит только от свойств канала и не зависит от R и n.

Данная оценка может быть улучшена [42], и для любого дискретного канала связи без памяти имеем

$$P_e \geq 1 - 2\exp(-n\alpha(R)), \qquad (53)$$

где

$$\alpha(R) = \\ = \min\left\{\frac{R-C}{2}, \max_{s\geq 0}\left[s\left(C + \frac{R-C}{2} - \ln g(s)\right)\right]\right\}, \qquad (54)$$

и

$$g(s) = \sum_{j,k} Q(k)P(j|k) \times \\ \times \exp\left\{s \ln \frac{P(j|k)}{\sum\limits_i Q(i)P(j|i)}\right\}. \qquad (55)$$

В нашем случае канал связи сводится к дискретному двоичному симметричному каналу, поэтому

$$Q(i) = \frac{1}{2}, \quad P(j|j) = 1 - \delta_E, \\ P(j|k) = 1 - \delta_E, \quad j \neq k, \quad j, i, k = 0, 1. \qquad (56)$$

При этом в (52)–(55) следует взять $C = C(\delta_E)$, $R \approx C(\delta_{AB})$. Тогда получим

$$R \approx C(\delta_{AB}) = 1 + (1-\delta_{AB})\log(1-\delta_{AB}) + \\ + \delta_{AB}\log\delta_{AB}, \quad R < C, \qquad (57)$$

$$C = C(\delta_E) = 1 + (1-\delta_E)\log(1-\delta_E) + \delta_E\log\delta_E, \qquad (58)$$

функция $g(s)$ определяется выражением

$$\ln g(s) = (s-1)\ln 2 + \ln[\delta_E^{s+1} + (1-\delta_E)^{s+1}], \qquad (59)$$

а показатель экспоненты в выражении (53) по порядку величины равен $n(R-C)$.

Таким образом, критерий секретности ключа (44)–(45) оказывается выполненным — подслушиватель имеет экспоненциально малую информацию о ключе

$$\Pr\{\{b_{A,B}(i)\} = \{b_E(i)\}\} < 2\exp(-n\alpha(R)) \approx \\ \approx 2\exp(-n(C(\delta_{AB}) - C(\delta_E))). \qquad (60)$$

Обратим внимание, что в квантовой криптографии на неортогональных состояниях (так называемый протокол BB84 [45]) допустимая вероятность ошибок, при которой протокол работает и позволяет создать секретный ключ в шенноновском пределе, не превосходит 11 % [20, 21]. Данный предел возникает из-за того, что в этом протоколе необходимо корректировать фазовые ошибки при измерениях в разных базисах, кроме bit-flip ошибок (переброс 0 в 1 и наоборот) [21]. Поэтому порог определяется из уравнения

$$1 = 2H(\delta_{AB}). \qquad (61)$$

В принципе, уже после коррекции ошибок (при $n \gg 1$) информация у подслушивателя о строке бит у A и B стремится к нулю. Тем не менее для усиления секретности может быть сделана процедура хэширования (privacy amplification).

8. КВАНТОВАЯ КРИПТОСИСТЕМА С СИНХРОНИЗАЦИЕЙ ЧАСОВ НА ПРИЕМНОМ И ПЕРЕДАЮЩЕМ КОНЦАХ

Опишем две возможные схемы релятивистской квантовой криптографии. Первая из обсуждаемых схем требует синхронизации часов на приемном и передающем концах. Точнее, фиксации общего начала отсчета времени в каждой посылке.

Вторая из обсуждаемых схем не требует общего начала отсчета по времени. Достаточно лишь двух одинаковых часов (генераторов тактовых импульсов) на приемном и передающем концах, которые запускаются независимо друг от друга. Знание длины квантового канала связи здесь также требуется.

Пусть длина квантового канала связи (L_{ch}) известна, и часы у наблюдателей имеют общее начало отсчета. Это может быть сделано по открытому общедоступному классическому каналу связи.

Схема приведена на рис. 4*a*. Временная эволюция состояний поясняется на пространственно-временной диаграмме, представленной на рис. 5*a*. Про-

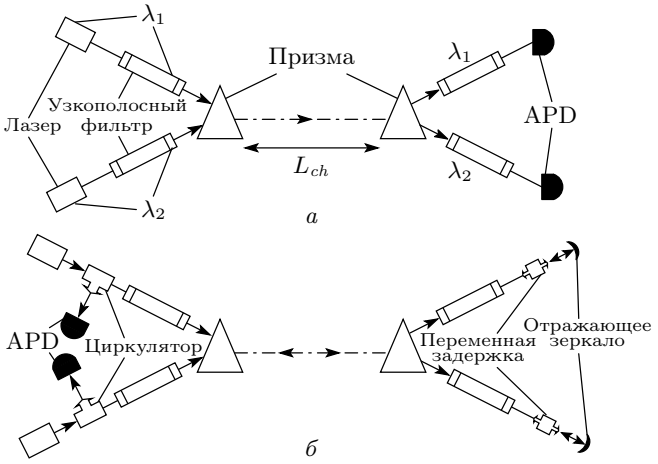

Рис. 4.

тяженные состояния показаны уже после прохождения фильтра. На передающем конце схема имеет два лазера, спектр выходного излучения которых центрирован вокруг разных длин волн λ_1 и λ_2. Спектры излучения не перекрываются. В фиксированный момент времени начала протокола случайно запускается один из лазеров, который выдает импульс с широким спектром $\Delta\omega_1$ и, соответственно, короткий по времени $\Delta t \sim 1/\Delta\omega_1$. Момент включения лазера анонсируется впоследствии через общедоступный (открытый) классический канал связи. Точность синхронизации часов Δt. Далее широкополосное состояние поступает на вход фильтра (рис. 4*а*). Каждый фильтр после лазеров вырезает из широкого спектра $\Delta\omega$ неперекрывающиеся узкие частотные полосы шириной Δk. Если мощность на выходе лазера в исходной широкой частотной полосе $\Delta\omega$ известна и может регулироваться, то будет известна также мощность в узкой вырезанной частотной полосе Δk, тем самым будет известно и среднее число фотонов μ в состоянии, которое направляется в канал связи после фильтра. Диспергирующая среда (призма на рис. 4) нужна для отклонения состояний, центрированных вокруг разных длин волн.

Вырезание узкой частотной полосы шириной Δk требует пространственно-временного интервала $\Delta T \sim 1/\Delta k$. Иначе говоря, через время ΔT протяженное состояние длиной $c \cdot \Delta T$ целиком поступает в канал связи. Точность выхода в канал связи переднего фронта протяженного состояния известна с точностью Δt. Соответственно, длительность состояния с узким частотным спектром Δk должна быть много больше времени Δt, с которой синхронизировано общее начало отсчета на приемном и передающем концах. Поскольку длина канала связи известна, а также известна протяженность состояния ΔT и момент выхода переднего фронта этого состояния в канал связи, то известно и время, необходимое для достижения приемного конца. На приемном конце перед каждым детектором APD (avalanche photodiode) стоит точно такой же фильтр, как на передающем конце, для того чтобы на детектор не проходили состояния, более короткие по времени, чем это возможно для частотной полосы Δk. Детекторы работают в ждущем режиме (в гейгеровской моде). Требуется, чтобы постоянная времени APD τ_D была много меньше длительности состояния, $\tau_D \ll \Delta T$. Пользователь B оставляет только те посылки, в которых срабатывание было во временном окне $(L_{ch}, L_{ch} + \Delta T)$ (рис. 5*а*). Время выхода переднего фронта состояния считаем равным $t_A = 0$, (см. рис. 5*а*). Фильтр на приемном конце перед детектором нужен для того, чтобы исключить перепосылку подслушивателем состояний, более коротких по времени и, соответственно, с широким частотным спектром, что могло бы скомпенсировать задержку при измерении протяженного состояния длительностью T.

9. ДВУХПРОХОДНАЯ КВАНТОВАЯ КРИПТОСИСТЕМА БЕЗ СИНХРОНИЗАЦИИ ЧАСОВ НА ПРИЕМНОМ И ПЕРЕДАЮЩЕМ КОНЦАХ

Двухпроходная схема (рис. 4*б*) отличается от предыдущей тем существенным моментом, что не требует установления общего начала отсчета времени, достаточно только знания длины канала связи. Формирование состояний происходит аналогично предыдущему. Если известны длина канала связи и момент посылки состояния, то также известен момент возврата состояния к участнику A. Идея детектирования подслушивателя состоит в том, что состояние после достижения приемного конца отражается и возвращается назад в участнику A, который, зная момент посылки состояния и длину канала связи, автоматически знает, в какой момент времени состояние целиком достигнет его стороны (в какое временное окно оно вернется). Сказанное поясняется пространственно-временной диаграммой на рис. 5*б*.

Работа такой схемы достигается введением в нее небольшого числа новых компонентов. На отражающем конце участник B случайно открывает один из каналов отражения, второй канал при этом закрыт. Далее через открытый канал участник A анонсирует только те посылки, когда состояние к нему вернулось и было зарегистрировано в правильном вре-

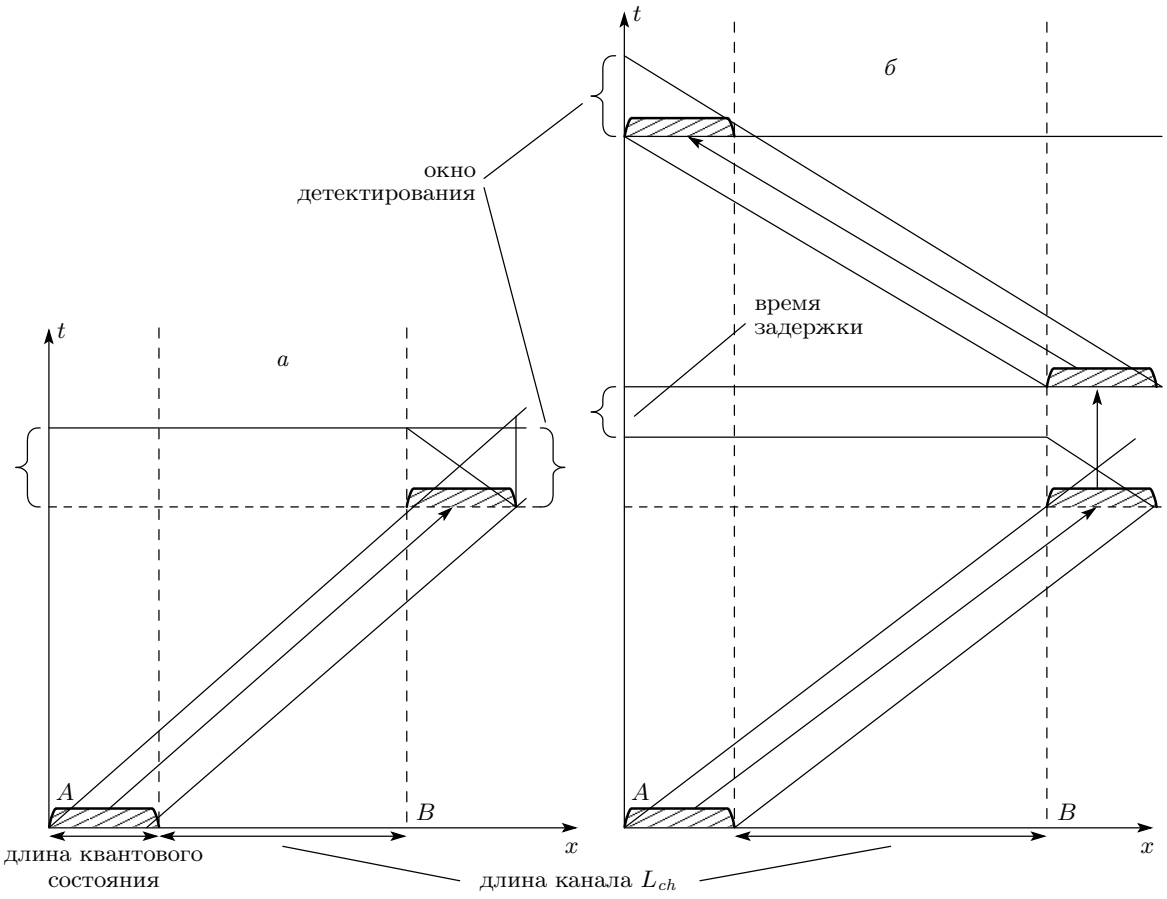

Рис. 5.

менном окне. Если участник B открыл канал не для того состояния, которое посылал A, то такая посылка выпадает, поскольку состояние не вернется к A. Если же B открыл правильный канал, а участник A затем сообщил через открытый, что состояние дало отсчет в правильном временном окне, то оба участника знают передаваемое состояние и передаваемый бит.

Если передний фронт состояния поступает в канал в момент времени t_A, то после возврата участник A должен оставлять только отсчеты во временном окне $(t_A{+}2L_{ch}{+}t_{B\ \ delay}, t_A{+}2L_{ch}{+}t_{B\ \ delay}{+}T)$. Здесь $t_{B\ \ delay}$ — случайная варьируемая задержка, вносимая участником B, которая сообщается для каждой посылки через открытый канал связи впоследствии (см. рис. 5*б*). Внесение случайной задержки важно для секретности протокола.

Наконец, обсудим работу прототипа для передачи ключей на орбитальные объекты (см. рис. 6*а–в*, схемы тракинга и позиционирования для краткости не показаны).

Технически гораздо более удобно формировать протяженные состояния, полученные из коротких по времени импульсов, чем приготавливать состояния с узким частотным спектром. Для этого достаточно использовать плечо разбалансированного интерферометра с двумя светоделителями. На рис. 6*а* показана двухпроходная схема без синхронизации часов на двух концах. Короткие состояния с длительностью порядка 1 нс в каждой посылке формируются двумя лазерами с разной длиной волны, которые попадают в окна прозрачности в атмосфере, например, 850 и 1000 нм. На данных длинах волн процент прохождения составляет около 74–75 %. Момент запуска одного из лазеров фиксируется (с точностью длительности импульса, например, 1 нс). Далее состояние поступает на плечо разбалансированного интерферометра, разность хода длинного и короткого путей превышает протяженность входного состояния (интерференции импульса самого на себе в плече нет). На выходе возникает новое протяженное состояние, представляющее со-

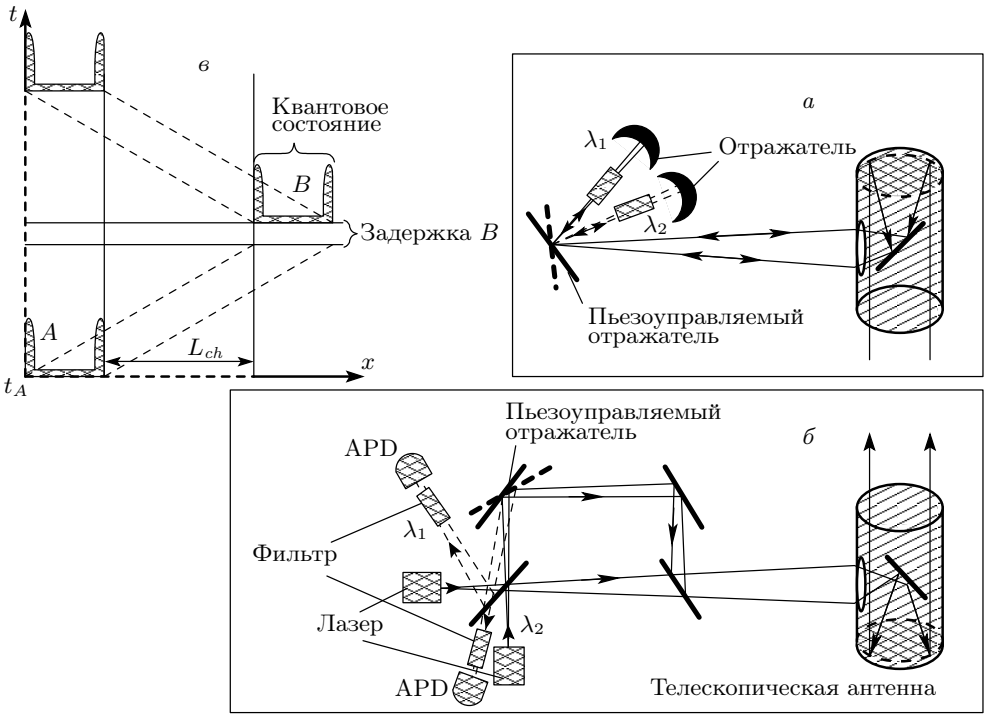

Рис. 6.

бой суперпозицию двух коротких «половинок» (пространственно-временная диаграмма процесса передачи–приема показана на рис. 6*в*), причем расстояние между «половинками» (протяженность нового состояния) должно быть больше, чем величина точности, с которой известно расстояние между наземным и орбитальным объектом. Далее после фокусировки через телескопическую систему сигнал передается на орбитальный объект. На приемном конце (рис. 6*б*) после приемной телескопической системы состояние поступает на управляемое пьезоманипуляторами зеркало и отражатели. Одно из двух положений зеркала в каждой посылке выбирается случайно и независимо от передающего конца. Случайная задержка на приемном конце у B здесь также необходима, величина задержки анонсируется участником B через открытый канал после сеанса передачи битовой последовательности. Если имеется совпадение (например, послано состояние с λ_1 и отражатель выставлен также для отражения состояния λ_1), то состояние возвращается на передающий конец. В противном случае посылка оказывается холостой, состояние не вернется к передающему концу. На передающем конце также имеется управляемое зеркало, положение которого зависит от переданного состояния. После возврата состояния с λ_1 положение зеркала таково, что состояние поступает в канал регистрации на APD-детектор для λ_1. Состояние непосредственно перед детектором представляет собой суперпозицию трех узких «пичков» (на рис. 6*б* не показаны), раздвинутых на разность длин длинного и короткого плеч интерферометра. Причем амплитуда центрального «пичка» в два раза больше переднего и заднего по времени «пичков». Момент срабатывания APD происходит случайно на одном из «пичков», данный момент времени фиксируется.

Извлечение секретного ключа из переданной последовательности и детектирование возможных попыток подслушивания проводится аналогично процедурам, описанным выше.

Преимущество при использовании протяженных состояний, состоящих из суперпозиции их двух «половинок», по сравнению с состояниями, у которых протяженность достигается за счет узкой частотной полосы, состоит в том, что их легче экспериментально реализовать и детектирование их более эффективно, поскольку не требуется держать APD-детектор обратно смещенным в течение длительного времени (время определяется всей протяженностью состояния), а только в короткие интервалы, когда «половинки» достигают APD. Данное

обстоятельство существенно уменьшает паразитные темновые отсчеты.

Приведем краткие числовые оценки. Пусть радиус орбиты спутника составляет $L_s \approx 1000$ км $= 10^8$ см. Скорость спутника $v_s \approx 5$ км/с $= 5 \cdot 10^5$ см/с, скорость света $c = 3 \cdot 10^{10}$ см/с. Точность, с которой может быть определено расстояние между наземным объектом и спутником, при посылке классического сигнала для определения расстояния определяется сдвигом спутника за время прохождения зондирующего сигнала с Земли на спутник и назад. Данное смещение есть

$$\frac{L_s v_s}{c} = \frac{10^8 \cdot 5 \cdot 10^5}{3 \cdot 10^{10}} \approx 1.7 \cdot 10^3 \text{ см} = 17 \text{ м}.$$

Поэтому растянутое состояние из двух половинок должно быть больше 17 м. Пусть протяженность состояния $L = 300$ м $= 3 \cdot 10^4$ см. Смещение спутника за время, необходимое для того чтобы обе «половинки» успели отразиться от зеркал у участника B, есть

$$\frac{L v_s}{c} = \frac{3 \cdot 10^4 \cdot 5 \cdot 10^5}{3 \cdot 10^{10}} = 5 \cdot 10^{-1} \text{ см} = 5 \text{ мм}.$$

Это означает, что за время отражения не требуется дополнительная подстройка отражателя, если диаметр телескопической антенны составляет величину порядка 10 см. Определение расстояния между орбитальным и наземным объектами может проводиться при помощи третьей стороны. Точности системы GPS или российской системы ГЛОНАСС достаточно для определения расстояния.

Поскольку в данной криптосистеме используются ортогональные состояния с неперекрывающимися частотными спектрами, схема допускает обобщение на мультиплексный случай. При мультиплексировании по частотным каналам увеличение скорости генерации ключа прямо пропорционально числу каналов в частотной полосе в окне прозрачности.

10. ЗАКЛЮЧЕНИЕ

Самой принципиальной проблемой для обеспечения секретности схем нерелятивистской квантовой криптографии, секретность которых основана на факте достоверной неразличимости неортогональных состояний, является затухание в квантовом канале связи. Начиная с некоторой критической величины (которая точно неизвестна), нерелятивистские протоколы квантовой криптографии не могут обеспечить безусловную секретность, которая гарантируется лишь фундаментальными запретами природы (квантовой механики).

Если проанализировать квантовые криптографические протоколы в канале с затуханием и доказательства их секретности, то проблемы с секретностью появляются, если подслушиватель может «заменить» имеющийся квантовый канал с затуханием на канал без затухания или с меньшим затуханием. Важно, что «замена» канала с затуханием на более хороший канал как в оптоволоконных системах, так и системах, работающих через открытое пространство, вовсе не означает, например, прокладку новой оптоволоконной линии. Существует простая стратегия для подслушивателя, которая эквивалентна «замене» квантового канала на более хороший без физической прокладки нового оптоволокна. Для этого достаточно иметь два узла для подслушивателя, один вблизи передающей стороны, второй — вблизи принимающей. Оптоволокно разрывается, и возле передающего узла в разрыв вставляется детектирующая аппаратура, а возле приемного — передающая. При таком расположении затуханием между узлами подслушивателя и узлами легитимных пользователей можно пренебречь. Вблизи передающей стороны подслушиватель проводит измерения, аналогичные тем, которые обсуждались в разд. 2. Если получен результат с определенным исходом («0» или «1»), то подслушиватель посылает на свой узел вблизи B данную информацию по открытому классическому каналу, которой можно всегда считать идеальным. На узле вблизи принимающий стороны второй соучастник подслушивателя готовит квантовое состояние ($|\varphi_0\rangle$ или $|\varphi_1\rangle$) в соответствии с полученной по классическому каналу информацией и направляет его к легитимному пользователю B по оптоволокну. Если получен результат с неопределенным исходом «?» (см. формулу (3)), то к легитимному участнику B квантовое состояния с ближнего к нему узла подслушивателя не посылается. Поскольку исходный квантовый канал был с затуханием, начиная с некоторой критической длины канала такое подслушивание невозможно обнаружить. Очевидно, что такая стратегия применима и при передаче ключа через открытое пространство. Замена квантового канала на более хороший в этом случае не означает улучшения свойств передающей среды (атмосферы).

Второй принципиальной проблемой является неоднофотонность источников. Вообще говоря, не обязательно использовать однофотонные состояния, однако при этом необходима такая процедура измерения на приемном конце, которая выделяет

пару многофотонных состояний как целостные объекты. Единственным примером такой процедуры на сегодняшний день является процедура гомодинного детектирования, которая с формальной точки зрения реализует измерение, описывающее проекцию на когерентное состояние. Такая процедура достаточно сложна, а криптографическая стойкость протоколов распространения ключей на многофотонных состояниях мало изучена. Если использовать для измерений стандартные процедуры детектирования при помощи лавинного фотодетектора, то однофотонность оказывается принципиально важной. Даже если удастся реализовать идеальный однофотонный источник (продвижения в этом направлении уже есть [16]), то это не снимет проблемы, связанной с затуханием.

На наш взгляд, проблема затухания в квантовых криптосистемах, основанных только на геометрических свойствах — достоверной неразличимости неортогональных квантовых состояний, — не может быть решена никакими ухищрениями и усложнениями протоколов обмена. Требуется привлечение в квантовую криптографию дополнительных фундаментальных принципов, которые бы гарантировали безусловную секретность при любом затухании, фактически не зависели бы от количества исчезающих (поглощенных) в квантовом канале связи фотонов. Таким фундаментальным принципом является принцип релятивистской причинности, который следует из ограничений специальной теории относительности, накладываемых на измеримость квантовых состояний. Затухание в квантовом канале связи, какое бы оно ни было, не может отменить ограничений специальной теории относительности и нарушить запреты на скорость передачи информации, диктуемые причинностью. Никакое затухание не позволяет получить информацию о протяженном квантовом состоянии безмассового квантованного поля (фотонов) быстрее, чем это разрешается специальной теорией относительности. В противном случае это означало бы возможность передавать классическую информацию между пространственно удаленными наблюдателями быстрее скорости света.

Привлечение новых фундаментальных физических принципов в квантовую криптографию позволяет сформулировать принципиально новый подход к обеспечению безусловной секретности квантовых криптосистем, который снимает выше упомянутые принципиальные трудности. Подобные квантовые криптосистемы естественно называть релятивистскими.

Таким образом, релятивистские квантовые криптосистемы остаются безусловно секретными. При этом, во-первых, любое затухание в квантовом канале связи снижает лишь скорость генерации ключа, но не влияет на его секретность. Во-вторых, не требуется строгая однофотонность источника, достаточно лишь присутствия однофотонной компоненты в состояниях. Схема остается безусловно секретной даже при сколь угодно малой доле (вероятности) однофотонной компоненты. Формально это означает, что состояние может иметь сколь угодно большое среднее число фотонов. Доля однофотонной компоненты влияет лишь на скорость генерации ключа, но не на его секретность.

Работа поддержана Академией криптографии РФ, а также РФФИ (грант № 02-02-16289).

ЛИТЕРАТУРА

1. В. А. Котельников, Отчет, Москва (1941).
2. C. E. Shannon, Bell Syst. Tech. J. **28**, 658 (1949).
3. G. S. Vernam, J. Amer. Inst. Elect. Eng. **55**, 109 (1926).
4. H. Kosaka, A. Tomita, Y. Nambu, T. Kimura, and K. Nakamura, E-print archives quant-ph/0306066.
5. D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, E-print archives quant-ph/0203118.
6. A. Muller, J. Breguet, and N. Gisin, Europhys. Lett. **23**, 383 (1993); A. Muller, H. Zbinden, and N. Gisin, Nature **378**, 449 (1995); A. Muller, H. Zbinden, and N. Gisin, Europhys. Lett. **33**, 335 (1996).
7. Ch. Marand and P. D. Tounsend, Opt. Lett. **20**, 1695 (1995); P. D. Tounsend, Nature **385**, 47 (1997); IEEE Photonics Tech. Lett. **10**, 1048 (1998).
8. R. Hughes, G. G. Luther, G. L. Morgan, and C. Simmons, Lect. Notes Comp. Sci. **1109**, 329 (1996); R. Hughes, G. Morgan, and C. Peterson, J. Mod. Opt. **47**, 533 (2000).
9. P. C. Sun, Y. Mazurenko, and Y. Fainman, Opt. Lett. **20**, 1062 (1995); Y. Mazurenko, R. Giust, and J. P. Goedgebuer, Opt. Commun. **133**, 87 (1997).
10. F. Grosshans, G. Van Assche, J. Wenger, R. Brourf, N. J. Cerf, and P. Grangier, Nature **421**, 238 (2003).
11. M. Martinelli, Opt. Commun. **72**, 341 (1989); J. Mod. Opt. **39**, 451 (1992).

12. C. Elliot, D. Pearson, and G. Troxel, E-print archives quant-ph/0307049.

13. C. Kurtsiefera, P. Zarda, M. Halder, P. M. Gorman, P. R. Tapster, J. G. Rarity, and H. Weinfurter, Preprint Los Alamos (2002).

14. R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson, New J. Phys. **4**, 43.1 (2002).

15. J. G. Rarity, P. R. Tapster, P. M. Gorman, and P. Knight, New J. Phys. **4**, 82.1 (2002).

16. A. Beveratos, R. Brouri, T. Gacoin, A. Villing, J.-P. Roizat, and P. Grangier, E-print archives quant-ph, 0206136.

17. N. Lütkenhaus, Phys. Rev. A **55**, 052304 (2000); G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).

18. A. Acin, N. Gisin, and V. Scarani, E-print archives quant-ph/0302037.

19. W. K. Wootters and W. H. Zurek, Nature **299**, 802 (1982).

20. C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992); C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).

21. D. Mayers and A. Yao, E-print archives quant-ph/9802025.

22. P. W. Shor and J. Preskill, E-print archives quant-ph/0003004.

23. W. Diffi and M. E. Hellman, IEEE Trans. on Inf. Theory **IT-22**, 644 (1976).

24. R. L. Rivest, A. Shamir, and L. Adleman, Commun. ACM **21**, 120 (1978).

25. Н. Н. Боголюбов, Д. В. Ширков, *Введение в теорию квантованных полей*, Наука, Москва (1973).

26. Л. Д. Ландау, Р. Пайерлс, Z. für Phys. **69**, 56 (1931); *Собрание трудов*, Наука, Москва (1969), т. 1, стр. 33, 56; Z. für Phys. **62**, 188 (1930).

27. N. Bohr and L. Rosenfeld, Math.-Fys. Medd., **12**, 3 (1933); Н. Бор, *Собрание научных трудов*, Наука, Москва (1969), т. 1, стр. 39.

28. M. Fleischhauer and M. D. Lukin, Phys. Rev. Lett. **84**, 5094 (2000).

29. W. H. Fuchs, J. of Math. Analysis and Appl. **9**, 317 (1964).

30. D. Slepian and H. O. Pollak, Bell Syst. Techn. J. **XL**, 40 (1961).

31. Н. Н. Боголюбов, А. А. Логунов, А. И. Оксак, И. Т. Тодоров, *Общие принципы квантовой теории поля*, Наука, Москва (1987).

32. A. M. Jaffe, Phys. Rev. **158**, 1454 (1967).

33. G. C. Hegerfeldt, Phys. Rev. D **10**, 3320 (1974); G. C. Hegerfeldt and S. N. M. Ruijsenaar, Phys. Rev. D **22**, 377 (1980).

34. Д. А. Киржниц, УФН **90**, 129 (1966).

35. Н. Винер, Р. Пэли, *Преобразование Фурье в комплексной области*, Наука, Москва (1964) [N. Wiener and R. Paley, *Fourier Transform in the Complex Domain*, New-York (1934)].

36. I. Bialynicki-Birula, Phys. Rev. Lett. **80**, 5247 (1998).

37. T. D. Newton and E. P. Wigner, Rev. Mod. Phys. **21**, 400 (1949).

38. A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).

39. E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury, E-print archives quant-ph/9912053.

40. Hoi-Kwong Lo and H. F. Chau, E-print archives quant-ph/9803006.

41. C. E. Shannon, Bell Syst. Tech. J. **27**, 397; 623 (1948).

42. Р. Галлагер, *Теория информации и надежная связь*, Советское радио, Москва (1974).

43. E. J. Mac Williams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Publ. Company, Amsterdam, New York, Oxord (1977).

44. J. Wolfowitz, Illinois J. of Math. **1**, 591 (1957).

45. C. H. Bennett and G. Brassard, in *Proc. of IEEE Int. Conf. on Comput. Sys. and Sign. Proces.*, Bangalore, India (1984), p. 175.