ЖЭТФ, 2003, том 124, вып. 5 (11), стр. 1172–1196

НОВЫЙ ПОДХОД К БЕЗУСЛОВНОЙ СЕКРЕТНОСТИ В РЕЛЯТИВИСТСКОЙ КВАНТОВОЙ КРИПТОГРАФИИ

С. Н. Молотков [a,b*]

[a] *Институт физики твердого тела Российской академии наук*
142432, Черноголовка, Московская обл., Россия

[b] *Факультет вычислительной математики и кибернетики,*
Московский государственный университет им. М. В. Ломоносова
119899, Москва, Россия

Поступила в редакцию 20 февраля 2003 г.

Предлагается принципиально новый подход к обеспечению секретного распространения ключа по открытым квантовым каналам связи. В отличие от предыдущих схем, где секретность основана на специальных свойствах неортогональных состояний в гильбертовом пространстве, секретность в предлагаемой схеме базируется на пространственно-временной структуре состояний и ограничениях, диктуемых специальной теорий относительности. Учет этих обстоятельств позволяет передавать секретный ключ при помощи практически любых квантовых состояний.

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

1. ВВЕДЕНИЕ

Главная задача криптографии состоит в конфиденциальной передаче информации между двумя или несколькими легитимными пользователями. При передаче конфиденциальной информации по открытым каналам связи используются различные системы шифрования. Абсолютно устойчивыми (секретными, не раскалываемыми) являются системы шифрования с одноразовыми ключами, часто называемые схемами Вернама [1]. Утверждение об абсолютной стойкости (секретности) схемы шифрования с одноразовым ключом, пожалуй, является единственным математически строгим результатом в криптографии. Впервые условия абсолютной стойкости были осознаны в работе Котельникова в 1941 г. В 1944 г. аналогичное утверждение было доказано в работе Шеннона и опубликовано в 1949 г. [2]. На формальном языке криптосистема абсолютно секретна, если взаимная информация

$$I(M;C) = H(C) - H(C|M) = 0, \qquad (1)$$

где M — бинарная строка из ансамбля сообщений, который следует передать, C — бинарная строка, описывающая зашифрованное сообщение из M. Из равенства (1) сразу следует, что условная вероятность появления конкретного шифротекста c при условии, что было выбрано сообщение m, есть

$$p(c|m) = p(c).$$

Это означает, что если вероятность появления зашифрованного сообщения c не зависит от самого сообщения m, то криптосистема будет абсолютно секретной.

Примером абсолютно стойкой криптосистемы является схема Вернама [1] с одноразовыми случайными ключами k (k — строка бит, известная только легитимным пользователям). Сообщения из ансамбля M сжимаются до строки длиной в m бит, равной $H(M)$, выбирается случайный ключ k длиной $H(M)$, шифротекст представляет собой бинарную строку

$$c = m \oplus k.$$

Условие однозначной дешифруемости имеет вид

$$I(M;C|K) = I(M). \qquad (2)$$

Дешифровка зашифрованного сообщения на приемном конце осуществляется посредством обратной операции

$$m = c \oplus k = (m \oplus k) \oplus k.$$

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

Это означает, что если ключ k случаен, известен только легитимным пользователям, его длина равна длине сообщения и ключ используется только один раз, то схема шифрования будет абсолютно стойкой (не раскалываемой). Главная трудность при реализации данной схемы состоит в распространении секретного ключа между пространственно удаленными пользователями.

Рассуждения, приведенные выше, являются чисто математическими и никак не апеллируют к законам физики. Однако вопрос о распространении ключа между удаленными в пространстве пользователями не может быть решен без обращения к физической реальности, поскольку сами понятия пространства и времени являются физическими понятиями. Несмотря на то, что информация является математическим понятием, носителями информации всегда являются конкретные физические объекты.

В классической физике, как нерелятивистской, так и релятивистской, состояния физических объектов описываются вещественными функциями координат и времени. Постулируется (и это отвечает опыту), что состояние физических объектов может быть, в принципе, измерено сколь угодно точно и без возмущения. Поэтому в рамках классической физики невозможно обеспечить секретное распространение ключа через открытый канал связи, поскольку невозможно гарантировать детектирование попыток пассивного подслушивания. Поэтому криптосистемы с одноразовыми ключами не получили широкого применения.

Из-за невозможности распространения секретного ключа при помощи классических сигналов через открытый канал связи достаточно широко используют криптосистемы с отрытыми ключами. Последнее стало возможным благодаря замечательному открытию сделанному Хеллманом и Диффи [3]. Криптосистемы с открытым ключом, также называемые системами типа RSA [4] (Ривест–Шамир–Адлеман), не требуют предварительного распространения общего секретного ключа. Секретность криптосистем с открытым ключом базируется на недоказанной сложности обращения некоторых функций с секретом (например, дискретного логарифма). Известные классические алгоритмы, выполняемые на вычислительном устройстве, работающем по законам классической физики, имеют экспоненциальную сложность по размеру входных данных, а полиномиальные алгоритмы неизвестны, хотя и не доказано, что они не существуют. В строгом смысле системы RSA не являются абсолютно стойкими, поскольку Шором [5] явно предъявлен квантовый алгоритм с полиномиальной сложностью для обращения дискретного логарифма, что позволяет, в принципе, раскалывать подобные схемы шифрования, поскольку нет принципиальных запретов на создание квантового компьютера. По крайней мере на сегодняшний день считается, что трудности — чисто технические, но они могут быть столь велики, что отодвинут создание квантового компьютера на многие десятилетия. В принципе, существует также опасность в раскалывании систем типа RSA, состоящая в том, что нет никаких строгих гарантий того, что не будет найден классический алгоритм с полиномиальной степенью сложности.

Таким образом, системы типа RSA, по-видимому, являются стойкими в классической физике, но перестают быть таковыми в квантовой области [5].

Квантовая криптография позволяет решить важную задачу о распространении секретного ключа по открытым квантовым каналам связи. В отличие от квантового компьютера, где продемонстрирована лишь работа отдельных вентилей для небольшого числа кубитов, успехи в практической реализации квантовых криптосистем гораздо более впечатляющие. Существуют работающие прототипы на расстояниях в несколько десятков километров (рекорд на сегодняшний день составляет 67 км [6]), как на оптоволоконных линиях (например, под Женевским озером, длина линии 23 км) [7], так и через открытое пространство.

Предлагаемый в данной работе подход к обеспечению секретности может оказаться практически более удобным, поскольку в нем используются частотные свойства состояний, которые являются более устойчивыми к внешним возмущениям, чем поляризационные степени свободы. Кроме того, большинство реализованных криптосистем в том или ином виде представляют собой модификации интерферометров типа Маха–Цандера. Наша схема не использует интерферометров.

2. КВАНТОВАЯ КРИПТОГРАФИЯ В НЕРЕЛЯТИВИСТСКОМ СЛУЧАЕ

Законы квантовой механики являются более ограничительными, чем законы классической физики в том смысле, что любое измерение (наблюдение) квантовой системы, вообще говоря, изменяет ее состояние. В квантовой механике открывается возможность реализовать безусловно секретное распространение ключа между пространственно удаленными пользователями и тем самым создать

абсолютно стойкую криптосистему с одноразовыми ключами. Под безусловной секретностью подразумевается секретность, которая гарантируется фундаментальными законами природы — законами квантовой механики.

Идея квантовой криптографии была высказана в работе Виснера [8] и стала общедоступной после работы Беннета, Брассара [9]. Безусловная секретность нерелятивистской квантовой криптографии основана на двух тесно связанных между собой запретах, диктуемых квантовой механикой: во-первых, невозможность копирования неизвестного квантового состояния — теорема «no cloning» [10], во-вторых, невозможность получить информацию о неортогональных квантовых состояниях без их возмущения [11].

Приведем элегантное доказательство второго утверждения, принадлежащее Беннету [11], поскольку оно потребуется для дальнейшего анализа. Пусть имеется два чистых состояния некоторой квантовой системы, описывающиеся векторами (лучами) в гильбертовом пространстве $|\varphi_0\rangle$, $|\varphi_1\rangle \in \mathcal{H}$, которые ассоциируются с классическими битами информации 0 и 1, соответственно. Пусть наблюдателю предъявляется одно из состояний, но неизвестно какое. Задача наблюдателя состоит в том, чтобы узнать, что это за состояние, и по возможности оставить его невозмущенным.

Доказательство проводится методом от противного. Предполагается, что наблюдатель (подслушиватель[1)]) может проводить с состоянием самые общие манипуляции, которые допускает квантовая механика. В наиболее общем виде это сводится к следующему. Подслушиватель имеет вспомогательную квантовую систему в некотором стандартном состоянии $|a\rangle \in \mathcal{H}_a$. Подслушиватель включает взаимодействие между предъявляемым состоянием ($|\varphi_0\rangle$ или $|\varphi_1\rangle$) и вспомогательной системой и позволяет им совместно эволюционировать некоторое время. Сказанное формально выражается в следующем:

$$|\varphi_0\rangle \to U(|\varphi_0\rangle \otimes |a\rangle), \tag{3}$$

$$|\varphi_1\rangle \to U(|\varphi_1\rangle \otimes |a\rangle), \tag{4}$$

где U — унитарный оператор, действующий в $\mathcal{H} \otimes \mathcal{H}_a$. Допустим, что в результате взаимодействия и совместной унитарной эволюции система остается в исходном состоянии, а вспомогательная система переходит в некоторое новое состояние, зависящее от неизвестного входного состояния:

$$U(|\varphi_0\rangle \otimes |a\rangle) = |\varphi_0\rangle \otimes |a_0\rangle, \tag{5}$$

$$U(|\varphi_1\rangle \otimes |a\rangle) = |\varphi_1\rangle \otimes |a_1\rangle. \tag{6}$$

Комплексное сопряжение одного из уравнений, например второго, дает

$$(\langle a| \otimes \langle\varphi_1|)U^{-1} = \langle a_1| \otimes \langle\varphi_1|. \tag{7}$$

Взятие скалярного произведения уравнений (5) и (7) приводит к выражению

$$\langle a| \otimes \langle\varphi_1|U^{-1}U|\varphi_0\rangle \otimes |a\rangle = \langle\varphi_1|\varphi_0\rangle\langle a_1|a_0\rangle. \tag{8}$$

В силу унитарности U имеем

$$\langle a|a\rangle\langle\varphi_1|\varphi_0\rangle = \langle a_1|a_0\rangle\langle\varphi_1|\varphi_0\rangle. \tag{9}$$

Поскольку чистые состояния являются нормированными векторами, имеем

$$\langle a|a\rangle = 1.$$

Далее имеются две принципиально разные возможности:

1) состояния неортогональны, $\langle\varphi_1|\varphi_0\rangle \neq 0$;

2) состояния ортогональны $\langle\varphi_1|\varphi_0\rangle = 0$.

Если состояния неортогональны, то возможно сокращение обеих частей (9) на сомножитель $\langle\varphi_1|\varphi_0\rangle \neq 0$, что дает

$$\langle a_1|a_0\rangle = 1. \tag{10}$$

Поскольку чистые состояния являются крайними точками выпуклого множества состояний, последнее условие означает, что $|a_1\rangle = |a_0\rangle$.

Таким образом, исходное предположение о том, что информационные состояния остаются невозмущенными, а состояние вспомогательной системы изменяется в зависимости от входного состояния, является неверным. Другими словами, это означает, что невозможно получить информацию о неортогональных состояниях без их возмущения. Любое наблюдение (измерение) над неортогональными состояниями возмущает их. Возмущение состояний изменяет переходные вероятности в канале и позволяет детектировать любые попытки подслушивания.

Различные предложения и практические реализации квантовых криптосистем неизбежно используют идею неортогональности.

Принципиально иная ситуация имеет место, когда состояния ортогональны, $\langle\varphi_1|\varphi_0\rangle = 0$. В этом

[1)] В ряде работ легитимных пользователей именуют Алиса, Боб, подслушивателя — Ева.

случае сокращение в обеих частях (9) на нулевой сомножитель невозможно, поэтому в этом случае нет никаких формальных ограничений на извлечение информации из ортогональных состояний без их возмущения. Строго говоря, в этом случае теорема не дает никаких запретов. Тот факт, что возможно извлечение информации об ортогональных состояниях без их возмущения, можно продемонстрировать, явно предъявив измерение, которое оставляет состояния невозмущенными и дает о них информацию. Действительно, измерение, которое дает информацию (даже достоверную с вероятностью единица) о состояниях без их возмущения, существует. Как и любое измерение, данное измерение описывается ортогональным или неортогональным разбиением единицы в $\mathcal{H}$. В данном случае измерение описывается ортогональным разбиением единицы в подпространстве $\mathcal{H}$, натянутом на вектора $|\varphi_{0,1}\rangle$, тогда имеем

$$I\{\Omega\} = \mathcal{P}_0 + \mathcal{P}_1, \quad \mathcal{P}_{0,1} = |\varphi_{0,1}\rangle\langle\varphi_{0,1}|. \tag{11}$$

Пространством результатов в данном случае является дискретное множество $\Omega = \{0,1\}$. Инструмент (часто также называемый супероператором), описывающий состояние квантовой системы после того как получен конкретный исход измерения, имеет вид

$$\mathcal{T}[\dots] = \mathcal{P}_0[\dots]\mathcal{P}_0 + \mathcal{P}_1[\dots]\mathcal{P}_1. \tag{12}$$

Вероятность взаимно исключающих исходов на любом из пары состояний равна

$$\Pr\{i\} = \mathrm{Tr}\{\mathcal{T}[|\varphi_i\rangle\langle\varphi_i|]\} = 1, \quad i = 0,1, \tag{13}$$

соответственно изменение состояния, если получен i исход, есть

$$|\varphi_i\rangle\langle\varphi_i| = \frac{\mathcal{T}[|\varphi_i\rangle\langle\varphi_i|]}{\Pr\{i\}}. \tag{14}$$

То есть возможно достоверное получение информации об ортогональных состояниях без какого-либо возмущения. По этой причине использование ортогональных состояний для квантовой криптографии в нерелятивистском случае даже не обсуждается, поскольку подслушиватель может, не возмущая состояний в канале связи, узнавать передаваемую информацию.

Обратим внимание на принципиально важное для дальнейшего обстоятельство.

Ортогональные состояния достоверно и без возмущения различимы, если они доступны для измерений целиком (как целостные объекты). В скрытом виде данный факт используется в доказательстве.

Слова «доступны как целостные объекты» означают, что доступно все гильбертово пространство состояний, где носитель состояния отличен от нуля. Поясним это на примере. Пусть состояния $|\varphi_{0,1}\rangle \in \mathcal{H}$ и пусть $\{|e_k\rangle\}$ — ортонормированный базис в $\mathcal{H}$,

$$|\varphi_{0,1}\rangle = \sum_{k<n} a_k^{(0,1)}|e_k\rangle + \sum_{k\geq n} a_k^{(0,1)}|e_k\rangle = \\ = |\tilde{\varphi}_{0,1}\rangle + |\tilde{\varphi}_{0,1}^{\perp}\rangle. \tag{15}$$

Далее для краткости положим

$$\{|e_k\rangle \in \mathcal{H}_1\}, \quad k < n,$$

$$\{|e_k\rangle \in \mathcal{H}_1^{\perp}\}, \quad k \geq n,$$

$$\mathcal{H} = \mathcal{H}_1 \oplus \mathcal{H}_1^{\perp}.$$

Пусть теперь состояния недоступны целиком. Более формально это означает, что любое измерение должно описываться разбиением единицы (ортогональным или неортогональным) лишь в доступной части гильбертова пространства. Пусть, например, для измерений доступно $\mathcal{H}_1$, поэтому разбиение единицы может содержать в разложении лишь базисные векторы из этого подпространства. В этом случае даже ортогональные состояния перестают быть достоверно неразличимыми, более того, достоверно и без возмущения неразличимы состояния, которые ортогональны при ограничении на доступное для измерений подпространство $\mathcal{H}_1$ ($\langle\tilde{\varphi}_1|\tilde{\varphi}_0\rangle = 0$). Данное утверждение по сути следует из нормировки квантового состояния. На первый взгляд, такая ситуация, когда для измерений доступна лишь часть пространства состояний, кажется искусственной. На самом деле она, наоборот, даже более типична. Поскольку не существует квантовых объектов вне пространства-времени, все результаты измерений, каким бы сложным ни было пространство результатов, будут неизбежно содержать пространственно-временные области. Поэтому координатное представление абстрактного гильбертова пространства состояний, хотя математически и эквивалентно любому другому представлению, является в определенном смысле выделенным. Реализовать ситуацию, когда пространство состояний целиком недоступно, достаточно просто. Для этого требуется лишь ограничить доступ к части координатного пространства, где отлична от нуля амплитуда состояния (волновая функция). В координатном представлении базисные векторы в $\mathcal{H}$ привязаны к координатному пространству и времени:

$$|e_k\rangle \to |x,t\rangle.$$

Применительно к задачам квантовой криптографии ситуацию, когда ограничен доступ к квантовому состоянию целиком, можно устроить, если использовать состояния, у которых пространственная протяженность состояния (волновой функции) превышает длину канала [12, 13]. В этом случае при распространении состояние в канале целиком никогда не присутствует [12, 13]. Однако такое требование не является необходимым для обеспечения секретности. Ниже мы увидим, что секретность можно обеспечить при использовании практически любых квантовых состояний.

К сожалению, в нерелятивистском квантовом случае, где нет ограничений на предельную скорость распространения, не удается реализовать секретный протокол распространения ключа, основанный на идее ограниченного доступа к квантовому состоянию.

Отметим, что факт достоверной неразличимости, даже для ортогональных квантовых состояний при ограниченном доступе к ним, носит общий характер и не зависит от конкретного представления $\mathcal{H}$. Действительно, любое измерение может быть описано при помощи разбиения единицы

$$I = I_1 + I_1^{\perp}, \tag{16}$$

где I_1 и $I_1^{\perp}$ — единицы в подпространствах $\mathcal{H}_1$ и $\mathcal{H}_1^{\perp}$. При ограниченном доступе к состояниям неизбежно будут иметь место исходы, которым придется приписывать неопределенный (?) результат. Вероятности таких исходов

$$\Pr\{?|i\} = \mathrm{Tr}\{|\varphi_i\rangle\langle\varphi_i|I_1^{\perp}\} \neq 0. \tag{17}$$

Например, при пространственном ограничении доступа к части амплитуды состояния такие исходы можно интерпретировать как исходы, имеющие место в области координатного пространства, недоступного наблюдателю. Полная вероятность исходов во всем пространстве равна единице, однако информацию о состоянии наблюдатель может извлекать только из той области пространства, которая доступна для его измерений. Если в доступной для измерений области пространства измерительный прибор не сработал (формально это означает, что исход имел место вне доступной области пространства), то наблюдатель такому исходу (?) может приписать с вероятностью $1/2$ любой результат (0 или 1). Иначе говоря, минимальное пространство результатов, позволяющее получать информацию о состояниях (0 или 1) будет неизбежно содержать неопределенные исходы $\Omega = \{0, 1, ?\}$, что не позволяет получать достоверную информацию даже об ортогональных состояниях.

3. КВАНТОВАЯ КРИПТОГРАФИЯ В РЕЛЯТИВИСТСКОМ СЛУЧАЕ

В классической физике, как это обсуждалось выше, невозможно секретное распространение ключа по открытому каналу. Законы квантовой механики являются более ограничительными, чем законы классической физики, и они уже позволяют реализовать секретное распространение ключа по открытому квантовому каналу связи. Секретность ключа гарантируется детектированием любых попыток подслушивания. Законы релятивистской квантовой теории поля являются более ограничительными по сравнению с законам нерелятивистской квантовой механики. Впервые ограничения, накладываемые на измеримость квантовых состояний в релятивистской области, обсуждались в работе Ландау и Пайерлса еще в 1931 г. [14]. Дальнейшее исследование было предпринято в работе Бора и Розенфельда [15].

Доказательство [11] о невозможности получения информации о неортогональных состояниях без их возмущения использует только геометрические свойства гильбертова пространства состояний и никоим образом не использует того факта, что существует пространство-время, и что все события, в том числе извлечение информации о состояниях в канале связи, также имеют место в пространстве-времени. Природа квантовой системы также не конкретизируется. В природе не существует абстрактных квантовых систем вне пространства-времени. Более того, сам факт существования пространства-времени приводит к тому, что существуют лишь определенные элементарные квантовые системы (частицы) в том смысле, что базисные векторы унитарных неприводимых представлений неоднородной группы Лоренца в гильбертовом пространстве трактуются как векторы состояний (волновые функции) элементарных частиц (электронов, позитронов, нейтрино, фотонов и т. д.). Хотя состояния квантовых систем в релятивистском случае описываются векторами в гильбертовом пространстве $\mathcal{H}$, сами векторы содержат внутреннюю «начинку» — сглаживающие функции (амплитуды), зависящие от пространственно-временных переменных [16, 17].

Кроме того, в любой реальной ситуации при передаче информации в квантовых криптосистемах на большие расстояния единственными приемлемыми

носителями являются фотоны — безмассовые частицы (состояния квантованного поля), распространяющиеся с предельно допустимой скоростью (скоростью света). Факт существования предельной скорости является фундаментальным законом природы. Далее, любая передача информации в пространстве-времени с помощью как классических, так и квантовых объектов, подразумевает наличие причинно-следственной связи между приготовлением носителя информации, его распространением, а также измерением над ним.

Тот факт, что носителями информации являются состояния безмассового квантованного поля, а также принцип релятивистской причинности позволяют построить принципиально новую безусловно секретную криптосистему, секретность которой основана на этих фундаментальных принципах, а не на геометрии гильбертова пространства состояний (точнее на особых свойствах неортогональных состояний в нем). В релятивистском случае возможна реализация секретного распространения ключа практически на любых состояниях квантованного фотонного поля (даже на ортогональных и эффективной протяженностью меньшей длины канала связи). Детектирование любых попыток подслушивания происходит по задержке результатов измерений. В нерелятивистском случае детектирование попыток подслушивания обнаруживается по изменению вектора состояний одного из неортогональных состояний. В релятивистском случае задержка также в определенном смысле является изменением состояния, поскольку сдвиг (трансляция) в пространстве-времени переводит его уже в другое состояние. Это место является принципиально новым и возможно позволит упростить экспериментальную реализацию. Например, можно использовать в качестве носителей ортогональные состояния с не перекрывающимся частотным спектром, что гораздо более удобно, чем кодирование в состояния поляризации, поскольку изменение частоты состояния более устойчиво к шумам, чем состояние поляризации. Кроме того, изменение состояний, связанное с задержкой, может быть экспериментально реализовано при помощи обычных фотодетекторов.

Рассмотрим теперь квантованное электромагнитное поле (фотоны). Операторы электромагнитного поля имеют вид [16] (далее $c = \hbar = 1$)

$$A_\mu^\pm(\hat{x}) = \frac{1}{(2\pi)^{3/2}} \times \times \int \frac{d\mathbf{k}}{\sqrt{2k_0}} \exp(\pm i\hat{k}\hat{x}) e_\mu^m(\mathbf{k}) a_m^\pm(\mathbf{k}) \quad (18)$$

и удовлетворяют коммутационным соотношениям

$$[A_\mu^-(\hat{x}), A_\nu^+(\hat{x}')]_- = i g_{\mu\nu} D_0^-(\hat{x} - \hat{x}'), \quad (19)$$

где $D_0^-(\hat{x} - \hat{x}')$ — коммутаторная функция для поля с нулевой массой:

$$\begin{aligned} D_0^\pm(\hat{x}) &= \pm \frac{1}{i(2\pi)^3} \int \frac{d\mathbf{p}}{2p_0} \exp(\pm i\hat{p}\hat{x}) = \\ &= \frac{1}{4\pi} \varepsilon(x_0)\delta(\hat{x}^2) \pm \frac{i}{4\pi\hat{x}^2}, \\ \varepsilon(x_0)\delta(\hat{x}^2) &\equiv \frac{\delta(x_0 - |\mathbf{x}|) - \delta(x_0 + |\mathbf{x}|)}{2|\mathbf{x}|}. \end{aligned} \quad (20)$$

Здесь величины со шляпками обозначают четырехмерные векторы:

$$\hat{k} = (k_0, \mathbf{k}), \quad \hat{x} = (x_0, \mathbf{x}).$$

Формально есть четыре сорта фотонов: два поперечных, продольный и временной, но два последних являются фиктивными и могут быть исключены из рассмотрения путем введения индефинитной метрики [16, 17]. Для наших целей наиболее короткий путь к ответу связан с использованием конкретной калибровки. Далее будем работать в подпространстве физических состояний в кулоновской калибровке $A_\mu = (\mathbf{A}, \varphi = 0)$, имея дело с двумя физическими поперечными состояниями электромагнитного поля. Операторная обобщенная функция является вектором в трехмерном пространстве:

$$\boldsymbol{\varphi}(\hat{x}) = \frac{1}{(2\pi)^{3/2}} \int \frac{d\mathbf{k}}{\sqrt{2k_0}} \sum_{s=\pm 1} \mathbf{w}(\mathbf{k}, s) \times \times \left\{ a(\mathbf{k}, s) \exp(-i\hat{k}\hat{x}) + a^+(\mathbf{k}, -s) \exp(i\hat{k}\hat{x}) \right\}. \quad (21)$$

Здесь $\mathbf{w}(\mathbf{k}, s)$ — трехмерный вектор, описывающий состояние спиральности $s = \pm 1$:

$$\begin{aligned} \mathbf{w}(\mathbf{k}, \pm) &= \frac{1}{\sqrt{2}} [\mathbf{e}_1(\mathbf{k}) \pm i\mathbf{e}_2(\mathbf{k})], \\ \mathbf{e}_1(\mathbf{k}) &\perp \mathbf{e}_2(\mathbf{k}), \quad |\mathbf{w}(\mathbf{k}, s)|^2 = 1, \end{aligned} \quad (22)$$

где $\mathbf{e}_{1,2}(\mathbf{k})$ — векторы, перпендикулярные $\mathbf{k}$. Операторы поля удовлетворяют уравнениям Максвелла

$$\nabla \times \boldsymbol{\varphi}(\hat{x}) = -i \frac{\partial}{\partial t} \boldsymbol{\varphi}(\hat{x}), \quad \nabla \cdot \boldsymbol{\varphi}(\hat{x}) = 0. \quad (23)$$

Сглаженные операторы поля могут быть записаны в виде

$$\boldsymbol{\varphi}(f) = \sum_{s=\pm 1} \int \boldsymbol{\varphi}(\hat{x}, s) f(\hat{x}, s)\, d\hat{x} = \frac{1}{(2\pi)^{3/2}} \times \times \int \frac{d\mathbf{k}}{\sqrt{2k_0}} \sum_{s=\pm 1} \mathbf{w}(\mathbf{k}, s) \left\{ f(\mathbf{k}, s) a^+(\mathbf{k}, s) + + f^*(\mathbf{k}, s) a(\mathbf{k}, s) \right\}, \quad (24)$$

где $f(\mathbf{k},s)$ представляют собой значения $f(\hat{k},s)$ на массовой поверхности ($f(\hat{k},s)$ — четырехмерный фурье-образ произвольной функции $f(\hat{x},s)$ из пространства основных функций $\Omega(\hat{x})$).

Будем рассматривать одномерную модель. Такое приближение физически оправдано, поскольку реальные оптоволоконные системы являются квазиодномерными объектами. Носителями информации являются чистые состояния безмассового квантованного поля (фотоны). Обобщенные базисные состояния порождаются действием полевых операторов (точнее обобщенных функций с операторными значениями) на циклический вакуумный вектор [16, 17]. С учетом требований лоренц-инвариантности полевые операторы не могут быть просто операторами в $\mathcal{H}$, пусть даже неограниченными. Если считать полевые операторы просто операторами, то в этом случае матричный элемент $\langle 0|\hat{\varphi}^-(\hat{x}')\hat{\varphi}^+(\hat{x})|0\rangle$, трактуемый как рождение частицы в $\hat{x}$, распространение и уничтожение в $\hat{x}'$, будет просто константой, не зависящей от $\hat{x},\hat{x}'$, что противоречит причинности [18].

Обобщенные функции с операторными значениями представляются как

$$\hat{\varphi}^+_\mu(\hat{x}) = \int d\hat{k}\exp(i\hat{k}\hat{x})a^+_\mu(\hat{k})\theta(k_0)\delta(\hat{k}^2), \qquad \hat{k}=(k_0,k), \quad \hat{x}=(x,t), \tag{25}$$

здесь $\mu = 0,1$ — индекс поляризации (спиральности), а коммутационные соотношения имеют вид

$$[a^-_{\mu'}(\hat{k}'),a^+_\mu(\hat{k})] = k_0\delta(k-k')\delta_{\mu,\mu'}. \tag{26}$$

Обобщенные базисные векторы (линейные непрерывные функционалы в $\mathcal{H}$) имеют вид

$$a^+_\mu(\hat{k})|0\rangle = |k\mu\rangle, \quad |\hat{x}\mu\rangle = \varphi_\mu(\hat{x})|0\rangle, \qquad \langle k\mu|k'\mu'\rangle = k_0\delta_{\mu\mu'}\delta(k-k'), \tag{27}$$

где $|0\rangle$ — вакуумный вектор, а $|k\mu\rangle$, $|\hat{x}\mu\rangle \in \Omega^*$ — пространство, сопряженное пространству основных функций Ω. Физические состояния (векторы в $\mathcal{H}$) получаются как результат сглаживания обобщенных операторных функций с основными функциями (амплитудами) из пространства $\Omega(\hat{x})$ (пространство бесконечно дифференцируемых функций убывающих на бесконечности быстрее любой обратной степени полинома):

$$|\varphi_\mu\rangle = \sum_\mu \int d\hat{x}\,\tilde{\varphi}_\mu(\hat{x})\varphi^+_\mu(\hat{x})|0\rangle = \sum_\mu \int \frac{dk}{k_0}\tilde{\varphi}_\mu(k,k_0=|k|)|k\mu\rangle. \tag{28}$$

Здесь амплитуда $\tilde{\varphi}_\mu(\hat{x})$ ($\tilde{\varphi}(k,k_0 = |k|)$) играет роль коэффициента разложения по обобщенным базисным состояниям. Конструкция $\tilde{\varphi}_\mu(\hat{x}) \in \Omega(\hat{x})$, $\hat{\varphi}_\mu(\hat{x}) \in \Omega^*(\hat{x})$, $|\varphi_\mu\rangle \in \mathcal{H}$ и $\Omega \subset \mathcal{H} \subset \Omega^*$ называется оснащенным гильбертовым пространством (тройкой Гельфанда) [17, 19].

Далее будем рассматривать состояния поля, распространяющиеся в одном направлении оси x ($k > 0$) (именно такие состояния переносят информацию между удаленными пользователями):

$$|\varphi_\mu\rangle = \int_0^\infty \frac{dk}{k}\tilde{\varphi}(k,k)|k\mu\rangle = \int_0^\infty dk\varphi(k)|k\mu\rangle = \int_{-\infty}^\infty d(x-t)\varphi(x-t)|x-t,\mu\rangle, \tag{29}$$

где

$$\varphi(k) = \frac{\tilde{\varphi}(k,k)}{\sqrt{k}}, \qquad \varphi(x-t) = \frac{1}{2\pi}\int_0^\infty \exp(-ik(x-t))\varphi(k)\,dk, \qquad |x-t,\mu\rangle = \int_0^\infty \exp(ik(x-t))|k\mu\rangle dk \tag{30}$$

и выполнено условие нормировки

$$\langle\varphi_\mu|\varphi_\mu\rangle = \int_0^\infty \frac{dk}{k}|\tilde{\varphi}(k,k)|^2 = \int_0^\infty dk|\varphi(k)|^2 = \int_{-\infty}^\infty d(x-t)|\varphi(x-t)|^2 = 1. \tag{31}$$

Физические состояния в $\mathcal{H}$ определяются значениями амплитуды на массовой поверхности. Амплитуда состояний, распространяющихся в одном направлении, зависит лишь от разности $\tau = x - t$. Это отражает тот факт, что если результат измерения имел место в момент t в окрестности точки $(x, x+dx)$, то такой же результат будет получен в момент t' в окрестности точки $(x', x'-x+t+dx)$. Далее для краткости будем говорить, что амплитуда $\varphi(\tau)$ задана на ветви светового конуса.

Индекс μ поляризации будем далее опускать как несущественный до тех пор, пока он не потребуется. В качестве информационных состояний выберем ортогональные состояния с не перекрывающейся частотной полосой. Амплитуды, отвечающие векторам состояний, для 0 и 1 выберем, соответственно, в виде

$$\mathrm{supp}\varphi_0(k) \in \{\Delta k\}_0$$

и

$$\mathrm{supp}\varphi_1(k) \in \{\Delta k\}_1.$$

Частотные полосы информационных состояний не перекрываются:

$$\{\Delta k\}_0 \bigcap \{\Delta k\}_1 = \emptyset,$$

при этом векторы состояний автоматически ортогональны:

$$\langle\varphi_0|\varphi_1\rangle = \int\limits_{\{\Delta k\}_0 \bigcap \{\Delta k\}_1} dk\varphi_0^*(k)\varphi_1(k) =$$

$$= \int\limits_{-\infty}^{\infty}\int\limits_{-\infty}^{\infty} d\tau d\tau' \varphi_0^*(\tau)\varphi_1(\tau')\left[\frac{1}{2}\delta(\tau-\tau') + \frac{i}{\pi}\frac{1}{\tau-\tau'}\right] =$$

$$= \int\limits_{-\infty}^{\infty} d\tau\, \varphi_0^*(\tau)\varphi_1(\tau) = 0, \quad (32)$$

где использовано интегральное представление обобщенной функции [20]

$$\int\limits_{-\infty}^{\infty} dx \exp(ik(x-t))\frac{1}{x-t+a} =$$

$$= i\pi\ \mathrm{sgn}(k)\exp(-ika). \quad (33)$$

Видно, что ортогональность состояний является нелокальным свойством в пространстве-времени в том смысле, что если фиксировано время t^* в $\tau = x - t^*$, то ортогональность «набирается» в большой (формально — бесконечно большой, см. ниже) пространственной области. Если же фиксирована координата x^* в $\tau = x^* - t$, то ортогональность «набирается» за счет большого промежутка времени. Далее данным соображениям будет придан операциональный смысл. Различимость ортогональных квантовых состояний при помощи измерений будет неизбежно требовать либо конечной области пространства (при фиксированном временном срезе), либо конечного времени (при фиксированной пространственной переменной).

Строго говоря, точная ортогональность и, соответственно, достоверный исход измерений требует формально бесконечной пространственно-временной области в силу принципиальной нелокализуемости состояний в квантовой теории поля.

По сути, 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). Факт нелокализуемости состояний в квантовой теории поля известен давно (см. физическое обсуждение данного вопроса, например, в [21]). В данном случае нелокализуемость может быть явно продемонстрирована как следствие теоремы Винера–Пэли [22]. Для нормированной функции $\varphi(k)$, такой что

$$\int\limits_0^{\infty} dk|\varphi(k)|^2 = 1, \quad (34)$$

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

$$\int\limits_{-\infty}^{\infty} \frac{\ln|\varphi(\tau)|}{1+\tau^2} d\tau < \infty. \quad (35)$$

Откуда 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 $\varphi(\tau)| \propto \exp(-\alpha|\tau|)$, то интеграл (35) расходится. Однако амплитуда может убывать сколь угодно близко к экспоненте с любым показателем $\alpha > 0$, т. е.

$$|\varphi(\tau)| \propto \exp\left(-\frac{\alpha|\tau|}{\ln(\ln\ldots|\tau|)}\right).$$

Подобной степени локализации фотонного поля можно добиться и в трехмерном случае [23], хотя долгое время после работы Ньютона и Вигнера считалось, что наиболее быстрое убывание в пространстве может быть лишь степенным со степенью $7/2$ [24].

Нелокализуемость амплитуды (отличие от нуля вне любого компакта) имеет глубокие корни, связанные с причинностью в релятивистской квантовой области. Например, как было показано Хегерфельдом [25], 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 релятивистской причинностью,

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. В недавней работе Бома и др. [26] было показано, что принцип причинности восстанавливается для распадных процессов в релятивистской области для средних значений наблюдаемых.

Грубо говоря, состояние свободного квантованного поля отлично от нуля везде и всегда, т. е. во всем пространстве-времени (см., например, (35)).

Принцип причинности в релятивистской квантовой области был впервые сформулирован в конечной форме Боголюбовым в 1955 г. [16]. В дифференциальной форме он выглядит как

$$\frac{\delta S^{+}(g(\hat{x}))}{\delta g(\hat{x})} S(g(\hat{y})) = 0, \quad \hat{x} < \hat{y}. \tag{36}$$

Это означает, что если состояние возмущено в некоторой области, где включено взаимодействие $g(\hat{x})$, то это не может сказаться на результатах измерений в областях $\hat{y}$, разделенных с данной пространственно-подобным интервалом.

Далее от принципа причинности нам потребуется то, что нельзя получить информацию о квантовом состоянии в некоторой пространственно-временной области до тех пор, пока состояние не достигнет этой области. Причем никакое состояние не может войти (или выйти) в область быстрее, чем со скоростью света. Более точно, нельзя получить конечную информацию, отличающуюся от нуля больше, чем на экспоненциально малую величину. Кроме того, чем меньшая доля состояния присутствует в области, доступной для измерений, тем меньше вероятность получения любого результата измерений. Это следует, по сути, из нормировки квантового состояния.

Тот факт, что амплитуда состояния отлична от нуля во всем пространстве, не является ограничительным для задач квантовой криптографии, поскольку всегда можно выбрать актуальную пространственно-временную область таких размеров, чтобы вне этой области доля нормировки амплитуды, набираемая вне этой области, была бы с любой наперед заданной точностью экспоненциально близка к нулю. Хотя сам по себе факт строгой нелокализуемости амплитуды и обусловлен принципиальными требованиями причинности, тем не менее, в конкретных задачах такая нелокализуемость носит скорее чисто технической характер. Сейчас мы придадим данным рассуждениям более операциональный смысл.

Пусть амплитуда состояния в импульсном представлении задана в конечной частотной полосе Δk, которая может быть произвольной ($\Delta k \in (0, \infty)$). Сейчас нас будет интересовать вопрос о том, как зависит вероятность обнаружения фотона внутри пространственно-временной области размером $2T$ при фиксированной частотной полосе от формы амплитуды состояния. Эти заготовки потребуются в дальнейшем при формулировке протокола генерации секретного ключа, поскольку форма амплитуды будет накладывать условия на необходимый размер пространственно-временной области, чтобы детектировать попытки подслушивания по задержке результатов измерений.

Любые измерения над квантовым состоянием описываются некоторым разбиением единицы в одночастичном подпространстве состояний

$$I = \int\limits_0^\infty \frac{dk}{k} |k\rangle\langle k| = \int\limits_{-\infty}^{\infty} \mathcal{M}(d\tau), \tag{37}$$

операторно-значная мера $\mathcal{M}(d\tau)$,

$$\mathcal{M}(d\tau) = \frac{d\tau}{2\pi} \left(\int\limits_0^\infty \frac{dk}{\sqrt{k}} \exp(-ik\tau)|k\rangle \right) \times \times \left(\int\limits_0^\infty \frac{dk'}{\sqrt{k'}} \exp(ik'\tau)\langle k'| \right) \tag{38}$$

описывает вероятность обнаружения фотона в интервале $(\tau, \tau + d\tau)$. Соответственно вероятность обнаружения фотона в конечной пространственно-временной области T (напомним, что амплитуда зависит лишь от разности $\tau = x - t$) есть

$$\Pr(T) = \mathrm{Tr}\{\mathcal{M}(T)|\varphi\rangle\langle\varphi|\} = \int\limits_{-T} T\, d\tau |\varphi(\tau)|^2, \tag{39}$$

где

$$\mathcal{M}(T) = \int\limits_{-T} T\mathcal{M}(d\tau), \quad \mathcal{M}(\overline{T}) = \int\limits_{\overline{T}} \mathcal{M}(d\tau), \quad \overline{T} = (-\infty, \infty) \setminus (-T, T). \tag{40}$$

Вероятность обнаружения вне области $(-T, T)$ (в остальной части пространства-времени) равна

$$\Pr(\overline{T}) = \mathrm{Tr}\{\mathcal{M}(\overline{T})|\varphi\rangle\langle\varphi|\} = 1 - \int\limits_T d\tau |\varphi(\tau)|^2. \tag{41}$$

Поскольку амплитуда зависит лишь от разности $\tau = x - t$, данные выражения можно интерпретировать следующим образом: во-первых, как вероятность обнаружения фотона в области координатного пространства размером $\Delta x = 2T$ в некоторый фиксированный момент времени или, во-вторых, как вероятность обнаружения его в окрестности фиксированной точки x в течение времени $\Delta t = 2T$ (смысл этого будет уточнен ниже).

Максимально возможная вероятность обнаружения однофотонного пакета в интервале T дается выражением

$$\Pr_{max}(T) = \max_{\{\|\varphi\|^2=1\}} \mathrm{Tr}\{\mathcal{M}(T)|\varphi\rangle\langle\varphi|\}, \qquad (42)$$

где максимум берется по всем формам пакетов $\varphi(k)$, носители которых лежат в частотной полосе Δk. Оптимальная форма находится из решения вариационной задачи на максимум функционала

$$\frac{\delta}{\delta\varphi}\left\{\frac{\mathrm{Tr}\{\mathcal{M}(T)|\varphi\rangle\langle\varphi|\}}{\int\limits_{\Delta k}|\varphi(k)|^2 dk}\right\} = 0, \qquad (43)$$

что приводит к решению задачи на собственные значения

$$\lambda_n\varphi_n(k) = \frac{1}{\pi}\int\limits_{\Delta k}\frac{\sin(k-k')T}{k-k'}\varphi_n(k')\,dk'. \qquad (44)$$

Наибольшее собственное число дает максимум функционала, а собственная функция этого собственного числа дает оптимальную форму состояния. Данное уравнение исследовалось ранее в работах [27, 28], собственные числа уравнения положительны и образуют убывающую последовательность с ростом номера n ($1 > \lambda_0 > \lambda_1 \ldots > 0$, $n = 0, 1, \ldots \infty$). 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 [27] (при больших значениях параметра $\Delta k \cdot T$ они быстро стремятся к 1, например, при $\Delta k \cdot T = 4$, $\lambda_0 = 0.99589$). Известна также асимптотика при фиксированном номере n от параметра $\Delta k \cdot T \gg 1$ [28]:

$$\lambda_n(\zeta) \sim 1 - \frac{4\sqrt{\pi}8^n}{n!}\zeta^{n+1/2}e^{-2\zeta}, \quad \zeta = \Delta k \cdot T, \qquad (45)$$

т. е. собственные числа экспоненциально близки к единице.

Таким образом, вероятность любого измерения при размере пространственной области (или временного интервала) $2T$ для состояния с носителем в частотной полосе Δk не может быть больше, чем

$$\Pr_{max}(T) \le 1 - O\left(\exp(-2\Delta k \cdot T)\right). \qquad (46)$$

Таким образом, выбирая размер области (или интервал времени), можно добиться того, что вероятность детектирования вне данного интервала будет сколь угодно мала. Например, вероятность 10^{-80} можно считать нулем, поскольку она меньше любой физически осмысленной величины (напомним, что число атомов в видимой части вселенной оценивается как 10^{80}). Поэтому факт нелокализуемости состояний в квантовой теории поля не является ограничивающим обстоятельством, поскольку всегда можно выбрать размер области (или временное окно) измерения, в которую состояние «вмещается» с экспоненциальной точностью целиком.

Применительно к задачам квантовой криптографии выбор интервала необходимого размера будет гарантировать, что подслушиватель будет иметь лишь экспоненциально малую информацию о передаваемом состоянии вне этой области (или временного интервала). Порядок величины интервала равен $2T$. Соответственно попытки подслушивания будут детектироваться легитимным пользователем на приемном конце за счет событий вне данного интервала (см. детали ниже).

Пусть имеется пара однофотонных состояний (пакеты), каждый с частотной полосой Δk, и пусть частотные полосы не перекрываются — состояния ортогональны и, значит, достоверно различимы. Однако сам по себе факт достоверной различимости подразумевает, что состояния должны быть доступны целиком, поскольку измерения, различающие данную пару состояний, требуют доступа к той области пространства, где состояние присутствует (в противном случае нечего измерять).

Покажем теперь, что если в канал связи посылается одно из ортогональных состояний ($|\varphi_0\rangle$ или $|\varphi_1\rangle$) каждое с частотной полосой Δk и частотные полосы не перекрываются, то извлечение любой информации о передаваемом состоянии с вероятностью, превышающей экспоненциально малую величину $O\left(\exp(-2\Delta k \cdot T)\right)$, будет приводить к неизбежной задержке результатов измерений у легитимного пользователя. По этой задержке детектируются попытки подслушивания.

Любая передача информации при помощи как квантовых, так и классических объектов подразумевает наличие трех стадий, связанных между со-

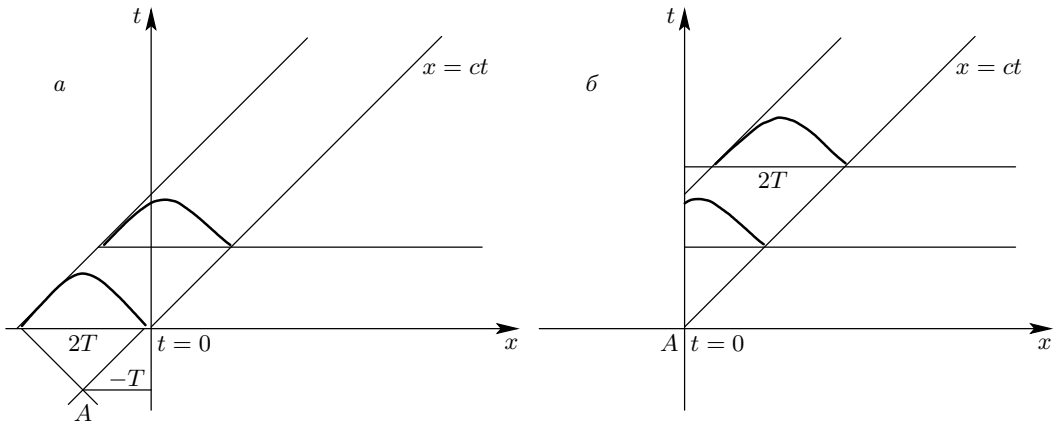

Рис. 1.

бой причинно-следственной связью: 1) приготовление носителя информации — квантового состояния, 2) распространение его через канал связи, 3) измерения на приемном конце с целью извлечения информации.

Пусть в начале протокола $t = 0$, момент известный всем, в том числе и подслушивателю, участник A приготавливает одно из состояний ($|\varphi_0\rangle$ или $|\varphi_1\rangle$) в контролируемой им пространственно-временной области размером $2T$. В такой области состояния могут быть приготовлены с положительным исходом с вероятностью $1 - O\left(\exp(-2\Delta k \cdot T)\right)$ (факт неудачного исхода — не приготовления состояния — не опасен для секретности ключа). Имеются две формально эквивалентные возможности. Участник A приготавливает состояние распределенным в пространстве устройством в момент $t = 0$ сразу во всей пространственной области размером $\Delta x = 2T$ (рис. 1*а*). В случае распределенного прибора[2)], участник A принимает решение в момент $t = -T$ о том, какое состояние 0 или 1, он будет готовить. Само состояние возникает в момент $t = 0$ сразу во всей пространственной области ($x < 0$, область $x > 0$ — область канала связи). Далее при $t > 0$ состояние начинает распространяться в канале связи. Другими словами, приготовление состояния распределенным прибором означает, что пространственная область $2T$ из-за требований причинности (рис. 1*а*) должна накрываться передней частью светового конуса с вершиной у наблюдателя A.

[2)] Пример распределенного прибора приведен в разд. 6. Прибор представляет собой призму и апертуры, помещенные на расстоянии $2T$ от призмы. Распределенность понимается в том смысле, что прибор как целое занимает пространственную область размером $2T$.

Хотя нет никаких формальных запретов на приготовление амплитуды состояния в момент $t = 0$ сразу во всей области пространства размером $2T$, однако в реальной ситуации более удобна процедура приготовления, разумеется, эквивалентная предыдущей, при помощи локализованного источника. Локализованность понимается в том смысле, что размеры источника $\delta x_{source} \ll T$, рис. 1*б*). Из локализованного источника состояние сразу начинает распространяться в канал связи.

Перейдем теперь к вопросу об извлечении информации в канале связи подслушивателем. По истечении времени $2T$ состояние оказывается с вероятностью, экспоненциально близкой к единице, целиком в канале. Эволюция состояния в канале описывается унитарным оператором трансляции, который имеет вид

$$U(\tau_0) = \int\limits_0^\infty \frac{dk}{k} \exp(ik\tau_0)|k\rangle\langle k| = \int\limits_{-\infty}^{\infty} |\tau + \tau_0\rangle\langle\tau| d\tau, \quad (47)$$

где τ_0 — величина трансляции в пространстве-времени. Состояние в момент времени $t > T$ представляется как

$$|\varphi_i\rangle = \int\limits_{\Delta k} dk \exp(-ik(x - t - T))\varphi_i(k)|k\rangle = \int\limits_{-\infty}^{\infty} dx \varphi_i(x - t - T)|x - t\rangle. \quad (48)$$

Покажем теперь, что любое получение не экспоненциально малой информации подслушивателем

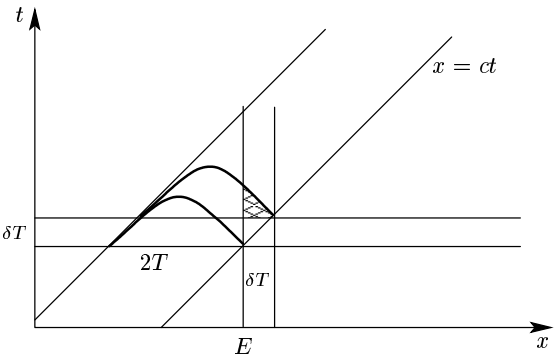

Рис. 2. Заштрихованная часть состояния позволяет подслушивателю извлечь информацию за счет доли нормировки состояния, которая набирается в этой области. Однако при этом неизбежна задержка на δT, поскольку без подслушивателя состояние успело бы распространиться на δT

приводит к детектируемой задержке на приемном конце.

Чтобы получить любую информацию о состоянии, необходимо иметь доступ к той части пространства, где отлична от нуля амплитуда состояния. Вернемся к доказательству Беннета [11]. Как следует из (3)–(9), нет запрета на то, чтобы различить ортогональные состояния без их возмущения. Однако при этом неявно используется тот факт, что состояния должны быть доступны целиком. Доступ к состоянию целиком не может быть получен быстрее, чем за время $2T$ (рис. 2). Очевидно, что (см. рис. 2), например, в область $x \geq x_E$ состояние не может войти быстрее, чем за время распространения $2T$. Причем этот факт диктуется лишь наличием предельной скорости распространения. Тот факт, что состояние является квантовым, пока не используется. Напомним, что подслушиватель знает момент приготовления состояния, т. е. то время, когда состояние целиком (с экспоненциальной точностью) окажется в канале.

Квантовая природа состояния важна для следующего. Вероятность получения любого результата измерений в некоторой пространственно-временной области не может быть больше, чем доля нормировки состояния, которая набирается в этой области. Получение любого результата измерения (независимо от того, ортогональны или неортогональны состояния) требует конечного времени (рис. 2). «Собирание» состояния в некоторой локальной области неизбежно приводит к задержке, поскольку, если бы не было «собирания» состояния, то исходное состояние успело бы уже распространиться дальше (рис. 2). Чем больше подслушиватель получает информации о состоянии, чем большую долю нормировки он собирает, тем к большей задержке это приводит. Поскольку амплитуда зависит лишь от разности $x - t$, можно провести рассуждения, фиксируя время и считая переменной координату, либо наоборот. Сделаем это для обоих случаев.

Пусть задано состояние с амплитудой $\varphi(x - t)$ (напомним, что это амплитуда безмассовой частицы, распространяющейся со скоростью света, $c = 1$). Пусть состояние сосредоточено в области $2T$, в том смысле, что

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

$\varphi(x - t_0)$ — амплитуда на временном срезе t_0. Чтобы иметь результат любого измерения с вероятностью, сколь угодно близкой к единице, требуются сразу все значения амплитуды состояния при всех x, которые имеет амплитуда в момент t_0 в той области, где она отлична от нуля, поскольку есть нормировка квантового состояния. Последнее может быть достигнуто посредством унитарного преобразования сразу над всем состоянием. В противном случае такое преобразование не будет унитарным. Унитарное преобразование над амплитудой состояния записывается в виде

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

Амплитуда $\tilde{\varphi}(x' - t)$ может быть отлична от нуля уже в меньшей пространственной области. Минимальный размер области по x' к моменту t диктуется релятивистским принципом причинности. 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 T, амплитуда исходного состояния может быть унитарным образом преобразована в состояние со сколь угодно сильно локализованной амплитудой в окрестности Г. Но это уже будет другое состояние. К моменту Г доступны значения амплитуды состояния при всех x. Теперь можно мгновенно получить исход измерения и иметь полную (с вероятностью единица) информацию о состоянии. Если пара исходных состояний была ортогональна, то можно унитарным преобразованием получить также пару ортогональных состояний к моменту Г и соответственно достоверно отличить одно от другого.

Подчеркну еще раз, что это будут уже другие ортогональные состояния. «Восстановление» или копирование состояния также может быть реализовано обратным унитарным преобразованием, «направленным» вперед во времени. Состояние с той же формой амплитуды может быть получено к моменту не ранее, чем это также диктуется релятивистской причинностью, и амплитуда его находится в передней части светового конуса, выпущенного из Г. Новое 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 $2T$ как раз на величину $2T$, если бы не было попыток получения информации о нем. Пока речь шла о получении информации о состоянии в канале с вероятностью единица (при этом подслушиватель с вероятностью единица не пройдет временной тест на задержку). Те же самые рассуждения годятся для получения информации с вероятностью меньшей единицы. Задержка при этом будет меньше $2T$.

Аналогичные рассуждения работают и в нерелятивистском случае. Если игнорировать ограничения специальной теории относительности, то из рассмотрений нужно выбросить ту часть, которая апеллирует к световому конусу. При этом унитарные преобразования можно делать формально мгновенно и из рассмотрения даже можно исключить явное присутствие координаты, оставив неявно только то, что при унитарном преобразовании состояние доступно целиком.

Аналогично можно провести рассуждения, когда состояние унитарным образом преобразуется в состояние вспомогательной локализованной системы (как правило, атомной, как это имеет место при «остановке» света [40]). Такое унитарное преобразование переводит состояние поля в вакуумное состояние из-за 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 со скоростью света пакета и достижения локализованной атомной системы. Данный процесс, если речь идет о получении результата с вероятностью единица, также требует времени $2T$ (однофотонный пакет целиком достигает атомной системы). При этом поле оказывается в другом — вакуумном состоянии. К моменту времени $2T$ с вероятностью единица можно выяснить, что это за состояние, и приготовить такое же, но с неизбежной задержкой на $2T$, которая будет иметь место по сравнению со свободным распространением исходного пакета.

Ситуация, когда состояние проходит как бы насквозь через вспомогательную локализованную квантовую систему и локально в каждый момент времени взаимодействует с ней локально (аналогично (3)–(9)), неизбежно приводит к возмущению исходного состояния.

Покажем это на простом примере. Локальность взаимодействия означает также неполную доступность гильбертова пространства состояний. Пусть исходное состояние

$$|\varphi\rangle = c_0|e_0\rangle + c_1|e_1\rangle, \quad \langle e_0|e_1\rangle, \tag{49}$$

где $|e_{0,1}\rangle$ — базисные векторы. Пусть $|a\rangle$ — локальная вспомогательная система. Пусть совместная унитарная эволюция имеет вид

$$|\varphi\rangle \to U(|\varphi\rangle \otimes |a\rangle) = \\ = c_0 U(|e_0\rangle \otimes |a\rangle) + c_1|e\rangle \otimes |a\rangle. \tag{50}$$

Локальность взаимодействия означает, что унитарное преобразование затрагивает лишь доступные базисные векторы ($|e_0\rangle$). Пусть в результате эволюции вспомогательная система переходит в новое состояние $|a'\rangle$. Пусть также для простоты $\langle a'|a\rangle = 0$, хотя это не принципиально. Состояние составной системы в результате эволюции имеет вид

$$|\Psi\rangle = U(|\varphi\rangle \otimes |a\rangle) = c_0 U(|e_0\rangle \otimes |a\rangle) + c_1|e\rangle \otimes |a\rangle = \\ = c_0|e_0\rangle \otimes |a'\rangle + c_1|e\rangle \otimes |a\rangle. \tag{51}$$

Тогда новое состояние исходной системы вычисляется как частичный след, взятый по степеням свободы вспомогательной системы:

$$|\tilde{\varphi}\rangle\langle\tilde{\varphi}| = \mathrm{Tr}_a\{|\Psi\rangle\langle\Psi|\} = \\ = |c_0|^2|e_0\rangle\langle e_0| + |c_1|^2|e_1\rangle\langle e_1|, \tag{52}$$

что отнюдь не то же самое, что состояние исходной системы до локального взаимодействия со вспомогательной системой:

$$|\varphi\rangle\langle\varphi| = (c_0|e_0\rangle + c_1|e_1\rangle)(c_0^*\langle e_0| + c_1^*\langle e_1|). \tag{53}$$

Обсудим теперь более детально измерения на приемном конце, позволяющие детектировать задержку. Сначала опишем их формально, а затем приведем их техническую реализацию. Оказывается, что такие измерения достаточно просто реализуются при помощи фильтров с полосой пропускания Δk и обычного фотодетектора (см. детали ниже).

Измерение на приемном конце описывается следующим разбиением единицы:

$$I(\Delta k) = \int\limits_{(\Delta k)_0} \frac{dk}{k}|k\rangle\langle k| + \int\limits_{(\Delta k)_1} \frac{dk}{k}|k\rangle\langle k| = \\ = \int\limits_{-\infty}^{\infty} \mathcal{M}(d\tau) = \int\limits_{-\infty}^{\infty} \mathcal{M}_0(d\tau) + \int\limits_{-\infty}^{\infty} \mathcal{M}_1(d\tau), \quad (54)$$

где $\mathcal{M}_i(d\tau)$, $i = 0, 1$ — операторно-значная мера:

$$\mathcal{M}_i(d\tau) = \frac{d\tau}{2\pi}\left(\int\limits_{\Delta k_i} \frac{dk}{\sqrt{k}}\exp(-ik\tau)|k\rangle\right) \times \\ \times \left(\int\limits_{\Delta k_i} \frac{dk'}{\sqrt{k'}}\exp(ik'\tau)\langle k'|\right). \quad (55)$$

Измерение устроено таким образом, что оно «пропускает» только те состояния, частотная полоса которых лежит в интервале $\{\Delta k\}_0$ или в $\{\Delta k\}_1$ (ширины полос считаем одинаковыми, различаются только их положения по оси частот). Или, другими словами, только те состояния, эффективная пространственно-временная протяженность которых не менее T. Вероятность получения результата на приемном конце на состоянии $|\varphi_0\rangle$ исхода, отвечающего 0 во временном окне $(L_{ch}, L_{ch} + 2T)$ (интервал, в котором с вероятностью экспоненциально близкой к единице оказывается состояние, если не было задержки), равна

$$\Pr(i, T) = \mathrm{Tr}\{\mathcal{M}_i(T)U(L_{ch})|\varphi_i\rangle\langle\varphi_i|U^{-1}(L_{ch})\} = \\ = \int\limits_{L_{ch}}^{L_{ch}+2T} d\tau|\varphi_i(\tau)|^2 = \\ = \lambda_0(2\Delta k \cdot T) = 1 - O\left(\exp(-2\Delta k \cdot T)\right), \quad (56)$$

унитарный оператор $U(L_{ch})$ описывает трансляцию состояния на длину канала связи. Вероятность обнаружения состояний вне временного окна экспоненциально мала.

Поскольку все измерения подслушивателя происходят в канале связи и дают информацию только тогда, когда состояние присутствует в нем, в данной схеме криптографии снимается проблема коллективных измерений, которая возникает в нерелятивистской квантовой криптографии, где все протоколы формулируются лишь в гильбертовом пространстве состояний (т. е. вне пространства-времени). Поэтому ключевой величиной в каждом акте передачи квантового состояния через канал связи является вероятность узнать передаваемый участником A бит и пройти тест при измерениях (54)–(56) у участника B на приемном конце. Тест считается пройденным, если измерения (54)–(56) дают исход внутри временного окна $(L_{ch}, L_{ch}+2T)$. Отметим, что при дальнейшей генерации ключа оставляются только те посылки, которые дали исход у B в этом окне. Разумеется, что подслушиватель может посылать заранее произвольно состояния, которые дадут исход у B в нужном временном окне. Это вылавливается уже при помощи протокола, когда часть посылок раскрывается, чтобы выяснить поток ошибок.

Вероятность того, что подслушиватель имеет хоть какую-то информацию о передаваемом состоянии, ограничена лишь величиной доступа к пространственной области, где состояние присутствует. Если подслушиватель хочет иметь доступ к области размером δT (пространственной или временной), то вероятность исхода любого измерения диктуется лишь размером этой области, и в силу условия нормировки состояния не может быть больше, чем

$$\Pr_E(\delta T) = \mathrm{Tr}\{\mathcal{M}(\delta T)|\varphi_i\rangle\langle\varphi_i|\} = \\ = \int\limits_{T-\delta T}^{T} d\tau|\varphi_i(\tau)|^2, \quad (57) \\ \delta T \in (-T, T).$$

Полная вероятность правильной идентификации состояния (без учета прохождения временного теста на приемном конце) складывается из двух частей. Если имела место регистрация состояния в области пространства-времени размером δT, то состояние идентифицируется однозначно (из-за ортогональности). Вероятность такого события равна $\Pr_E(\delta T)$ (57). Вероятность, когда никакой регистрации не было, есть $1 - \Pr_E(\delta T)$, при этом вероятность правильной идентификации состояния равна $1/2$, т. е. равна вероятности простого угадывания, поскольку не было никакой регистрации (прибор у подслушивателя не сработал).

Полная вероятность правильной идентификации во временном окне δT равна

$$\Pr_{OK}(\delta T) = 1 \cdot \Pr_E(\delta T) + \frac{1}{2} \cdot (1 - \Pr_E(\delta T)) = \\ = \frac{1}{2}(1 + \Pr_E(\delta T)) > \frac{1}{2}. \quad (58)$$

Из-за конечности скорости света доступ к области δT неизбежно приведет к задержке измерений во временном окне $(L_{ch}, L_{ch} + 2T)$ на приемном конце (рис. 3), поскольку измерения устроены таким образом, что не пропускают состояния с эффективной

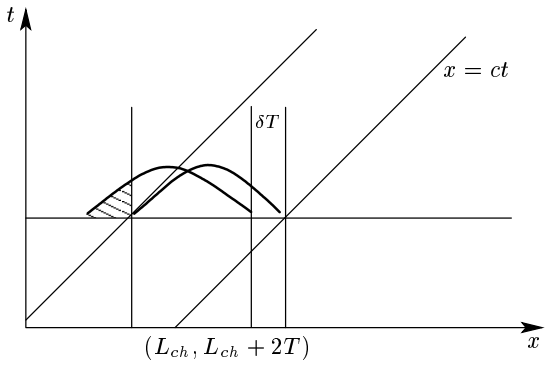

Рис. 3. Заштрихованная часть задержанного состояния не дает вклада в исходы измерений во временном окне $(L_{ch}, L_{ch}+2T)$ на приемном конце

протяженностью меньшей, чем $2T$ (соответственно, с частотной полосой, большей чем Δk). Более точно, операторная мера $\mathcal{M}(d\tau)$ (54), (55), описывающая измерение, содержит проектор на подпространство состояний лишь с носителями внутри частотной полосы Δk, а среди таких состояний наиболее короткими являются оптимальные состояния (44)–(46). Иначе говоря, любые другие состояния, даже без задержки, как более протяженные просто не вмещаются во временное (или пространственное окно) $(-T, T)$ с вероятностью большей, чем оптимальные состояния. Оптимальные состояния, если подслушиватель извлекает из них информацию о передаваемом бите, из-за неизбежной задержки (рис. 3), диктуемой наличием предельной скорости, также будут давать исходы вне временного окна $(L_{ch}, L_{ch}+2T)$ на приемном конце. Вероятность задержанному на δT состоянию пройти тест у B не превосходит величины

$$\begin{aligned}\mathrm{Pr}_B(\delta T) &= \mathrm{Tr}\{\mathcal{M}(\tau\in(L_{ch},L_{ch}+2T))U(L_{ch})\times\\ &\quad\times|\varphi_i\rangle\langle\varphi_i|U^{-1}(L_{ch})\}=\\ &=\int\limits_{L_{ch}}^{L_{ch}+2T}d\tau|\varphi(L_{ch}+\tau-\delta T)|^2=\\ &=\int\limits_{-T}^{T-\delta T}d\tau|\varphi(\tau)|^2. \quad (59)\end{aligned}$$

Вероятность пройти временной тест на приемном конце при задержке δT, и при условии, что регистрирующий прибор сработал (подслушиватель при этом знает передаваемое состояние), равна

$$\mathrm{Pr}_E(\delta T)\mathrm{Pr}_B(\delta T)=\mathrm{Pr}_E(\delta T)(1-\mathrm{Pr}_E(\delta T)). \quad (60)$$

Если задержка $\delta T=0$, то первый сомножитель, описывающий вероятность получения результата у подслушивателя, равен 0. Второй сомножитель описывает вероятность пройти тест на приемном конце. Если задержка $\delta T=2T$, то вероятность получения исхода у подслушивателя равна единице (экспоненциально близка к единице), но при этом вероятность пройти тест равна нулю.

Полная вероятность правильно идентифицировать передаваемое состояние и пройти тест на временную задержку на приемном конце есть

$$\begin{aligned}\delta_{OK}(\delta T)&=\mathrm{Pr}\{\mathrm{bit}_E=\\ &=\mathrm{bit}_A\wedge\mathrm{test}(\tau\in(L_{ch},L_{ch}+2T))=O'K\}=\\ &=(1-\mathrm{Pr}_E(\delta T))\cdot\frac{1}{2}\cdot1+\\ &\quad+\mathrm{Pr}_E(\delta T)\cdot1\cdot(1-\mathrm{Pr}_E(\delta T)). \quad (61)\end{aligned}$$

Первый сомножитель в первом слагаемом описывает вероятность того, что при заданной задержке δT прибор у подслушивателя не сработает, второй сомножитель дает вероятность правильной идентификации при отсутствии регистрации, равную $1/2$, третий — вероятность пройти тест на временную задержку. Эта вероятность равна единице, поскольку при отсутствии срабатывания детектора, состояние проходит «насквозь» через подслушивателя и без взаимодействия с его приборами. Аналогично для второго слагаемого. Первый сомножитель есть вероятность срабатывания регистрирующего прибора в один из каналов (0 или 1). При этом вероятность идентификации равна 1 (состояния ортогональны). Третий сомножитель — вероятность пройти тест на временную задержку.

Величина $\delta_{OK}(\delta T)$ достигает максимального значения при некотором δT. Обозначим это максимальное значение δ_{OK}^{max}. Для дальнейшего нам будет нужна минимальная величина ошибки подслушивателя δ_E о передаваемом бите при условии прохождения временного теста. Только такие исходы на приемном конце у B будут использованы в протоколе при создании секретного ключа. Пусть

$$\delta_E=1-\delta_{OK}^{max}. \quad (62)$$

Максимальная вероятность для подслушивателя узнать передаваемый бит и пройти тест достигается при $\mathrm{Pr}_E(\delta T)=1/4$. Тогда имеем

$$\delta_E=\frac{7}{16}=\frac{1}{2}-0.0625=43.75\,\%. \quad (63)$$

Соответственно, вероятность правильной идентификации состояния для подслушивателя о передавае-

мом бите участником A и одновременно пройти тест на приемном конце у участника B равна

$$\delta_{OK}^{max} = \frac{9}{16} = \frac{1}{2} + 0.0625 = 56.25\,\%. \qquad (64)$$

Покажем теперь, что в канале с шумом вероятность детектирования в любом временном окне не может превышать соответствующего значения в идеальном канале. Это будет означать, что величина (61) есть максимум того, на что может рассчитывать подслушиватель в смысле извлечения информации. Шум в канале не может увеличить извлекаемую подслушивателем информацию и увеличить вероятность прохождения теста.

Поскольку состояния в релятивистском случае описываются векторами в гильбертовом пространстве состояний, изменение состояния под действием шума может быть описано при помощи инструмента с учетом релятивистских ограничений на него. Общий вид инструмента есть [29]

$$\mathcal{T}[\dots] = \sum_k \mathcal{S}_k[\dots]\mathcal{S}_k^+, \quad \mathcal{S}_k = \sqrt{\lambda_k}|\phi_k\rangle\langle\psi_k|,$$
$$\sum_k \lambda_k \mathcal{S}_k \mathcal{S}_k^+ \le 1, \quad \lambda_k \ge 0, \qquad (65)$$

$$\begin{aligned}
&\mathrm{Tr}\{\mathcal{T}\ [|\varphi_{0,1}\rangle\langle\varphi_{0,1}|]\mathcal{M}(T)\} = \\
&\quad = \sum_k \mathrm{Tr}\{|\varphi_{0,1}\rangle\langle\varphi_{0,1}|(\mathcal{S}_k\mathcal{M}(T)\mathcal{S}_k^+)\} \le \\
&\quad \le \sum_k \lambda_k \mathrm{Tr}\{|\varphi_{0,1}\rangle\langle\varphi_{0,1}|(|\psi_k\rangle\langle\psi_k|)\} \le \\
&\le \sum_k \lambda_k |\langle\psi_k|\varphi_{0,1}\rangle|^2 \le \sum_k \lambda_k \langle\psi_k|\psi_k\rangle\langle\varphi_{0,1}|\varphi_{0,1}\rangle \le \\
&\quad \le \langle\varphi_{0,1}|\varphi_{0,1}\rangle = \int\limits_T dx\Big|\varphi(x)\Big|^2 = \\
&\quad = \int\limits_T dx\Big|\varphi(x-L_{ch})\Big|^2. \qquad (66)
\end{aligned}$$

Последнее равенство в (66) выражает тот факт, что амплитуда $\varphi(x)$ состояния

$$|\varphi_{0,1}\rangle = \int\limits_T dx\,\varphi(x)|x\rangle = \int\limits_T dx\,\varphi(x-L_{ch})|x\rangle \qquad (67)$$

в момент времени $t = 0$ целиком локализована в области $x \in (-T, T)$ и будет целиком локализована в области $x \in (-T, T) + L_{ch}$ в момент времени не более ранний, чем L_{ch}, который не может быть быстрее, чем $t = \mathrm{dist}\,(L_{ch})$. Строго говоря, в теории поля задача не является одночастичной в том смысле, что оператор $\hat{S}$ содержит процессы с рождением частиц и

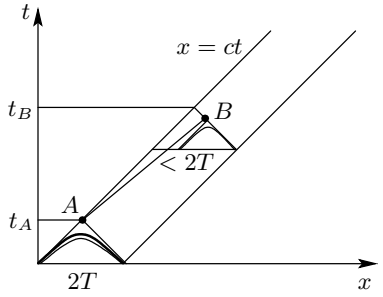

Рис. 4. Иллюстрация нарушения принципа релятивистской причинности. Гипотетическое сжатие состояния приводит к возможности передачи информации быстрее скорости света между A и B, поскольку эти точки разделены пространственно-подобным интервалом

поглощением других фотонов, попадающих в канал со стороны как шум или исчезающих в нем. Однако детектирование этих сторонних фотонов, очевидно, не дает подслушивателю дополнительной информации о передаваемом бите.

Другими словами, если в некоторой области пространства размером Ω набирается некоторая доля нормировки состояния, то в результате распространения и искажения формы состояния (пакета) не может возникнуть ситуация, когда в некоторой другой области пространства меньшего размера, $\mathrm{size}\{\Omega'\} < \mathrm{size}\{\Omega\}$, набиралась бы бóльшая величина нормировки. Если бы такое было возможно, то это позволяло бы передавать классическую информацию при помощи квантовых состояний быстрее скорости света, что противоречит одному из основных законов физики.

Действительно (см. рис. 4), пусть когда-то в прошлом была приготовлена пара одинаковых квантовых состояний. Пусть наблюдатель A проводит измерения только над одним из пары квантовых состояний, второе состояние распространяется к наблюдателю B. Наблюдатель A может получить информацию о квантовом состоянии в момент времени не раньше, чем t_A (состояние должно накрываться прошлой частью светового конуса, выпущенного из точки A). Всегда будут события, хотя и не с единичной вероятностью из-за принципиальной нелокализуемости квантового состояния, когда будет иметь место результат измерения у A. Когда результат имел место, участник A может послать классический (или сколь угодно сильно локализованный квантовый, см. (44)–(46)) сигнал участнику B. Согласно релятивистскому принципу причинности, участник B мо-

жет получить информацию не раньше, чем в момент t_B (рис. 4), и никогда не может получить ее в более ранние моменты, поскольку такие события будут разделены пространственно-подобным интервалом.

Пусть теперь состояние в результате эволюции и шума исказилось таким образом, что бóльшая величина нормировки набирается в меньшей пространственной области (состояние сжалось). Тогда участник B с той же самой вероятностью положительного исхода, что и у наблюдателя A, может получить информацию путем измерений над вторым квантовым состоянием раньше, чем он получил бы ту же самую информацию от A. В итоге участник B будет иметь информацию из измерений над вторым квантовым состоянием раньше, чем он мог бы получить ее от участника A в результате его измерений. Тот факт, что такие события не будут иметь место с единичной вероятностью, не важен, поскольку, используя не два, а большее число квантовых состояний, можно добиться вероятности, сколь угодно близкой к единице.

Таким образом, величина вероятности (61) получить какую бы ни было информацию о квантовом состоянии и пройти тест на временную задержку всегда меньше единицы для любых квантовых состояний. Данный факт позволяет организовать безусловно секретный криптографический протокол распространения ключа. Детектирование любых попыток подслушивания гарантируется фундаментальными законами природы — квантовой механикой и специальной теорией относительности. Причем факт ортогональности или неортогональности состояний, который был принципиален для обеспечения секретности в нерелятивистском случае, здесь таковым не является. Это означает, что в квантовой криптографии могут быть использованы любые квантовые состояния (разумеется, что должна быть выбрана надлежащая процедура измерений при детектировании задержек).

В заключение этого раздела заметим, что обычно произносимые в задачах квантовой криптографии слова о том, что любое измерение (наблюдение) над квантовыми состояниями приводит к их изменению (кроме ортогональных), можно перефразировать следующим образом: любое получение информации о квантовых состояниях требует доступа к той области пространства-времени, где состояние присутствует, что всегда неизбежно требует (из-за конечности скорости света) конечного времени. Сама структура состояний (ортогональность или неортогональность) не является принципиальной, а принципиальным является то, что любые квантовые состояния имеют носитель (амплитуду, сглаживающую функцию) в пространстве-времени Минковского. Пространство результатов измерений, на котором задается операторно-значная мера и которое может иметь любую структуру, неизбежно содержит пространственно-временные области, поскольку нет измерений, имеющих место вне пространства-времени. Хотя само по себе такое замечание кажется очевидным, тем не менее в задачах квантовой криптографии, как правило, это обстоятельство игнорируется, хотя и неявно подразумевается.

Необходимо отметить, что приведенные выше вероятности результатов измерений выражаются по сути через волновую функцию Ландау–Пайерлса [14]. Все результаты могут быть перевыражены через волновую функцию, предложенную Бялыницким-Бирулой [30], квадрат модуля которой в пространственно-временном представлении является локальной плотностью энергии. Амплитуды (волновые функции) связаны в этих двух представлениях соотношением

$$\sqrt{k}\varphi_{LP}(k) = \varphi_{B-B}(k). \tag{68}$$

Факт наличия пространства-времени позволяет также реализовать другие квантовые криптографические протоколы, которые не удается сформулировать, если принимать во внимание только структуру гильбертова пространства состояний. Одним из таких базовых криптографических протоколов является, так называемый протокол «coin flipping» («подбрасывание монеты по телефону»). В релятивистском квантовом случае можно сформулировать секретный протокол со сколь угодно малым смещением.

4. ПРОТОКОЛ ГЕНЕРАЦИИ СЕКРЕТНОГО КЛЮЧА

На сегодняшний день существуют несколько вариантов доказательства безусловной секретности. Поскольку не может существовать доказательства секретности вообще, необходимо доказывать секретность конкретного протокола обмена. Майерс был несомненно первым, кто четко сформулировал критерий секретности и доказал его [31]. Доказательство [31] относится к так называемому протоколу BB84 [9], этому же протоколу посвящена работа Ройчоудхури и др. [32]. Доказательство Ло и Чау [33] относится к протоколу на EPR-эффекте и, в отличие от [31, 32], требует наличия у легитимных пользова-

телей пока еще не существующего квантового компьютера. Шор и Прескил [34] упростили упомянутые доказательства путем явного введения в схему корректирующих кодов.

Основная сложность в доказательстве безусловной секретности возникает из-за того, что упомянутые протоколы формулируются как протоколы «обмена» в гильбертовом пространстве состояний и не используют явно соображений причинности и того факта, что легитимные пользователи являются пространственно удаленными в координатном пространстве. Хотя всегда реально передача информации 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. Формулировка протоколов, при которых используются лишь свойства пространства состояний, неизбежно приводит к необходимости доказывать устойчивость протоколов относительно коллективных измерений, учет которых и представляет наибольшую трудность.

Сформулируем сначала критерий секретности ключа. В отличие от [31], здесь мы примем другой 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, полученная в результате протокола, принята A и B как секретный ключ. Тогда ключ секретен, если выполняются следующие условия.

1. *Идентичность ключа.* Вероятность того, что каждый бит в строке из m бит, принятых как ключ, различается у A ($b_A(i)$) и B ($b_B(i)$), экспоненциально мала, т. е.

$$\forall \varepsilon_1 > 0 \quad \exists M, \quad \text{что}$$
$$\Pr\{b_A(i) \neq b_B(i)\} \leq e^{-M} \leq \varepsilon_1. \quad (69)$$

Или на языке взаимной информации между A и B о строке результирующих бит длиной m:

$$I(A;B) \geq m - 2^{-M'}. \quad (70)$$

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. То есть вероятность того, что подслушиватель знает любой бит в строке, принятой как секретный ключ, экспоненциально мала по сравнению с $1/2$:

$$\forall \varepsilon_2 > 0, \quad \exists \eta_2, \zeta \quad \text{что}$$
$$\Pr\{b_A(i) = b_E(i)\} \leq \frac{1}{2} + e^{-\eta_2}, \quad e^{-\eta_2} \leq \varepsilon_2. \quad (71)$$

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

$$I(A;E) \leq e^{-\eta_2} \leq \varepsilon_2, \quad I(B;E) \leq e^{-\eta_2} \leq \varepsilon_2. \quad (72)$$

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 между легитимными пользователями. Поскольку любое получение информации о передаваемых состояниях приводит к возникновению ошибок у легитимных пользователей, данное обстоятельство при надлежащем протоколе позволяет гарантировать, что если строка бит принята как ключ, то он одинаков у A и B и известен только им. Протокол выглядит следующим образом.

1. Участники A и B выбирают большое целое число $N \gg 1$. Протокол использует $2N$ бит.

2. Через открытый канал участники синхронизируют часы (длина линии связи считается известной заранее). Также через открытый канал анонсируются моменты посылки состояний t_i ($i = 1, \ldots, 2n$) и $t_{i+1} - t_i > 2T$.

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

4. Участник A посылает в моменты t_i состояния $|\varphi_{b_i}\rangle$ с носителями в частотной полосе Δk, которая также заранее оговаривается (формы состояний не обязаны быть оптимальными в смысле их локализации (44)–(46)).

5. Участник B проводит измерения на приемном конце, которые описываются разбиением единицы (54), (55), и анонсирует через открытый канал факт регистрации состояния.

6. После посылки всех состояний участником A, участник B сообщает через открытый канал номера тех посылок, в которых результаты измерений дали

исходы во временных окнах $(t_i + L_{ch}, t_i + L_{ch} + 2T)$. Посылки, в которых были исходы вне временных окон, отбрасываются. Пусть число таких исходов $2n$.

7. Участник A случайным образом выбирает n исходов из $2n$ и открыто сообщает значения битов, которые им посылались в каждой посылке.

8. 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, есть n_{OK} и $n_{\overline{OK}}$, где нет совпадения. Оценка вероятности ошибки есть $\delta_{err} = n_{\overline{OK}}/n_s$. При достаточно большом n_s вероятность ошибки в нераскрытой части посылок экспоненциально близка к δ_{err}.

9. Для оставшейся последовательности нераскрытых битов длиной n участники A и B исправляют ошибки. Для этого выбирается классический код корректирующий ошибки $[n, k, d]$ с минимальным расстоянием по Хэммингу d и числом кодовых слов 2^k. ($d > 2\delta_{err}n + 1$ для линейного кода либо $d > \delta_{err}n + 1$ для случайного линейного кода, см. ниже). Для этого участник A анонсирует открыто v_i $(r = n - k)$ проверочных строк данного кода $(i = 1, \ldots, r)$. Участник A также отрыто сообщает r проверочных битов четности $parity_i = v_i n_A$ (n_A и n_B — строки нераскрытых битов соответственно у A и B, которые, вообще говоря, не совпадают и различаются с вероятностью, сколь угодно близкой к единице, примерно в $\delta_{err}n$ позициях, которые подлежат коррекции).

10. Участник B, зная правильную четность подстрок, исправляет ошибки в своей последовательности n_{sB}. На этом этапе с вероятностью, сколь угодно близкой к единице, при достаточно большом n строки битов у A и B идентичны (см. ниже).

11. Далее A и B проводят усиление секретности ключа (так называемая процедура privacy-amplification). Выбирается некоторая хэш-функция и открыто анонсируется. Стратегия усиления секретности состоит в том, чтобы из строки битов $\hat{w} = \{w_i\}$ длиной k, возникшей в результате исправления ошибок при помощи корректирующего кода в 9) у A и B, получить строку меньшей длины $m < k$ такую, чтобы гарантировать, что она неизвестна подслушивателю (известна с экспоненциально малой вероятностью, диктуемой выбранным параметром секретности). Для этого участником A выбираются m строк $\hat{l} = \{l_i\}$ длиной k $(i = 1, \ldots, m)$. Окончательная секретная строка бит $\hat{key}$ длиной m получается как биты четности $\hat{key} = \hat{w}\hat{l}$.

12. Если недостаточно длины строки $\hat{w}$, чтобы обеспечить требуемую секретность ключа, протокол обрывается.

Полное математическое доказательство имеет смысл привести отдельно, здесь мы приведем лишь набросок доказательства с разъяснением интуитивных идей, лежащих в его основе.

При достаточно большом $2n$ (число посылок, в которых результаты измерений у B дали исход в правильном временном окне, см. разд. 6) оценка вероятности ошибок, возникших в раскрытой случайно выбранной части посылок длиной n из полного числа посылок $2n$, гарантирует с вероятностью, сколь угодно близкой к единице, что в нераскрытых n посылках число ошибок (несовпадающих битов у A и B) равно

$$n_{err} = \delta_{err} n. \tag{73}$$

Это обстоятельство позволяет выбрать линейный классический код корректирующий ошибки $[n, k, d]$ с кодовым расстоянием $d/n \geq 2\delta_{err}$ и содержащий

$$k \geq n(1 - H(2\delta_{err}))$$

информационных символов, который позволяет исправить ошибки в $(d-1)/2$ позициях с вероятностью, сколь угодно близкой к единице [35–37]. Здесь

$$H(x) = -x\log x - (1 - x)\log(1 - x) \tag{74}$$

бинарная энтропийная функция. Данное утверждение следует из достижимой границы Варшамова–Гильберта [37] для линейных кодов. Если использовать случайные линейные корректирующие коды, то данная оценка может быть улучшена, соответственно, имеем $d/n > \delta_{err}$, и оставшееся число информационных битов равно

$$k < n(1 - H(\delta_{err})) \tag{75}$$

(предел Шеннона). Однако оценка, следующая из неравенства Варшамова–Гильберта, является 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 конструктивной, а скорее является теоремой существования. То есть неизвестны регулярные коды, на которых данная граница может быть достигнута [37].

Протокол будет работать до тех пор, пока вероятность ошибки $\delta_{err} < \delta_E$. Код, выбранный A и B, должен исправлять все потоки ошибок, вероятность ко-

торых меньше δ_{err}. Поскольку подслушиватель может знать все используемые в протоколе биты с вероятностью ошибки $\delta_E \approx 43.75\,\%$, используя передаваемую по открытому каналу информацию при коррекции ошибок (сам корректирующий код и все проверочные строки четности), он может в принципе свести вероятность своих ошибок сколь угодно близко к нулю, если $\delta_{err} > \delta_E$.

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

$$d/n \geq \delta_{err}, \quad \text{но} \quad d/n < \delta_E, \tag{76}$$

который с вероятностью, сколь угодно близкой к единице (почти достоверностью при большом n), будет исправлять ошибки у A и B, но не будет исправлять их у подслушивателя. Число оставшихся (и уже одинаковых) битов у A и B в результате коррекции при достаточно больших $n \gg 1$ будет приблизительно равна

$$nC(\delta_{err}), \tag{77}$$

где

$$C(\delta_{err}) = 1 - H(\delta_{err}) \tag{78}$$

— пропускная способность классического симметричного бинарного канала связи.

По сути, при условии (76) подслушиватель находится в ситуации бинарного симметричного канала [35–37], 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 $\delta_{err} < \delta_E$), выглядит для него как передача сообщений со скоростью, превышающей пропускную способность канала связи между ним и A.

В этом случае при скоростях передачи выше пропускной способности можно воспользоваться оценкой Вольфовица [38] для вероятности ошибки на символ, которая у подслушивателя не меньше, чем

$$p_{err} > 1 - 4\frac{\text{const}}{n(C(\delta_{err}) - C(\delta_E))^2} - \\ - \exp\left[-\frac{n(C(\delta_{err}) - C(\delta_E))}{2}\right]. \tag{79}$$

Последнее означает, что предельная допустимая вероятность ошибок в канале связи $\delta_{err} \approx 21.875\,\%$, а соответственно, в шенноновском пределе $\delta_{err} \approx \approx 43.75\,\%$.

Обратим внимание, что в квантовой криптографии на неортогональных состояниях (так называемый протокол BB84 [9]) допустимая вероятность ошибок, при котором протокол работает и позволяет создать секретный ключ, есть $7.5\,\%$ (и в шенноновском пределе $11\,\%$). 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) [34]. Поэтому порог определяется из уравнения

$$1 = 2H(2\delta_{err}), \tag{80}$$

соответственно в пределе Шеннона

$$1 = 2H(\delta_{err}). \tag{81}$$

После процедуры коррекции ошибок строки бит у легитимных пользователей идентичны с вероятностью, сколь угодно близкой к единице.

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).

В качестве простого примера хэш-функции рассмотрим функцию, которая на выходе дает бит четности строки бит длиной m, который будет окончательным секретным битом. Секретный бит с вероятностью, сколь угодно близкой к единице, одинаков у легитимных участников A и B, а подслушиватель знает его со сколь угодно малой наперед заданной вероятностью. Если каждый бит в строке известен подслушивателю с вероятностью p_e, в отличие от легитимных пользователей, которые знают его с достоверностью, то ошибка в определении секретного бита четности есть (считаем, что m для определенности четно)

$$P_{err}(parity) = \sum_{i=odd}^{m-1} C_m^i p_e^i (1-p_e)^{m-i}, \tag{82}$$

суммирование проводится только по нечетным индексам i, потому что ошибка в определении бита четности возникает, если подслушиватель ошибается в нечетном числе позиций. Принимая во внимание, что

$$\frac{1}{2}[(x+y)^m - (x-y)^m] = \sum_{i=odd}^{m-1} C_m^i x^i y^{m-i}, \tag{83}$$

и полагая $x = p_e$ и $y = 1 - p_e$, находим

$$P_{err}(parity) = \frac{1}{2}[1 - (1 - 2p_e)^m]. \qquad (84)$$

Соответственно, вероятность того, что подслушиватель знает секретный бит, есть

$$P_{OK}(parity) = 1 - P_{err}(parity) = \\ = \frac{1}{2}[1 - (1 - 2p_e)^m] = \frac{1}{2} + \varepsilon, \qquad (85)$$

где ε — экспоненциально малая величина. Из (77) следует, что если число оставшихся битов после коррекции ошибок m достаточно велико, то всегда можно сделать вероятность правильной идентификации секретного бита подслушивателем экспоненциально малой по сравнению с вероятностью простого угадывания, которая всегда существует и равна $1/2$.

5. СКОРОСТЬ ГЕНЕРАЦИИ СЕКРЕТНОГО КЛЮЧА В РЕАЛЬНОМ ВРЕМЕНИ

Рассмотрим теперь вопрос о скорости генерации ключа в реальном времени. Предельная скорость генерации (бит/с) определяется как свойствами канала связи, внешними шумами, так и интенсивностью подслушивания. Поскольку действия подслушивателя ничем не ограничены, невозможно в общем виде установить скорость распространения ключа при наличии произвольного шума и подслушивателя. Например, подслушиватель может столь интенсивно вторгаться в канал связи, что совсем блокирует передачу ключа. Все схемы квантовой криптографии лишь гарантируют тот факт, что если все тесты, предписываемые протоколом, прошли успешно, то ключ секретен. Однако вполне осмысленным является ответ на вопрос о предельной скорости генерации ключа в реальном времени. Такая скорость зависит лишь от свойств квантового канала связи (в нашем случае — от частотной полосы пропускания) и по сути представляет собой пропускную способность квантового канала связи. Предельная скорость генерации ключа не может быть выше, чем пропускная способность.

К настоящему моменту получены красивые и глубокие результаты по пропускным способностям квантовых каналов связи, приведенные в прекрасном обзоре Холево [39]. Однако теоремы кодирования, из-за того что они формулируются лишь в терминах свойств гильбертова пространства состояний квантовых систем, не дают ответа на вопрос о пропускных способностях в реальном времени, а дают скорость передачи в смысле числа бит (≤ 1) на посылку. Для получения пропускной способности в реальном времени требуется явное введение в задачу пространства-времени. Когда информация кодируется в состояния поляризации, можно получить пропускную способность в реальном времени [41]. Здесь мы обобщим наши предыдущие результаты на случай, когда информация кодируется в «форму» пакета, точнее для случая, когда информационные состояния $|\varphi_{0,1}\rangle$ имеют не перекрывающиеся по частоте носители.

Квантовый канал задается отображением входных операторов матриц плотности в выходные операторы, которые также являются матрицами плотности. Такое отображение описывается инструментом или супероператором по другой терминологии. Оказывается, что измерения на приемном конце в конечном временном окне могут быть описаны введением некоторого супероператора, который порождает операторные меры $\mathcal{M}(T)$ и $I(\Delta k) - \mathcal{M}(T)$. Согласно теореме представления Крауса [29], любое отображение матриц плотности в матрицы плотности (супероператор), обладающее свойством сохранения следа, линейности и полной положительности, может быть представлено в виде

$$\mathcal{T}[\ldots] = \sum_k V_k[\ldots]V_k^+, \quad \sum_k V_k^+ V_k = I. \qquad (86)$$

Индекс k описывает пространство результатов измерений, которое может быть не только дискретным множеством, но и континуумом. Вероятность исходов измерений описывается операторно-значной мерой, которая связана с операторами в (86) следующим соотношением:

$$\mathcal{M}_k = V_k^+ V_k. \qquad (87)$$

Вероятность k-го исхода на входном состоянии с матрицей плотности ρ есть

$$\Pr(k) = \mathrm{Tr}\{\rho\mathcal{M}_k\}. \qquad (88)$$

Отметим, что, вообще говоря, сам супероператор по операторно-значной мере не всегда однозначно восстанавливается. Однако в нашем случае с этим не возникает трудностей.

Супероператор для нашего случая может быть представлен в виде прямой суммы, действующий на матрицы плотности с носителями в неперекрывающихся частотных полосах $\{\Delta k\}_0$ и $\{\Delta k\}_1$:

$$\mathcal{T}[\ldots] = \mathcal{T}_0[\ldots] \bigoplus \mathcal{T}_1[\ldots], \qquad (89)$$

где

$$\mathcal{T}_i[\rho_i] = \sqrt{\mathcal{M}_i(T)}\rho_i\sqrt{\mathcal{M}_i(T)}^{+} + \\ + \mathrm{Tr}\{(I_i(\Delta k) - \mathcal{M}_i(T))\rho_i\}|?\rangle\langle ?|, \quad (90)$$

где введено состояние $|?\rangle$, которое ортогонально первому слагаемому в (90) и описывает отсутствие исходов измерений наблюдателя во временном окне $(-T, T)$. Знак вопроса (?) в состоянии означает, что отсутствию исхода во временном окне $(-T, T)$ наблюдатель всегда вынужден приписывать неопределенный (inconclusive) результат. Имеет место несложно проверяемая формула

$$\sqrt{\mathcal{M}_i(T)} = \sqrt{\int_{-T}^{T}\frac{d\tau}{2\pi}\left(\int\limits_{\{\Delta k\}_i}\frac{dk}{\sqrt{k}}\exp(-ik\tau)|k\rangle\right)\left(\int\limits_{\{\Delta k\}_i}\frac{dk'}{\sqrt{k'}}\exp(ik'\tau)\langle k'|\right)} = \\ = \frac{1}{\pi}\int\limits_0^\infty\frac{d\zeta}{\zeta^{1/2}}\,\frac{\mathcal{M}_i(T)}{(\zeta I_i(\Delta k) + \mathcal{M}_i(T))} = \sum_{n=0}^{\infty}\sqrt{\lambda_n(2\Delta k\cdot T)}|\varphi_n(i)\rangle\langle\varphi_n(i)|, \quad (91)$$

где

$$|\varphi_n(i)\rangle = \int\limits_{\{\Delta k\}_i} dk\varphi_n(k)|k\rangle \quad (92)$$

(функция $\varphi_n(k)$ удовлетворяет интегральному уравнению (46) в соответствующей частотной полосе $\{\Delta k\}_i$, $i = 0, 1$).

Пропускная способность может быть вычислена по формуле Холево [39]:

$$C(T) = \\ = \max\{\pi_0, \pi_1\}\left\{H(\mathcal{T}[\rho]) - \sum_{i=0,1}\pi_i H(\mathcal{T}[\rho_i])\right\}, \quad (93)$$

где

$$H(\rho) = -\mathrm{Tr}\{\rho\log\rho\} \quad (94)$$

— квантовая энтропия фон Неймана. Входная матрица плотности имеет вид

$$\rho = \pi_0|\varphi_0\rangle\langle\varphi_0| + \pi_1|\varphi_1\rangle\langle\varphi_1|, \\ \rho_i = |\varphi_i\rangle\langle\varphi_i|, \quad i = 0, 1. \quad (95)$$

Здесь π_0, π_1 — априорные вероятности. Максимум в (93) достигается при $\pi_0 = \pi_1 = 1/2$, когда состояния 0 и 1 посылаются с равными вероятностями.

Если в качестве входных состояний выбираются оптимальные состояния, имеющие минимально возможную эффективную протяженность при данной частотной полосе, т. е. состояния (42)–(44), то пропускная способность в реальном времени будет равна

$$C(T) = \frac{1-\varepsilon}{T}\quad\left[\frac{\text{бит}}{\text{с}}\right], \quad 1-\varepsilon = \lambda_0(\Delta k\cdot T). \quad (96)$$

Величина $\lambda_0(\Delta k\cdot T)$ есть наибольшее собственное число интегрального уравнения (44). Выражение (96) совпадает с пропускной способностью бинарного классического канала со стиранием. Величина вероятности стирания ε связана со скоростью передачи в реальном времени и частотной полосой канала. Таким образом, даже в идеальном квантовом канале связи имеет место «шум», который обусловлен конечным временем наблюдения на приемном конце.

Если на выходном конце канала связи измерения проводятся в большом временном окне (формально бесконечном $T\to\infty$), то из-за достоверной различимости ортогональных состояний (в этом пределе состояния доступны целиком) число безошибочно декодируемых последовательностей равно $2^{nH(\rho)}$. Для ортогональных состояний не требуется коллективных измерений, а достаточно измерять состояния в каждой отдельной посылке. Если же измерения проводятся в конечном временном окне $(-T, T)$, то при измерениях будут исходы, когда измерительное устройство вообще не срабатывает в течение $2T$. Вероятность такого события ε, и соответственно, вероятность срабатывания внутри временного окна будет равна $1-\varepsilon$. Если срабатывание в течение T было, то состояния идентифицируются достоверно. При отсутствии исхода внутри временного окна можно считать, что имеет место стирание состояния (формально состояние переходит на приемном конце в некоторое новое состояние (?), формально также можно считать, что на входе это состояние посылается с вероятностью $p_? = 0$). Каждая типичная последовательность раздувается при этом в сферу Хэмминга (Hamming) радиуса $H(x|y)$. Здесь $H(x|y)$ — условная энтропия Шеннона входного ($x = \{0, 1, ?\}$) с вероятностями $\{p_0 = 1/2, p_1 = 1/2, p_? = 0\}$ и выходного ($y = \{0, 1, ?\}$) алфавитов и переходных вероятностей в канале

$$p(0|0) = p(1|1) = 1 - \varepsilon, \quad p(0|1) = p(1|0) = 0,$$

$$p(0|?) = p(1|?) = \varepsilon.$$

Поэтому число безошибочно декодируемых последовательностей при $n \to \infty$ будет равно

$$\frac{2^{nH(\rho)}}{2^{nH(x|y)}} = 2^{nI(x:y)}, \quad I(x:y) = 1 - \varepsilon, \qquad (97)$$

что совпадает с пропускной способностью классического бинарного стирающего канала связи [36] и определяет максимальную скорость передачи ключа при заданной полосе и временном окне наблюдения.

6. ПРОСТОЙ ПРИМЕР ВОЗМОЖНОЙ РЕАЛИЗАЦИИ КРИПТОСИСТЕМЫ

Обсудим теперь простой пример реализации криптосистемы. Данный пример носит иллюстративный характер и показывает лишь физическую интерпретацию проблемы. Рассмотрим приготовление состояний с конечной частотной полосой. Пусть источник (например, лазер) выдает на выходе короткое по времени (соответственно, с достаточно широким спектром по частоте, приблизительно равным $\Delta\Omega$) квантовое состояние. Время начала протокола при этом фиксируется с точностью $\Delta t \approx 1/\Delta\Omega$. Затем сигнал ослабляется до однофотонного уровня, что достигается прохождением через поглотитель. Затем состояние попадает на фильтр (среду с частотной дисперсией), который вырезает из широкого частотного спектра $\Delta\Omega$ полосы шириной, приблизительно равной $\{\Delta k\}_0 \ll \Delta\Omega$ (или полосу той же ширины, но центрированную возле другой несущей частоты $\{\Delta k\}_1 \ll \Delta\Omega$, см. рис. 5). Последнее в принципе может быть сделано аналогично классическому опыту Ньютона по разложению в спектр «белого» (с широким спектром) света. При каждой посылке открывается случайно одна из апертур (рис. 5). Чем дальше установлена апертура, тем с большей точностью можно вырезать необходимую частотную полосу из спектра. При этом вырезаемая частотная полоса, приблизительно равная $1/T \propto 1/L$, где L — расстояние до апертуры (эффективная протяженность состояния). Знак пропорциональности означает, что вырезаемая частотная полоса зависит от дисперсионных свойств призмы, т. е. от того, на какой угол отклоняется каждая спектральная компонента. Вероятность вырезания узкой полосы из сигнала с

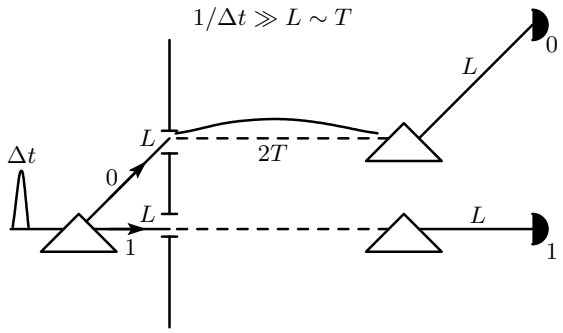

Рис. 5.

широким спектром, естественно, меньше единицы. То есть будут события, когда в канал ничего не распространяется, однако такие холостые исходы приготовления влияют только на эффективность, но не на секретность схемы. На выходе из апертуры состояние направляется в канал связи. Передний фронт выходит в канал связи приблизительно через время $\Delta t + L$. На приемном конце (рис. 5) используется такая процедура, что на детектор проходят только состояния, имеющие носитель в частотной полосе около $\{\Delta k\}_0$. Данное измерение является реализацией операторной меры, вырезающей (пропускающей) только частотную полосу около Δk (см. (54), (55)). Это не позволяет подслушивателю использовать короткие по времени (с широким частотным спектром) состояния для компенсации вносимой им временной задержки. Не задержанные состояния с носителем в частотной полосе около $\{\Delta k\}_0$ будут давать отсчеты во временном окне $(L_{ch}, L_{ch} + 2T)$, естественно, с точностью Δt. В протоколе используются только те события, которые дают измерения в данном временном окне. Характерная собственная постоянная времени τ_d детектора должна быть $\tau_d \ll T$. Фактически это требование возникает из-за того, что на временном интервале $2T$ необходимо набирать статистику отсчетов для временного теста на задержку.

Насколько нам известно, детекторы с постоянной времени $\tau_d \approx 10^{-8}$–10^{-9} с, являются достаточно стандартными устройствами. При этом эффективная протяженность состояния должна быть $T \approx 1/\Delta k \gg \tau_d$, что дает с запасом на два порядка степень монохроматичности состояния $\Delta k \approx 10^6$–10^7 Гц. Соответственно, эффективная протяженность $cT \approx 10$–100 м, что является достаточно мягким условием. Точность синхронизации часов должна быть $\max\{\tau_d, \Delta t\}$.

В реальных ситуациях оптоволоконная линия

связи не является прямой линией, соединяющей участников A и B. Это обстоятельство накладывает некоторое дополнительное ограничение на эффективную протяженность состояния. Последняя, по очевидным соображениям, не может быть меньше, чем $L_{curv} - L_{ch}$, где L_{curv} – истинная длина оптоволокна, а L_{ch} — длина прямой, соединяющей A и B. Кроме того, поскольку скорость света в оптоволокне c' несколько меньше предельной скорости света в вакууме ($c' < c$), это приводит к тому, что эффективная длина состояния не может быть меньше, чем $c(L_{curv} - L_{ch})/c'$.

Отметим, что криптосистема на частотных состояниях должна быть более устойчивой, чем системы на поляризационных состояниях, поскольку сбой частоты носителей происходит за счет рамановских процессов, которые возникают во втором порядке теории возмущений.

7. ЗАКЛЮЧЕНИЕ

Основное наблюдение, сделанное в данной работе, состоит в том, что учет ограничений, диктуемый специальной теорией относительности, позволяет использовать в квантовой криптографии для обеспечения безусловно секретной передачи ключа практически любые квантовые состояния. В отличие от предыдущих криптосистем, секретность которых основана на геометрии гильбертова пространства и свойствах неортогональных состояний в нем, данная схема в явном виде учитывает то обстоятельство, что любые квантовые состояния имеют носители в пространстве-времени Минковского. Кроме того, явный учет пространственно-временной структуры состояний позволяет реализовать другие важные квантовые криптографические протоколы.

Выражаю благодарность С. С. Назину за полезные обсуждения и критические замечания. Работа выполнена при финансовой поддержке РФФИ (грант № 02-02-16289), Минпромнауки (проекты №№ 40.020.1.1.1170, 37.029.1.1.0031), а также проектом ДН-ЕНН-02.

ЛИТЕРАТУРА

1. G. S. Vernam, J. Amer. Inst. Elect. Eng. **55**, 109 (1926).

2. C. E. Shannon, Bell Syst. Tech. J. **28**, 658 (1949).

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

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

5. P. W. Shor, *Proc. of 35th Ann. Symp. on the Foundations of Computer Science*, IEE Comput. Socie. Press, Los Alamitos, CA, p. 124; E-print archives quant-ph/9508027.

6. D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, E-print archives quant-ph/0203118.

7. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, E-print archives quant-ph/0101098; Rev. Mod. Phys. **74**, 145 (2002).

8. S. Wiesner, SIGACT News **15**, 78 (1983).

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

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

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

12. L. Goldenberg and L. Vaidman, Phys. Rev. Lett. **75**, 1239 (1995).

13. С. Н. Молотков, С. С. Назин, Письма в ЖЭТФ, **73**, 767 (2001); Письма в ЖЭТФ **76**, 79 (2002).

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

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

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

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

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

19. И. М. Гельфанд, Н. Я. Виленкин, *Некоторые применения гармонического анализа. Оснащенные гильбертовы пространства (Обобщенные функции, вып. 4)*, Физматгиз, Москва (1961).

20. Ю. А. Брычков, А. П. Прудников, *Интегральные преобразования обобщенных функций*, Наука, Москва (1977).

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

22. 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)].

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

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

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

26. S. Wickeramasekara and A. Bohm, E-print archives quant-ph/0302056.

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

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

29. K. Kraus, *States, Effects and Operations*, Springer-Verlag, Berlin (1983).

30. I. Bialynicki-Birula, in *Progr. in Opt.*, ed. by E. Wolf (1996), Vol. XXXVI, p. 245.

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

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

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

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

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

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

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

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

39. А. С. Холево, Проблемы передачи информации **8**, 63 (1972); **15**, 3 (1979); УМН **53**, 193 (1998); *Введение в квантовую теорию информации*, сер. *Соврем. мат. физ., вып. 5*, МЦНМО, Москва (2002).

40. M. Fleischauer and M. D. Lukin, Phys. Rev. Lett. **84**, 5094 (2000).

41. С. Н. Молотков, Письма в ЖЭТФ **76**, 683 (2002); **77**, 51 (2003).