Письма в ЖЭТФ, том 75, вып. 10, с. 617 – 623 © 2002 г. 25 мая

О предельной скорости генерации секретного ключа в квантовой криптографии в пространстве-времени

С. Н. Молотков

Институт физики твердого тела РАН, 142432 Черноголовка, Московская обл., Россия

Поступила в редакцию 2 апреля 2002 г.

Обсуждаются принципиальные ограничения на максимально допустимую скорость распространения секретного ключа в квантовой криптографии в реальном времени. Показано, что в квантовом канале с ограниченной полосой пропускания максимум скорости достигается в криптосистеме на ортогональных состояниях. Величина безразмерной скорости (число бит в единицу частотной полосы канала и в единицу времени) дается универсальной функцией $C(\lambda_0(\Delta k \cdot T))/\Delta k \cdot T$ (где $C(\lambda_0(\Delta k \cdot T))$ – пропускная способность бинарного классического канала, Δk – ширина полосы пропускания, $1/T$ – частота передачи квантовых состояний, λ_0 – наибольшее собственное число некоторого интегрального уравнения).

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

Вопрос о максимально возможной скорости передачи секретного ключа в квантовой криптографии представляет не только чисто принципиальный, но и практический интерес. Для распространения секретного ключа в квантовой криптографии необходимы два канала связи – квантовый, по которому передаются квантовые состояния, несущие информацию о секретном ключе, и открытый – вспомогательный классический канал [1]. Ниже будут рассмотрены ограничения, накладываемые параметрами квантового канала связи, в частности, полосой пропускания, на предельную скорость генерации секретного ключа. Ограничения на предельную скорость генерации ключа возникают фактически из-за того, что хотя состояния квантовой системы и описываются векторами (лучами) в гильбертовом пространстве $\mathcal{H}$, тем не менее, должны иметь носители в пространстве-времени Минковского [2]. Кроме того, состояния в $\mathcal{H}$ должны быть ассоциированы с физическими объектами (частицами), которые распространяются при передаче информации в пространстве-времени Минковского. Приписывание базисных векторов, относящихся к различным неприводимым представлениям группы Пуанкаре в $\mathcal{H}$, состояниям различных частиц (фотонам, электронам и т.д.) является одним из основных положений при интерпретации квантовой теории поля [2].

Все квантовые криптосистемы можно условно разделить на три типа: на неортогональных состояниях [1], EPR-эффекте [3] и ортогональных состояниях [4,5]. Секретность криптографии на неортогональных состояниях основывается на невозможности получения информации о них без их возмущения [1]. В отличие от неортогональных, ортогональные состояния достоверно различимы при условии, что они доступны целиком для измерения (фактически целиком доступен носитель состояния в пространстве-времени Минковского), и становятся достоверно неразличимыми, если недоступны целиком. Более того, они остаются достоверно неразличимыми, даже если они остаются ортогональными при ограничении на любую пространственно-временную область [5][1]. Протоколы распространения секретного ключа на ортогональных состояниях устроены таким образом, что состояния при распространении через канал связи никогда не присутствуют в нем целиком единовременно [4, 5]. Для детектирования попыток подслушивания в криптографии на ортогональных состояниях существенно наличие предельной скорости распространения квантовых состояний, диктуемой специальной теорией относительности [4, 5]. Для криптосистем на неортогональных состояниях пространственно-временная структура состояний явно нигде не учитывается, поскольку для протоколов формально достаточно лишь факта неортогональности векторов состояний как элементов $\mathcal{H}$. Напротив, для криптосистем на ортогональных состояниях пространственно-временная структура состояний учитывается сразу и явно, как необходимый элемент в протоколах обмена.

Ниже будет показано, что учет пространственно-временной структуры квантовых состояний приводит в квантовом канале с конечной частотной полосой пропускания к ограничениям на предельную скорость распространения секретного ключа. Причем

[1] Обратим внимание на то, что в схеме [4] состояния в канале эффективно неортогональны, в отличие от [5].

эти ограничения, если не игнорировать того обстоятельства, что информация переносится конкретными физическими объектами, оказываются, по-сути, одними и теми же для криптографии на неортогональных и ортогональных состояниях. Ограничения на свойства квантового канала связи реально всегда существуют. Например, в случае оптоволокна всегда существует ограничение, связанное с конечной полосой пропускания. В случае криптографии через открытое пространство также существует ограничение, накладываемое окном прозрачности в атмосфере. То есть, ограничение на полосу пропускания является достаточно общим.

Обсудим сначала ограничения на предельную скорость генерации ключа для криптосистем на неортогональных состояниях. Количество классической информации, которое может быть передано от одного участника (A) криптографического протокола к другому (B) при помощи квантовых состояний, дается максимумом взаимной информации, величина которой ограничена неравенством Холево [6]:

$$I(A;B)=\max_{E_i}\sum_i\left\{\pi_0\,\mathrm{Tr}\{\rho_0E_i\}\log_2\left(\frac{\mathrm{Tr}\{\rho_0E_i\}}{\mathrm{Tr}\{\rho E_i\}}\right)+\right.$$
$$\left.+\,\pi_1\,\mathrm{Tr}\{\rho_1E_i\}\log_2\left(\frac{\mathrm{Tr}\{\rho_1E_i\}}{\mathrm{Tr}\{\rho E_i\}}\right)\right\}\le$$
$$\le S(\rho)-\sum_{i=0,1}\pi_iS(\rho_i),\quad S(\rho)=-\mathrm{Tr}\{\rho\log_2\rho\},\qquad(1)$$

где $S(\rho)$ – энтропия фон Неймана, $\pi_{0,1}$ – априорные вероятности, с которыми посылаются квантовые состояния $\rho_{0,1}$ и $\rho=\pi_0\rho_0+\pi_1\rho_1$ $(\pi_0+\pi_1=1)$, E_i – измеряющие операторы, удовлетворяющие разложению единицы $I=\sum_iE_i$. Далее будем рассматривать чистые состояния $\rho_{0,1}=|\varphi_{0,1}\rangle\langle\varphi_{0,1}|$, в этом случае $S(\rho_1)=0$. Максимальная "скорость" генерации ключа дается пропускной способностью квантового канала. Последняя представляет собой максимум по всевозможным входным априорным распределениям взаимной информации (1) [7] (максимум достигается при $\pi_0=\pi_1=1/2$):

$$C=-\left[\left(\frac{1-\varepsilon}{2}\right)\log_2\left(\frac{1-\varepsilon}{2}\right)+\right.$$
$$\left.+\left(\frac{1+\varepsilon}{2}\right)\log_2\left(\frac{1+\varepsilon}{2}\right)\right],\quad\varepsilon=|\langle\varphi_0|\varphi_1\rangle|.\qquad(2)$$

Величина C дает количество информации в классических битах (≤1) на одну посылку при достаточно длинной передаваемой последовательности, которое может быть передано со сколь угодно малой ошибкой [8]. Соответственно, величина $1/C$ определяет количество посылок ("скорость"). Данные рассуждения относятся к ситуации без подслушивателя. При наличии подслушивателя невозможно сделать никаких общих заключений о скорости генерации ключа, поскольку подслушивание может быть столь интенсивным, что совсем блокирует передачу ключа.

Максимум "скорости" (пропускной способности) генерации ключа для криптосистемы на неортогональных состояниях не может превышать скорости для ортогональных состояний. Для достижения "скорости" генерации, равной пропускной способности для неортогональных состояний в асимптотическом пределе больших последовательностей, требуются коллективные измерения над блоками состояний [9] (измерения, сводящиеся к проекции на подпространство типичных последовательностей). Для ортогональных состояний коллективные измерения не требуются. Достаточно индивидуальных измерений над состоянием в каждой посылке. Измерение сводится к тензорному произведению индивидуальных измерений, каждое из которых дается разложением единицы вида

$$I=E_0+E_1,\quad E_{0,1}=|\varphi_{0,1}\rangle\langle\varphi_{0,1}|,\qquad(3)$$

где $E_{0,1}$ – проекторы на состояния. Измерение над последовательностью длины N дается разложением единицы:

$$I^{\otimes N}=\overbrace{I\otimes I\ldots\otimes I}^{N}.\qquad(4)$$

Измерения, сводящие к проектированию либо на отдельные состояния, либо на их блоки, ничего не говорят о скорости генерации ключа в реальном времени, так как проекторы явно не содержат информации о пространственно-временной структуре состояний. Поскольку все события для наблюдателей неизбежно происходят в пространстве-времени Минковского, то измерения должны явно или опосредованно содержать информацию о пространственно-временных областях. В нерелятивистской квантовой механике такое замечание не дает ничего нового, поскольку отсутствует ограничение на предельную скорость распространения. В квантовой теории поля невозможно игнорировать ограничения, диктуемые специальной теорией относительности на предельную скорость распространения квантовых объектов.

Будем далее ассоциировать с векторами $|\varphi_{0,1}\rangle\in\in\mathcal{H}$ однофотонные состояния. Также будем считать, как это обычно делается, что информация кодируется состояниями поляризации фотонов. При "нерелятивистском" квантовомеханическом рассмотрении

фотонов, часто используемом в задачах квантовой теории информации, как правило, пространственные степени свободы игнорируются, и оставляются поляризационные степени свободы, описываемые векторами в гильбертовом пространстве с $\dim\mathcal{H}=2$. Не существует ни спина электрона, ни поляризации фотона в отрыве от пространственных степеней свободы. Более того, для фотонного квантованного поля из-за его безмассовости и поперечности, строго говоря, пространственные и поляризационные степени свободы даже невозможно представить в факторизованном виде. Для наших целей будет достаточно рассматривать одномерную безмассовую частицу с двумя состояниями поляризации. Такая ситуация является идеализацией, но отражает основные черты квазиодномерных как оптоволоконных систем, так и узких пучков света. Состояния безмассового свободного квантованного поля порождаются действием полевых операторов (обобщенных функций с операторными значениями) [2] на вакуумный вектор[2)]:

$$\varphi_\mu^+(\hat{x})=\frac{1}{\sqrt{2\pi}}\int d\hat{k}\delta(\hat{k}^2)\theta(k_0)\mathrm{e}^{i\hat{k}\hat{x}}a_\mu^+(k),$$
$$\hat{k}=(k,k_0),\quad \hat{x}=(x,t),\quad d\hat{k}=dkdk_0, \tag{5}$$
$$\hat{k}\hat{x}=kx-k_0t,\ [a_\nu^-(k),a_\mu^+(k)]=k_0\delta(k-k')\delta_{\nu,\mu}.$$

Индексы $\mu,\nu=0,1$ нумеруют два базисных состояния поляризации. Физические состояния квантованного поля $|\varphi_\mu\rangle\in\mathcal{H}$ получаются как результат сглаживания операторных обобщенных функций с основными функциями $\varphi(\hat{x})\in\Omega(\hat{x})$ ($\Omega(\hat{x})$ – пространство основных функций [2]); $\varphi_\mu^+(\hat{x})|0\rangle\in\Omega(\hat{x})^*$ – обобщенные собственные векторы (линейные непрерывные функционалы в $\mathcal{H}$), и $\Omega(\hat{x})\subset\mathcal{H}\subset\Omega^*(\hat{x})$ – оснащенное гильбертово пространство (тройка Гельфанда) [10];

$$|\varphi_\mu\rangle=\int d\hat{x}\varphi(\hat{x})\varphi_\mu^+(\hat{x})|0\rangle=$$
$$=\int d\hat{k}\tilde{\varphi}(\hat{k})\delta(\hat{k}^2)\theta(k_0)a_\mu^+(k)|0\rangle=$$
$$=\int\limits_{-\infty}^{\infty}\frac{dk}{k_0}\tilde{\varphi}(k,k_0=|k|)|k,\mu\rangle,$$
$$|k,\mu\rangle=a_\mu^+(k)|0\rangle,\quad \langle k',\nu|k,\mu\rangle=k_0\delta_{\mu,\nu}\delta(k-k'). \tag{6}$$

Условие нормировки

$$\langle\varphi_\mu|\varphi_\mu\rangle=\int\limits_{-\infty}^{\infty}\frac{dk}{k_0}|\tilde{\varphi}(k,k_0=|k|)|^2=$$
$$=\int\limits_{-\infty}^{\infty}dk|\varphi(k)|^2=1,\quad \varphi(k)=\frac{\tilde{\varphi}(k,k_0=|k|)}{\sqrt{k_0}}. \tag{7}$$

Считаем, что состояния отличаются только состоянием поляризации и имеют одинаковую пространственную амплитуду $\tilde{\varphi}(\hat{k})$. Состояния $|\varphi_\mu\rangle$ определяются значениями амплитуды $\tilde{\varphi}(\hat{k})$ на массовой поверхности $k_0=|k|$. При передаче информации между двумя участниками естественно рассматривать состояния, распространяющиеся в одном направлении ($k>0$). В этом случае все величины зависят от разности $\tau=x-t$ – переменная на одной из ветвей светового конуса.

Измерение, достоверно различающее пару ортогональных состояний, дается разложением единицы вида (2) в одночастичном подпространстве состояний. Проекторы неизбежно включают в себя пространственную часть вектора состояний. Состояния различаются достоверно, если имеется доступ ко всему состоянию целиком (той области пространства, где отлична от нуля амплитуда состояния $\varphi(x,t)$). Формально амплитуда отлична от нуля во всем пространстве. Этот факт следует из теоремы Винера-Пэли [11]: фурье-образ нормированной функции $\varphi(k)$ ($k\geq 0$)

$$\int\limits_0^\infty dk|\varphi(k)|^2=1, \tag{8}$$

равной нулю на полуоси (при $k<0$), но не равной нулю тождественно, должен удовлетворять условию

$$\int\limits_{-\infty}^{\infty}\frac{\ln|\varphi(\tau)|}{1+\tau^2}d\tau<\infty,$$
$$\varphi(\tau)=\int\limits_0^\infty dk\mathrm{e}^{-k\tau}\varphi(k),\quad \tau=x-t. \tag{9}$$

Амплитуда состояния, как следует из (9), не может спадать экспоненциально, но может спадать на бесконечности сколь угодно близко к экспоненте $|\varphi(\tau)|\propto e^{-\alpha|\tau|/\ln(\ln(\ln(...\ln|\tau|)}$, где $\alpha>0$ может быть сколь угодно большим.

Реально измерения не могут охватывать все пространство, доступ ко всему пространству требовал бы бесконечно времени из-за наличия предельной скорости. Если измерение проводится в конечной доступной области, то пространством результатов яв-

[2)] Строго говоря, операторные обобщенные функции должны удовлетворять уравнениям Максвелла $i\partial\boldsymbol{\varphi}/\partial t=-\nabla\times\boldsymbol{\varphi}$, и $\nabla\cdot\boldsymbol{\varphi}=0$.

ляется $\Theta = (\Omega \times (0,1) \bigcup \overline{\Omega})$, где Ω – область, доступная для детектирования, и $\mu = (0,1)$ описывают каналы для ортогональных состояний поляризации. Область $\overline{\Omega}$ недоступна для измерения.

$$I = \bigoplus_{\mu=0,1} \int\limits_{\Delta k} \frac{dk}{k} |k,\mu\rangle\langle\mu,k| = \bigoplus_{\mu=0,1} \left(\mathcal{M}(\Omega,\mu) + \mathcal{M}(\overline{\Omega},\mu) \right), \tag{10}$$

где

$$\mathcal{M}(\Omega,\mu) = \int\limits_{\Omega} \mathcal{M}(d\tau,\mu), \quad \mathcal{M}(\overline{\Omega},\mu) = \int\limits_{\overline{\Omega}} \mathcal{M}(d\tau,\mu), \quad \overline{\Omega} \bigcup \Omega = (-\infty,\infty), \tag{11}$$

$$\mathcal{M}(d\tau,\mu) = \left(\int\limits_{\Delta k} \frac{dk}{\sqrt{k}} \mathrm{e}^{ik\tau} |k,\mu\rangle \right) \times \left(\int\limits_{\Delta k} \frac{dk'}{\sqrt{k'}} \mathrm{e}^{-ik'\tau} \langle k',\mu| \right) \frac{d\tau}{2\pi}. \tag{12}$$

Разложение единицы (12) является формальным описанием прибора, которое может быть интерпретировано следующим образом. Если считать пространством результатов пространственные области x, то измерение следует понимать как распределенный по x прибор, который выдает случайный результат в окрестности некоторой точки $(x, x+dx)$ в момент времени t. Если фиксировать x (локальный прибор), то измерение описывает прибор, работающий в ждущем режиме, который выдает результат в случайный момент времени $(t, t+dt)$. То обстоятельство, что операторная мера $\mathcal{M}(d\tau,\mu)$ зависит лишь от разности $\tau = x - t$ (координата на левой ветви светового конуса), а не отдельно от x и t, выражает тот факт, что если результат с какой-то вероятностью может быть получен в окрестности x в момент t, то с той же вероятностью он может быть получен в другой точке x', но в момент $t' = x' - x + t$. Размер доступной области на световом конусе определяет время получения окончательного результата. Далее для краткости будем называть измерение с исходами в доступной области Ω на световом конусе измерением во временном окне $\Omega = (-T,T)$ (результат не может быть получен наблюдателем быстрее, чем за время T [12]). Вероятность правильной идентификации состояний с ортогональными поляризациями во временном окне $(-T,T)$ равна [5]

$$p = p(0|0) = p(1|1) = \frac{1}{2}\left(1 + \mathrm{Tr}\{\mathcal{M}(\Omega,\mu)|\varphi_\mu\rangle\langle\varphi_\mu|\}\right) = \frac{1}{2}\left(1 + \int\limits_{-T}^{T} |\varphi(\tau)|^2 d\tau\right), \tag{13}$$

и, соответственно, вероятность ошибки

$$1 - p = p(0|1) = p(1|0) = 1 - p(0|0) = 1 - p(1|1). \tag{14}$$

Отметим, что если бы мы имели дело с двумя протяженными в пространстве классическими сигналами (электромагнитной волной с двумя ортогональными состояниями поляризации), для их достоверного различения было бы достаточно любой сколь угодно малой области, где сигнал присутствует. Для квантовых состояний фактически из-за того, что вектор состояния должен быть нормирован ($\int\limits_{-\infty}^{\infty} |\varphi(x,t)|^2 dx = \int\limits_{-\infty}^{\infty} |\varphi(x,t')|^2 dx = 1$, t и t' любые), для локально ортогональных состояний вероятность правильного различения пропорциональна доле интеграла нормировки, которая набирается в доступной для измерения области. По этой же причине коллективные измерения не дают большей вероятности различения, чем индивидуальные.

Пропускная способность из-за ортогональности состояний (точнее, их локальной ортогональности) дается формулой для классического симметричного бинарного канала:

$$C(p) = 1 - C_H(p), \quad C_H(p) = -(1-p)\log_2(1-p) - p\log_2 p. \tag{15}$$

Если нет никаких ограничений на свойства квантового канала, то можно посылать через него сколь угодно сильнолокализованные по τ состояния. В этом случае то, что состояния можно детектировать со сколь угодно малой ошибкой в сколь угодно малом временном окне $(-T,T)$, означает, что их можно передавать со сколь угодно высокой скоростью. Точнее говоря, для любого заранее выбранного $T < \varepsilon$, и $\delta > 0$ состояние может быть выбрано так, чтобы вероятность правильного различения была сколь угодно близка к единице:

$$p = \frac{1}{2}\left(1 + \int\limits_{-T}^{T} |\varphi(\tau)|^2 d\tau\right) > 1 - \delta, \quad \delta \to 0. \tag{16}$$

Будем теперь считать, что полоса пропускания канала ограничена интервалом энергий $\Delta\omega = \Delta k$ ($c = 1$ – скорость света). Само положение окна пропускания по оси энергий несущественно. Задача при этом сводится к нахождению оптимальной формы состояния $\varphi(k)$ ($\varphi(\tau)$, при которой при заданной полосе пропускания канала и выбранной скорости передачи $1/T$ достигается максимальная пропускная способность $C(p)$ (достигается максимум вероятности регистрации состояния во временном окне $(-T, T)$). Таким образом, требуется найти состояния, на которых достигается максимум функционала:

$$\mathcal{F}(|\varphi\rangle) = \max_{\mathrm{supp}|\varphi\rangle\in\Delta k} \frac{\mathrm{Tr}\{\mathcal{M}(\tau\in(-T,T))|\varphi\rangle\langle\varphi|\}}{\||\varphi\rangle\|^2} =$$

$$= \max_{\mathrm{supp}|\varphi\rangle\in\Delta k} \frac{\frac{1}{2\pi}\int\limits_{-T}^{T}|\varphi(\tau)|^2 d\tau}{\int\limits_{\Delta k}|\varphi(k)|^2 dk}. \qquad (17)$$

Вариация функционала $\delta\mathcal{F}/\delta\varphi = 0$ приводит к интегральному уравнению

$$\lambda_n\varphi_n(k) = \frac{1}{\pi}\int\limits_{\Delta k}\varphi_n(k')\frac{\sin(k-k')T}{(k-k')}dk'. \qquad (18)$$

Максимальное собственное число дает максимум функционала, а собственная функция этого собственного числа дает оптимальную форму состояния. Данное уравнение исследовалось ранее в работах [13,14], 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 [13] (при больших значениях параметра $\Delta k \cdot T$ они быстро стремятся к единице, например, при $\Delta k \cdot T = 4$, $\lambda_0 = 0.99589$). Известна также асимптотика при *фиксированном номере* n от параметра $\Delta k \cdot T \to \infty$ [14]:

$$\lambda_n(c) \sim 1 - \frac{4\sqrt{\pi}8^n}{n!}c^{n+1/2}e^{-2c}, \quad c = \Delta k \cdot T, \qquad (19)$$

то есть собственные числа экспоненциально близки единице. Последнее означает, что ошибка при различении ортогональных состояний при большом временном окне ($T \gg 1/\Delta k$) экспоненциально мала, а пропускная способность канала экспоненциально близка к единице.

Согласно стандартной трактовке пропускной способности, последняя означает, что найдется случайный код со "скоростью" передачи R, сколь угодно близкой к C, но $R < C$, который позволит при достаточно длинной последовательности передавать информацию в C классических бит в пересчете на одну посылку со сколь угодно малой вероятностью ошибки. При этом, как мы видим, каждая посылка и измерение происходят со скоростью в реальном времени $1/T$. Скорость генерации одного бита в ключе в физическом времени есть $C(\lambda_0(\Delta k{\cdot}T))/T$. Реально скорость передачи на неортогональных состояниях поляризации будет всегда несколько меньше, поскольку пропускная способность для неортогональных состояний всегда меньше, чем для ортогональных (при их одинаковой пространственной форме).

При малых значениях параметра $\Delta k{\cdot}T \ll 1$ собственное число $\lambda_0 \sim \Delta k \cdot T$, и пропускная способность $C \sim (\Delta k \cdot T)^2 \ll 1$.

Перейдем теперь к скорости генерации ключа в криптосистеме на протяженных ортогональных состояниях [5]. В случае ортогональных состояний их неразличимость для подслушивателя и возможность детектировать любые попытки подслушивания основаны на том, что состояние никогда единовременно не присутствует в канале связи целиком и что существует предельная скорость распространения. На первый взгляд, из-за того, что приходится использовать состояния, которые имеют протяженные носители в пространстве-времени, может показаться, что генерация ключа в реальном времени будет более медленной. Однако оказывается, что при данной полосе пропускания квантового канала связи теоретический максимум генерации секретного ключа достигается как раз для криптосистемы на ортогональных протяженных состояниях, а не для криптосистемы на неортогональных состояниях. Прежде чем показать данный факт, приведем интуитивные наводящие соображения. Протяженность состояния не может быть меньше длины канала $L_{ch} = cT_{ch}$ [5]. Это означает, что состояние должно быть достаточно узкополосным ($\Delta k_{ch} < 1/T_{ch}$). При данной полосе пропускания Δk можно посылать одновременно N состояний с ортогональными поляризациями и неперекрывающимися носителями в k-пространстве ($N \sim \Delta k/\Delta k_{ch}$). Детектирование каждого состояния требует временного окна не меньше, чем T_{ch}, но при этом передаются сразу N состояний по независимым каналам. Физическое время на один бит в ключе $T \sim N \cdot T_{ch} = N/\Delta k_{ch} = N/N \cdot \Delta k$, что совпадает с предыдущим случаем. Причем разбиение частотной полосы Δk можно произвести на любое число независимых каналов, лишь бы полоса каждого из них не была слишком велика (не более $\Delta k_{ch} < 1/T_{ch}$). Фактически такое разбиение аналогично мультиплекси-

рованию в классическом случае. Канал в этом случае представляет собой N независимых каналов с полосой пропускания δk_i ($\delta k_i \bigcap \delta k_j = \emptyset, \bigcup_i \delta k_i = \Delta k$) каждый. Далее все δk_i будем считать одинаковыми. В каждый канал параллельно посылаются N состояний $\{|\varphi_\mu^i\rangle\}$, где $|\varphi_\mu^i\rangle = \int\limits_{\delta k_i} dk\varphi(k)|k,\mu\rangle$.

Разложение единицы, описывающее измерение в подпространстве, натянутом на обобщенные векторы $|k,\mu\rangle$, $k \in \Delta k$, имеет вид

$$I(\Delta k) = \bigoplus_{i=1\ldots N} I(\delta k_i),\ I(\delta k_i) = \bigoplus_{\mu=0,1} \int\limits_{\delta k_i} \frac{dk}{k} |k,\mu\rangle\langle\mu,k|. \tag{20}$$

Детектирующие операторы для каждого канала имеют вид

$$I(\delta k_i) = \bigoplus_{\mu=0,1} \left(\mathcal{M}_i(\Omega_\delta,\mu) + \mathcal{M}_i(\overline{\Omega}_\delta,\mu)\right), \quad \Omega_\delta = (-T_\delta, T_\delta),\ \ \overline{\Omega}_\delta = (-\infty,\infty) - \Omega_\delta, \tag{21}$$

$$\mathcal{M}_i(\Omega_\delta,\mu) = \int\limits_{-T_\delta}^{T_\delta} \frac{d\tau}{2\pi} \left(\int\limits_{\delta k_i} dk \mathrm{e}^{ik\tau}|k,\mu\rangle\right)\left(\int\limits_{\delta k_i} dk' \langle k',\mu|\mathrm{e}^{-ik'\tau}\right) \tag{22}$$

и аналогично для $\mathcal{M}_i(\overline{\Omega}_\delta,\mu)$. Вероятность правильной идентификации состояний в каждом канале во временном окне $(-T_\delta, T_\delta)$ дается выражением

$$p_i = p(0_i|0_i) = p(1_i|1_i) = \frac{1}{2}\left(1 + \mathrm{Tr}\{\mathcal{M}_i(\Omega_\delta,\mu)|\varphi_\mu^i\rangle\langle\varphi_\mu^i|\}\right) = \frac{1}{2}\left(1 + \lambda_0(\delta k_i \cdot T_\delta)\right), \tag{23}$$

здесь 0_i и 1_i соответствуют 0 и 1 в каждом канале. Максимум p_i в каждом канале (и, соответственно, минимум ошибки) достигается на состояниях, дающих максимум функционала, аналогичного (17), с заменой $\Delta k \to \delta k_i$ и $T \to T_\delta$.

Поскольку собственные числа интегрального уравнения (18) зависят лишь от произведения полосы пропускания на временное окно, то суммарная пропускная способность по всем N независимым каналам дается выражением

$$\sum_{i=1}^{N} C(\lambda_0(\delta k_i \cdot T_\delta)) = N \cdot C(\lambda_0(\delta k_i \cdot T_\delta)). \tag{24}$$

Поскольку полосы пропускания отдельных каналов одинаковы, $\delta k_i = \Delta k/N$ и верхняя граница δk_i определяется длиной канала связи, то выбирая временное окно $T_\delta = T \cdot N$, приходим к тому, что для передачи одного секретного бита при достаточно длинной последовательности по одному из каналов со сколь угодно малой ошибкой требуется физическое время

$$T_N = \frac{T \cdot N}{N \cdot C(\lambda_0(\delta k_i \cdot T_\delta))} = \frac{T}{C(\lambda_0(\Delta k \cdot T))}. \tag{25}$$

Поскольку состояния могут передаваться параллельно сразу по N независимым каналам, то на один бит требуется время $T = T_N/N$, что совпадает с предыдущим случаем.

Данные формулы надо понимать в асимптотическом смысле. Поскольку состояния в отдельных частотных каналах или отдельных посылках становятся ортогональными (достоверно различимыми) только в асимптотическом пределе (соответственно, неортогональные операторнозначные меры $\mathcal{M}(\tau \in (-T,T))$ становятся ортогональными проекторами $I(\Delta k)$),

$$I(\Delta k) = \lim_{\Delta k \cdot T \to \infty} \bigoplus_{\mu=0,1} \mathcal{M}(\tau \in (-T,T)). \tag{26}$$

Однако выход на предел происходит экспоненциально быстро по параметру $\Delta k \cdot T$. Поэтому формулами для пропускной способности канала можно реально пользоваться уже при $\Delta k \cdot T \approx 2$. Поскольку пропускная способность является только функцией $\Delta k \cdot T$, то удобнее ввести безразмерную величину $C(\lambda_0(\Delta k \cdot T))/\Delta k \cdot T$, которая может быть интерпретирована как число бит в единицу частотной полосы и в единицу времени. Значения этой величины для нескольких значений параметра $\Delta k \cdot T$ приведены ниже (собственные числа λ_0 взяты из численных расчетов [12]). При больших $\Delta k \cdot T \approx 2$ пропускная способность экспоненциально близка к $C(\lambda_0(\Delta k \cdot T))/\Delta k \cdot T \propto 1/\Delta k \cdot T$:

$\Delta k \cdot T$:	0.5	1.0	2.0	4.0
$\frac{C(\lambda_0(\Delta k \cdot T))}{\Delta k \cdot T}$:	0.14067	0.25148	0.33684	0.24467

Выражение для скорости генерации ключа, когда пространственные амплитуды состояний в последовательных посылках перекрываются, по-видимому, не может быть получено без рассмотрения конкретной модели квантового канала связи.

Для случая неортогональных состояний, так же как для криптографии на ортогональных состояниях, могут быть использованы состояния с протяженными носителями (с произвольной эффективной протяженностью, больше или меньше длины канала связи), которые одновременно посылаются в канал связи в мультиплексном режиме. Предельная скорость генерации ключа при этом будет определяться тем же

выражением, поскольку она зависит лишь от произведения $\Delta k \cdot T$, и будет меньше, чем для ортогональных состояний.

Отметим в заключение, что выражение для безразмерной скорости генерации секретного ключа $C(\lambda_0(\Delta k \cdot T))/\Delta k \cdot T$ является лоренц-инвариантным (остается одинаковым в разных инерциальных системах отсчета), что может быть показано детально аналогично тому, как это делалось в [15]. Данный факт следует из лоренц-инвариантности скалярного $\hat{k} \cdot \hat{x} = kx - k_0 t$ ($c = 1$, $k_0 = |k|$), для фотона распространяющегося в одном направлении $k_0 = k$ ($k > 0$). При переходе в другую инерциальную систему отсчета $k' = (k - \beta k_0)/\sqrt{1-\beta^2} = k\sqrt{(1-\beta)/(1+\beta}$, и поскольку для безмассового поля время и координата входят лишь в комбинации $T' = x' - t'$ и $T = x - t$, то $T' = (x + \beta t)/\sqrt{1-\beta^2} - (t + \beta x)/\sqrt{1-\beta^2} = T\sqrt{(1+\beta)/(1-\beta)}$. Поэтому произведение $\Delta k \cdot T = \Delta k' \cdot T'$ остается лоренц-инвариантным.

Выражаю благодарность К. А. Валиеву, С. С. Назину, Ю. И. Ожигову, Л. А. Федичкину, В. Н. Яшникову за обсуждения и замечания.

Работа поддержана Российским фондом фундаментальных исследований (проект # 02-02-16289), а также проектом "Квант" (37.029.1.1.0031).

1. C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992); C. H. Bennett, G. Brassard, and N.D.Mermin, Phys. Rev. Lett. **68**, 557 (1992).
2. Н. Н. Боголюбов, А. А. Логунов, А. И. Оксак, И. Т. Тодоров, *Общие принципы квантовой теории поля*, М.: Наука, 1987.
3. A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
4. L. Goldenberg and L. Vaidman, Phys. Rev. Lett. **75**, 1239 (1995); quant-ph/9506030.
5. S. N. Molotkov and S. S. Nazin, quant-ph/106046, JETP Lett. **73**, 682 (2001).
6. A. S. Holevo, Problems of Information Transmission **9**, 177 (1973).
7. А. С. Холево, Успехи мат. наук **53**, 193 (1998).
8. C. E. Shannon, Bell Syst. Techn. J. **27**, 3397 (1948); **27**, 623 (1948).
9. P.Hausladen, R. Jozsa, B. Schumacher et al., Phys. Rev. **A54**, 1869 (1996).
10. И. М. Гельфанд, Н. Я. Виленкин, *Некоторые применения гармонического анализа. Оснащенные гильбертовы пространства (Обобщенные функции, вып.4)*, М.: Физматгиз, 1961.
11. N. Wiener and R. Palley, *Fourier Transform in the Complex Domain*, American Mathematical Society, New York, 1934.
12. С. Н. Молотков, С. С. Назин, *О релятивистских ограничениях на различимость ортогональных квантовых состояний*, ЖЭТФ N6 (2002), в печати.
13. D. Slepian and H. O. Pollak, Bell Syst. Techn. J. **XL**, 40 (1961).
14. W. H. Fuchs, J. of Mathem. Analysis and Appl. **9**, 317 (1964).
15. С. Н. Молотков, Письма в ЖЭТФ **74**, 477 (2001).