Письма в ЖЭТФ, том 74, вып. 10, с. 580 – 585

Об эффективности повторителей на ЭПР эффекте для квантовой криптографии в канале с затуханием

С. Н. Молотков

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

Поступила в редакцию 30 октября 2001 г.

Приведены соображения, основанные на фундаментальном неравенстве Холево, а также на прямых вычислениях о том, что в канале с затуханием требуется экспоненциально большое число посылок на один бит в ключе с ростом длины канала. Показано, что результаты недавней работы (L.-M.Duan, M.Lukin, J.I.Cirac, P.Zoller [4]) о том, что экспоненциальный рост ресурсов для квантовой криптографии в канале с затуханием может быть, путем генерации сквозной ЭПР пары, сведен с полиномиальному, не верен. Поэтому результаты [4] не решают принципиальной проблемы, ограничивающей практическое применение квантовой криптографии на расстояниях превышающих длину затухания.

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

Квантовая криптография позволяет в принципе обеспечить безусловную секретность распространения ключа между пространственно удаленными пользователями [1,2]. Одним из основных ограничителей при практическом использовании квантовых криптосистем на больших расстояниях является затухание в оптоволокне. Для стандартных оптоволоконных линий расстояние, на котором могут работать квантовые криптосистемы, ограничено несколькими десятками километров [3]. Экспоненциальный рост числа посылок с длиной канала на один бит на приемном конце оказывается неприемлемым при практическом использовании. Недавно появилась работа [4], где предложена квантовая криптосистема с повторителями на ЭПР состояниях, в которой, по утверждению [4], требуются лишь полиномиальные ресурсы с ростом расстояния. Если бы это было так, то вопрос об использовании квантовой криптографии на больших расстояниях можно было бы считать в принципе решенным. К сожалению, утверждение работы [4], на наш взгляд, является ошибочным. В классических коммуникационных оптоволоконных системах проблема затухания решается при помощи повторителей, действие которых сводится к измерению классического сигнала, созданию копии с большей интенсивностью (усилению) и передаче на следующий узел. В квантовом случае, если информационные состояния принадлежат к неортогональному базису, копирование невозможно [5]. Поэтому распространение ключа цепочке от узла к узлу приводит к экспоненциальному уменьшению его длины даже в идеальном канале. Этот факт следует из неравенства Холево [6]. Взаимная информация о ключе между двумя узлами принципиально ограничена величиной

$$I(x;y) \leq \mathrm{Tr}\{\rho\log\rho\} - \sum_i p_i \mathrm{Tr}\{\rho_i \log\rho_i\}, \qquad (1)$$

где p_i – априорная информация появления i символа (состояния ρ_i) из алфавита на входе. Для бинарного канала (алфавит x, y состоит из двух символов, 0 и 1) взаимная информация между входом и выходом канала связи равна

$$I(x;y) \leq 1, \qquad (2)$$

причем равенство достигается тогда и только тогда, когда состояния ρ_i коммутируют (для чистых состояний это означает, что они ортогональны). Поэтому при передаче ключа по цепочке от узла к узлу взаимная информация (длина ключа) убывает экспоненциально даже в идеальном канале:

$$I(n) \propto (I(x;y))^n, \qquad (3)$$

здесь n – число узлов.

Обратим здесь внимание на то, что в релятивистском случае в квантовой криптографии могут быть использованы ортогональные состояния [7, 8]. В этом случае распространение ключа по цепочке в идеальном канале не приводит к уменьшению длины ключа, поскольку $I(x;y) = 1$. По этой причине релятивистские квантовые криптосистемы в конечном счете могут оказаться более эффективными для применений. Таким образом, для ортогональных состояний из-за их классичности в смысле различимости достигается максимум взаимной информации. Для неортогональных состояний взаимная информация всегда меньше

единицы. Поэтому рассмотрим канал с затуханием для ортогональных состояний, то есть канал, действие шума в котором сводится к тому, что ортогональные состояния достигают выхода с определенной вероятностью, зависящей от длины. Емкость бинарного канала связи (количество бит, которое может быть передано со сколь угодно малой ошибкой) определяется как максимум взаимной информации по всевозможным входным состояниям:

$$C_H = \max_{\{p_i,\rho_i\}} I(x;y), \tag{4}$$

где взаимная информация

$$I(x;y) = S(x) - H(p), \tag{5}$$

$S(x)$ – входная шенноновская информация:

$$S(x) = -\sum_{x=0,1} p(x)\log_2 p(x) = 1, \quad p(0) = p(1) = \frac{1}{2}, \tag{6}$$

и $H(p)$ – энтропийная функция:

$$H(p) = -p\log_2 p - (1-p)\log_2(1-p), \tag{7}$$

где p – условная вероятность:

$$p(x=0|y=0) = p(x=1|y=1) = \\ = 1 - p = \frac{1}{2}(1+p(L)),$$

$$p(x=0|y=1) = p(x=1|y=0) = p = \frac{1}{2}(1-p(L)), \tag{8}$$

$p(L) = 1\cdot\exp(-L)$ – вероятность достичь приемного конца, L – длина канала связи. Переходные вероятности в (8), например $p(x=0|y=0)$, означают, что если было послано состояние, отвечающее нулю, то вероятность правильного детектирования есть $1\cdot p(L) + (1/2)(1-p(L))$. Первое слагаемое есть вероятность достичь приемного конца ($p(L)$), умноженная на вероятность правильного различения, которая равна единице для ортогональных состояний. Второе слагаемое описывает случай, когда состояние не достигает приемного конца (вероятность $1-p(L)$). В этом случае вероятность правильной идентификации при отсутствии состояния на выходе равна $1/2$ – вероятности простого угадывания. Аналогично для других переходных вероятностей в (8). Для емкости канала от длины имеем

$$C_H(L) = 1 - H(p) = -\frac{1}{2}[(1+p(L))\log_2(1+p(L)) + \\ + (1-p(L))\log_2(1-p(L))] \approx p^2(L) = e^{-2L}. \tag{9}$$

Ошибка на приемном конце фактически связана с отсутствием состояния. Из-за экспоненциально малой емкости канала при больших L на один бит на приемном конце требуется передать экспоненциально много входных состояний. Данная емкость канала, диктуемая неравенством Холево, относится к случаю, когда состояния напрямую посылаются через канал связи. Если имеется заранее распределенная ЭПР пара между входным и приемным концами, то емкость канала может быть другой (см., например, [9,10]). Авторами [4] предлагалось распространить ЭПР пару между входом и выходом канала, используя процесс переброса запутанности по цепочке между соседними ЭПР парами, сгенерированными на промежуточных узлах. При этом сделано ошибочное утверждение, что такой процесс будет требовать полиномиальных, а не экспоненциальных ресурсов в зависимости от длины. Дело в том, что даже если в канале нет других процессов декогерентности и имеется лишь затухание, и даже если ЭПР пары в каждом промежуточном узле генерируются с вероятностью единица, то все равно процесс генерации результирующей ЭПР пары между концами канала требует экспоненциально большого числа попыток. Данное обстоятельство связано с тем, что при переброске запутанности между двумя соседними сегментами требуется совместное измерение пар фотонов из левой и правой ЭПР пар. Измерение будет успешным, если каждый фотон достигнет измерительного устройства. Причем вероятность сразу обоим фотонам из соседних ЭПР пар достичь измерительного устройства равна произведению вероятностей для отдельных фотонов p_1. Из-за затухания данная вероятность зависит от длины сегментов экспоненциально – $p_1 \propto \exp(-L_s)$. Для успешной генерации сквозной ЭПР пары между входом и выходом требуется, чтобы измерения, осуществляющие переброс запутанности, были успешными на **всех** сегментах, что приводит к тому, что вероятность успешной генерации сквозной ЭПР пары $\propto \exp(-nL_s)$ (n – число сегментов, $nL_s = L$ – полная длина канала). Понятие экспоненциального затухания в зависимости от длины канала связи подразумевает, что будут проводиться локальные в координатном пространстве измерения. Точнее говоря, характерные размеры области, в которой проводится измерение, должны быть существенно меньше длины затухания. В классическом случае это означает, что такие локальные измерения сигнала в окрестностях точек, удаленных на некоторую длину, будут давать результат, вероятность которого убывает экспоненциально от расстояния между этими точками. При рассмотрении квантовых состояний, которые описы-

ваются векторами в гильбертовом пространстве требуется "привязка" этих состояний к пространству-времени Минковского. Когда подразумеваются измерения в малых пространственных областях без явного введения подобной "привязки", то есть оставаясь только в гильбертовом пространстве (например, как это делается в [4]), также невозможно осмысленно ввести понятие экспоненциального затухания в зависимости от длины. Будем рассматривать одномерную ситуацию. Одночастичное состояние безмассовой релятивистской частицы (фотона) порождается операторнозначными обобщенными функциями $\varphi^+(\hat{x})$ [11], удовлетворяющими коммутационным соотношениям

$$[\varphi^-(\hat{x}),\varphi^+(\hat{x}')]=0, \tag{10}$$

если $\hat{x}\sim\hat{x}'$ пространственно-подобны. Физические нормированные состояния ($|\psi\rangle\in\mathcal{H}$) определяются как результат сглаживания операторных обобщенных функций с основными функциями $\psi(\hat{x})$ (см. детали в [11])

$$|\psi\rangle=\int d\hat{x}\psi(\hat{x})\varphi^+(\hat{x})|0\rangle=\int_{-\infty}^{\infty}\frac{dk}{k_0}\psi(k,k_0=|k|)|\hat{k}\rangle,$$

$$\begin{gathered}\varphi^+(\hat{x})=\frac{1}{\sqrt{2\pi}}\int d\hat{k}\mathrm{e}^{i\hat{k}\hat{x}}\delta(\hat{k}^2)\theta(k_0)a^+(\hat{k}),\\ \psi(\hat{k})=\psi(k,k_0)=\int d\hat{x}\mathrm{e}^{-i\hat{k}\hat{x}}\psi(\hat{x}),\\ a^+(\hat{k})|0\rangle=|\hat{k}\rangle,\quad \langle\hat{k}|\hat{k}'\rangle=k_0\delta(k-k').\end{gathered} \tag{11}$$

Для состояний распространяющихся в одном направлении, которые используются при передаче информации по каналам связи, значение амплитуды $\psi(k,k_0=|k|)$ на массовой поверхности содержит лишь компоненты с $k>0$. Поляризационную структуру состояний пока не учитываем.

Эволюция состояний в идеальном канале связи представляет собой трансляцию в пространстве-времени Минковского ($\hat{x}=(x,x_0)$), описывается оператором трансляций в группе Пуанкаре и является аналогом оператора эволюции во времени: $U(t)=\exp(-iHt)$ в нерелятивистском случае. Трансляция состояния на вектор $\hat{a}=(a,a_0)$ дается выражением

$$|\psi(\hat{a})\rangle=\hat{\mathbf{T}}(\hat{a})|\psi\rangle=\int d\hat{x}\psi(\hat{x})\hat{\mathbf{T}}(\hat{a})\varphi^+(\hat{x})\hat{\mathbf{T}}^{-1}(\hat{a})\hat{\mathbf{T}}(\hat{a})|0\rangle. \tag{12}$$

С учетом инвариантности вакуумного вектора $\hat{\mathbf{T}}(\hat{a})|0\rangle=|0\rangle$ имеем

$$\begin{aligned}\hat{\mathbf{T}}(\hat{a})\varphi^+(\hat{x})\hat{\mathbf{T}}^{-1}(\hat{a})&=\varphi(\hat{x}+\hat{a}),\\ \hat{\mathbf{T}}(\hat{a})a^+(\hat{k})\hat{\mathbf{T}}^{-1}(\hat{a})&=e^{i\hat{k}\hat{a}}a^+(\hat{k}).\end{aligned} \tag{13}$$

Измерение, связанное с обнаружением частицы в окрестности точки $(x,x+dx)$ в момент времени x_0, описывается разложением единицы:

$$\begin{aligned}I=\int_{-\infty}^{\infty}dx\left(\int_{-\infty}^{\infty}\frac{dk}{\sqrt{k_0}}\mathrm{e}^{-i\hat{k}\hat{x}}|\hat{k}\rangle\right)\times\\ \times\left(\int_{-\infty}^{\infty}\frac{dk'}{\sqrt{k_0'}}\langle\hat{k}'|\mathrm{e}^{i\hat{k}'\hat{x}}\right)=\int_{-\infty}^{\infty}\mathcal{M}(\hat{x},dx),\end{aligned} \tag{14}$$

соответственно вероятность

$$\begin{aligned}\Pr\{\hat{x},dx\}=\mathrm{Tr}\{\mathcal{M}(\hat{x},dx)|\psi(\hat{a})\rangle\langle\psi(\hat{a})|\}=\\ =\left|\psi(\hat{x}+\hat{a})\right|^2dx,\end{aligned} \tag{15}$$

$$\psi(\hat{x}+\hat{a})=\int_0^{\infty}\frac{dk}{\sqrt{k_0}}\psi(k,k_0=|k|)\mathrm{e}^{i\hat{k}(\hat{x}+\hat{a})}.$$

Для состояний распространяющихся в одном направлении ($k>0$, $k_0=k$) вероятность зависит лишь от разности $x-x_0$

$$\begin{gathered}\Pr\{x-x_0,dx\}=\left|\psi(x-x_0+(a-a_0))\right|^2dx,\\ \psi(x-x_0)=\int_0^{\infty}\frac{dk}{\sqrt{k}}\mathrm{e}^{ik(x-x_0)}\psi(k,k).\end{gathered} \tag{16}$$

Если имеется канал с затуханием, то оператор трансляции в (12), (13) должен быть заменен на $\hat{\mathbf{S}}(\hat{a})$-матрицу, которая является аналогом нерелятивистского инструмента (супероператора). В идеальном канале $\hat{\mathbf{S}}(\hat{a})$-матрица совпадает с оператором трансляции. Супероператор может быть представлен в виде [12]

$$\hat{\boldsymbol{\mathcal{T}}}_{\hat{a}}[...]=\hat{\mathbf{S}}(\hat{a})[...]\hat{\mathbf{S}}^+(\hat{a}). \tag{17}$$

Действие $\hat{\mathbf{S}}^+(\hat{a})$ на состояние $|\psi\rangle$ при трансляции в канале с экспоненциальным затуханием означает, что матричные элементы $\hat{\mathbf{S}}(\hat{a})$ представимы в виде

$$\langle\hat{k}|\hat{\mathbf{S}}(\hat{a})|\hat{k}'\rangle=e^{-\gamma|a-a_0|+i\hat{k}\hat{a}}k_0\delta(k-k'), \tag{18}$$

в отличие от матричных элементов $\hat{\mathbf{S}}(\hat{a})$-матрицы (оператора трансляций (13)) в идеальном канале, которые имеют вид

$$\langle\hat{k}|\hat{\mathbf{T}}(\hat{a})|\hat{k}'\rangle=e^{i\hat{k}\hat{a}}k_0\delta(k-k'). \tag{19}$$

При этом вероятность обнаружить частицу в окрестности точки $(x,x+dx)$ в момент времени x_0 равна

$$\begin{aligned}\Pr_{decay}\{\hat{x},dx\}=e^{-\gamma a}\left|\psi(\hat{x}+\hat{a})\right|^2dx=\\ =\mathrm{e}^{-\gamma|a-a_0|}\Pr\{\hat{x},dx\},\end{aligned} \tag{20}$$

то есть вероятность обнаружения экспоненциально убывает по сравнению с соответствующей вероятностью в идеальном канале (15). Перейдем теперь к двухчастичному ЭПР состоянию. Запутанное по поляризациям двухчастичное состояние может быть представлено в виде

$$|\psi_{EPR}\rangle = \frac{1}{\sqrt{2}} \iint d\hat{x}_1 d\hat{x}_2 \psi(\hat{x}_1, \hat{x}_2) \times$$

$$\times [\varphi^+(\hat{x}_1, +)\varphi^+(\hat{x}_2, -)\varphi^+(\hat{x}_1, -)\varphi^+(\hat{x}_2, +)]|0\rangle =$$

$$= \frac{1}{\sqrt{2}} \iint d\hat{k}_1 d\hat{k}_2 \psi(\hat{k}_1, \hat{k}_2)\delta(\hat{k}_1^2)\delta(\hat{k}_2^2)\theta(k_{01})\theta(k_{02}) \times$$

$$\times [a^+(\hat{k}_1+)a^+(\hat{k}_2-) + a^+(\hat{k}_1-)a^+(\hat{k}_2+)]|0\rangle =$$

$$= \frac{1}{\sqrt{2}} \iint \frac{dk_1 dk_2}{k_{01}k_{02}} \psi\left(k_1, k_{01} = |k_1|; k_2, k_{02} = |k_2|\right) \times$$

$$\times \left(|\hat{k}_1+, \hat{k}_2-\rangle + |\hat{k}_1-, \hat{k}_2+\rangle\right). \qquad (21)$$

Здесь $\varphi^+(\hat{x}, \pm)$ – полевые операторы рождения для состояний с поляризациями $\pm$. Строго говоря, из-за наличия общего вакуумного вектора в системе тождественных частиц в общем случае невозможно представить измерение над двухчастичным состоянием в виде тензорного произведения [13]. Однако, если отдельные подсистемы имеют "метки", то осмысленно говорить об измерении над отдельными подсистемами, хотя само разложение единицы, описывающее измерение, не представляется в виде тензорного произведения. В нашем случае такой "меткой" может служить волновой вектор. Будем считать, что $k_1 > 0$, а $k_2 < 0$ (фотоны в ЭПР паре распространяются в разные стороны). Измерение, описываемое проекцией на определенное состояние поляризации, является нелокальным в координатном пространстве в том смысле, что результат с вероятностью сколь угодно близкой к единице может быть получен, если пространственная область, где проводится измерение, целиком накрывает пространственную часть амплитуды состояния. ЭПР корреляции для поляризаций при измерении в ограниченных областях пространства двумя наблюдателями описываются разложением единицы:

$$I_2 = \sum_{s_1,s_2=\pm} \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} \frac{dk_1 dk_2}{k_{01}k_{02}} |\hat{k}_1 s_1, \hat{k}_2 s_2\rangle\langle\hat{k}_2 s_2, \hat{k}_1 s_1| =$$

$$= \sum_{s_{1,2}=\pm} \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} dx_1 dx_2 \mathcal{M}(\hat{x}_1 s_1, \hat{x}_2 s_2), \qquad (22)$$

$$\mathcal{M}(\hat{x}_1 s_1, \hat{x}_2 s_2) =$$

$$= \left(\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} \frac{dk_1 dk_2}{\sqrt{k_{01}k_{02}}} e^{-i(\hat{k}_1\hat{x}_1 + \hat{k}_2\hat{x}_2)} |\hat{k}_1 s_1, \hat{k}_2 s_2\rangle\right) \times$$

$$\times \left(\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} \frac{dk_1' dk_2'}{\sqrt{k_{01'}k_{02}'}} e^{i(\hat{k}_1'\hat{x}_1 + \hat{k}_2'\hat{x}_2)} \langle\hat{k}_1' s_1, \hat{k}_2' s_2|\right).$$

Вероятность получения результата двумя наблюдателями в каналах поляризации σ_1 и σ_2 в окрестностях точек $(x_1, x_1 + dx_1)$ в момент x_{01} и $(x_2, x_2 + dx_2)$ в момент x_{02} по определению равна

$$\Pr\{\hat{x}_1\sigma_1, \hat{x}_2\sigma_2\} dx_1 dx_2 =$$

$$\mathrm{Tr}\{\mathcal{M}(\hat{x}_1\sigma_1, \hat{x}_2\sigma_2)|\psi_{EPR}\rangle\langle\psi_{EPR}|\} =$$

$$= (\delta_{\sigma_1,+}\delta_{\sigma_2,-} + \delta_{\sigma_1,-}\delta_{\sigma_2,-})|\psi(\hat{x}_1, \hat{x}_2)|^2 dx_1 dx_2, \qquad (23)$$

$$\psi(\hat{x}_1, \hat{x}_2) = \int_0^{\infty}\int_0^{\infty} \frac{dk_1 dk_2}{\sqrt{k_{01}k_{02}}} \times$$

$$\times e^{ik_1(x_1 - x_{01})} e^{-ik_2(x_2 + x_{02})} \psi(k_1, k_1, -k_2, -k_2). \qquad (24)$$

Первый сомножитель в (23) описывает ЭПР корреляции по поляризациям, а второй учитывает долю состояния, связанную с пространственной частью. Нет формальных запретов выбрать пространственную амплитуду таким образом, чтобы она была сильнолокализованной. Измерения, проводимые в ограниченных областях, будут давать полную корреляцию по состояниям поляризации (сомножитель в (23), отвечающий за пространственную часть состояния всегда близок к единице при интегрировании по сколь угодно малой области наблюдения – $\int\int dx_1 dx_2 |\psi(\hat{x}_1, \hat{x}_2)|^2 \approx 1$). Если использовать протяженные (почти монохроматические [4]) состояния, то второй сомножитель в (23) будет приводить к уменьшению вероятности корреляций при измерениях в ограниченных пространственных областях, меньших эффективной протяженности состояния. Будем считать, что амплитуда является сильнолокализованной. Пусть теперь в окрестностях отдельных узлов x_i в момент x_0 генерируются ЭПР пары, которые затем распространяются в узлы для измерений, связанных с перебросом запутанности. Имеем

$$|\psi_{i,i+1}\rangle = \frac{1}{\sqrt{2}} \int\int d\hat{x}_1 d\hat{x}_2 \psi(\hat{x}_1 - \hat{x}_i, \hat{x}_2 - \hat{x}_i) \times$$

$$\times [\varphi^+(\hat{x}_1+)\varphi^+(\hat{x}_2-) + \varphi^+(\hat{x}_1-)\varphi^+(\hat{x}_2+)]|0\rangle, \qquad (25)$$

причем считаем, что временной аргумент $\hat{x}_i = (x_i, x_{0i})$ одинаков при всех $i = 1, 2...n$ (ЭПР пары генерируются одновременно). Это не является существенным, но упрощает выкладки. Все расстояния между соседними узлами также считаем одинаковыми. Измерения по перебросу запутанности между соседними i и $i+1$ ЭПР состояниями проводятся в малых окрестностях узлов $\hat{y}_{i,i+1} = (y_{i,i+1}, y_0)$. Положительный исход измерения может возникнуть лишь в момент y_0 (из-за сильной локализации пространственной амплитуды), который определяется временем долета частиц из узлов, где генерируется ЭПР пара, до узлов, где проводятся измерения по перебросу запутанности. Измерения в окрестностях точек $\hat{y}_{i,i+1}$ по перебросу запутанности даются разложением единицы:

$$I_2 = \frac{1}{2}\sum_{s_{1,2},\alpha=\pm}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} dy_1 dy_2 \times$$

$$\times\left(\iint \frac{dk_1 dk_2}{\sqrt{k_{01}k_{02}}} e^{-i\hat{k}_1(\hat{y}_1-\hat{y}_{i,i+1})-i\hat{k}_2(\hat{y}_2-\hat{y}_{i,i+1})}\times\right.$$

$$\left.\times(|k_{i+1}s_1, \hat{k}_{i+2}s_2\rangle + \alpha|k_{i+1}-s_1, \hat{k}_{i+2}-s_2\rangle)\right)\times$$

$$\times\left(\iint \frac{dk_1' dk_2'}{\sqrt{k_{01}'k_{02}'}} \mathrm{e}^{i\hat{k}_1'(\hat{y}_1-\hat{y}_{i,i+1})+i\hat{k}_2'(\hat{y}_2-\hat{y}_{i,i+1})}\times\right.$$

$$\left.\times(\langle s_1\hat{k}_{i+1}, s_2\hat{k}_{i+2}| + \alpha\langle -s_1\hat{k}_{i+1}, -s_2\hat{k}_{i+2}|)\right) =$$

$$= \int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\mathcal{M}(\hat{y}_1-\hat{y}_{i,i+1}, \hat{y}_2-\hat{y}_{i,i+1}, dy_1 dy_2). \quad (26)$$

Эволюция состояний в канале с затуханием получается действием инструмента аналогично (17), (19) на каждую из частиц в ЭПР парах. Учитывая структуру $\psi(\hat{x}_1, \hat{x}_2)$, его действие сводится к

$$\hat{\mathbf{S}}_2(-\hat{a}, \hat{a})|\psi_{i,i+1}\rangle = \frac{1}{\sqrt{2}}\int_0^{\infty}\int_0^{\infty}\frac{dk_1 dk_2}{\sqrt{k_{01}k_{02}}}\times$$

$$\times\psi_1(k_1, k_1)\psi_1(k_2, k_2)e^{ik_1[(x_1+a)-(x_0+a_0)]-\gamma|a-a_)|}\times$$

$$\times e^{-ik_2[(x_2+a)-(x_0+a_0)]-\gamma|a+a_0|}(|\hat{k}_1+, \hat{k}_2-\rangle + |\hat{k}_1-, \hat{k}_2+\rangle), \quad (27)$$

что отвечает трансляции с затуханием одной из частиц в положительном, а второй, в отрицательном направлениях оси x. Образования сквозной ЭПР пары за счет переброса запутанности между всеми соседними парами имеет место только тогда, когда результаты измерений во всех промежуточных узлах дали положительный результат, вероятность которого дается выражением

$$\Pr\{\hat{x}_2-\hat{y}_{2,3}, \hat{x}_3-\hat{y}_{2,3}, \ldots \hat{x}_{n-1}-\hat{y}_{n-2,n-1}\}\times$$

$$\times dx_2 dx_3 \ldots dx_{n-2}dx_{n-1} =$$

$$= \mathrm{Tr}\left\{\left(\hat{\mathbf{S}}_2\rho_{1,2}\hat{\mathbf{S}}_2^+\right)\left(\hat{\mathbf{S}}_2\rho_{3,4}\hat{\mathbf{S}}_2^+\right)\ldots\left(\hat{\mathbf{S}}_2\rho_{n-1,n-2}\hat{\mathbf{S}}_2^+\right)\times\right.$$

$$\times\mathcal{M}(\hat{x}_2-\hat{y}_{2,3}\hat{x}_3-\hat{y}_{2,3}, dx_2dx_3)\ldots\times$$

$$\times\ldots\mathcal{M}(\hat{x}_{n-2}-\hat{y}_{n-2,n-1}, \hat{x}_{n-1}-$$

$$\left.-\hat{y}_{n-2,n-1}, dx_{n-2}dx_{n-1})\right\} =$$

$$= \left(e^{-\gamma a}\left|\psi_2(x_2-y_{2,3}-(x_0-y_0))\right|^2 dx_2\right)$$

$$\ldots\left(e^{-\gamma a}\left|\psi_{n-1}(x_{n-1}-y_{n-2,n-1}-(x_0-y_0))\right|^2 dx_{n-1}\right). \quad (28)$$

Считаем, что над крайними частицами 1 и n измерения не проводятся и они остаются свободными (по этим состояниям берется след с единичным оператором). Каждый из сомножителей описывает вероятность детектирования пары частиц из соседних ЭПР пар в промежуточных узлах. Положительный исход имеет место лишь при условии, что **все** детекторы сработали. Вероятность такого исхода есть

$$\Pr \propto e^{-n\gamma a} = e^{-\gamma L}, \quad L = n\cdot a, \quad (29)$$

и убывает экспоненциально, в отличие от утверждения работы [4] о степенном убывании с изменением длины канала. Последнее означает, что для создания сквозной ЭПР пары требуется экспоненциально большое число попыток генерации промежуточных ЭПР пар. По-видимому, единственный способ применения квантовой криптографии на больших расстояниях состоит в создании каналов связи на основе новых материалов с меньшей константой затухания по сравнению с имеющимися оптоволоконными системами.

Выражаю благодарность С. С. Назину за полезные обсуждения и замечания. Работа поддержана проектами “Физические основы квантовых вычислений”, “Электронные состояния” и Российским фондом фундаментальных исследований (# 02-02-16289).

1. C. H. Bennett and G.Brassard, *Quantum Cryptography: Public Key Distribution and Coin Tossing*, Proc.of IEEE Int. Conf. on Comput. Sys. and Sign. Proces., Bangalore, India, December 1984, p.175.

2. A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
3. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, quant-ph/0101098.
4. L.-M. Duan, M. Lukin, J. I. Cirac, and P. Zoller, quant-ph/0105105.
5. C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992); C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
6. A. S. Kholevo, Problems of Information Transmission, **9** 177 (1973).
7. L. Goldenberg and L. Vaidman, Phys. Rev. Lett. **75**, 1239 (1995); quant-ph/9506030.
8. S. N. Molotkov, S. S. Nazin, quant-ph/0008008, Письма в ЖЭТФ, **73**, 767 (2001).
9. C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliya, quant-ph/0160052.
10. A. S. Holevo, quant-ph/0106075.
11. Н. Н. Боголюбов, А. А. Логунов, А. И. Оксак, И. Т. Тодоров, *Общие принципы квантовой теории поля*, М.: Наука, 1987.
12. K. Kraus, *States, Effects and Operations*, Springer-Verlag, Berlin, 1983.
13. R. Laiho, S. N. Molotkov, and S. S. Nazin, Phys. Lett. **A275**, 36 (2000); Phys. Lett. **A278**, 9 (2000).