Письма в ЖЭТФ, том 73, вып. 12, с. 767 – 771 25 июня

Роль причинности в обеспечении безусловной секретности релятивистской квантовой криптографии

С. Н. Молотков, С. С. Назин

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

Поступила в редакцию 15 мая 2001 г.

Вопрос о безусловной секретности квантовой криптографии (секретности, которая гарантируется лишь фундаментальными законами природы, а не техническими ограничениями) является одним из центральных в квантовой теории информации. Предложена релятивистская квантовая криптосистема и показана ее безусловная секретность относительно любых попыток подслушивания. Соображения релятивистской причинности позволяют показать секретность криптосистемы простыми средствами. Кроме того, поскольку схема не использует коллективные измерения и квантовые коды, то она может быть реализована экспериментально уже на сегодняшнем уровне оптоволоконных технологий.

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

Идея квантовой криптографии была впервые высказана в работе [1]. Идея эта стала общедоступной после опубликования работы [2]. Существенное продвижение возникло после работ [3, 4]. В [3] предложен вариант криптосистемы на EPR-эффекте [5]. В работе [4] было показано, что для детектирования попыток подслушивания достаточно использовать любую пару неортогональных состояний. В дальнейшем было предложено большое число вариантов квантовых криптосистем и их реализаций [6]. На сегодняшний день существуют три варианта доказательства безусловной секретности. Доказательство [7] относится к так называемому протоколу BB84 [2], этому же протоколу посвящена работа [8]. Доказательство [9] относится к протоколу на EPR-эффекте [3], и в отличие от [7] требует наличия у легитимных пользователей квантового компьютера. В [10] сделана попытка упрощения упомянутых доказательств путем явного введения в схему квантовых кодов. Первая релятивистская схема квантовой криптографии была предложена в [11]. Набросок доказательства безусловной секретности данной схемы содержится в [12]. Впервые ограничения, накладываемые на измеримость квантовых состояний в релятивистской области обсуждались в работе Ландау и Пайерлса еще в 1931 г. [13]. Дальнейшее исследование было предпринято в работе Бора и Розенфельда [14].

Протокол секретен, если для *любого* $N \geq 1$ *и любых* $\varepsilon_1 > 0$ и $\varepsilon_2 > 0$ его параметры (используемые состояния, измерения и т.д.) могут быть выбраны так, что:

1) Вероятность того, что строки $s_A(N)$ и $s_B(N)$ отличаются хотя бы в одном бите, меньше $\varepsilon_1 > 0$, то есть

$$\Pr\{s_A(N) \neq s_B(N)\} \leq \varepsilon_1, \tag{1}$$

другими словами (в терминах взаимной информации между A и B), для любого $\varepsilon_1' > 0$ можно добиться того, чтобы выполнялось неравенство

$$I(A;B) \geq N - \varepsilon_1'; \tag{2}$$

2) вероятность того, что подслушивателю E известна строка $s_A(N)$, превосходит вероятность простого угадывания 2^{-N} не более чем на ε_2:

$$\Pr\{s_A(N) = s_E(N)\} \leq 2^{-N} + \varepsilon_2, \tag{3}$$

это эквивалентно тому, что он имеет сколь угодно малую информацию о строках $s_A(N)$ и $s_B(N)$, принятых как ключ длины N легитимными пользователями:

$$I(A;E) \leq \varepsilon_2, \quad I(B;E) \leq \varepsilon_2. \tag{4}$$

Если требуется передать один бит классической информации, то состояниям классических битов 0 и 1 участник A сопоставляет квантовые состояния с матрицами плотности ρ_0 и ρ_1 (которые могут выбираться с априорными вероятностями π_0 и π_1, $\pi_0 + \pi_1 = 1$. Измерения описываются разложениями единицы в пространстве состояний – $\sum_i E_i = I$. Доступная информация у B о бите A в результате измерений определяется как максимальная взаимная информация по всевозможным измерениям:

$$I(A;B,\rho_0;\rho_1) =$$
$$= \max_{\{E_i\}} \sum_i \left\{ \pi_0 \mathrm{Tr}\{\rho_0 E_i\} \log_2 \left(\frac{\mathrm{Tr}\{\rho_0 E_i\}}{\mathrm{Tr}\{\rho E_i\}} \right) + \right.$$
$$\left. + \pi_1 \mathrm{Tr}\{\rho_1 E_i\} \log_2 \left(\frac{\mathrm{Tr}\{\rho_1 E_i\}}{\mathrm{Tr}\{\rho E_i\}} \right) \right\}. \tag{5}$$

Существует фундаментальная верхняя граница на доступную информацию, которая дается неравенством, доказанным в работе Холево [15] (см. также [16]):

$$I(A;B,\rho_0;\rho_1) \le S_{vN}(\rho) - \textstyle\sum_{i=0,1}\pi_i S_{vN}(\rho_i),$$
$$S_{vN}(\rho) = -\mathrm{Tr}\{\rho\log(\rho)\}, \tag{6}$$

$S_{vN}(\rho)$ – энтропия фон Неймана [17], причем равенство достигается тогда, и только тогда, когда матрицы плотности ρ_0 и ρ_1 коммутируют. Для чистых состояний последнее означает, что равенство в (4) достигается только для ортогональных состояний ($\rho_{0,1} = |\psi_{0,1}\rangle\langle\psi_{0,1}|$ и $\langle\psi_0|\psi_1\rangle = 0$). В этом случае доступная информация достигает максимального значения

$$I^{\max}(A;B,\rho_0;\rho_1) = 1$$
$$E_0 = \mathcal{P}_0 = |\psi_0\rangle\langle\psi_0|, \quad E_1 = \mathcal{P}_1 = |\psi_1\rangle\langle\psi_1|. \tag{7}$$

Поэтому ниже мы примем простую одномерную модель, которая содержит необходимые ограничения, диктуемые соображениями релятивистской причинности [18].

Легитимные пользователи контролируют пространственно-удаленные области Ω_A и Ω_B протяженности L. Участник A в момент начала протокола $t_A = 0$ приготавливает равновероятно одно из двух ортогональных состояний, отвечающих 0 или 1, следующего вида:

$$|\psi_{0,1}\rangle = \int_0^\infty dk\mathcal{F}(k)a^+_{0,1}(k)|0\rangle =$$
$$= \int_0^\infty dk\mathcal{F}(k)|k,e_{0,1}\rangle = |\mathcal{F},e_{0,1}\rangle, |k,e_{0,1}\rangle = a^+_{0,1}(k)|0\rangle,$$
$$\langle k,e_i|k',e_j\rangle = \delta(k-k')\delta_{ij}, \tag{8}$$

где $a^+_{0,1}(k)$ – оператор рождения фотона с импульсом $k > 0$ и одним из ортогональных состояний поляризации e_0 и e_1, $\mathcal{F}(k)$ – амплитуда состояния в k-представлении, $i,j = 0,1, k \in (0,\infty)$. В координатном представлении состояния имеют вид

$$|\psi_{0,1}\rangle = \int_{-\infty}^\infty \mathcal{F}(x-t)|x,t\rangle\otimes|e_{0,1}\rangle, \tag{9}$$

$$\mathcal{F}(x-t) = \int_0^\infty dk\mathcal{F}(k)e^{ik(x-t)},$$
$$\langle k|x,t\rangle = \frac{1}{\sqrt{2\pi}}e^{ik(x-t)}, \quad x,t\in(-\infty,\infty). \tag{10}$$

Нормировка векторов состояний в координатном представлении с учетом [19]

$$\int_{-\infty}^\infty dx e^{ik(x-t)}\frac{1}{x-t+a} = i\pi\ \mathrm{sgn}(k)e^{-ika}, \tag{11}$$

$$\langle\psi_{0,1}|\psi_{0,1}\rangle = \langle\mathcal{F}|\mathcal{F}\rangle =$$
$$= \int_{-\infty}^\infty\int_{-\infty}^\infty dxdx'\mathcal{F}(x-t)\mathcal{F}^*(x'-t)[\frac{1}{2}\delta(x-x') +$$
$$+ \frac{i}{\pi}\frac{1}{x-x'}] = \int_{-\infty}^\infty |\mathcal{F}(x-t)|^2dx. \tag{12}$$

Состояния выбираются почти "монохроматическими" так, что амплитуда $\mathcal{F}(\tau) \approx \mathrm{const} \approx 1/\sqrt{L}$ представляет собой "полочку" с точностью до хвостов на концах, и

$$\int_{\{L\}} dx|\mathcal{F}(x-t)|^2 = 1-\delta, \quad \delta\to 0. \tag{13}$$

Спадание на концах может быть выбрано сколь угодно резким и таким, чтобы сделать δ сколь угодно малым. Последнее будем считать выполненным, и параметр δ будет с любым запасом самым малым в задаче (см. детали в [20–22]).

Для протокола существенно, что длина квантового канала L_{ch} должна быть меньше эффективной протяженности состояний $L_{ch} < L$.

Участник B, контролируя область Ω_B размера L, в более поздний момент времени t_B, когда состояние целиком достигает этой области, производит измерения, которые описываются разложением единицы:

$$I = \int_{-\infty}^\infty dx|x,t_B\rangle\langle x,t_B|\otimes I_{\mathbf{C}^2} =$$
$$= \mathcal{P}_0(t_B) + \mathcal{P}_1(t_B) + \mathcal{P}_\perp(t_B),$$
$$\mathcal{P}_{0,1}(t_B) = |\mathcal{F}_{t_B},e_{0,1}\rangle\langle\mathcal{F}_{t_B},e_{0,1}|, \tag{14}$$

$$|\mathcal{F}_{t_B},e_{0,1}\rangle = \int_{-\infty}^\infty dx\mathcal{F}(x-t_B)|x,t_B\rangle\otimes|e_{0,1}\rangle,$$
$$x\in\Omega_B, \quad \mathcal{P}_\perp(t_B) = I - \mathcal{P}_0(t_B) - \mathcal{P}_1(t_B). \tag{15}$$

На словах данное измерение означает, что участник B осуществляет измерение, сводящееся к взятию проекции на одно из состояний, амплитуда которого целиком будет в области Ω_B. Вероятности исходов в момент времени t_B равны

$$\Pr\{i,t_B;j\} = \mathrm{Tr}\{|\psi_i\rangle\langle\psi_i|\mathcal{P}_j(t_B)\} =$$
$$= \delta_{ij}\int_{\{L\}} dx|\mathcal{F}(x-t_B)|^2 = \delta_{ij}, \quad x\in\Omega_B. \tag{16}$$

Полная вероятность ошибки складывается из двух составляющих. Первая отвечает ситуации, когда

прибор у подслушивателя вообще не сработал. При этом вероятность ошибки равна 1/2 (равна просто вероятности ошибки при простом угадывании). Вторая часть ошибки складывается из ошибки, когда прибор у подслушивателя в доступной ему области сработал. Из-за локальной ортогональности вероятность этой ошибки равна нулю. Более формально, полная ошибка есть

$$P_e(t_E) = P_e(\Omega_E, t_E) + P_e(\overline{\Omega}_E, t_E), \tag{17}$$

где Ω_E – область, доступная для подслушивателя (соответственно $\overline{\Omega}_E$ – недоступная область, то есть дополнение Ω_E до полного координатного пространства); t_E – момент времени, к которому относится измерение в области Ω_E. Полное разложение единицы есть

$$\begin{gathered} I = I(\Omega_E, t_E) + I(\overline{\Omega}_E, t_E), \\ I(\overline{\Omega}_E, t_E) = \sum_{i=0,1} \int\limits_{\overline{\Omega}_E} dx |x, t_E, e_i\rangle\langle x, t_E, e_i|, \\ I(\Omega_E, t_E) = \sum_{i=0,1} \int\limits_{\Omega_B} dx |x, t_E, e_i\rangle\langle x, t_E, e_i|. \end{gathered} \tag{18}$$

Минимальная вероятность ошибки $P_e(\Omega_E, t_E)$ определяется минимизацией по всевозможным разложениям единицы $I(\Omega_E)$ [16]:

$$P_e(\Omega_E, t_E) = \tag{19}$$

$$= \min_{E_0, E_1} \left\{ \frac{1}{2}\mathrm{Tr}\{|\psi_0\rangle\langle\psi_0|E_1\} + \frac{1}{2}\mathrm{Tr}\{|\psi_1\rangle\langle\psi_1|E_0\} \right\}.$$

$E_{0,1}$ легко находятся, и полная ошибка $P_e(\Omega_E, t_E) \equiv 0$ при различении равна

$$\begin{gathered} E_{0,1} = \int\limits_{\Omega_E} dx |x, t_E; e_{0,1}\rangle\langle x, t_E; e_{0,1}|, \\ P_e(\overline{\Omega}_E t_E) = \tfrac{1}{2} N(\overline{\Omega_E}, t_E) = \frac{1}{2}\int\limits_{\overline{\Omega}_E} dx |\mathcal{F}(x - t_E)|^2. \end{gathered} \tag{20}$$

Соответственно, вероятность правильной идентификации бита A подслушивателем E при фиксированном размере доступной области Ω_E равна

$$\begin{aligned} P_{OK}(t_E) &= 1 - P_e(\overline{\Omega}_E t_E) - P_e(\Omega_E t_E) = \\ &= \frac{1}{2}\left(1 + \int\limits_{\Omega_E} dx |\mathcal{F}(x - t_E)|^2\right). \end{aligned} \tag{21}$$

Доступная информация подслушивателя о бите A может быть вычислена по формуле (5) с учетом того, что измерение описывается разложением единицы $\{E_i\} = \{I_{\overline{\Omega}_E}, E_0, E_1\}$. Доступная информация складывается из двух частей. Первая описывает ту часть взаимной информации, которую дают исходы в недоступной области. Вторая – исходы в доступной области Ω_E. Имеем

$$\begin{aligned} I(A; E, \Omega_E, t_E) = I(A; E, \rho_0, \rho_1, \Omega_E, t_E) + \\ + I(A; E, \rho_0, \rho_1, \overline{\Omega}_E, t_E). \end{aligned} \tag{22}$$

Вычисление по формуле (5) с учетом $\{E_i\} = \{I_{\overline{\Omega}_E}, E_0, E_1\}$ и $\pi_0 = \pi_1 = 1/2$ дает

$$\begin{gathered} I(A; E, \rho_0, \rho_1, \overline{\Omega}_E, t_E) = 0, \\ \mathrm{Tr}\{\rho_{0,1} I_{\overline{\Omega}_E}\} = \frac{1}{2}\mathrm{Tr}\{\rho I_{\overline{\Omega}_E}\}, \quad \rho = \frac{1}{2}(\rho_0 + \rho_1), \end{gathered} \tag{23}$$

$$\begin{gathered} I(A; E, \rho_0, \rho_1, \Omega_E, t_E) = \int\limits_{\Omega_E} dx |\mathcal{F}(x - t_E)|^2, \\ \mathrm{Tr}\{\rho_0 E_0\} = \mathrm{Tr}\{\rho_1 E_1\} = \mathrm{Tr}\{\rho E_{0,1}\}. \end{gathered} \tag{24}$$

Пусть эффективное увеличение области подслушивателя (по сравнению с доступной ему длиной канала связи) есть χ. Вероятность ошибки подслушивателя при различении состояний равна

$$\begin{aligned} \mathrm{Pr}_E\{\chi\} &= \frac{1}{2}\left(1 + \int\limits_{\{L_{ch}+\chi\}} dx |\mathcal{F}(x - t_E)|^2\right) = \\ &= \frac{1}{2}\left(1 + \frac{L_{ch} + \chi}{L}\right). \end{aligned} \tag{25}$$

Вероятность пройти тест на задержку у легитимного пользователя B при его измерении (14), (15) для любого состояния $|\tilde{\mathcal{F}}\rangle$, задержанного на время (расстояние) χ, определяется как

$$\begin{aligned} \mathrm{Pr}_B\{\chi\} &= \mathrm{Tr}\{|\tilde{\mathcal{F}}\rangle\langle\tilde{\mathcal{F}}|(\mathcal{P}_0(t_B) + \mathcal{P}_1(t_B))\} = \\ &= \left| \int\limits_{\{L-\chi\}} dx \mathcal{F}(x - t_B)\tilde{\mathcal{F}}^*(x - t_B) \right|^2 \le \\ \le \left(\int\limits_{\{L-\chi\}} dx |\mathcal{F}(x - t_B)|^2 \right) &\left(\int\limits_{\{L-\chi\}} dx |\tilde{\mathcal{F}}(x - t_B)|^2 \right) \le \\ &\le \left(1 - \tfrac{\chi}{L}\right). \end{aligned} \tag{26}$$

Достаточно ограничиться чистыми задержанными состояниями $\tilde{\mathcal{F}}$. Ограничение пределов интегрирования областью $L - \chi$ связано с тем, что из-за существования предельной скорости распространения ни одно задержанное на время χ состояние не может достичь к моменту измерения t_B правой крайней части области L.

Таким образом, для подслушивателя вероятность узнать передаваемый бит и пройти при этом тест у B равна

$$\Pr\{bit_E = bit_A \bigwedge pass\ test, \chi\} = \Pr_E\{\chi\} \cdot \Pr_B\{\chi\} =$$

$$= \frac{1}{2}\left(1 + \frac{L_{ch} + \chi}{L}\right) \cdot \left(1 - \frac{\chi}{L}\right),\ \Pr = \frac{1}{2}\left(1 + \frac{L_{ch}}{L}\right). \tag{27}$$

Максимум вероятности в (27) достигается *на краю интервала при* $\chi = 0$.

Покажем теперь, что в канале с шумом вероятность (27) не может превышать соответствующего значения в идеальном канале. Изменение состояния под действием шума может быть описано при помощи инструмента с учетом релятивистских ограничений на него. Общий вид инструмента есть [24–27]

$$\mathcal{T}[...] = \sum_k \mathcal{S}_k[...]\mathcal{S}_k^+, \quad \mathcal{S}_k = \sqrt{\lambda_k}|\phi_k\rangle\langle\varphi_k|, \quad \sum_k \lambda_k \mathcal{S}_k \mathcal{S}_k^+ \le 1, \quad \lambda_k \ge 0, \tag{28}$$

$$\mathrm{Tr}\{\mathcal{T}[|\psi_{0,1}\rangle\langle\psi_{0,1}|]I(\Omega_E, t_e)\} =$$
$$= \sum_k \mathrm{Tr}\{|\psi_{0,1}\rangle\langle\psi_{0,1}|(\mathcal{S}_k I(\Omega_E, t_e)\mathcal{S}_k^+)\} \le$$
$$\le \sum_k \lambda_k \mathrm{Tr}\{|\psi_{0,1}\rangle\langle\psi_{0,1}|(|\varphi_k\rangle\langle\varphi_k|)\} \le$$
$$\le \sum_k \lambda_k |\langle\varphi_k|\psi_{0,1}\rangle|^2 \le$$
$$\le \sum_k \lambda_k \langle\varphi_k|\varphi_k\rangle\langle\psi_{0,1}|\psi_{0,1}\rangle \le \langle\psi_{0,1}|\psi_{0,1}\rangle =$$
$$= \int_{\Omega_A} dx \left|\mathcal{F}(x - t_A)\right|^2 = \int_{\Omega_E} dx \left|\mathcal{F}(x - t_E)\right|^2. \tag{29}$$

Последнее равенство в (29) выражает тот факт, что амплитуда состояния

$$|\psi_{0,1}\rangle = \int\limits_{\Omega_A} dx \mathcal{F}(x - t_A)|x, t_A\rangle \otimes |e_{0,1}\rangle =$$
$$= \int\limits_{\Omega_E} dx \mathcal{F}(x - t_E)|x, t_E\rangle \otimes |e_{0,1}\rangle, \tag{30}$$

$\mathcal{F}(x - t_A)$ в момент времени t_A целиком локализована в области $x \in \Omega_A$ и будет целиком локализована в области $x \in \Omega_E$ в момент времени, не более ранний, чем t_E, который не может быть быстрее, чем $t_E = t_A + \mathrm{dist}(\Omega_E, \Omega_A)$. *Таким образом, вероятность узнать отдельный передаваемый бит и пройти тест у легитимного пользователя B для подслушивателя не превышает величины* $Pr = 1/2(1 + L_{ch}/L)$ *в идеальном канале.*

• В заранее оговоренные моменты времени участник A приготавливает и посылает в канал связи последовательно состояния $|\psi_{0,1}\rangle$, а участник B осуществляет измерения, описываемые разложением единицы (14), (15). Остаются только те посылки, которые прошли тест.

• Участники A и B раскрывают часть посылок, подсчитывают количество несоответствий и получают оценку вероятности ошибки – p_{err}.

• Участник A в оставшейся последовательности битов называет *номера* тех посылок, в которых посылались либо только 0, либо только 1. Данные номера посылок объединяются в группы по k штук. При этом участник B осуществляет коррекцию ошибок в каждом блоке по мажоритарному принципу [28]. Величина k выбирается такой, чтобы уменьшить эффективную ошибку в каждом блоковом бите $\tilde{bit}(i)$ ($\tilde{0} = \overbrace{\{0,0,...0\}}^{k}$ и $\tilde{1} = \overbrace{\{1,1,...1\}}^{k}$) до уровня $\approx p_{err}^k \ll p_{err}$. После этого происходит нумерация уже блоковых битов.

• Участники из блоковых битов формируют $N + M$ битов четности $Bit = \sum_{i=1}^{n} \oplus \tilde{bit}(i)$. Для этого участник A называет номера (в новой нумерации блоковых битов), которые будут включены в каждый бит четности.

• Для $N + M$ битов четности $Bit(j)$, $j = 1..N + M$, производится процедура из M раундов хэширования. Для этого в каждом раунде участник A выбирает случайную строку s_l длиной $N + M - l$ ($l = 1...M$) и сообщает ее открыто B. Затем A и B проверяют четности подмножества битов в своих строках (Bit_A и Bit_B) сравнивая четности со строкой s_l, поскольку $s_l \cdot Bit_A = s_l \cdot Bit_B = (s_l \cdot Bit_A) \oplus (s_l \cdot Bit_B) = s_l \cdot (Bit_A \oplus Bit_B)$. Если четности подстрок совпадают, то из последовательностей Bit_A и Bit_B отбрасывается по одному биту из оговоренной позиции. Проводится M раундов. В итоге вероятность того, что тесты на четность в M раундах прошли успешно, а оставшиеся строки из N битов четности Bit_A и Bit_B не совпадают, равна [29]

$$\Pr\{s_A(N) \ne s_B(N)\} = 2^{-M}. \tag{31}$$

Выбором надлежащего M всегда можно добиться того, чтобы вероятность отличия строки из N битов была сколь угодно малой.

• Каждый бит четности может быть составлен из блоковых битов числом способов, равным [30]

$$\frac{1}{2}\sum_{i=0}^{n} C_{n\cdot k}^{i\cdot k} = \frac{2^{n\cdot k}}{2k}\sum_{l=1}^{k} \cos^{n\cdot k}\left(\frac{l\pi}{k}\right)\cos(nl\pi) \approx \frac{1}{2k}2^{n\cdot k}. \tag{32}$$

Информация Хартли I множества блоковых строк представляет собой (с точностью до округления) число двоичных символов, необходимых для идентификации четности строки, и практически равна полному числу двоичных строк длиной $n \cdot k$:

$$I = \log_2\left(\frac{2^{n\cdot k}}{2k}\sum_{l=1}^{k} \cos^{n\cdot k}\left(\frac{l\pi}{k}\right)\cos(nl\pi)\right) \approx \eta\, n \cdot k, \quad \eta \approx 1, \tag{33}$$

то есть требуется знание почти всех битов в строке. Вероятность узнать каждый бит и пройти тест не превышает (27), поэтому условная вероятность того, что подслушиватель знает N результирующих битов, переданных A и принятых как ключ, есть (напомним, что $(1+L_{ch}/L)/2<1$)

$$\begin{gathered}\Pr\{s_A(N)=s_E(N)\}= \\ 2^{-N}\{1+2\cdot 2^{-\eta n\cdot k}[(1+L_{ch}/L)]^{\eta\cdot n\cdot k}\}^N= \\ =2^{-N}(1+2\zeta)^N, \\ \zeta=2^{-\eta n\cdot k}[(1+L_{ch}/L)]^{\eta\cdot n\cdot k}.\end{gathered} \tag{34}$$

Взаимная информация подслушивателя о строке результирующих битов A есть

$$\begin{gathered}I(A;E)=I(A)-I(A|E),\quad I(A)=-\log_2 2^{-N}, \\ I(A|E)=-\log_2\Pr\{s_A(N)=s_E(N)\},\end{gathered} \tag{35}$$

где $I(A)$ – собственная информация строки результирующих битов длиной N, $I(A|E)$ – условная информация E о строке битов A. Для взаимной информации [31] между A и E с учетом (34), (35) имеем

$$\begin{gathered}I(A;E)=N-N+N\log_2(1+2\zeta)\approx\frac{2N\cdot\zeta}{\ln 2}= \\ =2N\cdot 2^{-\eta n\cdot k}[(1+L_{ch}/L)]^{\eta\cdot n\cdot k}/\ln 2\ll 1.\end{gathered} \tag{36}$$

При заданных N, L_{ch}, L ($L_{ch}<L$) (см. (36)) может быть сделана экспоненциально малой по параметру $n\cdot k$:

• Покажем теперь, что взаимная информация E о строке результирующих битов у B также экспоненциально мала. Взаимная информация между A и B есть

$$\begin{gathered}I(A;B)=I(A)-I(A|B)= \\ =-\log_2 2^{-N}+\log_2\Pr\{s_A(N)=s_B(N)\}= \\ =N+\log_2(1-2^{-M})\approx N-2^{-M}/\ln 2.\end{gathered} \tag{37}$$

Воспользуемся теперь неравенством треугольника для условных информаций, и окончательно имеем

$$\begin{gathered}I(A|E)\le I(A|B)+I(B|E), \\ I(B|E)\ge N-(2N\cdot\zeta-2^{-M})/\ln 2, \\ I(B;E)\le(2N\cdot\zeta-2^{-M})/\ln 2\ll 1.\end{gathered} \tag{38}$$

Таким образом, доказана вторая часть критерия секретности (3), (4).

Работа поддержана Российским фондом фундаментальных исследований (проект # 99-02-18127).

1. S. Wiesner, SIGACT News **15**, 78 (1983).
2. C. H. Bennett and G.Brassard, Proc. of IEEE Int. Conf. on Comput. Sys. and Sign. Proces., Bangalore, India, December 1984, p. 175.
3. A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
4. C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992); C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
5. A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).
6. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, quant-ph/0101098.
7. D. Mayers and A. Yao, quant-ph/9802025.
8. E. Biham, M. Boyer, P. O. Boykin et al., quant-ph/9912053.
9. Hoi-Kwong Lo and H. F. Chau, quant-ph/9803006.
10. P. W. Shor and J. Preskill, quant-ph/0003004.
11. L. Goldenberg and L. Vaidman, Phys. Rev. Lett. **75**, 1239 (1995); quant-ph/9506030.
12. S. N. Molotkov and S. S. Nazin, quant-ph/0008008.
13. Л. Д. Ландау, Р. Пайерлс, Zeits. für Phys., **69**, 56 (1931); *Собрание трудов*, т. 1, 1969, М.: Наука, с. 56.
14. Н. Бор, Л. Розенфельд, Math.-Fys. Medd. **12**, 3 (1933); *Собрание научных трудов*, М.: Наука, 1971.
15. А. С. Холево, Problems of Information Transmission **9**, 177 (1973) [Проблемы передачи информации **9**, 3 (1973)].
16. C. A. Fuchs, quant-ph/9601020.
17. J.von Neumann, *Mathematical Foundations of Quantum Mechanics*, Princeton University, Princeton, NJ, 1955.
18. Н. Н. Боголюбов, Известия АН СССР, сер. физ. **19**, 237 (1955); Н. Н. Боголюбов, Д. В.Ширков, *Введение в теорию квантованных полей*, М.: Наука, 1973.
19. Ю. А. Брычков, А. П. Прудников, *Интегральные преобразования обобщенных функций*, М.: Наука, 1977.
20. Д. А. Киржниц, УФН **90**, 129 (1966).
21. A. M. Jaffe, Phys. Rev. **158**, 1454 (1967).
22. I. Bialynicki-Birula, Phys. Rev. Lett. **80**, 5247 (1998).
23. Н. Винер, Р. Пэли, *Преобразование Фурье в комплексной области*, М.: Наука, 1964 [N. Wiener and R. Paley, *Fourier Transform in the Complex Domain*, New-York, 1934.]
24. E. B. Devis, *Quantum Theory of Open Systems*, Academic Press, London, 1976.
25. K. Kraus, *States, Effects and Operations*, Springer-Verlag, Berlin, 1983.
26. A. S. Holevo, *Lectures on Statistical Structure of Quantum Theory*, 1999, p. 1.
27. P. Busch, M. Grabowski, and P. J. Lahti, *Operational Quantum Physics*, Springer Lecture Notes in Physics, v. **31**, 1995.
28. E. J. Mac Williams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Publ. Company, Amsterdam, New York, Oxord, 1977.
29. C. H. Bennett, Tal Mor, and J.Smolin, Phys. Rev. **A54**, 2675 (1996); Tal Mor, quant-ph/9906073.
30. А. П. Прудников, Ю. А. Брычков, О. А. Маричев, *Интегралы и ряды, Элементарные функции*, М.: Наука, 1981.
31. C. E. Shannon, Bell Syst. Tech. Jour. **27**, 397; **27**, 623 (1948).