Письма в ЖЭТФ, том 73, вып. 2, стр. 114 – 120 25 января

Квантовая привязка к биту в канале с шумом

С. Н. Молотков[1)], *С. С. Назин*

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

Поступила в редакцию 5 декабря 2000 г.

При достаточно общих предположениях о свойствах квантового канала с шумом предложен квантовый протокол, позволяющий реализовать секретную привязку к биту с вероятностью, сколь угодно близкой к единице.

PACS: 03.65.-w, 89.70.+c

Идея о том, что квантовая физика может обеспечить большую секретность при передаче информации, чем классическая, была высказана в [1]. В дальнейшем вслед за [2, 3] появилось большое число работ, посвященных секретному распространению ключа (квантовая криптография). Кроме протокола распространения ключа существуют другие важные для приложений, а также имеющие самостоятельный интерес криптографические протоколы. Это так называемые протоколы Bit Commitment (BC) и Coin Tossing (CT) [4, 5]. Квантовый вариант этих протоколов был предложен в работе [6].

BC представляет собой такой протокол обмена, который позволяет двум пространственно удаленным и не доверяющим друг другу участникам A и B реализовать следующую схему. Участник A посылает B часть информации о своем секретном бите ($b = 0$ или 1, стадия commitment) так, чтобы по части информации B не смог узнать, что задумал A. Однако эта часть информации устроена так, чтобы A на стадии раскрытия, когда B потребует оставшуюся часть информации, не смог изменить значения своего секретного бита b. Протокол CT – это такая схема, которая позволяет двум не доверяющим друг другу пространственно удаленным участникам реализовать честный выбор жребия.

Классические варианты протоколов основаны на недоказанной вычислительной сложности некоторых функций-ловушек (функций, обращение которых требует экспоненциально больших затрат на классическом компьютере) [7, 8].

Считалось, что квантовые протоколы, основанные не на вычислительной сложности, а на фундаментальных запретах, диктуемых квантовой механикой, являются безусловно секретными [9]. Однако впоследствии было показано [10,11], что нерелятивистский квантовый BC является несекретным. Участник A может обманывать в свою пользу, и обман остается незамеченным, при помощи так называемой EPR-атаки (EPR – Эйнштейн – Подольский – Розен [12]). Доказательство возможности EPR-атаки по существу основано на результате работы [13] об измерениях над квантовыми ансамблями составных систем.

Все упомянутые нерелятивистские квантовые протоколы основаны лишь на свойствах квантовых состояний в гильбертовом пространстве и не содержат явно эффектов распространения состояний от одного пространственно удаленного участника протокола к другому. В реальной ситуации передача информации от одного участника к другому происходит в пространстве-времени Минковского. Явный учет данного обстоятельства расширяет возможности для конструирования квантовых релятивистских протоколов [14], а также заметно упрощает доказательство их секретности [15]. Ограничения, накладываемые специальной теорией относительности на измеримость квантовых состояний, позволяют реализовать секретные протоколы BC и CT в идеальном канале [16]. Неэффективность EPR-атаки в релятивистском случае базируется на том обстоятельстве, что протяженное в пространстве-времени квантовое состояние не может быть мгновенно изменено. Кроме того, невозможно мгновенное и достоверное различение даже одного из пары ортогональных состояний. Ограничения, накладываемые специальной теорией относительности на измеримость состояний квантовых систем, обсуждались еще в работе Ландау и Пайерлса [17].

В данной работе предлагается релятивистский квантовый протокол BC в квантовом канале с шумом. На интуитивном уровне идея протоколов достаточно проста. Участник A приготавливает (включа-

[1)] e-mail: molotkov@issp.ac.ru

ет источник) одно из пары ортогональных состояний, отвечающих 0 или 1, которые по мере формирования направляются в канал связи с предельно допустимой скоростью (скоростью света c; далее $c = 1$). Пока состояния недоступны участнику B целиком, он не может достоверно узнать, каково значение секретного бита – 0 или 1. Участник A не может влиять (опять же из-за существования предельной скорости распространения) на ту часть состояния, которая ушла в канал связи (происходит привязка A к биту – стадия commitment). Когда состояние становится доступным B целиком, он может достоверно (из-за ортогональности состояний) узнать значение секретного бита и сравнить это значение с тем, что сообщит ему A по классическому каналу на стадии раскрытия. Ограничения, накладываемые специальной теорией относительности на измеримость квантовых состояний, позволяют в явном виде реализовать исходную идею протокола B о предоставлении части информации одному из участников, а ограничение доступа в координатном пространстве автоматически приводит к ограничению части гильбертова пространства состояний даже для "внутренних" степеней свободы квантовой системы (спина, поляризации), поскольку они не существуют в отрыве от пространственных степеней свободы.

В протоколе используется пара однофотонных состояний с ортогональными поляризациями и пространственной амплитудой специального вида, отвечающих 0 и 1:

$$\psi_{0,1}\rangle = \int\limits_0^\infty dk\mathcal{F}(k)a^+(k)|0\rangle \otimes |e_{0,1}\rangle =$$

$$= \int\limits_0^\infty dk\mathcal{F}(k)|k\rangle \otimes |e_{0,1}\rangle = |\mathcal{F}\rangle \otimes |e_{0,1}\rangle, \qquad (1)$$

где $a^+(k)$ – оператор рождения состояния с импульсом (энергией) $k > 0$, $\mathcal{F}(k)$ – амплитуда в k-представлении, $|e_{0,1}\rangle$ – состояние поляризации, и

$$\int\limits_0^\infty dk|\mathcal{F}(k)|^2 = 1, \quad [a(k), a^+(k')] = \delta(k-k'),$$

$$\langle e_i|e_j\rangle = \delta_{ij}, \quad i,j = 0,1, \quad k \in (0.\infty). \qquad (2)$$

В координатно-временном τ-представлении состояния имеют вид

$$|\psi_{0,1}\rangle = \int\limits_{-\infty}^\infty d\tau\mathcal{F}(\tau)|\tau\rangle\otimes|e_{0,1}\rangle, \quad \mathcal{F}(\tau) = \int\limits_0^\infty dk\mathcal{F}(k)e^{-ik\tau},$$

$$\langle k|\tau\rangle = \frac{1}{\sqrt{2\pi}}e^{ik\tau}, \quad \tau = t - x, \quad \tau \in (-\infty,\infty), \qquad (3)$$

где $\mathcal{F}(\tau)$ – амплитуда в τ-представлении. Такая запись отражает интуитивные представления о пакете, движущемся в положительном направлении оси x со световой скоростью и имеющем пространственно-временную форму $\mathcal{F}(\tau)$. Условие нормировки в τ-представлении с учетом [18] имеет вид

$$\int\limits_{-\infty}^\infty e^{ik\tau}\frac{1}{\tau+a} = i\pi\ \mathrm{sgn}(k)e^{-ika},$$

$$\langle\psi_{0,1}|\psi_{0,1}\rangle = \langle\mathcal{F}|\mathcal{F}\rangle =$$

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

$$= \int_{-\infty}^\infty |\mathcal{F}(\tau)|^2 d\tau. \qquad (4)$$

Для протокола будут важны два обстоятельства: 1) существует предельная скорость распространения состояний; 2) ортогональные состояния достоверно неразличимы, если они недоступны целиком (даже если они остаются ортогональными при ограничении на доступную для измерений область). Значения классических битов 0 и 1 сопоставляются двум ортогональным состояниям поляризации $|e_0\rangle$ и $|e_1\rangle$. Поскольку не существует состояния поляризации вне пространственных степеней свободы $\mathcal{F}(\tau)$, то для достоверного (с вероятностью 1) различения состояний требуется доступ ко всей пространственной области, где отлична от нуля амплитуда $\mathcal{F}(\tau)$. Говоря точнее, при любом измерении в ограниченной области τ имеется отличная от нуля ошибка при различении состояний. Любое измерение описывается разложением единицы в $\mathcal{H}$ [19–23], а при доступе к ограниченной области $\Delta(\tau)$ ($\overline{\Delta}(\tau)$ – дополнение до полного пространства $\tau \in (-\infty,\infty)$) дается разложением единицы вида

$$I = \int\limits_{-\infty}^\infty d\tau|\tau\rangle\langle\tau| \otimes I_{C^2} =$$

$$= \int\limits_{\Delta(\tau)} d\tau|\tau\rangle\langle\tau| \otimes (\mathcal{P}_0 + \mathcal{P}_1) + \int\limits_{\overline{\Delta}(\tau)} d\tau|\tau\rangle\langle\tau| \otimes I_{C^2},$$

$$\mathcal{P}_{0,1} = |e_{0,1}\rangle\langle e_{0,1}|, \qquad (5)$$

где $\mathcal{P}_{0,1}$ – проекторы на состояние поляризаций $|e_{0,1}\rangle$. Если исход измерения имеет место в доступной для

измерения области $\Delta(\tau)$, то вероятности исходов в двух ортогональных каналах $\mathcal{P}_0$ и $\mathcal{P}_1$ имеют вид

$$\mathrm{Tr}\{\rho(0,1)(I(\Delta(\tau))\otimes\mathcal{P}_{0,1})\} = \int\limits_{\Delta(\tau)} d\tau|\mathcal{F}(\tau)|^2 = N(\Delta(\tau)),$$

$$\mathrm{Tr}\{\rho(0,1)(I(\Delta(\tau))\otimes\mathcal{P}_{1,0})\} \equiv 0, \qquad (6)$$

где $\rho(0,1) = |\psi_{0,1}\rangle\langle\psi_{0,1}|$ и $N(\Delta(\tau))$ – доля исходов в доступной области. При этом вероятность ошибки из-за ортогональности каналов $p_e(\Delta(\tau)) = 0$. Однако если результат не был получен в доступной для измерений области, то вероятность ошибки $p_e(\bar{\Delta}(\tau)) = 1/2$, и доля таких исходов

$$\mathrm{Tr}\{\rho(0,1)\left(I(\overline{\Delta}(\tau))\otimes I_{C^2}\right)\} =$$

$$= \int\limits_{\overline{\Delta}(\tau)} d\tau|\mathcal{F}(\tau)|^2 = N(\overline{\Delta}(\tau)). \qquad (7)$$

Полная ошибка равна

$$P_e = p_e(\Delta(\tau))N(\Delta(\tau)) + p_e(\overline{\Delta}(\tau))N(\overline{\Delta}(\tau)) =$$

$$= 0\cdot N(\Delta(\tau)) + \frac{1}{2}\cdot N(\overline{\Delta}(\tau)) = \frac{1}{2}\int\limits_{\overline{\Delta}(\tau)} d\tau|\mathcal{F}(\tau)|^2 \neq 0. \quad (8)$$

В протоколе используются состояния с пространственно-временной амплитудой специального вида, представляющей собой состояние из двух сильно локализованных и разнесенных на интервал τ_0 половинок:

$$\mathcal{F}(\tau) = \frac{1}{\sqrt{2}}[f(\tau) + f(\tau-\tau_0)],$$

$$\int\limits_{-\Delta\tau}^{\Delta\tau} d\tau|f(\tau)|^2 = \int\limits_{-\Delta\tau+\tau_0}^{\Delta\tau+\tau_0} d\tau|f(\tau-\tau_0)|^2 = 1-\delta, \quad (9)$$

$$\delta \ll 1, \quad \Delta\tau \ll \tau_0,$$

где величина δ выбирается сколь угодно малой. Амплитуда $f(\tau)$ не может иметь компактного носителя [23], однако возможна сколь угодно сильная локализация и спадание сколь угодно близкое к экспоненциальному [23, 24]. Далее параметр δ будем для краткости опускать, имея в виду, что он может быть выбран с любым запасом самым малым в задаче. Последнее означает, что если доступная область пространства-времени τ накрывает интервал $-\Delta\tau < \tau < \Delta\tau + \tau_0$, то вероятность ошибки при этом (8) $P_e = 0$. Напротив, если доступна лишь одна из половинок состояния, то вероятность ошибки (8) $P_e = 1/4$. На словах это означает, что для того, чтобы достоверно отличить пару ортогональных состояний вида (9), требуется доступ к пространственно-временной области размером $\approx \tau_0$, который из-за существования предельной скорости распространения не может быть получен быстрее, чем за время τ_0.

Входными состояниями, посылаемыми участником A в квантовый канал связи, являются $\rho_{in}(0,1) = (|e_{0,1}\rangle\otimes|\mathcal{F}\rangle)(\langle\mathcal{F}|\otimes\langle e_{0,1}|)$. Описание квантового канала связи с шумом фактически сводится к заданию инструмента (иногда называемого супероператором) [19–22, 23], переводящего входные матрицы плотности в выходные (не обязательно нормированные). Всякий квантовый канал связи задает афинное отображение множества входных матриц плотности во множество матриц плотности на выходе. Любое такое отображение сводится к заданию инструмента $\boldsymbol{\mathcal{T}}$,

$$\rho_{out}(0,1) = \boldsymbol{\mathcal{T}}[\rho_{in}(0,1)] =$$

$$= \int\limits_{\infty}^{\infty}\int\limits_{\infty}^{\infty} d\tau d\tau' \rho_{out}(\tau,\tau')|\tau\rangle\langle\tau'|\otimes\rho(e_0,e_1) =$$

$$= \sum_{i=1}^{\infty}\lambda_i(|e_{i,0,1}\rangle\otimes|u_i\rangle)(\langle u_i|\otimes\langle e_{i,0,1}|), \qquad (10)$$

где $|u_i\rangle = \int\limits_{-\infty}^{\infty} d\tau u_i(\tau)|\tau\rangle$ – собственные векторы оператора выходной матрицы плотности (ядра $\rho_{out}(\tau,\tau')$). С учетом (4) имеем

$$\int\limits_{\infty}^{\infty} d\tau'\rho_{out}(\tau,\tau')u_i(\tau') = \lambda_i u_i(\tau),$$

$$\int\limits_{\infty}^{\infty} d\tau u_i(\tau)u_j^*(\tau) = \delta_{ij}, \quad \sum_{i=1}^{\infty}\lambda_i \leq 1. \qquad (11)$$

Векторы поляризации на выходе есть $|e_{i,0,1}\rangle = \alpha_{i,0,1}|e_0\rangle + \beta_{i,0,1}|e_1\rangle$ $(|\alpha_{i,0,1}|^2 + |\beta_{i,0,1}|^2 = 1)$. Любой инструмент может быть представлен в виде $\boldsymbol{\mathcal{T}}[\rho] = \sum_i V_i\rho V_i^+$, с $\sum_i V_iV_i^+ \leq I$ [19–22] (здесь нам достаточно ограничиться дискретным пространством результатов i). Применительно к нашему случаю такое представление может быть записано в виде

$$\boldsymbol{\mathcal{T}}[\ldots] = \sum_{i=1}^{\infty}\lambda_i(|e_{i,0,1}\rangle\otimes|u_i\rangle)(\langle e_{0,1}|\otimes$$

$$\otimes\langle\mathcal{F}|)[\ldots](|\mathcal{F}\rangle\otimes|e_{0,1}\rangle)(\langle u_i|\otimes\langle e_{i,0,1}|) + \boldsymbol{\mathcal{T}}_\perp[\ldots], \quad (12)$$

где $\boldsymbol{\mathcal{T}}_\perp[\ldots]$ – часть инструмента, которая дает тождественный нуль на линейной оболочке векторов $|\mathcal{F}\rangle\otimes|e_{0,1}\rangle$.

Поскольку время сохранения секретного бита определяется протяженностью состояний (τ_0), длина

канала может быть любой; поэтому далее ее можно положить без ограничения общности равной 0. Фактически задание инструмента является описанием свойств квантового канала связи аналогично тому, как это происходит в классическом случае, когда задается распределение вероятностей на выходном алфавите для каждого символа из входного алфавита. На интуитивном уровне такое отображение можно понимать (с некоторыми оговорками) как преобразование входного состояния $|\psi_{0,1}\rangle$ с формой $\mathcal{F}(\tau)$ и поляризацией $e_{0,1}$ в одно из выходных с формой $u_i(\tau)$ и поляризацией $e_{i,0,1}$, имеющих место с вероятностью λ_i. Тот факт, что сумма вероятностей не превосходит единицы, $\sum_i \lambda_i \le 1$, можно трактовать применительно к нашему случаю как исчезновение (поглощение) фотона в канале. Свойства канала определяются функциями $u_i(\tau)$ и вероятностями λ_i, которые считаются известными из априорных соображений (и могут быть определены из калибровки канала). Если возможно выбрать новый интервал локализации половинок состояний на выходе $D\tau$ так, чтобы было

$$\forall\, i = 1, \infty, \quad \frac{1}{2}\int\limits_{-D\tau}^{D\tau} d\tau |u_i(\tau)|^2 = \frac{1}{2} - \delta,$$

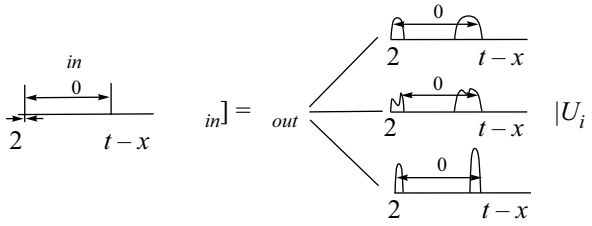
$$\frac{1}{2}\int\limits_{-D\tau+\tau_0}^{D\tau+\tau_0} d\tau |u_i(\tau)|^2 = \frac{1}{2} - \delta, \quad D\tau \ll \tau_0, \qquad (13)$$

где δ, как и ранее (9), сколь угодно мало, то канал является пригодным для реализации предлагаемого протокола. Иначе говоря, канал устроен так, что сильно локализованные состояния на входе еще остаются сильно локализованными на выходе с точностью $D\tau \ll \tau_0$ и $D\tau > \Delta\tau$ (см. рисунок), но могут изменять форму и поляризацию. Величина $D\tau$ будет определять точность, с которой обнаруживается возможная задержка выбора секретного бита участником A (задержка посылки состояния в канал связи). Вероятность детектирования состояний на выходе участником B в пространственно-временном окне $\Delta(\tau)$, накрывающем лишь одну из половинок $u_i(\tau)$, вне зависимости от исхода в каналах $\mathcal{P}_{0,1}$ равна

$$\Pr\{\Delta(\tau)\} = \mathrm{Tr}\{\boldsymbol{\mathcal{T}}[\rho_{in}(0,1)]\,(I(\Delta(\tau)\otimes I_{C^2})\} =$$

$$= \sum_{i=1}^{\infty}\lambda_i \int_{\Delta(\tau)} d\tau |u_i(\tau)|^2 \le (\frac{1}{2} - \delta)\sum_{i=1}^{\infty}\lambda_i \le \frac{1}{2} - \delta \le \frac{1}{2} \qquad (14)$$

и может быть сделана сколь угодно близкой (с экспоненциальной точностью путем соответствующего выбора $D\tau$ и τ_0) к $1/2$. При этом вероятность различения состояний при доступе только к половинке (то есть в течение времени $\approx \tau_0$) не лучше $1/2\cdot 1/2 = 1/4$ (8).



Вычислим теперь вероятность ошибки, когда состояния становятся доступными целиком по истечении времени протокола $D\tau + \tau_0 \approx \tau_0$ (напомним, что в идеальном канале такая ошибка различения равна нулю). Если состояние доступно целиком (по истечении времени $\approx \tau_0$ после начала протокола), то вероятность исхода в одном из каналов $\mathcal{P}_{0,1}$ равна

$$\Pr\{\Delta(\tau) + \overline{\Delta}(\tau)\} =$$

$$= \mathrm{Tr}\{\boldsymbol{\mathcal{T}}[\rho_{in}(0,1)]\,(I(\Delta(\tau)\otimes I_{C^2})\} = \sum_{i=1}^{\infty}\lambda_i \le 1. \qquad (15)$$

Тот факт, что $\Pr\{\Delta(\tau) + \overline{\Delta}(\tau)\} \le 1$ означает, что не все состояния достигают выхода канала, то есть с вероятностью $1 - \sum_{i=1}^{\infty}\lambda_i$ состояния поглощаются в канале (формально с такой вероятностью они никогда не доступны для измерений B). В этом случае, когда у B не было срабатывания измерительного устройства вообще, он может только угадывать, что было послано. При этом вклад в вероятность ошибки от таких событий есть $1/2(1 - \sum_{i=1}^{\infty}\lambda_i)$. Вычислим теперь вклад в ошибку, когда было срабатывание у B. Измерение, минимизирующее ошибку при различении двух состояний поляризации на "честных" входных состояниях, посылаемых A, дается следующим разложением единицы (см. детали, например, в [26]):

$$\sum_{i=1}^{\infty}\mathcal{P}_i\otimes(E_0+E_1) + \mathcal{P}_\perp\otimes I_{C^2} = I\otimes I_{C^2},$$

$$\mathcal{P}_i = |u_i\rangle\langle u_i|, \quad \mathcal{P}_\perp = I - \sum_{i=1}^{\infty}\mathcal{P}_i, \qquad (16)$$

$$E_0 + E_1 = I_{C^2}, \quad E_0 = |\tilde{e}_0\rangle\langle\tilde{e}_0|,$$

$$I_{C^2} = |e_0\rangle\langle e_0| + |e_1\rangle\langle e_1|, \qquad (17)$$

где $|\tilde{e}_0\rangle$ – собственные векторы оператора:

$$\Gamma = \gamma_{00}|e_0\rangle\langle e_0| + \gamma_{01}|e_0\rangle\langle e_1| + \gamma_{10}|e_1\rangle\langle e_0| + \gamma_{11}|e_1\rangle\langle e_1|, \qquad (18)$$

$$\gamma_{00} = \frac{1}{2}\sum_{i=1}^{\infty}\lambda_i(|\alpha_{i,1}|^2 - |\alpha_{i,0}|^2),$$

$$\gamma_{11} = \frac{1}{2}\sum_{i=1}^{\infty}\lambda_i(|\beta_{i,1}|^2 - |\beta_{i,0}|^2), \qquad (19)$$

$$\gamma_{01} = \frac{1}{2}\sum_{i=1}^{\infty}\lambda_i(\alpha_{i,1}\beta^*_{i,0} - \alpha_{i,0}\beta^*_{i,1}), \quad \gamma_{10} = \gamma^*_{01}.$$

Полная ошибка при различении состояний поляризации на "честных" входных состояниях, когда они доступны целиком, может быть представлена с учетом (18) и того факта, что априорные вероятности выбора состояний 0 или 1 участником A равны $1/2$, в виде

$$P_e = \frac{1}{2}(1 - \sum_{i=1}^{\infty}\lambda_i) + \frac{1}{2}\mathrm{Tr}\{\boldsymbol{\mathcal{T}}[\rho_{in}(0)]((\sum_{i=1}^{\infty}\mathcal{P}_i)\otimes E_1)\} +$$

$$+\frac{1}{2}\mathrm{Tr}\{\boldsymbol{\mathcal{T}}[\rho_{in}(1)]((\sum_{i=1}^{\infty}\mathcal{P}_i)\otimes E_0)\} = \frac{1}{2} - |\gamma_2| < \frac{1}{2}, \qquad (20)$$

где γ_2 – отрицательное собственное число оператора Γ в (18):

$$\gamma_2 = \frac{1}{2}(\gamma_{00} + \gamma_{11}) - \frac{1}{2}\sqrt{(\gamma_{00} - \gamma_{11})^2 + 4|\gamma_{01}|^2}. \qquad (21)$$

Если считать, что поляризации $|e_0\rangle$ и $|e_1\rangle$ сбиваются в канале одинаково, то $\gamma_2 = -|\gamma_{01}|$. В идеальном канале ошибка $P_e = 0$, как следует из (18)–(20).

Протокол выглядит следующим образом. 1) Участники контролируют только свои локальные окрестности. Предварительно они договариваются о времени начала протокола, виде состояний ($\mathcal{F}(\tau)$) и базисе поляризаций для 0 и 1 ($|e_{0,1}\rangle$). 2) Участник A кодирует секретный бит b (0 или 1) битом четности по N состояниям $\tilde{0}$ и $\tilde{1}$, состоящим из блоков по k штук ($b = \sum_{j=1}^{N}\oplus a[i,j]$, $i = 1..k$; все $a[i,j]$, принадлежащие одному блоку, одинаковы) и посылает $k\cdot N$ состояний вперемешку по $k\cdot N$ квантовым каналам связи, а участник B осуществляет измерения (16). 3) На стадии раскрытия при любом $\Delta\tau < \tau < \Delta\tau + \tau_0$ B может затребовать по классическому каналу, что было послано A. 4) По истечении времени действия протокола B сопоставляет результаты своих измерений с тем, что сообщил A. 5) Если все тесты проходят успешно, протокол завершается; в противном случае обрывается.

До истечения времени действия протокола вероятность правильного определения секретного бита участником B лишь на экспоненциально малую величину превышает $1/2$ – вероятность простого угадывания. Действительно, число двоичных строк длины $k\cdot N$ при блоковом представлении 0 и 1 есть, соответственно, (по поводу суммирования см. [27])

$$N_{\mathrm{odd}} = N_{\mathrm{even}} = \frac{1}{2}\sum_{m=0}^{N} C_{N\cdot k}^{m\cdot k} =$$

$$= \frac{2^{N\cdot k}}{2k}\sum_{l=1}^{k}\cos^{N\cdot k}(\frac{l\pi}{k})\cos(lN\pi) \approx \frac{1}{2K}2^{N\cdot k}, \qquad (22)$$

и практически равно полному числу двоичных строк длиной $N\cdot k$. Шенноновская информация [28–30] множества блоковых строк представляет собой (с точностью до округления) число двоичных символов, необходимых для идентификации четности строки,

$$I = \log_2\left(\frac{2^{N\cdot k}}{2k}\sum_{l=1}^{k}\cos^{N\cdot k}\left(\frac{l\pi}{k}\right)\cos(lN\pi)\right) \approx$$

$$\approx \eta\ N\cdot k, \quad \eta \approx 1, \qquad (23)$$

то есть требуется знание почти всех битов в строке. Однако при доступе только к половинке состояния ($\Delta\tau < \tau < \Delta\tau + \tau_0$) вероятность ошибки при определении бита в каждой позиции даже в канале без шума не лучше $1/4$ (8). Поэтому вероятность того, что участник B узнает бит четности до окончания протокола, не превосходит

$$P(\mathrm{parity}) = \frac{1}{2} + 2^{-\frac{\eta}{2}N\cdot k}. \qquad (24)$$

Вычислим теперь вероятность ошибки при определении бита четности участником B после истечения времени протокола. Блоковое представление по k (четное) штук устойчиво (ошибки исправляются по методу мажоритарного голосования), если число ошибок в каждом блоке не более $(k/2) - 1$. Вероятность ошибки в блоковом $\tilde{0}$ или $\tilde{1}$ есть

$$P_e(k) = \sum_{i=\frac{k}{2}}^{k} C_k^i P_e^i (1-P_e)^{k-i} \approx$$

$$\approx \sqrt{\frac{2}{\pi k}}[2\sqrt{P_e(1-P_e)}]^k, \qquad (25)$$

которая выбором k может быть сделана меньше любой наперед заданной величины. Полная ошибка в определении бита четности равна (N считаем четным)

$$P_e(\mathrm{parity}) = \sum_{i=odd}^{N-1} C_N^i P_e^i(k)(1-P_e(k))^{N-i}, \qquad (26)$$

суммирование ведется только по нечетным индексам i, поскольку ошибка в бите четности возникает при сбое в нечетном числе блоков. С учетом

$$\frac{1}{2}[(x+y)^N - (x-y)^N] = \sum_{i=odd}^{N-1} C_N^i x^i y^{N-i}, \qquad (27)$$

полагая $x = P_e(k)$ и $y = 1 - P_e(k)$ ($x + y = 1$), находим

$$P_e(\mathrm{parity}) = \frac{1}{2}[1 - (1-2P_e(k))^N]. \qquad (28)$$

Выбором достаточно большого k при заданном квантовом канале можно сделать $P_e(k)$ сколь угодно малой и такой, чтобы $NP_e(k) \ll 1$ было экспоненциально мало. При этом ошибка при определении бита четности по истечении времени протокола также сколь угодно мала, и вероятность правильного определения сколь угодно близка к 1.

Обсудим теперь устойчивость протокола относительно обмана участником A. Поскольку минимальное расстояние по Хэммингу между двумя блоковыми строками разной четности равно k (минимальное число различных позиций), то для того, чтобы изменить четность полной строки, требуется изменить, как минимум, k позиций. Поскольку вероятность правильного определения каждого блокового $\tilde{0}$ или $\tilde{1}$ не хуже, чем (25) $1-P_e(k) \to 1$ ($P_e(k)$ экспоненциально мала), вероятность обмана со стороны участника A, необнаруживаемого участником B, не превышает этой величины.

Протокол также устойчив относительно задержки выбора секретного бита участником A после начала протокола. Напомним, что при "честных" незадержанных входных состояниях вероятность исхода в канале $\mathcal{P}_\perp = I - \sum_{i=1}^{\infty} \mathcal{P}_i$ равна нулю::

$$\begin{aligned}
\Pr(\Delta(\tau) + \overline{\Delta}(\tau)) &= \mathrm{Tr}\{(\boldsymbol{\mathcal{T}}[\rho_{in}(0,1)] + \\
&+ \boldsymbol{\mathcal{T}}_\perp[\rho_{in}(0,1)])(\mathcal{P}_\perp \otimes I_{C^2})\} = \\
&= \mathrm{Tr}\left\{ \left(\left(\left(\sum_i \lambda_i |\alpha_{i,0,1}|^2 \mathcal{P}_i \right) \otimes |e_0\rangle\langle e_0| + \right.\right.\right. \\
&+ \left(\sum_i \lambda_i \alpha_{i,0,1} \beta^*_{i,0,1} \mathcal{P}_i \right) \otimes |e_0\rangle\langle e_1| + \\
&+ \left(\sum_i \lambda_i \beta_{i,0,1} \alpha^*_{i,0,1} \mathcal{P}_i \right) \otimes |e_1\rangle\langle e_0| + \\
&+ \left. \left(\sum_i \lambda_i |\beta_{i,0,1}|^2 \mathcal{P}_i \right) \otimes |e_1\rangle\langle e_1| \right) \times \\
&\left. \times (I - \sum_j \mathcal{P}_j) \otimes I_{C^2} \right\} = 0, \qquad (29)
\end{aligned}$$

с учетом того, что $|\alpha_{i,0,1}|^2 + |\beta_{i,0,1}|^2 = 1$ и $\mathcal{P}_i \mathcal{P}_j = \delta_{ij} \mathcal{P}_i$.

Любое задержанное более чем на $D\tau$ входное состояние может быть обнаружено с вероятностью, сколь угодно близкой к 1. Для этого нам потребуются ограничения, накладываемые на инструмент (12) специальной теорией относительности (точнее, существованием предельной скорости распространения). Если на входе любого квантового канала связи приготовлено сильно локализованное состояние (в том смысле, что квадрат амплитуды $\int_{-\Delta\tau}^{\Delta\tau} d\tau |\mu(\tau)|^2 = 1 - \delta$, δ экспоненциально мала, и $\Delta\tau \to 0$), то такое состояние на выходе канала не может быть зарегистрировано быстрее, чем через время $t = L/c$ (точнее, регистрации с вероятностью сколь угодно близкой к 1 будет иметь место во временном окне $-\Delta\tau + L/c \le t \le \Delta\tau + L/c$), L – длина канала. Применительно к нашему случаю инструмент (12) должен переводить состояния, приготовленные на входе в более поздний момент, в состояния, которые появляются на выходе также в более поздний момент. Причем величина сдвига переднего фронта амплитуды состояний на выходе не может быть меньше соответствующего сдвига на входе.

Любое входное задержанное состояние может быть представлено в виде (поляризационные степени свободы здесь для краткости опускаем)

$$\rho_{\mathrm{delay}} = \sum_l \mu_l |\mu_l\rangle\langle\mu_l|, \quad \sum_l \mu_l = 1,$$

$$|\mu_l\rangle = \int_{-\infty}^{\infty} d\tau \mu_l(\tau) |\tau\rangle, \qquad (30)$$

где $|\mu_l\rangle$ – собственные состояния матрицы плотности, и функции $\mu_l(\tau)$ имеют носитель, который не перекрывается с носителем передней половинки ни одной из функций $u_i(\tau)$ в интервале $D\tau$, получающихся на выходе канала из незадержанных состояний. На выходе канала ρ_{delay} перейдет в матрицу плотности такую, что носители собственных функций $|\eta_k\rangle$ также не будут перекрываться с передней половинкой $u_i(\tau)$ в интервале $D\tau$:

$$(\boldsymbol{\mathcal{T}} + \boldsymbol{\mathcal{T}}_\perp)[\rho_{delay}] = \sum_k \eta_k |\eta_k\rangle\langle\eta_k|,$$

$$\sum_k \eta_k \le 1, \quad |\eta_k\rangle = \int_{-\infty}^{\infty} d\tau \eta_k(\tau) |\tau\rangle. \qquad (31)$$

Из сказанного следует, что $|\langle\eta_k|u_i\rangle|^2 \le 1/2$, поскольку $\eta_k(\tau)$ не накрывает переднюю половинку $u_i(\tau)$, где набирается $1/2$ квадрата модуля $u_i(\tau)$.

Вероятность исхода на задержанных состояниях в канале $\sum_i \mathcal{P}_i < I$

$$\mathrm{Tr}\left\{ \left(\sum_k \eta_k |\eta_k\rangle\langle\eta_k| \right) \left(\sum_i \mathcal{P}_i \right) \right\} < 1, \qquad (32)$$

на незадержанных состояниях вероятность исхода равна 1. Аналогично, вероятность исхода в канале $\mathcal{P}_\perp = I - \sum_{i=1}^{\infty} \mathcal{P}_i$ (напомним, что на "честных" состояниях данная вероятность равна нулю), имеем

$$\mathrm{Tr}\left\{ \left(\sum_k \eta_k |\eta_k\rangle\langle\eta_k| \right) \left(I - \sum_i \mathcal{P}_i \right) \right\} = p_\perp \ne 0. \qquad (33)$$

Сумма вероятностей исходов в обоих каналах равна единице, если все состояния достигают выхода канала (не поглощаются, то есть $\sum_k \eta_k = 1$).

Детектирование задержки выбора секретного бита (задержка состояния) обнаруживается по появлению исходов в канале $\mathcal{P}_\perp$ с вероятностью $p_\perp$. Для изменения бита четности достаточно задержать состояния лишь в одном из блоков по k штук. Вероятность задержать k состояний и остаться незамеченным для участника A равна вероятности того, что все k задержанных состояний не дадут результата в канале $\mathcal{P}_\perp$, и тем самым будут имитировать статистику исходов измерений для "честных" состояний. Имеем

$$P_{\text{cheat}} = (1 - p_\perp)^k \ll 1, \qquad (34)$$

что может быть достигнуто при известной $p_\perp$ выбором достаточно большого k.

Таким образом, протокол позволяет реализовать честный протокол bit commitment с вероятностью, сколь угодно близкой к единице.

Работа поддержана Российским фондом фундаментальных исследований (проект # 99-02-18127), а также проектом "Физические основы квантового компьютера", программой "Перспективные технологии и устройства микро- и наноэлектроники" (проект # 02.04.5.2.40.T.50).

1. S. Wiesner, SIGACT News **15**, 78 (1983).
2. A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
3. C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992); C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
4. M. Blum, *Coin flipping by telephone: A protocol for solving impossimle problems*, Proc. 24th IEEE Comp. Conf., 1982, p.133, also in: SIGACT News **15**, 23 (1983).
5. P. A. Feldman, *A practical scheme for non-interactive verifable secret sharing*, Proc. 28th Annu. Symp. on Foun. of Comput. Sci., 1987, p.469.
6. 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.
7. P. W. Shor, Proc. 35th Annu. Symp. on Foun. of Comput. Sci., Santa Fe, NM, USA, Ed. S. Goldwasser, IEEE Comput. Soc. Press, Los Alamitos, 1994, p.124.
8. А. Ю. Китаев, УМН **52**, вып.6(318), 54 (1997).
9. C. Cré peau, *What is going on with Quantum Bit Commitment*, Crypto-96.
10. H.-K. Lo and H. F. Chau, Phys. Rev. Lett. **78**, 3410 (1997).
11. D. Mayers, Phys. Rev. Lett. **78**, 3414 (1997).
12. A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).
13. L. P. Hugston, R. Jozsa, and W.K.Wootters, Phys. Lett. **A183**, 14 (1993).
14. L. Goldenberg and L. Vaidman, Phys. Rev. Lett. **75**, 1239 (1995); quant-ph/9506030.
15. S. N. Molotkov and S. S. Nazin, quant-ph/0008008.
16. S. N. Molotkov and S. S. Nazin, quant-ph/9911055; quant-ph/9910034; ЖЭТФ, **117**, 818 (2000); Письма в ЖЭТФ, **70**, 684 (1999).
17. Л. Д. Ландау, Р. Пайерлс, Zeits. für Phys., **69**, 56 (1931); *Собрание трудов*, т.1, М.: Наука, 1969, стр.56.
18. Ю. А. Брычков, А. П. Прудников, *Интегральные преобразования обобщенных функций*, М.: Наука, 1977.
19. E. B. Devis, *Quantum Theory of Open Systems*, Academic Press, London, 1976.
20. A. S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory*, North Holland Publishing Corporation, Amsterdam, 1982; A. S. Holevo, *Lectures on Statistical Structure of Quantum Theory*, 1999, pp.1–177.
21. K. Kraus, *States, Effects and Operations*, Springer-Verlag, Berlin, 1983.
22. P. Busch, M. Grabowski, and P.J.Lahti, *Operational Quantum Physics*, Springer Lecture Notes in Physics, v.**31**, 1995.
23. Н. Н. Боголюбов, А. А. Логунов, И. Т. Тодоров, *Основы аксиоматического подхода в квантовой теории поля*, М.: Наука, 1969.
24. I. Bialynicki-Birula, Phys. Rev. Lett. **80**, 5247 (1998).
25. W. F. Stinespring, *Positive functions on C^* algebras*, Proc. of the Amer. Math. Soc. **6**, 211 (1955).
26. C. A. Fuchs, quant-ph/9601020.
27. А. П. Прудников, Ю. А. Брычков, О. А. Маричев, *Интегралы и ряды, Элементарные функции*, М.: Наука, 1981.
28. C. E. Shannon, *Mathematical Theory of Communication*, Bell Syst. Tech. Jour. **27**, 397; 623 (1948).
29. Р. Галлагер, *Теория информации и надежная связь*, М.: Советское Радио, 1974.
30. I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discreter Memoryless Systems*, Akademiai, Kiado–Budapest, 1981.