Письма в ЖЭТФ, том 100, вып. 9, с. 674 – 682

Волновые функции вытянутого сфероида и мультиплексирование в релятивистской квантовой криптографии на ортогональных состояниях

С. Н. Молотков[1)], *Т. А. Потапова*[+]

Институт физики твердого тела РАН, 142432 Черноголовка, Россия

Академия криптографии РФ, 121552 Москва, Россия

Факультет вычислительной математики и кибернетики, МГУ им. Ломоносова, 119991 Москва, Россия

[+]*Факультет информационных технологий и вычислительной техники, Национальный исследовательский университет "Высшая школа экономики", 101000 Москва, Россия*

Поступила в редакцию 25 сентября 2014 г.

Релятивистская квантовая криптография, кроме геометрических свойств векторов состояний квантовой системы в гильбертовом пространстве, использует свойства носителей квантовых состояний в пространстве-времени Минковского. Физический тип квантового объекта-переносчика информации с предельно допустимой скоростью в пространстве-времени – принципиально важен. Сама структура пространства-времени, точнее неприводимых представлений группы Пуанкаре, в гильбертовом пространстве диктует появление безмассовых частиц – фотонов. В этом смысле релятивистские системы квантовой криптографии для передачи криптографических ключей фактически используют структуру самого пространства-времени. Это позволяет гарантировать секретность ключей даже при применении *ортогональных состояний*.

DOI: 10.7868/S0370274X14210127

Введение. Секретность ключей в нерелятивистской квантовой криптографии основана на геометрических свойствах векторов в гильбертовом пространстве состояний квантовой системы – на запрете копирования и на запрете достоверного различения *неортогональных состояний* [1–3]. *Ортогональные состояния принципиально не могут использоваться в квантовой криптографии*, т.к. они достоверно и без возмущения различимы и могут быть скопированы. Кроме того, свойства векторов состояний, точнее их носителей, в реальном пространстве-времени никак явно не фигурируют. Неважен также и физический тип квантового объекта-переносчика информации (электрон, фотон и т.д.). Важен только вектор состояния квантовой системы.

Для обеспечения секретности криптографических ключей релятивистская квантовая криптография, кроме фундаментальных запретов квантовой механики на различимость квантовых состояний, использует фундаментальные ограничения, диктуемые релятивистской причинностью. Общая идея, лежащая в основе релятивистской квантовой криптографии, физически достаточно прозрачна. Любое квантовое состояние, являясь вектором в комплексном гильбертовом пространстве, имеет носитель в пространстве-времени Минковского. Квантовое состояние есть нормированный вектор. При доступе к ограниченной области пространства-времени вероятность исхода любого измерения квантового состояния не может превышать долю нормировки, которая набирается в данной области. Различение протяженных квантовых состояний требует доступа к конечной области пространства-времени, где сосредоточен носитель состояний. Доступ к конечной области из-за конечности скорости света требует конечного времени, что неизбежно приводит к задержкам исходов измерений на приемной стороне.

Исходная идея релятивистской квантовой криптографии [4] оказалась практически неработоспособной, поскольку потребовалось растягивать квантовые состояния на длину, бóльшую длины канала связи[2)]. В дальнейшем оказалось, что не требуется использовать столь протяженные *неортогональные со-*

[1)]e-mail: sergei.molotkov@gmail.com

[2)]Отметим, что критика Переса [5] работы [4] вполне справедлива, поскольку подслушиватель в канале всегда "видит" *неортогональные состояния*.

стояния. Кроме того, что более существенно, можно гарантировать секретность ключей даже при не строго однофотонном источнике и произвольных меняющихся потерях в канале связи [6] (см. экспериментальную реализацию системы в [7]), что недостижимо для нерелятивистских протоколов квантовой криптографии.

Вопрос о том, можно ли гарантировать секретность ключей при использовании ортогональных состояний с протяженностью, меньшей длины линии связи, до сих пор остается открытым.

Оказывается, что для решения данной задачи, а также спектрального уплотнения (мультиплексирования) при передаче секретных ключей идеально подходят квантовые состояния, которые имеют пространственно-временную форму волновых функций вытянутого сфероида (*Prolate Spheroidal Wave Functions*, PSWF). Одно из основных свойств данных функций, которое гарантирует секретность передаваемых ключей, состоит в том, что при заданной частотной полосе они являются максимально локализованными по времени (пространству). Это не позволяет подслушивателю скомпенсировать задержки при измерениях. Мы сначала опишем основные необходимые для дальнейшего свойства PSWF. Затем мы предъявим сам протокол релятивистского распределения ключей на *ортогональных состояниях* и проведем анализ его стойкости, включая атаки из подвижных систем отсчета.

Основные свойства волновых функций вытянутого сфероида. Волновые функции вытянутого сфероида появились в работах [8–11] в связи задачами передачи частотно-ограниченных сигналов (*band limited signals*). Они возникают следующим образом. Пусть имеется сигнал, описываемый временной функцией $\varphi(t)$ $(-\infty < t < \infty)$. Пусть спектр сигнала сосредоточен в конечной полосе, вне которой он тождественно равен нулю:

$$\varphi(\omega) \equiv \tilde{\varphi}(\omega, \Omega), \quad \omega \in (-W + \Omega, W + \Omega),$$

$$\varphi(t) = \int_{-W}^{W} \varphi(\omega) e^{i\omega t} dt,$$

где Ω – несущая частота (далее мы ее опускаем). Какова должна быть форма сигнала, чтобы он был также максимально локализован и в заданном временном интервале $(-T/2, T/2)$? Иначе говоря, при каких условиях концентрация сигнала $\alpha^2(T)$ по времени достигает максимума

$$\alpha^2(T) = \frac{\int_{-T/2}^{T/2} |\varphi(t)|^2 dt}{\int_{-\infty}^{\infty} |\varphi(t)|^2 dt}? \qquad (1)$$

Условие (1) может быть переписано в виде

$$\alpha^2(T) = \int_{-W}^{W} \int_{-W}^{W} \frac{\sin[\pi T(\omega' - \omega'')]}{\pi(\omega' - \omega'')} \times$$
$$\times \varphi(\omega')\varphi^*(\omega'')d\omega' d\omega'' \left[\int_{-W}^{W} \varphi(\omega')\varphi^*(\omega')d\omega' \right]^{-1}. \qquad (2)$$

Функции с интегрируемым квадратом, $\varphi(\omega) \in \in \mathcal{L}^2(-W, W)$, фигурирующие в (2), должны удовлетворять интегральному уравнению

$$\alpha^2(T)\varphi(\omega) = \int_{-W}^{W} \frac{\sin[\pi T(\omega - \omega')]}{\pi(\omega - \omega')} \varphi(\omega')d\omega'. \qquad (3)$$

Замена переменных $\omega, \omega' \to Wx, Wy$, $\varphi(Wy) = \psi(y)$, $\alpha^2(T) = \lambda$, $c = \pi WT$ приводит (3) к стандартному виду:

$$\lambda\psi(x) = \int_{-1}^{1} \frac{\sin[c(x - y)]}{\pi(x - y)} \psi(y)dy. \qquad (4)$$

Ядро уравнения положительно. Поэтому решения существуют при определенном бесконечном наборе собственных чисел, которые удовлетворяют условию $1 > \lambda_0 \geq \lambda_1 \geq \ldots \geq \lambda_n$ ($\lambda_n \to 0$ при $n \to \infty$). Соответствующие собственные функции $\psi_0(x), \psi_1(x), \ldots, \psi_n(x)$ есть решения интегрального уравнения

$$\lambda_n\psi_n(x) = \int_{-1}^{1} \frac{\sin[c(x - y)]}{\pi(x - y)} \psi_n(y)dy. \qquad (5)$$

Собственные функции (5) обладают замечательным свойством двойной ортогональности [8–11]. Они ортогональны на бесконечном и на конечном интервале по времени (естественно, ортогональны их фурье-образы в конечной частотной полосе):

$$\int_{-\infty}^{\infty} \psi_n(x)\psi_m^*(x)dx = \delta_{nm}, \ \int_{-1}^{1} \psi_n(x)\psi_m^*(x)dx = \lambda_n\delta_{nm}. \qquad (6)$$

(Это свойство будет использовано для квантовых состояний. Ортогональность на конечном временном интервале означает безошибочную различимость соответствующих квантовых состояний.) Кроме того, собственные числа λ_n также имеют замечательное свойство локализации [12].

Многие полезные свойства собственных функций были получены на основе следующего наблюдения. Дифференциальный оператор[3)]

$$\mathcal{D}_x = \frac{d}{dx}\left[(1-x^2)\frac{d}{dx}\right] - c^2x^2 \qquad (7)$$

приводит к задаче на собственные значения на отрезке $(-1,1)$:

$$\frac{d}{dx}\left[(1-x^2)\frac{d\psi(x)}{dx}\right] - c^2x^2\psi(x) = \chi\psi(x), \qquad (8)$$

где собственные числа $0 < \chi_0 \le \chi_1 \le \ldots \le \chi_n$. Собственные функции $\psi_n(x)$ задачи на собственные значения (8) образуют полный ортонормированный набор на отрезке $(-1,1)$ и на интервале $(-\infty,\infty)$ на множестве функций с интегрируемым квадратом $\mathcal{L}^2(-1,1)$. Указанное наблюдение [8–12] состоит в том, что дифференциальный и интегральный операторы (5), (7) коммутируют на множестве функций $\mathcal{L}^2(-1,1)$:

$$\mathcal{D}_x\int_{-1}^{1}\frac{\sin[c(x-y)]}{\pi(x-y)}\psi(y)dy = \int_{-1}^{1}\frac{\sin[c(x-y)]}{\pi(x-y)}\mathcal{D}_y\psi(y)dy. \qquad (9)$$

Отсюда следует, что собственные векторы обоих операторов совпадают. Функции $\psi_n(x)$ имеют n нулей на отрезке $(-1,1)$, являются четными при четном n и нечетными при нечетном n.

Свойство самоподобия. Следующее интересное свойство состоит в самоподобии:

$$\int_{-1}^{1} e^{2\pi ixt}\psi_n(t)dt = \alpha_n(c)\psi_n\left(\frac{2\pi x}{c}\right), \quad -\infty < x < \infty, \qquad (10)$$

т.е. сама функция и ее фурье-образ функционально совпадают и отличаются только масштабным фактором.

Локализация собственных значений. По-видимому, наиболее важным для практических применений является свойство локализуемости собственных чисел (а согласно (1) и собственных функций) в зависимости от параметра $c = 2WT$. При больших значениях этого параметра ($c \gg 1$) имеется примерно $N = 2WT$ собственных чисел λ_n, которые экспоненциально близки к единице по параметру c. Соответственно собственные функции целиком сконцентрированы на конечном интервале $(-1,1)$. Их "хвосты" вне этого интервала экспоненциально малы. Остальные функции с $n > 2WT$ сконцентрированы вне интервала $(-1,1)$ и лишь с экспоненциальной малостью присутствуют внутри него. *Хотя все функции простираются по времени от $-\infty$ до ∞, степень их локализации принципиально различна.* Данное свойство означает, что для функций с конечным частотным спектром $\omega \in (-W,W)$ асимптотически существует только $N = 2WT$ функций (степеней свободы), которые полностью сконцентрированы на конечном временном интервале.

Имеются следующие результаты по асимптотике собственных чисел [12]:

$$\lim_{c\to\infty}\lambda_n = \begin{cases} 0, & n = (1+\eta)\dfrac{2c}{\pi}, \\ (1+e^{\pi b})^{-1}, & n = \dfrac{2c}{\pi} + \dfrac{b}{\pi}\log c, \\ 1, & n = (1-\eta)\dfrac{2c}{\pi}, \end{cases} \qquad (11)$$

где b, η – числа порядка единицы. Из (11) следует, что существует $N = 2WT$ собственных чисел и функций, которые полностью локализованы на интервале $(-1,1)$, а также переходная область небольшого размера $\approx \log(2WT\ )$ по параметру $2WT$ перехода от собственных чисел $\lambda_n = 1$ к собственным числам $\lambda_n = 0$. Качественное поведение собственных чисел как функций параметра $2WT$ приведено на рис. 1.

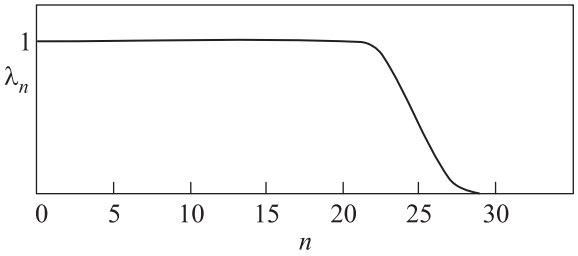

Рис. 1. Значения собственных чисел уравнения (5) (параметр $2c/\pi = 25$)

Имеется также замечательный аналитический результат Фукса [12] по асимптотике собственных чисел:

$$1 - \lambda_n \approx 4\sqrt{\pi}\,8^n a^{2n+1}e^{-2a^2}, \quad a\to\infty, \quad a^2 = c, \qquad (12)$$

полученный путем асимптотического разложения дифференциального уравнения, которое связывает значения собственных функций и собственных чисел:

$$\frac{d\lambda_n(a)}{da} = 4\lambda_n(a)\varphi_n^2(a). \qquad (13)$$

[3)] Данный дифференциальный оператор [13] является оператором для уравнения Гельмгольца (Helmholtz), $\Delta\Phi + k^2\Phi = 0$, для потенциала $\Phi(\xi,\eta,\phi)$ в сфероидальных координатах $x = \xi\eta$, $y = \sqrt{(\xi^2-1)(1-\eta)}\cos\phi$, $z = \sqrt{(\xi^2-1)(1-\eta)}\sin\phi$. Уравнение принимает вид $(\xi^2-1)\frac{d^2\Phi_{nm}(c,\xi)}{d\xi^2} + 2\xi\frac{d\Phi_{nm}(c,\xi)}{d\xi} - [\lambda_{nm}(c) - c^2\xi^2 + \frac{m^2}{\xi^2-1}]\Phi_{nm}(c,\xi) = 0$ ($c = k/2$). При $m = 0$ дифференциальный оператор переходит в (7).

$2WT$-теорема. Для сигналов $\varphi(\omega)$ с ограниченным частотным спектром $\omega \in (-W, W)$ имеет место важная теорема. Ее часто называют теоремой об оцифровке или $2WT$-теоремой. Данная теорема была доказана независимо и в разное время несколькими авторами. Итак, теорема Найквиста–Котельникова–Уитекера–Шеннона [14–17] о представлении частотно-ограниченных сигналов гласит, что

$$\varphi(t) = \sum_{n=-\infty}^{\infty} \varphi(n/2W) \frac{\sin[2\pi W(t - n/2W)]}{2\pi W(t - n/2W)}, \quad (14)$$

где $\varphi(n/2W)$ – амплитуда сигнала в отсчетные моменты времени $t_n = n/2W$. Неформальный смысл данной теоремы сводится к тому, что для восстановления непрерывного сигнала в любой момент времени достаточно знать его значения только в дискретные отсчетные моменты времени. Формально частотно-ограниченный сигнал $\varphi(t)$ не может быть строго локализован в конечном временном интервале T. Он простирается на $t \in (-\infty, \infty)$. Поэтому формально требуются значения сигнала в бесконечном числе отсчетных моментов времени.

Функции вытянутого сфероида придают представлению (14) четкий математический смысл. Среди всех частотно-ограниченных сигналов есть множество сигналов, протяженных по времени T и практически равных нулю вне этого интервала:

$$\int_{|t|>T} |\varphi(t)|^2 dt < \epsilon, \quad (15)$$

где ϵ – сколь угодно малая константа. Такие сигналы могут быть с точностью ϵ приближенно описаны набором из $N = 2WT$ функций вытянутого сфероида $\varphi_i(t)$ [18]:

$$\int_{-T/2}^{T/2} \left[\varphi(t) - \sum_{i=0}^{N(T,\epsilon)} a_i \varphi_i(t) \right]^2 dt < \epsilon. \quad (16)$$

Выражение (16) позволяет придать четкий математический смысл "фольклорному" утверждению: *сигнал с частотно-ограниченным спектром, длящийся по времени T, имеет $N(T, \epsilon) = 2WT$ степеней свободы* (*может быть приближен сколь угодно точно $N(T, \epsilon)$ отсчетными функциями*). Аналогичное (16) свойство имеет место для сигналов с почти ограниченным частотным спектром

$$\int_{|\omega|>2W} |\varphi(\omega)|^2 d\omega < \epsilon'. \quad (17)$$

Асимптотическое число степеней свободы для таких сигналов есть $N(W, \epsilon') = 2WT$. Для сигналов (15) и (17), приближенно ограниченных по частоте и времени, (детали см. в [18])

$$\lim_{T\to\infty} \frac{N(T, W, \epsilon, \epsilon')}{T} = 2W,$$
$$\lim_{W\to\infty} \frac{N(T, W, \epsilon, \epsilon')}{2W} = T. \quad (18)$$

Это означает, что реальный сигнал вовсе не обязан быть строго, например частотно, ограниченным. *Чтобы не усложнять выкладки, ниже мы рассматриваем строго частотно-ограниченные сигналы. Это не меняет результатов и в общем случае.*

Информационные квантовые состояния и их измерение. Квантовые состояния, имеющие пространственно-временную форму PSWF, имеют вид

$$|\varphi_i\rangle = \int_{-W+\Omega}^{W+\Omega} \varphi_i(\omega)|\omega\rangle d\omega = \int_{-W}^{W} \varphi_i(\omega, \Omega)|\omega\rangle d\omega,$$
$$\langle\omega|\omega'\rangle = \delta(\omega - \omega'), \quad (19)$$

где $|\omega\rangle$ – монохроматическое состояние. Далее мы опускаем в аргументе Ω, имея в виду, что $(-W + \Omega, W + \Omega) \in (0, \infty)$. Квадрат модуля $|\varphi_i(\omega)|^2 d\omega$ представляет собой энергию спектральной компоненты поля на частоте ω. Измерение состояний сводится к пропусканию их через частотный фильтр (проектирование на соответствующие состояния поля $|\varphi_i\rangle\langle\varphi_i| = \left(\int_{-W+\Omega}^{W+\Omega} \varphi_i(\omega)|\omega\rangle d\omega\right)\left(\int_{-W+\Omega}^{W+\Omega} \varphi_i^*(\omega')|\omega'\langle d\omega'\right)$) и последующее измерение интегральной интенсивности поля $|\varphi_i(t)|^2$ во временном окне $\int_{-T/2}^{T/2} |\varphi_i(t)|^2 dt$. *Далее везде, где это необходимо, считаем, что временное окно привязано к соответствующему месту в пространстве.* Такое измерительное устройство представляет собой мультиплексор с одним входом и $N = 2WT$ выходами. На выходах стоят детекторы. Они активируются во временном интервале $(-T/2, T/2)$. Каждое из $N = 2WT$ неискаженных состояний на входе даст отсчет с вероятностью $\lambda_i(WT)$ только в i-м канале, отвечающем i-му состоянию.

Амплитуды поля $\varphi_i(\tau) = \int_{-W}^{W} e^{i\omega\tau} \varphi_i(\omega) d\omega$ (где $\tau = x - ct$ – координата на световом конусе) удовлетворяют соотношениям двойной ортогональности [8–11] (см. формулу (6)):

$$\int_{-\infty}^{\infty} \varphi_i(\tau)\varphi_j^*(\tau) d\tau = \delta_{ij},$$
$$\int_{-T/2}^{T/2} \varphi_i(\tau)\varphi_j^*(\tau) d\tau = \lambda_i(WT)\delta_{ij}.$$

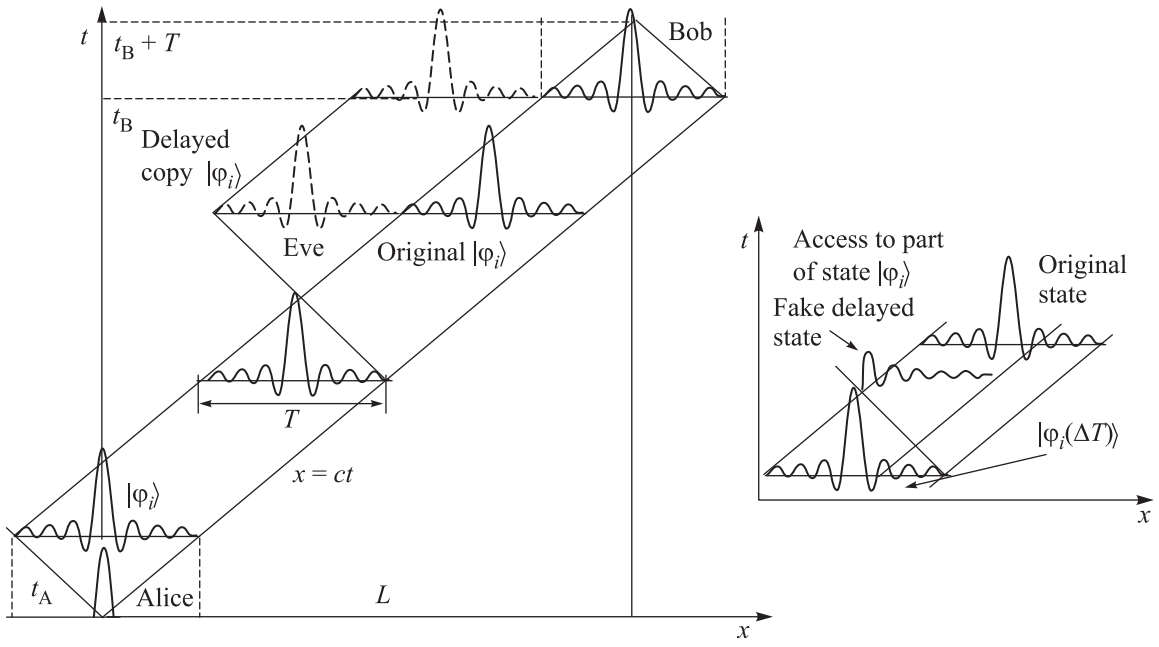

Рис. 2. Процедуры приготовления и детектирования протяженных состояний (слева). Показан также процесс вторжения в канал связи с измерением и приготовлением сдвинутой по времени на T копии исходного состояния. На вставке приведены процессы измерения и приготовления, когда подслушиватель получает доступ только к части носителя состояния ΔT, а затем приготовления ошибочного состояния, сдвинутого назад по времени на величину ΔT по отношению с исходному

Протокол релятивистского квантового распределения ключей на PSWF состояниях.

1. Используется алфавит $\{|\varphi_i\rangle\}_{i=1}^N$ из $N = 2WT$ квантовых состояний. Частотный интервал $(-W, W)$ задан внешними условиями, например окном прозрачности атмосферы. Пространственно-временная протяженность состояний $(-T/2, T/2)$ выбирается из условия, согласно которому подслушиватель не может скомпенсировать задержки при измерениях из-за разности скоростей света в нижних слоях атмосферы и в вакууме (показатель преломления воздуха отличается от единицы в четвертом знаке). Расстояние между передающей и приемной станциями известно (L).

2. Случайно и равновероятно выбирается одно из $N = 2WT$ состояний, которое будет послано в канал связи. Каждая посылка начинается в известный момент времени $t_A = 0$. Алиса в $t_A = 0$ и $x_A = 0$ (рис. 2) готовит сильно локализованное по времени состояние. Протяженность локализованного состояния $\delta T \ll T$. Соответственно частотный спектр $\delta W \gg 2W$.

3. Алиса унитарным образом переводит сильно локализованное состояние в одно из протяженных PSWF-состояний (рис.2). Релятивистская причинность диктует, что такое преобразование требует времени не меньше T (высота передней части светового конуса, выпущенного из точки $t_A = 0$, $x_A = 0$). Далее PSWF-состояние свободно распространяется через канал связи на приемную сторону.

4. Поскольку момент отправки и длина линии связи известны, известно и время прибытия (если не было вторжения в канал) на приемную сторону. Так как протяженные состояния ортогональны, унитарным преобразованием они могут быть переведены в локализованные состояния, которые также будут ортогональными, а значит безошибочно различимыми. Релятивистская причинность диктует минимально необходимое время для такого преобразования (высота прошлой части светового конуса, накрывающего PSWF-состояния; см. рис. 2). Формально измерения описываются разложением единицы:

$$\mathrm{id}_T = \sum_{i=1}^{N} \mathcal{P}_i^L, \quad \mathcal{P}_i^L = |\varphi_i^L\rangle\langle\varphi_i^L|, \tag{20}$$

где $\mathcal{P}_i^L$ – проектор на PSWF-состояния на приемной станции (отметим, что проекторы не локальны в пространстве-времени), id_T – единичный оператор на подпространстве PSWF-состояний. Поскольку состояния ортогональны на интервале $(-T/2, T/2)$, они безошибочно различимы на приемной стороне. Вероятность исхода от i-го состояния равна λ_i. Так как

все $\lambda_i < 1$, иногда отсчетов не будет. Однако это не приводит к ошибкам различения.

5. После передачи серии состояний протокол продолжается аналогично другим протоколам квантового распределения ключей. Подчеркнем, что из-за ортогональности состояний не требуется согласования базисов.

Неформальные причины стойкости протокола относительно подслушивания. Ортогональность (безошибочная различимость) квантовых состояний является нелокальным свойством. Для безошибочного различения одного из ортогональных состояний требуется полный доступ к носителю состояния в пространстве-времени Минковского в той области, на которой набирается ортогональность. Подслушиватель также может безошибочно различать ортогональные состояния. Однако из-за релятивистской причинности (конечности скорости света) доступ к конечной области требует конечного времени. Например, подслушиватель также может сделать унитарное преобразование, преобразующее протяженные ортогональные состояния в ортогональные локализованные (рис. 2). Однако на это требуется конечное время, равное высоте светового конуса, накрывающего носитель состояния. После безошибочного измерения подслушиватель может приготовить копию исходного состояния, что также требует конечного времени, равного высоте передней части светового конуса, выпущенного из точки получения исхода измерения. При этом копия неизбежно окажется сдвинутой назад по времени относительно свободно распространяющихся исходных состояний (см. рис. 2). Задержанное состояние не прибудет на приемную станцию в нужный момент времени и не будет зарегистрировано (как в данном примере, когда подслушиватель целиком задерживает состояние). Подслушиватель не обязан пытаться "накрывать" всю область носителя состояния световым конусом. Он может попытаться получить доступ лишь к части носителя состояния (см. вставку к рис. 2). Имея доступ только к части носителя ортогональных состояний, подслушиватель будет видеть эффективно неортогональные состояния. Пусть доступна часть носителя $\Delta T < T$. Соответствующими состояниями являются $|\varphi_i(\Delta T)\rangle$. Неортогональные состояния уже принципиально не могут быть безошибочно различимы. Однако доступ даже к части носителя требует конечного времени (см. вставку к рис. 2), зависящего от протяженности области носителя. Необходимое время не меньше высоты прошлой части светового конуса, накрывающего часть области носителя. После различения состояний, но уже с некоторой ошибкой из-за эффективной неортогональности подслушиватель может приготовить свое состояние протяженностью T. Это также потребует конечного времени. Ошибочное состояние подслушивателя прибудет на приемную сторону вовремя, но даст отсчет с ошибкой, что приведет к детектированию подслушивателя. Таким образом, осталось связать наблюдаемую ошибку на приемной стороне с задержкой подслушивателя и, соответственно, с получаемой им информацией о передаваемых состояниях.

Измерения на приемной стороне используют проекцию на состояния в конечной частотной полосе (аналог частотного фильтра). При заданной частотной полосе PSWF являются самыми короткими по времени среди состояний. Поэтому атака, когда подслушиватель задерживает состояние (получает результат в конце заднего фронта, а взамен сразу посылает короткое по времени и, соответственно, с широким спектром состояние), не проходит. Фильтр на приемной стороне не позволяет подслушивателю подменить истинные состояния более короткими.

Длина секретного ключа. Пусть подслушиватель получает доступ к части носителя состояния ΔT (см. вставку к рис. 2). В дальнейшем это приведет к задержке результатов измерений на приемной стороне. Вероятность для подслушивателя получить исход в j-м канале измерений, если исходное состояние – i-е, есть

$$p_{\mathrm{A|E}}(j|i) = \left| \int_{-T/2}^{-T/2+\Delta T} \varphi_i(\tau)\varphi_j^*(\tau)d\tau \right|^2 . \qquad (21)$$

Условная вероятность в (21) является растущей функцией задержки ΔT. При $\Delta T \to T$ она стремится к $\lambda_i \approx 1$. Взаимная информация между подслушивателем и передающей стороной равна

$$I(\mathrm{A;E},\Delta T) = \sum_{i=1}^{N}\sum_{j=1}^{N} p_{\mathrm{AE}}(i,j)\log\frac{p_{\mathrm{AE}}(i,j)}{p_{\mathrm{A}}(i)p_{\mathrm{E}}(j)},$$

$$p_{\mathrm{AE}}(i,j) = p_{\mathrm{A|E}}(j|i)p_{\mathrm{A}}(i), \quad p_{\mathrm{E}}(j) = \sum_{i=1}^{N} p_{\mathrm{AE}}(i,j), \qquad (22)$$

где $p_{\mathrm{A}}(i) = 1/N$, поскольку состояния посылаются равновероятно.

Подслушиватель перепосылает то состояние, которое он интерпретировал как результат своих измерений. Соответствующие переходные вероятности на приемной стороне при наличии подслушивателя равны

$$p_{\mathrm{A|B}}(k|i) = \sum_{j=1}^{N} p_{\mathrm{B|E}}(j|k)p_{\mathrm{A|E}}(j|i). \qquad (23)$$

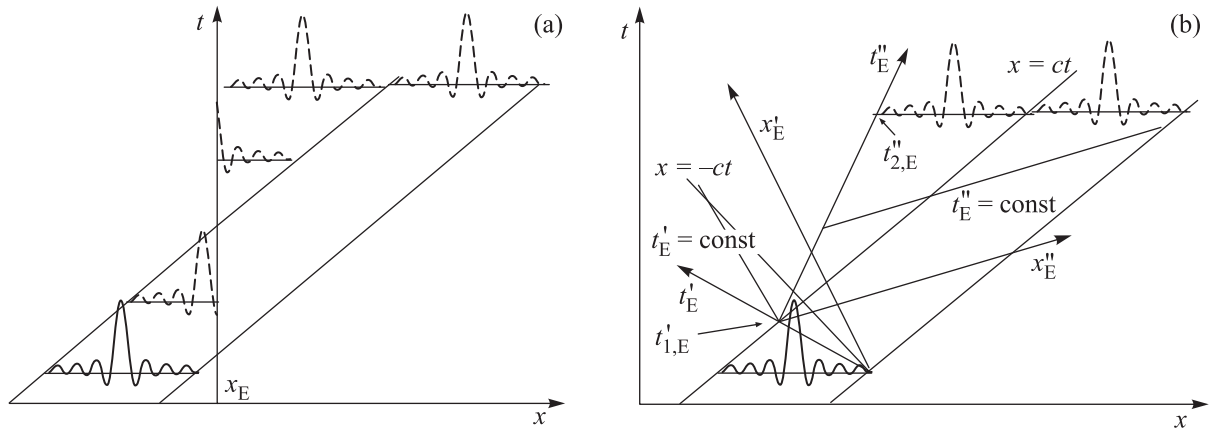

Рис. 3. (a) – Схема процессов измерения и приготовления копии исходного состояния локальным прибором, расположенным в точке $x_{\rm E}$. (b) – Аналогичные процессы в подвижной системе отсчета подслушивателя $(t'_{\rm E}, x'_{\rm E})$, движущейся навстречу состоянию при измерении, и системе $(t''_{\rm E}, x''_{\rm E})$, движущейся навстречу приемной станции при приготовлении копии

Условная вероятность $p_{B|E}(j|k)$ в (23) является убывающей функцией задержки ΔT, вносимой подслушивателем. Величина

$$p_{\rm B|E}(k|j) = \left| \int_{-T/2}^{T/2} \varphi_k(\tau)\varphi_j(\tau - \Delta T)d\tau \right|^2 \qquad (24)$$

есть вероятность получить исход в k-м канале измерений (при проектировании на k-е состояние) от задержанного на время ΔT j-го состояния. Соответственно взаимная информация между передающей и приемной сторонами равна

$$I({\rm A{:}B}, \Delta T) = \sum_{i=1}^{N}\sum_{k=1}^{N} p_{\rm AB}(i,k)\log\frac{p_{\rm AB}(i,k)}{p_{\rm A}(i)p_{\rm B}(k)},$$

$$p_{\rm AB}(i,k) = p_{\rm A|B}(k|i)p_{\rm A}(i), \quad p_{\rm B}(k) = \sum_{i=1}^{N} p_{\rm AB}(i,k). \qquad (25)$$

После передачи длинной серии посылок передающая сторона случайным образом раскрывает часть переданных состояний (впоследствии эта часть выбрасывается). Указываются посылки, в которых посылалось состояние $|\varphi_0\rangle$, посылки, где было $|\varphi_1\rangle$, и т.д. Это позволяет оценить для каждого состояния долю ошибочных отсчетов и, соответственно, переходные вероятности в (18), а далее – параметр ΔT, переходные вероятности подслушивателя и взаимную информацию в (17) и (20). Отметим, что подслушиватель может подслушивать не все посылки, а только их часть. Данные оценки дают возможность после исправления ошибок через открытый канал и дальнейшего сжатия (хеширования) очищенного ключа до нужной величины, зависящей от процента ошибок, получить секретный ключ в асимптотическом пределе длинных последовательностей размером

$$R = I({\rm A{:}B}, \Delta T) - I({\rm A{:}E}, \Delta T) \qquad (26)$$

в пересчете на одну позицию. Полное доказательство секретности требует бóльшего места и будет приведено отдельно.

Атака на передаваемый ключ из движущейся системы отсчета. Поскольку секретность ключей в релятивистской квантовой криптографии основана на фундаментальных ограничениях специальной теории относительности, неизбежно требуется рассмотреть атаки на передаваемый ключ из движущихся систем отсчета. Выше были рассмотрены атаки подслушивателя из неподвижной по отношению к приемной и передающим станциям системы отсчета. На первый взгляд замедление времени в подвижной системе отсчета, *движущейся сначала в одном направлении, а затем в противоположном, приводит к замедлению времени по отношению к неподвижной системе (так называемый парадокс близнецов)*. (Наиболее компактное и четкое объяснение данного парадокса можно найти в [19].) Это могло бы приводить к экономии времени при измерениях квантовых состояний. Беглое интуитивное соображение сводится к следующему. Если подслушиватель движется навстречу квантовому состоянию, то, казалось бы, он может "просмотреть" его за более короткое время. Однако сразу возникает контраргумент: скорость света (распространения квантового состояния) инвариантна, т.е. одинакова во всех системах отсчета. Поэтому имеет смысл чуть более детально рассмотреть данную ситуацию. Как будет видно ни-

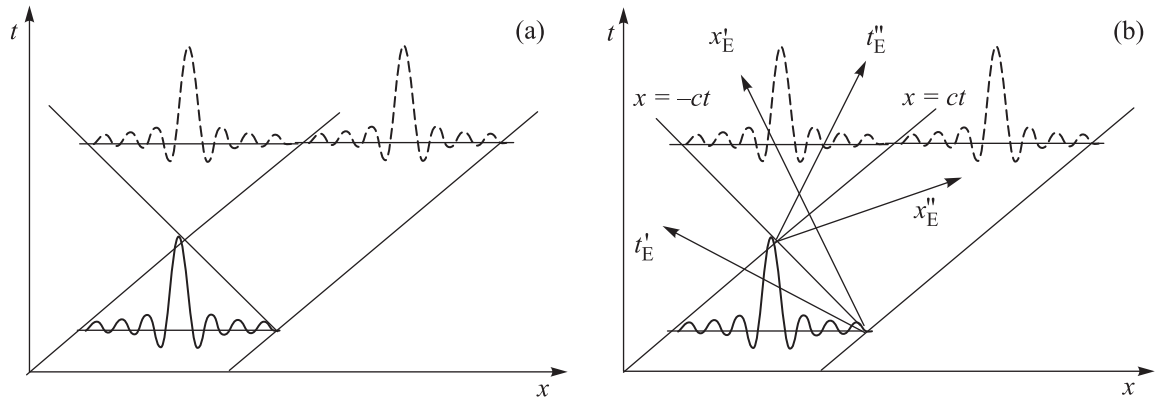

Рис. 4. (a) – Схема процессов измерения и приготовления состояния нелокальным в пространстве прибором в неподвижной системе отсчета подслушивателя. (b) – То же самое в движущихся системах отсчета. Направление движения систем отсчета аналогично рис. 3b

же, атаки из движущихся систем отсчета ничего, по сути, не меняют для подслушивателя. Рассмотрим две ситуации.

1. Измерения подслушивателя осуществляются локальным прибором в неподвижной системе отсчета, расположенным в точке x_E (рис. 3a). Такая ситуация реализуется в экспериментах по "остановке" света. Используется атомный ансамбль, система уровней которого представляет Λ-конфигурацию (детали см. в [20]). Фактически происходит совместная унитарная эволюция, управляемая внешним классическим полем, по преобразованию (перекачке) состояния поля в атомные степени свободы, точнее в исходное состояние двух систем: атомный ансамбль в основном состоянии $|\mathrm{ground}\rangle_{\mathrm{at}}$ и однофотонное состояние поля $|\varphi\rangle_{\mathrm{phot}}$ (где φ – пространственная форма однофотонного пакета). В результате совместной эволюции

$$|\mathrm{ground}\rangle_{\mathrm{at}} \otimes |\varphi\rangle_{\mathrm{phot}} \to U_{\mathrm{at,phot}}\left(|\mathrm{ground}\rangle_{\mathrm{at}} \otimes |\varphi\rangle_{\mathrm{phot}}\right) = \\ = |\mathrm{st.ex}\rangle_{\mathrm{at}} \otimes |\mathrm{vac}\rangle_{\mathrm{phot}} \qquad (27)$$

состояние фотонного поля оказывается вакуумным (отсутствие реального фотона), а атомная система переходит в некоторое устойчивое возбужденное состояние. Оператор эволюции зависит от внешнего управляющего классического поля, позволяющего перевести атомную систему из возбужденного промежуточного состояния, из которого возможна спонтанная рекомбинация в $|\mathrm{ground}\rangle_{\mathrm{at}}$, в устойчивое возбужденное состояние $|\mathrm{st.ex}\rangle_{\mathrm{at}}$, из которого рекомбинация на основной уровень запрещена правилами отбора. Внешнее поле позволяет осуществить эволюцию (27) обратимым образом:

$$U^{-1}_{\mathrm{at,phot}}\left(|\mathrm{st.ex}\rangle_{\mathrm{at}} \otimes |\mathrm{vac}\rangle_{\mathrm{phot}}\right) = |\mathrm{ground}\rangle_{\mathrm{at}} \otimes |\varphi\rangle_{\mathrm{phot}}. \qquad (28)$$

Такая эволюция требует конечного времени T, которое необходимо для того, чтобы весь однофотонный пакет достиг атомной системы. Обратная эволюция требует того же времени: пакет длительностью T должен "покинуть" систему. Это будет приводить к задержкам как при измерении, так и при приготовлении состояния. Данный процесс в неподвижной системе отсчета схематически показан на рис. 3a.

Аналогичный процесс в подвижной системе отсчета показан на рис. 3b. Подслушиватель движется навстречу состоянию поля. Передний фронт пакета расположен в начале координат подвижной системы отсчета подслушивателя, а задний (левый) движется по оси t'_E по мировой линии $x = ct$. В момент $t'_{1,E}$ он оказывается перекачен в атомные степени свободы. Далее подслушиватель переходит в систему отсчета, движущуюся в сторону приемной станции, пытаясь скомпенсировать потерю времени. В момент времени t''_E в координате x''_E он инициирует приготовление состояния, что может быть реализовано только к моменту времени $t''_{1,E}$. Как видно рис. 3b, состояние оказывается задержанным по отношению к свободно распространяющемуся исходному состоянию на величину его протяженности T. (Для большей наглядности копия состояния показана в исходной неподвижной системе координат.)

Ситуация, показанная на рис. 4 отвечает измерению состояния распределенным в пространстве прибором, который в один и тот же момент имеет доступ сразу ко всей пространственной области, где присутствует состояние. Рис. 4a отвечает атаке из

неподвижной системы отсчета подслушивателя. Измерение и дальнейшее приготовление копии состояния требуют "накрытия" носителя состояния прошлой частью светового конуса при измерении и передней – при приготовлении. На рис. 4b показана атака подслушивателя из подвижной системы отсчета, движущейся навстречу состоянию при измерении. Приготовление копии состояния происходит из системы отсчета, движущейся в сторону приемной станции. Обе процедуры требуют накрытия пространственной области, равной протяженности носителя состояния, световым конусом, который является лоренц-инвариантом, не зависящим от системы отсчета. Как видно из рис. 4b, атаки из подвижных систем отсчета приводят ровно к такой же задержке по времени копии состояния относительно исходного, как и атаки из неподвижных систем отсчета.

Выражаем благодарность С.П. Кулику за полезные обсуждения. С.Н.М. благодарит коллег по Академии криптографии РФ за постоянную поддержку.

1. W. K. Wooters and W. H. Zurek, Nature **299**, 802 (1982).
2. C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
3. 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.
4. L. Goldenberg and L. Vaidman, Phys. Rev. Lett. **75**, 1239 (1995).
5. A. Peres, Phys. Rev. Lett. **77**, 3264 (1996).
6. S. N. Molotkov, JETP **112**, 370 (2012); JETP Lett. **94** 469 (2011); JETP Lett. **96**, 342 (2012).
7. I. V. Radchenko, K. S. Kravtsov, S. P. Kulik, and S. N. Molotkov, arXiv:quant-ph/1403.3122; Laser Phys. Lett. **11**, 065203 (2014).
8. D. Slepian and H. O. Pollak, Bell Syst. Tech. J. **40**, 43 (1961).
9. H. J. Landau and H. O. Pollak, Bell Syst. Tech. J. **40**, 65 (1961).
10. H. J. Landau and H. O. Pollak, Bell Syst. Tech. J. **41**, 1295 (1962).
11. D. Slepian, Bell Syst. Tech. J. **43**, 3009 (1964).
12. W. H. J. Fuchs, J. Math. Analysis and Appl. **9**, 317 (1964).
13. R. Courant and D. Hilbert, *Methods in Mathematical Physics*, Interscience Publishers, N.Y. (1955), v. I.
14. В. А. Котельников, *О пропускной способности "эфира" и проволоки в электросвязи*, Всесоюз. энерг. комиссия, Материалы к первому всес. съезду по вопросам реконстр. дела связи и разв. слаботочной промыш. (1933).
15. H. Nyquist, *Certain topics in telegraph transmission theory*, AIEE trans., April (1928), p. 617.
16. J. Whittteker, *Interpolation function theory*, Cambridge tracts in Mathematics and Math. Phys., IV, Cambr. Univ. Press (1935).
17. C. Shannon, PIRE **37**, 10 (1949).
18. D. Slepian, Proc. IEEE, **64**, 292 (1976).
19. C. G. Darwin, Nature **180**, 976 (1957).
20. M. Fleischhauer and M. D. Lukin, Phys. Rev. Lett. **84**, 5094 (2000).