ЖЭТФ, 2001, том 119, вып. 5, стр. 1001–1010

ПРОСТОЕ ДОКАЗАТЕЛЬСТВО БЕЗУСЛОВНОЙ СЕКРЕТНОСТИ РЕЛЯТИВИСТСКОЙ КВАНТОВОЙ КРИПТОГРАФИИ

С. Н. Молотков*[*], *С. С. Назин

Институт физики твердого тела Российской академии наук
142432, Черноголовка, Московская обл., Россия

Поступила в редакцию 27 июня 2000 г.

Предложено простое доказательство безусловной секретности релятивистской квантовой криптосистемы на ортогональных состояниях. Ограничения, накладываемые специальной теорией относительности, позволяют заметно упростить доказательство по сравнению с нерелятивистскими криптосистемами на неортогональных состояниях. Для данного протокола существенна пространственно-временная структура квантовых состояний, которая не учитывается в нерелятивистских протоколах, где используются только свойства пространства состояний носителей информации. Как следствие, упрощение возникает из-за неэффективности коллективных измерений подслушивателя, учет которых представляет особую трудность в нерелятивистском случае.

PACS: 89.70.+c, 03.65.-w

1. ВВЕДЕНИЕ

Нерелятивистская квантовая криптография, в отличие от классической криптографии, основанной на законах классической физики, базируется на фундаментальных законах нерелятивистской квантовой механики [1, 2]. Секретность классической криптографии основывается на недоказанной сложности вычисления определенных функций, например, дискретного логарифма. При этом подразумевается, что вычисления функции и обратной к ней будут осуществляться на физическом устройстве, работающем по законам классической физики. Неявно также подразумевается, что распространение информации между легитимными пользователями осуществляется при помощи классических объектов. Поскольку законы классической физики не запрещают одновременное и без возмущения измерение любых динамических переменных классической системы, в рамках классической физики невозможно устроить гарантированное детектирование попыток подслушивания при передаче информации от одного легитимного пользователя к другому. Поэтому секретность классических криптосистем не может быть основана на детектировании попыток подслушивания при распространении ключа и базируется лишь на экспоненциальной сложности вычисления информации о ключе.

Законы классической физики являются лишь приближенным описанием действительности. Более точное описание дает нерелятивистская квантовая механика. Квантовая механика позволяет в принципе реализовать вычислительное устройство (квантовый компьютер), обладающее для ряда задач бóльшей вычислительной мощностью по сравнению с классическим вычислительным устройством. Задача факторизации, которая возникает при расшифровке ключа подслушивателем, в ряде классических криптосистем с открытым ключом является экспоненциально трудоемкой (неразрешимой) для классического компьютера, и становится лишь полиномиально трудоемкой (разрешимой) для квантового компьютера [3]. Поэтому законы нерелятивистской квантовой механики не позволяют построить безусловно секретный обмен информацией с использованием известных классических алгоритмов. Под безусловной секретностью понимается секретность, основанная на запретах, диктуемых фундаментальными законами природы, а не технических (вычислительных) сложностях.

Запрещая безусловно секретную классическую криптографию (в том смысле, как это сказано вы-

[*]E-mail: molotkov@issp.ac.ru

ше), квантовая механика открывает возможности для квантовой криптографии. Квантовая криптография основывается на детектировании попыток подслушивания, что гарантируется законами квантовой механики, когда в качестве носителей информации используются квантовые системы.

Нерелятивистская квантовая криптография базируется на двух обстоятельствах, диктуемых постулатами нерелятивистской квантовой механики.

1. Неизвестное квантовое состояние не может быть скопировано (no cloning-теорема) [4].

2. Невозможно получить информацию о квантовых состояниях, принадлежащих неортогональному базису, без их возмущения [5].

Для ортогональных состояний в нерелятивистской квантовой механике подобный запрет отсутствует. Более того, нет запретов на мгновенное и без возмущения различение ортогональных состояний. Поэтому использование ортогональных состояний для нерелятивистских квантовых криптосистем даже не обсуждается.

Нерелятивистские квантовые криптосистемы по существу не используют пространственно-временную специфику квантовых состояний (поскольку и no cloning-теорема, и утверждение о невозможности получения информации о квантовых состояниях, принадлежащих неортогональному базису, без их возмущения носят совершенно общий характер). В нерелятивистских квантовых криптографических протоколах используются лишь свойства гильбертова пространства состояний носителей информации. Эффекты распространения состояний между удаленными пользователями явно не учитываются, поскольку являются несущественными. Говоря точнее, из-за отсутствия предельной скорости распространения, попытки привлечь пространственно-временную специфику состояний, по-видимому, не могут привести к чему-то новому применительно к задачам квантовой криптографии.

Аккуратное доказательство безусловной секретности нерелятивистских квантовых протоколов обмена, когда действия как подслушивателя, так и легитимных пользователей ограничены лишь законами квантовой механики, представляет собой очень трудную задачу. На сегодняшний день имеется несколько доказательств различной степени сложности и проведенных при различных исходных предположениях. Однако ввиду сложности проблемы единое общепринятое мнение отсутствует [6–9].

Нерелятивистская квантовая механика, так же как классическая физика, является приближенным описанием природы. Более полное описание, учитывающее пространственно-временную структуру и ограничения, накладываемые специальной теорией относительности, дает релятивистская квантовая теория. Последняя, из-за отсутствия осмысленной интерпретации релятивистской квантовой механики, сразу возникает как квантовая теория поля.

Квантовая теория поля не закрывает нерелятивистскую квантовую криптографию, так как состояния квантовополевых систем, так же как и в нерелятивистской квантовой механике, описываются лучами в физическом гильбертовом пространстве [10]. Поскольку нерелятивистские квантовые криптографические протоколы используют лишь свойства состояний в гильбертовом пространстве, нерелятивистские протоколы выживают и в теории поля. Существенно новое для криптографических задач квантовая теория поля может дать только при явном учете пространственно-временной структуры состояний в протоколах. Точнее говоря, лишь при учете того обстоятельства, что хотя сами состояния описываются так же, как в нерелятивистской квантовой механике, лучами в гильбертовом пространстве, они порождаются полевыми операторами (точнее, обобщенными функциями с операторными значениями), в которых и заложена информация о структуре пространства-времени. Полевые операторы подчиняются коммутационным соотношениям, выражающим принцип микропричинности. Последний является следствием ограничений, накладываемых теорией относительности — отсутствие причинно-следственной связи для точек пространства-времени Минковского, разделенных пространственноподобным интервалом. Кроме того, теория поля явно позволяет учитывать и использовать при построении криптографических протоколов эффекты распространения состояний в пространстве-времени Минковского.

Ограничения, накладываемые теорией поля и специальной теорией относительности, приводят к существенному отличию для ряда задач квантовой теории информации (см. подробности [11, 12]) по сравнению с нерелятивистским случаем. Впервые ограничения, накладываемые специальной теорией относительности на измеримость квантовых состояний, обсуждались еще в работе Ландау и Пайерлса в 1931 г. [13]. Качественные соображения работы [13], основанные на рассмотрении соотношений неопределенности вместе с ограничениями для предельной скорости, привели к выводу о том, что в релятивистской области оказывается уже невозможным точное определение, например, импульса (в отличие от нерелятивистского случая) ни за какое ко-

нечное время.

Ниже приведем простой пример безусловно секретной релятивистской квантовой криптосистемы в канале с шумом, использующей в качестве носителей информации состояния квантованного поля (фотонов). Из-за более ограничительных законов релятивистской квантовой теории поля доказательство безусловной секретности сильно упрощается по сравнению с нерелятивистским случаем. Кроме того, данная схема достаточно просто может быть реализована экспериментально, в отличие от безусловно секретных протоколов обмена в нерелятивистском случае, где при доказательстве секретности существенно используются коллективные измерения, которые неясно как реализовать экспериментально. Данная схема явно использует причинно-следственные эффекты и лишь индивидуальные измерения.

Приводимые ниже рассуждения навеяны работой [14], которая, на наш взгляд, не была правильно оценена [15]. Дальнейшие усовершенствования [16] свели ее фактически к нерелятивистской криптосистеме на неортогональных состояниях, по сути выбросив основную новую идею.

Основная идея состоит в том, что «внутренние» степени свободы квантового поля (спиральности фотона) используются для кодирования передаваемой информации, а пространственные степени свободы — для детектирования подслушивания. Этот существенно новый момент по сравнению с нерелятивистским случаем позволяет при учете требований специальной теории относительности детектировать попытки подслушивания по задержке передаваемого состояния и гарантировать получение нулевой информации подслушивателем. Тот факт, что передаваемые состояния являются состояниями квантованного поля, также важен для протокола.

Квантовая теория поля позволяет использовать для криптосистем даже ортогональные состояния. Поскольку в релятивистском случае, так же как и в нерелятивистском, состояния системы описываются лучами в гильбертовом пространстве состояний, остаются справедливыми запреты на клонирование неизвестного состояния и на достоверную без возмущения различимость неортогональных состояний (поскольку при доказательстве этих требований используются только свойства пространства состояний).

Для дальнейшего будут важны два обстоятельства, диктуемые квантовой теорией поля (см. подробности в [17, 18]).

1. Для достоверного различения пары ортогональных состояний свободного квантованного поля требуется доступ ко всей области пространства-времени Минковского, где отличен от нуля носитель состояния. Ортогональные состояния свободного квантованного поля достоверно и без возмущения различимы формально лишь за бесконечное время из-за принципиальной нелокализуемости — невозможности сконструировать состояния поля с компактным носителем в координатном пространстве, порождаемые в четырехмерном импульсном пространстве носителями, заданными на массовой поверхности.

2. Теорией допускается существование свободных квантованных полей, сколь угодно сильно локализованных в пространстве-времени (с любой степенью локализации и убыванием, сколь угодно близким к экспоненциальному).

Принципиальная нелокализуемость диктуется локальным характером квантовой теории поля.

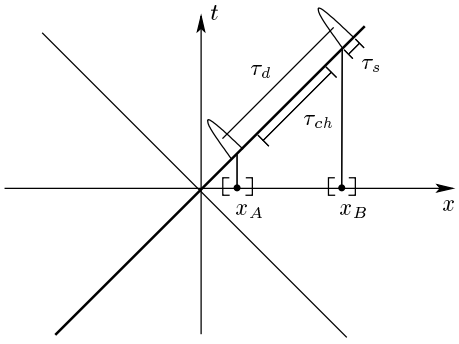
Последнее обстоятельство существенно для криптографии, поскольку позволяет приготавливать состояния, сколь угодно сильно локализованные, т. е. так, чтобы состояния имели наперед заданные сколь угодно малые и сколь угодно близкие к экспоненциальным хвосты вне контролируемой легитимными пользователями области пространства-времени. Вероятность различения двух ортогональных состояний квантованного поля может варьироваться за счет эффектов распространения поля из контролируемой области пространства-времени Минковского в доступную для измерений область, от $1/2$ (полная неразличимость) до 1 (достоверная различимость). Точнее говоря, вероятности получения результата за конечное время, за счет приготовления сильно локализованных состояний поля, могут отличаться от $1/2$ или от 1 на сколь угодно малую заранее выбранную величину. Этот параметр может быть выбран с огромным запасом самым малым в задаче. Из-за существования предельной скорости распространения как квантованного поля, так и классических (в том числе измерительных) объектов, доступ ко всей области существования поля, состоящего из двух сколь угодно сильно локализованных, но разнесенных в пространстве «половинок», может быть принципиально получен лишь за конечное время. Поэтому по мере получения информации вероятность различения состояний меняется от $1/2$ до 1 принципиально за конечное время. Сильная локализация «половинок», разнесенных на τ_d, позволяет устроить протокол так, что вероятность различения $P(\tau) = 1/2$ при $0 \le \tau < \tau_d$, и скачком возрастает до $P(\tau) = 1$ при $\tau = \tau_d$ (на масштабе $\Delta\tau \ll \tau_d$ локализации состояния). Размазывание скачка регулирует-

ся локализацией каждой «половинки» состояния и может быть сделана экспоненциально сколь угодно малой.

Поскольку релятивистская квантовая криптография явно использует пространственно-временную структуру состояний, доказательство секретности не может быть проведено без учета конкретной геометрии системы и должно явно ее учитывать, в отличие от нерелятивистского случая, в котором используется только структура пространства состояний.

2. ИЗМЕРЕНИЯ, ИСПОЛЬЗУЕМЫЕ В ПРОТОКОЛЕ

Рассмотрим теперь измерения, используемые в протоколе. Поскольку необходимо учитывать конкретную геометрию, будем рассматривать простую одномерную модель, которая содержит все особенности, диктуемые теорией поля. Будем рассматривать частицы (кванты поля), движущиеся со световой скоростью и спектром на одномерной массовой поверхности (передней части одномерного светового конуса в импульсном представлении, $k^2 - k_0^2 = 0$). Каждый из пользователей, A и B, контролирует окрестности точек $x_{A,B}$ (см. рисунок). Размеры контролируемых областей в окрестностях точек диктуются локализованностью состояний и могут быть сделаны сколь угодно малыми (должны быть порядка величины локализации состояний). В такой геометрии достаточно рассматривать состояния, распространяющиеся от x_A к x_B с импульсами $k > 0$. Все состояния заданы на одной ветви светового конуса $\tau = x - t$ ($c = 1$). Гильбертово пространство состояний носителей есть $\mathcal{H}_k \otimes \mathbf{C}^2$, где $\mathcal{H}_k$ относится к пространственным, а $\mathbf{C}^2$ — к внутренним (поляризационным) степеням свободы.



Рассмотрим пару ортогональных состояний:

$$|\psi_{0,1}\rangle = \frac{1}{\sqrt{2}} \int\limits_0^\infty f(k)|k\rangle \otimes (|+\rangle \pm |-\rangle)dk, \qquad (1)$$

где $|\pm\rangle \in \mathbf{C}^2$ — ортогональные базисные состояния, и

$$\langle k|k'\rangle = \delta(k-k'), \quad k,k' > 0, \quad \int\limits_0^\infty |f(k)|^2 dk = 1.$$

В координатном представлении состояния на ветви одномерного светового конуса имеют вид

$$|\psi_{0,1}\rangle = \frac{1}{\sqrt{2}} \int\limits_{-\infty}^\infty f(\tau)|\tau\rangle \otimes (|+\rangle \pm |-\rangle)d\tau, \qquad (2)$$
$$\tau = x - t,$$

$$|\tau\rangle = \int\limits_0^\infty e^{-ik\tau}|k\rangle dk, \quad f(\tau) = \int\limits_0^\infty e^{ik\tau} f(k)dk.$$

Базис $\{|\tau\rangle\}$ неортогонален:

$$\langle\tau|\tau'\rangle = \delta_+(\tau-\tau') \neq \delta(\tau-\tau').$$

Измерение, позволяющее достоверно различать данную пару ортогональных состояний, дается разложением единицы в $\mathcal{H}_k \otimes \mathbf{C}^2$ (и аналогично разложением в $\mathcal{H}_\tau \otimes \mathbf{C}^2$, здесь $\mathcal{H}_\tau$ — пространство, изоморфное $\mathcal{H}_k$, натянутое на базис $\{|\tau\rangle\}$).

Измерение представляется в виде

$$\mathcal{M}_0 + \mathcal{M}_1 = I_k \otimes I_{\mathbf{C}^2}, \qquad (3)$$
$$\mathcal{M}_{0,1} = I_k \otimes \mathcal{P}_{0,1} = I_\tau \otimes \mathcal{P}_{0,1},$$

$$\mathcal{P}_0 = |0\rangle\langle 0|, \quad \mathcal{P}_1 = |1\rangle\langle 1|,$$

$$|0\rangle = \frac{1}{\sqrt{2}}\left(|+\rangle + |-\rangle\right), \quad |1\rangle = \frac{1}{\sqrt{2}}\left(|+\rangle - |-\rangle\right),$$

$$I_k = \int\limits_0^\infty |k\rangle\langle k|dk = I_\tau =$$

$$= \int\limits_{-\infty}^\infty |\tau\rangle\langle\tau|d\tau = \int\limits_{-\infty}^\infty \mathcal{M}(d\tau), \qquad (4)$$

$$\mathcal{M}(d\tau) = \left(\int\limits_0^\infty e^{-ik\tau}|k\rangle dk\right)\left(\int\limits_0^\infty e^{ik'\tau}\langle k'|dk'\right)d\tau.$$

Отметим, что измерение (4) является нелокальным на световом конусе.

Носитель состояния $f(\tau)$ на световом конусе может быть выбран сколь угодно сильно локализованным в пределе $|f(\tau)|^2 \to \delta(\tau)$. Строго говоря, в теории поля состояния, заданные на массовой поверхности, не могут иметь компактного носителя в пространстве-времени Минковского. Однако можно построить состояние, сколь угодно сильно локализованное, с хвостами сколь угодно близкими к экспоненциальным [18]. Последнее означает, что может быть выбрано такое временное окно $\Delta\tau$, что вероятность регистрации состояния в данном временном окне может быть сделана сколь угодно близкой к единице. Будем считать, что состояние (фактически форма пакета $f(\tau)$) и интервал $\Delta\tau$ выбраны так, что вероятность регистрации вне временного окна $\Delta\tau$ за счет «хвостов» состояния, не вмещающихся в $\Delta\tau$, может быть сделана экспоненциально сколь угодно близкой к нулю. Этот параметр далее считаем с запасом самым малым параметром в задаче. Более точно, вероятность результата измерения входных состояний $|\psi_{0,1}\rangle$ во временном окне $\Delta\tau$ в канале 0 (канал, отвечающий $\mathcal{P}_0$) и, соответственно, в канале 1 ($\mathcal{P}_1$) (см. формулу (4)) имеет вид

$$\begin{aligned}\Pr\{\Delta\tau, |\psi_{0,1}\rangle\} = \\ = \mathrm{Tr}\left\{\left(\left(\int\limits_{-\Delta\tau}^{\Delta\tau}\mathcal{M}(d\tau)\right)\otimes\mathcal{P}_{0,1}\right)|\psi_{0,1}\rangle\langle\psi_{0,1}|\right\} = \\ = \int\limits_{-\Delta\tau}^{\Delta\tau}|f(\tau)|^2 d\tau = 1-\delta,\end{aligned}$$

где величина δ набирается за счет хвостов состояния

$$\int\limits_{|\tau|>\Delta\tau}|f(\tau)|^2 d\tau = \delta \to 0.$$

Иначе говоря, в задаче имеются два развязанных между собой параметра: $\Delta\tau$ — характерная величина локализации состояния (интервал выбирается так, чтобы интеграл от квадрата амплитуды состояния $f(\tau)$ на нем был сколь угодно близок к единице); τ_d — величина раздвижки двух «половинок» состояния, которая должна быть такой, чтобы хвосты от «половинок» с любой наперед заданной точностью не дотягивались друг до друга ($\Delta\tau \ll \tau_d$). Далее для удобства рассуждений (с учетом сделанных оговорок) будем считать носитель компактным, так как это не повлияет на окончательный результат.

Сделаем одно замечание. Обсуждаемое измерение нельзя трактовать как измерение с длительностью по времени $\Delta\tau$. При каждом акте результат измерения (показание классического прибора, например, фотодетектора с малой постоянной времени (формально бесконечно малой) и работающего в ждущем режиме) возникает в случайный момент времени $(\tau, \tau+d\tau)$ с плотностью вероятности

$$\begin{aligned}\Pr\{d\tau, |\psi_{0,1}\rangle\} = \mathrm{Tr}\left\{\left(\left(\mathcal{M}(d\tau)\right)\otimes\mathcal{P}_{0,1}\right)|\psi_{0,1}\rangle\langle\psi_{0,1}|\right\} = \\ = |f(\tau)|^2 d\tau.\end{aligned}$$

Такая интерпретация естественна и согласуется с классическим пределом, когда измеряется классический сигнал с формой во времени $f(\tau)$.

Пусть состояния $|\psi_0\rangle$ (или $|\psi_1\rangle$) приготавливаются в момент τ_i (с точностью $\Delta\tau$ для приготовления такого состояния требуется контролировать область пространства-времени размером $\Delta\tau$):

$$|\psi_{0,1}\rangle = \frac{1}{\sqrt{2}}\int\limits_{-\infty}^{\infty}\left(f(\tau-\tau_i)|\tau\rangle\otimes\left(|+\rangle \pm |-\rangle\right)\right)d\tau, \quad (5)$$

затем совершается унитарное преобразование, которое не зависит от приготовленного состояния:

$$\begin{aligned}|\psi_{0,1}(\tau_d)\rangle = U|\psi_{0,1}\rangle = \\ = \frac{1}{\sqrt{2}}\int\limits_{-\infty}^{\infty}\left(f(\tau-\tau_i-\tau_d)|\tau\rangle\otimes|+\rangle \pm\right. \\ \left.\pm\, f(\tau-\tau_i)|\tau\rangle\otimes|-\rangle\right)d\tau. \quad (6)\end{aligned}$$

Точность момента приготовления определяется шириной носителя состояния $f(\tau)$.

Матричные элементы унитарного оператора имеют вид

$$\begin{aligned}\langle+|\langle\tau'|U|\tau\rangle|+\rangle = \delta_+(\tau-\tau'-\tau_d) = \\ = \int\limits_0^{\infty}\exp\left\{ik(\tau-\tau'-\tau_d)\right\}, \quad (7)\end{aligned}$$

$$\langle-|\langle\tau'|U|\tau\rangle|-\rangle = \delta_+(\tau-\tau'), \quad \langle\pm|\langle\tau'|U|\tau\rangle|\mp\rangle = 0.$$

Данное унитарное преобразование является нелокальным на световом конусе $\tau = x - t$ (при $\tau_d \neq 0$), последнее означает, что для его реализации требуется доступ к области на световом конусе размером τ_d (с точностью $\Delta\tau$). Физически данное унитарное преобразование отвечает сдвигу (задержке) по световому конусу «половинки» состояния с компонентой поляризации $|-\rangle$. Если преобразование осуществляется при фиксированном x (локально в координатном пространстве), то необходимо время $\Delta t = \tau_d$

(так как $\tau = x - t$), либо область координатного пространства $\Delta x = c\tau_d$ ($c = 1$), если преобразование проводится в фиксированный момент времени, но нелокально в пространстве (в области координатного пространства размером $\Delta x = c\tau_d$).

Пространственно-временной интервал τ_d на ветви светового конуса не зависит от выбора системы отсчета, поскольку световой конус является лоренц-инвариантным. В силу этого подслушиватель не может использовать парадокс близнецов [17].

Растянутые состояния $|\psi_0(\tau_d)\rangle$ и $|\psi_1(\tau_d)\rangle$ являются ортогональными. Однако свойство ортогональности является нелокальным в том смысле, что для выяснения ортогональности необходим доступ к области пространства-времени (интервалу) $\geq \tau_d$ с точностью $\Delta\tau \to 0$. Иначе говоря, ортогональность является нелокальным свойством и в гильбертовом пространстве $\mathcal{H}_\tau$ в том смысле, что требуется доступ ко всем состояниям $|\tau\rangle$ (доступ к области пространства-времени $\tau \geq \tau_d$), на которые натянуто $\mathcal{H}_\tau$.

Во всех нерелятивистских квантовых криптографических протоколах подразумевается, что гильбертовы пространства состояний всегда целиком доступны как легитимным пользователям, так и подслушивателю. В релятивистском случае доступ может регулироваться за счет эффектов распространения состояния из области, контролируемой легитимным пользователем, в область, доступную для подслушивателя. «Растягивание» состояния и ограничение на предельную скорость распространения классических объектов и квантовых состояний позволяет построить протокол так, что целиком состояние никогда не доступно для подслушивателя. Точнее говоря, попытка получить доступ к состоянию целиком требует доступа ко всему интервалу, где состояние присутствует. Однако из-за конечности скорости света попытки получить доступ к конечной области пространства-времени приводят к неизбежной задержке в регистрации состояния легитимным пользователем. Фактически по этой причине коллективные измерения, которые эффективны в нерелятивистском случае (из-за доступности всем участникам протокола всего пространства состояний) и учет которых и представляет наибольшую трудность при доказательстве безусловной секретности, несущественны. Это позволяет рассматривать только индивидуальные измерения в каждой посылке, поскольку детектирование подслушивания обнаруживается по задержке регистрации у легитимного пользователя в каждой посылке.

Если имеется доступ к интервалу $2T$, центрированному в τ_0, $T_0 = (-T + \tau_0, \tau_0 + T)$ и $2T < \tau_d + \Delta\tau$, то никакое измерение над состояниями $|\psi_0(\tau_d)\rangle$ и $|\psi_1(\tau_d)\rangle$ не различает эти состояния (состояния кажутся одинаковыми). Формально последнее выражается ограничением матрицы плотности на подпространство $\mathcal{H}_{T_0}$, натянутое на состояния $|\tau\rangle$, носитель которых принадлежит интервалу T_0. Для матрицы плотности имеем

$$\rho_T = \mathrm{Tr}\left\{\left(\left(\int\limits_{T_0}\mathcal{M}(d\tau)\right)\otimes I_{\mathbf{C}^2}\right)|\psi_{0,1}(\tau_d)\rangle\langle\psi_{0,1}(\tau_d)|\right\} = \frac{1}{2}\int\limits_{T_0}|f(\tau)|^2 d\tau\otimes|+\rangle\langle+| + \frac{1}{2}\int\limits_{T_0}|f(\tau-\tau_d)|^2 d\tau\otimes|-\rangle\langle-|. \quad (8)$$

Если интервал $T_0 < \tau_d + \Delta\tau$ одновременно не накрывает носители состояний с разными поляризациями (см. рисунок), тогда только одна из функций $f(\tau)$, либо $f(\tau - \tau_d)$ отлична от нуля. Таким образом, никакие измерения в области пространства-времени (интервале $T_0 < \tau_d + \Delta\tau$) не различают ортогональные состояния. Вероятность различения состояний есть $1/2$ (равна вероятности простого угадывания). Из-за ограничения на предельную скорость доступ к интервалу τ_d не может быть получен быстрее, чем величина самого интервала.

3. ОПИСАНИЕ ПРОТОКОЛА

Легитимные пользователи A и B контролируют окрестности точек x_A и x_B, $x_A < x_B$ (см. рисунок). Часы у пользователей считаются синхронизированными. Величина контролируемых окрестностей должна быть $\Delta x_{A,B} \sim \Delta\tau$. Ширина носителя состояния $\Delta\tau \to 0$ считается известной и является самым малым параметром в задаче. Длина канала ($x_B - x_A = \tau_{ch}$) также считается известной (однако не требуется абсолютно точное знание τ_{ch}).

1. Пользователь A готовит равновероятно одно из состояний, отвечающих 0 или 1, в случайный момент времени τ_i (с точностью $\Delta\tau$)

$$|\psi_{0,1}\rangle = \frac{1}{\sqrt{2}}\int\limits_{-\infty}^{\infty} f(\tau-\tau_i-\tau_A)|\tau\rangle\otimes(|+\rangle \pm |-\rangle)d\tau, \quad \tau_A = x_A. \quad (9)$$

Формально интегрирование по $d\tau$ в (9) проводится по всей ветви светового конуса, однако реально в

формировании состояния участвуют базисные векторы $|\tau\rangle$ из интервала $\Delta\tau$.

2. «Половинка» состояния (с компонентой $|+\rangle$) направляется в канал связи, а вторая «половинка» с компонентой $|-\rangle$ задерживается, что описывается унитарным преобразованием $U_A(\tau_d)$ (такая интерпретация унитарного преобразования естественна, поскольку $U_A(\tau_d)$ имеет матричные элементы со сдвигом по световому конусу только для компоненты поляризации $|+\rangle$):

$$|\psi_{0,1}(\tau_d)\rangle = U_A(\tau_d)|\psi_{0,1}\rangle = \\ = \frac{1}{\sqrt{2}}\int\limits_{-\infty}^{\infty}(f(\tau-\tau_i-\tau_A-\tau_d)|+\rangle \pm \\ \pm f(\tau-\tau_i-\tau_A)|-\rangle)\otimes|\tau\rangle d\tau. \quad (10)$$

Преобразование является нелокальным, реализация его в окрестности точки x_A требует времени τ_d, и не зависит от состояния 0 или 1.

3. Распространение состояния от A к B формально описывается унитарной трансляцией $U(\tau_{ch})$ вдоль ветви светового конуса на интервале τ_{ch} ($\tau_{ch} = x_B - x_A$):

$$|\psi_{0,1}(\tau_{ch})\rangle = U(\tau_{ch})|\psi_{0,1}(\tau_d)\rangle = \\ = \frac{1}{\sqrt{2}}\int\limits_{-\infty}^{\infty}(f(\tau-\tau_i-\tau_A-\tau_d-\tau_{ch})|+\rangle \pm \\ \pm f(\tau-\tau_i-\tau_A-\tau_{ch})|-\rangle)\otimes|\tau\rangle d\tau. \quad (11)$$

4. Пользователь B проводит унитарное преобразование $U_B(-\tau_d)$, не зависящее от входного состояния, которое сводит «половинки» состояний вместе (сдвиг «половинки» с компонентой $|+\rangle$ назад и навстречу $|-\rangle$ может быть реализован при помощи светоделителей, зеркал и линии задержки):

$$U_B(-\tau_d)|\psi_{0,1}(\tau_{ch})\rangle = \\ = \frac{1}{\sqrt{2}}\int\limits_{-\infty}^{\infty} f(\tau-\tau_i-\tau_A-\tau_{ch})(|+\rangle \pm |-\rangle)\otimes|\tau\rangle d\tau. \quad (12)$$

Матричные элементы оператора $U_B(-\tau_d)$ имеют вид аналогичный $U_A(\tau_d)$, но с заменой $\tau_d \to -\tau_d$:

$$\langle+|\langle\tau'|U_B(-\tau_d)|\tau\rangle|+\rangle = \delta_+(\tau-\tau'+\tau_d),$$

$$\langle-|\langle\tau'|U_B(-\tau_d)|\tau\rangle|-\rangle = \delta_+(\tau-\tau'),$$

$$\langle\pm|\langle\tau'|U_B(-\tau_d)|\tau\rangle|\mp\rangle = 0.$$

5. После преобразования $U_B(-\tau_d)$ пользователь осуществляет измерение, реализующее разложение единицы (3), (4). Пространством результатов является множество $\Theta = \{i, \tau : i = 0,1; \tau \in (-\infty,\infty)\}$ (индекс $i = 0,1$ и описывает исходы в каналах 0 или 1),

$$\int\limits_{-\infty}^{\infty}\mathcal{M}(d\tau)\otimes(\mathcal{P}_0+\mathcal{P}_1) = I_\tau\otimes I_{\mathbf{C}^2}. \quad (13)$$

Измерение описывает вероятность получения результата в интервале $\Delta\tau$ и в канале 0 или 1, которая дается выражением

$$\Pr\{(\Delta\tau)\} = \int\limits_{\Delta\tau}|f(\tau-\tau_i-\tau_A-\tau_{ch})|^2 d\tau. \quad (14)$$

Результат отличен от нуля, если интервал $\Delta\tau$ накрывает носитель состояния. Из-за ортогональности состояний исходы в каналах регистрации у B однозначно совпадают с посылками A (без учета шума).

Выбор $\tau_d > \tau_{ch}$ означает, что в канале всегда доступна лишь часть состояния (имеется лишь доступ к части пространства состояний $\mathcal{H}_\tau$), причем доступ к части пространства состояний гарантирует, что информация о состояниях равна нулю (вероятность различения состояний равна $1/2$). Из-за ограничения на предельную скорость распространения доступ ко второй «половине» состояния требует доступа к интервалу $\tau > \tau_d > \tau_{ch}$, что приводит к неизбежной задержке момента регистрации легитимным пользователем B.

6. Пользователь B сообщает через открытый канал момент регистрации τ_B состояния (последний из-за узости носителя $f(\tau)$ известен с точностью $\Delta\tau \to 0$). Если регистрации не было, то данная посылка отбрасывается. После сообщения B момента регистрации A сообщает момент посылки τ_i. Если время регистрации у B $\tau_B = \tau_i + \tau_d + \tau_{ch}$ (с точностью $\Delta\tau$), то попытка принимается. Если обнаружена задержка момента регистрации (более чем на τ_d), то попытка отбрасывается.

Принципиально важно, что отсутствие факта задержки момента регистрации у B уже гарантирует, что подслушиватель имеет нулевую информацию о состоянии, переданном пользователем A (вероятность различения состояний подслушивателем равна $1/2$). Отклонение вероятности от $1/2$ определяется экспоненциальными хвостами состояния, и оно за счет растягивания «половинок» (увеличения τ_d) может быть сделано экспоненциально сколь угодно малым. При отсутствии задержки, в случае компактного носителя состояния $f(\tau)$, информация подслушивателя о передаваемом состоянии строго равна нулю.

7. Об оставшихся посылках подслушиватель имеет нулевую информацию, однако из-за шума в канале (процессов декогерентности) последовательность 0 и 1 еще не идентична у легитимных пользователей. Неидентичность может быть вызвана как подслушивателем, так и естественным шумом. Например, подслушиватель может зарегистрировать первую «половинку» состояния, передаваемого A. Такая регистрация может быть проведена за время $\Delta\tau \to 0$ (тем самым подслушивателем будет определено время τ_i). Затем сразу после регистрации подслушиватель готовит произвольно свое состояние с носителем $f(\tau)$, которое не вызовет задержки в регистрации у B, но вызовет несоответствие с состоянием, посланным A, что будет восприниматься как шум в канале. Вероятность определения момента приготовления состояния подслушивателем, как следует из (8), равна $1/2$ (из-за доступа лишь к «половине» состояния), причем сам по себе факт регистрации подслушивателем дает ему нулевую информацию. Вероятность угадывания состояния равна $1/2$. Полная вероятность правильного определения состояния, проходившего через канал, равна $1/2 \cdot 1/2 = 1/4$. Заметим, что вероятность правильного угадывания подслушивателем состояния в каждой посылке, когда последний вообще ничего не делает, равна $1/2$. На первый взгляд, это выглядит парадоксально, так как подслушиватель имеет доступ к каналу связи, а вероятность в два раза меньше, чем при простом угадывании без доступа к каналу связи. Однако ничего удивительного в этом факте нет, поскольку при простом угадывании достаточно угадать одну из двух возможностей (0 или 1). При детектировании необходимо определить еще и момент приготовления состояния τ_i (чтобы данная посылка не была отброшена легитимными пользователями), а вероятность регистрации «половинки» состояния равна $1/2$. Поэтому в случае доступа к каналу связи вероятность ошибочной интерпретации перехватываемого состояния, равная $3/4$, включает в себя и вероятность ошибочного определения самого факта посылки какого бы то ни было состояния вообще в данном временном интервале, равную $1/2$: поскольку факт регистрации дает нулевую информацию о самом состоянии, требуется угадать его, а вероятность такого угадывания есть $1/2$.

Таким образом, если легитимные пользователи оставляют лишь посылки, при которых не было задержки регистрации (точнее, задержка не превышала $\tau_d + \tau_{ch}$), то этот факт гарантирует, что вероятность определения состояния при вторжении в канал связи не превышает $1/4$. Последняя в два раза меньше вероятности правильного угадывания без вторжения в канал.

Возникает забавная ситуация, которая не имеет места в нерелятивистском случае. Если иметь в виду, что цель подслушивателя состоит в том, чтобы иметь максимальную информацию о ключе при минимальной вероятности быть обнаруженным легитимными пользователями, то в этом смысле правильная стратегия подслушивателя состоит в простом угадывании (при этом не нужен доступ к каналу связи) того, что посылается в каждой попытке. При этом достаточно иметь доступ лишь к классическому каналу связи (чтобы знать общее число принятых посылок), который, впрочем, всегда в задачах квантовой криптографии доступен всем. В этом случае вероятность обнаружения подслушивателя равна нулю, поскольку он не вносит искажений в канал. Вторжение в канал связи подслушивателем имеет смысл, если вероятность получения информации (в пересчете на одну принятую легитимными пользователями посылку) превышает вероятность простого угадывания, равную $1/2$.

Таким образом, максимальная вероятность правильной идентификации подслушивателем каждой принятой законными пользователями попытки равна $1/2$.

8. Остается только выяснить вопрос об идентичности ключа у законных пользователей. Рассмотрим сначала канал без шума. После окончания сеанса и принятия $2N$ посылок A и B производят процедуру $m < 2N$ раундов случайного хэширования (проверки на четность со случайной строкой битов, см. подробности в [19]). После каждого раунда длина исходной последовательности из $2N$ бит уменьшается на 2 бита. Если при m раундах хэширования четности совпадают, то вероятность того, что оставшиеся у A и B последовательности длиной $2N - 2m$ не совпадают, не превышает 2^{-m}, т. е. A и B имеют одинаковый ключ с вероятностью, экспоненциально близкой к единице. Вероятность того, что подслушиватель имеет достоверную информацию о ключе и остается незамеченным, как следует из обсуждения выше, не превышает $2^{-2(N-m)}$.

Пусть теперь в канале имеет место шум, что приводит к ошибке в регистрации у B, например, за счет поворота поляризации, и пусть вероятность такого процесса есть $p < 1$ (вероятность того, что A посылал 0, а B зарегистрировал 1, и наоборот). Законные пользователи оставляют, как и ранее, только те посылки, в которых не было задержки по времени. После проведения серии, когда оставлены $4N$ посылок, A и B раскрывают $2N$ посылок и произво-

дят оценку величины шума в канале (вероятности p). Знание вероятности ошибки при пересылке одиночного бита позволяет в принципе (при достаточно длинной последовательности) выбрать подходящий классический блоковый код [20], который эффективно позволяет уменьшить ошибку для кодированного слова до сколь угодно малой величины.

Например, A сообщает B через открытый канал только номера посылок, в которых он посылал 1, объединяя их в группы по $2k$ посылок и аналогично для 0. В итоге возникают блоки размером $2k$ (кодированные 1 и 0). Далее по мажоритарному голосованию B исправляет ошибки в каждой группе (такое кодирование позволяет исправлять $k-1$ ошибку). Блоки, где возникает k ошибок, отбрасываются (B сообщает номера этих групп по открытому каналу). В оставшихся группах вероятность ошибки не превышает $p^k \ll p$. Теперь пользователи имеют последовательность групп (новые $\tilde{1}$ и $\tilde{0}$) размером $2\tilde{N}$. Далее проводится процедура хэширования, аналогичная описанной выше, из m раундов. В результате появляется последовательность длиной $2(\tilde{N}-m)$. Вероятность того, что оставшаяся последовательность длиной $2(\tilde{N}-m)$ идентична у пользователей A и B при условии того, что при m раундах случайного хэширования четности проверенных последовательностей совпадают, не менее $1-2^{-(\tilde{N}-m)}$. Блоковое кодирование нужно лишь для того, чтобы увеличить вероятность выживания оставшейся последовательности при хэшировании. Процедура хэширования возможна сразу для исходной (не блоковой) последовательности, однако при этом из-за шума вероятность не обнаружить сбоя четности при хэшировании будет мала. Однако если последовательность проходит тест, то она секретна и идентична с описанными выше вероятностями. Вероятность того, что подслушиватель имеет достоверную информацию о ключе и остается незамеченным, с запасом не превышает $2^{-2(\tilde{N}-m)}$ (поскольку достаточно угадать по одному биту из каждой кодовой группы). Такая простая схема кодирования, очевидно, не является оптимальной, но она позволяет наиболее просто и наглядно сформулировать криптографический протокол.

Авторы выражают благодарность В. Л. Голо за проявленный интерес и обсуждение результатов работы.

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (проект 99-02-18127), а также проекта «Физические основы квантового компьютера» и программы «Перспективные технологии и устройства микро- и наноэлектроники» (проект 02.04.5.2.40.Т.50).

ЛИТЕРАТУРА

1. S. Wiesner, *Conjugate coding*, Sigact News **15**, 78 (1983).

2. C. H. Bennett and G. Brassard, *Quantum cryptography: Public key distribution and coin tossing*, *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, December (1984), p. 175.

3. P. W. Shor, *Proceedings 35th Annual Symposium on Foundations of Computer Science*, Santa Fe, NM, USA, ed. by S. Goldwasser, IEEE Comput. Soc. Press, Los Alamitos (1994), p. 124.

4. W. K. Wootters and W. H. Zurek, Nature **299**, 802 (1982).

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. D. Mayers, E-print archives quant-ph/9802025 (1998).

7. H.-K. Lo and H. F. Chau, E-print archives quant-ph/9803006 (1998).

8. E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury, E-print archives quant-ph/9912053 (1999).

9. P. W. Shor and J. Preskill, E-print archives quant-ph/0003004 (2000).

10. Н. Н. Боголюбов, А. А. Логунов, А. И. Оксак, И. Т. Тодоров, *Общие принципы квантовой теории поля*, Наука, Москва (1987).

11. A. Kent, E-print archives quant-ph/9810067, quant-ph/9810068 (1998), Phys. Rev. Lett. **83**, 1447 (1999).

12. S. N. Molotkov and S. S. Nazin, E-print archives quant-ph/9911055 (1999), quant-ph/9910034 (1999). R. Laiho, S. N. Molotkov, and S. S. Nazin, E-print archives quant-ph/0005067, quant-ph/0005068 (2000).

13. Л. Д. Ландау, Р. Пайерлс, Z. Phys. **69**, 56 (1931); Л. Д. Ландау, *Собрание трудов*, т. 1, Наука, Москва (1969), с. 56.

14. L. Goldenberg and L. Vaidman, Phys. Rev. Lett. **75**, 1239 (1995); E-print archives quant-ph/9506030 (1995).

15. A. Peres, E-print archives quant-ph/9509003 (1995).

16. M. Koashi and N. Imoto, Phys. Rev. Lett. **79**, 2383 (1997).

17. R. Laiho, S. N. Molotkov, and S. S. Nazin, E-print archives quant-ph/00006010 (2000).

18. I. Bialynicki-Birula, Phys. Rev. Lett. **80**, 5247 (1998).

19. C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, E-print archives quant-ph/9604024 (1996).

20. E. J. Mac Williams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Publ. Company, Amsterdam, New York, Oxford (1977).