Письма в ЖЭТФ, том 76, вып. 1, с. 79 – 85 © 2002 г. 10 июля

Релятивистская квантовая криптография на "остановленных" фотонах

С. Н. Молотков[1)]

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

Поступила в редакцию 28 мая 2002 г.

Предлагается новая релятивистская квантовая криптографическая система, в которой носителями информации являются протяженные однофотонные состояния с ортогональными поляризациями и эффективной длиной, превышающей длину канала связи. В качестве процедуры детектирования и приготовления протяженных состояний используется эффект "остановки" света. Секретность криптосистемы относительно любых попыток подслушивания обеспечивается как квантовостью состояний, так и наличием предельной скорости распространения. В данной схеме процедуры приготовления и детектирования являются локальными в пространстве, но требуют конечного времени в зависимости от протяженности состояний. Причем процедура подготовки к детектированию на приемном конце начинается еще до того, как состояние покинуло источник на передающем конце.

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

Безусловная секретность распространения ключа в квантовых криптосистемах основана не на технических ограничениях подслушивателя, а на фундаментальных запретах, диктуемых квантовой механикой и квантовой теорией поля, которые позволяют детектировать любые попытки подслушивания. Детектирование попыток подслушивания в квантовых криптосистемах обеспечивается теоремой запрета на копирование квантовых состояний, а также невозможностью получения информации о неортогональных состояниях без их возмущения [1, 2] (no cloning теорема). Обычно в квантовых криптосистемах используются лишь свойства векторов состояний как элементов абстрактного гильбертова пространства $\mathcal{H}$ и не используется конкретная реализация $\mathcal{H}$ (его привязка к координатному пространству в нерелятивистском или пространству-времени Минковского, соответственно, в релятивистском случае). Любая передача информации представляет собой физический процесс в пространстве-времени Минковского, который осуществляется при помощи конкретных физических объектов, классических или квантовых. Квантовые состояния (векторы в $\mathcal{H}$) должны быть ассоциированы с конкретными частицами (фотонами, электронами и т.д.). В квантовой теории поля различные типы частиц описываются базисными векторами различных унитарных представлений группы Пуанкаре, которые неизбежно имеют носители (амплитуды – сглаживающие функции) в пространстве-времени Минковского. Такое сопоставление унитарных представлений группы Пуанкаре является основополагающим принципом при интерпретации квантовой теории поля [3].

В релятивистских квантовых криптосистемах, в которых явно учитывается пространственно-временная структура квантовых состояний, а также факт их распространения в пространстве-времени и существование предельной скорости, требование неортогональности, необходимое в криптосистемах, где используются лишь свойства векторов состояний как элементов $\mathcal{H}$, не является обязательным [4, 5].

Достоверная различимость и возможность копирования ортогональных состояний имеет место только в случае, когда состояния доступны целиком (целиком доступна пространственно-временная область, где отлична от нуля амплитуда состояния). Если ортогональные состояния недоступны как целостные объекты, то они достоверно неразличимы и не могут быть скопированы.

Данная ситуация не вступает в конфликт с no cloning теоремой, а скорее проясняет пределы применимости последней. При доказательстве теоремы ничего, кроме свойств векторов состояний как элементов гильбертова пространства, не используется [2]. Теорема *не запрещает* получать информацию о состояниях без возмущения последних. В этом смысле ортогональные состояния аналогичны классическим, поэтому считается, что они мало интересны для задач квантовой теории информации. Однако, если не игнорировать факта существования

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

пространства-времени Минковского[2)], то набор различных ситуаций с использованием ортогональных состояний оказывается более богатым. Криптосистема, которая рассматривается ниже, представляет собой такой пример.

Релятивистские криптографические протоколы на ортогональных состояниях устроены таким образом, что состояния по мере их распространения через канал связи никогда единовременно не присутствуют целиком в канале связи (в области, доступной для подслушивания). Данное обстоятельство вместе с конечностью скорости света позволяет детектировать любые попытки подслушивания. Причем необходимо отличать два случая. В первом случае состояния при ограничении на область пространства-времени в канале становятся эффективно неортогональными, во втором случае остаются ортогональными (локально ортогональными) в области, доступной для подслушивания. Неразличимость локально ортогональных состояний при неполном доступе к ним вытекает, по сути, из условия нормировки состояний. Даже если состояния локально ортогональны в доступной области пространства-времени, то вероятность просто факта их регистрации всегда меньше единицы и не может быть больше интеграла нормировки, который набирается в этой области. Попытки расширить доступную область (за счет пространства или времени), приводит к неизбежной задержке на приемном конце, которая и детектируется.

Поскольку пространственно-временная структура состояний существенна для релятивистских криптографических протоколов, то процедуры приготовления, распространения через канал связи и измерения должны описываться явно. Измерение *как целостных объектов* протяженных однофотонных состояний с длиной в несколько десятков километров является далеко не тривиальной задачей[3)]. С формальной точки зрения измерение отличающее с достоверностью пару ортогональных протяженных состояний $|\varphi_{0,1}\rangle$, описывается ортогональными проекторами $E_{0,1} = |\varphi_{0,1}\rangle\langle\varphi_{0,1}|$, реализующими разложение единицы в подпространстве $\mathcal{H}$, натянутом на данные векторы. Разложение единицы является формальным описанием физического устройства, которое из-за нелокальности проекторов должно быть протяженным в координатном пространстве. Нелокальность измерения, описываемого проекторами на данные состояния, возникает из-за того, что прибор должен реализовывать проекцию на состояния в некоторой пространственной области в некоторый фиксированный момент времени. Реализовать подобный нелокальный в пространстве детектор технически вряд ли возможно.

Дальнейшая идея реализации измерения при помощи локализованного в пространстве прибора, различающего с достоверностью пару ортогональных состояний с протяженностью в десятки километров, состоит в использовании локализованной вспомогательной системы. Такое измерение будет нелокальным во времени в следующем смысле. За счет взаимодействия (совместной унитарной эволюции) протяженного однофотонного состояния и вспомогательной системы в течение времени $\Delta t \approx L/c$ (L – эффективная протяженность однофотонного состояния, c – скорость света) однофотонное состояние переходит в вакуумное, а вспомогательная система – в некоторое новое состояние в зависимости от входного фотонного состояния. По истечении времени Δt измеряется новое состояние вспомогательной системы. Аналогично для процедуры приготовления. Можно приготовить распределенным в пространстве прибором состояние в некоторый момент времени, или приготавливать состояние локализованным в пространстве источником в течение времени Δt. Поскольку амплитуда (сглаживающая функция, см. ниже) фотонного поля, распространяющегося в одном направлении, зависит только от разности $\tau = x - ct$, то условие, когда требуется "много пространства – L" можно заменить условием, когда требуется "много времени – L/c".

Изложим кратко схему криптографии, использующую "много пространства". Ортогональные состояния $|\varphi_{0,1}\rangle$ приготавливаются в заранее оговоренный момент времени t_A в области пространства, контролируемой участником A. Протяженные однофотонные состояния с ортогональными поляризациями могут быть представлены в виде

$$\varphi^{+}_{\mu}(\hat{x}) = \frac{1}{\sqrt{2\pi}} \int d\hat{k}\delta(\hat{k}^2)\theta(k_0)e^{i\hat{k}(\hat{x}-\hat{x}_A)}a^{+}_{\mu}(k), \qquad (1)$$

$$\hat{k} = (k, k_0), \quad \hat{x} = (x, t), \quad d\hat{k} = dkdk_0,$$

$$\hat{k}\hat{x} = kx - k_0 t, \quad [a^{-}_{\nu}(k), a^{+}_{\mu}(k)] = k_0\delta(k-k')\delta_{\nu,\mu}.$$

Здесь $\hat{x}_A = (x_A, t_A)$ описывают выбор начала отсчета времени и оси координат. Индексы $\mu, \nu = 0, 1$ ну-

[2)] В противном случае, где же наблюдатели, будучи классическими объектами, получают информацию о результатах измерений над квантовыми состояниями.

[3)] Современные лазеры на твердотельной матрице с примесями редкоземельных элементов и распределенной обратной связью, совместимые с оптоволоконными системами, позволяют получать на выходе состояния с шириной полосы частотного спектра $\Delta\omega \sim 1$ кГц. Пересчет на эффективную протяженность состояния дает $L \sim c/\Delta\Omega \sim 300$ км.

меруют два базисных состояния поляризации. Физические состояния квантованного поля $|\varphi_\mu\rangle \in \mathcal{H}$ получаются как результат сглаживания операторных обобщенных функций с основными функциями $\varphi(\hat{x}) \in \Omega(\hat{x})$ ($\Omega(\hat{x})$ – пространство основных функций [3]); $\varphi^+_\mu(\hat{x})|0\rangle \in \Omega(\hat{x})^*$ – обобщенные собственные векторы (линейные непрерывные функционалы в $\mathcal{H}$), и $\Omega(\hat{x}) \subset \mathcal{H} \subset \Omega^*(\hat{x})$ – оснащенное гильбертово пространство (тройка Гельфанда) [6]:

$$|\varphi_\mu\rangle = \int d\hat{x}\varphi(\hat{x}-\hat{x}_A)\varphi^+_\mu(\hat{x})|0\rangle =$$

$$= \int d\hat{k}\tilde{\varphi}(\hat{k})\delta(\hat{k}^2)\theta(k_0)e^{-i(kx_A-k_0t_A)}a^+_\mu(k)|0\rangle =$$

$$= \int\limits_{-\infty}^{\infty} \frac{dk}{k_0}e^{-i(kx_A-k_0t_A)}\tilde{\varphi}(k,k_0=|k|)|k,\mu\rangle =$$

$$= \int\limits_{-\infty}^{\infty} dx\varphi(x-x_A-(t-t_A))|x-t\rangle, \qquad (2)$$

$$\varphi(\tau) = \int\limits_0^{\infty} dk e^{-k\tau}\varphi(k), \quad \tau = x-t,$$

$$|k,\mu\rangle = a^+_\mu(k)|0\rangle, \quad \langle k',\nu|k,\mu\rangle = k_0\delta_{\mu,\nu}\delta(k-k'),$$

Условие нормировки

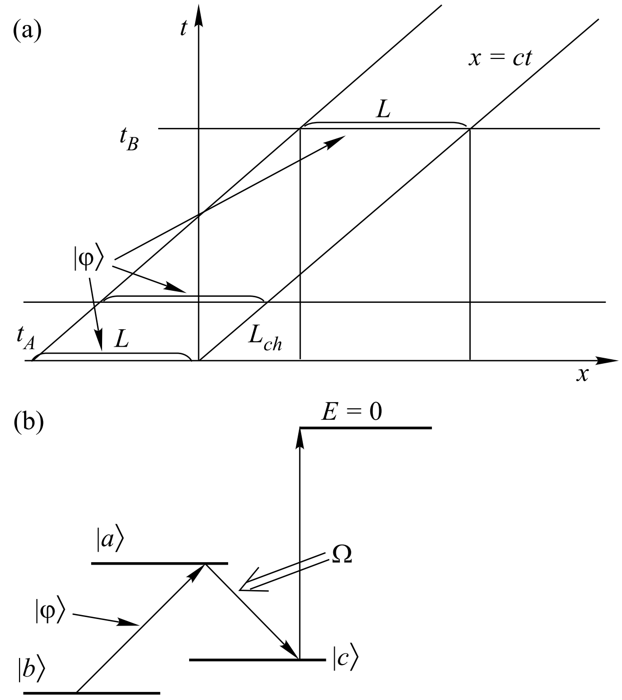
$$\langle\varphi_\mu|\varphi_\mu\rangle = \int\limits_{-\infty}^{\infty} \frac{dk}{k_0}|\tilde{\varphi}(k,k_0=|k|)|^2 = \int\limits_{-\infty}^{\infty} dk|\varphi(k)|^2 = 1,$$

$$\varphi(k) = \frac{\tilde{\varphi}(k,k_0=|k|)}{\sqrt{k_0}}. \qquad (3)$$

Состояния $|\varphi_\mu\rangle$ определяются значениями амплитуды $\tilde{\varphi}(\hat{k})$ на массовой поверхности $k_0 = |k|$. При передаче информации между двумя участниками естественно рассматривать состояния, распространяющиеся в одном направлении ($k > 0$). В этом случае все величины зависят от разности $\tau = x - t$ – переменная на одной из ветвей светового конуса.

Состояние (1), (3) может быть интерпретировано как состояние с амплитудой $\varphi(x - x_A - (t - t_A))$ приготовленное в области, контролируемой участником A в момент времени t_A. Нет запретов на приготовление состояния в момент времени t_A в некоторой области. При этом требуется пространственная область размером $\sim$ size$\varphi(x - x_A) \neq 0$, где отлична от нуля амплитуда состояния рисунка (a).

Строго говоря, амплитуда отлична от нуля вне любой компактной области пространства-времени,



поскольку сглаживающая функция $\varphi(\tau) \in \Omega(\tau)$ ($\Omega(\tau)$ – пространство основных, быстро убывающих функций (см. детали в [3]). Любая функция из $\Omega(\tau)$ может быть приближена с любой степенью точности функциями с компактными носителями из $\tilde{\varphi} \in \mathcal{D}(\tau)$ так, что $\||\varphi\rangle - |\tilde{\varphi}\rangle\| < \delta$, для любого δ (норма порождается скалярным произведением в $\mathcal{H}$) [3,6] [4]).

Распространение через канал связи длиной L_{ch} описывается оператором унитарной трансляции в пространстве-времени

$$U_{ch} = \bigoplus_{\mu=0,1} \int\limits_0^{\infty} \frac{dk}{k}e^{-ik(L_{ch}-t_{ch})}|k,\mu\rangle\langle k,\mu|, \qquad (4)$$

$$|\varphi_\mu\rangle_{ch} = U_{ch}|\varphi_\mu\rangle =$$

$$= \int\limits_0^{\infty} dk e^{-ik(x-L_{ch}-x_A-(t-t_{ch}-t_A)}\varphi(k)|k,\mu\rangle. \qquad (5)$$

Участник B в момент времени $t_B = t_A + \mathrm{size}\{\varphi(x - - t_A)\} + x_A + L_{ch}$, когда состояние достигает контролируемой им области, проводит измерение, которое описывается ортогональным разложением единицы, реализуемым проекторами на "транслированные" в пространстве-времени состояния

$$I = \bigoplus_{\mu=0,1} |\varphi_\mu\rangle_{ch\,ch}\langle\varphi_\mu| = U_{ch}(\bigoplus_{\mu=0,1} |\varphi_\mu\rangle\langle\varphi_\mu|)U^{-1}_{ch}. \quad (6)$$

[4]) Оценки на убывание амплитуды на бесконечности можно получить напрямую [5], исходя из теоремы Винера-Пэли [7].

Такое разложение является формальным описанием распределенного в пространстве прибора, взаимодействующего с состоянием в один и тот же момент времени сразу во всей области локализации состояния в момент времени t_B.

Для обеспечения секретности и детектирования любых попыток подслушивания требуется, чтобы протяженность состояния превышала длину канала связи. Более формально это требование сводится к тому, чтобы измерения в пространственной области размером L_{ch} давали вероятность регистрации состояния, меньшую единицы, независимо от момента времени. Данная вероятность дается величиной

$$\Pr(t, L_{ch}) = \mathrm{Tr}\{\mathcal{M}(t, L_{ch}, \mu)|\varphi_\mu\rangle\langle\varphi_\mu|\} < 1, \qquad (7)$$

где проекторно-значная мера

$$\mathcal{M}(t, L_{ch}, \mu) = \\ = \int\limits_{L_{ch}} dx \left(\int\limits_0^\infty dk e^{ik(x-t)}|k,\mu\rangle\right) \times \\ \times \left(\int\limits_0^\infty dk' \langle k',\mu| e^{-ik'(x-t)}\right), \qquad (8)$$

$$I = \bigoplus_{\mu=0,1} \mathcal{M}(t,\infty,\mu) = \bigoplus_{\mu=0,1} \int\limits_0^\infty \frac{dk}{k}|k,\mu\rangle\langle k,\mu|;$$

время здесь является параметром. Мы не останавливаемся на деталях формального доказательства секретности, которое подробно приведено в [5]. Хотя для формального доказательства безразлично, какая реализация измерения используется, однако техническая реализация процедуры детектирования, когда измерение проводится в фиксированный момент времени и требуется "много пространства", представляется практически не реализуемой.

Перейдем к случаю, когда приготовление и детектирование состояний осуществляются при помощи локализованного прибора, но в течение некоторого времени. Такое измерение реализуется при помощи "остановки" фотонов [8]. Идея состоит в том, чтобы использовать вспомогательную локализованную (с размером $\ll L_{ch}, L$) в пространстве квантовую систему (ячейку с газом атомов или твердотельную матрицу с примесями редкоземельных элементов [9, 10]). Когда амплитуда однофотонного состояния достигает вспомогательной системы, находящейся в исходном состоянии $|\mathbf{b}\rangle$, включается внешнее управляющее классическое поле на время $\Delta t \approx L/c$, приводящее к суперпозиции фотонного поля и атомной системы. Когда фотонное состояние целиком успевает войти в ячейку, то внешнее поле выключается, атомная система оказывается в новом состоянии $|\mathbf{c}_\mu\rangle$, а фотонная компонента квантового состояния оказывается в вакуумном состоянии $|0\rangle$. Здесь $|\mathbf{b}\rangle$ и $|\mathbf{c}_\mu\rangle$ для краткости описывают коллективные переменные атомной подсистемы (см. детали в [8]). Данный процесс описывается совместной унитарной эволюцией:

$$|\varphi_\mu\rangle \otimes |\mathbf{b}_\mu\rangle \to \bigoplus_{\mu=0,1} U_\mu(\Delta t)(|\varphi_\mu\rangle \otimes |\mathbf{b}_\mu\rangle) \to |0\rangle \otimes |\mathbf{c}_\mu\rangle. \qquad (9)$$

Затем над локализованной в пространстве атомной системой производится измерение, описывающееся проекционным измерением $\mathcal{P}_\mu = |\mathbf{c}_\mu\rangle\langle\mathbf{c}_\mu|$.

Приготовление протяженного однофотонного состояния может быть реализовано обращением совместной унитарной эволюции (9)

$$|0\rangle \otimes |\mathbf{c}_\mu\rangle \to U_\mu(\Delta t)(|0\rangle \otimes |\mathbf{c}_\mu\rangle) \to |\varphi_\mu\rangle \otimes |\mathbf{b}_\mu\rangle. \qquad (10)$$

Поэтому рассмотрим только процедуру детектирования. Унитарное преобразование реализуется при помощи взаимодействия однофотонного состояния с атомами газа, находящегося в магнитном поле. Магнитное поле приводит к расщеплению почти вырожденного уровня $\{|\mathbf{b}\rangle,\ |\mathbf{c}\rangle\}$, расстояние между уровнями и чередование этих уровней по энергии регулируются посредством изменения величины и направления магнитного поля. Переходы между уровнями $|\mathbf{b}\rangle \longleftrightarrow |\mathbf{a}\rangle$ и $|\mathbf{c}\rangle \longleftrightarrow |\mathbf{a}\rangle$ имеют место при ортогональных состояниях круговой поляризации (спиральности) σ_+ и σ_-. Исходно однократно заполненным состоянием является низший по энергии уровень $|\mathbf{b}\rangle$ (или $|\mathbf{c}\rangle$ в зависимости от направления магнитного поля). Протяженное однофотонное состояние (с узким частотным спектром) за счет взаимодействия с атомами газа вызывает переходы $|\mathbf{b}\rangle \to |\mathbf{a}\rangle$, а классическое управляющее излучение, которое может включаться на требуемое время, вызывает переходы $|\mathbf{a}\rangle \to |\mathbf{c}\rangle$, тем самым приводя к перебросу с верхнего возбужденного уровня на нижний. Поскольку переходы между $|\mathbf{c}\rangle$ и $|\mathbf{b}\rangle$ запрещены, то электрон может находится на уровне $|\mathbf{c}\rangle$ сколь угодно долго. Запутанное состояние атомных уровней в данной конфигурации и однофотонного состояния называют dark-polariton. Степень запутанности атомных уровней и квантованного фотонного поля зависит от величины управляющего классического излучения. Запутанное состояние *в ячейке с атомами*, например, для значения спиральности $\mu = 0$ (значения индекса

$\mu = 0, 1$ отвечают состояниям циркулярной поляризации $\sigma_{\pm}$), может быть представлено в виде

$$|\Psi\rangle = \cos\theta(t)|\mathbf{b}_0\rangle \otimes |\varphi_0(\theta(t))\rangle - \sin\theta(t)|\mathbf{c}_0\rangle \otimes |0\rangle,$$
$$\mathrm{tg}\theta(t) = \frac{g\sqrt{N}}{\Omega(t)}, \tag{11}$$

где N – число атомов в ячейке, g – константа взаимодействия квантованного фотонного поля с атомной системой, $\Omega(t)$ – так называемая частота классического управляющего поля. Компонента вектора состояния, отвечающая однофотонному квантованному полю в среде с атомами, имеет вид (считаем, что среда находится при $x > 0$)

$$|\varphi_0(\theta(t))\rangle = \int\limits_0^{\infty} dx\varphi\left(x - \int\limits_0^{t} dt'\cos^2\theta(t'), 0\right)|\tau(\theta(t))\rangle,$$

$$\tau(\theta(t)) = x - \int\limits_0^{t} dt'\cos^2\theta(t'). \tag{12}$$

Изменение поля так, чтобы $\theta = 0 \to \theta = \pi/2$, приводит к преобразованию амплитуды однофотонного состояния в атомные степени свободы (“остановка” света). При $\theta \to 0$ скорость распространения и амплитуда фотонного состояния стремятся к нулю, $v = \cos^2(\theta)$ (соответственно, квадрат модуля амплитуды однофотонного состояния $\propto \cos^2\theta \to 0$ и доля вакуумной компоненты фотонного поля $\propto \sin^2\theta \to 1$). Заметим, что при этом интенсивность классического управляющего поля $\Omega \propto \cos\theta \to 0$ эффективно отвечает выключению поля. На первый взгляд, это противоречит интуиции. Пока поле включено (интенсивность его велика) и по мере того, как квантованное фотонное поле входит в ячейку с атомами (на это требуется характерное время $\Delta t \approx L/c$, L – эффективная протяженность состояния), оно вызывает переходы $|\mathbf{b}\rangle \to |\mathbf{a}\rangle$, классическое поле при этом приводит к быстрым переходам $|\mathbf{a}\rangle \to |\mathbf{c}\rangle$ ($\Omega \gg g\sqrt{N}$). Когда однофотонное состояние целиком вошло в ячейку, классическое поле должно быть выключено, в противном случае оно вызовет обратные переходы электронов из $|\mathbf{c}\rangle$ в $|\mathbf{a}\rangle$. “Остановка” света не является в обычном смысле слова остановкой, как это имеет место для массивных частиц. Из-за безмассовости фотонного поля при стремлении скорости к нулю амплитуда однофотонного состояния также стремится к нулю.

Совместная унитарная эволюция (перекачка фотонного состояния в атомные степени свободы) еще не является измерением. Задача теперь сводится к измерению состояния атомной подсистемы (реализации проекционного измерения $\mathcal{P}_c = |\mathbf{c}\rangle\langle\mathbf{c}|$). По истечении времени Δt совместной унитарной эволюции включается дополнительное классическое излучение – поле с частотой, которая соответствует переходу со связанного состояния $|\mathbf{c}\rangle$ в непрерывный спектр. В дальнейшем регистрируется ток, переносимый непосредственно возбужденными электронами либо предварительно усиленный до приемлемого для регистрации уровня. Данная схема на “остановленных” фотонах представляет собой специализированный детектор, позволяющий различать протяженные однофотонные состояния (грубо говоря, реализовывать проекционные измерения для фотонов). Практически для всех типов фотодетекторов последней стадией является выбивание электрона из связанного состояния и регистрация тока (см. рисунок (b)).

Таким образом, криптографический протокол состоит из процедур приготовления состояния, распространения его через канал связи и детектирования.

i) Приготовление одного из ортогональных состояний $\rho_A(\mathbf{c}_\nu) = |\mathbf{c}_\nu(A)\rangle\langle\mathbf{c}_\nu(A)|$ с поляризациями $\nu = 0$ или $\nu = 1$ участником A начинается в момент времени t_A и длится $\Delta t \approx L/c$, одновременно участник B приготавливает свою вспомогательную систему из двух атомных систем во взаимно ортогональных состояниях $\mu = 0$ и $\mu = 1$, $\rho_B(\mathbf{b}_\nu) = |\mathbf{b}_\nu(B)\rangle\langle\mathbf{b}_\nu(B)|$. Фотонное поле при этом находится в вакуумном состоянии.

$$U_\nu^{-1}(t_A, t_A+\Delta t)\left(\rho_A(\mathbf{c}_\nu)\otimes|0\rangle\langle 0|\otimes\bigoplus_{\mu=0,1}\rho_B(\mathbf{b}_\mu)\right)\times$$
$$\times\, U_\nu(t_A, t_A + \Delta t). \tag{13}$$

ii) Распространение через канал связи и достижение состоянием целиком приемного конца в течение времени $\approx (L + L_{ch})/c$,

$$U_{ch}U_\nu^{-1}(t_A, t_A + \Delta t)\times$$
$$\times\left(\rho_A(\mathbf{c}_\nu)\otimes|0\rangle\langle 0|\otimes\bigoplus_{\mu=0,1}\rho_B(\mathbf{b}_\mu)\right)\times$$
$$\times\, U_\nu(t_A, t_A + \Delta t)U_{ch}^{-1}. \tag{14}$$

iii) “Остановка” однофотонного состояния, которая начинается в момент $t_B = t_A + L_{ch}/c$ и длится в течение времени $\Delta t \approx L/c$,

$$\bigoplus_{\mu=0,1} U_\mu(t_B, t_B+\Delta t) U_{ch} U^{-1}(t_A, t_A+\Delta t) \times (\rho_A(\mathbf{c}_\nu)\otimes|0\rangle\langle 0|\otimes\rho_B(\mathbf{b}_\mu)) \times \times U_\mu(t_B, t_B+\Delta t)^{-1} U_{ch}^{-1} U_\nu(t_A, t_A+\Delta t) = = \delta_{|\nu-\mu|,0}\rho_A(\mathbf{b}_\nu)\otimes|0\rangle\langle 0|\otimes \otimes\rho_B(\mathbf{c}_\mu)\bigoplus\delta_{|\nu-\mu|,1}\rho_A(\mathbf{c}_\nu)\otimes|0\rangle\langle 0|\otimes\rho_B(\mathbf{b}_\mu). \quad (15)$$

iv) Локальное в пространстве измерение атомных степеней свободы $|\mathbf{c}_\mu(B)\rangle$ участником В при помощи проекционного измерения

$$I_{\mathbf{c}}(B) = \bigoplus_{\mu=0,1} |\mathbf{c}_\mu(B)\rangle\langle\mathbf{c}_\mu(B)|. \quad (16)$$

Использование символа суммы подпространств, а не символа тензорного произведения в (13)–(16) означает, что нас интересуют исходы лишь в одной из ячеек ($\mu=0$ или $\mu=1$), а не в двух сразу ($\mu=0$ и $\mu=1$).

Технически данную ситуацию можно реализовать, приготовив две ячейки с атомами, расположенные, например, последовательно друг за другом и в которых магнитное поле отличается величиной и направлением. При этом квантованное однофотонное поле совместно с классическим управляющим полем вызывают рамановские переходы в той подсистеме В (с тем значением μ), где эти переходы возможны. После этого включение другого классического поля вызывает переходы электронов из состояния $|\mathbf{c}_\mu\rangle$ в непрерывный спектр с последующей регистрацией обычным фотоумножителем. Каждая ячейка подсвечивается классическим излучением со своей частотой, необходимой, чтобы вызвать переходы в непрерывный спектр. При этом сигнал тока будет возникать только в ячейке, где имели место рамановские переходы (состояние $|\mathbf{c}_\mu\rangle$ было заполнено электронами). В принципе не требуется полной остановки света, а достаточно только замедления распространения в ячейке. При этом желательно, чтобы длительность возбуждающего сигнала, переводящего электроны в непрерывный спектр, была короче времени распространения замедленного однофотонного поля в ячейке. Величина отношения сигналов в этом случае по отношению к ситуации, когда была бы полная остановка, будет равна $\sin^2\theta$, то есть доле заполнения состояния $|\mathbf{c}_\mu\rangle$ (см. формулу (11)).

Отметим, что приготовление, распространение и детектирование ("остановка" однофотонного состояния) представляют собой единый процесс. Как видно из (13)–(15), "остановка" переднего фронта состояния начинается еще до того, как задний фронт покинул источник. Строго говоря, соотношения (11), (12) получены в адиабатическом приближении (см. детали в [8]), однако это не является ограничивающим обстоятельством, поскольку само плавное включение и выключение классического управляющего поля может происходит на "хвостах" переднего и заднего фронтов однофотонного состояния.

Отметим также, что приготовление протяженного состояния может быть получено при помощи вырезания фильтром узкой спектральной полосы из короткого (широкополосного) состояния. В рассмотренных выше примерах протяженность L определяется спектральной шириной атомных уровней $|\mathbf{a}\rangle$ (например, в экспериментах [9] L составляла несколько километров). При этом пространственно-временная протяженность амплитуды состояния определяется шириной спектра $\Delta\omega$, и с большой точностью вероятность регистрации в течение времени Δt (время действия классического управляющего поля в (9)) дается соотношением $\approx 1-\mathcal{O}(e^{-\Delta\omega\Delta t})$ (о точных соотношениях см. [11]).

Известное простое и изящное доказательство no cloning теоремы [2] *не запрещает* существование унитарного оператора, действующего в $\mathcal{H}_A\otimes\mathcal{H}_B$, который в результате совместной эволюции позволяет перевести вспомогательную систему (ancilla) в разные состояния в зависимости от одного из входных ортогональных состояний без возмущения последнего. Тот факт, что унитарный оператор действует в $\mathcal{H}_A\otimes\mathcal{H}_B$, неявно предполагает доступ к квантовым состояниям как целостным объектам. При этом теорема ничего не говорит о самой структуре этого унитарного оператора. Учет пространственно-временной структуры квантовых состояний, которая неизбежно существует, приводит к большему разнообразию различных ситуаций для ортогональных состояний. Приведенный выше достаточно простой пример использования ортогональных состояний для квантовой криптографии не исчерпывает всех возможных приложений для них.

Выражаю благодарность С. С. Назину за полезные обсуждения и критические замечания.

Работа поддержана Российским фондом фундаментальных исследований (проект # 02-02-16289), а также проектами # 40.020.1.1.1170 и 37.029.1.1.0031.

---

1. W.K. Wootters and W.H. Zurek, Nature **299**, 802 (1982).
2. C.H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992); C.H. Bennett, G. Brassard, and N.D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).

3. Н. Н. Боголюбов, А. А. Логунов, А. И. Оксак, И. Т. Тодоров, *Общие принципы квантовой теории поля*, М.: Наука, 1987.
4. L. Goldenberg and L. Vaidman, Phys. Rev. Lett. **75**, 1239 (1995); quant-ph/9506030.
5. S. N. Molotkov and S. S. Nazin, JETP Lett. **73**, 682 (2001), quant-ph/106046.
6. И. М. Гельфанд, Н. Я. Виленкин, *Некоторые применения гармонического анализа. Оснащенные гильбертовы пространства (Обобщенные функции, вып.4)*, М.: Физматгиз, 1961.
7. N. Wiener and R. Palley, *Fourier Transform in the Complex Domain*, American Mathematical Society, New York, 1934.
8. M. Fleischhauer and M. D. Lukin, Phys. Rev. Lett. **84**, 5094 (2000).
9. C. Liu, Z. Dutton, C. H. Behroozi, and L. V. Hau, Nature **409**, 490 (2001); D. F. Phillips, A. Fleischhauer, A. Mair et al., Phys. Rev. Lett. **86**, 783 (2001).
10. A. V. Turukhin, V. S. Sudarshanam, M. S.Shahriar et al., Phys. Rev. Lett. **88**, 023602-1 (2002).
11. С. Н. Молотков, Письма в ЖЭТФ **75**, N11 (2002).