ЖЭТФ, 2001, том 120, вып. 4 (10), стр. 1004–1026

РЕЛЯТИВИСТСКИЕ КВАНТОВЫЕ ПРОТОКОЛЫ: BIT COMMITMENT И COIN TOSSING

С. Н. Молотков [*], ***С. С. Назин***

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

Поступила в редакцию 21 ноября 2000 г.

Предлагаются релятивистские квантовые протоколы, реализующие схемы привязки к биту (bit commitment) и подбрасывания монеты на расстоянии (выбор жребия, coin tossing). Идея протоколов основана на том, что протяженные в пространстве нестационарные ортогональные квантовые состояния достоверно неразличимы, если они целиком недоступны для измерений. По мере распространения из области, контролируемой одним из участников протокола, в область, доступную для измерений вторым участником, они становятся достоверно различимыми при доступе к ним целиком. Для протокола существенны как квантовость состояний, так и факт наличия предельной скорости распространения, диктуемый специальной теорией относительности.

PACS: 89.70.+c, 03.65.-w

1. ВВЕДЕНИЕ

В нерелятивистской квантовой механике любое измерение над квантовой системой наблюдателем, вообще говоря, приводит к возмущению исходного состояния системы. Из-за отсутствия ограничений на предельную скорость нет формальных запретов на проведение измерений, в том числе и нелокальных в пространстве, мгновенно.

Специальная теория относительности накладывает дополнительные ограничения на измерения уже в классическом случае. Из-за существования предельной скорости уже нельзя проводить нелокальные измерения над классическим объектом за сколь угодно малое время.

В релятивистской квантовой теории поля должны возникать дополнительные ограничения на измеримость наблюдаемых по сравнению с нерелятивистской квантовой механикой. По-видимому, впервые вопрос о принципиальных ограничениях, накладываемых специальной теорией относительности на измеримость различных динамических переменных квантовой системы, рассматривался в работе Ландау и Пайерлса [1]. Качественные соображения работы [1], основанные на рассмотрении соотношений неопределенности вместе с ограничением на предельную скорость, привели к выводу о том, что « ... все фигурирующие в волновой механике физические величины в релятивистской области оказываются уже неопределимыми». В нерелятивистской квантовой механике не запрещается в принципе сколь угодно точное измерение, например импульса квантовой системы, за сколь угодно малое (нулевое) время. Оператор импульса является нелокальным, и собственное состояние оператора импульса (плоская волна) является бесконечно протяженным в пространстве. Разумеется, плоская волна не является физически реализуемым состоянием, поскольку она не нормирована. Однако такое состояние может быть приближено сколь угодно точно состоянием, локализованным в сколь угодно большой, но конечной пространственной области, причем таким состоянием, что среднее значение оператора импульса, измеренное на этом состоянии, будет сколь угодно близко к значению импульса в состоянии плоской волны. Такое измерение импульса подразумевает доступ целиком к состоянию, присутствующему в сколь угодно большой пространственной области. В нерелятивистской квантовой механике нет запретов на получение доступа к любой области за нулевое время, поэтому нет ограничений в принципе на сколь угодно точное мгновенное измерение, напри-

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

мер, импульса. С учетом ограничений специальной теории относительности доступ к бесконечной области требует бесконечного времени, и в этом смысле физические величины являются неопределимыми (точнее говоря, неопределимыми, если мы требуем точного их определения за конечное время).

Если требовать точного измерения импульса (т. е. использовать собственное состояние оператора импульса, точнее говоря, обобщенный собственный вектор), то он является неопределимым уже и в нерелятивистском случае из-за нереализуемости точно плоской волны. Можно лишь сколь угодно точно приближаться к точному измерению. Существенно, что в нерелятивистской квантовой механике нет никаких запретов на время, необходимое для получения результата. В релятивистском случае также нет запретов на сколь угодно точное измерение, например, импульса, однако необходимость доступа к формально бесконечной области для точного измерения импульса требует бесконечного времени. Воспринимаемые таким образом утверждения работы [1] о невозможности определения точного значения импульса не содержат никакого внутреннего противоречия.

Дальнейшее исследование вопроса об измерениях над квантовыми системами в релятивистском случае было сделано в работе Бора и Розенфельда [2]. Насколько мы можем судить, аргументы работы [2] не отменяют ограничений, высказанных в работе [1] относительно необходимого времени, поскольку эти соображения фактически следуют из ограничений, диктуемых специальной теорией относительности. Практически в неизменном виде аргументы работы [1] воспроизводятся позднее в [3].

Ниже нас будет интересовать вопрос об ограничениях, диктуемых релятивистской квантовой теорией, на вероятность достоверного различения двух состояний квантовой системы. Поскольку в качестве носителей информации используются фотоны, которые являются существенно релятивистскими частицами, ограничения, накладываемые на измерения в релятивистском случае, являются принципиальными. Кроме того, возникающие ограничения на различимость могут только расширить возможности для конструирования различных криптографических протоколов в релятивистском случае.

Все нерелятивистские квантовые криптографические протоколы в том или ином виде используют следующие два обстоятельства. Во-первых, это так называемая «no cloning»-теорема [4] о невозможности копирования неизвестного квантового состояния, т. е. утверждение о невозможности процесса

$$|A\rangle|\psi\rangle \to U(|A\rangle|\psi\rangle) = |B_\psi\rangle|\psi\rangle|\psi\rangle,$$

где $|A\rangle$ и $|B_\psi\rangle$ — состояния аппарата до и после копирования, U — некоторый унитарный оператор. Такой процесс запрещен в силу линейности и унитарности эволюции в квантовой механике. Во-вторых, это невозможность даже более слабого процесса получения какой бы то ни было информации об одном из двух неортогональных состояний без их возмущения [5], т. е. запрет на процесс вида

$$|A\rangle|\psi_1\rangle \to U(|A\rangle|\psi_1\rangle) = |A_{\psi_1}\rangle|\psi_1\rangle,$$

$$|A\rangle|\psi_2\rangle \to U(|A\rangle|\psi_2\rangle) = |A_{\psi_2}\rangle|\psi_2\rangle$$

с $|A_{\psi_1}\rangle \neq |A_{\psi_2}\rangle$, если $\langle\psi_1|\psi_2\rangle \neq 0$, что означает невозможность достоверного различения неортогональных состояний. Для ортогональных состояний такого запрета не существует. Более того, в нерелятивистской квантовой механике, вообще говоря, нет запрета на мгновенное (сколь угодно быстрое) достоверное различение ортогональных состояний в любой момент времени без их возмущения. Если имеется пара ортогональных состояний в гильбертовом пространстве $\mathcal{H}$, $|\psi_{1,2}\rangle \in \mathcal{H}$ и $\langle\psi_1|\psi_2\rangle = 0$, то состояния достоверно различимы при помощи измерения, описывающегося ортогональным разложением единицы в $\mathcal{H}$:

$$\mathcal{P}_1 + \mathcal{P}_2 + \mathcal{P}_\perp = I, \quad \mathcal{P}_{1,2} = |\psi_{1,2}\rangle\langle\psi_{1,2}|,$$

$$\mathcal{P}_\perp = I - \mathcal{P}_1 - \mathcal{P}_2,$$

где $\mathcal{P}_{1,2}$ — проекторы на подпространства $\mathcal{H}_{1,2}$, натянутые на $|\psi_{1,2}\rangle$, $\mathcal{P}_\perp$ — проектор на подпространство $\mathcal{H}_{1,2}^\perp = (\mathcal{H}_1 \oplus \mathcal{H}_2)^\perp$. Вероятность получения исхода 1 на множестве результатов $\Theta = \{1, 2, \perp\}$, если входным состоянием является, например, $|\psi_1\rangle$, равна

$$\Pr\{|\psi_1\rangle\} = \mathrm{Tr}\{|\psi_1\rangle\langle\psi_1|\mathcal{P}_1\} = 1, \tag{1}$$

а в каналах $\mathcal{P}_{2,\perp}$ тождественно равна нулю:

$$\Pr\{|\psi_1\rangle\} = \mathrm{Tr}\{|\psi_1\rangle\langle\psi_1|\mathcal{P}_{2,\perp}\} = 0, \tag{2}$$

и аналогично для входного состояния $|\psi_2\rangle$. Данные соотношения означают, что ортогональные состояния различимы достоверно. Более того, состояния различимы без возмущения и мгновенно. При этом подразумевается, что гильбертово пространство состояний доступно целиком. Поскольку не существует физических систем вне координатного пространства, доступ к гильбертову пространству состояний

автоматически подразумевает доступ к той области координатного пространства, где отличен от нуля носитель состояния.

В релятивистском случае невозможность мгновенного получения доступа к конечной области пространства приводит к тому, что ортогональные протяженные в координатном пространстве состояния различимы достоверно как целостные объекты только в том случае, если они доступны для измерения целиком (т. е. измерительная аппаратура имеет доступ ко всей пространственной области, где отличны от нуля носители состояний). Данное обстоятельство будет использовано ниже при построении протокола.

Многие криптографические задачи сводятся к ряду примитивных криптографических протоколов обмена. Таковыми являются протокол распространения ключа (криптография) [6–8], протоколы привязки к биту (bit commitment) и подбрасывания монеты — выбор жребия на расстоянии (coin tossing) [9–12]. Протокол привязки к биту является более сильным протоколом, чем задача о подбрасывании монеты на расстоянии в том смысле, что если можно реализовать привязку к биту, то на ее основе можно сформулировать протокол подбрасывания монеты.

В словесном и неформализованном виде протокол привязки к биту обычно формулируется так. Имеются два пространственно удаленных участника протокола A и B. Участник A на стадии привязки к биту (commitment) выбирает значение секретного бита 0 или 1 и посылает часть информации о нем участнику B, причем по части информации B не может достоверно узнать, что задумал A. Точнее говоря, в идеальном случае вероятность правильной идентификации за счет измерений по части информации о секретном бите составляет $1/2$, т. е. равна вероятности простого угадывания. Затем на стадии раскрытия B может затребовать у A оставшуюся часть информации о бите. В идеальном случае участник B на стадии раскрытия должен с достоверностью (вероятностью 1) восстановить секретный бит, задуманный A. Кроме того, у A не должно оставаться возможности изменить значение задуманного бита уже после того, как он передал первую часть информации к B.

Протокол подбрасывания монеты на расстоянии формулируется следующим образом. Пространственно удаленные участники A и B, каждый из которых не доверяет другому и имеет все допустимые возможности для обмана в свою пользу, должны обменяться информацией так, чтобы в итоге (в идеале с вероятностью 1) они должны были согласиться с тем, что возникший в результате протокола бит является честным жребием. Если участники могут обмениваться информацией только по классическому каналу связи, то задача может даже казаться неразрешимой.

Понятно, что если можно реализовать секретный протокол bit commitment, то на его основе можно устроить протокол подбрасывания монеты на расстоянии. Для этого участник B после стадии commitment и до стадии раскрытия должен попытаться угадать секретный бит, задуманный A (который после стадии раскрытия будет известен достоверно). Если B угадывает секретный бит, то выигрывает он, в противном случае выигрывает A.

В качестве простого примера протокола bit commitment приводят иногда следующий протокол. Участник A записывает задуманный бит на листке бумаги и помещает его в сейф, который отправляет к B (стадия commitment), а ключ от сейфа оставляет у себя до стадии раскрытия. Несмотря на простоту данного примера, он содержит все главные черты протоколов, основанных на классических носителях информации. В данном примере B получает от A в свое распоряжение не часть информации о секретном бите, а сразу всю. Поэтому законы природы не запрещают (имея достаточные технические возможности) узнать значение секретного бита еще до стадии раскрытия. Аналогичная ситуация имеет место и в протоколах, основанных на вычислительной сложности некоторых функций-ловушек (например, дискретного логарифма) [13]. В подобных протоколах A представляет B значение y (где $y = a^b \bmod p$; a и p известны заранее, а четность b является секретным битом). Предоставленной информации о b (значение функции y) уже достаточно, чтобы достоверно узнать (вычислить посредством нахождения дискретного логарифма) значение секретного бита. Однако для известных классических вычислительных алгоритмов такое вычисление требует больших (даже экспоненциально больших) вычислительных ресурсов; правда, до сих пор не доказано, что не существует более эффективных (полиномиальных) классических алгоритмов.

Для случая, когда A и B могут обмениваться информацией лишь по классическому каналу связи, задача была решена в работе [13]. В строгом смысле протокол [13] не является секретным относительно обмана одним из участников, поскольку основан на недоказанной сложности вычисления дискретного логарифма [13].

В таких протоколах также предоставляется не «часть», а вся информация, и законы природы не запрещают, используя эту информацию, еще до стадии раскрытия (например, используя квантовый компьютер [14, 15], который, правда, еще весьма далек от экспериментальной реализации) узнать значение секретного бита.

Используя в качестве носителей информации классические (нерелятивистские) объекты, невозможно реализовать безусловно секретный протокол bit commitment (секретность которого основана лишь на фундаментальных запретах законов природы, а не на технических возможностях), когда предоставляется «часть» классического объекта (например, пространственно-протяженный сигнал, лишь часть которого до стадии раскрытия доступна участнику B). Поскольку доступная для B часть сигнала до стадии раскрытия должна выглядеть одинаково для значений бита 0 или 1 (чтобы B имел нулевую информацию о бите до стадии раскрытия), оставшаяся в распоряжении A часть классического объекта (сигнала) должна различаться для значений бита 0 и 1. Законы нерелятивистской классической физики не запрещают мгновенно изменить оставшуюся у A часть сигнала так, чтобы переделать 0 в 1 и наоборот, перед тем как предоставить ее участнику B непосредственно перед стадией раскрытия, т. е. ничто не запрещает A изменить значение задуманного бита. Поэтому в рамках нерелятивистской классической физики невозможно реализовать безусловно секретный протокол bit commitment.

Нерелятивистские квантовые протоколы в качестве носителей информации используют квантовые системы. Протоколы в общих чертах выглядят следующим образом. Выбирается гильбертово пространство состояний $\mathcal{H}_s$, которому принадлежат состояния носителей информации. A выбирает состояния системы $|\psi_{0,1}\rangle \in \mathcal{H}_s$, соответствующие 0 или 1, и посылает их к B. Как правило, состояния выбираются неортогональными. Существенно, что пространство состояний $\mathcal{H}_s$ неявно подразумевается доступным целиком в течение всего протокола как для A, так и B. Требование того, чтобы до стадии раскрытия матрицы плотности состояний, отвечающих 0 и 1, выглядели для B одинаково, приводит к возможности необнаруживаемого обмана участником A участника B при помощи EPR-атаки [16, 17]. При этом, грубо говоря, весь протокол затрагивает лишь пространство состояний систем. Однако такая ситуация является фиктивной и не отвечающей реальной ситуации при передаче информации. Более точно, имеется в виду следующее. Участники протокола не могут контролировать все пространство, а контролируют лишь определенные области (пределы своих лабораторий, измерительные устройства и т. д.). Кроме того, все измерения происходят также в реальном пространстве и времени (или пространстве-времени, если речь идет о релятивистском случае). Нерелятивистская квантовая механика не запрещает создание запутанных состояний физически различимых систем (нас интересует только этот случай, так как если обе системы тождественны, то невозможно провести измерение, затрагивающее только одну из них). Поэтому, если участники контролируют лишь неперекрывающиеся области, то запутанное состояние из $\mathcal{H}_s \otimes \mathcal{H}_a$ автоматически обязано быть нелокальным и в координатном пространстве. Волновые функции обеих подсистем из $\mathcal{H}_s$ и $\mathcal{H}_a$ должны иметь одновременно носители как в области, контролируемой A, так и в области, контролируемой B (в противном случае состояние для участников не будет запутанным). Последнее означает, что каждый из участников имеет доступ как к пространству состояний $\mathcal{H}_s$, так и к $\mathcal{H}_a$, и может по своему усмотрению проводить измерения и унитарные преобразования над подсистемами в силу их физической различимости, т. е. локальность преобразований в пространстве состояний $\mathcal{H}_s \otimes \mathcal{H}_a$ (в смысле манипуляций в одном из подпространств состояний) не означает локальности в координатном пространстве. Иными словами, пространство состояний носителей информации в подобного рода нерелятивистских квантовых протоколах (когда пространственно-временная структура состояний носителей информации явно не учитывается) доступно обоим пользователям. В этом смысле такие протоколы не реализуют идею о предоставлении части информации о носителе секретного бита.

Явное использование эффектов распространения состояний в координатном пространстве, когда участнику B доступна лишь часть состояния из-за его протяженности в пространстве, в нерелятивистском случае, по-видимому, не может привести к чему-то новому применительно к упомянутым задачам из-за отсутствия предельной скорости распространения.

Постановка задачи, когда используется только специфика пространства состояний $\mathcal{H}$, не отвечает реальной ситуации при передаче информации в реальном пространстве-времени. Более естественна постановка, когда участники протокола располагаются в пределах своих лабораторий и контролируют пространственные области в их окрестности. Естественно, что A и B не могут контролировать все координ-

натное пространство одновременно и иметь к нему доступ.

Впервые явное использование эффектов распространения состояний (учет их пространственно-временной структуры) применительно к задаче квантовой криптографии рассматривался в работе [18] (которая, как нам кажется, в свое время не была правильно оценена [19, 20]). Учет ограничений, накладываемых специальной теорией относительности и квантовой механикой (квантовой теорией поля), заметно упрощает доказательство безусловной секретности релятивистских квантовых криптосистем [21, 22]. Кроме того, теория поля накладывает дополнительные принципиальные ограничения, например, на телепортацию квантовых состояний [23].

Недавно были предложены классические протоколы привязки к биту и подбрасывания монеты на расстоянии, учитывающие существование предельной скорости распространения сигнала (информации) [24]. Релятивистский классический протокол [24] является безусловно секретным (т. е. секретность основана только на фундаментальных законах природы) и позволяет в принципе задерживать вторую стадию протокола, т. е. сохранять информацию о секретном бите, задуманном A, сколь угодно долго. Для реализации протокола требуется, чтобы каждый из участников A и B контролировал по два пространственно-разделенных узла.

Идея релятивистских квантовых протоколов bit commitment и coin tossing, использующих ортогональные состояния, высказывалась ранее в работах [25]. Идея протоколов [25] базировалась на двух простых обстоятельствах. Первое состоит в том, что два ортогональных (а значит, достоверно различимых, если они целиком доступны для измерений) состояния становятся эффективно неортогональными (достоверно неразличимыми) при ограничении на подпространство. Данный факт имеет место и в нерелятивистской квантовой механике. Если имеется пара протяженных в координатном пространстве ортогональных состояний, например,

$$(\psi_0,\psi_1)=\int\limits_{-\infty}^{\infty}\psi_0^*(x)\psi_1(x)\,dx=0,$$

$$\psi_{0,1}(x)\in\mathcal{L}^2(-\infty,\infty,dx),$$

то они становятся эффективно неортогональными при ограничении на подпространство (конечную область в координатном пространстве Ω):

$$(\psi_0,\psi_1)_\Omega=\int\limits_{\Omega}\psi_0^*(x)\psi_1(x)\,dx\neq 0.$$

Второе существенное обстоятельство — это наличие предельной скорости распространения как квантовых состояний, так и классических объектов, диктуемое специальной теорией относительности. Оно гарантирует, что доступ ко всему состоянию целиком (области, где присутствует состояние) не может быть получен мгновенно.

В отличие от работ [25], где состояние не имело «внутренних» степеней свободы, использование состояний с «внутренними» степенями свободы (например, спиральности для фотонов) позволяет упростить протоколы.

Говоря точнее, состояния для 0 и 1 вида

$$|\psi_{0,1}\rangle=\psi(x)\otimes|e_{0,1}\rangle,\quad \langle e_0|e_1\rangle=0,$$

ортогональны (из-за внутренних степеней свободы), даже если целиком они и недоступны для измерений (для измерений доступна лишь часть координатного пространства, где отлична от нуля функция $\psi(x)$), но при этом они не различимы достоверно: вероятность различения (вероятность получения отсчета в одном из ортогональных каналов 0 или 1) может быть сделана сколь угодно малой, если доступна лишь часть состояния, поскольку вероятность отсчета в конечной области пространства Ω есть

$$\langle\psi_i|\psi_i\rangle_\Omega=\int\limits_{\Omega}|\psi(x)|^2\,dx<1,\quad i=0,1,$$

и выбором размера области и вида $\psi(x)$ она может быть сделана сколь угодно малой. Последнее фактически диктуется условием нормировки состояния

$$\int\limits_{-\infty}^{\infty}|\psi(x)|^2\,dx=1.$$

Наша идея протокола в общих чертах состоит в следующем. Участник A контролирует некоторую конечную область координатного пространства и готовит в ней квантовое состояние в оговоренный протоколом момент времени, которое распространяется в канал связи и постепенно становится доступным для измерений участнику B в области, которую A уже не контролирует. Имея доступ лишь к части квантового состояния в реальном пространстве, B не может иметь достоверную информацию о секретном бите (достоверно отличить 0 от 1), причем можно выбрать состояния так, чтобы вероятность различения 0 и 1 за счет измерений у B была сколь угодно близкой к 1/2 (вероятности случайного угадывания) в течение сколь угодно большого (но заранее оговоренного в начале протокола) промежутка времени. При этом никаких фундаментальных

ограничений на то, чтобы выбрать данный интервал сколь угодно большим, не существует (хотя технически это и может быть сложно). Факт существования предельной скорости позволяет выбрать состояния таким образом, что когда часть состояния покидает область, контролируемую A, и становится недоступной, участник A уже не может изменить свое состояние (значение задуманного бита). По истечении времени протокола, когда состояния становятся доступными для измерений B целиком, он получает о них информацию с вероятностью, сколь угодно близкой к единице. Для данного протокола существенны как квантовость состояний, так и факт существования предельной скорости, диктуемый специальной теорией относительности.

В разд. 2 описаны состояния и измерения, используемые в протоколах, в разд. 3 и 4 приведены протоколы bit commitment и coin tossing для состояний с компактными носителями, в разд. 5 внесены необходимые изменения в протоколы, учитывающие принципиальную нелокализуемость состояний в теории поля. В Заключении кратко изложены основные полученные в статье результаты.

2. СОСТОЯНИЯ И ИЗМЕРЕНИЯ, ИСПОЛЬЗУЕМЫЕ В ПРОТОКОЛЕ

Поскольку в протоколе явно используется пространственно-временная структура состояний, он не может быть сформулирован без учета конкретной геометрии системы. Будем рассматривать одномерную модель, которая содержит все необходимые для протокола особенности, диктуемые теорией поля. Подобная модель часто используется в квантовой оптике. Будем иметь в виду состояния поля, отвечающие безмассовому полю, состояния которого задаются в импульсном представлении на массовой поверхности $k_0^2 - k^2 = 0$. Для нас будут существенны состояния, распространяющиеся в положительном направлении оси x ($k > 0$). Считаем, что участник A контролирует область в окрестности x_A, а B — в окрестности x_B ($x_A < x_B$).

Далее все функции считаются зависящими от разности $\tau = t - x$; скорость света полагаем равной единице, $c = 1$. Такое представление отражает интуитивные представления о пакете, движущемся со световой скоростью. Собственный вектор $|k\rangle$ оператора импульса, отвечающий значению импульса k, является обобщенным собственным вектором (точнее, линейным непрерывным функционалом на элементах из плотного подмножества в $\mathcal{H} = \mathcal{L}^2(0, \infty, d\xi)$) и имеет вид

$$\langle \xi | k \rangle = \delta(k - \xi). \tag{3}$$

Состояния $|\psi\rangle$ из $\mathcal{H}$ могут быть разложены по обобщенным состояниям:

$$|\psi\rangle = \int_0^\infty \langle k|\psi\rangle |k\rangle \, dk, \tag{4}$$

где значение функционала $\langle k|$ на элементах $|\psi\rangle$ есть

$$\langle k|\psi\rangle = \int_0^\infty \psi(\xi)\delta(k - \xi)\, d\xi = \psi(k),$$

т. е. амплитуда состояния $|\psi\rangle$ в k-представлении. Соответственно, амплитуда состояния $|k\rangle$ в τ-представлении имеет вид

$$\begin{aligned} &\langle k|\tau\rangle = \frac{1}{\sqrt{2\pi}} e^{ik\tau}, \quad k \in (0, \infty), \\ &\tau \in (-\infty, \infty), \quad \tau = t - x. \end{aligned} \tag{5}$$

Такая форма записи отражает интуитивные представления о плоской волне (состоянии с определенным значением импульса), движущейся со световой скоростью.

Для протокола будет существенно, что квантовые состояния распространяются с предельно допустимой световой скоростью. В τ-представлении ортогональные состояния (пакеты), отвечающие 0 и 1 и используемые в протоколе, имеют вид

$$\begin{aligned} &|\psi_{0,1}\rangle = \int_{-\infty}^\infty f(\tau)|\tau\rangle \, d\tau \otimes |e_{0,1}\rangle, \\ &\langle e_0|e_1\rangle = 0, \quad \langle e_{0,1}|e_{0,1}\rangle = 1, \end{aligned} \tag{6}$$

где состояния $|e_{0,1}\rangle$ отвечают внутренним степеням свободы (например, спиральности для фотона).

Условие нормировки состояний имеет вид

$$\langle \psi_{0,1}|\psi_{0,1}\rangle = \int_{-\infty}^\infty \int_{-\infty}^\infty f(\tau) f^*(\tau') \langle \tau|\tau'\rangle \, d\tau d\tau' = 1, \tag{7}$$

где

$$\begin{aligned} \langle \tau|\tau'\rangle = \frac{1}{2\pi}\delta_+(\tau - \tau') = \frac{1}{2\pi}\int_0^\infty e^{ik(\tau - \tau')}\, dk = \\ = \frac{1}{2}\delta(\tau - \tau') + \frac{i}{\pi}\,\frac{1}{\tau - \tau'}. \end{aligned} \tag{8}$$

Введем амплитуду состояния в k-представлении, которую определим как

$$f(\tau) = \int_0^\infty f(k) e^{-ik\tau} dk. \tag{9}$$

Далее для нормировки состояния с учетом (5)–(7) имеем

$$\langle \psi_{0,1} | \psi_{0,1} \rangle = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f(\tau) f^*(\tau') \times \times \left[\frac{1}{2} \delta(\tau - \tau') + \frac{i}{\pi} \frac{1}{\tau - \tau'} \right] d\tau d\tau'. \tag{10}$$

Подстановка в (8) амплитуды в k-представлении из (7) с учетом того, что [26]

$$\int_{-\infty}^{\infty} e^{ik\tau} \frac{1}{\tau + a} d\tau = i\pi \operatorname{sign} k \cdot e^{-iak}, \tag{11}$$

дает

$$\langle \psi_{0,1} | \psi_{0,1} \rangle = \int_{-\infty}^{\infty} |f(\tau)|^2 d\tau = 1. \tag{12}$$

Требование микропричинности [27] приводит к тому, что полевые операторы, порождающие состояния поля, принадлежащие гильбертову пространству состояний, своим действием на вакуумный вектор, должны коммутировать (или антикоммутировать), если они относятся к пространственно-подобным областям. Коммутатор полевых операторов, как известно, является обобщенной функцией (см. детали в [27]). Для того чтобы можно было говорить о локальных свойствах обобщенных функций, основные функции должны обладать определенными свойствами (фактически принадлежать пространству $\mathcal{J}(\hat{x})$ — пространству бесконечно-гладких функций, убывающих на бесконечности быстрее, чем $|\hat{x}|^{-n}$ для любого натурального n). Иными словами, состояния свободного поля не могут иметь компактный носитель (т. е. быть отличными от нуля лишь в конечной области пространства и принадлежать пространству $\mathcal{D}(\hat{x})$), т. е. состояния свободного поля являются принципиально нелокализуемыми. Однако теория поля разрешает состояния, сколь угодно сильно локализованные в пространстве и убывающие сколь угодно близко к экспоненциальной зависимости (см., например, [28–32]). Кроме того, функции из $\mathcal{D}(\hat{x})$ с компактным носителем образуют плотное множество в $\mathcal{J}(\hat{x})$, т. е. любая функция из $\mathcal{J}(\hat{x})$ может быть приближена функциями из $\mathcal{D}(\hat{x})$ с любой степенью точности.

Применительно к нашей одномерной модели нелокализуемость может быть усмотрена из теоремы Винера–Пэли [33], поскольку условие нормировки (10) с учетом (7) означает квадратичную интегрируемость амплитуды в k-представлении и накладывает ограничения на асимптотическое поведение функции $f(\tau)$:

$$f(\tau) = \int_0^\infty f(k) e^{-ik\tau} dk, \quad \int_{-\infty}^{\infty} \frac{|\ln|f(\tau)||}{1+\tau^2} d\tau < \infty. \tag{13}$$

Как следует из (11), функция $f(\tau)$ не может иметь компактный носитель по τ и не может убывать экспоненциально, но может быть сделана сколь угодно сильно локализованной и с убыванием, сколь угодно близким к экспоненциальному, например,

$$f(\tau) \propto \exp\left\{ -\frac{\alpha\tau}{\ln(\ln(\ldots \ln \tau))} \right\}, \tag{14}$$

где α может быть любым положительным числом.

Для наглядности и удобства сформулируем сначала протокол для состояний с компактным носителем (поскольку функции из $\mathcal{D}(\tau)$ образуют плотное множество и любая функция $f(\tau)$ может быть приближена с любой степенью точности функциями из $\mathcal{D}(\tau)$), а затем внесем необходимые изменения для нелокализованных состояний.

Пусть состояние $f(\tau)$ имеет компактный носитель, $\operatorname{supp} f(\tau) = (-\Delta\tau, \Delta\tau)$ ($\Delta\tau$ может быть выбрано сколь угодно малым). В формирование состояний дают вклад лишь векторы $|\tau\rangle$ из области $(-\Delta\tau, \Delta\tau)$ на световом конусе

$$|\psi_{0,1}\rangle = \int_{-\Delta\tau}^{\Delta\tau} f(\tau) |\tau\rangle \, d\tau \otimes |e_{0,1}\rangle. \tag{15}$$

В отличие от нерелятивистских квантовых протоколов, где не используется явно пространственно-временная структура состояний и не существенны эффекты приготовления состояний (точнее говоря, в нерелятивистской квантовой механике нет запретов на мгновенное (в любой момент времени) приготовление состояний из $\mathcal{H}$, даже нелокальных в координатном пространстве), в теории поля ситуация иная. Приготовление состояний требует доступа к конечной области (даже если считать носитель компактным) пространства-времени. В одномерной ситуации требуется либо область координатного пространства размером $\Delta x = 2\Delta\tau$, если состояние приготавливается нелокальным источником в фиксированный момент времени t, либо конечный интервал времени $\Delta t = 2\Delta\tau$, если состояние

испускается точечным источником в точке x. Поэтому в релятивистском случае протокол не может быть сформулирован без учета конкретной геометрии системы. Одномерная ситуация наиболее проста для анализа, поскольку здесь все величины зависят от одной переменной $\tau = x - t$. Если иметь в виду, что в экспериментах используются квазиодномерные оптоволоконные системы, то рассмотрение модельной одномерной ситуации является вполне осмысленным.

Рассмотрим теперь «растянутые» состояния, которые потребуются для протокола, состоящие из двух половинок, разнесенных на световом конусе на интервал τ_0, и имеющие вид

$$|\psi_{0,1}(\tau_0)\rangle = \\ = \frac{1}{\sqrt{2}} \int (f(\tau) + f(\tau - \tau_0))|\tau\rangle) d\tau \otimes |e_{0,1}\rangle. \quad (16)$$

Здесь и ниже принята нормировка

$$\int\limits_{-\infty}^{\infty} |f(\tau)|^2 d\tau = \int\limits_{-\infty}^{\infty} |f(\tau - \tau_0)|^2 d\tau = 1, \\ \mathrm{supp} f(\tau) \cap \mathrm{supp} f(\tau - \tau_0) = \varnothing. \quad (17)$$

Поскольку исходное состояние имеет носитель в $(-\Delta\tau, \Delta\tau)$, для приготовления состояния требуется контролировать область на световом конусе $(-\Delta\tau, \Delta\tau + \tau_0)$ (либо область координатного пространства $\Delta x = (-\Delta\tau, \Delta\tau + \tau_0)$, если приготовление проводится нелокальным прибором в фиксированный момент времени, либо требуется время $\Delta t = (-\Delta\tau, \Delta\tau + \tau_0)$, если состояние испускается локальным источником в точке x).

Обсудим теперь индивидуальные измерения, осуществляемые вторым участником протокола над отдельным состоянием. Измерения даются разложением единицы, причем пространством результатов измерений является множество $\Omega = \{\tau \in (-\infty, \infty), i = 0, 1\}$:

$$I = \left(\int\limits_{-\infty}^{\infty} \mathcal{M}(d\tau) \right) \otimes (\mathcal{P}_0 + \mathcal{P}_1) = \\ = \left(\int\limits_{-\infty}^{\infty} d\tau \left(\int\limits_{0}^{\infty} e^{ik\tau} |k\rangle \, dk \right) \left(\int\limits_{0}^{\infty} e^{-ik'\tau} \langle k'| \, dk' \right) \right) \otimes \\ \otimes (\mathcal{P}_0 + \mathcal{P}_1), \quad \langle k|k'\rangle = \delta(k - k'), \quad (18)$$

где $|k\rangle$ — формальный собственный вектор с заданным k, и

$$\mathcal{M}(d\tau) = |\tau\rangle\langle\tau| \, d\tau, \quad \mathcal{P}_0 = |e_0\rangle\langle e_0|, \quad \mathcal{P}_1 = |e_1\rangle\langle e_1|.$$

Нам также потребуется описание распространения состояний через квантовый канал связи из области, контролируемой A, в область, контролируемую B. Такое распространение дается унитарной трансляцией состояния $|\psi_{0,1}\rangle$ вдоль ветви светового конуса $\tau = x - t$:

$$\mathcal{U}_{ch}(\tau_{ch})|\psi_{0,1}\rangle = |\psi_{0,1,\tau_{ch}}\rangle = \frac{1}{\sqrt{2}} \times \\ \times \int (f(\tau - \tau_{ch}) + f(\tau - \tau_0 - \tau_{ch})) \, d\tau \otimes |e_{0,1}\rangle, \quad (19)$$

здесь τ_{ch} — длина канала связи. Соотношение между «протяженностью» состояния $(2\Delta\tau + \tau_0)$ и длиной канала связи (τ_{ch}) должно быть таким, чтобы

$$\tau_{ch} < \tau_0 + 2\Delta\tau,$$

поэтому без потери общности можно считать, что $\tau_{ch} = 0$ (поскольку его длина может быть любой, лишь бы она не превосходила «протяженности» состояний).

Вероятность получения результата у пользователя B в канале i в интервале $d\tau$ на входном состоянии $|\psi_j(\tau_0)\rangle$ дается выражением

$$\Pr\{d\tau; i, j\} = \\ = \mathrm{Tr}\left\{ \left((\mathcal{M}(d\tau)) \otimes \mathcal{P}_i \right) |\psi_j(\tau_0)\rangle\langle\psi_j(\tau_0)| \right\} = \\ = \delta_{ij} \frac{1}{2} \left\{ |f(\tau)|^2 + |f(\tau - \tau_0)|^2 \right\} d\tau. \quad (20)$$

Данное выражение описывает плотность вероятности получения результата в одном из ортогональных (различимых) каналов для 0 $(i = j = 0)$ и 1 $(i = j = 1)$ в интервале $d\tau$. На интуитивном уровне такое измерение может быть интерпретировано как реализуемое с помощью фотодетектора с малым (формально с нулевым) внутренним временем срабатывания, работающего в ждущем режиме. Результат измерения является случайным событием, происходящим в интервале $d\tau$ с плотностью вероятности (20).

Вероятность зарегистрировать состояния в конечном интервале $\Delta(\tau)$ (при $i = j$) дается выражением

$$\Pr\{\Delta(\tau)\} = \int\limits_{\Delta(\tau)} \Pr\{d\tau; i, i\} = \\ = \frac{1}{2} \left\{ \int\limits_{\Delta(\tau)} |f(\tau)|^2 d\tau + \int\limits_{\Delta(\tau)} |f(\tau - \tau_0)|^2 d\tau \right\}. \quad (21)$$

Если интервал $\Delta(\tau)$ (доступная область на световом конусе) не накрывает носитель состояния целиком

(например, если накрывается только одна из половинок состояния), то вероятность получения результата равна $1/2$. Однако если результат получен, то из-за ортогональности каналов регистрации $\mathcal{P}_0$ и $\mathcal{P}_1$ состояния идентифицируются однозначно. Поэтому в течение времени $\Delta\tau \le \tau \le \tau_0 + \Delta\tau$ вероятность ошибки при идентификации состояния за счет измерений составляет $1/4$. Соответственно, вероятность правильной идентификации равна $3/4$. При простом угадывании без измерений ошибка составляет $1/2$.

Отметим еще раз, что данное измерение ни в коем случае не может быть интерпретировано как длящееся конечное время $\Delta(\tau)$. Каждый раз результат измерения возникает случайно в какой-то момент времени t с плотностью вероятности (20).

По истечении времени $\tau_0 + 2\Delta\tau$, когда состояние целиком попадает в область, доступную для измерений у B, 0 или 1 идентифицируются из-за ортогональности состояний однозначно.

Таким образом, распространение состояний с предельно допустимой скоростью позволяет явно и естественно реализовать идею о предоставлении участником A части информации (части квантового состояния) о задуманном секретном бите. Квантовый характер состояний существен для протокола, поскольку для классического сигнала, если бы $f(\tau)$ описывала форму сигнала с различной поляризацией e_0 или e_1, вероятность идентификации состояний даже при доступе только к половинке состояния составляла бы 1, а не $3/4$, как в квантовом случае. Вероятность $3/4$ в квантовом случае при доступе к половине состояния фактически следует из нормировки состояния.

Данный результат может быть получен несколько иным способом, позволяющим прояснить отличие ситуации, когда для измерений доступна лишь часть гильбертова пространства состояний, т. е. часть носителя состояния. Найдем измерение, минимизирующее ошибку при различении двух состояний, описываемых матрицами плотности, когда доступна лишь часть носителя состояний. Матрицы плотности имеют вид

$$\rho_{0,1} = \left\{ \frac{1}{\sqrt{2}} \left(\int\limits_{-\infty}^{\infty} [f(\tau) + f(\tau-\tau_0)] |\tau\rangle \, d\tau \right) \times \right.$$
$$\left. \times \frac{1}{\sqrt{2}} \left(\int\limits_{-\infty}^{\infty} [f^*(\tau') + f^*(\tau'-\tau_0)] \langle\tau'| \, d\tau' \right) \right\} \otimes$$
$$\otimes |e_{0,1}\rangle\langle e_{0,1}| = \rho(f) \otimes \rho(0,1). \quad (22)$$

Получим теперь выражение для ошибки при различении состояний $\rho_{0,1}$, когда для измерений доступна лишь часть пространства-времени. Формально задача сводится к случаю, когда имеется область $\Delta(\tau)$, доступная для измерений, а остальная часть пространства-времени недоступна для измерений (эту область обозначим $\overline{\Delta}(\tau) = (-\infty,\infty)\backslash\Delta(\tau)$).

Измерение дается разложением единицы, которое состоит из двух слагаемых. Одно слагаемое представляет собой единицу в подпространстве, натянутом на базисные векторы $|\tau\rangle$, принадлежащие интервалу $\Delta(\tau)$, а второе — на векторы из недоступной для измерений области

$$\overline{\Delta}(\tau) = (-\infty,\infty)\backslash\Delta(\tau).$$

Имеем

$$I \otimes \mathbf{C}^2 = I(\Delta\tau) \otimes \mathbf{C}^2 + I(\overline{\Delta}(\tau)) \otimes \mathbf{C}^2 =$$
$$= \left(\int\limits_{\Delta(\tau)} |\tau\rangle\langle\tau| \, d\tau \right) \otimes \mathbf{C}^2 +$$
$$+ \left(\int\limits_{\overline{\Delta}(\tau)} |\tau\rangle\langle\tau| \, d\tau \right) \otimes \mathbf{C}^2. \quad (23)$$

Пусть состояние ρ_0 предъявляется для измерений с априорной вероятностью π_0, а состояние ρ_1 с вероятностью π_1 ($\pi_0 + \pi_1 = 1$). Далее $\pi_0 = \pi_1 = 1/2$, т. е. 0 или 1 загадываются участником B равновероятно.

Поскольку для измерений доступна лишь часть пространства-времени (и автоматически это означает ограничение доступа к гильбертову пространству состояний, поскольку базисные состояния нумеруются с помощью τ), полная ошибка складывается из двух слагаемых. Первое слагаемое ($P_e(\overline{\Delta}(\tau))$) отвечает тому, что измерительное устройство у участника B не сработало (исход имел место в недоступной области). Второе ($P_e(\Delta(\tau))$) описывает ошибку при различении состояний, когда исход имел место в доступной для измерений участником B области.

Вероятность того, что состояние не было обнаружено участником B (его измерительное устройство не сработало), есть

$$P(\overline{\Delta}(\tau)) = \mathrm{Tr}\left\{ (\pi_0\rho_0 + \pi_1\rho_1) \left(I(\overline{\Delta}(\tau)) \otimes \mathbf{C}^2 \right) \right\} =$$
$$= \pi_0 p_0 + \pi_1 p_1, \quad p_0 = p_1 = p,$$
$$p = \frac{1}{2} \int\limits_{\overline{\Delta}(\tau)} [|f(\tau)|^2 + |f(\tau-\tau_0)|^2] \, d\tau. \quad (24)$$

Вероятность исхода в недоступной области для состояния ρ_0 при заданной априорной вероятности предъявления состояния есть

$$p_0 = \frac{\pi_0 p}{\pi_0 p + \pi_1 p} = \pi_0, \tag{25}$$

и, соответственно, для состояния ρ_1 с заданной априорной вероятностью π_1, есть

$$p_1 = \frac{\pi_1 p}{\pi_0 p + \pi_1 p} = \pi_1. \tag{26}$$

Вероятность ошибки, т. е. вероятность того, что состояние было идентифицировано участником B как ρ_0, а на самом деле было послано ρ_1 и наоборот, есть

$$P_e(\overline{\Delta}(\tau)) = \pi_0 p_1 + \pi_1 p_0. \tag{27}$$

Если в доступной области находится лишь одна из половинок состояний (носитель $f(\tau)$ или $f(\tau - \tau_0)$ находится в недоступной области) и, соответственно, одна из половинок находится в недоступной для измерений области, то вероятность ошибки при исходе в недоступной области, как следует из (24)–(27), есть $P_e(\overline{\Delta}(\tau)) = 1/2$.

В общем случае измерение, минимизирующее вероятность ошибки, дается при бинарной решающей функции разложением единицы вида

$$\begin{aligned}\tilde{E}_0 + \tilde{E}_1 = I(\Delta(\tau)) \otimes I_{\mathbf{C}^2} = \\ = I(\Delta(\tau)) \otimes (E_0 + E_1)\,,\end{aligned} \tag{28}$$

где, в отличие от [34, 36], разложение дается при ограничении на подпространство $\Delta(\tau)$. Минимальная вероятность ошибки находится минимизацией по всевозможным разложениям (см. подробности в [34, 36])

$$\begin{aligned}P_e(\Delta(\tau)) = \\ = \min_{\{\tilde{E}_0, \tilde{E}_1\}} \Big(\pi_0 \mathrm{Tr}\{\rho_0 \tilde{E}_1\} + \pi_1 \mathrm{Tr}\{\rho_1 \tilde{E}_0\}\Big)\,,\end{aligned} \tag{29}$$

где π_0 и π_1 — вероятности появления матриц плотности ρ_0 и ρ_1 соответственно (в нашей задаче $\pi_0 = \pi_1 = 1/2$ — вероятности приготовления 0 и 1).

С учетом (28) вероятность ошибки сводится к следующему:

$$P_e(\Delta(\tau)) = \pi_0 \mathrm{Tr}\{\rho(f) I(\Delta(\tau))\} + \mathrm{Tr}\{\Gamma \tilde{E}_0\}, \tag{30}$$

$$\Gamma = \pi_1 \rho_1 - \pi_0 \rho_0.$$

Нахождение минимума $P_e(\Delta(\tau))$ сводится к минимизации $\mathrm{Tr}\{\Gamma \tilde{E}_0\}$ по всевозможным операторам $\tilde{E}_0$.

Поскольку доступная для измерений область ограничена интервалом $\Delta(\tau)$, имеем

$$\begin{aligned}\mathrm{Tr}\{\Gamma \tilde{E}_0\} = \mathrm{Tr}_{\Delta(\tau)}\{\Gamma \tilde{E}_0\} = \\ = \mathrm{Tr}_{\Delta(\tau)}\{\rho(f)\} \mathrm{Tr}\{(\pi_1 \rho(1) - \pi_0 \rho(0)) E_0\} = \\ = \left\{ \frac{1}{2} \int\limits_{\Delta(\tau)} [|f(\tau)|^2 + |f(\tau - \tau_0)|^2]\, d\tau \right\} \mathrm{Tr}\{\Gamma E_0\}.\end{aligned} \tag{31}$$

Поскольку

$$0 \le E_0 \le I(\Delta(\tau)) \otimes I_{\mathbf{C}^2},$$

имеем

$$\mathrm{Tr}\{\Gamma E_0\} \ge \mathrm{Tr}\{\Gamma\} = \sum_i \gamma_i. \tag{32}$$

Минимальная ошибка определяется отрицательными собственными числами γ_i оператора

$$\Gamma = \pi_1 \rho(1) - \pi_0 \rho(0)$$

(см. [36]). Оператор $\tilde{E}_0$ должен удовлетворять условиям

$$\begin{aligned}\langle \gamma_i | \tilde{E}_0 | \gamma_i \rangle = 1, \quad \gamma_i \le 0, \\ \langle \gamma_i | \tilde{E}_0 | \gamma_i \rangle = 0, \quad \gamma_i \ge 0,\end{aligned} \tag{33}$$

где $|\gamma_i\rangle$ — собственные векторы оператора

$$\Gamma = \sum_i \gamma_i |\gamma_i\rangle \langle \gamma_i|.$$

Матрица оператора Γ в базисе $\{|e_0\rangle, |e_1\rangle\}$ имеет вид

$$\Gamma = \begin{pmatrix} \pi_1 & 0 \\ 0 & -\pi_0 \end{pmatrix},$$

ее единственное отрицательное собственное число есть

$$\gamma_2 = -\pi_0 = -1/2. \tag{34}$$

Соответственно, операторы $\tilde{E}_0$ и $\tilde{E}_1$ равны

$$\begin{aligned}\tilde{E}_0 = I(\Delta(\tau)) \otimes \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \\ \tilde{E}_1 = I(\Delta(\tau)) \otimes \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.\end{aligned} \tag{35}$$

Для минимальной ошибки получаем

$$P_e(\Delta(\tau)) = \overline{f^2(\Delta(\tau))} \left(\pi_0 + \sum_{\gamma_i \le 0} \gamma_i \right), \tag{36}$$

где введено обозначение

$$\overline{f^2(\Delta(\tau))} = \frac{1}{2} \int\limits_{\Delta(\tau)} \left[|f(\tau)|^2 + |f(\tau - \tau_0)|^2 \right] d\tau. \quad (37)$$

Окончательно для вероятности ошибки, когда исход имеет место в доступной для измерений области, имеем

$$P_e(\Delta(\tau)) = \overline{f^2(\Delta(\tau))}(\pi_0 - \pi_0) = \\ = \frac{1}{2}\left(\frac{1}{2} - \frac{1}{2}\right) = 0, \quad (38)$$

$$\overline{f^2(\Delta(\tau))} = \frac{1}{2}.$$

На интуитивном уровне данный результат может быть интерпретирован следующим образом. Допустим, что требуется различить пару однофотонных протяженных в пространстве состояний с разными (ортогональными) спиральностями. Вероятность различения равна единице лишь при доступе к состояниям целиком (соответственно, вероятность ошибки равна нулю). Несмотря на то что базисные векторы для различных значений спиральности ортогональны, из-за протяженности в пространстве состояния идентифицируются не достоверно, если они (их пространственная часть) не доступны целиком. Физически это связано с тем, что не существует состояния спиральности вне пространственных степеней свободы. Из-за нормировки по пространственным степеням свободы вероятность срабатывания измерительной установки у пользователя B при любом измерении не превосходит единицы. Достоверное различение состояний даже с разными (ортогональными) спиральностями требует принципиально конечного времени, так как из-за ограничения, накладываемого специальной теорией относительности, доступ к состоянию целиком не может быть получен быстрее, чем эффективная протяженность состояния, деленная на скорость света.

Полная ошибка при большом числе испытаний равна доле состояний из полного числа, которые идентифицируются неправильно. Доля (вероятность) исходов в доступной области равна

$$N(\Delta(\tau)) = \mathrm{Tr}\{(\pi_0\rho_0 + \pi_1\rho_1)(I(\Delta(\tau)) \otimes I_{\mathbf{C}^2})\}, \quad (39)$$

соответственно, доля исходов в недоступной области

$$N(\overline{\Delta}(\tau)) = \mathrm{Tr}\{(\pi_0\rho_0 + \pi_1\rho_1)(I(\overline{\Delta}(\tau)) \otimes I_{\mathbf{C}^2})\}. \quad (40)$$

Полная вероятность ошибки представляет собой сумму ошибки при исходе в недоступной области, умноженной на долю таких исходов, и произведения ошибки при исходе в доступной области на долю таких исходов. Имеем для вероятности полной ошибки

$$P_e = P_e(\overline{\Delta}(\tau))N(\overline{\Delta}(\tau)) + P_e(\Delta(\tau))N(\Delta(\tau)). \quad (41)$$

При доступе к половинкам состояний имеем

$$P_e = \frac{1}{2}\cdot\frac{1}{2} + 0\cdot\frac{1}{2} = \frac{1}{4}, \quad (42)$$

$$P_e(\overline{\Delta}(\tau)) = \frac{1}{2}, \quad N(\overline{\Delta}(\tau)) = \frac{1}{2},$$

$$P_e(\Delta(\tau)) = 0, \quad N(\Delta(\tau)) = \frac{1}{2}.$$

Соответственно, вероятность правильной идентификации составляет $3/4$.

Данный результат означает по сути следующее. Если участник A случайно и равновероятно приготавливает одно из состояний ρ_0 или ρ_1 и предъявляет для измерений участнику B, то с вероятностью $1/2$ измерительное устройство срабатывает в одном из каналов, отвечающих 0 или 1. Если измерительная установка у пользователя B сработала, то состояния идентифицируются однозначно. Однако если у участника B прибор не сработал, то ему остается только угадывать, что это за состояние. Вероятность того, что прибор не сработает, есть $1/2$; при этом вероятность правильного угадывания равна $1/2$. Для таких событий вероятность правильной идентификации

$$1/2 \cdot 1/2 = 1/4.$$

Полная вероятность правильного определения есть

$$1/2 + 1/4 = 3/4.$$

В этом случае вероятность $1 - P_e$ совпадает с вероятностью правильной идентификации секретного бита.

Такая вероятность правильной идентификации неприемлемо велика для построения протокола (существенно превышает $1/2$). Ситуация радикально меняется, если секретный бит представляет собой бит четности по N состояниям. Как мы увидим ниже, в этом случае вероятность правильной идентификации бита четности участником B лишь на экспоненциально малую величину превосходит $1/2$ (т. е. вероятность простого угадывания, которая является наихудшим вариантом).

Рассмотрим теперь вопрос о том, какова вероятность ошибки при различении 0 и 1, когда последние кодируются как бит четности, определяемый по

N ортогональным состояниям. Задача о бите четности по N состояниям, когда каждый бит кодируется одним из неортогональных состояний и пространство состояний доступно целиком, рассматривалась ранее в работе [37].

Вычислим сначала ошибку различения при исходах в доступной области. Если случайно выбирается строка из N битов, которой соответствует матрица плотности $\rho_{0,1}$ из 2^N возможных комбинаций (из них $2^N/2$ четные и $2^N/2$ нечетные), то задача сводится к различению двух матриц плотности для четных и нечетных строк:

$$\hat{\rho}_0 = \frac{2}{2^N} \sum_{(i_1 \oplus i_2 \oplus \ldots \oplus i_N)=0} \overbrace{\rho_{i_1} \otimes \rho_{i_2} \otimes \ldots \otimes \rho_{i_N}}^{N} = \\ = \frac{2}{2^N} \left(\rho(f) \otimes \rho(f) \otimes \ldots \otimes \rho(f)\right) \otimes \\ \otimes \sum_{(i_1 \oplus i_2 \oplus \ldots \oplus i_N)=0} \rho(i_1) \otimes \rho(i_2) \otimes \ldots \otimes \rho(i_N), \\ i_k = 0, 1, \quad k = 1, \ldots, N. \quad (43)$$

$$\hat{\rho}_1 = \frac{2}{2^N} \sum_{(i_1 \oplus i_2 \oplus \ldots \oplus i_N)=1} \overbrace{\rho_{i_1} \otimes \rho_{i_2} \otimes \ldots \otimes \rho_{i_N}}^{N} = \\ = \frac{2}{2^N} \left(\rho(f) \otimes \rho(f) \otimes \ldots \otimes \rho(f)\right) \otimes \\ \otimes \sum_{(i_1 \oplus i_2 \oplus \ldots \oplus i_N)=1} \rho(i_1) \otimes \rho(i_2) \otimes \ldots \otimes \rho(i_N), \\ i_k = 0, 1 \quad k = 1, \ldots, N. \quad (44)$$

Измерение, минимизирующее ошибку при различении матриц плотности $\hat{\rho}_0$ и $\hat{\rho}_1$, дается разложением единицы

$$\left(I(\Delta(\tau)) \otimes I_{\mathbf{C}^2}\right)^{\otimes^N} = \hat{\tilde{E}}_0 + \hat{\tilde{E}}_1 = \\ = I(\Delta(\tau))^{\otimes^N} \otimes \left(\hat{E}_0 + \hat{E}_1\right), \quad \hat{E}_0 + \hat{E}_1 = I_{\mathbf{C}^2}^{\otimes^N}. \quad (45)$$

Вероятность ошибки в этом случае

$$P_e(\Delta(\tau)) = \pi_0 \mathrm{Tr}\left\{\hat{\rho}_0 \left(I(\Delta(\tau))^{\otimes^N} \otimes I_{\mathbf{C}^2}^{\otimes^N}\right)\right\} + \\ + \mathrm{Tr}\left\{\hat{\Gamma}\left(I(\Delta(\tau))^{\otimes^N} \otimes \hat{E}_0\right)\right\}. \quad (46)$$

Соответственно, минимальная величина ошибки дается формулой, аналогичной (28), и определяется отрицательными собственными числами γ_i оператора

$$\hat{\Gamma} = \left(\overline{f^2(\Delta)}\right)^N \left(\pi_1 \hat{\rho}(1) - \pi_0 \hat{\rho}(0)\right) = \\ = \left(\overline{f^2(\Delta)}\right)^N \Gamma. \quad (47)$$

В базисе векторов, упорядоченных в четные и нечетные относительно суммы индексов множества, оператор Γ имеет вид

$$\Gamma = \frac{1}{2^N} \begin{pmatrix} 1 & 0 & 0 & \ldots \\ 0 & 1 & 0 & \ldots \\ . & . & . & \ldots \\ . & . & . & \ldots \\ 0 & \ldots & -1 & 0 \\ 0 & 0 & \ldots & -1 \end{pmatrix}, \quad (48)$$

$$\text{нечетные} \begin{cases} |e_0\rangle \ldots |e_1\rangle \\ \ldots \\ |e_1\rangle \ldots |e_0\rangle \end{cases} \\ \text{четные} \begin{cases} |e_0\rangle \ldots |e_0\rangle \\ \ldots \\ |e_1\rangle \ldots |e_1\rangle \end{cases}.$$

Окончательно, минимальная вероятность ошибки при определении результирующего бита четности по N ортогональным состояниям, недоступным целиком, равна ($\pi_0 = 1/2$)

$$P_e(\Delta(\tau)) = \\ = \left(\overline{f^2(\Delta)}\right)^N \left(\frac{1}{2} + \left(\frac{1}{2^N} \sum_{\gamma_i \le 0}^{2^N/2} (-1)\right)\right). \quad (49)$$

При доступе лишь к половине каждого состояния ($\overline{f^2(\Delta)} = 1/2$) имеем

$$P_e(\Delta(\tau)) = \left(\frac{1}{2}\right)^N \left(\frac{1}{2} - \frac{1}{2^N} \cdot \frac{2^N}{2}\right) = 0. \quad (50)$$

Вероятность ошибки (если исход имел место в доступной области) из-за ортогональности каналов равна 0. Данную формулу нужно понимать следующим образом. Если все N исходов имели место в доступной области, то вероятность ошибки из-за ортогональности состояний равна нулю. То же самое остается справедливым, если исход в доступной области имел место для m состояний (в этом случае в (47), (48) N надо заменить на m). Таким образом, если исходы от состояний имели место в доступной области, то эти состояния становятся достоверно известными.

Однако исходы могут иметь место также и в недоступной области.

По мере того как состояние за счет распространения в область, доступную для измерения, становится целиком доступным, $\overline{f^2(\Delta)} \to 1$, вероятность

ошибки $P_e \to 0$. Ортогональные состояния достоверно различимы при полном доступе к ним.

Займемся теперь подсчетом вероятности правильной идентификации бита четности. Полное число бинарных строк длиной N равно 2^N, причем возможны исходы как в доступной, так и в недоступной областях. Полное пространство событий состоит из двух элементов. Первый представляет собой событие, когда все N исходов имели место в доступной области. В этом случае вероятность правильной идентификации бита четности равна 1. Однако вероятность такого события, когда доступна половинка каждого состояния, равна

$$\overline{f^2(\Delta)}^N = 2^{-N}.$$

Второй элемент пространства событий представляет собой все остальные исходы (т. е. когда в доступной области было не более $N-1$ исходов). Вероятность всех таких исходов (когда для измерений доступна половинка каждого состояния) есть

$$\sum_{k=0}^{N-1} C_N^k \overline{f^2(\Delta)}^k (1-\overline{f^2(\Delta)})^{N-k} = \\ = \sum_{k=0}^{N-1} C_N^k \frac{1}{2^k}\,\frac{1}{2^{N-k}} = 1 - \overline{f^2(\Delta)}^N = 1 - 2^{-N}. \quad (51)$$

Для таких исходов вероятность ошибки при определении бита четности равна $1/2$. Действительно, в распоряжении у B есть строка длиной k ($k \le N-1$), четность которой достоверно известна. Однако четность оставшейся строки длиной $N-k$ (для исходов в недоступной области) может быть с вероятностью $1/2$ как четной, так и нечетной. Поэтому результирующая четность полной строки из N бит известна лишь с вероятностью $1/2$, поскольку знание части строки из k бит не влияет на вероятность знания четности полной строки.

Результирующая ошибка в определении четности равна сумме двух слагаемых. Первое относится к событию, когда все исходы имели место в доступной области, второе — для остальных событий. Каждое слагаемое есть произведение вероятности ошибки в определении бита четности на вероятность самого события. Окончательно имеем

$$P_e(parity) = \frac{1}{2}\left(1-2^{-N}\right) + 0\cdot 2^{-N} = \\ = \frac{1}{2} - \frac{1}{2}\cdot 2^{-N}. \quad (52)$$

Соответственно, вероятность правильной идентификации бита четности участником B, пока ему доступна половинка состояний, равна

$$P_c(parity) = 1 - P_e(parity) = \frac{1}{2} + \frac{1}{2}\cdot 2^{-N} \quad (53)$$

и превосходит вероятность простого угадывания лишь на экспоненциально малую величину.

Таким образом, в течение времени τ_0 ($\Delta\tau < \tau < \Delta\tau+\tau_0$) после начала протокола участник B имеет экспоненциально малую информацию о секретном бите.

Однако такая схема представления секретного бита как бита четности по N битам еще недостаточна для протокола, поскольку она дает неприемлемо большую вероятность обмана участником A (вероятность задержать выбор бита и остаться незамеченным).

Для того чтобы избежать этого, необходимо кодировать каждый из N битов блоком из k одинаковых бит (величина k будет определена ниже), которые посылаются вперемешку по Nk каналам.

Приведем, наконец, выражение для вероятности ошибки при различении матриц плотности, отвечающих 0 и 1, когда бит четности кодируется блоками длиной k, каждый из которых состоит либо из одних нулей, либо из одних единиц. В протоколе секретным битом, задуманным участником A, является бит четности по N штукам 0 и 1, причем каждый 0 и 1 представляется блоком по k штук. Такое представление блоком каждого бита будет нужно для контроля участником B отсутствия обмана со стороны участника A.

В этом случае полное число комбинаций бинарных строк есть 2^{Nk}. Число четных и нечетных среди них при кодировании 0 и 1 блоками по k штук есть

$$S_{odd,even} = \frac{1}{2}\sum_{m=0}^{N-1} C_{Nk}^{mk} = \\ = 2^{Nk}\left(\frac{1}{2k}\right)\sum_{l=1}^{k}\cos^{Nk}\left(\frac{l\pi}{k}\right)\cos\left(Nl\pi\right) \approx 2^{Nk}, \quad (54)$$

т. е. фактически равно полному числу способов разместить $(N-l)k$ единиц и lk нулей (при $0 \le l \le N$) по Nk ячейкам [35].

Обратим внимание на то, что если бы позиция каждого блока была фиксирована заранее (нули и единицы из разных блоков не перемешаны), то число возможных комбинаций четных и нечетных строк было бы лишь 2^N, что при больших k экспоненциально меньше, чем 2^{Nk} (см. (54)).

Остальные

$$N_{rest} = 2^{Nk} - S_{odd} - S_{even} \ll 2^{Nk}$$

комбинаций никакими разбиениями на блоки по k штук, каждый из которых содержит только либо 0, либо 1, не входят по определению ни в одно из множеств S_{odd} и S_{even}. Данное обстоятельство будет важно для протокола.

Оператор $\hat{\Gamma}$, аналогичный (48), в базисе, упорядоченном для четных и нечетных блоковых состояний, и остальных (для определенности считаем k четным)

$$S_{even} \to \begin{cases} \overbrace{|e_0\rangle \otimes |e_0\rangle \otimes \ldots \otimes |e_0\rangle}^{k} \otimes \overbrace{\ldots \ldots \ldots}^{k} \cdots \overbrace{\ldots \ldots \ldots}^{k} \otimes \overbrace{|e_0\rangle \otimes |e_0\rangle \otimes \ldots \otimes |e_0\rangle}^{k} \\ \text{другие комбинации } |e_0\rangle \text{ и } |e_1\rangle \text{ с четным} \\ \text{количеством } k\text{-блоков } \overbrace{|e_1\rangle \otimes |e_1\rangle \otimes \ldots \otimes |e_1\rangle}^{k} \\ \text{(всего } N \text{ блоков)} \\ \overbrace{|e_1\rangle \otimes |e_1\rangle \otimes \ldots \otimes |e_1\rangle \ldots}^{k} \otimes \overbrace{\ldots \ldots \ldots}^{k} \cdots \overbrace{\ldots \ldots \ldots}^{k} \otimes \overbrace{|e_1\rangle \otimes |e_1\rangle \otimes \ldots \otimes |e_1\rangle}^{k} \end{cases} \tag{55}$$

$$S_{odd} \to \begin{cases} \overbrace{|e_0\rangle \otimes |e_0\rangle \otimes \ldots \otimes |e_0\rangle}^{k} \otimes \overbrace{\ldots \ldots \ldots}^{k} \cdots \overbrace{\ldots \ldots \ldots}^{k} \otimes \overbrace{|e_1\rangle \otimes |e_1\rangle \otimes \ldots \otimes |e_1\rangle}^{k} \\ \text{другие комбинации } |e_0\rangle \text{ и } |e_1\rangle \text{ с нечетным} \\ \text{количеством } k\text{-блоков } \overbrace{|e_1\rangle \otimes |e_1\rangle \otimes \ldots \otimes |e_1\rangle}^{k} \\ \text{(всего } N \text{ блоков)} \\ \overbrace{|e_1\rangle \otimes |e_1\rangle \otimes \ldots \otimes |e_1\rangle \ldots}^{k} \otimes \overbrace{\ldots \ldots \ldots}^{k} \cdots \overbrace{\ldots \ldots \ldots}^{k} \otimes \overbrace{|e_0\rangle \otimes |e_0\rangle \otimes \ldots \otimes |e_0\rangle}^{k} \end{cases} \tag{56}$$

имеет вид

$$\hat{\Gamma} = \begin{pmatrix} \hat{I}_{S_{odd}} & 0 & 0 \\ 0 & -\hat{I}_{S_{even}} & 0 \\ 0 & 0 & \hat{0} \end{pmatrix}, \tag{57}$$

где $\hat{I}_{S_{odd}}$ ($\hat{I}_{S_{even}}$) — единичные матрицы размера $S_{odd} \times S_{odd}$ ($S_{even} \times S_{even}$), а $\hat{0}$ — нулевая матрица размера $N_{rest} \times N_{rest}$.

Измеряющие операторы $\hat{E}_0$ и $\hat{E}_1$ имеют в том же базисе вид

$$\hat{E}_0 = \begin{pmatrix} \hat{0} & 0 & 0 \\ 0 & \hat{I}_{S_{even}} & 0 \\ 0 & 0 & \hat{0} \end{pmatrix}, \quad \hat{E}_1 = \begin{pmatrix} \hat{I}_{S_{odd}} & 0 & 0 \\ 0 & \hat{0} & 0 \\ 0 & 0 & \hat{I} \end{pmatrix}. \tag{58}$$

Вероятность ошибки при различении блокового бита четности при Nk исходах в доступной области равна

$$P_e(\Delta(\tau)) = \left(\overline{f^2(\Delta)}\right)^{Nk} \times \left(\frac{1}{2} - \frac{1}{2^{(S_{even}+S_{odd})}} \sum_{\substack{i=1 \\ \gamma_i \le 0}}^{2^{S_{even}}} (-1)\right) = 0. \tag{59}$$

Ошибка равна нулю при любом числе состояний, измерения над которыми дали исход в доступной области.

Подсчитаем теперь ошибку при идентификации бита четности при блоковом представлении по k штук. Исходы могут иметь место как в доступной, так и в недоступной областях. Вычислим сначала минимально необходимое число исходов в доступной области, при котором четность строки идентифицируется с достоверностью. Прямой подсчет представляет достаточно трудоемкую задачу, поэтому для получения оценки удобно рассуждать следующим образом (фактически это рассуждение на языке шенноновских типичных последовательностей [38], см. также [39]). Вернемся на время к ситуации, ко-

гда каждый бит представляется блоком единичной длины $k = 1$. Мощность множества всех строк есть $\Omega = 2^N$, соответственно информация отдельного элемента множества (строки) есть $I = \log_2 |\Omega|$ и представляет собой (с точностью до округления) число двоичных символов, необходимых для индивидуализации элемента. Если каждый символ (в нашем случае срабатывание детектора в доступной области) возникает с вероятностью p, то вероятность идентификации элемента есть p^I.

При блоковом представлении мощность множества дается выражением (54) и требуемое число двоичных символов для индивидуализации есть

$$I = \log_2 \left(\frac{2^{Nk-1}}{k} \sum_{l=1}^{k} \cos^{Nk} \left(\frac{l\pi}{k} \right) \cos(Nl\pi) \right) = \\ = \alpha(N,k)(Nk), \quad (60)$$

что представляет собой число исходов в доступной области для определения четности строки.

Соответственно, вероятность такого события ($p = \overline{f^2(\Delta)} = 1/2$) равна

$$P_{acc} = p^{\alpha(N,k)(Nk)} = 2^{-\alpha(N,k)(Nk)}. \quad (61)$$

Для таких исходов ошибка равна нулю. Соответственно, вероятность для исходов в недоступной области

$$P_{unacc} = 1 - P_{acc} = 1 - 2^{-\alpha(N,k)(Nk)}; \quad (62)$$

вероятность ошибки при определении бита четности при этом равна

$$P_e(parity) = \frac{1}{2} \left(1 - 2^{-\alpha(N,k)(Nk)} \right) + \\ + 0 \cdot 2^{-\alpha(N,k)(Nk)}. \quad (63)$$

Соответственно, вероятность правильного определения бита четности лишь на экспоненциально малую величину превосходит вероятность простого угадывания:

$$P_c(parity) = 1 - P_e(parity) = \frac{1}{2} + 2^{-\alpha(N,k)(Nk)}. \quad (64)$$

Заметим, что число строк при блоковом представлении, когда нули и единицы из разных блоков перемешаны, по порядку величины равно полному числу строк ($\approx 2^{Nk}$) и каждая блоковая строка выглядит почти так же, как если бы длина блока k была равна 1. Поэтому для определения четности строки она требуется, с точностью до поправочного множителя $\alpha(N,k)$ (см. (60)), почти целиком.

Если бы позиция блоков была заранее фиксирована, то мощность множества была бы $2^N/2$ и требовалось бы N бинарных испытаний. Однако вероятность каждого такого испытания p равна сумме вероятностей иметь в каждом блоке 1 или 2, или ... k исходов в доступной области:

$$p = \sum_{l=1}^{k} C_k^l \frac{1}{2^l} \frac{1}{2^{(k-l)}} = 1 - 2^{-k}. \quad (65)$$

Соответственно, вероятность иметь N исходов (узнать четность при доступе к половинкам состояний для участника B)

$$P_{acc} = p^N = (1 - 2^{-k})^N \quad (66)$$

была бы высока (при сравнимых N и k).

Теперь остается показать, что после того как состояния становятся доступными для измерения целиком по истечении времени $\tau_0 + \Delta\tau \approx \tau_0$, вероятность обмана участником A стремится к нулю. Точнее говоря, требуется показать, что после начала протокола участник A уже не может переменить свое решение о задуманном секретном бите (изменить решение после начала протокола и остаться незамеченным с экспоненциально малой вероятностью 2^{-Nk}).

В протоколе Nk состояний посылаются одновременно вперемешку по Nk каналам. Детектирование отсутствия обмана со стороны участника A осуществляется при помощи измерения, которое описывается разложением единицы вида

$$I^{\otimes^{Nk}} \otimes I_{\mathbf{C}^2}^{\otimes^{Nk}} = (\mathcal{P}_0(f) + \mathcal{P}_1(f) + \mathcal{P}_\perp)^{\otimes^{Nk}}, \quad (67)$$

где

$$\mathcal{P}_{0,1}(f) = \left(\frac{1}{\sqrt{2}} \int_{-\infty}^{\infty} [f(\tau) + f(\tau - \tau_0)] |\tau\rangle \, d\tau \right) \times \\ \times \left(\frac{1}{\sqrt{2}} \int_{-\infty}^{\infty} [f^*(\tau') + f^*(\tau' - \tau_0)] \langle\tau'| \, d\tau' \right) \otimes \\ \otimes |e_{0,1}\rangle\langle e_{0,1}|, \quad (68)$$

$$\mathcal{P}_\perp = I \otimes I_{\mathbf{C}^2} - \mathcal{P}_0(f) - \mathcal{P}_1(f).$$

В каждом из Nk каналов измерений возможны три исхода, отвечающие $\mathcal{P}_0(f)$, $\mathcal{P}_1(f)$ и $\mathcal{P}_\perp(f)$. Если

участник A использует правильные состояния, то вероятность исходов

$$\begin{aligned}
&\Pr\{\rho_0,0\} = \mathrm{Tr}\{\rho_0\mathcal{P}_0(f)\} \equiv 1,\\
&\Pr\{\rho_1,1\} = \mathrm{Tr}\{\rho_1\mathcal{P}_1(f)\} \equiv 1,\\
&\Pr\{\rho_0,1\} = \mathrm{Tr}\{\rho_0\mathcal{P}_1(f)\} \equiv 0,\\
&\Pr\{\rho_1,0\} = \mathrm{Tr}\{\rho_1\mathcal{P}_0(f)\} \equiv 0,\\
&\Pr\{\rho_{0,1},\perp\} = \mathrm{Tr}\{\rho_{0,1}\mathcal{P}_\perp(f)\} \equiv 0,
\end{aligned} \tag{69}$$

т. е. если A использует правильные состояния, то все исходы с вероятностью 1 должны иметь место только в $\mathcal{P}_0(f)$, $\mathcal{P}_1(f)$.

Задержка решения участником A на время, превосходящее $2\Delta\tau$, означает, что он должен использовать состояния, которые не накрывают переднюю половинку правильного растянутого состояния, т. е. состояние начинает приготавливаться участником A после начала протокола по истечении времени, превосходящего $2\Delta\tau$. На всех таких состояниях ρ, носитель которых не накрывает переднюю половину правильного состояния, вероятность исхода в каналах $\mathcal{P}_0(f)$, $\mathcal{P}_1(f)$ не превышает $1/2$. Действительно,

$$\begin{aligned}
\mathrm{Tr}\{\rho\mathcal{P}_{0,1}(f)\} &= \\
&= \frac{1}{2}\int\limits_{-\Delta\tau}^{\Delta\tau}\int\limits_{-\Delta\tau}^{\Delta\tau} f(\tau)\rho(\tau,\tau')f^*(\tau')\,d\tau d\tau' + \\
&+ \frac{1}{2}\int\limits_{\tau_0-\Delta\tau}^{\tau_0+\Delta\tau}\int\limits_{\tau_0-\Delta\tau}^{\tau_0+\Delta\tau} f(\tau)\rho(\tau,\tau')f^*(\tau')\,d\tau d\tau' \le \\
&\le \frac{1}{2}\,\frac{1}{(2\Delta\tau)^2}\int\limits_{-\Delta\tau}^{\Delta\tau}\int\limits_{-\Delta\tau}^{\Delta\tau} |\rho(\tau,\tau')|\,d\tau d\tau' \le \frac{1}{2},\\
&\qquad |\rho(\tau,\tau')| \le 1,
\end{aligned} \tag{70}$$

если носитель

$$\rho = \int\limits_{-\infty}^{\infty}\int\limits_{-\infty}^{\infty} \rho(\tau,\tau')|\tau\rangle\langle\tau'|\,d\tau d\tau',$$

$$\mathrm{Tr}\{\rho\} = \int\limits_{-\infty}^{\infty}\int\limits_{-\infty}^{\infty} \delta_+(\tau-\tau')\rho(\tau,\tau')\,d\tau d\tau' = \int\limits_{-\infty}^{\infty} \rho(\tau,\tau)\,d\tau = 1,$$

не накрывает передней половинки правильного состояния,

$$\mathrm{supp}\rho(\tau,\tau') \cap \mathrm{supp}f(\tau-\tau_0) = \varnothing.$$

Таким образом, при идеальном канале связи любая задержка состояния приводит к тому, что вероятность исхода в $\mathcal{P}_0(f)$, $\mathcal{P}_1(f)$ не превышает $1/2$. Точнее говоря, в каждом отдельном эксперименте исход измерения даже на задержанных более чем на $2\Delta\tau$ состояниях может иметь место только в каналах $\mathcal{P}_0(f)$, $\mathcal{P}_1(f)$ и отсутствовать в канале $\mathcal{P}_\perp(f)$. Вероятность такого исхода есть $1/2$. Однако вероятность того, что в k экспериментах все исходы измерений на задержанных состояниях будут иметь место только в каналах $\mathcal{P}_0(f)$, $\mathcal{P}_1(f)$ и имитировать статистику для незадержанных состояний, составляет уже 2^{-k}. Далее это обстоятельство используется в протоколе.

Перейдем теперь к формулировке протокола.

3. ПРОТОКОЛ BIT COMMITMENT ДЛЯ СОСТОЯНИЙ С КОМПАКТНЫМ НОСИТЕЛЕМ В ИДЕАЛЬНОМ КАНАЛЕ СВЯЗИ

1. Участники перед протоколом оговаривают вид состояний (величину локализации $\Delta\tau$ и форму носителя состояния $f(\tau)$), а также время τ_0, в течение которого будет длиться протокол и A будет удерживать секретный бит. Последнее может быть выбрано сколь угодно большим (мы не обсуждаем при этом технические сложности). Оговариваются также N и k.

2. Участник A задумывает секретный бит, который является битом четности строки из N представителей

$$b = \sum_{i=1}^{N} a[i,j],$$

где $a[i,j]$ — бит 0 или 1, представитель из блока j (j — номер блока из k штук). Все биты в блоке (с одним номером j) одинаковые.

3. В момент начала протокола, который также оговаривается заранее, участник A начинает готовить Nk растянутых состояний из двух половинок, и по мере формирования они распространяются в Nk квантовых каналах связи. Состояния могут посылаться и по одному каналу последовательно, при этом время проведения протокола увеличивается. Длину канала с учетом сделанных выше оговорок считаем равной нулю. Последнее фактически означает, что B контролирует только свою лабораторию (окрестность точки x_B) и не контролирует остальное пространство и канал связи, т. е. A может располагаться прямо у порога лаборатории B. При этом A

может лишь контролировать окрестность точки x_A, где приготавливаются состояния. Состояния из разных блоков $a[i,j]$ посылаются по разным каналам вперемешку.

4. Время для стадии раскрытия участником B может быть выбрано любым из интервала $\Delta\tau < \tau < \tau_0 + \Delta\tau$. Участник A должен сообщить по запросу B через классический канал, какие состояния посылались в каждом квантовом канале и принадлежность каждого канала к определенному блоку, т. е. принадлежность каждого канала к блоку и значение его представителя $a[i,j]$.

5. Участник B проводит измерения, описывающиеся разложением единицы (67), (68). Состояния ортогональны (а значит, и достоверно различимы), но из-за нелокальности проекторов $\mathcal{P}_{0,1}$ для получения результата на правильных состояниях с достоверностью (67) необходим доступ ко всем состояниям целиком, что требует времени $2\Delta\tau + \tau_0$. Затем B сравнивает результаты своих измерений в каждом квантовом канале с тем, что сообщил ему A по классическому каналу. В случае идеальных квантовых каналов связи все измерения в каналах, относящихся к одному блоку, должны давать результат лишь в одинаковых каналах 0 или 1. Если хотя бы в одной позиции B обнаруживает несоответствие своих измерений с тем, что сообщил A, он обрывает протокол.

Заметим, что если A играет честно (в момент начала протокола посланы правильные растянутые состояния, т. е. четность строки из Nk битов действительно выбрана), то после этого уже никакими перегруппировками нельзя изменить четность. Противное означало бы, что множества четных и нечетных строк при таком блоковом представлении перекрываются.

6. Если A не принимает решение о выборе бита в начале протокола, точнее, если A принимает решение после времени $\Delta\tau$, но, естественно, до стадии обмена по классическому каналу ($\Delta\tau < \tau < \tau_0 + \Delta\tau$), то это означает, что он будет посылать состояния, отличные от $|\psi_{0,1}\rangle$. Отсчеты в каждом из каналов $\mathcal{P}_{0,1}$ на любых состояниях, отличных от правильных, будут происходит с вероятностью не более $1/2$. Для того чтобы изменить решение о секретном бите, участнику A достаточно задержать решение в одном из блоков, т. е. он должен задерживать состояния в целом блоке из k штук. Вероятность остаться незамеченным для A, если им посылаются k задержанных состояний, есть 2^{-k} (как следует из (70)).

7. Вероятность иметь достоверную информацию о секретном бите для участника B, до того как он получит доступ к состояниям целиком, не превосходит $1/2 + 2^{-\alpha(N,k)Nk}$ (см. (64)).

Таким образом, протокол позволяет реализовать исходную идею bit commitment, когда одним из участников предоставляется часть информации, по которой второй участник имеет до стадии раскрытия лишь экспоненциально малую информацию о секретном бите. В то же время участник A не может изменить задуманный секретный бит после начала протокола. Точнее говоря, вероятность недетектируемого изменения секретного бита после начала протокола экспоненциально мала.

Подобная схема позволяет реализовать честный протокол с вероятностью не хуже, чем $1 - 2^{-k}$, которая экспоненциально близка к единице при больших k.

4. ПРОТОКОЛ COIN TOSSING ДЛЯ СОСТОЯНИЙ С КОМПАКТНЫМ НОСИТЕЛЕМ В ИДЕАЛЬНОМ КАНАЛЕ СВЯЗИ

Хотя протокол подбрасывания монеты может быть построен на основе протокола bit commitment, имеет смысл сформулировать протокол явно.

1. Участники A и B договариваются о состояниях аналогично предыдущему протоколу. Каждый из них в момент начала протокола посылает навстречу другому вперемешку N блоков по k состояний, так что бит четности по N блокам у каждого участника представляет задуманный им бит (соответственно b_A и b_B). Заранее также оговаривается, кто их них выигрывает, если результирующий бит четности $b = b_A \oplus b_B$ равен нулю или единице.

2. В некоторый момент времени τ ($-\Delta\tau < \tau < \tau_0 + \Delta\tau$) один из участников, например A, сообщает по классическому каналу номера посылок и принадлежность каждой посылки к блоку, причем эта информация сообщается только для половины блоков от всех состояний. Затем B для другой половины номеров своих каналов, не совпадающих с номерами каналов, сообщенных A, сообщает аналогичную информацию только после получения таковой от A. Затем A, после получения информации от B, сообщает для оставшихся номеров каналов принадлежность к блокам и какое состояние посылалось в каждом из них. Затем B сообщает аналогичную информацию об оставшихся своих номерах каналов. Поскольку длина канала $\tau_{ch} < \tau_0$, обмен по классическому каналу может быть проведен в то время,

пока каждому из участников доступна лишь половина каждого состояния.

3. Пока состояния не доступны целиком, вероятность каждому из участников в результате своих измерений получить информацию о бите четности партнера аналогично предыдущему протоколу не превышает $1/2$.

4. Участники проводят измерения, описывающиеся разложением единицы (67), (68). Состояния ортогональны, но из-за нелокальности проекторов $\mathcal{P}_{0,1}$ для получения результата на правильных состояниях с достоверностью (69) необходим доступ ко всем состояниям целиком, что требует времени $2\Delta\tau + \tau_0$.

5. По истечении времени $\tau_0 + \Delta\tau$, когда состояния становятся целиком доступными обоим участникам, каждый из них проверяет статистику измерений и соответствие классической информации с тем, что получено в каждом канале у обоих участников. Протокол обрывается, если хотя бы в одном канале нет соответствия результатов измерений с классической информацией (когда обнаружен сбой 0 на 1 и наоборот).

6. Вероятность каждому из участников узнать бит четности другого до момента, пока состояния не станут целиком доступны, превосходит вероятность простого угадывания не более, чем на экспоненциально малую величину — $2^{-\alpha(N,k)Nk}$ (аналогично предыдущему протоколу). В итоге возникает честный бит четности (жребий) $b = b_A \oplus b_B$ с с вероятностью, экспоненциально близкой к единице $(1 - 2^{-k})$.

Разумеется, один из участников, даже если оба посылают правильные состояния, может оборвать протокол при невыигрышном для него результирующем бите, ссылаясь на то, что у него нет соответствия информации, полученной по классическому каналу и в квантовых измерениях. Такая ситуация уже не относится собственно к рассматриваемой задаче и должна разрешаться другими средствами.

Заметим, что передача информации по классическому каналу участниками необходима для того, чтобы избежать стратегии обмана, связанной с переносылом назад квантовых состояний партнера. Например, один из участников вообще может не посылать свои состояния, а «отражать» назад состояния партнера. В этом случае участник, который выигрывает, если суммарный бит четности равен

$$b = b_A \oplus b_B = 0,$$

может таким способом обманывать в свою пользу, поскольку при этом $b_A \equiv b_B$ и $b = 0$.

Сообщение каждым из участников по классическому каналу информации только о половине состояний требуется также для того, чтобы избежать стратегии с перепосылом. Если одним из участников сообщается информация сразу о всех состояниях, то второй участник, который использует стратегию перепосыла для квантовых состояний, может также перепослать эту информацию назад по классическому каналу (разумеется, предварительно узнав ее) назад к другому участнику по классическому каналу, поскольку $\tau_{ch} < \tau_0$. Когда последовательно сообщается информация о половине состояний, такая стратегия не срабатывает.

5. ПРОТОКОЛ BIT COMMITMENT ДЛЯ СОСТОЯНИЙ С НЕЛОКАЛИЗОВАННЫМ НОСИТЕЛЕМ В ИДЕАЛЬНОМ КАНАЛЕ СВЯЗИ

Пока мы рассматривали протокол для состояний с компактным носителем (функции $f(\tau) \in \mathcal{D}(\tau)$). Такие функции образуют плотное множество в пространстве функций, описывающих состояние свободного поля (функции $f(\tau) \in \mathcal{J}(\tau)$ нигде не обращаются в нуль). Однако в теории поля не запрещаются состояния, заданные на массовой поверхности, сколь угодно сильно локализованные и убывающие сколь угодно близко к экспоненциальной зависимости, например (14). Поэтому всегда можно выбрать состояния так, чтобы измерения над ними в конечной области на световом конусе τ давали вероятность исхода, сколь угодно близкую к единице, т. е. чтобы вклад от хвостов состояний на бесконечности был сколь угодно мал. Точнее говоря, состояния (функции $f(\tau)$) и область измерения могут быть выбраны такими, чтобы вероятность результата в области $\Delta(\tau)$ была равна

$$\Pr\{\Delta(\tau); i, i\} = \mathrm{Tr}\left\{\left(\left(\int\limits_{-\Delta\tau}^{\Delta\tau} \mathcal{M}(d\tau)\right) \otimes \mathcal{P}_i\right) \times \right.$$

$$\left. \times\ |\psi_i\rangle\langle\psi_i|\right\} = \int\limits_{-\Delta\tau}^{\Delta\tau} |f(\tau)|^2\, d\tau = 1 - e^{-\xi} \to 1, \quad (71)$$

$$|\psi_i\rangle = \int\limits_{-\infty}^{\infty} f(\tau)|\tau\rangle\, d\tau \otimes |e_i\rangle, \quad f(\tau) \in \mathcal{J}(\tau), \quad i = 0, 1,$$

где ξ может быть сколь угодно велико. Вклад от хвостов состояния вне области $(-\Delta\tau, \Delta\tau)$ равен

$$e^{-\xi} = \int\limits_{|\tau|>\Delta\tau} |f(\tau)|^2 d\tau = \\ = \mathrm{Tr}\left\{\left(\left(\int\limits_{|\tau|>\Delta\tau} \mathcal{M}(d\tau)\right)\otimes\mathcal{P}_i\right)|\psi_i\rangle\langle\psi_i|\right\}. \quad (72)$$

Для сохранения аналогии со случаем состояний с компактным носителем будем записывать растянутые состояния с некомпактным носителем в виде

$$|\psi_{0,1}\rangle = \frac{1}{\sqrt{2}}\int\limits_{-\infty}^{\infty}[f(\tau)+f(\tau-\tau_0)]|\tau\rangle\, d\tau\otimes|e_{0,1}\rangle, \\ f(\tau)\in\mathcal{J}(\tau), \quad (73)$$

где носитель $f(\tau)$ ($f(\tau-\tau_0)$), как и ранее для одногорбого состояния (13), сильно локализован в интервале $(-\Delta\tau, \Delta\tau)$ (или $(-\Delta\tau+\tau_0, \Delta\tau+\tau_0)$). Условие нормировки дает

$$\frac{1}{2}\int\limits_{-\Delta\tau}^{\Delta\tau}|f(\tau)|^2 d\tau = \frac{1}{2}\int\limits_{-\Delta\tau+\tau_0}^{\Delta\tau+\tau_0}|f(\tau-\tau_0)|^2 d\tau = \\ = \frac{1}{2}-\frac{1}{2}e^{-\xi}\to\frac{1}{2} \quad (74)$$

и

$$\frac{1}{2}\int\limits_{\tau>|\Delta\tau|}|f(\tau)|^2 d\tau + \frac{1}{2}\int\limits_{\tau+\tau_0>|\Delta\tau|}|f(\tau-\tau_0)|^2 d\tau + \\ +\frac{1}{2}\int\limits_{-\infty}^{\infty}[f^*(\tau)f(\tau-\tau_0)+f(\tau)f^*(\tau-\tau_0)]\,d\tau = e^{-\xi}. \quad (75)$$

Измерения над растянутым состоянием в конечном окне $\Delta(\tau_0) = (-\Delta\tau, \tau_0+\Delta\tau)$ дают результат с вероятностью

$$\Pr\{\Delta(\tau_0); i, i\} = \\ = \mathrm{Tr}\left\{\left(\left(\int\limits_{-\Delta\tau}^{\Delta\tau+\tau_0}\mathcal{M}(d\tau)\right)\otimes\mathcal{P}_{0,1}\right)|\psi_{0,1}\rangle\langle\psi_{0,1}|\right\} = \\ = 1-O(e^{-\xi}). \quad (76)$$

Последнее слагаемое возникает за счет перекрытия хвостов от половинок состояния, центрированных в $\tau=0$ и $\tau=\tau_0$, и не превышает $O(e^{-\xi})$.

Таким образом, статистика измерений на растянутых состояниях должна давать результаты в интервале $(-\Delta\tau, \Delta\tau+\tau_0)$ с вероятностью $1-O(e^{-\xi})\to 1$, экспоненциально близкой к единице. Вне этого интервала вероятность отсчетов не превышает $O(e^{-\xi})$ и может быть сделана (путем выбора $f(\tau)$, $\Delta\tau$ и τ_0) сколь угодно малой.

Для приготовления делокализованного состояния с $f(\tau)\in\mathcal{J}(\tau)$ требуется формально бесконечное время (если, например, состояние испускается точечным источником), либо необходим доступ ко всему координатному пространству (если состояние готовится в данный момент времени нелокальным источником). Любой реальный протокол может длиться лишь конечное время. Для того чтобы избежать подобных формальных трудностей, удобно рассуждать (как это обычно делается) следующим образом. Участник A контролирует окрестность точки x_A и адиабатически (при $t\to-\infty$) включает источник, который порождает из вакуумного состояния вектор $|\psi_{0,1}(\tau_0)\rangle$. Действие источника описывается действием $\hat{S}(\tau,-\infty)$-матрицы на вакуумное состояние (пока мы оставляем в стороне вопрос о конкретной реализации такого источника):

$$|\psi_{0,1}(\tau)\rangle = \hat{S}(\tau,-\infty)|0\rangle = \\ = \int\limits_{-\infty}^{\tau}[f(\tau')+f(\tau'-\tau_0)]|\tau'\rangle)\,d\tau'\otimes|e_{0,1}\rangle, \quad (77)$$

которое по мере формирования направляется в канал связи.

На интуитивном уровне такой источник можно представлять как атомную систему (например, атом) с подходящим спектром, который возбуждается классическим источником специальной формы, включаемым адиабатически, и высвечивается в канал связи (по поводу приготовления нестандартных одно- и двухфотонных состояний см., например, [40]).

Пользователь B осуществляет измерение, которое описывается разложением единицы, аналогичным (67):

$$\mathcal{P}_0(\Delta)+\mathcal{P}_1(\Delta)+\mathcal{P}_\perp(\Delta) = I\otimes I_{\mathbf{C}^2}, \\ I = \int\limits_{-\infty}^{\infty}|\tau\rangle\langle\tau|\,d\tau, \quad (78)$$

$$\mathcal{P}_{0,1}(\Delta) = \left(\frac{1}{\sqrt{2}}\int\limits_{-\Delta\tau}^{\Delta\tau+\tau_0}[f(\tau)+f(\tau-\tau_0)]|\tau\rangle\,d\tau\right)\times$$
$$\times\left(\frac{1}{\sqrt{2}}\int\limits_{-\Delta\tau}^{\Delta\tau+\tau_0}[f(\tau')+f(\tau'-\tau_0)]\langle\tau'|\,d\tau'\right)\otimes$$
$$\otimes|e_{0,1}\rangle\langle e_{0,1}|, \quad (79)$$

и далее

$$\mathcal{P}_\perp(\Delta) = I - \mathcal{P}_0(\Delta) - \mathcal{P}_1(\Delta). \quad (80)$$

На правильных растянутых состояниях измерение (78)–(80) дает результат с вероятностями

$$\begin{aligned}&\mathrm{Tr}\{\rho_{0,1}\mathcal{P}_{0,1}(\Delta)\} = 1 - O(e^{-\xi}),\\ &\mathrm{Tr}\{\rho_{0,1}\mathcal{P}_\perp(\Delta)\} = O(e^{-\xi}).\end{aligned} \quad (81)$$

Аналогично предыдущему (67), (68), измерение (78)–(80) на любых состояниях ρ, не сосредоточенных сразу в обоих интервалах $(-\Delta\tau,\Delta\tau)$ и $(-\Delta\tau+\tau_0,\Delta\tau+\tau_0)$, дает

$$\begin{aligned}&\int\limits_{-\Delta\tau}^{\Delta\tau}\int\limits_{-\Delta\tau}^{\Delta\tau}\delta_+(\tau-\tau')\rho(\tau,\tau')\,d\tau d\tau' = \frac{1}{2} - \frac{1}{2}e^{-\xi},\\ &\int\limits_{-\Delta\tau+\tau_0}^{\Delta\tau+\tau_0}\int\limits_{-\Delta\tau+\tau_0}^{\Delta\tau+\tau_0}\delta_+(\tau-\tau')\rho(\tau,\tau')\,d\tau d\tau' =\\ &\qquad = \frac{1}{2} - \frac{1}{2}e^{-\xi}.\end{aligned} \quad (82)$$

То есть задержка состояний по времени более чем на $2\Delta\tau$ будет приводить к тому, что вероятность исхода на таких состояниях в канале $\mathcal{P}_{0,1}$ падает от почти единицы (81) до почти $1/2$ (82):

$$\mathrm{Tr}\{\rho\mathcal{P}_{0,1}\} = \frac{1}{2} - \frac{1}{2}e^{-\xi} \quad (83)$$

и, соответственно, в канале $\mathcal{P}_\perp$ вероятность возрастает почти с нуля (79) до почти $1/2$ (82):

$$\mathrm{Tr}\{\rho\mathcal{P}_\perp\} = \frac{1}{2} - \frac{1}{2}e^{-\xi}. \quad (84)$$

Пользователь A, как и в предыдущем случае, готовит Nk состояний и направляет их в каналы связи. Вероятность для B получить информацию о секретном бите четности, задуманном A, пока доступна только «половина» состояний ($\Delta\tau \le \tau \le \Delta\tau+\tau_0$), не превышает

$$P_c(parity) \approx \frac{1}{2} + \left(\frac{1}{2} - O(e^{-\xi})\right)^{\alpha(N,k)Nk}. \quad (85)$$

Вероятность задержать решение хотя бы в одном из блоков по k штук участником A и остаться незамеченным не превышает

$$\left(\frac{1}{2} - O(e^{-\xi})\right)^k. \quad (86)$$

Вероятность успешного завершения протокола (все Nk состояний дают результат в каналах $\mathcal{P}_{0,1}$) есть

$$\left(1 - O(e^{-\xi})\right)^{\alpha(N,k)Nk} \quad (87)$$

и выбором N, k и ξ может быть сделана сколь угодно близкой к единице.

6. ЗАКЛЮЧЕНИЕ

Таким образом, существование предельной скорости распространения квантовых состояний позволяет сконструировать релятивистские квантовые протоколы bit commitment и coin tossing, причем в явном виде удается провести исходную идею протокола, когда один из участников предоставляет только часть информации (часть квантового состояния) о секретном бите. Однако статистическая природа результатов измерений над квантовыми состояниями не позволяет реализовать (по крайней мере для обсуждаемого нами протокола) честный протокол с вероятностью единица. Тем не менее, возможен честный протокол с вероятностью, сколь угодно близкой к единице. Кроме того, принципиальная нелокализуемость состояний квантованного поля также накладывает ограничения на вероятность честного исхода протокола в течение конечного времени. Однако возможность существования в теории поля сколь угодно сильно локализованных состояний позволяет для произвольного времени τ_0 (времени хранения секретного бита) построить честный протокол с любой наперед заданной вероятностью, сколь угодно близкой к единице.

В отличие от нерелятивистских протоколов, где существенна только структура состояний в гильбертовом пространстве, в рассматриваемых релятивистских протоколах явно присутствуют стадии приготовления и распространения состояний в пространстве-времени между пространственно-удаленными пользователями. Поскольку в природе не существует состояний спина и спиральности вне пространственных степеней свободы квантовой системы, учет пространственных степеней свободы расширяет возможности для конструирования квантовых криптографических протоколов.

Обратим еще раз внимание на то, что в протоколе используются ортогональные состояния. Вероятность ошибки для ортогональных состояний при их различении возникает из-за того, что измерение над состоянием может вообще не дать никакого результата (не будет срабатывания классического прибора, отклонения «стрелки»), если состояние не присутствует в пространственно-временной области, где находится прибор. Поэтому при измерении существуют три исхода: классический измерительный прибор сработал в одном из каналов $\mathcal{P}_0$ или $\mathcal{P}_1$, или не сработал вообще. В случае срабатывания прибора состояния различаются однозначно. Если доступна лишь часть состояния, то существует ненулевая вероятность того, что прибор не сработает вообще, и эта вероятность тем ближе к единице, чем меньшая часть состояния доступна для измерения. В этом случае остается только угадывать, что это за состояние (соответственно, вероятность ошибки для такого исхода измерения классического прибора равна $1/2$).

Поскольку не существует спина или спиральности вне пространственных степеней свободы, ограничение доступа к координатному пространству автоматически ограничивает доступ к гильбертову пространству состояний. Возможна даже такая ситуация, когда состояние системы вообще недоступно (амплитуда состояния равна нулю в пространственной области, доступной для измерения).

Отметим, что данная ситуация отличается от ситуации, обсуждаемой в [41] в связи разъяснением работы [18] по квантовой криптографии на ортогональных состояниях. Для пары ортогональных состояний композитной системы из двух подсистем a и b с пространством состояний $\mathcal{H}_a \otimes \mathcal{H}_b$ имеем

$$|\psi_0\rangle = \alpha_0|\phi_0(a)\rangle \otimes |\phi_0(b)\rangle + \beta_0|\phi_1(a)\rangle \otimes |\phi_1(b)\rangle,$$

$$|\psi_1\rangle = \alpha_1|\phi_0(a)\rangle \otimes |\phi_0(b)\rangle + \beta_1|\phi_1(a)\rangle \otimes |\phi_1(b)\rangle,$$

где коэффициенты $\alpha_{0,1}$ и $\beta_{0,1}$ таковы, что состояния $|\psi_0\rangle$ и $|\psi_1\rangle$ ортогональны,

$$\langle\psi_0|\psi_1\rangle = 0.$$

Если имеется доступ только к одной подсистеме, например $\mathcal{H}_a$, то состояния другой подсистемы b неортогональны:

$$\rho_1 = \mathrm{Tr}_{\mathcal{H}_a}\{|\psi_1\rangle\langle\psi_1|\}, \quad \rho_0 = \mathrm{Tr}_{\mathcal{H}_a}\{|\psi_0\rangle\langle\psi_0|\},$$

$$\mathrm{Tr}_{\mathcal{H}_b}\{\rho_0\rho_1\} \neq 0,$$

и, значит, достоверно не различимы. В нашем случае состояния остаются ортогональными даже при ограничении на подпространство и неразличимость возникает только благодаря пространственно-временной структуре состояний.

Протокол может быть обобщен для канала с шумом [42], поскольку исходная ортогональность состояний позволяет использовать классические коды [43].

В данной схеме время протокола ($\approx \tau_0$) определяется эффективной протяженностью состояний, которая для фотонов может быть оценена из ширины частотного спектра. Достижимая на сегодняшний день минимальная ширина спектра в оптическом диапазоне в кольцевых оптоволоконных резонаторах составляет $\Delta\omega \approx 10$ кГц. Эффективная длина состояния

$$L \approx c/\Delta\omega = 3 \cdot 10^{10}/10^4 \text{ см} = 3 \cdot 10^6 \text{ см} \quad (30 \text{ км}).$$

Соответственно, время

$$\tau_0 \approx 1/\Delta\omega \approx 10^{-3} \text{ с}.$$

Хотя никаких фундаментальных ограничений на то, чтобы сделать время τ_0 сколь угодно большим (соответственно, $\Delta\omega$ сколь угодно малым) не существует, технически данная задача является очень сложной. Однако это обстоятельство несущественно для протокола coin tossing, поскольку время для получения честного жребия τ_0 может быть любым. Для протокола bit commitment величина времени τ_0 существенна, поскольку она определяет время, в течение которого может сохраняться секретный бит. Такая ситуация является достаточно общей при экспериментальной реализации различных систем для передачи и обработки «квантовой информации», когда принципиальные возможности разрешены законами квантовой механики, однако реализовать их технически на сегодняшний день очень сложно.

Отметим также, что для передач на большие расстояния реально используются оптоволоконные системы, в которых скорость распространения несколько меньше скорости света в вакууме. Данное обстоятельство не является ограничительным, лишь бы время раздвижки «половинок» состояний было больше, чем длина канала, деленная на скорость света в оптоволокне.

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (грант №99-02-18127), а также поддержана проектом «Физические основы квантового компьютера» и программой «Перспективные технологии и устройства микро- и наноэлектроники» (грант №02.04.5.2.40.Т.50).

ЛИТЕРАТУРА

1. L. Landau and R. Peierls, Z. Phys. **69**, 56 (1931); Л. Д. Ландау, *Собрание научных трудов*, Наука, Москва (1969), т. 1.

2. N. Bohr and L. Rosenfeld, Math.-Fys. Medd. **12**, 3 (1933); Н. Бор, *Собрание научных трудов*, Наука, Москва (1971), т. 1.

3. В. Б. Берестецкий, Е. М. Лифшиц, Л. П. Питаевский, *Квантовая электродинамика*, Наука, Москва (1982).

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. S. Wiesner, SIGACT News **15**, 78 (1983).

7. C. H. Bennett and G. Brassard, in *Proc. IEEE Int. Conf. on Computers, Systems, and Signal Processing*, IEEE, New York (1984), p. 175.

8. A. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

9. G. Brassard, C. Crépeau, R. Jozsa, and D. Langlois, in *Proc. 34th Annual IEEE Symp. on the Foundation of Computer Science*, IEEE Cmp. Soc. Press, Los Alamitos, California (1993), p. 362.

10. G. Brassard and C. Crépeau, *Advances in Cryptology: Proc. of Crypto'90, Lecture Notes in Computer Science*, Springer-Verlag, Berlin (1991), vol. 537, p. 49.

11. M. Ardehali, E-print archives quant-ph/9603015.

12. D. Mayers, L. Salvail, and Y. Chiba-Kohno, E-print archives quant-ph/9904078.

13. M. Blum, Coin Flipping by Telephone: a Pritocol for Solving Impossible Problems, in *Proc. 24th IEEE Comp. Conf.* (1982), p. 133; in: SIGACT News **15**, 23 (1983).

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

15. А. Ю. Китаев, УМН **52**, 54 (1997).

16. H.-K. Lo and H. F. Chau, Phys. Rev. Lett. **78**, 3410 (1997).

17. D. Mayers, Phys. Rev. Lett. **78**, 3414 (1997).

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

19. A. Peres, E-print archives quant-ph/9509003.

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

21. S. N. Molotkov and S. S. Nazin, E-print archives quant-ph/0008008.

22. R. Laiho, S. N. Molotkov, and S. S. Nazin, E-print archives quant-ph/00006010.

23. R. Laiho, S. N. Molotkov, and S. S. Nazin, E-print archives quant-ph/0005067; quant-ph/0005068; Phys. Lett. A **275**, 37 (2000).

24. A. Kent, E-print archives quant-ph/9810067; quant-ph/9810068; quant-ph/9906103; Phys. Rev. Lett. **83**, 1447 (1999).

25. S. N. Molotkov and S. S. Nazin, E-print archives quant-ph/9911055; quant-ph/9910034; ЖЭТФ **117**, 818 (2000); Письма в ЖЭТФ **70**, 684 (1999).

26. Ю. А. Брычков, А. П. Прудников, *Интегральные преобразования обобщенных функций*, Наука, Москва (1977).

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

28. Н. Н. Мейман, ЖЭТФ **47**, 1966 (1964).

29. Д. А. Киржниц, УФН **90**, 129 (1966).

30. A. M. Jaffe, Phys. Rev. **158**, 1454 (1967).

31. Н. Н. Боголюбов, А. А. Логунов, И. Т. Тодоров, *Основы аксиоматического подхода в квантовой теории поля*, Наука, Москва (1969).

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

33. Н. Винер, Р. Пэли, *Преобразование Фурье в комплексной области*, Наука, Москва (1964) [N. Wiener and R. Paley, *Fourier Transform in the Complex Domain*, American Mathematical Sociaty, New York (1934)].

34. C. W. Helstrom, Information and Control **10**, 254 (1967); К. Хелстром, *Квантовая теория проверки гипотез и оценивания*, Мир, Москва (1979) [C. W. Helstrom, *Quantum Detection and Estimation Theory*, Mathematics in Science and Engineering, vol. 123, Academic Press (1976)].

35. А. П. Прудников, Ю. А. Брычков, О. А. Маричев, *Интегралы и ряды. Элементарные функции*, Наука, Москва (1981).

36. C. A. Fuchs, E-print archives quant-ph/9601020.

37. C. H. Bennett, Tal Mor, and J. Smolin, Phys. Rev. A **54**, 2675 (1996); Tal Mor, E-print archives quant-ph/9906073.

38. C. E. Shannon, Bell Syst. Tech. J. **27**, 397, 623 (1948).

39. I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, Akademiai, Kiado–Budapest (1981).

40. С. Н. Молотков, С. С. Назин, Письма в ЖЭТФ **63**, 646 (1996); А. В. Крашенинников, С. Н. Молотков, С. С. Назин, Л. А. Опенов, ЖЭТФ **110**, 1257 (1997); K. M. Gheri, C. Saavedra, P. Törmä, J. I. Cirac, and P. Zoller, Phys. Rev. A **58**, R2627 (1998).

41. Tal Mor, Phys. Rev. Lett. **80**, 3137 (1998).

42. С. Н. Молотков, С. С. Назин, Письма в ЖЭТФ **73**, 107 (2001).

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