Письма в ЖЭТФ, том 70, вып.10, стр.684 - 689 © 1999г. 25 ноября

РЕЛЯТИВИСТСКОЕ КВАНТОВОЕ ПОДБРАСЫВАНИЕ МОНЕТЫ

С.Н.Молотков и С.С.Назин

Институт физики твердого тела РАН

142432 Черноголовка, Московская обл., Россия

Поступила в редакцию 28 сентября 1999 г.

Предлагается релятивистский квантовый протокол обмена, позволяющий реализовать "подбрасывание монеты на расстоянии" между двумя участниками. Протокол обмена основан на том обстоятельстве, что в релятивистской квантовой механике достоверное различение пары ортогональных состояний требует конечного времени, зависящего от структуры самих состояний.

PACS: 03.65.Bz, 03.67.-a, 42.50.Dv

Протокол подбрасывания монеты относится к одному из простейших криптографических протоколов и сводится к следующему. Допустим, что два участника A и B, не доверяющих друг другу хотят бросить жребий, например, при помощи монеты или генератора случайных чисел, который равновероятно выбрасывает 0 или 1. Если выпадает 0, то выигрывает A, если 1 – B. В случае, когда A и B находятся в одном месте, задача тривиальна, если же A и B пространственно удалены и могут общаться лишь по каналу связи, то задача может даже казаться неразрешимой, поскольку A и B всегда могут обманывать партнера в свою пользу. Когда A и B могут обмениваться информацией лишь по классическому каналу связи, для этого случая задача была решена Блюмом [1]. В строгом смысле протокол [1] не является секретным относительно обмана одним из участников, поскольку основан на недоказанной вычислительной сложности вычисления дискретного логарифма [1]. Например, если бы один из участников имел у себя в распоряжении квантовый компьютер (пока, правда, не реализованный экспериментально), то он всегда бы имел возможность выигрывать за счет быстрого вычисления дискретого логарифма [2,3].

Если кроме классического канала связи между A и B имеется еще и квантовый канал связи, то возможны различные квантовые протоколы обмена, секретность которых основана не на вычислительной сложности, а на фундаментальных законах природы (квантовой механики). Были предложены и исследованы протоколы распространения секретного ключа – квантовая криптография (quantum key distribution) [4–6], квантовый протокол "привязки" к биту (quantum bit commitment) [7–9], квантового подбрасывания монеты (quantum coin tossing) [10], квантовой рулетки (quantum gambling) [11] и квантового разделения секрета (quantum secret sharing) [12]. Ранее было показано, что идеальное квантовое подбрасывание монеты в рамках нерелятивистской квантовой механики невозможно [13,14]. Под идеальным понимается такой протокол, в результате которого вероятность принятия обоими участниками того, что не было обмана, равно строго единице, и вероятность выпадения 0 или 1 равна 1/2. Возможен, однако, протокол, когда вероятность честного жребия принимается обоими участниками с вероятностью, сколь угодно близкой к единице [10].

Недавно был предложен протокол привязки к биту (bit commitment) и протокол подбрасывания монеты, учитывающие наличие предельной скорости распространения сигнала [15]. Носителями информации в этой схеме являются классические

состояния. Протоколы основаны на том, что участники A и B имеют по два пространственно удаленных и контролируемых ими узла (см. детали в [15]).

Ниже будет приведен пример релятивистского квантового протокола подбрасывания монеты в реальном времени.

Все квантовые криптографические протоколы в том или ином виде используют два обстоятельства. No cloning-теорема [16] – невозможность копирования неизвестного квантового состояния, то есть невозможность 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 – унитарный оператор. Такой процесс запрещен в силу линейности и унитарной эволюции в квантовой механике. Невозможен даже более слабый процесс – невозможность получения информации об одном из пары неортогональных состояний без их возмущения [17]:

$$|A\rangle|\psi_1\rangle \to U(|A\rangle|\psi_1\rangle) = |A_{\psi_1}\rangle|\psi_1\rangle, \quad |A\rangle|\psi_2\rangle \to U(|A\rangle|\psi_2\rangle) = |A_{\psi_2}\rangle|\psi_2\rangle,$$

Невозможность того, чтобы было $|A_{\psi_1}\rangle \neq |A_{\psi_2}\rangle$, если $\langle\psi_1|\psi_2\rangle \neq 0$, то есть невозможности достоверного различения неортогональных состояний. Для ортогональных состояний такого запрета не существует. Поэтому почти все криптографические протоколы используют в качестве носителей информации неортогональные состояния. Исключение составляет протокол, предложенный в работе [18].

Ортогональные состояния различимы с достоверностью, причем в рамках нерелятивистской квантовомеханической теории измерений различение двух ортогональных состояний может быть сделано мгновенно. По сути по этим причинам невозможно построить криптографические протоколы на ортогональных состояниях в рамках нерелятивистской квантовой механики.

В релятивистской квантовой теории поля ситуация иная. Физические наблюдаемые поля, относящиеся к точкам, разделенным пространственно-подобным интервалом, не могут быть связаны причинно-следственной связью, а коммутатор операторов поля обращается в нуль вне светового конуса [19]

$$[u^-(\hat{x}_1), u^+(\hat{x}_2)]_\pm = -iD^-(\hat{x}_1 - \hat{x}_2), \tag{1}$$

где $u^\pm(\hat{x})$ – операторы поля, $\hat{x}_{1,2}$ – точки четырехмерного пространства-времени, $D^-(\hat{x}_1 - \hat{x}_2)$ – отрицательно-частотная коммутаторная функция [19]. Последнее обстоятельство накладывает ограничение на время, необходимое для достоверного (за один акт измерения) различения пары ортогональных состояний.

Прежде чем перейти к изложению протокола, обсудим состояния и измерения, используемые в протоколе. Любое одночастичное состояние поля может быть представлено в виде

$$|\psi_{1,2}\rangle = \int \psi_{1,2}(\hat{p})\delta(\hat{p}^2 - m^2)u^+(\hat{p})d\hat{p}|0\rangle, \tag{2}$$

где интегрирование ведется по массовой поверхности, $\psi_{1,2}(\hat{p})$ – амплитуда поля, $|0\rangle$ – вакуумное состояние. Далее будем иметь дело с безмассовыми частицами (например, фотонами). В этом случае под оператором поля $u^+(\hat{p})$ будем понимать оператор рождения фотона в кулоновской калибровке. Будем также считать, что амплитуды

$\psi_{1,2}(\hat{p})$ таковы, что состояния $|\psi_{1,2}\rangle$ ортогональны:

$$\langle\psi_1|\psi_2\rangle = \int\int \psi_1^*(\mathbf{p}')\psi_2(\mathbf{p})\langle 0|u^-(\mathbf{p}')u^+(\mathbf{p})|0\rangle \frac{d\mathbf{p}'\,d\mathbf{p}}{\sqrt{2p_0'}\sqrt{2p_0}} = \int \psi_1^*(\mathbf{p})\psi_2(\mathbf{p})\frac{d\mathbf{p}}{2p_0} = 0, \tag{3}$$

$$[u^-(\mathbf{p}'), u^+(\mathbf{p})]_- = \delta(\mathbf{p}' - \mathbf{p}).$$

Законченная теория измерений в квантовой теории поля, в отличие от нерелятивистской квантовой механики, отсутствует. Для одночастичных же состояниях поля будем действовать по аналогии с нерелятивистским случаем. Измерение, позволяющее достоверно различать два ортогональных состояния, дается разложением единицы в подпространстве одночастичных состояний

$$\mathcal{P}_1 + \mathcal{P}_2 + \mathcal{P}_\perp = \mathcal{I}, \quad \mathcal{P}_\perp = \mathcal{I} - \mathcal{P}_1 - \mathcal{P}_2, \quad \mathcal{P}_i\mathcal{P}_j = \delta_{ij}\mathcal{P}_i, \tag{4}$$

$$\mathcal{I} = \int u^+(\mathbf{p})|0\rangle\langle 0|u^-(\mathbf{p})\frac{d\mathbf{p}}{2p_0}, \quad \mathcal{P}_{1,2} = \left(\int \psi_{1,2}(\mathbf{p}')u^+(\mathbf{p}')|0\rangle\frac{d\mathbf{p}'}{2p_0'}\right) \times$$

$$\times \left(\int \langle 0|u^-(\mathbf{p})\psi_{1,2}^*(\mathbf{p})\frac{d\mathbf{p}}{2p_0}\right). \tag{5}$$

Вероятность получения результата при входном состоянии $|\psi_1\rangle$ равна

$$\mathrm{Pr}_1(\psi_1) = \langle\psi_1|\mathcal{P}_1|\psi_1\rangle \equiv 1, \quad \mathrm{Pr}_{2,\perp}(\psi_1) = \langle\psi_1|\mathcal{P}_{2,\perp}|\psi_1\rangle \equiv 0, \tag{6}$$

аналогично для состояния $|\psi_2\rangle$. Измерения (4), (5) являются нелокальными в том смысле, что требуется доступ ко всей области пространства, где присутствует поле. Интуитивно понятно, что если мы имеем дело с электромагнитным полем в некоторой области пространства (это означает, что в предъявленном нам состоянии в некоторый момент времени квантовомеханические средние наблюдаемых поля отличны от нуля в этой области), то для определения состояния поля измерительное устройство должно иметь доступ ко всей этой области. Даже если в каждой точке информация о состоянии поля, получаемая в результате локального взаимодействия между полем и измерительным устройством, возникает мгновенно, все равно требуется некоторое время для передачи этой информации наблюдателю, расположенному в некоторой фиксированной точке пространства. Ясно, что где бы ни находился наблюдатель, по порядку величины это время не может быть меньше, чем $L/2c$, где c – скорость света, а L – диаметр области ненулевого поля.

Для протокола будет существенно лишь то, что ортогональные состояния в релятивистском случае могут быть достоверно различимы лишь за конечное время, которое зависит от структуры самих состояний. Другими, словами ортогональные состояния являются эффективно неразличимыми (неразличимыми достоверно) в течение некоторого конечного времени и становятся достоверно различимыми по истечении этого времени.

Для получения информации о состоянии поля измерение должно захватывать ту область пространства, в которой сосредоточено поле. Поэтому, если изначально поле приготавливается в некоторой контролируемой (недоступной для одного из участников обмена) области пространства-времени и затем распространяется в область, доступную для измерения, то состояние становится полностью доступным за конеч-

ное время. Амплитуда распространения поля удовлетворяет принципу причинности

$$\langle\psi_{1,2}(\hat{x}_1)|\psi_{1,2}(\hat{x}_2)\rangle = -i\psi^*_{1,2}(-i\frac{\partial}{\partial \mathbf{x}_1})\psi_{1,2}(i\frac{\partial}{\partial \mathbf{x}_2})D_0^-(\hat{x}_1-\hat{x}_2), \tag{7}$$

где $D_0^-(\hat{x})$ - отрицательно-частотная функция

$$D_0^-(\hat{x}) = \frac{i}{(2\pi)^{3/2}}\int d\hat{k}\delta(\hat{k}^2)\theta(-k^0)\exp(i\hat{k}\hat{x}) = \frac{1}{4\pi}\varepsilon(x^0)\delta(\lambda), \tag{8}$$

$$\varepsilon(x^0) = \theta(x^0)-\theta(-x^0), \quad \lambda^2 = (x^0)^2 - \mathbf{x}^2; \tag{9}$$

здесь $|\psi_{1,2}(\hat{x})\rangle$ – состояние в $\hat{x}$-представлении:

$$|\psi_{1,2}(\hat{x})\rangle = \int \psi_{1,2}(\mathbf{p})e^{i\hat{p}\hat{x}}u^+(\mathbf{p})\frac{d\mathbf{p}}{\sqrt{2p_0}}|0\rangle. \tag{10}$$

Заметим, что при $\hat{x}_1 = \hat{x}_2$

$$\mathrm{Pr}_{1,2}(\psi_{1,2}) = \langle\psi_{1,2}|\mathcal{P}_{1,2}|\psi_{1,2}\rangle = |\langle\psi_{1,2}(\hat{x}_1)|\psi_{1,2}(\hat{x}_2)\rangle|_{\hat{x}_1=\hat{x}_2}|^2 = \tag{11}$$

$$= -\left|\psi^*_{1,2}(-i\frac{\partial}{\partial \mathbf{x}_1})\psi_{1,2}(i\frac{\partial}{\partial \mathbf{x}_2})\right|^2 D_0^-(\hat{x}_1-\hat{x}_2)D_0^+(\hat{x}_2-\hat{x}_1)\big|_{\hat{x}_1=\hat{x}_2}.$$

Несмотря на произведение двух сингулярных обобщенных функций ($D_0^-(\hat{x}) = -D_0^+(-\hat{x})$) при $\hat{x}^2 = 0$ в (11), такое произведение определяет обобщенную функцию, поскольку всегда существует свертка двух обобщенных функций с носителем в передней части светового конуса [19].

Перейдем теперь к описанию протокола. Заранее оговаривается вид состояний $|\psi_1\rangle$ (отвечает 0) и $|\psi_2\rangle$ (соответствует 1). Протокол начинается в $t = 0$. Каждый из участников в $t = 0$ начинает приготавливать N состояний. Число N оговаривается также заранее. Самым плохим является тот случай, когда каждый из участников, с одной стороны, полностью контролирует только непосредственную окрестность своей лаборатории, а с другой стороны, может разместить свою аппаратуру сколь угодно близко к лаборатории другого участника, если он хочет обмануть последнего. Это означает, что протокол должен быть устойчив в ситуации, когда один из пользователей может мгновенно передавать информацию другому, то есть когда длина линии связи между ними эффективно равна нулю. Реально достаточно потребовать, чтобы эффективный размер области локализации состояния существенно превосходил длину канала связи. Формально ситуация, когда длина канала связи равна нулю, означает, что пользователи не могут контролировать пространство вне своей лаборатории в окрестности $x_{A,B}$. В момент $t = 0$ каждый из участников включает источник состояний, которые сразу начинают распространяться в канал связи и становятся доступными для измерения. Для различения состояний с достоверностью (или с вероятностью, сколь угодно близкой к единице) требуется конечное время T. Измерение для различения состояний с достоверностью описывается разложением единицы (4), (5), которое выписывается однозначно.

По истечении времени $T/2$ сначала A сообщает B какие состояния им были посланы, причем A сообщает это лишь для $N/2$ своих состояний. Затем B, после получения инфрмации от A, сообщает для другой половины состояний $N/2$, что им было реально послано. Только после получения классической информации от B, A сообщает ему вторую оставшуюся половину $N/2$ состояний. После получения от A, B раскрывает свою оставшуюся половину состояний.

В итоге участники могут проверить соответствие классической информации, полученной друг от друга, со своими квантовомеханическими измерениями. При любом единичном сбое, например, когда A сообщил, что i-состояние было, например, $|\psi_1\rangle$ (0), а у B сработал детектор на $|\psi_2\rangle$ (1), протокол обрывается. Наличие классической информации от друг друга и достоверная различимость ортогональных квантовых состояний не позволяют подменить даже один бит, что будет важно при вычислении результирующего бита четности. Далее, если в результате обмена принимается отсутствие обмана (имеется соответствие квантовых измерений с классической информацией), вычисляется бит четности $c = c_1 \oplus c_2 \oplus \ldots c_N$ ($c_i = a_i \oplus b_i$, a_i, b_i – биты, соответственно, A и B), который и является жребием.

Обсудим возможные стратегии обмана, например, участником A. Прежде всего, сообщение классической информации участниками друг другу необходимо, чтобы исключить возможность перепосыла состояний, которые получает A, сразу назад к B без их выяснения. Если иметь в виду фотоны, то A достаточно поставить зеркало сразу в точке выхода состояний B в канал связи. Далее, пусть, например, заранее оговорено, что при выпадении 0 выигрывает A. Тогда, если бы не требовалось сообщать классическую информацию, A получает состояния от B и, не пытаясь выяснить их, посылает их сразу назад к B. Очевидно, что бит четности в этом случае всегда будет 0 (выигрывает A), так как $a_i \equiv b_i$, $c_i = a_i \oplus b_i = b_i \oplus b_i \equiv 0$, $c = c_1 \oplus c_2 \oplus \ldots c_N \equiv 0$. Если же A должен сообщать по классическому каналу, что им реально было послано к B, то такой обман исключается.

Поочередное раскрытие через классический канал по половине состояний необходимо для того, чтобы исключить следующую стратегию обмана (которую, кстати, легко проглядеть). Поскольку B контролирует лишь пространство своей лаборатории вблизи точки x_B, то A может разместиться вблизи x_B, и после перепосыла квантовых состояний назад к B, A на стадии обмена классической информацией практически мгновенно может передать к B назад полученную от него по классическому каналу информацию. При этом если B сообщает, что им было послано сразу по всем N состояниям (которые A перепослал назад), то A может мгновенно вернуть к B классическую информацию. При поочередном раскрытии по половине состояний такая стратегия не срабатывает.

Для протокола существенно, что состояния являются квантовыми. Если бы состояния были классическими, то, например, A всегда бы мог последовательно в каждый момент времени в течении времени протокола "отбирать" от каждого состояния, полученного от B, сколь угодно малую часть для измерений (на это нет запретов в классической физике) и одновременно перепосылая состояния назад к B без их искажения. "Отобранная" сколь угодно малая часть состояний могла бы использоваться для выяснения состояний B в течение времени протокола и затем сообщения их по классическому каналу. В этом случае A всегда выигрывает. Для квантовых состояний такая стратегия невозможна, так как невозможны измерения в последовательные моменты времени без искажений.

Поскольку для достоверного различения ортогональных состояний требуется конечное время, то в течение времени $0 \leq t \leq T$ состояния достоверно неразличимы и являются эффективно неортогональными. Вероятность правильного детектирования состояния является растущей функцией времени $P(t)$: ($P(0) = 1/2$ (простое угадывание) и $P(T) = 1$). Конкретный вид $P(t)$ зависит от конкретных состояний и для нас несуществен. Участник A не может задерживать посылку своих состояний,

иначе они не будут зарегистрированы в течение времени T (при большом N будут события вне $0 \leq t \leq T$). Одна из возможных стратегий обмана могла бы состоять в корректировке уже посланных состояний участником A в зависимости от результата измерения над состояниями B. В этом случае A должен уже получить результат измерений над состоянием B к некоторому моменту времени t (вероятность этого $p(t)$), а B еще должен не успеть зарегистрировать состояние A (вероятность такого события $1 - p(t)$). Вероятность успешного обмана $P_{ch} = p(t)(1 - p(t))$. Максимум P_{ch} достигается при $p(t_c) = 1/2$ и равен $1/4$, что меньше, чем вероятность простого угадывания, которая равна $1/2$. В принципе A мог бы выполнить коллективное измерение сразу над N состояниями посланными от B [20], однако из-за эффективной неортогональности состояний в течение времени T вероятность правильной идентификации бита четности при этом по-прежнему достигает единицы лишь при $t = T$.

Сделаем в заключение одно замечание. Возможность идентификации состояния с вероятностью единица в течение конечного интервала времени T зависит от того, существуют ли для данного типа частиц состояния с конечным носителем в пространстве. Если речь идет о фотонах, то на сегодняшний день известны лишь состояния с экспоненциальной локализацией энергии [21]. Для протокола это не слишком существенно, поскольку интервал времени может быть выбран достаточно большим, чтобы обеспечить экспоненциально близкую к единице вероятность различения двух ортогональных состояний.

Работа поддержана Российским фондом фундаментальных иследований (проект 99-02-18127) и проектом 02.04.5.2.40.T.50 программы "Перспективные технологии и устройства микро- и наноэлектроники".

---

1. M.Blum, *Coin flipping by telephone: A protocol for solving impossible problems*, Proc. 24th IEEE Comp. Conf., 1982, p.133-137, also in: SIGACT News **15**, 23 (1983).
2. P.W.Shor, *Proc. 35th Annual Symposium on Foundations of Computer Science*, Santa Fe, NM, USA, Ed. S.Goldwasser (IEEE Comput. Soc. Press, Los Alamitos) 1994, p.124.
3. А.Ю.Китаев, УМН **52**, 54 (1997).
4. S.Wiesner, SIGACT News **15**, 78 (1983).
5. C.H.Bennett and G.Brassard, in *Proc. IEEE Int. Conf. on Computers, Sytems, and Signal Processing*, IEEE, New York, 1984, p.175.
6. A.Ekert, Phys. Rev. Lett. **67**, 661 (1991).
7. G.Brassard, C.Crépeau, R.Jozsa, and D.Langlois, *Proc. of the 34th Annual IEEE Symposium on the Foundation of Computer Science*, IEEE Cmp. Soc., Los Alamitos, California, 1993, p.362.
8. G.Brassard and C.Crépeau, *Advances in Cryptology: Proc. of Crypto'90, Lecture Notes in Computer Science*, vol.537, 1991, p.49, Springer-Verlag, Berlin.
9. M.Ardehali, quant-ph/9603015.
10. D.Mayers, L.Salvail, and Y. Chiba-Kohno, quant-ph/9904078.
11. L.Goldenberg, L.Vaidman, and S.Wiesner, quant-ph/9808001.
12. H.F.Chau, quant-ph/9901024.
13. H.-K.Lo and H.F.Chau, Phys. Rev. Lett. **78**, 3410 (1997).
14. D.Mayers, Phys. Rev. Lett. **78**, 3414 (1997).
15. A.Kent, quant-ph/9810067, quant-ph/9810068, Phys. Rev. Lett. **83**, 1447 (1999); quant-ph/9906103.
16. W.K.Wootters and W.H.Zurek, Nature, **299**, 802 (1982).
17. C.H.Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
18. L.Goldenberg and L.Vaidman, Phys. Rev. Lett. **75**, 1239 (1995).
19. Н.Н.Боголюбов, Д.В.Ширков, *Введение в теорию квантованных полей*, М.: Наука, 1973.
20. Tal Mor, quant-ph/9906073.
21. I.Bialynicki-Birula, Phys. Rev. Lett. **80**, 5247 (1998).