Письма в ЖЭТФ, том 93, вып. 6, с. 389 – 393

Квантовое распределение ключей без передачи квантового состояния как целого через канал связи

С. Н. Молотков

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

Академия Криптографии Российской Федерации

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

Поступила в редакцию 1 февраля 2011 г.

Приведен пример квантового распределения ключей на запутанном однофотонном и вакуумном состоянии. В данной схеме однофотонное квантовое состояние никогда и ни в какие моменты времени как целое не передается через канал связи.

Значение классического бита информации (0 или 1) может быть ассоциировано с состоянием квантовой системы. Обычно неявно подразумевается, что при передаче информации квантовая система как целое распространяется через канал связи от передатчика к приемнику. Возникает интересный вопрос. Можно ли в принципе передавать классическую информацию при помощи квантовых состояний, не передавая при этом квантовое состояние как целое через канал связи? Уточним слова *"как целое"*. Более точно это означает, что если пытаться регистрировать только сам факт присутствия однофотонного квантового состояния в канале связи, то состояние случайно будет зарегистрировано только, например, в половине посылок. Однако при этом бит информации с вероятностью единица (с достоверностью) передается в каждой посылке.

Несмотря на кажущуюся парадоксальность данного рассуждения (см. также рис.1), как будет пока-

1	*1*	*0*	*1*	*0*	*0*	*1*	*0*	*1*
	*			*		*	*	

Рис.1. Первая строка – передача информации. Вторая строка – факт регистрации фотона (случайные отсчеты фотодетектора)

зано ниже, такая ситуация допускается и является простым следствием законов квантовой механики.

Поскольку ответ на первый вопрос оказывается положительным, то второй вопрос звучит так. Возможно ли использовать данное свойство для секретной передачи ключей, и какие при этом могут возникнуть дополнительные возможности для квантовой криптографии?

Ниже предлагается система квантовой криптографии, в которой *квантовое состояние никогда, ни в какие моменты времени, как целое никогда не передается и не распространяется через канал связи* между пространственно удаленными пользователями.

Одной из центральных задач криптографии является распределение ключей. Квантовая механика позволяет реализовать передачу ключей таким образом, что их секретность гарантируется фундаментальными законами природы [1 – 4].

За последние годы было предложено множество протоколов квантовой криптографии и систем распределения ключей на их основе (см. обзор [4]). Все системы квантовой криптографии можно разделить на две группы. В первой группе для гарантии секретности ключей используются фундаментальные запреты квантовой механики на достоверную различимость неортогональных квантовых состояний [3].

Ко второй группе относятся системы, которые кроме ограничений квантовой механики используют дополнительные ограничения, диктуемые специальной теорией относительности [5, 6]. Данные системы квантовой криптографии [5, 6] для гарантии секретности ключей в основном используют факт существования предельной скорости распространения сигналов. Совместные ограничения квантовой механики и специальной теории относительности позволяют использовать даже ортогональные (то есть достоверно различимые) квантовые состояния для передачи секретных ключей [5]. Однако для при этом приходится использовать состояния с протяженностью больше длины канала связи [5, 6]. В дальнейшем ограничение на протяженность состояния больше длины линии связи было снято [7]. Кроме того, оказалось, что гарантировать секретность ключей можно и для многофотонных информационных состояний и при любой величине затухания (соответственно длине) в квантовом канале связи, чего не удается пока достичь ни в одном из известных протоколов нерелятивистской квантовой криптографии [4].

Во всех упомянутых системах квантовой криптографии информационные квантовые состояния *всегда проходят через канал связи между передающей и приемной станциями* (Алисой и Бобом). В некоторых релятивистских протоколах квантовые состояния через канал связи передаются в два этапа, так что целиком единовременно квантовое состояние не присутствует в канале связи [5, 6]. Однако квантовое состояние, хотя и в разные моменты времени, все равно проходит через канал связи как целое, поэтому оно доступно подслушивателю целиком, пусть даже с задержкой во времени.

Приведем сначала пример передачи информации, когда однофотонное квантовое состояние как целое никогда не проходит через канал связи, а затем приведем пример системы квантовой криптографии.

Идея схемы достаточно проста и представлена на рис.2. Для передачи одного бита информации Алиса случайно активирует однофотонный источник S. После этого локализованное однофотонное состояние поступает на симметричный светоделитель BS. Состояние на одном из входов светоделителя – однофотонный пакет, на втором – вакуумное состояние, общее состояние – $|\Psi\rangle = |1\rangle \otimes |vac\rangle$[1]. После прохождения через симметричный светоделитель BS состояние преобразуется как

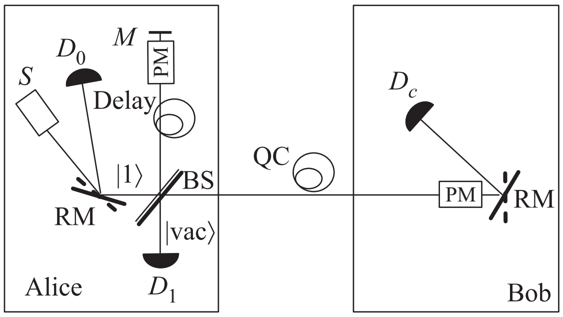

Рис.2. $D_{0,1}$ – информационные детекторы, D_c – контрольный детектор, PM – фазовые модуляторы, RM – вращающиеся зеркала, BS – симметричный светоделитель, S – источник однофотонных состояний, QC – квантовый канал связи, $Delay$ – линия задержки, равная по длине квантовому каналу связи, M – неподвижное зеркало. Условно показано состояние, приготовленное Алисой $|1\rangle \otimes |vac\rangle$

[1] Формализм для преобразования квантовых состояний при прохождении через различные (линейные и нелинейные) оптические элементы был развит в свое время в работах Манделя и др., поэтому простые технические детали опускаем (см. монографию [13] и имеющиеся там ссылки).

$$|\Psi\rangle \rightarrow |\Psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|1\rangle_A \otimes |vac\rangle_B + |vac\rangle_A \otimes |1\rangle_B). \tag{1}$$

Состояние (1) является составным. Подсистема B направляется через канал связи к Бобу, а подсистема A остается под контролем Алисы. Боб осуществляет локальные преобразования над подсистемой B – $I_A \otimes U_B$ (I_A – единичный оператор в подпространстве A, U_B – унитарный оператор в подпространстве B). Преобразование сводится к изменению относительной фазы между состояниями подсистем A и B. Такое преобразование реализуется при помощи фазового модулятора PM (рис.2). Значение фазы $\varphi_B = 0$ отвечает значению бита 0, $\varphi_B = \pi$ – значению бита 1. Учитывая инвариантность вакуумного состояния, имеем

$$|\Psi^{\varphi_B}\rangle_{AB} = \frac{1}{\sqrt{2}}(|1\rangle_A \otimes |vac\rangle_B + e^{i\varphi_B}|vac\rangle_A \otimes |1\rangle_B). \tag{2}$$

Подсистема A остается в распоряжении Алисы и поступает на линию задержки, длина которой равна длине линии связи. После отражения подсистемы B на стороне Боба, подсистемы A и B собираются на светоделителе BS. В зависимости от выбора фазы φ_B подсистемы A и B собираются в канале 0, либо 1. Если Боб выбрал значение фазы $\varphi_B = 0$, то состояние в (2) $|\Psi^{\varphi_B=0}\rangle_{AB}$ приведет к отсчету в детекторе D_0. Если Боб выбрал $\varphi_B = \pi$, состояние $|\Psi^{\varphi_B=\pi}\rangle_{AB}$ в (2) даст срабатывание детектора D_1. Срабатывание детектора D_0 или D_1 однозначно указывает Алисе на выбор бита Бобом. В результате между Бобом и Алисой передается один бит информации.

Состояние системы в канале связи получается взятием частичного следа по недоступной подсистеме A; имеем

$$\rho = \mathrm{Tr}_A\{|\Psi^{\varphi_B}\rangle_{AB\,AB}\langle\Psi^{\varphi_B}|\} = \\ = \tfrac{1}{2}(|vac\rangle_{B\,B}\langle vac| + |1\rangle_{B\,B}\langle 1|). \tag{3}$$

Отсюда следует, что однофотонная компонента (второе слагаемое в (3)) присутствует в канале связи с вероятностью 1/2, поэтому однофотонный пакет в канале связи в каждой посылке может быть зарегистрирован случайно лишь с вероятностью 1/2 независимо от входного состояния. Однако при этом с достоверностью можно передавать бит информации в каждой посылке.

Данное явление фактически аналогично плотному кодированию (dense coding) при помощи двухчастичной ЭПР пары [8]. При плотном кодировании Алиса готовит ЭПР пару и одну частицу направляет к Бобу. Боб, локально манипулируя состоянием *только одной частицы*, а затем возвращая ее Алисе для измерений, может передать *два бита* информации в каждой посылке. Сам факт регистрации одной частицы у Боба (соответственно в канале связи) при этом имеет место в каждой посылке. В нашем случае Боб манипулирует только, условно говоря, "половинкой" однофотонного пакета (доступной ему частью в общей суперпозиции), поэтому передается один бит информации. Соответственно, сам факт регистрации фотона в канале имеет место только в половине посылок.

Перейдем к построению протокола квантового распределения ключей. Для достижения секретности ключей необходимо сделать добавления в протокол обмена. Если Боб выбирает только два значения фазы $\varphi_B = 0, \pi$, то система несекретна. Пусть теперь Боб, аналогично протоколу BB84 [2], случайно и независимо от Алисы выбирает следующие значения фазы. Сначала случайно и равновероятно выбирается базис $+$ или $\times$, затем случайно и равновероятно выбирается 0 или 1. Значения фазы при этом: базис $+$, $\varphi_B = 0$ – 0, $\varphi_B = \pi$ – 1. И аналогично в базисе $\times$: $\varphi_B = \pi/2$ – 0, $\varphi_B = -3\pi/2$ – 1. При возврате состояния от Боба, Алиса при помощи фазового модулятора (PM рис.2) случайно и независимо от Боба, локально манипулирует с подсистемой A, действуя унитарным оператором $U_A \otimes I_B$, выбирает два значения фазы: $\varphi_A = 0$ – базис $+$, $\varphi_A = \pi/2$ – базис $\times$. Далее через открытый канал сравниваются базисы в разных посылках, значения битов 0,1 при этом не раскрываются. Если базисы не совпали, то посылки отбрасываются. В тех посылках, где базисы совпали, имеем

$$|\Psi^{\varphi_B,\varphi_A}\rangle_{AB} = \\ = \frac{1}{\sqrt{2}}(e^{i\varphi_A}|1\rangle_A \otimes |vac\rangle_B + e^{i\varphi_B}|vac\rangle_A \otimes |1\rangle_B). \quad (4)$$

При совпадающих базисах срабатывание того или иного детектора однозначно указывает Алисе на выбор бита Бобом. Имеем:

$$\text{базис} \quad + : \quad \varphi_A = 0, \quad \varphi_B = \begin{pmatrix} 0 & \text{детектор } D_0 \\ \pi & \text{детектор } D_1 \end{pmatrix}, \quad (5)$$

$$\text{базис } \times : \ \varphi_A = \frac{\pi}{2}, \ \varphi_B = \begin{pmatrix} \pi/2 & \text{детектор } D_0 \\ 3\pi/2 & \text{детектор } D_1 \end{pmatrix}. \quad (6)$$

Покажем, что такая передача ключей является секретной. Наиболее общая атака Евы, которой доступно состояние только в канале связи, сводится к использованию вспомогательной квантовой системы (ancilla) $|A\rangle_E$, которая взаимодействует с передаваемым состоянием [9]. После такого взаимодействия ancilla и передаваемое состояние оказываются запутанными. Искаженное передаваемое состояние направляется к Алисе, а ancilla остается в квантовой памяти. После проведения измерений Алисой, Ева производит коллективные оптимальные измерения сразу над всеми ancilla в квантовой памяти.

Удобно ввести новые обозначения для состояний в канале связи после изменения фазы Бобом. Имеем в базисе $+$:

$$|0_+\rangle_{AB} = \frac{1}{\sqrt{2}}(|\overline{0}\rangle_{AB} + |\overline{1}\rangle_{AB}), \\ |1_+\rangle_{AB} = \frac{1}{\sqrt{2}}(|\overline{0}\rangle_{AB} - |\overline{1}\rangle_{AB}), \quad (7)$$

и в базисе $\times$

$$|0_\times\rangle_{AB} = \frac{1}{\sqrt{2}}(|\overline{0}\rangle_{AB} + i|\overline{1}\rangle_{AB}), \\ |1_\times\rangle_{AB} = \frac{1}{\sqrt{2}}(|\overline{0}\rangle_{AB} - i|\overline{1}\rangle_{AB}), \quad (8)$$

где $|\overline{0}\rangle_{AB} = |1\rangle_A \otimes |vac\rangle_B$, и $|\overline{1}\rangle_{AB} = |vac\rangle_A \otimes |1\rangle_B$. Действия Евы описываются унитарным оператором, действующим в пространстве состояний $\mathcal{H}_{AB} \otimes \mathcal{H}_E$, где $\mathcal{H}_{AB} = (\mathcal{H}_0 \oplus \mathcal{H}_1)_A \otimes (\mathcal{H}_0 \oplus \mathcal{H}_1)_B$, $(\mathcal{H}_{0,1})_{AB}$ – фоковские пространства состояний без фотонов и с одним фотоном. И $|A\rangle_E \in \mathcal{H}_E$ – пространство состояний Евы, размерность и структура которого будет уточнена ниже.

Достаточно рассмотреть действия Евы только на состояния в базисе $+$, так как состояния в базисе $\times$ получаются линейным преобразованием. Имеем

$$|\widetilde{\Psi}_{0_+}\rangle_{ABE} = (I_A \otimes U_{BE})(|0_+\rangle_{AB} \otimes |A\rangle_E) = \\ = \frac{1}{2}\left(|0_+\rangle_{AB} \otimes |A_{00}\rangle_E + |1_+\rangle_{AB} \otimes |A_{01}\rangle_E\right), \quad (9)$$

$$|\widetilde{\Psi}_{1_+}\rangle_{ABE} = (I_A \otimes U_{BE})(|1_+\rangle_{AB} \otimes |A\rangle_E) = \\ = \frac{1}{2}\left(|1_+\rangle_{AB} \otimes |A_{11}\rangle_E + |0_+\rangle_{AB} \otimes |A_{10}\rangle_E\right), \quad (10)$$

где I_A – единичный оператор в пространстве состояний Алисы, поскольку оно недоступно подслушивателю.

Требования унитарности и симметрии между базисами $+$ и $\times$ позволяют однозначно параметризовать унитарный оператор U_{BE} и определить искаженные состояния Евы. Вводя обозначения

$$|A_{00}\rangle_E = |a_{00}\rangle_E + |a_{11}\rangle_E + |a_{01}\rangle_E + |a_{10}\rangle_E, \\ |A_{11}\rangle_E = |a_{00}\rangle_E + |a_{11}\rangle_E - (|a_{01}\rangle_E + |a_{10}\rangle_E), \quad (11)$$

$$|A_{01}\rangle_E = |a_{00}\rangle_E - |a_{11}\rangle_E - (|a_{01}\rangle_E - |a_{10}\rangle_E),$$
$$|A_{10}\rangle_E = |a_{00}\rangle_E - |a_{11}\rangle_E + (|a_{01}\rangle_E + |a_{10}\rangle_E), \quad (12)$$

где состояния $|a_{ij}\rangle_E$ имеют вид

$$|a_{00}\rangle_E = \sqrt{1-Q}|e_1\rangle_E \otimes |e_1\rangle_E,$$
$$|a_{11}\rangle_E = \sqrt{1-Q}(\cos(\alpha)|e_1\rangle_E \otimes |e_1\rangle_E + + \sin(\alpha)|e_2\rangle_E \otimes |e_1\rangle_E, \quad (13)$$

$$|a_{01}\rangle_E = \sqrt{Q}|e_1\rangle_E \otimes |e_2\rangle_E,$$
$$|a_{10}\rangle_E = \sqrt{Q}(\cos(\alpha)|e_1\rangle_E \otimes |e_2\rangle_E + + \sin(\alpha)|e_2\rangle_E \otimes |e_2\rangle_E, \quad (14)$$

здесь $|e_{1,2}\rangle_E$ – базисные ортонормированные векторы состояний в пространстве Евы $\mathcal{H}_E$ размерности 4, и $Q = (1-\cos(\alpha))/2$. Таким образом, атака Евы (унитарный оператор U_{BE}), параметризуется одним параметром Q, который имеет смысл вероятности ошибки, производимой Евой на стороне Алисы. Действительно, вероятность того, что Боб выбрал значения бита 0 или 1 и Алиса получила правильный результат, есть

$$\Pr(i|j) = \mathrm{Tr}_{ABE}\{|\widetilde{\Psi}_i\rangle_{ABE\,ABE}\langle\widetilde{\Psi}_i||j\rangle_{AB\,AB}\langle j|\} = = \begin{cases} 1-Q, & i=j \\ Q, & i\neq j \end{cases}, \quad (15)$$

где $i,j = 0_+, 1_+, 0_\times, 1_\times$. Как следует из (15), величина Q имеет смысл вероятности ошибки. После измерений Алиса и Боб связаны бинарным классическим каналом связи с вероятностью ошибки Q. Взаимная информация в пересчете на одну оставленную посылку равна $I(A;B) = 1 - h(Q)$ ($h(Q) = = -Q\log(Q) - (1-Q)\log(1-Q)$ – бинарная энтропийная функция).

Состояния Евы получаются взятием частичного следа по пространству состояний Алисы и Боба и имеют вид

$$\rho^E_{0_+,1_+} = \mathrm{Tr}_{AB}\{|\widetilde{\Psi}_{0_+,1_+}\rangle_{ABE\,ABE}\langle\widetilde{\Psi}_{0_+,1_+}|\}. \quad (16)$$

Информация Евы ограничена величиной Холево [10], которая дает достижимую верхнюю границу для величины классической информации, и может быть извлечена из квантового ансамбля; получаем

$$I(A;E) \le \chi(\rho^E_{0_+}, \rho^E_{1_+}),$$
$$\chi(\rho^E_{0_+}, \rho^E_{1_+}) = H\left(\frac{1}{2}(\rho^E_{0_+} + \rho^E_{1_+})\right) - \quad (17)$$
$$-\frac{1}{2}\left(H(\rho^E_{0_+}) + H(\rho^E_{0_+})\right) = h(Q),$$

где $H(\rho) = -\mathrm{Tr}\{\rho\log(\rho)\}$ – энтропия фон Неймана. Распространение секретных ключей возможно до тех пор, пока $I(A;B) > I(A;E)$ [1,9]. Величина критической ошибки Q_c на стороне Алисы, до которой гарантируется секретное распределение ключей, определяется из равенства взаимных информаций, что дает $1 - h(Q_c) = h(Q_c)$, $Q_c \approx 11\%$.

Кроме атаки на состояние в квантовом канале связи, возможны также атаки, связанные с активным зондированием активных оптических элементов на передающей и приемной станциях [11]. Наиболее опасным является зондирование состояния фазового модулятора у Боба, поскольку его состояние однозначно указывает на передаваемый бит ключа. Для детектирования таких атак используется контрольный детектор D_c (рис.2). Ева может зондировать состояние модулятора по отражению многофотонного (классического) состояния. Для детектирования таких попыток Боб случайно в ряде посылок направляет состояние на контрольный детектор. Если активного зондирования нет, то срабатывание детектора произойдет только в половине контрольных проверок при достаточно длинной серии, так как в состоянии Алисы присутствует однофотонная компонента только с вероятностью 1/2 (см. формулу (3)). Если срабатываний больше половины, то это превышение Боб должен списать на действия Евы. Поскольку Боб выбирает контрольные посылки случайно, то в информационных посылках доля посылок с активным зондированием такая же. Устранение этой информации о ключе у Евы может быть достигнуто дополнительным сжатием финального ключа.

Таким образом, вопрос, поставленный выше, имеет положительный ответ. В таком виде схема, возможно, представляет чисто академический интерес. Выигрыш возникает, если использовать идею с разделением не однофотонного, а многофотонного состояния на стороне Алисы на две подсистемы. "Часть" состояния используется Алисой как реперное при измерениях и сравнении с "частью" состояния от Боба. Такие схемы оказываются устойчивыми против PNS (Photon Number Splitting [12]) атаки и не имеют ограничения по длине линии связи, в отличие от всех предыдущих схем [4]. Детальное изложение требует большего места и будет приведено отдельно.

Выражаю благодарность коллегам по Академии криптографии Российской Федерации за постоянную поддержку, а также С.П. Кулику за интенсивные и плодотворные обсуждения. Работа частично поддержана проектом Российского фонда фундаментальных исследований # 11-02-00455.

1. W. K. Wooters and W. H. Zurek, Nature. **299**, 802 (1982).
2. C. H. Bennett and G. Brassard, *Quantum Cryptography: Public Key Distribution and Coin Tossing*, Proc. of IEEE Int. Conf. on Comput. Sys. and Sign. Proces., Bangalore, India, December 1984, p. 175.
3. C. H. Bennett, Phys. Rev. lett. **68**, 3121 (1992).
4. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf et al., Rev. Mod. Phys. **81**, 1301 (2009).
5. L. Goldenberg and L. Vaidman, Phys. Rev. Lett. **75**, 1239 (1995).
6. M. Koashi and N. Imoto, Phys. Rev. Lett. **79**, 2383 (1997).
7. С. Н. Молотков, ЖЭТФ **139**, вып. 3 (2011).
8. C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
9. R. Renner, arXiv: quant-ph/0512258.
10. A. S. Holevo, Usp. Mat. Nauk **53**, 193 (1998).
11. А. В. Корольков, К. Г. Катамадзе, С. П. Кулик, С. Н. Молотков, ЖЭТФ **137**, 429 (2010).
12. G. Brassard, N. Lütkenhaus, T. Mor, and B. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).
13. Л. Мандель, Э. Вольф, *Оптическая когерентность и квантовая оптика*, М.: Физматлит, 2000; L. Mandel and E. Wolf, *Optical Coherence and Quantum Optics*, Cambridge University Press, 1995.