Письма в ЖЭТФ, том 88, вып. 9, с. 729 – 733 10 ноября

Квантовое распределение ключа на бифотонах-куквартах с проверочными состояниями

А. П. Шурупов, С. П. Кулик

Физический факультет МГУ им. М.В. Ломоносова, 119992 Москва, Россия

Поступила в редакцию 13 августа 2008 г.

После переработки 18 сентября 2008 г.

Рассматривается операциональное включение подкласса перепутанных состояний в протокол квантового распределения ключа, основанного на бифотонах-куквартах. Предлагается использовать четыре состояния Белла в качестве проверочных – для оценки уровня ошибок, оставляя подкласс 12 факторизованных поляризационных состояний бифотонов в качестве информационных. Проведен элементарный анализ двух стратегий вторжения в квантовый канал связи и скорости генерации ключа.

PACS: 42.50.Dv, 42.65.Lm

1. Введение. Увеличение размерности гильбертова пространства, D, квантовых состояний рассматривается как один из физических способов увеличения секретности квантовой криптографии. Секретность определяется допустимым уровнем ошибок, превышение которого не гарантирует распределение строки битов, из которой (после проведения процедур коррекции ошибок и усиления секретности) строится ключ. Увеличение этого уровня, в некотором смысле, является одной из основных задач квантовой криптографии и приводит к устойчивости протоколов к различным атакам злоумышленников и/или росту дальности распределения ключа.

На сегодняшний день предложено несколько более или менее реалистических физических систем, являющихся прототипом для практической реализации квантового распределения ключа (КРК) на многоуровневых состояниях (для которых $D > 2$). Среди них выделим пространственные моды пучков светового поля [1], однофотонные состояния в комбинированном фазово-временном пространстве [2], бифотоны в многоплечевом интерферометре [3], пространственные моды бифотонного поля [4], четырехфотонные поляризационные состояния [5], бифотоны, генерируемые последовательностью лазерных импульсов [6] и поляризационные однопучковые бифотоны-куквартs ($D = 4$), когда два фотона принадлежат одной пространственной моде, но имеют разные поляризации и фиксированные невырожденные частоты [7].

По простоте и эффективности реализации поляризационные куквартs являются перспективным классом состояний для построения протоколов КРК в многомерном гильбертовом пространстве. Одним из преимуществ таких систем является возможность кодирования и передачи информации в состояния пар фотонов (в том числе и перепутанные), *распространяющиеся в одном направлении*. Другое преимущество – использование хорошо развитых в классической телекоммуникации методов частотной селекции и поляризационной модуляции сигналов. Вместе с тем, в качестве недостатка использования куквартов-бифотонов упоминается тот факт, что реализованные на сегодняшний день состояния и схемы их измерения не охватывают полного набора поляризационных двухфотонных состояний, а именно, – подкласса перепутанных состояний [8]. Следовательно, использование подобных систем в КРК не раскрывает полного спектра их возможностей и сводится лишь к манипуляции с факторизованными состояниями типа

$$|\Psi_1\rangle \otimes |\Psi_2\rangle, \qquad (1)$$

где кет-векторы обозначают состояния фотонов 1 и 2. Действительно, если генерация двухфотонных перепутанных состояний на практике не встречает серьезных трудностей, то их детерминистическое измерение принципиально невозможно на основе только линейных оптических устройств [9]. Этот аргумент является решающим в дискуссии о выборе того или иного подкласса двухфотонных состояний для демонстрации КРК на состояниях с размерностью $D = 4$. Вместе с тем возникает вопрос: возможно ли построение реалистичного протокола на бифотонах-куквартах, в который вовлечены перепутанные состояния?

В данной работе предлагается протокол КРК с использованием так называемых “подстановочных” двухфотонных перепутанных состояний. Эти состояния не являются информационными, а используются только для проверки вторжения в квантовый канал

злоумышленника. В качестве информационных выступают факторизованные состояния (1), использовавшиеся ранее для демонстрации расширенного протокола BB84 [10] на бифотонах-куквартах [11, 12]. Таким образом, в протоколе оказываются задействованными все представители класса двухфотонных поляризационных состояний – как факторизованные, так и перепутанные, в то время как измерение происходит в удобных базисах факторизованных состояний.

2. Описание протокола. По сути, протокол представляет собой расширенную версию BB84 с редуцированным набором взаимно-несмещенных базисов[1)] [13]. Рассматриваются три базиса из пяти возможных:

$$\text{I.}\quad |H_1\rangle\otimes|H_2\rangle,\ |H_1\rangle\otimes|V_2\rangle,\ |V_1\rangle\otimes|H_2\rangle,\ |V_1\rangle\otimes|V_2\rangle, \tag{2а}$$

$$\text{II.}\quad |D_1\rangle\otimes|D_2\rangle,\ |D_1\rangle\otimes|A_2\rangle,\ |A_1\rangle\otimes|D_2\rangle,\ |A_1\rangle\otimes|A_2\rangle, \tag{2б}$$

$$\text{III.}\quad |R_1\rangle\otimes|R_2\rangle,\ |R_1\rangle\otimes|L_2\rangle,\ |L_1\rangle\otimes|R_2\rangle,\ |L_1\rangle\otimes|L_2\rangle. \tag{2в}$$

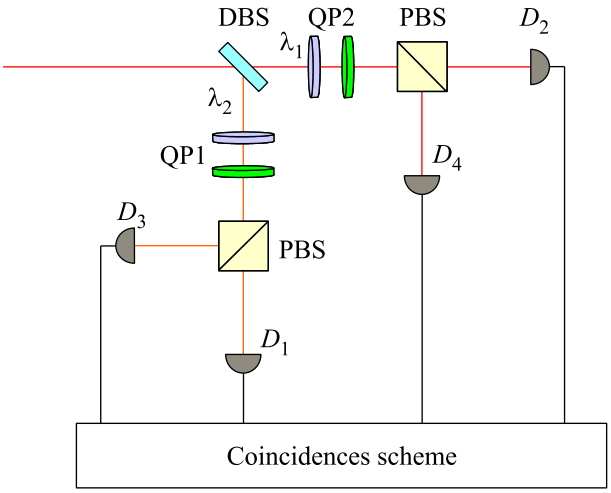
Символы $|H\rangle$, $|V\rangle$, $|D\rangle$, $|A\rangle$, $|R\rangle$, $|L\rangle$ обозначают поляризационные однофотонные состояния с горизонтальной, вертикальной, наклонной и циркулярной поляризациями, соответственно: $|H\rangle = a^+|vac\rangle$, $|V\rangle = b^+|vac\rangle$, $|D(A)\rangle = \frac{1}{\sqrt{2}}(|H\rangle + (-)|V\rangle)$, $|R(L)\rangle = \frac{1}{\sqrt{2}}(|H\rangle + (-)i|V\rangle)$, где a^+, b^+ – операторы рождения фотонов в горизонтальной и вертикальной поляризационной модах, $|vac\rangle$ – вакуумное состояние. Индексы 1 и 2 в выражениях (1), (2) нумеруют центральные частоты в спектре каждого однофотонного состояния, составляющего бифотон. Два оставшихся базиса построены из перепутанных состояний

$$\text{IV.}\quad \begin{array}{l} |R_1,H_2\rangle + |L_1,V_2\rangle;\ |R_1,H_2\rangle - |L_1,V_2\rangle; \\ |L_1,H_2\rangle + |R_1,V_2\rangle;\ |L_1,H_2\rangle - |R_1,V_2\rangle, \end{array} \tag{3а}$$

$$\text{V.}\quad \begin{array}{l} |H_1,R_2\rangle + |V_1,L_2\rangle;\ |H_1,R_2\rangle - |V_1,L_2\rangle; \\ |H_1,L_2\rangle + |V_1,R_2\rangle;\ |H_1,L_2\rangle - |V_1,R_2\rangle \end{array} \tag{3б}$$

и не используются в протоколе.

Алиса случайно выбирает состояния из трех базисов (всего 12 состояний) и посылает их Бобу. Боб измеряет состояния в одном из случайно выбранных базисов (2), причем имеется простая измерительная схема [11], которая дает детерминистический результат, если выбранный базис совпал с тем, из которого посылалось состояние (см. рисунок). Такая схема состоит из дихроичного светоделителя, не чувствительного к поляризации, в каждом из выходных плеч которого помещен поляризационный светоделитель. Схема задействует одну пространственную моду на входе и имеет четыре моды на выходе, в которые установлены счетчики фотонов. Импульсы, поступающие со счетчиков, подаются на четырехвходовое устройство, регистрирующее парные совпадения импульсов с идентификацией входов, которое служит для дискриминации событий. Смена базисов осуществляется путем установки поляризационных преобразователей – полуволновых и четвертьволновых фазовых пластинок после дихроичного светоделителя. Например, при выборе базиса (2а) эти пластинки не используются. "Наклонный" базис (2б) соответствует установке полуволновых пластинок, ориентированных под углом 22.5°. Циркулярному базису (2с) отвечают четвертьволновые пластинки, установленные под углом 45°. Так срабатывание пары детекторов D_3D_2 в базисе (2а) однозначно соответствует регистрации состояния $|V_1H_2\rangle$ и т.д.



Детерминистическая схема измерения состояния бифотонов-куквартов. DBS – дихроичный светоделитель, на котором происходит разделение входного состояния на пространственные моды с различными длинами волн. Поляризационные преобразователи QP1 и QP2, состоящие из четвертьволновой и полуволновой пластинок, служат для выбора базиса измерения. PBS – поляризационные светоделители. Схема совпадений с идентификацией входов (Coincidence scheme) служит для селекции событий

[1)] Взаимно-несмещенными называют базисы, строящиеся на ортонормированных состояниях, удовлетворяющих условиям: $|\langle e_i|e_j\rangle|^2 = 1/D$, если векторы $|e_i\rangle$, $|e_j\rangle$ принадлежат разным базисам, и $|\langle e_i|e_j\rangle|^2 = 0$, $i \neq j$ и $|\langle e_i|e_i\rangle|^2 = 1$ для векторов, принадлежащих одному базису. Максимально возможное число взаимно-несмещенных базисов для системы размерностью D равно $D+1$, а общее число состояний составляет $D(D-1)$.

В общем случае, если Алиса посылала состояние $|\psi_{\text{Alice}}\rangle$, то вероятность измерения состояния $|\psi_{\text{Bob}}\rangle$ в такой схеме

$$F = |\langle\psi_{\text{Alice}}|\psi_{\text{Bob}}\rangle|^2. \qquad (4)$$

Предположим, что наряду с состояниями (2) Алиса посылает в квантовый канал четыре состояния Белла с вероятностью q:

$$|\Psi_{12}^{\pm}\rangle = \frac{1}{\sqrt{2}}(|H_1\rangle|V_2\rangle \pm |V_1\rangle|H_2\rangle), \qquad (5а)$$

$$|\Phi_{12}^{\pm}\rangle = \frac{1}{\sqrt{2}}(|H_1\rangle|H_2\rangle \pm |V_1\rangle|V_2\rangle). \qquad (5б)$$

После завершения передачи квантовых состояний Боб сообщает Алисе по открытому аутентичному каналу связи базисы, в которых он производил измерения, но не результат измерений. Оставляются лишь исходы событий, в которых базисы измерения и приготовления совпадали, то есть те, в которых измеренное и передаваемое состояния должны быть идентичны (при отсутствии вторжения в квантовый канал связи). Затем Алиса сообщает Бобу, какие именно и в какие моменты времени состояния Белла она посылала. Боб оценивает уровень возмущения этих состояний в соответствии с таблицей, которая для состояний (5) строится по правилу (4).

Результат проецирования проверочных состояний в факторизованные, принадлежащие трем взаимно-несмещенным базисам (2)

Измерение		Приготовление: проверочные состояния			
базис	состояние	$\|\Phi^+\rangle$	$\|\Phi^-\rangle$	$\|\Psi^+\rangle$	$\|\Psi^-\rangle$
I	$\|H_1\rangle\|H_2\rangle$	1/2	1/2	0	0
	$\|H_1\rangle\|V_2\rangle$	0	0	1/2	1/2
	$\|V_1\rangle\|H_2\rangle$	0	0	1/2	1/2
	$\|V_1\rangle\|V_2\rangle$	1/2	1/2	0	0
II	$\|D_1\rangle\|D_2\rangle$	1/2	0	1/2	0
	$\|D_1\rangle\|A_2\rangle$	0	1/2	0	1/2
	$\|A_1\rangle\|D_2\rangle$	0	1/2	0	1/2
	$\|A_1\rangle\|A_2\rangle$	1/2	0	1/2	0
III	$\|R_1\rangle\|R_2\rangle$	0	1/2	1/2	0
	$\|R_1\rangle\|L_2\rangle$	1/2	0	0	1/2
	$\|L_1\rangle\|R_2\rangle$	1/2	0	0	1/2
	$\|L_1\rangle\|L_2\rangle$	0	1/2	1/2	0

Действительно, рассмотрим результат проецирования (4) на примере посылки синглетного, $|\Psi^-\rangle$, и триплетного, $|\Phi^+\rangle$, состояний и последующего их проецирования в пары состояний из третьего базиса:

$$|\langle\Psi^-|R_1\rangle|R_2\rangle|^2 = \frac{1}{8}|(\langle H_1|\langle V_2| - \langle V_1|\langle H_2|)\times$$

$$\times(|H_1\rangle + i|V_1\rangle)(|H_2\rangle + i|V_2\rangle)|^2 = 0, \qquad (6а)$$

$$|\langle\Phi^+|R_1\rangle|L_2\rangle|^2 = \frac{1}{8}|(\langle H_1|\langle V_2| - \langle V_1|\langle H_2|)\times$$

$$\times(|H_1\rangle + i|V_1\rangle)(|H_2\rangle - i|V_2\rangle)|^2 = \frac{1}{2}. \qquad (6б)$$

Заметим, что, согласно таблице, результат измерения синглетного состояния $|\Psi^-\rangle$ не зависит от выбора базиса, что является следствием его инвариантности. Другим примечательным результатом, следующим из таблицы, является то, что в любом базисе некоторые проверочные состояния не дают отсчета с единичной вероятностью! Следовательно, срабатывание пары детекторов в таком случае вызвано только несанкционированным вторжением в канал связи (или технической ошибкой). Отсутствие совпадений фотоотсчетов при определенных проекционных измерениях максимально перепутанных состояний – проявление хорошо известного в квантовой оптике эффекта двухфотонной интерференции [14].

Состояния (5) используются как проверочные. Это значит, что измерительная станция по-прежнему проецирует принимаемые состояния случайно в один из базисов (2). Использование состояний типа (5) в качестве информационных повлекло бы за собой существенное усложнение измерительной схемы, поскольку потребовало построение проектора на перепутанные состояния. Это нереалистично на современном уровне развития экспериментальной техники.

3. Анализ подслушивания и скорости генерации ключа. Поскольку общее число и вид информационных состояний не изменился по сравнению со случаем расширенного протокола BB84 на куквартах [11], все оценки уровня секретности, полученные в [12], остаются в силе. Изменения касаются лишь чувствительности протокола к внешним атакам и скорости генерации ключа.

3.1. *Прием-пересылка.* Предположим, что злоумышленник (Ева) производит проекционное измерение передаваемого состояния в одном из базисов, использующихся легитимными пользователями. Результат измерения перепосылается Бобу. Тогда, в случае, если базисы Евы и Боба совпадают (с вероятностью $P = 1/3$), вносимое возмущение минимально и равно нулю. Если же базисы не совпадают, ошибка на информационных состояниях (2) будет составлять 3/4, а на проверочных (5) – 1/2. Для протокола на трех базисах вероятность выбора Евой неправильного базиса равна 2/3, и в итоге среднее возмущение информационных состояний составит $D_{\text{inf}} = 2/3 \times 3/4 = 50\%$, а проверочных $D_{\text{test}} = 2/3 \times 1/2 = 33.33\%$. Таким образом, вероятность возмущения в протоколе

на проверочных состояниях в $D_{\rm inf}/D_{\rm test} = 1.5$ меньше, чем в оригинальном.

3.2. *Оптимальная атака.* Если Ева производит так называемую оптимальную атаку (см., например, [12, 15]), она связывает передаваемое состояние $|i\rangle$ со своей вспомогательной системой $|E\rangle$ унитарным преобразованием

$$U(|i\rangle \otimes |E\rangle) \to \sqrt{1-D}|i\rangle \otimes |E_{i,i}\rangle + \\ + \sum_{j=1}^{3} \sqrt{\frac{D}{3}}|i+j\rangle \otimes |E_{i,i+j}\rangle, \qquad (7)$$

где $|j\rangle$ $(j = 0, \ldots 4)$ – ортонормированные векторы одного из базисов (2). Вероятность измерения состояния $|\psi\rangle$ после проекционного измерения Боба составляет

$$F = \langle\psi|\rho^{(i)}_{B,\rm out}|\psi\rangle, \qquad (8)$$

где $\rho^{(i)}_{B,\rm out} = {\rm Tr}_E[U(|i\rangle\otimes|E\rangle)(\langle E|\otimes\langle i|U^+)]$ – редуцированная матрица плотности состояния $|i\rangle$, посланного Алисой и полученного Бобом после операции оптимального подслушивания. В результате процедуры сравнения базисов вероятность правильного измерения составляет $F = 1-D$, а суммарная величина возмущения $D_{\rm inf} = D$. В случае, когда Алиса посылала проверочное состояние, в среднем Боб зарегистрирует ошибку $D_{\rm test} = 2/3D$ – результат, соответствующий атаке прием-пересылка!

3.3. *Равномерная деполяризация.* Отдельной задачей является построение универсального унитарного оператора, действие которого проявляется в статистическом "рассеивании" однофотонных поляризационных состояний из (2) равномерно по сфере Пуанкаре. Такой оператор отвечал бы за модель естественной деполяризации и описывал поляризационное возмущение состояний как при распространении в свободном пространстве, так и в оптических волокнах. Построить такой универсальный оператор пока не представляется возможным.

3.4. *Скорость генерации ключа.* Предположим, что за время сеанса связи передано N состояний, а возмущение в канале связи оценивается по выборке из M состояний. Если проверочные состояния не используются, то в обычном протоколе [11, 12] после процедуры сравнения базисов и оценки возмущения у легитимных пользователей остается $n = N/3 - M$ квартов информации. Для обсуждаемого протокола на проверочных состояниях число доступных квартов оказывается больше $n' = (N-M)/3 > n$! Если же оценку возмущения в "оригинальном" протоколе производить по доле q, оставшихся *после* сравнения базисов квартов $m = q(N/3)$ (и $m' \equiv M = qN$ для протокола на проверочных состояниях), то число доступных квартов в обоих протоколах будет совпадать $n = (N/3)(1-q)$. Однако в этом случае число событий, по которым оценивается возмущение в канале связи, будет больше для протокола на проверочных состояниях $m'/m = 3$. Таким образом, проигрыш в вероятности обнаружить ошибку (пункты 3.1 и 3.2) с двукратным запасом компенсируется увеличением скорости генерации ключа: $m'/m = 2D_{\rm inf}/D_{\rm test}$. Параметр q при этом остается в руках экспериментатора и выбирается, исходя из конкретного уровня технических (или иных) ошибок, присутствующих в сыром ключе.

4. Заключение. Представляется, что с практической точки зрения, предпочтение следует отдавать протоколу на факторизованных состояниях бифотонов-куквартов, принадлежащих трем базисам (2) [11, 12]. Такие состояния легко приготовить и качество их приготовления – в силу простоты и доступности всех требуемых поляризационных элементов – оказывается весьма велико: вплоть до 99.9%. Простая измерительная схема, апробированная в [7, 11], позволяет выполнять детерминистические измерения всех 12 состояний. Использование полного набора из пяти взаимно-несмещенных базисов, включающего восемь перепутанных состояний (3), нецелесообразно, поскольку, прежде всего, требует построения сложной проекционной схемы. Обсуждаемое в данной работе компромиссное решение – вовлечение четырех (или менее) максимально-перепутанных состояний в качестве проверочных, при сохранении 12 факторизованных состояний (2) в качестве информационных, позволяет обойтись простой измерительной схемой и лишь слегка усложняет приготовительную часть системы КРК [7, 11]. При этом растет скорость генерации ключа при *сохранении* уровня секретности – результат, неожиданный для схем, использующих состояния высокой размерности, когда платой за рост скорости генерации ключа служит уменьшение секретности [13].

Авторы выражают благодарность С.Н. Молоткову за обсуждение результатов.

Работа поддержана грантами Российского фонда фундаментальных исследований # 08-02-12091-офи, # 07-02-91581-АСП-а, # 06-02-16769-а, # 08-02-00559, а также грантом поддержки ведущих научных школ # НШ-796.2008.2.

1. M.N. Soskin, V.N. Gorshkov, M.V. Vasnetsov et al., Phys. Rev. A **56**, 4065 (1997); A. Vaziri, J-W. Pan, T. Jennewein et al., Phys. Rev. Lett. **91**, 227902 (2003); A. Vaziri, G. Weihs, and A. Zeilinger, Phys. Rev. Lett.

89, 240401 (2002); D. Collins, N. Gisin, N. Linden et al., Phys. Rev. Lett. **88**, 040404 (2002); N. Langford, R. B. Dalton, M. D. Harvey, and J. L. O'Brien, Phys. Rev. Lett. **93**, 053601 (2004).

2. С. П. Кулик, С. Н. Молотков, А. П. Маккавеев, Письма в ЖЭТФ **85**, 354 (2007).
3. R. T. Thew, S. Tanzilini, A. Acin et al., Quant. Inf. Comp. **4**, 93 (2004); R. T. Thew, A. Acin, H. Zbinden, and N. Gisin, Phys. Rev. Lett. **93**, 010503 (2004).
4. M. N. O'Sullivan-Hale, I. A. Khan, R. W. Boyd, and J. C. Howell, Phys. Rev. Lett. **94**, 220501 (2005); L. Neves, G. Lima, J. G. Aguirre Gomez et al., Phys. Rev. Lett. **94**, 100501 (2005); G. M. D'Ariano, P. Mataloni, and M. F. Sacchi, Phys. Rev. A **71**, 062337 (2005).
5. A. Lamas-Linares, J. C. Howell, and D. Bouwmeester, Nature **412**, 887 (2001); J. C. Howell, A. Lamas-Linares, and D. Bouwmeester, Phys. Rev. Lett. **88**, 030401 (2002).
6. H. Riedmatten, I. Marcikic, V. Scarani et al., Phys. Rev. A **69**, 050304(R) (2004).
7. Ю. И. Богданов, Р. Ф. Галеев, С. П. Кулик и др., Письма в ЖЭТФ **82**, 180 (2005); G. A. Maslennikov, S. P. Kulik, E. V. Moreva, and S. S. Straupe, Phys. Rev. Lett. **97**, 023602 (2006); Yu. I. Bogdanov, R. F. Galeyev, G. A. Maslennikov, and E. V. Moreva, Phys. Rev. A **73**, 063810 (2006).
8. H. Zbinden and H. Weinfurter, частное сообщение.
9. L. Vaidman and N. Yoran, Phys. Rev. A **59**, 116 (1999); N. Lutkenhaus, J. Calsamiglia, and K.-A. Suominen, Phys. Rev. A **59**, 3295 (1999).
10. H. Bechmann-Pasquinucci and A. Peres, Phys. Rev. Lett. **85**, 3313 (2000).
11. С. П. Кулик, Е. В. Морева, Г. А. Масленников, ЖЭТФ **129**, 1 (2006).
12. С. П. Кулик, А. П. Шурупов, ЖЭТФ **131**, 842 (2007).
13. H. Bechmann-Pasquinucci and W. Tittel, Phys. Rev. A **61**, 062308 (2000).
14. Y. H. Shih and C. O. Alley, Phys. Rev. Lett. **61**, 2921 (1988); Д. Н. Клышко, ЖЭТФ **111**, 1955 (1997).
15. M. Bourennane, A. Karlsson, and G. Bjork, Phys. Rev. A **64**, 012306 (2001); F. Caruso, H. Bechmann-Pasquinucci, and C. Machiavello, Phys. Rev. A **72**, 032340 (2005).