ЖЭТФ, 2006, том 129, вып. 5, стр. 814–829

К ВОПРОСУ О ПРАКТИЧЕСКОЙ КВАНТОВОЙ КРИПТОГРАФИИ НА МНОГОУРОВНЕВЫХ СИСТЕМАХ

С. П. Кулик [*a], ***Г. А. Масленников*** [b], ***Е. В. Морева*** [c]

[a] *Московский государственный университет им. М. В. Ломоносова*
119992, Москва, Россия

[b] *Национальный университет Сингапура*
119077, Сингапур, Республика Сингапур

[c] *Московский инженерно-физический институт (государственный университет)*
115409, Москва, Россия

Поступила в редакцию 14 октября 2005 г.

Рассматриваются физические принципы работы протокола квантового распределения ключа на четырехуровневых оптических системах. Носителями квантовой информации выступают поляризационные состояния, получаемые при частотно-невырожденном коллинеарном спонтанном параметрическом рассеянии света. Особенностью схемы является то, что генерация всех необходимых неортогональных состояний осуществляется при помощи одного нелинейного кристалла. Измерение всех состояний из выбранного базиса происходит детерминистически. Обсуждаются результаты первых экспериментов по преобразованию базисных поляризационных состояний четырехуровневых оптических систем.

PACS: 03.67.Hk, 42.25.Ja, 42.50.Dv

1. ВВЕДЕНИЕ

Основными проблемами классической криптографии являются аутентификация и распределение ключа. Первая проблема связана с распознаванием легитимных пользователей друг другом. Вторая проблема призвана обеспечить наличие у сторон идентичного секретного ключа, который в дальнейшем используется для кодирования и декодирования информации. Безусловно секретным (по Шеннону) является такой ключ, который представляет собой набор случайных (двоичных) символов, длина которого не меньше длины передаваемого сообщения и который используется лишь один раз. Однако снабжать каждое сообщение новым секретным ключом представляется трудоемкой и дорогостоящей задачей. На сегодняшний день известны способы частичного решения проблемы распределения ключа. Некоторые из них связаны с так называемыми двухключевыми или асимметричными протоколами. Они принадлежат к классу вычислительно стойких, т. е. когда раскрытие ключа становится экономически невыгодным или когда вычисление требует больше времени, чем время «ценности» сообщения. Примером асимметричных способов шифрования служит метод, предложенный в 1976 г. У. Диффи и М. Хеллманом [1]. Другим решением проблемы распределения ключа является использование квантовых носителей информации — квантовая криптография. На основе квантовых состояний, в принципе, можно генерировать безусловно секретные ключи и легко их менять. Однако заметим, что квантовое распределение ключа не решает проблему аутентификации.

Квантовая криптография [2] является, по всей видимости, единственной ветвью науки о квантовой информации и квантовой связи [3], реализованной на приборном уровне. Безусловная секретность ключа, распределенного между легитимными пользователями при помощи квантовых систем, определяется теоремой о запрете клонирования неизвестного квантового состояния [4]. В известных на сегодняшний день квантовых криптографических системах используется кодирование информации в неортого-

*E-mail: skulik@qopt.phys.msu.su

нальных состояниях двухуровневых систем, или кубитах, наиболее известными из которых являются протокол на двух ($B92$) [5], четырех [6] и шести [7] состояниях. Вместе с тем в литературе рассматривается множество других способов реализации секретных сообщений на основе квантовых состояний, например, протокол на перепутанных состояниях [8, 9]. Однако на практике секретность квантового распределения ключа (КРК) ограничена рядом факторов. Это ошибки и потери, возникающие в канале связи при передаче, отличие приготовленных состояний от идеальных, погрешности системы измерения (например, вызванные шумовыми отсчетами фотодетекторов) и т. д. Именно перечисленные ошибки в основном ограничивают длину канала связи, в пределах которой гарантирована секретность КРК. Кроме очевидного технологического способа преодоления этих препятствий, заключающегося в совершенствовании всех узлов квантовых криптографических систем, существует и другой — физический. Он основан на использовании состояний более высокой размерности гильбертова пространства. Конкретной реализации семейства квантовых состояний в четырехмерном пространстве, а также его измерению и посвящена настоящая работа.

2. КВАНТОВОЕ РАСПРЕДЕЛЕНИЕ КЛЮЧА ПРИ ПОМОЩИ СОСТОЯНИЙ С РАЗМЕРНОСТЬЮ $D > 2$

Впервые идея протокола КРК на состояниях размерности $D > 2$ была высказана в работе [10]. Предложенный Пересом и Бечманн-Пасквинучи протокол КРК является обобщением на трехуровневые[1)] системы известного кубитового протокола $BB84$ [6]. Согласно работе [10], квантовые состояния, в которых кодируется информация, принадлежат четырем взаимно несмещенным базисам, каждый из которых является ортонормированным и состоит из тройки векторов. По определению, векторы, принадлежащие семейству взаимно несмещенных базисов, удовлетворяют следующим условиям:

$$|\langle e_i|e_j\rangle|^2 = \frac{1}{D}\,, \tag{1а}$$

если векторы $|e_i\rangle, |e_j\rangle$ принадлежат разным базисам,

$$|\langle e_i|e_j\rangle|^2 = 0, \quad i \neq j, \quad |\langle e_i|e_i\rangle|^2 = 1, \tag{1б}$$

если векторы, принадлежат одному базису. Здесь D — размерность гильбертова пространства.

Можно показать [11], что существует набор $M = D + 1$ взаимно несмещенных базисов, если только размерность пространства D удовлетворяет условию

$$D = p^k,$$

где p — простое число, а k — целое. Так, для $D = 3$, 4 число базисов составляет[2)]

$$M_3 = 4, \quad M_4 = 5.$$

Полное число используемых состояний равно $m = MD$; для трехуровневых систем протокол строится на 12 состояниях, для четырехуровневых систем — на 20 состояниях.

С геометрической точки зрения среди векторов, принадлежащих взаимно несмещенным базисам, нет выделенных: проекция заданного вектора на любой другой (неортогональный ему) имеет одну и ту же величину. Именно это свойство и используется при построении протоколов КРК.

Распределение ключа при помощи квантовых состояний высокой размерности по сути не отличается от сценария обычных кубитовых протоколов. Случайная строка символов соответствующей размерности (например, 0, 1, 2, 3, если $D = 4$) кодируется в последовательности m неортогональных состояний из M случайно выбранных (но заданных) базисов. Выбранные состояния последовательно посылаются через квантовый канал связи от одного легитимного пользователя другому. При этом посылающая сторона запоминает (но не сообщает) базис, к которому принадлежит то или иное отправляемое состояние. Принимающая сторона случайно выбирает базис, в котором проводится измерение полученных состояний, и запоминает результат. По окончании сеанса связи две стороны по открытому каналу[3)] обмениваются информацией о базисах, в которых были закодированы (или измерены) состояния. Если базисы совпадают, то по результату измерения однозначно восстанавливается исходное состояние в данной посылке. Если базисы не совпадают, то результат

[1)] Определение D-уровневой системы, относящееся к энергетическим состояниям, вообще говоря, здесь не вполне уместно, поскольку никаких реальных «уровней» в этих системах нет. Однако в настоящее время эта терминология общепринята, и мы будем ее придерживаться.

[2)] Соответствующие базисные квантовые состояния называются кутритами (qutrits) и куквартами (ququarts).

[3)] Под открытым каналом связи понимается такой, когда передаваемую по нему информацию можно извлечь, но нельзя изменить.

измерения не учитывается при формировании ключа. В идеальном случае, когда не возникает ошибок при (де)кодировании и передаче информации, после отбрасывания результатов, соответствующих несовпадающим базисам, у пользователей остаются идентичные строки символов, которые и служат так называемым сырым ключом. При наличии вмешательства в квантовый канал передаваемое состояние искажается (как следствие теоремы о запрете клонирования неизвестного состояния). Наличие ошибок, в том числе вызванных попытками подслушивания, обнаруживается легитимными пользователями при помощи специальных протоколов, например, путем раскрытия частей ключа и сравнения их по открытому каналу. При этом раскрытая часть выводится из итогового ключа, длина которого, соответственно, уменьшается. В дальнейшем ключ сжимается — эти этапы обработки ключа являются классическими, поскольку стороны оперируют с классической строкой битов (или дитов), однако сами процедуры чистки ключа зависят от типа протокола. Отметим, что для каждого протокола КРК существует максимальный уровень ошибок, исправление которых гарантирует секретность ключа. Так, для протокола *BB*84 этот уровень составляет 11 %.

Впоследствии итоговым ключом кодируется/декодируется сообщение. Простота процедуры КРК позволяет сопровождать каждое последующее сообщение собственным ключом. Тем самым выполняются основные требования к безусловной секретности передаваемого сообщения: длина ключа должна быть не меньше длины сообщения и ключ должен использоваться только один раз.

Обсуждению анализа секретности протокола КРК на системах высокой размерности посвящен ряд работ [12–17]. При простейшей стратегии подслушивания перехват–пересылка, злоумышленник поступает так же, как и легитимная принимающая сторона. Он перехватывает квантовые состояния, проводит измерение в случайном базисе, а затем пересылает в квантовый канал то состояние, которое получилось в результате измерения. Таким образом, в случае, если злоумышленник правильно угадал базис, он извлекает всю информацию о посланном состоянии, пересылает его и не вносит возмущения. Однако, если базис им угадан неправильно, возмущение, вносимое такой стратегией, статистически обнаружимо. Анализируются ситуации, когда принимающая легитимная сторона правильно выбрала базис, но, вместе с тем, состояние оказывается искаженным вследствие неправильного выбора базиса (и пересылкой возмущенного состояния) подслушивателем. Для квантовых систем высокой размерности такой анализ был сделан в работе [13].

Если перехватываются все или даже часть состояний, то возникает вероятность ошибки в передаче. Эта величина служит важной характеристикой протокола и в идеальном случае определяется только возмущением, вносимым подслушивателем:

$$E_B = \eta \left(1 - \frac{1}{M}\right)\left(1 - \frac{1}{D}\right). \qquad (2)$$

Второй множитель в формуле (2) определяет вероятность неправильного угадывания базиса из M возможных, третий — вероятность детектирования неправильного состояния из D возможных. Здесь η — доля перехваченных злоумышленником состояний. Например, в случае размерности пространства $D = 4$ злоумышленник неправильно угадывает базис в $4/5$, или в 80 % случаев. Поскольку после выполнения измерения он приготавливает и пересылает случайное состояние, вероятность ошибки у второго легитимного пользователя оказывается $3/4$ (75 %) даже при правильно выбранном базисе (в отличие безошибочного результата при отсутствии подслушивания). В среднем подслушиватель извлекает $I_E = 1/5$ полезной информации (если измерять ее в квартах[4)]); это приводит к уровню ошибок в передаче (error rate)

$$E_B = \frac{3}{4} \cdot \frac{4}{5} = \frac{3}{5}.$$

Вывод о наличии возмущения в квантовом канале связи, которое неизбежно связывается с попыткой подслушивания, делается после процедуры сравнения базисов.

Одним из критериев эффективного подслушивания является максимизация отношения

$$Q = \frac{I_E}{E_B}.$$

Атака на ключ тем эффективнее, чем больше это отношение [10]. Соответственно, защищенность протокола по отношению к определенному типу атаки на ключ определяется степенью малости величины Q. В табл. 1 приведены значения E_B и Q для некоторых протоколов КРК: *BB*84 [6], протокола на основе 6 состояний кубитов [7], кутритов [10] и куквартов [12]

[4)] Связь между информационным содержанием, выраженным в битах и дитах, дается соотношением $I_{dit} = I_{bit} \log_D 2$, так что кодировка информации в квартах в два раза плотнее, чем в битах.

для атак типа «перехват–пересылка». Видно, что использование систем более высокой размерности (в данном случае кутритов и куквартов) увеличивает стойкость КРК.

Важно отметить, что с увеличением размерности пространства используемых для передачи состояний увеличивается доля не включаемых в рассмотрение результатов измерений. Действительно, поскольку принимающая сторона случайно выбирает базис, в котором проводится измерение, вероятность детерминированного результата с однозначным исходом равна $1/M$. Доля отбрасываемых состояний, которые не участвуют в формировании сырого ключа, составляет

$$T = 1 - \frac{1}{M}\,.$$

Соответственно, укорачивается итоговый ключ — это плата за увеличение секретности протокола. Сравнение величин T для разных протоколов КРК также приводится в табл. 1. Компромиссное решение было предложено в работе [12]. Повышение секретности предлагалось обеспечивать, используя квантовые состояния более высокой размерности гильбертова пространства, а скорость формирования ключа повысить за счет вовлечения не всех возможных взаимно несмещенных базисов. При этом, как было показано в работе [12], небольшое увеличение значения Q по сравнению со случаем использования всех M базисов оправдано, прежде всего, с практической точки зрения значительным ростом скорости генерации сырого ключа.

В работах [12–17] анализируются и другие стратегии подслушивания, например, атаки в промежуточном базисе, атаки с использованием универсальной квантовой клонирующей машины (УККМ)[5)]. В работе [14] рассматриваются два типа атак: индивидуальные, когда подслушиватель перехватывает отдельные кудиты и когерентные, когда он воздействует на набор кудитов одновременно. Для индивидуальных атак допускается оптимальная стратегия применения квантовой клонирующей машины. Показывается, что увеличение размерности пространства приводит к уменьшению достижимой подслушивателем информации при заданном уровне ошибок на принимающей стороне. Эта тенденция сохраняется как при использовании состояний из всех $D+1$ базисов, так и для двух базисов. В работе [13] оценивается максимальная эффективная скорость передачи ключа в зависимости от размерности D и ошибки, возникающей на принимающей стороне при использовании УККМ.

[5)] При действии УККМ, впервые рассмотренной в [18], подслушиватель создает два состояния, которые максимально близки к перехватываемому, насколько это позволяет теорема о запрете клонирования. Одна «копия» остается у него, а вторая пересылается принимающей стороне. Затем при объявлении легитимными пользователями базисов по открытому каналу, подслушиватель выполняет измерения в правильном базисе, поэтому в среднем у него окажется такое же количество информации. Однако, в силу неточности копирования, подслушиватель возмущает передаваемые состояния, что обнаруживается легитимными пользователями при статистическом анализе результатов измерений.

3. ОПТИЧЕСКИЕ СОСТОЯНИЯ С РАЗМЕРНОСТЬЮ $D > 2$ В ЭКСПЕРИМЕНТЕ

На сегодняшний день известно несколько физических процессов, на основе которых удается построить оптические состояния с размерностью $D > 2$. Как правило, они основаны на эффекте параметрического рассеяния света (спонтанного (СПР) или вынужденного). Все эти системы обладают рядом достоинств и недостатков, но в целом можно утверждать, что процедуры контроля за основными этапами эволюции квантовых состояний (генерацией, передачей и измерением) сравнительно ненадежны.

3.1. Пространственные моды пучков светового поля

Естественным базисом для представления пространственной структуры пучка света служит семейство гауссовых мод (Гаусса – Эрмита и Гаусса – Лягерра). Иногда в таких случаях говорят о топологическом заряде и орбитальном угловом моменте фотонов, который определяется модами Гаусса – Лягерра в цилиндрических координатах [19]. Эти моды описывают спиральную структуру волнового фронта и фазовые сингулярности. Помещая в пучок специально изготовленные голограммы, можно выделять те или иные моды, тем самым анализируя пространственную структуру или модовый состав пучка. Если же расположить голограммы в пучках с сильной пространственной корреляцией, как это имеет место при СПР, то удается приготовить перепутанные состояния — суперпозиции нескольких коррелированных гауссовых мод. В работах [20, 21] сообщалось о генерации перепутанных кутритов вида

$$\Psi = \frac{1}{\sqrt{3}}\left\{|0_s, 0_i\rangle + |1_s, 1_i\rangle + |2_s, 2_i\rangle\right\}, \qquad (3)$$

где вектор $|m_s, n_i\rangle$ обозначает состояние с фотоном $s(i)$ на одном из трех выходов анализатора простран-

Таблица 1

	Протокол				
	Кубиты ($BB84$), 4 состояния	Кубиты, 6 состояний	Кутриты, 12 состояний	Кукварты, 20 состояний	Кукварты, 8 состояний
D	2	2	3	4	4
M	2	3	4	5	2
E_B	1/4	1/3	1/2	3/5	3/8
$Q = I_B/E_B$	2	1	1/2	1/3	4/3
T	1/2	1/3	1/4	1/5	1/2

ственной структуры пучка. На основе состояний (3) были проверены неравенства типа неравенства Белла в трехмерном случае [22]. В работе [23] был развит метод измерения таких состояний при помощи набора голограмм с заданным расположением фазовых дислокаций.

В настоящее время активно развивается технология изготовления адаптивных голограмм. Возможно, в скором времени данный метод приготовления перепутанных состояний с размерностью $D > 2$ станет одним из основных, поскольку он обеспечит приготовление и измерение широкого набора состояний такого типа с изменяемыми комплексными амплитудами.

3.2. Бифотоны в многоплечевом интерферометре

Если сигнальный и холостой фотоны, составляющие бифотон, независимо направить в интерферометр, имеющий три плеча разной длины, а затем выбрать только такие моменты времени, в которые оба фотона одновременно появляются на выходе, возникает суперпозиция вида [24, 25]:

$$\Psi = c_s|1_s, 1_s\rangle + c_m|1_m, 1_m\rangle + c_l|1_l, 1_l\rangle. \qquad (4)$$

Вектор $|1_s, 1_s\rangle$ обозначает состояние, при котором оба фотона прошли через короткие плечи, $|1_m, 1_m\rangle$ — через средние плечи и $|1_l, 1_l\rangle$ — через длинные плечи. Перепутанные состояния вида (4) являются прямым обобщением на многомерный случай тех, которые были получены в известных экспериментах Фрэнсона с кубитами [26]. Модули амплитуд вероятностей $c_{s,m,l}$ можно регулировать, задавая коэффициенты отражения входных светоделителей, а относительные фазы — с помощью задержек, вводимых в то или иное плечо. Однако, если фазовые задержки просто регулируются при помощи соответствующих модуляторов, модули коэффициентов пропускания постоянны для данного интерферометра — это основной недостаток при работе с кудитами на основе многоплечевых интерферометров.

3.3. Пространственные моды бифотонного поля при спонтанном параметрическом рассеянии света

В последнее время появилось несколько экспериментальных работ, в которых для приготовления многоуровневой системы используется эффект поперечной группировки бифотонного поля. В этих экспериментах на пути сигнальных и/или холостых фотонов независимо помещаются наборы диафрагм [27] или щелей [28], выделяющих определенную конфигурацию пространственных мод. Приготавливаются состояния вида

$$\Psi = \frac{1}{\sqrt{D}} \sum_{l=-l_D}^{l_D} \exp\{i\alpha_l\}|l_s\rangle|l_i\rangle, \qquad (5)$$

где D — число диафрагм (щелей), задающее размерность пространства, а вектор $|l_{s,i}\rangle$ обозначает, что сигнальный (s) или холостой (i) фотон прошел через диафрагму с номером l.

Здесь же упомянем и так называемые гиперперепутанные состояния, когда перепутывание в составной квантовой системе возникает больше чем по одному параметру — новый объект в экспериментальной квантовой информации. В связи в этим следует отметить работу [29], в которой предло-

жен способ генерации состояний на основе частотно-вырожденного неколлинеарного СПР вида

$$\Psi = \frac{1}{\sqrt{2}}\left\{c_1|H_{a_1}, H_{b_2}\rangle + c_2|V_{a_1}, V_{b_2}\rangle + \right.$$
$$\left. + c_3|H_{a_2}, H_{b_1}\rangle + c_4|V_{a_2}, V_{b_1}\rangle\right\}. \quad (6)$$

Здесь, кроме пространственных корреляций вида $|a_1, b_2\rangle \pm |b_1, a_2\rangle$ (пара фотонов в модах a_1, b_2 или пара фотонов в модах b_1, a_2) имеются и поляризационные компоненты, позволяющие получать состояния куквартов (6) с $D = 4$.

3.4. Четырехфотонные поляризационные состояния

Квантовые состояния с размерностью $D = 3$ можно приготовить на основе вынужденного параметрического рассеяния, когда на выходе кристалла, обладающего квадратичной восприимчивостью, образуются четверки фотонов [30]. При двукратном прохождении лазерного импульса через нелинейный кристалл и согласовании групповых задержек, возникающих как между фотонами в паре, так и между отдельными парами, образуется перепутанное поляризационное состояние в паре пространственных мод:

$$\Psi = b_1|(2H)_1, (2V)_2\rangle +$$
$$+ b_2|(HV)_1, (|VH\rangle_2)\rangle + b_3|(2V)_1, (2H)_2\rangle. \quad (7)$$

Символ $|(2H)_1, (2V)_2\rangle$ означает, что два фотона с горизонтальной поляризацией находятся в пространственной моде «1», а два фотона с вертикальной поляризацией — в моде «2». Такое состояние представляет собой кутрит. Достоинством такого способа приготовления состояния с $D = 3$ является возможность манипуляции с перепутанными трехуровневыми системами. Так, в работе [31] были проверены неравенства типа неравенств Белла для перепутанных систем со спином 1 [22, 32, 33]. Однако существенным недостатком приготовления такого класса состояний является сложность управления амплитудами $b_{1,2,3}$.

3.5. Бифотоны, генерируемые последовательностью лазерных импульсов

Для этого способа достигнуто рекордное значение размерности пространства оптической квантовой системы $D = 21$ [34]. Последовательность из D когерентных лазерных импульсов генерирует бифотоны в частотно-вырожденном и коллинеарном режимах. Между импульсами устанавливаются фиксированные фазовые соотношения. Интенсивность лазерного излучения подобрана так, чтобы бифотон мог родиться не более чем от одного импульса серии. В этом случае возникает суперпозиция двухфотонных состояний в разные моменты времени, определяемые периодом следования импульсов накачки:

$$\Psi = \sum_{j=1}^{D} c_j \exp\{i\phi_j\}|j_A, j_B\rangle, \quad (8)$$

где член $c_j \exp\{i\phi_j\}|j_A, j_B\rangle$ означает, что бифотон родился от импульса (или во временном окне) j с амплитудой c_j и фазой ϕ_j. По-видимому, такой метод приготовления многоуровневых состояний является наиболее эффективным, поскольку и амплитуды, и относительные фазы базисных состояний в (8) легко меняются при помощи соответствующих амплитудных и фазовых модуляторов. Следовательно, таким образом можно приготавливать произвольное состояние кудита! Однако проблему представляет измерение состояния, поскольку для восстановления всех амплитуд и фаз нужно использовать стабильный D-плечевой интерферометр и соответствующее число фотодетекторов, объединенных схемами парных совпадений.

Кроме перечисленных методов приготовления D-уровневых систем существует еще один, основанный на поляризационных состояниях однопучкового спонтанного параметрического рассеяния света.

4. БИФОТОНЫ КАК ЧЕТЫРЕХУРОВНЕВЫЕ СИСТЕМЫ

Одним из объектов, при помощи которых можно приготавливать квантовые состояния размерности $D = 2, 3, 4$, является бифотонное поле, рождающееся в процессе СПР света в средах без центра инверсии [35]. На сегодняшний день СПР представляется простым и эффективным методом генерации полей в неклассическом состоянии. В стационарных условиях часто́ты полей в двух модах (s, i) связаны с частотой поля накачки (p) соотношением

$$\omega_s + \omega_i = \omega_p, \quad (9)$$

а направления распространения задаются законом дисперсии нелинейного кристалла и его геометрическими размерами.

Как правило, используются такие режимы генерации СПР, когда поперечными размерами кристаллов можно пренебречь.

В первом порядке теории возмущений по амплитуде накачки вектор состояния бифотонного поля имеет следующую структуру:

$$\Psi = \left(1 + \frac{1}{2}\sum_{\mathbf{k}_s,\mathbf{k}_i} F_{\mathbf{k}_s,\mathbf{k}_i} a^\dagger_{\mathbf{k}_s} a^\dagger_{\mathbf{k}_i}\right)|0\rangle, \qquad (10)$$

где функция $F_{\mathbf{k}_s,\mathbf{k}_i}$ — амплитуда бифотона в спектральном представлении, описывающая форму двухфотонного волнового пакета. Максимальная интенсивность полей в двух модах $\mathbf{k}_s, \mathbf{k}_i$ достигается при нулевой расстройке фазового синхронизма $|\mathbf{\Delta}| = 0$, а угловые и частотные ширины излучаемых полей определяются функцией

$$I_{s,i} \propto \sin c^2\left(\frac{|\mathbf{\Delta}|L}{2}\right), \qquad (11)$$

L — размер кристалла в направлении волны распространения накачки,

$$\mathbf{\Delta} = \mathbf{k}_s + \mathbf{k}_i - \mathbf{k}_p \qquad (12)$$

— волновая расстройка.

Феноменологически процесс СПР объясняется спонтанным распадом фотона лазерной накачки на пары фотонов, энергии и импульсы которых удовлетворяют соотношениям (9), (12). Эти законы сохранения обусловливают сильную корреляцию частот, направлений разлета и моментов рождения пары фотонов или бифотонов.

В работах [36, 37] был рассмотрен коллинеарный и вырожденный по частотам режим генерации бифотонов. Поляризационные состояния в одной пространственной моде излучения СПР были названы кутритами (qutrits), поскольку описывались суперпозицией трех базисных векторов:

$$|\Psi_3\rangle = c'_1|H,H\rangle + c'_2|H,V\rangle + c'_3|V,V\rangle. \qquad (13)$$

Здесь $c'_{1,2,3}$ — нормированные амплитуды состояний, а векторы

$$|H,H\rangle \equiv |H\rangle \otimes |H\rangle = \frac{(a^\dagger)^2}{\sqrt{2}}|vac\rangle,$$

$$|H,V\rangle \equiv |H\rangle \otimes |V\rangle = a^\dagger b^\dagger |vac\rangle,$$

$$|V,V\rangle \equiv |V\rangle \otimes |V\rangle = \frac{(b^\dagger)^2}{\sqrt{2}}|vac\rangle$$

выписаны в фоковском представлении как результат действия на вакуум операторов рождения в горизонтальной ($a^\dagger$) и вертикальной ($b^\dagger$) поляризационных модах.

В дальнейшем был разработан удобный подход, позволивший визуализировать кутриты на сфере Пуанкаре [38], сформулирован [39] и апробирован операциональный критерий ортогональности кутритов [40], развиты статистические процедуры измерения произвольных состояний кутритов [41, 42] и, наконец, их приготовления [43].

Концепция кутрита как состояния бифотонного поля основывается на вырожденности всех степеней свободы бифотона, кроме поляризационных. Снятие вырождения по какому-нибудь параметру, например, по частоте или направлению распространения, приводит к появлению дополнительного слагаемого в выражении (13):

$$|\Psi_4\rangle = c_1|H_1,H_2\rangle + c_2|H_1,V_2\rangle + c_3|V_1,H_2\rangle + c_4|V_1,V_2\rangle. \qquad (14)$$

Состояние (14) представляет собой суперпозицию четырех ортогональных векторов-состояний и называется куквартом (квантовая система с размерностью $D = 4$). В общем случае состояние (14) является нефакторизованным, т. е. оно непредставимо в виде прямого произведения поляризационных состояний отдельных сигнальных (s) и холостых (i) фотонов, составляющих бифотон:

$$\Psi_4 \neq \left(a_1|H_1\rangle + b_1|V_1\rangle\right)_s \otimes \left(a_2|H_2\rangle + b_2|V_2\rangle\right)_i. \qquad (15)$$

Процедура измерения произвольного кукварта, построенного на пространственных степенях свободы бифотонов, рассматривалась в работе [44]. Протоколы статистического восстановления куквартов, полученных за счет снятия вырождения бифотонного поля по частоте, исследовались в работе [45].

5. ПРОТОКОЛ КРК НА БИФОТОНАХ-КУКВАРТАХ

Основными физическими компонентами протокола КРК являются процедуры приготовления, передачи и измерения квантовых состояний из заданного набора. Нетрудно показать, что семейства состояний куквартов ($D = 4$), принадлежащих пя-

ти ($M = 5$) взаимно несмещенным базисам, имеют вид[6)]

$$M = 1: \ |H_1, H_2\rangle, \ |H_1, V_2\rangle, \ |V_1, H_2\rangle, \ |V_1, V_2\rangle; \quad (16а)$$

$$M = 2: \ |+45^\circ_1, +45^\circ_2\rangle, \ |+45^\circ_1, -45^\circ_2\rangle, \ |-45^\circ_1, +45^\circ_2\rangle, \ |-45^\circ_1, -45^\circ_2\rangle; \quad (16б)$$

$$M = 3: \ |R_1, R_2\rangle, \ |R_1, L_2\rangle, \ |L_1, R_2\rangle, \ |L_1, L_2\rangle; \quad (16в)$$

$$M = 4: \ |R_1, H_2\rangle + |L_1, V_2\rangle, \ |R_1, H_2\rangle - |L_1, V_2\rangle, \ |L_1, H_2\rangle + |R_1, V_2\rangle, \ |L_1, H_2\rangle - |R_1, V_2\rangle; \quad (16г)$$

$$M = 5: \ |H_1, R_2\rangle + |V_1, L_2\rangle, \ |H_1, R_2\rangle - |V_1, L_2\rangle, \ |H_1, L_2\rangle + |V_1, R_2\rangle, \ |H_1, L_2\rangle - |V_1, R_2\rangle. \quad (16д)$$

В выражениях (16) использованы следующие обозначения:

$$|\pm 45^\circ_j\rangle \equiv \frac{1}{\sqrt{2}} \left\{|H_j\rangle \pm |V_j\rangle\right\},$$

$$R_j \equiv \frac{1}{\sqrt{2}} \left\{|H_j\rangle + i|V_j\rangle\right\},$$

$$L_j \equiv \frac{1}{\sqrt{2}} \left\{|H_j\rangle - i|V_j\rangle\right\},$$

$j = 1, 2$, которые можно назвать диагональными ($|\pm 45^\circ\rangle$) и циркулярными ($|R\rangle, |L\rangle$) представлениями поляризационного кубита. Оказывается, что 12 состояний бифотонов-куквартов, составляющих первые три базиса, могут быть легко приготовлены и измерены в эксперименте.

5.1. Приготовление

Замечательной особенностью куквартов, в отличие от кутритов, составляет тот факт, что все базисные состояния первых трех базисов (16) могут быть получены из бифотонов, генерированных лишь в одном кристалле! Это утверждение лежит в основе принципиального различия между четырехуровневыми и трехуровневыми бифотонными системами. Действительно, для вырожденного по частоте однопучкового режима генерации бифотонов-кутритов имеется инвариант преобразований группы $SU(2)$; такие преобразования выполняются оптическими поляризационными элементами — фазовыми пластинками, ротаторами и проч. Это — степень поляризации, определяемая через параметры Стокса:

$$P_3 = \sqrt{\sum_{k=1}^{3} \left(\frac{1}{2}\langle S_k\rangle\right)^2}. \quad (17)$$

[6)] Используется фоковское представление состояния с обозначениями, аналогичными (6). Операторы $a^\dagger_{1,2}$, $b^\dagger_{1,2}$ действуют в двух частотных модах 1 и 2.

Для бифотонов-кутритов (6) параметры Стокса и степень поляризации выражаются через амплитуды состояний $c'_{1,2,3}$ [36, 46]:

$$\frac{\langle S_1\rangle}{2} = \frac{\langle a^\dagger a - b^\dagger b\rangle}{2} = |c'_1|^2 - |c'_3|^2,$$
$$\frac{\langle S_2\rangle}{2} = \frac{\langle a^\dagger b + ab^\dagger\rangle}{2} = \sqrt{2}\ \mathrm{Re}(c'_1{}^* c'_2 + c'_3{}^* c'_2), \quad (18)$$
$$\frac{\langle S_3\rangle}{2} = \frac{\langle -i(a^\dagger b - ab^\dagger)\rangle}{2} = \sqrt{2}\,\mathrm{Im}(c'_1{}^* c'_2 + c'_3{}^* c'_2),$$

$$P_3 = \sqrt{|c'_1|^2 - |c'_3|^2 + 2|c'_1{}^* c'_2 + c'_2 c'_3{}^*|^2}\,. \quad (19)$$

Вследствие этого базисные состояния кутритов, имеющие разные степени поляризации, невозможно преобразовать друг в друга при помощи фазовых пластинок. Например, нельзя получить состояние $|H, H\rangle$, обладающее степенью поляризации $P = 1$, из состояния $|H, V\rangle$ со степенью поляризации $P = 0$.

Поэтому для приготовления необходимого для КРК набора состояний кутритов нужно использовать как минимум два нелинейно-оптических кристалла [47]. В общем же случае требуются три нелинейных кристалла, объединенных в сложную интерферометрическую схему, обладающую всеми недостатками, присущими схемам такого рода, главные из которых — нестабильность во времени, необходимость прецизионного контроля относительной фазы состояний и высокие требования к совмещению в пространстве-времени разных компонент состояний [43].

Для двухчастотного представления поляризационного состояния поля такие базовые понятия как параметры Стокса и степень поляризации нуждаются в уточнении [48, 49]. Действительно, операторы рождения и уничтожения, через которые выражаются эти величины, формально вводятся для излучения в виде плоских волн, поэтому в двухчастотном случае они будут зависеть от времени: во временной структуре поля будут проявляться биения, которые не связаны с поляризационной структурой. Для описания поляризационных характеристик можно воспользоваться концепцией оператора квазиспина: для нескольких пространственно-временных мод компоненты оператора квазиспина представляют собой суммы соответствующих операторов по всем модам [50].

В обсуждаемом примере двухчастотного бифотонного поля запрета на преобразование базисных состояний с изменением степени поляризации больше не существует, поскольку теряет смысл понятие последней. Для осуществления таких преобразований можно использовать дихроичные поляризацион-

ные элементы, т. е. элементы, которые осуществляют заданные преобразования на каждой из двух длин волн.

Рассмотрим бифотон, который образован парой фотонов с центральными длинами волн $\lambda_1 = 702$ нм и $\lambda_2 = 605.2$ нм[7]. Преобразования между состояниями, принадлежащими первому базису в (9), достигаются с помощью обычных фазовых пластин при учете эффекта частотной дисперсии материала, из которого изготовлены пластинки. Толщины пластин l и номера интерференционных порядков для соответствующих преобразований $|V_1, V_2\rangle \to |V_1, H_2\rangle$ вычисляются из соотношений

$$\frac{(2m_1+1)\lambda_1}{2\Delta n_1} = \frac{m_2\lambda_2}{\Delta n_2}, \tag{20}$$

$$\frac{m_1\lambda_1}{\Delta n_1} = \frac{(2m_2+1)\lambda_2}{2\Delta n_2}. \tag{21}$$

Они приведены в табл. 2 для кристаллического кварца. Здесь использованы следующие обозначения: $m_{1,2}$ — интерференционные порядки для длин волн λ_1 и λ_2,

$$\Delta n_1 \equiv (n_o - n_e)_1 = 0.00906,$$

$$\Delta n_2 \equiv (n_o - n_e)_2 = 0.00896$$

— величины двулучепреломления кварца на указанных длинах волн, а вносимая пластинкой разность фаз для каждой длины волны равна

$$\delta_{1,2} = \frac{\pi l \Delta n_{1,2}}{\lambda_{1,2}}. \tag{22}$$

Состояния, принадлежащие второму и третьему базисам (16), приготавливаются аналогично. Переход к базису 2 проводится при помощи ахроматической полуволновой пластинки[8], ориентированной под углом 22.5° к вертикали; переход к базису 3 — при помощи четвертьволновой пластинки, ориентированной под углом 45°. Заметим, что состояния из базисов 5 и 6, представляющие собой суперпозиции состояний Белла, можно приготовить лишь с помощью как минимум двух кристаллов [51]. Таким образом, для реализации двух- и трехбазисного протоколов КРК на бифотонах-куквартах достаточно лишь одного кристалла, набора ахроматических фазовых пластин и пластин нулевого порядка.

[7] Спектральная ширина каждой компоненты определяется толщиной и дисперсией используемого кристалла.

[8] Такие пластинки позволяют осуществлять заданные поляризационные преобразования в широком спектральном интервале.

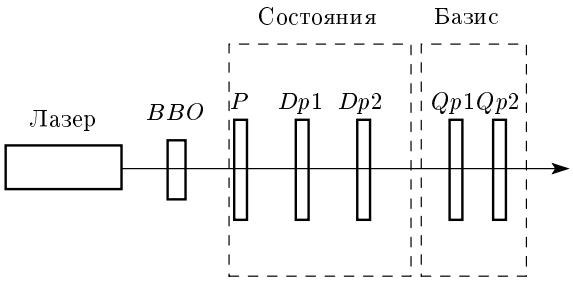

Рис. 1. Схема приготовления 12 базисных состояний в трех взаимно несмещенных базисах. BBO — нелинейный кристалл, P — ахроматическая пластинка, осуществляющая преобразование $|V_1, V_2\rangle$ в $|H_1, H_2\rangle$, $Dp1, 2$ — дихроичные фазовые пластинки, $Qp1, 2$ — пластинки, осуществляющие смену базиса

На рис. 1 показана схема приготовления всех 12 квантовых состояний, необходимых для реализации трехбазисного протокола КРК. Преобразования в пределах одного базиса осуществляются с помощью дихроичных фазовых пластин $Dp1$, $Dp2$ и ахроматической пластинки (либо пластинки нулевого порядка) P, а смена базисов проводится при помощи четверть- и полуволновых пластин $Qp1$ и $Qp2$.

5.1.1. Эксперимент по осуществлению базисных преобразований бифотонов-куквартов

Рассмотрим эксперимент по приготовлению состояния $|H_1, V_2\rangle$ из состояния $|V_1, V_2\rangle$ (рис. 2). Накачкой для СПР служит гелий-кадмиевый лазер с длиной волны 325 нм. Кристалл йодата лития ($LiIO_3$) длиной 1.5 см с синхронизмом типа I излучает пары фотонов в исходном состоянии $|V_1, V_2\rangle$. Кристалл вырезан под углом 59° к оптической оси. При такой ориентации кристалл излучает пары фотонов, так что коллинеарному синхронизму отвечают длины волн $\lambda_1 = 702$ нм и $\lambda_2 = 605.2$ нм, а спектральная ширина каждой компоненты составляет около 2 нм. Преобразование

$$|V_1, V_2\rangle \to |H_1, V_2\rangle$$

осуществляется с помощью пластинки, которая является полуволновой на длине волны λ_1 и волновой — на длине волны λ_2. При этом такая пластинка должна быть ориентирована под углом 45° к вертикали. В эксперименте использовались кварцевые пластинки толщиной 3.716 мм ($Dpo1$), 0.315 мм ($Dpo2$). Если пластинки $Dpo1$ и $Dpo2$ расположить

Таблица 2

Преобразование	Разность фаз δ_1, вносимая пластинкой	Номера порядков m_1 и m_2	Толщина пластинки l, мм
$\|V_1, V_2\rangle \to \|H_1, V_2\rangle$	$\frac{\pi}{2}$	8; 10	665
		14; 17	1135
	π	47; 51	3406
$\|V_1, V_2\rangle \to \|V_1, H_2\rangle$	π	3; 3	234
	$\frac{\pi}{2}$	26; 30	2037
		32; 37	2505

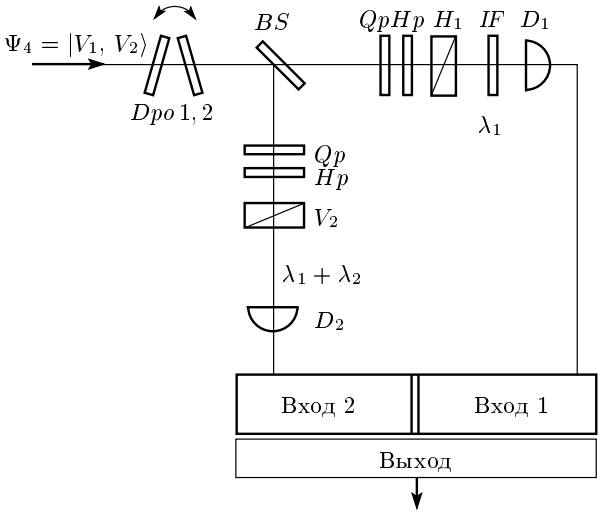

Рис. 2. Установка для преобразования базисных состояний кукварта. $Dpo1,2$ — поворачивающиеся кварцевые пластинки, BS — неполяризационный светоделитель, Qp — четвертьволновая пластинка, Hp — полуволновая пластинка, $H_1(V_2)$ — горизонтальный (вертикальный) — поляризатор, IF — интерференционный фильтр, $D_{1,2}$ — фотодетекторы

так, чтобы их оптические оси были ортогональны, то эффективная толщина составной пластинки составит 3.401 мм. Наклоняя пластины навстречу друг другу, можно добиться плавного сдвига фазы на длине волны $\lambda_1 = 702$ нм в пределах

$$1.37 \le \frac{\delta_1}{m_1} \le 1.44,$$

а на длине волны $\lambda_2 = 605.2$ нм в пределах

$$2.9 \le \frac{\delta_2}{m_2} \le 3.14.$$

При достижении нужных фазовых сдвигов результатом преобразования становится искомое состояние:

$$|H_1, V_2\rangle \equiv \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = G \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = G|V_1, V_2\rangle. \qquad (23)$$

Матрица, входящая в выражение (23), описывает поляризационные преобразования группы $SU(2)$, выполняемые над кукварами, и имеет следующую структуру [45, 46]:

$$G = \begin{pmatrix} t_1 & r_1 \\ -r_1^* & r_1^* \end{pmatrix} \otimes \begin{pmatrix} t_2 & r_2 \\ -r_2^* & r_2^* \end{pmatrix} = \\ = \begin{pmatrix} t_1 t_2 & t_1 r_2 & r_1 t_2 & r_1 r_2 \\ -t_1 r_2^* & t_1 t_2^* & -r_1 r_2^* & r_1 t_2^* \\ -r_1^* t_2 & -r_1^* r_2 & t_1^* t_2 & t_1^* r_2 \\ r_1^* r_2^* & -r_1^* t_2^* & -t_1^* r_2^* & t_1^* t_2^* \end{pmatrix}, \qquad (24)$$

с комплексными коэффициентами пропускания

$$t_j = \cos\delta_j + i \sin\delta_j \cos 2\alpha$$

и отражения

$$r_j = \sin\delta_j \sin 2\alpha$$

(индекс $j = 1, 2$ относится к фотонам с частотами ω_1 и ω_2 соответственно, α — угол между оптической осью пластины и вертикальным направлением). В силу невырожденности частот оптическая толщина пластинки

$$\delta_j = \pi(n_{ej} - n_{oj})l/\lambda_j$$

(l — геометрическая толщина пластины) различается для сигнального и холостого фотонов. При наклоне пластинок оптическая толщина изменяется,

так что, варьируя угол θ, можно плавно перестраивать фазовую задержку, вносимую пластинкой между обыкновенной и необыкновенной составляющими поля:

$$\delta_j = \frac{\pi l}{\lambda j}\left(\frac{n_{ej}^2}{\sqrt{n_{ej}^2 - \sin^2\theta}} - \frac{n_{oj}^2}{\sqrt{n_{oj}^2 - \sin^2\theta}}\right). \quad (25)$$

Для выделения нужного состояния измерительная схема была настроена на регистрацию горизонтальной поляризации в первом канале и вертикальной — во втором. Для частотной селекции бифотона со спектральными компонентами λ_1 и λ_2 в канал 1 помещался интерференционный фильтр, пропускающий излучение с центральной длиной волны 702 нм и полушириной 3 нм. При этом в канале 2 присутствовали обе спектральные компоненты. Однако, поскольку регистрации бифотона соответствует совпадение фотоотсчетов двух детекторов, такая схема однозначно выделяла данный бифотон. В каждом канале был установлен стандартный набор преобразователей, выделяющих заданную поляризацию. Такие преобразователи (или поляризационные фильтры) представляют собой последовательность четверть- и полуволновой пластинок и поляризатора. Используемая измерительная схема позволяет полностью осуществить восстановление входного состояния кукварта [42, 44].

На рис. 3 показаны нормированные зависимости числа единичных фотоотсчетов в каналах 1 и 2 (рис. 3*а,б*), а также числа совпадений фотоотсчетов (рис. 3*в*) от угла наклона пластинок *Dpo*1 и *Dpo*2, определяющего эффективную толщину. Сплошная линия соответствует результатам расчетов, точки — экспериментальным данным.

Необходимым (но не достаточным) условием адекватности осуществляемых преобразований является совпадение значений углов наклона пластинок, отвечающих максимумам в канале 1, и в совпадениях фотоотсчетов. Действительно, поскольку измерительная схема настроена на выделение состояния $|H_1, V_2\rangle$, наибольшая скорость счета совпадений

$$R_c \approx \langle a_1^\dagger a_1 b_2^\dagger b_2\rangle = \sin^2\delta_1 \cos^2\delta_2 \quad (26)$$

отвечает именно такому входному состоянию. В выражении (26) учтено, что вклад в совпадения отсчетов дают лишь параметрически сопряженные моды, т. е. моменты четвертого порядка $\langle a_1^\dagger a_1 b_1^\dagger b_1\rangle$, $\langle a_1^\dagger a_1 b_1^\dagger b_2\rangle$, $\langle a_1^\dagger a_1 b_2^\dagger b_1\rangle$ равны нулю.

С другой стороны, поскольку в канале 1 выделяется горизонтальная поляризация, а в канале 2 — вертикальная, скорости счета единичных отсчетов, пропорциональные интенсивностям, имеют вид

$$I_1 \approx \langle a_1^\dagger a_1\rangle = |t_1|^2 \sin^2\delta_1, \quad (27)$$

$$I_2 \approx \langle b_1^\dagger b_1\rangle + \langle b_2^\dagger b_2\rangle = |r_1|^2 \cos^2\delta_1 + |r_2|^2 \cos^2\delta_2. \quad (28)$$

Поэтому из совпадения максимумов зависимостей (26) и (27) и при учете (25) следует необходимость выполнения искомого преобразования

$$|V_{\lambda_1}, V_{\lambda_2}\rangle \to |H_{\lambda_1}, V_{\lambda_2}\rangle.$$

Из расчетных кривых (сплошные линии на рис. 3) видно, что данное преобразование осуществляется в области первого максимума. Одинаковое расположение минимумов в зависимостях совпадений фотоотсчетов и интенсивности в канале 1 от угла наклона θ определяет необходимое условие преобразования в состояние, ортогональное тому, на которое настроена измерительная схема.

Для того чтобы убедиться, что измеренное состояние соответствует расчетному $|H_1, V_2\rangle$ в положении пластинок, отвечающему первому максимуму на рис. 3, была проведена частичная томография кукварта. Измерялись диагональные компоненты поляризационной матрицы плотности состояния (14)[9)]

$$\rho = |\Psi_4\rangle\langle\Psi_4|.$$

Значения измеренных и теоретически ожидаемых моментов представлены в табл. 3. Мера соответствия приготовленных состояний теоретическим для первого базиса из (16) составила

$$F = |\langle\Psi_{theor}|\Psi_{exp}\rangle|^2 = 0.87.$$

Причиной отличия значения F от единицы является резкая зависимость эффективности поляризационных преобразований от длины волны. Например, при неточности установки длины волны в первом канале на 1.5 нм, что соответствует половине полосы пропускания интерференционного фильтра, теоретическое значение F меняется в интервале от 0.83 до 1.0. Кроме того, выбранная толщина пластинки не обеспечивает точного достижения необходимых значений фазовых сдвигов. Как следствие, теоретическое значение F не достигает своего максимального значения. Наконец, учет конечной ширины спектра бифотонного излучения приводит к тому, что разные спектральные компоненты приобретают разный набег фаз на толщине пластинки.

[9)] Детальное статистическое исследование восстановленных состояний куквартов проводилось в работах [45, 52].

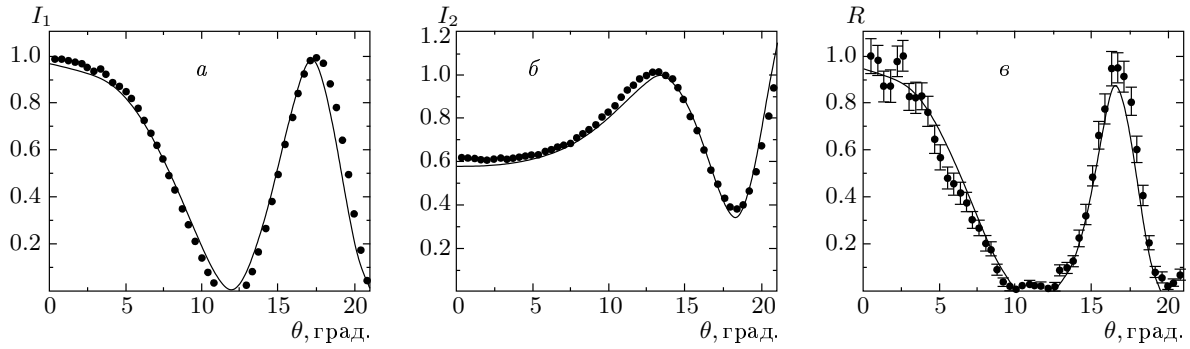

Рис. 3. Графики зависимости нормированного числа единичных фотоотсчетов и совпадений от угла поворота кварцевых пластинок ($Dpo1, 2$); *а* — фотоотсчеты в первом канале, *б* — фотоотчеты во втором канале, *в* — совпадения. Теоретическая линия — сплошная кривая, экспериментальные данные — точки. На графиках для единичных фотоотсчетов (*а, б*) погрешность соразмерна с размерами точек

Таблица 3

Компоненты поляризационной матрицы плотности	Начальное состояние $\|V_1, V_2\rangle$	Преобразованное состояние $\|H_1, V_2\rangle$	
	Теория	Теория	Эксперимент
$c_1^* c_1$	0	0	0.093
$c_2^* c_2$	0	1	0.868
$c_3^* c_3$	0	0	0.019
$c_4^* c_4$	1	0	0.020

Однако расчет показывает, что интегрирование по ширине спектра бифотонного поля не дает значительного уменьшения значения F при условии правильного выбора центральной длины волны.

5.2. Передача состояний

Недостатком любых схем КРК, основанных на поляризационных состояниях, является то, что такие состояния практически невозможно передавать по оптоволоконным линиям. Из-за локальных напряжений и деформаций, а также из-за флуктуаций температуры состояние поляризации света на выходе сложным образом связано с входным и меняется во времени. Поэтому при использовании в качестве квантового канала оптоволоконных линий применяется кодирование в других степенях свободы [2]. Поляризационное кодирование возможно при КРК в открытом пространстве (см., например, [53]). Учет уровня ошибок, связанных с влиянием деполяризации при распространения бифотонов-куквартов через турбулентную атмосферу представляет собой отдельную задачу как в теоретическом, так и в экспериментальном плане и выходит за рамки данной работы.

5.3. Измерение состояний

На рис. 4 показана схема регистрации, позволяющая измерять состояния в одном из трех базисах 1, 2 и 3 из (16). Схема состоит из дихроичного светоделителя DBS, разделяющего в пространстве частотные моды 1 и 2. Перед светоделителем находятся две фазовые пластинки, которые осуществляют смену базисов. При повороте четвертьволновой пластины Qp на угол 45° происходит переход к «циркулярному» базису 3, а при повороте полуволновой пластины Hp на угол 22.5° — переход к «диагональному» базису 2. Далее в каждом плече симметрично располагаются поляризационные светоделители $PBS1$ и $PBS2$, каждый из которых пропускает излучение с горизонтальной поляризацией (H) и отра-

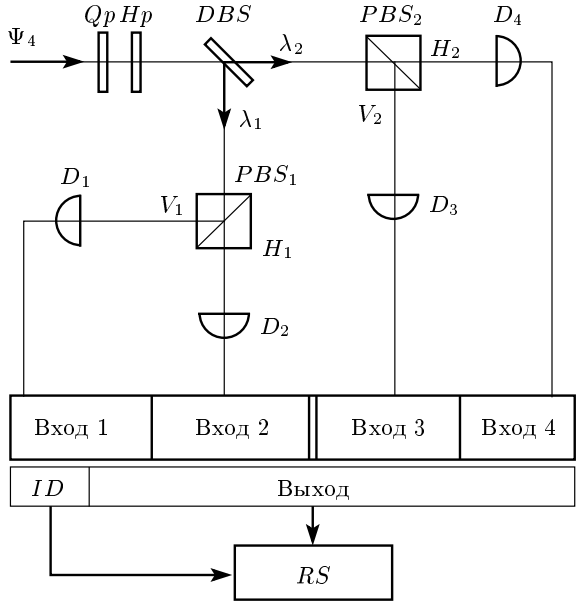

Рис. 4. Схема установки для измерения двенадцати базисных состояний в трех взаимно несмещенных базисах. DBS — дихроичный светоделитель, $PBS_{1,2}$ — поляризационный светоделитель, Qp — четвертьволновая пластинка, Hp — полуволновая пластинка, $D_{1,2,3,4}$ — фотодетектор, RS — система обработки информации, ID — идентификатор выходов

жает излучение с вертикальной поляризацией (V). В двух парах выходных плеч этих светоделителей помещены детекторы, работающие в режиме счета фотонов. Импульсы фототока с выходов детекторов подаются на четырехканальную схему парных совпадений. Она генерирует выходной импульс каждый раз, когда на любых двух входах присутствует пара импульсов, совпадающих во времени в пределах окна T_{coin}. Вместе с выходным импульсом коррелятор выдает сигнал идентификации (ID) тех пар входов, с которых поступили совпадающие импульсы. Система обработки информации (RS) служит для выработки сырого ключа.

Рассмотрим режимы работы приемной схемы, например, для первого («измерительного») базиса. Для этого нужно убедиться, что все четыре базисных ортонормированных состояния $|H_1, H_2\rangle$, $|H_1, V_2\rangle$, $|V_1, H_2\rangle$ и $|V_1, V_2\rangle$ однозначно идентифицируются.

Состояние $|H_1, H_2\rangle$: при поступлении на вход этого базисного состояния, после разделения разночастотных мод на дихроичном светоделителе DBS, срабатывают детекторы D_2 и D_4.

Состояние $|H_1, V_2\rangle$: срабатывают детекторы D_2 и D_3.

Состояние $|V_1, H_2\rangle$: срабатывают детекторы D_1 и D_4.

Состояние $|V_1, V_2\rangle$: срабатывают детекторы D_1 и D_3.

Аналогично происходит работа схемы для циркулярного и измерительного базисов. При повороте пластинки Qp индекс состояния H меняется на R, а V — на L, при повороте пластинки Hp индексы меняются по правилу: $H \to +45°$, $V \to -45°$.

Заметим, что однозначная регистрация состояний, принадлежащих четвертому и пятому базисам, в данной схеме невозможна. В конечном счете проблема регистрации этих состояний сводится к задаче измерения состояний Белла, которая с помощью линейно-оптических устройств не решается [54]. Однако для двух- и трехбазисного протоколов КРК полной идентификации состояний из первых трех базисов оказывается вполне достаточно.

6. ОБСУЖДЕНИЕ

Прежде всего, отметим, что обсуждаемая реализация четырехуровневой системы — поляризационные состояния невырожденного по частоте бифотонного поля — обладает рядом принципиальных достоинств по сравнению с рассматривавшимися ранее. Главные из них — простота генерации и измерений необходимых для КРК состояний. Как было отмечено, все необходимые для протокола состояния могут быть приготовлены при помощи одного нелинейно-оптического кристалла — как следствие снятия вырождения бифотонного поля по частоте. Проведенные эксперименты продемонстрировали высокое качество линейных преобразований этих состояний. Кроме того, измерительная часть не вносит нежелательных потерь, присущих схемам на основе бифотонов и содержащих светоделители. Для сравнения отметим, что в обсуждаемом в работе [55] протоколе КРК на кутритах верхняя граница успешно регистрируемых состояний составляет лишь 8 % (при правильно выбранном базисе). Такой низкий процент потенциально измеряемых состояний связан с разрушением бифотонного характера поля на светоделителях, не сохраняющих поляризацию. Принципиальным в выборе измерительной схемы для куквартов оказывается наличие дихроичного зеркала, разделяющего в пространстве разночастотные моды, и наличие поляризационных светоделителей в обоих его плечах. Такие светоделители об-

ладают низкими собственными потерями (порядка 10^{-3}–10^{-4}) и широко используются в поляризационной оптике. Отметим также, что нежелательное в квантово-криптографических схемах увеличение числа фотодетекторов (из-за аддитивно вносимых темновых шумов) в данной схеме несущественно, поскольку регистрируемым событием служит совпадение фотоотсчетов. Действительно, вклад событий (в единицу времени), вызванных случайными совпадениями темновых отсчетов, подчиняющихся пуассоновской статистике, пропорционален произведению скоростей последних и окна схемы совпадений:

$$W_{coin} = W_1 W_2 T_{coin}.$$

Нетрудно убедиться, что при выборе размера окна порядка 1 нс и при характерных для современных однофотонных детекторов скоростях счета темновых импульсов 100 Гц уровень ошибок этого вида намного меньше типичной величины 10^{-5} нс$^{-1}$ [2].

Одним из вариантов обсуждаемых в работе способов выполнения поляризационных преобразований над базисными состояниями частотно-невырожденного бифотонного поля могла бы служить схема с двумя идентичными призмами, разделяющими в пространстве частотные моды, и фазовыми пластинками, помещенными в одну из мод между ними. Представляется, однако, что подобная схема не очень удобна на практике. Действительно, при использовании кварцевых призм для разделения мод с длинами волн $\lambda_1 = 702$ нм и $\lambda_2 = 605.2$ нм на длину порядка 2 мм потребуется разнести их на расстояние около 1 м. Кроме того, при таком способе поперечное сечение получившегося пучка будет неоднородным по частоте. Такая дополнительная параметризация выводит начальные состояния бифотонов из пространства куквартов (две поляризационные и две частотные моды) в восьмимерное пространство (две поляризационные, две частотные и две пространственные моды).

К недостаткам системы, оперирующей с бифотонными состояниями, относится двукратный уровень (по сравнению с однофотонными) потерь: разрушение такого состояния происходит при потере любого фотона, из составляющих пару. Этот фактор приводит к уменьшению скорости генерации ключа. Последовательный учет влияния двухфотонной природы информационных носителей на предельный уровень ошибок при КРК, связанный с возмущениями поля при распространении, насколько нам известно, еще не проводился.

В настоящей работе затронуты лишь физические принципы приготовления и измерения куквартов. Обсуждение технических аспектов реализации протокола КРК, хотя они и составляют важнейший элемент любой системы КРК, выходит за рамки данной статьи. Заметим лишь, что на практике все указанные преобразования можно осуществить при помощи специальных электрооптических модуляторов, изменяющих заданным образом поляризационные состояния одновременно для пары выбранных длин волн. Для синхронизации всех процессов приготовления и измерения состояний удобнее использовать импульсный лазер. В то же время отсутствие каких-либо интерферометров, наличие которых характерно для большинства систем квантового распределения ключа, делает схему стабильной во времени и снимает проблемы, связанные с согласованием пространственно-временных компонент квантовых состояний.

Авторы выражают благодарность В. П. Карасеву и А. В. Масалову за плодотворные обсуждения, а С. С. Страупе — за помощь в проведении эксперимента. Работа выполнена в рамках междисциплинарного научного проекта МГУ им. М. В. Ломоносова № 4-2005 и программы поддержки ведущих научных школ (грант № НШ-4586.2006.2), а также при финансовой поддержке РФФИ (гранты №№ 03-02-16444, 06-02-16769).

ЛИТЕРАТУРА

1. W. Diffie and M. Hellman, IEEE Trans. on Inform. Theory **IT-22**, 644 (1976).

2. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

3. *Физика квантовой информации*, под ред. Д. Боумейстера, А. Экерта, А. Цайлингера, Постмаркет, Москва (2002).

4. W. K. Wooters and W. Zurek, Nature **299**, 802 (1982).

5. Ch. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).

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

7. D. Bruss, Phys. Rev. Lett. **81**, 3018 (1998); H. Bechmann-Pasquinucci and N. Gisin, Phys. Rev. A **59**, 4238 (1999).

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

9. С. Н. Молотков, Письма в ЖЭТФ **76**, 71 (2002); D. V. Sych, B. A. Grishanin, and V. N. Zadkov, Phys. Rev. A **70**, 052331 (2004).

10. H. Bechmann-Pasquinucci and A. Peres, Phys. Rev. Lett. **85**, 3313 (2000).

11. W. K. Wooters and B. D. Fields, Ann. Phys. (Leipzig) **191**, 363 (1989).

12. H. Bechmann-Pasquinucci and W. Tittel, Phys. Rev. A **61**, 062308 (2000).

13. M. Bourennane, A. Karlsson, and G. Bjork, Phys. Rev. A **64**, 012306 (2001).

14. N. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002).

15. D. Bruss and C. Macchiavello, Phys. Rev. Lett. **88**, 127901 (2002).

16. Д. В. Хорошко, С. Я. Килин, Опт. и спектр. **94**, 691 (2003).

17. F. Caruso, H. Bechmann-Pasquinucci, and C. Macchiavello, E-print archives quant/ph/0505146.

18. V. Buzek and M. Hillery, Phys. Rev. Lett. **81**, 5003 (1998).

19. M. N. Soskin, V. N. Gorshkov, M. V. Vasnetsov, J. T. Malos, and N. R. Heckenberg, Phys.Rev.A **56**, 4065 (1997).

20. A. Vaziri, J.-W. Pan, T. Jennewein, G. Weihs, and A. Zeilinger, Phys. Rev. Lett. **91**, 227902 (2003).

21. A. Vaziri, G. Weihs, and A. Zeilinger, Phys. Rev. Lett. **89**, 240401 (2002).

22. D. Collins, N. Gisin, N. Linden, S. Massar, and S. Popesku, Phys. Rev. Lett. **88**, 040404 (2002).

23. N. Langford, R. B. Dalton, M. D. Harvey, and J. L. O'Brien, Phys. Rev. Lett. **93**, 053601 (2004).

24. R. T. Thew, S. Tanzilini, A. Acin, H. Zbinden, and N. Gisin, Quant. Inf. Comp. **4**, 93 (2004).

25. R. T. Thew, A. Acin, H. Zbinden, and N. Gisin, Phys. Rev. Lett. **93**, 010503 (2004).

26. J. D. Franson, Phys. Rev. Lett. **62**, 2205 (1989).

27. M. N. O'Sullivan-Hale, I. A. Khan, R. W. Boyd, and J. C. Howell, Phys. Rev. Lett. **94**, 220501 (2005).

28. L. Neves, G. Lima, J. G. Aguirre Gomez, C. H. Monken, C. Saavedra, and S. Padua, Phys. Rev. Lett. **94**, 100501 (2005).

29. G. M. D'Ariano, P. Mataloni, and M. F. Sacchi, Phys. Rev. A **71**, 062337 (2005).

30. A. Lamas-Linares, J. C. Howell, and D. Boumeester, Nature **412**, 887 (2001).

31. J. C. Howell, A. Lamas-Linares, and D. Boumeester, Phys. Rev. Lett. **88**, 030401 (2002).

32. D. Kaszlikovski, P. Gnasinski, M. Zukowski, W. Miklaszewski, and A. Zeilinger, Phys. Rev. Lett. **85**, 4418 (2000).

33. D. Kaszlikovski, L. C. Kwek, J.-L. Chen, M. Zukowski, and C. H. Oh, Phys. Rev. A **65**, 032118 (2002).

34. H. Riedmatten, I. Marcikic, V. Scarani, W. Tittel, H. Zbinden, and N. Gisin, Phys. Rev. A **69**, 050304(R) (2004).

35. Д. Н. Клышко, *Фотоны и нелинейная оптика*, Наука, Москва (1980).

36. А. В. Бурлаков, Д. Н. Клышко, Письма в ЖЭТФ **69**, 795 (1999).

37. A. V. Burlakov, M. V. Chekhova, O. A. Karabutova, D. N. Klyshko, and S. P. Kulik, Phys. Rev. A **60**, R4209 (1999).

38. А. В. Бурлаков, М. В. Чехова, Письма в ЖЭТФ **75**, 505 (2002).

39. А. А. Жуков, Г. А. Масленников, М. В. Чехова, Письма в ЖЭТФ **76**, 696 (2002).

40. M. V. Chekhova, L. A. Krivitsky, S. P. Kulik, and G. A. Maslennikov, Phys. Rev. A **70**, 053801 (2004).

41. Ю. И. Богданов, Л. А. Кривицкий, С. П. Кулик, Письма в ЖЭТФ **78**, 804 (2003).

42. Yu. Bogdanov, M. Chekhova, L. Krivitsky, S. P. Kulik, L. C. Kwek, M. K. Tey, C. Ch. Oh, and A. A. Zhukov, Phys. Rev. A **70**, 042303 (2004).

43. Yu. Bogdanov, M. Chekhova, S. P. Kulik, G. Maslennikov, M. K. Tey, and C. Ch. Oh, Phys. Rev. Lett. **93**, 23503 (2004).

44. D. F. V. James, P. G. Kwiat, W. J. Munro, and A. G. White, Phys. Rev. A **64**, 052312 (2001).

45. Ю. И. Богданов, Р. Ф. Галеев, С. П. Кулик, Г. А. Масленников, Е. В. Морева, Письма в ЖЭТФ **82**, 180 (2005).

46. Д. Н. Клышко, ЖЭТФ **111**, 1955 (1997).

47. Л. А. Кривицкий, С. П. Кулик, Г. А. Масленников, М. В. Чехова, ЖЭТФ **127**, 1 (2005).

48. В. П. Карасев, А. В. Масалов, ЖЭТФ **126**, 63 (2004).

49. A. Sehat, J. Soderholm, G. Bjork, P. Espinoza, A. B. Klimov, L.-L. Sanchez-Soto, Phys. Rev. A **71**, 033818 (2005).

50. V. P. Karassiov, J. Phys. A **26**, 4345 (1993).

51. Y. H. Kim, S. P. Kulik, and Y. Shih, Phys. Rev. A **63**, 060301 (2001).

52. Yu. I. Bogdanov, R. F. Galeyev, S. P. Kulik, G. A. Maslennikov, and E. V. Moreva, submitted to Phys. Rev. A.

53. C. Kurtseifer, M. Halder, P. Zarda, H. Weinfurter, P. R. Tapster, and J. G. Rarity, Nature, **419**, 450 (2002).

54. N. Lutkenhaus, J. Calsamiglia, and K.-A. Suominen, Phys. Rev. A **59**, 3295 (1999).

55. G. A. Maslennikov, A. A. Zhukov, M. V. Chekhova, and S. P. Kulik, J. Opt. B **5**, 530 (2003).