УЧЕНЫЕ ЗАПИСКИ КАЗАНСКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА
Том 148, кн. 1 Физико-математические науки *2006*

УДК 535.41+535.232.6

ПОЛЯРИЗАЦИОННЫЕ ПРЕОБРАЗОВАНИЯ БИФОТОНОВ

С.П. Кулик, Е.В. Морева, С.С. Страупе

Аннотация

В работе рассматриваются преобразования поляризационных состояний оптических четырехуровневых систем. Предложена простая экспериментальная процедура приготовления и измерения поляризационных состояний бифотонов, которая может быть использована в протоколах квантового распределения ключа. Полученные экспериментальные результаты свидетельствуют о высоком качестве получаемых состояний.

Введение

Интерес, проявляемый в последнее время к изучению многоуровневых квантовых систем (кудитов), обусловлен во-многом возможностью их использования в протоколах квантового распределения ключа (КРК). КРК решает одну из основных проблем классической криптографии – проблему распространения секретного ключа. Как известно, абсолютная секретность передаваемого сообщения может быть достигнута только при шифровании его с использованием случайного, секретного и применяемого только один раз ключа, имеющего длину не меньше длины сообщения. Протокол КРК представляет собой процедуру, позволяющую распространить ключ между легитимными пользователями, обеспечив при этом его секретность.

Рассмотрим основные принципы, лежащие в основе КРК, на примере протокола, использующего кудиты и являющегося прямым обобщением на многомерный случай известного протокола BB84 [1]. Случайная последовательность символов, например двоичных цифр (классических битов), кодируется с помощью состояний многоуровневой квантовой системы. Кодирование производится в неортогональных состояниях из некоторого набора базисов, выбор между которыми осуществляется случайным образом. Состояния передаются получателю, который осуществляет измерение в произвольном базисе из того же набора. После этого стороны по открытому каналу обмениваются информацией о том, в каких базисах производилось кодирование и измерение. При несовпадении базисов результат измерения отбрасывается. Таким образом, в отсутствие подслушивания у пользователей формируется идентичная последовательность символов, служащая в дальнейшем секретным ключом для шифрования сообщения. Вмешательство подслушивающей стороны неизбежно приводит к появлению несовпадающих результатов при измерении в одинаковых базисах, что является прямым следствием известной теоремы о запрете копирования неизвестного квантового состояния [2]. Следовательно, сравнив часть ключа, не используемую в дальнейшем, пользователи могут выявить наличие подслушивателя.

Существенной деталью КРК является выбор базисов, в которых производится кодирование: среди используемых базисов не должно быть выделенных, все результаты измерения в любом, неправильно выбранном базисе должны быть равновероятны. Этому требованию отвечают так называемые взаимно-несмещенные

базисы: ортонормированные базисы, удовлетворяющие условию

$$|\langle\Psi_i \mid \Phi_j\rangle|^2 = \frac{1}{d}, \tag{1}$$

если $|\Psi_i\rangle$ и $|\Phi_j\rangle$ принадлежат разным базисам. Можно показать, что в гильбертовом пространстве, размерность которого $d = p^k$, где p – простое число, а k – целое, существует ровно $d+1$ взаимно-несмещенных базисов. Использование всех базисов при КРК необязательно, для реализации описанного протокола достаточно $M \geq 2$ базисов [3].

При использовании подслушивателем простейшей стратегии – атаке типа «перехват-пересылка» – количество получаемой им информации определяется формулой: $I_E = \eta\dfrac{\log_2 d}{M}$, где η – доля перехваченных состояний. При этом вероятность возникновения ошибки равна $E_B = \eta\left(1-\dfrac{1}{M}\right)\left(1-\dfrac{1}{d}\right)$. Таким образом, увеличение размерности пространства и числа используемых базисов увеличивает возмущение, вносимое подслушивателем. Для каждого протокола КРК существует ограничение на количество ошибок, вызываемых как возможным подслушиванием, так и шумом в канале, при превышении которого невозможно гарантировать секретность ключа, например, для протокол BB84 оно составляет 11%. Использование кудитов позволяет увеличить допустимый уровень шума в канале. Этот вывод является одним из основных стимулов для исследования многоуровневых систем.

1. Оптические четырехуровневые системы

Одним из способов получения квантовых состояний размерностью $d > 2$ является использование процесса спонтанного параметрического рассеяния света (СПР) [4]. При СПР частоты и волновые вектора полей в двух модах, условно называемых сигнальной (s) и холостой (i), связаны с соответствующими параметрами накачки (p) соотношениями

$$\omega_s + \omega_i = \omega_p, \tag{2}$$

$$\mathbf{k}_s + \mathbf{k}_i - \mathbf{k}_p = \mathbf{\Delta}, \tag{3}$$

где $\mathbf{\Delta}$ – расстройка определяемая параметрами нелинейного кристалла. Рассмотрим коллинеарный ($\mathbf{k}_s = \mathbf{k}_i$), частотно-невырожденный ($\omega_s \neq \omega_p$) режим СПР. Поляризационное состояние бифотоного поля, генерируемого в таком процессе, в фоковском представлении имеет вид:

$$|\Psi\rangle = c_1\,|H_1\rangle\,|H_2\rangle + c_2\,|H_1\rangle\,|V_2\rangle + c_3\,|V_1\rangle\,|H_2\rangle + c_4\,|V_1\rangle\,|V_2\rangle\,, \tag{4}$$

где $|H\rangle$ и $|V\rangle$ соответствуют горизонтальной и вертикальной поляризации, а индексы 1 и 2 – различным частотным модам. Гильбертово пространство в данном случае четырехмерно (такие состояния называют куквартами), следовательно, существует пять взаимно-несмещенных базиса, соответствующие базисные состояния имеют вид

$$\begin{gathered}
1.\ |H_1, H_2\rangle\,; |H_1, V_2\rangle\,; |V_1, H_2\rangle\,; |V_1, V_2\rangle\,; \\
2.\ |{+45}^\circ_1, {+45}^\circ_2\rangle\,; |{+45}^\circ_1, {-45}^\circ_2\rangle\,; |{-45}^\circ_1, {+45}^\circ_2\rangle\,; |{-45}^\circ_1, {-45}^\circ_2\rangle\,; \\
3.\ |R_1, R_2\rangle\,; |R_1, L_2\rangle\,; |L_1, R_2\rangle\,; |L_1, L_2\rangle\,; \\
4.\ |R_1, H_2\rangle + |L_1, V_2\rangle\,; |R_1, H_2\rangle - |L_1, V_2\rangle\,; |L_1, H_2\rangle + |R_1, V_2\rangle\,; |L_1, H_2\rangle - |R_1, V_2\rangle \\
5.\ |H_1, R_2\rangle + |V_1, L_2\rangle\,; |H_1, R_2\rangle - |V_1, L_2\rangle\,; |H_1, L_2\rangle + |V_1, R_2\rangle\,; |H_1, L_2\rangle - |V_1, R_2\rangle\,.
\end{gathered} \tag{5}$$

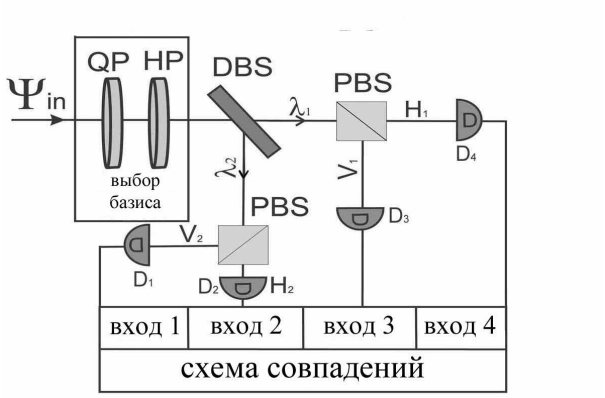

Рис. 1. Схема измерения базисных состояний

Здесь $|R\rangle$ и $|L\rangle$ соответствуют состояниям фотонов с правой и левой циркулярными поляризациями, а $|+45^\circ_1\rangle$ и $|+45^\circ_1\rangle$ – состояниям фотонов, линейно поляризованных под $\pm 45^\circ$ к вертикали.

Базисные состояния первых трех из указанных базисов могут быть получены путем поляризационных преобразований бифотонов, генерируемых в одном нелинейном кристалле. Как отмечалось выше, этих состояний вполне достаточно для реализации протокола КРК. Поляризационные кукварты представляют собой удобный объект для КРК ввиду наличия для них простой детерминистической схемы, позволяющей различить все состояния выбранного базиса. Нетрудно видеть, что схема, представленная на рис. 1, обеспечивает срабатывание одного и только одного из детекторов, если входное состояние принадлежит базису 1 из (5). Переход к базисам 2 и 3 осуществляется введением на входе схемы дополнительной полуволновой и четвертьволновой фазовой пластинки соответственно.

2. Поляризационные преобразования

Рассматриваемые преобразования осуществляются фазовой пластинкой, действующей независимо на каждый фотон из пары. Если ввести обозначения $|H_{1,2}\rangle = \begin{pmatrix}1\\0\end{pmatrix}_{1,2}$ и $|V_{1,2}\rangle = \begin{pmatrix}0\\1\end{pmatrix}_{1,2}$, то действие пластинки будет описываться матрицей унитарного преобразования вида

$$\mathbf{G} = \begin{pmatrix} t_1 & r_1 \\ -r_1^* & t_1^* \end{pmatrix} \otimes \begin{pmatrix} t_2 & r_2 \\ -r_2^* & t_2^* \end{pmatrix} = \begin{pmatrix} t_1t_2 & t_1r_2 & r_1t_2 & r_1r_2 \\ -t_1r_2^* & t_1t_2^* & -r_1r_2^* & r_1t_2^* \\ -r_1^*t_2 & -r_1^*r_2 & t_1^*t_2 & t_1^*r_2 \\ r_1^*r_2^* & -r_1^*t_2^* & -t_1^*r_2^* & t_1^*t_2^* \end{pmatrix}, \tag{6}$$

где $t_k = \cos\delta_k + i\sin\delta_k\cos 2\gamma$; $r_k = i\sin\delta_k\sin 2\gamma$, $k = 1,2$. Здесь δ_k – вносимая пластинкой на длине волны λ_k разность фаз, γ – угол наклона оптической оси пластинки к вертикали. К примеру, преобразованию $|V_1, V_2\rangle \to |V_1, H_2\rangle$ соответствуют значения $\delta_1 = \pi$, $\delta_2 = \pi/2$, $\gamma = 45^\circ$. Толщина и номера интерференционных порядков для такой фазовой пластинки, изготовленной из одноосного кристалла, вычисляются из соотношений

$$\begin{aligned} \delta_1 = \pi &= \frac{\pi m_1 l(n_e - n_o)_1}{\lambda_1}, \\ \delta_2 = \frac{\pi}{2} &= \frac{\pi m_2 l(n_e - n_o)_2}{\lambda_2}. \end{aligned} \tag{7}$$

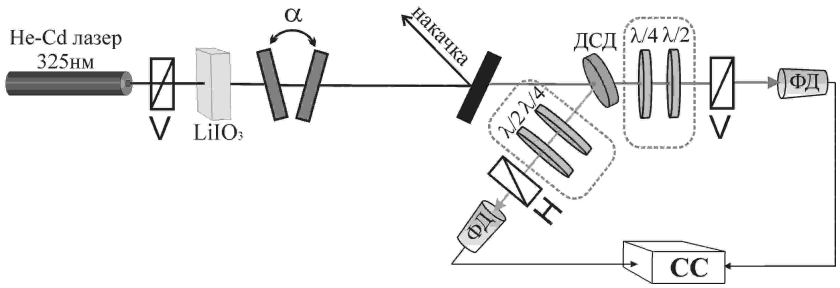

Рис. 2. Схема экспериментальной установки

В эксперименте длины волн сигнального и холостого излучений имели значения $\lambda_1 = 702$ нм, $\lambda_2 = 605$ нм, для них $(n_e - n_o)_1 = 0.00896$, $(n_e - n_o)_2 = 0.00906$, искомая толщина пластинки составляет 3406 мкм. Требования к точности соответствия длины используемой пластины расчетной очень высоки, что делает ее изготовление крайне затруднительным. На практике одна пластина заменялась двумя толщиной 3716 мкм и 315 мкм, ориентированными под углами $+45°$ и $-45°$ к вертикали. Наклоном одной пластины относительно другой можно плавно изменять вносимую такой системой разность фаз, добиваясь выполнения соотношений (7). Такое преобразование эквивалентно изменению оптической толщины δ одной «составной» пластины.

Преобразование $|V_1, V_2\rangle \to |H_1, V_2\rangle$ осуществляется аналогичным образом. Для этого преобразования используется полуволновая пластинка нулевого порядка, ориентированная под углом $45°$ к вертикали. Таким образом, поляризационные преобразования позволяют получить произвольное базисное состояние из базиса 1. Состояния второго и третьего базисов легко получаются из состояний первого введением дополнительных пластинок нулевого порядка – полуволновой пластинки, ориентированной под углом $22.5°$ к вертикали для перехода к базису 2, и четвертьволновой, ориентированной под углом $45°$ к вертикали для перехода к базису 3. Состояния, принадлежащие остальным двум взаимно-несмещенным базисам, не могут быть приготовлены рассмотренным методом, однако, как указывалось выше, их использование не является необходимым для реализации протокола КРК.

3. Экспериментальная реализация преобразований

Схема экспериментальной установки изображена на рис. 2. Накачкой служило излучение He-Cd лазера с длиной волны 325 нм и горизонтальной поляризацией. В нелинейном кристалле $LiIO_3$ с синхронизмом типа I генерировалось состояние $|V_1, V_2\rangle$ с длинами волн сигнального и холостого излучений $\lambda_1 = 702$ нм и $\lambda_2 = 605$ нм.

Измерительная схема состоит из дихроичного светоделителя, разделяющего частотные моды излучения (702 нм – в проходящем канале, 605 нм – в отраженном), набора из четвертьволновых и полуволновых пластинок, поляризатора и фотодетектора в каждом канале. Такая схема позволяет, меняя наклон оптических осей пластинок к вертикали, выделять в каждом из каналов произвольное поляризационное состояние [5]. Сигналы с фотодетекторов направляются на вход схемы совпадений.

На рис. 3 приведена зависимость числа совпадений в отсчетах детекторов в первом и втором каналах от угла наклона фазовой пластины α для случая, когда измерительная схема настроена на выделение состояния $|H_1, V_2\rangle$, то есть для вер-

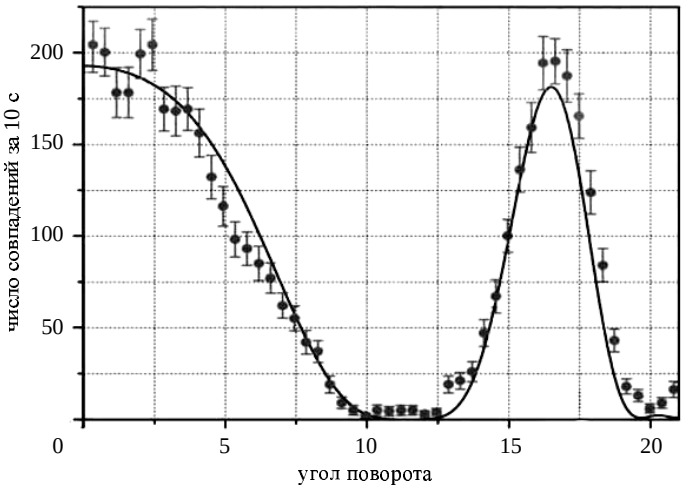

Рис. 3. Зависимость числа совпадений от ориентации фазовых пластинок

тикальной поляризации в первом канале и для горизонтальной во втором. Точке максимума соответствует угол наклона, при котором разность фаз, вносимая «составной» пластиной, удовлетворяет соотношению (7), и, следовательно, пластина осуществляет преобразование $|V_1, V_2\rangle \to |H_1, V_2\rangle$.

Табл. 1

Преобразование	$\lvert c_1\rvert^2$	$\lvert c_2\rvert^2$	$\lvert c_3\rvert^2$	$\lvert c_3\rvert^2$	F
$\lvert V_1, V_2\rangle \to \lvert V_1, H_2\rangle$	0.017	0	0.0983	0	98%
$\lvert V_1, V_2\rangle \to \lvert H_1, V_2\rangle$	0.024	0.931	0.003	0.042	94%
$\lvert V_1, V_2\rangle \to \lvert +45^\circ_1, -45^\circ_2\rangle$	0.010	0.963	0	0.027	96%
$\lvert V_1, V_2\rangle \to \lvert -45^\circ_1, +45^\circ_2\rangle$	0.010	0.010	0.884	0.097	88%
$\lvert V_1, V_2\rangle \to \lvert L_1, R_2\rangle$	0.019	0.001	0.939	0.040	92%
$\lvert V_1, V_2\rangle \to \lvert R_1, L_2\rangle$	0	0.941	0.010	0.049	95%

Все состояния из первых трех взаимно-несмещенных базисов (5) были получены экспериментально, преобразованием состояния $|V_1, V_2\rangle$. Для проверки правильности осуществления преобразований производилась частичная томография кукварта (эта процедура подробно описана в [6]). Преобразования, соответствующие диагональные элементы матрицы плотности системы $\rho = |\Psi\rangle\langle\Psi|$ и мера соответствия измеренного состояния ожидаемому представлены в табл. 1. Высокие значения F свидетельствуют о хорошем качестве получаемых состояний.

Заключение

Рассмотренный метод приготовления базисных состояний куквартов, основанный на применении поляризационных преобразований, может быть использован в системах КРК. К достоинствам предложенного метода можно отнести возможность приготовления всех базисных состояний из трех взаимно-несмещенных базисов с использованием одного нелинейного кристалла, отсутствие интерферометрических схем и связанных с ними нестабильностей, низкий уровень измерительных

потерь. При практической реализации КРК необходимо использование поляризационных модуляторов, позволяющих осуществлять преобразования с высокой скоростью.

Работа выполнена при финансовой поддержке РФФИ (проекты 05-02-16391а, 06-02-16769а, 06-02-16393а), гранта поддержки ведущих российских научных школ 4586.2006.2 и гранта ФАНИ 2006-РИ-19.0/001/593.

Summary

S.P. Kulik, E.V. Moreva, S.S. Straupe. Polarization transformations of biphotons.

A method of polarization ququart's bases states preparation using polirization transformations is discussed. All states out of three mutually unibased bases were prepared experimentally with high fidelity values. The proposed method can be used in quantum key distribution protocols using polarization ququarts as information carriers. The advantages of such realization of ququarts are the possibility to generate all the required states with single nonlinear crystal, low measurement losses and the fact that the experimental setup is free from any unstable interferometric schemes. All bases states out of the chosen basis can be distinguished deterministicaly using a simple scheme that makes polarization ququarts a useful object for quantum key distribution.

Литература

1. *Bennett C.H., Brassard G.* Quantum cryptography: Public key distribution and coin tossing // Proc. of IEEE Intern. Conf. on Computers, Systems and Signal Processing, Bangalore, India, Dec. – Los Alamitos, Calif.: IEEE Computer Society Press, 1984. – P. 175–179.
2. *Wooters W.K., Zurek W.* A single quantum cannot be cloned // Nature. – 1982. – V. 299. – P. 802–803.
3. *Bechmann-Pasquinucci H., Tittel W.* Quantum cryptography using larger alphabets // Phys. Rev. A. – 2000. – V. 61. – P. 062308-1–062308-6.
4. *Клышко Д.Н.* Фотоны и нелинейная оптика. – М.: Наука, 1980. – 258 с.
5. *James D.F.V., Kwiat P.G., Munro W.J., White A.G.* Measurement of qubits // Phys. Rev. A. – 2001. – V. 64. – P. 052312-1–052312-15.
6. *Кулик С.П., Масленников Г.А., Морева Е.В.* К вопросу о практической квантовой криптографии на многоуровневых системах // ЖЭТФ. – 2006. – Т. 129, № 5. – С. 814–829.

Поступила в редакцию
17.02.06

Кулик Сергей Павлович – доктор физико-математических наук, профессор кафедры квантовой электроники Московского государственного университета им. М.В. Ломоносова.

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

Морева Екатерина Васильевна – аспирант кафедры квантовой электроники Московского государственного университета им. М.В. Ломоносова.

E-mail: *moreva_ e@mail.ru*

Страупе Станислав Сергеевич – студент кафедры квантовой электроники Московского государственного университета им. М.В. Ломоносова.

E-mail: *straups@yandex.ru*