Письма в ЖЭТФ, том 96, вып. 5, с. 367 – 373 10 сентября

О квантовом распределении ключей на композитных фотонах – поляризационных кутритах

С. П. Кулик[+], *С. Н. Молотков*[+*×], *И. В. Радченко*[°]

[+] *МГУ им. Ломоносова, 119991 Москва, Россия*

[*] *Академия криптографии РФ, 103025 Москва, Россия*

[×] *Институт физики твердого тела РАН, 142432 Черноголовка, Россия*

[°] *Институт общей физики им. Прохорова РАН, 119991 Москва, Россия*

Поступила в редакцию 4 июля 2012 г.

Поляризационные состояния фотона являются наиболее естественными степенями свободы для кодирования классических бит информации. Двумерность пространства состояний, связанного с поляризационными степенями свободы фотона, недостаточна для многих задач передачи информации при помощи квантовых состояний. В работе предлагается использовать поляризационные степени свободы композитных состояний фотонов (поляризационных кутритов) для секретной передачи криптографических ключей.

Введение. На сегодняшний день использование квантовых состояний отдельных фотонов для защищенной передачи информации по квантовым каналам связи интенсивно исследуется как теоретически, так и экспериментально. В результате возникли прототипы систем квантового распределения ключей, секретность которых гарантируется фундаментальными запретами квантовой механики на копирование и различимость квантовых состояний [1–4]. Хотя фундаментальные законы природы и гарантируют стойкость таких систем, существующие технологические ограничения, связанные в основном с отсутствием однофотонных источников и характеристиками лавинных фотодетекторов, могут приводить к уязвимости данных систем по отношению к ряду атак [4]. Уязвимость была продемонстрирована для некоторых систем экспериментально [5]. Потери в линии связи приводят к ограничениям на предельную длину линий связи, при которой гарантируется секретность ключей. При больших потерях (соответственно, длине линии) из-за поглощения фотонов в канале фотодетектор начинает регистрировать собственные темновые шумы, которые приводят к ошибкам в информационной последовательности на приемной стороне. Любой протокол квантовой криптографии гарантирует секретность, только если величина ошибки не превышает определенного значения (обычно $< 20\%$) [4]. Было затрачено немало усилий теоретиков по модификации систем квантовой криптографии с целью увеличить критическую ошибку [4]. Первый довольно очевидный и подробно исследованный способ увеличения критической ошибки состоит в увеличении размерности N пространства состояний $N = \dim\mathcal{H}$ квантовой системы. При этом приближение критической ошибки к теоретически достижимому пределу в 50% происходит достаточно медленно ($\propto 1/\sqrt{N}$) [6]. Второй способ увеличения критической ошибки состоит в увеличении числа базисов, в которых приготавливаются информационные квантовые состояния. Приближение к теоретическому пределу по критической ошибке происходит по логарифмическому закону от числа базисов. Однако при большом числе базисов из-за отбрасывания посылок с несовпадающими базисами на приемной и передающей стороне падает эффективность передачи. При передаче ключей через открытое пространство (в отличие от оптоволокна, где состояние поляризации не сохраняется при распространении) наиболее удобными и естественными степенями свободы, в которые кодируются классические биты, являются поляризационные степени свободы фотона. Оказывается, что достичь теоретического предела по критической ошибке можно уже при конечной размерности пространства состояний квантовой системы $\mathcal{H} = 3$, а не асимптотически по N, как в пространствах большой размерности [6]. Однако размерности пространства состояний, связанного с поляризационными степенями свободы одиночных фотонов, недостаточно, поскольку оно является всего лишь двумерным (при заданном направлении распространения).

Один из способов решения проблемы увеличения размерности пространства состояний заключается в использовании квантовых состояний составных

(композитных) частиц – пар фотонов (бифотонов-кутритов).

Наша идея состоит в том, что информация о ключе кодируется в разные состояния поляризации *композитной частицы как целой*, представляющей собой пару фотонов – поляризационный кутрит. Размерность пространства состояний кутрита как раз равна $\dim(\mathcal{H}_{QTR}) = 3$. Такие пары коррелированных фотонов возникают в процессах спонтанного параметрического рассеяния (конверсии) фотонов вниз по энергии. Впервые такой процесс генерации бифотонов был предсказан теоретически Д.Н. Клышко [7], а затем исследован экспериментально в группе А.Н. Пенина [8]. Процедура измерения, которая формально сводится к проецированию на различные состояния пары фотонов, должна отличать разные информационные состояния композитной частицы, а также любые возмущения этих состояний, возникающие при вторжении в канал связи. *Схема измерений составных частиц является нетривиальной.* Дело в том, что конечная стадия измерения состояний фотонов, в том числе и бифотонов, сводится к фотодетектированию. Современные фотодетекторы, работающие в режиме счета отдельных фотонов, не различают число фотонов, т.е. не могут отличить однофотонные состояния от двухфотонных и т.д. Поэтому приходится прибегать к схемам совпадения отсчетов при фотодетектировании и предварительным преобразованиям квантовых состояний.

Схема квантового распределения ключей на кутритах. Ниже приведена схема квантовой криптографии на кутритах, в которой достигается теоретический предел по критической ошибке в 50%. Квантовое состояние общего вида для кутрита в частотно-вырожденном случае имеет вид

$$|\Psi\rangle = c_1|HH\rangle + c_2|HV\rangle + c_3|VV\rangle, \quad \sum_{i=1}^{3}|c_i|^2 = 1, \tag{1}$$

где $|\mu\nu\rangle = a_\mu^+ a_\nu^+|\mathrm{vac}\rangle$ – бозевские операторы рождения фотонов в поляризационных состояниях, $\mu, \nu = H, V$ – горизонтальная и вертикальная поляризации фотона. Размерность пространства состояний, связанного с поляризационными степенями свободы фотона, равна $\dim(\mathcal{H}) = 2$. Для пары фотонов в частотно-вырожденном случае (частоты и направления распространения совпадают) пространство состояний представляет собой симметризованное тензорное произведение (как следствие симметрии относительно перестановки частиц, $|HV\rangle = |VH\rangle$): $\dim(\mathcal{H}_{QTR}) = \dim[\mathrm{Sym}(\mathcal{H}\otimes\mathcal{H})] = 3$.

Информационные состояния. В схеме используется 4 базиса. В каждом базисе имеется по два ортогональных состояния, отвечающих 0 и 1. Состояния из разных базисов попарно неортогональны. Общее число информационных состояний равно $2^3 = 8$. Состояния имеют вид

$$\text{базис}\quad H+ \quad \begin{cases} |0_{H+}\rangle = \dfrac{1}{\sqrt{2}}(|HH\rangle + |HV\rangle), \\ |1_{H+}\rangle = \dfrac{1}{\sqrt{2}}(|HH\rangle - |HV\rangle); \end{cases}$$

$$\text{базис}\quad V+ \quad \begin{cases} |0_{V+}\rangle = \dfrac{1}{\sqrt{2}}(|VV\rangle + |HV\rangle), \\ |1_{V+}\rangle = \dfrac{1}{\sqrt{2}}(|VV\rangle - |HV\rangle); \end{cases} \tag{2}$$

$$\text{базис}\quad H\times \quad \begin{cases} |0_{H\times}\rangle = \dfrac{1}{\sqrt{2}}(|HH\rangle + i|HV\rangle), \\ |1_{H\times}\rangle = \dfrac{1}{\sqrt{2}}(|HH\rangle - i|HV\rangle); \end{cases}$$

$$\text{базис}\quad V\times \quad \begin{cases} |0_{V\times}\rangle = \dfrac{1}{\sqrt{2}}(|VV\rangle + i|HV\rangle), \\ |1_{V\times}\rangle = \dfrac{1}{\sqrt{2}}(|VV\rangle - i|HV\rangle). \end{cases} \tag{3}$$

Важно подчеркнуть, что состояния из разных базисов попарно неортогональны, т.е. достоверно не различимы.

Алиса случайно и равновероятно выбирает один из базисов, H или V. Далее внутри базиса она также равновероятно выбирает подбазис, "+" или "×". И наконец, она выбирает 0 или 1. На приемной стороне случайно и равновероятно выбирается одно из четырех измерений в базисах $H+$, $H\times$ или $V+$, $V\times$. Каждое из четырех измерений описывается разложением единицы в пространстве состояний кутритов:

$$\begin{aligned} I_{QTR} &= |HH\rangle\langle HH| + |HV\rangle\langle HV| + |VV\rangle\langle VV| = \\ &= |0_{H+}\rangle\langle 0_{H+}| + |1_{H+}\rangle\langle 1_{H+}| + |VV\rangle\langle VV| = \\ &= |0_{H\times}\rangle\langle 0_{H\times}| + |1_{H\times}\rangle\langle 1_{H\times}| + |VV\rangle\langle VV| = \\ &= |0_{V+}\rangle\langle 0_{V+}| + |1_{V+}\rangle\langle 1_{V+}| + |HH\rangle\langle HH| = \\ &= |0_{V\times}\rangle\langle 0_{V\times}| + |1_{V\times}\rangle\langle 1_{V\times}| + |HH\rangle\langle HH|. \end{aligned} \tag{4}$$

Каждое разложение единицы (4) описывает *отдельное измерение* в соответствующем базисе. При выборе определенного базиса каждому элементарному исходу (например, $0_{H+}, 1_{H+}, VV$) в нашем случае

сопоставляется ортогональный проектор на определенное *квантовое состояние композитной частицы – поляризационного кутрита*. Заметим, что в отсутствие подслушивателя, если состояния посылаются, например, в базисах $H+,\times$, то никогда не появится отсчетов, связанных с регистрацией состояний $|VV\rangle$ (канал измерений VV (4)). Отметим для дальнейшего, что в базисе $H+$ исходы $0_{H+}, 1_{H+}$ являются информационными, т.е. интерпретируются как 0 и 1, а отсчеты в канале измерений VV – контрольными.

Экспериментальные схемы приготовления и измерения квантовых состояний. Для приготовления семейства состояний бифотонов-кутритов используется схема, показанная на рис. 1. Спонтанное параметрическое рассеяние с синхронизмом первого типа рождается в нелинейном кристалле NC (бета-борат бария) в неколлинеарном вырожденном по частоте режиме. При этом волновые вектора сигнального и холостого фотонов отличаются только по направлению: $\mathbf{k}_s \neq \mathbf{k}_i$, $|\mathbf{k}_s| = |\mathbf{k}_i| = |\mathbf{k}_p|/2$, $\mathbf{k}_p$ – волновой вектор фотона накачки. На выходе кристалла поляризации обоих фотонов, составляющих бифотон, параллельны: $|V_s\rangle = |V_i\rangle$. Зеркала M2 и M3 выбираются поляризационно-нечувствительными, а зеркало M1 служит для блокировки мощного излучения лазерной накачки. Поляризационные преобразователи RP1 и RP2 унитарно преобразуют исходные поляризации каждого из фотонов в любую наперед заданную (произвольную), так что после отражения от зеркала M2 поляризационное состояние бифотона $|\Psi\rangle = |P_s\rangle \otimes |Q_i\rangle$, где $|P_s\rangle = \alpha|V_s\rangle + \beta|H_s\rangle$ и $|Q_i\rangle = \gamma|V_i\rangle + \eta|H_i\rangle$ – произвольные состояния сигнального и холостого фотонов соответственно. Интерференционный фильтр IF служит для выделения узкого спектрального диапазона $\Delta\omega$ в окрестности центральной частоты генерации $\omega_s = \omega_i = \omega_p/2$. Потери, вносимые зеркалом M2, несущественны, поскольку они влияют только на скорость генерации исходных состояний. Такая схема представляется предпочтительной в силу простоты экспериментальной реализации.

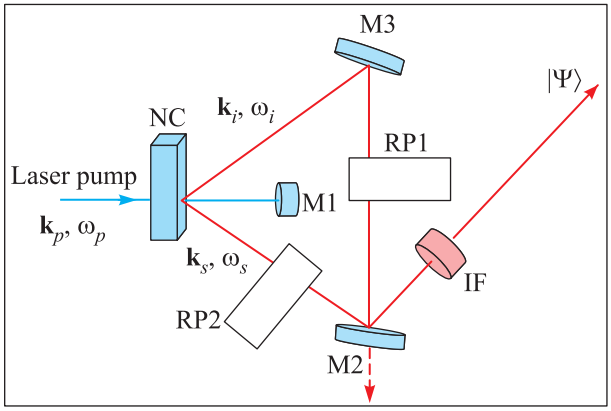

Рис. 1. Схема приготовления композитных состояний фотонов-кутритов.

Главная проблема при реализации измерений состоит в том, что конечной стадией регистрации состояний фотонного поля является отсчет (*click*) фотодетектора. На сегодняшний день детекторы, работающие в режиме счета фотонов, не различают число фотонов, а для измерений (4) требуется различать различные двухфотонные композитные состояния фотонного поля. Схема детектирования, реализующая измерения (4), представлена на рис. 2. Общая идея реализации состоит в разделении композитного двухфотонного состояния на пару отдельных фотонов с предварительными преобразованиями поляризационных и фазовых степеней свободы. Возможны ситуации, когда оба фотона попадают в один детектор. Для различения таких событий используется схема совпадений отсчетов. Учитывается только часть тех событий, которые дают отсчеты в двух разных детекторах. Проследим преобразования на примере выбора базиса $H+$, когда с передающей стороны посылается 0, $|0_{H+}\rangle = a_H^+ \frac{(a_H^+ + a_V^+)}{\sqrt{2}}|\text{vac}\rangle$. Удобно преобразовывать не состояния, а операторы, как это обычно делается в квантовой оптике [9]. Удобно также представить операторы, относящиеся к одному состоянию в каждом оптическом пути, в виде столбца для суперпозиций горизонтальной и вертикальной компонент

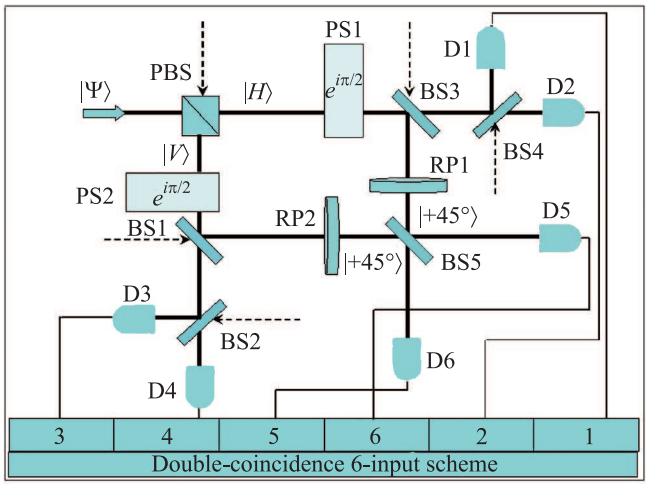

Рис.2. Схема измерения состояний кутритов. Оптические пути показаны жирными линиями, вакуумные оптические входы – штриховыми, электрические соединения – тонкими

операторов рождения: $\frac{(a_H^+ + a_V^+)}{\sqrt{2}} \to \frac{1}{\sqrt{2}} \begin{pmatrix} a_H^+ \\ a_V^+ \end{pmatrix}$. При прохождении состояния через поляризационный светоделитель (PBS) операторы преобразуются следующим образом:

$$\frac{1}{\sqrt{2}} \begin{pmatrix} a_H^+ \\ a_V^+ \end{pmatrix}_{|\psi\rangle} \to \frac{1}{\sqrt{2}} \begin{pmatrix} a_H^+ \\ 0 \end{pmatrix}_{|H\rangle} \otimes \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ a_V^+ \end{pmatrix}_{|V\rangle}.$$

После этого состояние попадает на фазовые модуляторы PS1 и PS2 в канале распространения $|H\rangle$ и $|V\rangle$:

$$\frac{1}{\sqrt{2}} \begin{pmatrix} a_H^+ \\ 0 \end{pmatrix}_{|H\rangle} \otimes \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ a_V^+ \end{pmatrix}_{|V\rangle} \to$$

$$\to \frac{1}{\sqrt{2}} \begin{pmatrix} e^{i\phi_H} a_H^+ \\ 0 \end{pmatrix}_{\mathrm{PSI}} \otimes \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ e^{i\phi_V} a_V^+ \end{pmatrix}_{\mathrm{PS2}}.$$

При этом в базисе $H+$ относительные фазы между компонентами поляризации не накладываются ($\phi_H = \phi_V = 0$). В базисе $H\times$ фаза изменяется на ($\phi_H = \pi/2$, $\phi_V = 0$), в $V+$ ($\phi_H = \phi_V = 0$), в $V\times$ ($\phi_H = 0$, $\phi_V = \pi/2$). Поскольку для примера рассматривается базис $H+$, после прохождения светоделителя BS3 имеем

$$\frac{1}{\sqrt{2}} \begin{pmatrix} e^{i\phi_H} a_H^+ \\ 0 \end{pmatrix}_{\mathrm{PSI}} \to$$

$$\to \frac{1}{2} \begin{pmatrix} e^{i\phi_H} a_H^+ \\ 0 \end{pmatrix}_{\mathrm{BS3}} \otimes \frac{1}{2} \begin{pmatrix} e^{i\phi_H} a_H^+ \\ 0 \end{pmatrix}_{\mathrm{RP1}}.$$

После прохождения следующего светоделителя, BS4 состояния перед детекторами D1 и D2 описываются операторами

$$\frac{1}{2} \begin{pmatrix} e^{i\phi_H} a_H^+ \\ 0 \end{pmatrix}_{\mathrm{BS3}} \to$$

$$\to \frac{1}{2\sqrt{2}} \begin{pmatrix} e^{i\phi_H} a_H^+ \\ 0 \end{pmatrix}_{\mathrm{D1}} \otimes \frac{1}{2\sqrt{2}} \begin{pmatrix} e^{i\phi_H} a_H^+ \\ 0 \end{pmatrix}_{\mathrm{D2}}.$$

Вторая "половина" суперпозиции состояний после светоделителя BS3 проходит через поляризационный преобразователь (например, четвертьволновую пластинку). Это приводит к повороту поляризации на угол 45°. Она становится равной

$$\frac{1}{\sqrt{2}} \begin{pmatrix} e^{i\phi_H} a_H^+ \\ 0 \end{pmatrix}_{\mathrm{PSI}} \to \frac{1}{2} \begin{pmatrix} e^{i\phi_H} a_H^+ \\ e^{i\phi_H} a_V^+ \end{pmatrix}_{\mathrm{RPI}}.$$

Поскольку левое ($|V\rangle$) и правое ($|H\rangle$) плечи интерферометра симметричны, преобразования операторов аналогичны рассмотренным выше. На входе светоделителя BS5, расположенного перед входом в фотодетекторы D5 и D6, возникает интерференция состояний, распространяющихся по левому и правому плечам интерферометра:

$$\frac{1}{2} \begin{pmatrix} e^{i\phi_H} a_H^+ \\ e^{i\phi_H} a_V^+ \end{pmatrix}_{\mathrm{RPI}} \otimes \frac{1}{2} \begin{pmatrix} e^{i\phi_V} a_H^+ \\ e^{i\phi_V} a_V^+ \end{pmatrix}_{\mathrm{RP2}} \to$$

$$\to \frac{1}{2\sqrt{2}} \begin{pmatrix} (e^{i\phi_H} + e^{i\phi_V}) a_H^+ \\ (e^{i\phi_H} + e^{i\phi_V}) a_V^+ \end{pmatrix}_{\mathrm{D5}} \otimes$$

$$\otimes \frac{1}{2\sqrt{2}} \begin{pmatrix} (e^{i\phi_H} - e^{i\phi_V}) a_H^+ \\ (e^{i\phi_H} - e^{i\phi_V}) a_V^+ \end{pmatrix}_{\mathrm{D6}}.$$

Аналогично производятся преобразования оператора a_H^+, описывающего второй фотон в состоянии $|0_{H+}\rangle$. Возможны различные комбинации отсчетов фотодетекторов в схеме совпадений. Оба фотона из композитного состояния могут попасть в один из детекторов. Такие события отбрасываются. Фотоны могут попасть и в разные детекторы. Часть таких событий также отбрасывается. Полезными являются только такие события (напомним, что речь идет о состояниях в базисе $H+$), когда срабатывает один из детекторов в каждой паре (D1 или D2 и D5 или D6). Действительно, если входным состоянием являлось $|0_{H+}\rangle$, то на входе детектора D5 появится состояние $|H\rangle + |V\rangle$ (с точностью до нормировочного множителя), а на входе детектора D6 из-за деструктивной интерференции состояний, распространяющихся по левому и правому плечам интерферометра, отсчета не будет. Второй фотон с поляризацией H попадает равновероятно на один из детекторов D1 или D2. На входах этих детекторов появляется состояние (с точностью до нормировочного множителя) $|H\rangle$. Если входным было состояние $|1_{H+}\rangle$, то конструктивная интерференция возникнет в детекторе D6, а в детекторе D5 из-за знака "минус" перед компонентой $|HV\rangle$ ($|1_{H+}\rangle = \frac{1}{\sqrt{2}}(|HH\rangle - |HV\rangle)$) будет наблюдаться деструктивная интерференция (отсутствие отсчета). Важно отметить, что из-за неразличимости (тождественности) фотонов неважно, какая из компонент состояния фотона с H-поляризацией пойдет в детекторы D1 и D2, а какая – в детекторы D5 и D6. Таким образом, события в детекторе D5 в базисе $H+$ при условии отсчета в одном из детекторов D1 или D2 интерпретируются как 0. Отсчет в детекторе D6 (также при условии отсчета в детекторах D1 или D2) интерпретируется как 1.

Поскольку состояния из базиса $H+$ и базиса $H\times$ неортогональны, подслушиватель принципиально не

может их различить. Последнее означает, что если вместо состояния из базиса $H+$ будет послано любое из состояний в базисе $H\times$, то это приведет к неполной деструктивной интерференции в одном из детекторов D5 или D6, что вызовет ошибки. Состояния из базисов $H+,\times$ и $V+,\times$ также попарно неортогональны. Поэтому, кроме ошибок при отсчетах в информационных детекторах D5 и D6, неизбежно возникнут отсчеты *в двух* детекторах D3 и D4. Такие события с некоторой вероятностью всегда будут происходить, поскольку если вместо любого состояния из базисов $H+,\times$ подслушиватель перепошлет любое состояние из базисов $V+,\times$, то возникнут одновременные отсчеты сразу в двух детекторах D3 и D4. Последнее будет иметь место из-за того, что такие состояния неизбежно содержат компоненты $|VV\rangle$, которые после разделения на поляризационно-чувствительном светоделителе PBS на входе интерферометра с некоторой вероятностью попадут в детекторы D3 и D4. Такие события интерпретируются как контрольные отсчеты. Они принципиально важны для достижения теоретического предела по ошибке в 50%. Аналогичная ситуация имеет место и в других базисах.

После передачи серии состояний легитимные пользователи отбрасывают посредством сообщений через открытый аутентичный канал связи те посылки, в которых базисы не совпадали. Отбрасываются также посылки (уже при совпадающих базисах), в которых были отсчеты, не соответствующие информационной таблице. Оставшиеся посылки содержат последовательность событий, которые интерпретируются как 0 и 1 либо как контрольные отсчеты. Доля контрольных отсчетов также раскрывается. Пусть доля контрольных отсчетов в сохраненной последовательности есть δ. Часть последовательности из посылок, в которых были отсчеты 0 или 1, раскрывается, и производится оценка вероятности ошибки Q. Далее раскрытая часть отбрасывается. В итоге на передающей стороне имеется последовательность 0 и 1, а на приемной – последовательность 0 и 1 (но с ошибками), а также позиции с контрольными отсчетами вместо 0 и 1. Данный протокол распределения ключей является двухпараметрическим: вторжение в квантовый канал связи приводит не только к ошибкам на приемной стороне с вероятностью Q, но и к контрольным отсчетам с вероятностью δ в тех контрольных детекторах, где их никогда не должно быть в отсутствие подслушивателя. Мы приводим таблицу для интерпретации различных событий в схеме совпадений фотоотсчетов в разных базисах.

Бит/базис	$H+,\times$	$V+,\times$
0	D5	D5
1	D6	D6
Контрольный отсчет	D3 или D4	D1 или D2

Критическая ошибка квантового протокола распределения ключей на кутритах. Покажем, что критическая ошибка протокола Q_c, до которой гарантируется секретное распределение ключей, может достигать теоретического предела в 50%. Получим длину секретного ключа в асимптотическом пределе бесконечно длинных передаваемых последовательностей. Как известно [10], наиболее общей атакой является коллективная атака: подслушиватель в каждой посылке использует вспомогательное состояние (*ancilla* – $|E\rangle_E$), которое приводится во взаимодействие с передаваемым состоянием. Взаимодействие описывается унитарным оператором U_{BE}. Затем, накапливая свои вспомогательные состояния в квантовой памяти, подслушиватель производит измерения сразу над всей последовательностью. Удобно считать, что копию посланного состояния Алиса сохраняет у себя, причем эта копия не доступна для подслушивателя. Исходное состояние имеет вид $|x\rangle_A\otimes|x\rangle_B\to|\psi\rangle_{ABE}=|x\rangle_A\otimes U_{BE}(|x\rangle_B\otimes|E\rangle_E)$, где $|x\rangle_{A,B}$ – одно из информационных состояний (2), (3). После измерений на приемной стороне и сохранения посылок с совпадающими базисами Алиса имеет битовую строку $X=\{0,1\}^n$, а Боб – последовательность $Y=\{0,1,c\}^n$. Поскольку ситуация симметрична по базисам, индекс базиса далее опускаем. После измерений на приемной стороне и интерпретации их результатов Алиса и Боб связаны классическим каналом с переходными вероятностями $p_{X|Y}(x|y)$:

$$p_{X|Y}(x|y)=$$
$$=\mathrm{Tr}_E\{{}_A\langle x|\otimes{}_B\langle y|\psi_R\rangle_{ABE}\,{}_{ABE}\langle\psi_R|y\rangle_B\otimes|x\rangle_A\},\quad(5)$$

где

$$|x\rangle_A=\{|0^{H,V,+,\times}\rangle_A,|1^{H,V,+,\times}\rangle_A\}\to\{0,1\}$$

и

$$|y\rangle_B=\{|0^{H,V,+,\times}\rangle_B,|1^{H,V,+,\times}\rangle_B,|VV\rangle_B$$

либо

$$|HH\rangle_B\}\to\{0,1,c\}.$$

Ситуация описывается совместным состоянием Алиса–Боб–Ева:

$$\sigma_{XYE}=\sum_{x\in X,y\in Y}\sigma_{xyE},$$

$$\sigma_{xyE}={}_A\langle x|\otimes{}_B\langle y|\psi\rangle_{ABE}\,{}_{ABE}\langle\psi|y\rangle_B\otimes|x\rangle_A.$$

Длина секретного ключа в асимптотическом пределе бесконечно длинных последовательностей $n \to \infty$ (точнее, доля секретных бит в пересчете на посылку) равна (детали см. в [10])

$$r_{\text{secr}} \le H(X|E) - H(X|Y). \tag{6}$$

Формула (6) учитывает как коррекцию ошибок, так и сжатие очищенного ключа универсальными хэш-функциями второго порядка [11, 12].

Вычисление условных квантовых энтропий фон Неймана достаточно провести только для матрицы плотности σ_{XYE}. Имеем $H(X|E) = H(\sigma_{XE}) - H(\sigma_E)$, $\sigma_{XE} = \mathrm{Tr}_Y\{\sigma_{XYE}\}$, $\sigma_E = \mathrm{Tr}_{XY}\{\sigma_{XYE}\}$, где $H(\sigma_{XE}) = -\mathrm{Tr}\{\sigma_{XE}\log\sigma_{XE}\}$ и $H(\sigma_E) = -\mathrm{Tr}\{\sigma_E\log\sigma_E\}$ – энтропии фон Неймана. Величина $H(X|Y)$ фактически является классической условной энтропией Шеннона для распределения вероятностей (5). Для вычисления энтропии фон Неймана $H(X|E)$ удобно воспользоваться энтропийными соотношениями неопределенностей [13]:

$$H(X|E) + H(X|Y) \ge 2\log\frac{1}{C}. \tag{7}$$

С учетом (2), (3) константа C в (7) равна $C = |{}_A\langle 0^{H+,\times}|0^{V+,\times}\rangle_A| = |{}_A\langle 0^{H+,\times}|1^{V+,\times}\rangle_A| = |{}_A\langle 1^{H+,\times}|1^{V+,\times}\rangle_A| = 1/2$. С учетом симметрии между 0 и 1, а также симметрии между базисами после измерений, для длины секретного ключа находим

$$r_{\text{secr}} \le 2\log\frac{1}{C} - 2H(X|Y). \tag{8}$$

После измерений на приемной стороне, корреляция между последовательностями символов X у Алисы и Y у Боба описывается симметричным классическим каналом связи с двумя состояниями на входе и тремя – на выходе (рис. 3). С учетом симметрии

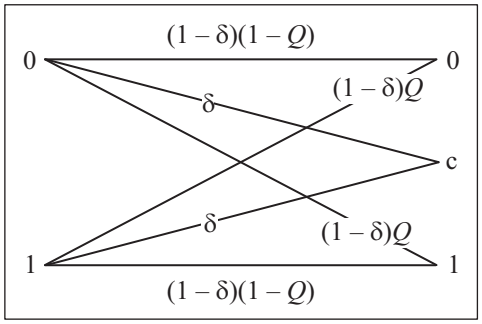

Рис. 3. Схематическое изображение классического канала связи Алиса–Боб

и условий нормировки условных вероятностей параметризация осуществляется однозначно. Последнюю удобно выбрать в следующем виде: $p_{X|Y}(0|0) = p_{X|Y}(1|1) = (1-\delta)(1-Q)$, $p_{X|Y}(0|1) = p_{X|Y}(1|0) = (1-\delta)Q$, $p_{X|Y}(0|c) = p_{X|Y}(1|c) = \delta$. Величины δ и Q имеют смысл вероятности отсчетов в контрольных детекторах (D3 и D4 для базисов $H+,\times$, D1 и D2 для базисов $V+,\times$) и вероятности ошибки в информационных детекторах D5 и D6. Окончательно для длины секретного ключа находим

$$r_{\text{secr}} \le \left[1 - (1-\delta)h(Q) - h(\delta)\right], \qquad h(z) = -z\log_2 z - (1-z)\log_2(1-z). \tag{9}$$

При некоторых критических значениях (δ_c, Q_c) длина секретного ключа (9) обращается в нуль: $r_{\text{secr}}(\delta_c, Q_c) = 0$. Наблюдаемые параметры (δ, Q) находятся “ в руках” подслушивателя. Однако Алиса и Боб могут объявить, что протокол будет прерываться, если вероятность δ контрольных отсчетов превысит некоторую величину, близкую к нулю ($\delta \approx 0$). В этом случае подслушивателю остается только возможность регулировать величину наблюдаемой ошибки Q. Как видно из (9), при $\delta \to 0$ критическая ошибка протокола $Q_c \to 1/2$, т.е. стремится к теоретическому пределу.

Заключение. В работе предложена практическая схема квантового распределения ключей, использующая кодирование ключа в поляризационные степени свободы композитных состояний пары фотонов – поляризационного кутрита. Критическая ошибка, до которой гарантируется секретное распределение ключей в данной схеме, достигает величины 50%, что существенно превышает критическую ошибку для всех известных протоколов.

Работа частично поддержана проектами РФФИ # 10-02-00204 и 11-02-00455.

1. W. K. Wootters and W. H. Zurek, Nature **299**, 802 (1982).
2. C. H. Bennett and G. Brassard, *Proc. of IEEE Int. Conf. on Comput. Sys. and Sign. Proces.*, Bangalore, India, 1984, p. 175.
3. C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
4. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf et al., Rev. Mod. Phys. **81**, 1301 (2009).
5. L. Lydersen, C. Wiechers, C. Wittmann et al., Nature Photonics **4**, 686 (2010).
6. N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002).

7. Д. Н. Клышко, *Когерентный распад фотонов в нелинейной среде. Доклад на всесоюзном совещании по нелинейным свойствам сред*, Черноголовка, 1966; Д. Н. Клышко, Письма в ЖЭТФ **6**, 4902 (1967).
8. Д. Н. Клышко, А. Н. Пенин, Б. Ф. Полковников, Письма в ЖЭТФ **2**, 11 (1970).
9. Л. Мандель, Э. Вольф, *Оптическая когерентность и квантовая оптика*, М.: Физматлит, 2000, 895 с. [L. Mandel and E. Wolf, *Optical Coherence and Quantum Optics*, Cambridge University Press, 1995].
10. R. Renner, arXiv/quant-ph: 0512258.
11. J. L. Carter and M. N. Wegman, J. Comp. Syst. Sci. **18**, 143 (1979).
12. C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, IEEE Trans. on Inf. Theory **41**, 1915 (1995).
13. M. Tomamichel and R. Renner, arXiv/quant-ph: 10092015.