Письма в ЖЭТФ, том 91, вып. 1, с. 51 – 57 © 2010 г. 10 января

Квантовое распределение ключей с детерминистическим приготовлением и измерением квантовых состояний

С. Н. Молотков

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

Академия Криптографии Российской Федерации, Москва, Россия

Факультет вычислительной математики и кибернетики, МГУ им. М.В. Ломоносова, 199991 Москва, Россия

Поступила в редакцию 8 декабря 2009 г.

Предложена новая детерминистическая оптическая схема для приготовления и регистрации квантовых состояний в квантовой криптографии, которая позволяет увеличить эффективность, при прочих равных условиях, в 4 раза по сравнению со всеми существующими системами. Таким образом, эффективность оптической части доведена до максимума в части приготовления и регистрации квантовых состояний.

Введение. Квантовая криптография – квантовое распределение ключей, позволяет не только обнаруживать любые попытки подслушивания при передаче ключей, но и гарантировать секретность ключей, если поток ошибок на приемной стороне не превосходит некоторой критической величины, зависящей от протокола (способа) передачи ключей [1]. Причем секретность ключей гарантируется не техническими или вычислительными ограничениями подслушивателя, а фундаментальными запретами квантовой механики на различимость неортогональных квантовых состояний. Последнее, фактически, является следствием соотношений неопределенности Гайзенберга для некоммутирующих наблюдаемых [2, 3].

Любая система квантовой криптографии на физическом уровне содержит на передающей стороне устройства для приготовления квантовых состояний. Процедура приготовления называется кодированием – сопоставлением классическим битам 0 и 1 квантовых состояний по специальному протоколу. На приемной стороне осуществляется преобразование квантовых состояний к форме, приемлемой для регистрации фотодетекторами.

На формальном уровне в квантовой механике нет принципиальных запретов на приготовление любого квантового состояния с вероятностью, равной единице. Аналогично нет формальных ограничений для регистрации любого из набора ортогональных состояний также с вероятностью единица.

В реальности существуют экспериментальные, но не фундаментальные, ограничения для приготовления и детектирования состояний. Принята следующая терминология. Если экспериментальная схема позволяет приготовить (или измерить) квантовое состояние с достоверностью (вероятностью единица), то такая схема приготовления (измерения) называется детерминистической. Если экспериментальная схема устроена таким образом, что приготовление (измерение) состояний происходит лишь с определенной вероятностью, то схема называется вероятностной.

Поскольку речь идет о фотонах, то будем иметь в виду оптическую схему. Более того линейную оптическую схему, которой будет достаточно для наших целей. Любая оптическая схема, с формальной точки зрения, реализует унитарное преобразование входных квантовых состояний в выходные. Детерминистическое приготовление состояний, применительно к нашему случаю, означает, что если на один из входов схемы подается квантовое состояние, то на выходе в одном из каналов с вероятностью единица будет нужное квантовое состояние. В вероятностной схеме, если каждый раз на один из входов подается квантовое состояние, то на одном из выходов будет требуемое квантовое состояние, но с вероятностью меньше единицы. Причем появление на нужном выходе квантового состояния будет случайным и неконтролируемым. На остальных выходах, в силу унитарности схемы, также случайно будут возникать квантовые состояния, которые приходится отбрасывать.

Если в экспериментах по квантовой оптике, которые всегда проводятся с накоплением статистики фотоотсчетов, вероятностное приготовление и регистрация квантовых состояний не играет критической роли, то в квантовой криптографии, где *каждый* отсчет дает вклад в ключ, разница между вероятностной и детерминистической регистрациями (приготовлением) квантовых состояний играет принципиальную роль.

Протокол квантового распределения ключей BB84 [1] как базовый используется практически во всех системах квантовой криптографии. В протоколе BB84 используются два сопряженных базиса $+$ и $\times$. Информационные состояния в базисе $+$ имеют вид

$$|0^+\rangle = \frac{1}{\sqrt{2}}(|1\rangle + |2\rangle), \quad |1^+\rangle = \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle), \qquad (1)$$

и в сопряженном базисе $\times$

$$|0^\times\rangle = \frac{1}{\sqrt{2}}(|1\rangle + i|2\rangle), \quad |1^\times\rangle = \frac{1}{\sqrt{2}}(|1\rangle - i|2\rangle). \qquad (2)$$

Состояния, отвечающие 0 и 1 внутри каждого базиса, ортогональны, поэтому при известном базисе достоверно различимы. В разных базисах состояния попарно неортогональны, то есть достоверно неразличимы, что неизбежно приводит к ошибке подслушивателя (см. [1, 4]).

Практически во всех оптоволоконных системах квантовой криптографии логические биты кодируются в относительную разность фаз между базисными состояниями $|1\rangle$ и $|2\rangle$ – $\frac{1}{\sqrt{2}}(|1\rangle + e^{i\varphi}|2\rangle)$.

Выбор относительной фазы следующий (см. таблицу:

Basis	Bit	Alice φ_A	Bob φ_B
$+$	0	$\varphi_A = 0$	$\varphi_B = 0$
	1	$\varphi_A = \pi$	
$\times$	0	$\varphi_A = \frac{\pi}{2}$	$\varphi_B = \frac{\pi}{2}$
	1	$\varphi_A = \frac{3\pi}{2}$	

(3)

На сегодняшний день в качестве источника однофотонных (точнее, квазиоднофотонных) состояний используется сильно ослабленное, до уровня 0.1–0.2 в среднем фотона в импульсе, лазерное излучение. Поскольку выходное излучение лазера является когерентным состоянием с пуассоновской статистикой по числу фотонов, то это означает, что в среднем примерно в каждой десятой посылке присутствует однофотонный пакет, а в остальных посылках в канал ничего не поступает (на выходе вакуумное состояние). Остальные посылки с экспоненциально убывающей вероятностью по числу фотонов содержат два, три и т.д. фотонов. Хотя нужно отметить, что имеются эксперименты (см., например, [5]) по созданию истинно однофотонных источников для целей квантовой криптографии. В тех непустых посылках, когда в канал поступает однофотонный пакет, состояние может быть представлено в виде

$$|\psi_j\rangle = \int_0^\infty dk e^{-ik\tau_j}\psi(k)|k\rangle, \quad |k\rangle = a^+(k)|\mathrm{vac}\rangle,$$

где $a^+(k)$ – оператор рождения состояния с импульсом k (рассматриваем состояния, распространяющиеся в одном направлении), $|\mathrm{vac}\rangle$ – вакуумное состояние. Чтобы прояснить смысл τ_j, удобно перейти в пространственно-временное представление. Имеем

$$|\psi_j\rangle = \int_{-\infty}^\infty d\tau\psi(\tau - \tau_j)|\tau\rangle, \quad |\tau\rangle = \int_0^\infty dk e^{-i\tau k}|k\rangle,$$

$$\psi(\tau) = \int_0^\infty dk e^{ik(\tau-\tau_j)}\psi(k), \quad \tau = x - c_f t,$$

здесь c_f – скорость распространения в оптоволокне. Таким образом, τ_j отвечает за момент приготовления состояния. Считаем, что состояние $|\psi_j\rangle$ является локализованным во временно́м окне $(\tau_j - \delta, \tau_j + \delta)$. Вероятность получения отсчета при измерении во временном окне $d\tau$ равна

$$\Pr(d\tau) = \mathrm{Tr}\{|\tau\rangle\langle\tau|\psi\rangle\langle\psi|\}d\tau = |\psi(\tau)|^2 d\tau.$$

Считаем, что состояние локализовано во временно́м окне $(\tau_j - \delta, \tau_j + \delta)$ $(\delta \ll \tau_{j+1} - \tau_j)$. Далее для краткости будем обозначать такое состояние как $|j\rangle$. Далее будем иметь дело только с состояниями, которые являются суперпозицией состояний, локализованных в равно отстоящих по времени интервалах, тогда можно считать набор таких локализованных состояний, базисными.

Все опубликованные работы по оптоволоконной квантовой криптографии используют вероятностную схему приготовления и регистрации квантовых состояний. Идея использования интерферометра для приготовления и регистрации состояний в квантовой криптографии восходит к работе [2], которая впоследствии стала общепринятой, и как базовая используется во всех известных работах по реализации систем квантовой криптографии [6–27] (рис.1))[1].

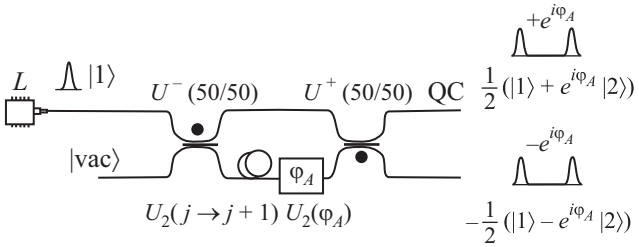

Рис.1. Стандартная оптическая схема для вероятностного приготовления квантовых состояний в BB84

Вероятностное приготовление состояний. Интерферометр Маха-Цандера необходим для того,

[1] Для самодостаточности работы и удобства чтения приводится стандарная схема приготовления и детектирования состояний.

чтобы из однофотонного состояния, локализованного в одном временно́м окне, получить любое из четырех информационных состояний (1). После запуска лазера на короткое время возникает локализованное квантовое состояние, которое после прохождения по верхнему и нижнему путям разбалансированного интерферометра Маха-Цандера, преобразуется в новое состояние, представляющее собой *суперпозицию* двух базисных состояний, локализованных в двух соседних временны́х окнах. Расстояние по времени между передним и задним фронтом ("половинками") равно разности хода по верхнему и нижнему пути интерферометра.

Для изменения относительной фазы используется фазовый модулятор, который включается на определенное время. Физически фазовый модулятор на основе пьезоэлемента изменяет длину оптического пути по верхнему или нижнему плечам.

Подчеркнем, что состояние в верхнем и нижнем выходах – это единое квантовое состояние. Нормировка квадратов модулей амплитуд по верхнему и нижнему выходам в сумме дает единицу. Кроме того, форма пространственно-временны́х амплитуд состояния в разных плечах одинакова, поскольку данное состояние получено из одного квантового состояния посредством "расщепления" на симметричном светоделителе. К тому же, если детектировать состояние, то результат регистрации возникнет *случайно с вероятностью* $1/2$ *лишь в одном канале.* Таким образом, в канал связи по одному выходу поступит квантовое состояние требуемого вида лишь с вероятностью $1/2$. Случайно с вероятностью $1/2$ также возникает состояние на втором (холостом) выходе, то есть при каждом запуске лазера в канал пойдет состояние лишь в половине посылок.

Светоделитель 50/50, задержка, "постоянный" и переменный фазовые модуляторы. Действие различных оптических элементов может быть описано следующим набором операторов[2)]:

$$U^{\pm}(50/50) = \frac{1}{\sqrt{2}} \begin{pmatrix} I & \pm I \\ \mp I & I \end{pmatrix},$$
$$U_2(j \to j+1) = \begin{pmatrix} I & 0 \\ 0 & \sum_{j=-\infty}^{\infty} |j+1\rangle\langle j| \end{pmatrix}, \tag{4}$$

$$U_2(\varphi) = \begin{pmatrix} I & 0 \\ 0 & e^{i\varphi} I \end{pmatrix},$$
$$U_2(\pi_1) = \begin{pmatrix} I & 0 \\ 0 & e^{i\pi}|1\rangle\langle 1| + \sum_{j=-\infty, j\neq 1}^{\infty} |j\rangle\langle j| \end{pmatrix}. \tag{5}$$

Светоделитель ($U^{\pm}(50/50)$) выполняет роль полупрозрачного зеркала. С формальной точки зрения, осуществляет унитарный поворот между состояниями в двух пространственных каналах. На рисунках точка на светоделителе указывает на канал прохождения (отражения) с изменением фазы на π.

Линия задержки ($U_2(j \to j+1)$) – в нижнем (верхнем) плече интерферометра. На физическом уровне любое состояние локализованное в окне j сдвигается на одну позицию ($\tau_{j+1} - \tau_j$) по времени. Физическая реализация представляет собой дополнительный кусок оптоволокна.

"Постоянный" фазовый модулятор ($U_2(\varphi)$) – в нижнем (верхнем) плече инферферометра. Это управляемая линия задержки на основе пьезоэлемента, которая приводит к изменению длины оптического пути на величину порядка длины волны. Приложение напряжения к фазовому модулятору приводит к сдвигу состояния по времени и появлению дополнительной разности фаз между состояниями в верхнем и нижнем плечах интерферометра. Под "постоянным" здесь понимается модулятор, к которому напряжение прикладывается в начале каждой посылки и остается неизменным до следующей посылки состояний.

Переменный фазовый модулятор в нижнем ($U_2(\pi_1)$) (или верхнем) плече. Смысл действия сводится к тому, что к данному модулятору прикладывается напряжение *только на момент прохождения передней или задней "половинки" состояния в одном и том же плече.* В отличие от "постоянного" фазового модулятора, который приводит к дополнительной разности фаз между амплитудами состояний в разных (верхнем и нижнем) каналах, данный фазовый модулятор изменяет относительную разность фаз между передней и задней "половинками" состояния в одном и том же плече интерферометра. Обычно такой способ модуляции используют при интегральном

[2)] Отметим во избежании путаницы, что операторы (4)–(6) не следует путать с операторами однокубитных операций, обычно используемых в квантовых схемах (см., например, [27]), и в которых элементы матрицы являются числами (матричными элементами оператора) в каком-то вычислительном базисе, которые действуют на коэффициенты разложения квантового состояния в этом базисе. Здесь сами матричные элементы являются операторами, которые действуют на *сами квантовые состояния* в разных пространственных каналах (плечах интерферометра).

оптоволоконном интерферометре Маха-Цандера, в котором нельзя вставить модулятор непосредственно в плечо интерферометра [24, 25].

$$U_1(\varphi) = \begin{pmatrix} e^{i\varphi} I & 0 \\ 0 & I \end{pmatrix},$$
$$U_1(j \to j+1) = \begin{pmatrix} \sum_{j=-\infty}^{\infty} |j+1\rangle\langle j| & 0 \\ 0 & I \end{pmatrix}, \quad (6)$$

и, наконец, единичный оператор

$$I = \sum_{j=-\infty}^{\infty} |j\rangle\langle j|.$$

Полный оператор, описывающий оптический тракт передающей части, имеет вид (см. рис.1)

$$U_{\text{Prob}}^{\text{Prep}}(\varphi_A) = U^-(50/50) U_2(j \to j+1) U_2(\varphi_A) U^+(50/50). \quad (7)$$

Входным состоянием является локализованное однофотонное состояние по верхнему каналу, которое удобно записать в виде вектор-столбца $\begin{pmatrix} |1\rangle \\ |\text{vac}\rangle \end{pmatrix}$, с учетом того, что вакуумное состояние ортогонально всем операторам в (4–6), имеем на выходе состояние

$$U_{\text{Prob}}^{\text{Prep}}(\varphi_A) \begin{pmatrix} |1\rangle \\ |\text{vac}\rangle \end{pmatrix} = \frac{1}{2} \begin{pmatrix} (|1\rangle + e^{i\varphi_A}|2\rangle) \\ -(|1\rangle - e^{i\varphi_A}|2\rangle) \end{pmatrix}. \quad (8)$$

Работа схемы достаточно проста. В каждой посылке локализованное по времени состояние на первом светоделителе "расщепляется" на верхний и нижний пути интерферометра с одинаковыми амплитудами. Задерживается в нижнем плече, а затем происходит управляемое изменение оптической длины пути посредством приложения напряжения к модулятору. Данное изменение оптического пути приводит к появлению относительной разности фаз для амплитуд в нижнем и верхнем плечах. На втором светоделителе амплитуда в верхнем плече и задержанная с дополнительной фазой в нижнем плече, "расщепляются" на два канала. Амплитуда по верхнему выходу идет в линию связи, а второй выход является холостым.

Таким образом, каждое состояние, поступающее на вход интерферометра, только с вероятностью $1/2$ поступает затем в линию связи.

Вероятностные измерения состояний. На рис.2 представлена стандартная схема, используемая во всех работах по детектированию состояний в квантовой криптографии[3)]. На приемной стороне Боб случайно и независимо от Алисы выбирает базис (фактически относительную фазу между двумя "половинками" квантового состояния в соответствии с таблицей). После проведения серии посылок Алисы и измерений Боба, через открытый канал Алиса и Боб раскрывают базисы, которые они использовали (+ или ×), но не раскрывают сами состояния (0 или 1). Посылки, где базисы не совпадали, отбрасываются. В оставшихся посылках выбор базисов (относительных фаз) у них синхронизирован. Боб производит измерения в центральном временно́м окне 2. Отсчет по верхнему детектору происходит с вероятностью (11,12) и указывает Бобу, какой бит, 0 или 1, посылала Алиса. *Однако отсчеты в информационном окне 2 происходят лишь с суммарной вероятностью* $1/2$. *В остальных временны́х (боковых 1 и 3) окнах отсчеты происходят суммарно по всем окнам с вероятностью* $1/2$. Данные отсчеты не несут для Боба никакой информации о передаваемом Алисой бите, поэтому отбрасываются как "мусорные". Таким образом, после отбрасывания посылок при согласования базисов, из каждой дошедшей до Боба посылки лишь половина идет в ключ, то есть эффективный выход на приемной стороне равен $1/2$.

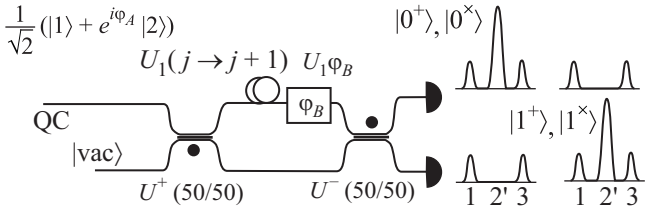

Рис.2. Стандартная оптическая схема для вероятностного детектирования квантовых состояний в BB84

На формальном уровне преобразование на приемной части описывается следующим оператором.

$$U_{\text{Prob}}^{\text{Measure}}(\varphi_B) = U^+(50/50) U_1(j \to j+1) U_1(\varphi_B) U^-(50/50). \quad (9)$$

На вход поступает нормированное квантовое состояние. Состояние на выходе перед детекторами имеет вид

[3)] Отметим, что двухпроходные схемы квантовой криптографии [15, 16, 18 – 21], где процедуры и регистрации происходят на одной из сторон, также используют вероятностный способ, поскольку используют базовый элемент на основе интерферометра Маха-Цандера, аналогичный рис.1, 2.

$$U_{\rm Prob}^{\rm Measure}(\varphi_B)\frac{1}{\sqrt{2}}\begin{pmatrix}(|1\rangle+e^{i\varphi_A}|2\rangle)\\|{\rm vac}\rangle\end{pmatrix}=$$

$$\frac{1}{\sqrt{8}}\begin{pmatrix}(|1\rangle+(e^{i(\varphi_A}+e^{i\varphi_B)})|2\rangle+e^{i(\varphi_A+\varphi_B)}|3\rangle)\\(-|1\rangle-(e^{i(\varphi_A}-e^{i\varphi_B)})|2\rangle+e^{i(\varphi_A+\varphi_B)}|3\rangle)\end{pmatrix}. \quad (10)$$

Работа схемы аналогична работе передающей части. Разница лишь в том, что на вход поступает состояние из суперпозиции двух "половинок". По верхнему пути амплитуды (обе "половинки") задерживаются и приобретают общую относительную фазу по отношению к амплитудам в нижнем плече. Выходной светоделитель обеспечивает интерференцию передней "половинки" по нижнему каналу и задней "половинки" задержанного в верхнем плече состояния. По существу, это интерференция нулевого порядка в том смысле, что пакет интерферирует сам на себе, поскольку передняя и задняя "половинки" происходят из одного и того же состояния. Фаза в каждой посылке выбирается такой, чтобы состояния, отвечающие единице, конструктивная интерференция передней верхней и задней нижней "половинок" имела место в верхнем детекторе (up), а деструктивная – на нижнем (down). Для нуля, наоборот, конструктивное сложение амплитуд имеет место по нижнему детектору, а деструктивное (гашение интерференции) – по верхнему.

Детекторы работают в стробируемом режиме – активируются только в определенное временно́е окно. При этом вероятность срабатывания детектора пропорциональна квадрату модуля амплитуды квантового состояния в этом временно́м окне. Вероятность детектирования по верхнему каналу в информационном временно́м окне 2 есть

$$\Pr(2,{\rm up})=\frac{1}{8}|e^{i\varphi_A}+e^{i\varphi_B}|^2, \quad (11)$$

соответственно, по нижнему каналу во втором окне

$$\Pr(2,{\rm down})=\frac{1}{8}|e^{i\varphi_A}-e^{i\varphi_B}|^2. \quad (12)$$

Вероятности отсчетов в остальных окнах, 1 и 3, по верхнему и нижнему детекторам не зависят от разности фаз, являются "мусорными" и отбрасываются. Имеем

$$\Pr(1,{\rm down})=\Pr(1,{\rm up})=\Pr(3,{\rm down})=\Pr(3,{\rm up})=\frac{1}{8}. \quad (13)$$

Вероятность таких событий составляет $1/2$. Соответственно вероятность полезных информационных отсчетов также $1/2$. Таким образом, суммарная эффективность передающей и приемной частей равна $1/4$ (естественно, без учета отбрасывания примерно половины посылок при согласовании базисов.)

Возникает вопрос, нельзя ли сделать детерминистическими приготовление и измерение состояний. Такая схема предлагается ниже и позволяет увеличить эффективность системы в 4 раза.

Детерминистическое приготовление состояний. Приведем новую схему, которая позволяет детерминированно на каждое, поступающее на вход схемы состояние, посылать преобразованное состояние в канал связи. Оптическая схема для детерминированного приготовления квантовых состояний приведена на рис.3. Оператор, описывающий работу данной схемы, имеет вид

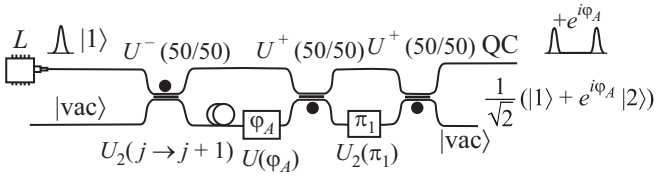

Рис.3. Оптическая схема для детерминистического приготовления квантовых состояний

$$U_{\rm Determ}^{\rm Prep}(\varphi_A)=U^-(50/50)U_2(j\to j+1)\times$$
$$\times U_2(\varphi_A)U^+(50/50)U(\pi_1)U^+(50/50). \quad (14)$$

Входным в каждой посылке является состояние аналогичное предыдущему случаю. Состояние на выходе имеет вид

$$U_{\rm Determ}^{\rm Prep}(\varphi_A)\begin{pmatrix}|1\rangle\\|{\rm vac}\rangle\end{pmatrix}=\frac{1}{\sqrt{2}}\begin{pmatrix}(|1\rangle+e^{i\varphi_A}|2\rangle)\\|{\rm vac}\rangle\end{pmatrix}. \quad (15)$$

Как следует из (15), в каждой посылке с вероятностью единица в канал связи поступает требуемое состояние.

В схему добавлена пара новых существенны́х элементов. Первый элемент – дополнительный светоделитель, который фактически приводит к формированию второго интерферометра Маха-Цандера с равной длиной плеч в верхнем и нижнем каналах[4)]. Второй элемент – управляемый фазовый модулятор, который меняет относительную разность фаз между двумя половинками в нижнем плече второго интерферометра. Вместе данные элементы позволяют "погасить"

[4)] Отметим, что на рисунках, чтобы не загромождать их техническими (хотя и существенными) деталями, не приведены тонкие подстройки разности длин плеч, которые всегда присутствуют (см., например, в [22]).

состояние на холостом выходе. В итоге, в каждой посылке состояние, поступающее на вход схемы, с вероятностью единица поступает в канал связи в виде преобразованного состояния.

Детерминистическое измерение состояний. Схема для детерминистического измерения состояний приведена на рис.4. Данной схеме отвечает опе-

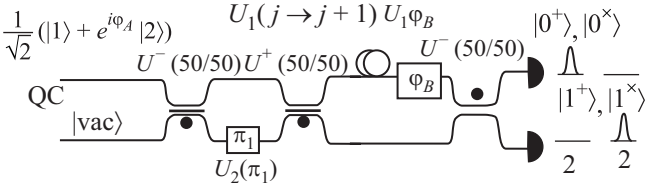

Рис.4. Оптическая схема для детерминистического измерения квантовых состояний

ратор

$$U^{\mathrm{Measure}}_{\mathrm{Determ}}(\varphi_B) = U^+(50/50)U_2(\pi_1) \times$$
$$\times\, U^+(50/50)U_1(j \to j+1)U_1(\varphi_B)U^-(50/50). \quad (16)$$

Входным является одно из состояний (1). Для выходного состояние перед детекторами находим

$$U^{\mathrm{Measure}}_{\mathrm{Determ}}(\varphi_B)\frac{1}{\sqrt{2}}\begin{pmatrix} (|1\rangle + e^{i\varphi_A}|2\rangle) \\ |\mathrm{vac}\rangle \end{pmatrix} =$$
$$= \frac{1}{2}\begin{pmatrix} (e^{i\varphi_A} + e^{i\varphi_B})|2\rangle \\ -(e^{i\varphi_A} - e^{i\varphi_B})|2\rangle \end{pmatrix}. \quad (17)$$

Дополнительный светоделитель и управляемый переменный фазовый модулятор в нижнем плече позволяют избавиться от "мусорных" не информационных компонент состояния перед детекторами во временны́х окнах 1 и 3. Все выходные состояния локализованы только во втором временно́м окне, причем с нужными фазовыми соотношениями. Таким образом, если после согласования базисов произошел отсчет в верхнем детекторе, то это событие однозначно и с вероятностью единица интерпретируется Бобом как логический 0. Срабатывание нижнего детектора во 2 временно́м окне также однозначно интерпретируется как логическая 1.

Заключение. Предложена новая схема приготовления и детектирования квантовых состояний, которая позволяет увеличить быстродействие по сравнению со всеми известными реализациями систем квантовой криптографии в 4 раза при прочих равных условиях. *Детерминистическое приготовление состояний становится особенно важным при строго однофотонном источнике.* При каждом акте испускания в канал гаратированно будет поступать нужное квантовое состояние. В случае использования квазиоднофотонного источника (ослабленного лазерного излучения) увеличение эффективности на передающей части в 2 раза не столь принципиально, так как всегда используется ослабитель, который может быть вставлен непосредственно перед входом в квантовый канал связи. При этом интенсивность излучения лазера на входе в оптическую схему и величина ослабления аттенюатора подобраны так, чтобы в среднем в канал связи поступало 0.1–0.2 фотона в импульсе.

Детерминистическое детектирование принципиально важно, поскольку квантовая эффективность фотодетекторов в телекоммуникационном диапазоне длин волн 1.3–1.55 мкм не высока.

Таким образом, при детерминистическом приготовлении и регистрации квантовых состояний устранены все ограничения по эффективности, вытекающие из структуры оптической схемы, тем самым достигнута предельная эффективность – приготовление квантовых состояний на передающей стороне и их преобразование на приемной стороне перед регистрацией фотодетекторами происходят с вероятностью единица.

Выражаю благодарность коллегам по Академии Криптографии Российской Федерации за постоянную поддержку. Автор также благодарит С.П. Кулика и А.Н. Пенина за полезные обсуждения. Работа частично поддержана проектом Российского фонда фундаментальных исследований # 08-02-00559.

1. C. H. Bennett, G. Brassard, Proc.of IEEE Int. Conf. on Comput. Sys. and Sign. Proces., Bangalore, India, December 1984, p. 175.
2. C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992); C. H. Bennett, *Interferometric Quantum Key Distribution System*, April 26 (1994), Date of Patent, Patent Number 5, 307, 410.
3. W. K. Wooters, W. H. Zurek, Nature **299**, 802 (1982).
4. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, arXiv:quant-ph/0101098; Rev. Mod. Phys. **74**, 145 (2002).
5. T. Gaebel, I. Popa, A. Gruber et al., New. J. of Phys. **6**, 98 (2004).
6. R. J. Hughes, G. L. Morgan, and C. G. Peterson, arXiv:quant-ph/9904038.
7. R. J. Hughes, D. M. Alde, P. Dyer et al., Contemp. Phys. **36**, 149 (1995).
8. R. J. Hughes, G. G. Luther, G. L. Morgan et al., *Quantum Cryptography over undergraond Optical Fibers*, Proc. Advances in Cryptology – Crypto'96, Springer-Verlag, Berlin, 1996, p. 329.

9. A. Muller, J. G. Rarity, P. R. Tapster et al., Elec. Lett. **23**, 634 (1993).
10. A. Muller, H. Zbinden, and N. Gisin, Europhys. Lett. **33**, 335 (1996).
11. C. Marand and P. D. Townsend, Opt. Lett. **20**, 1695 (1995).
12. P. D. Townsend, Nature **385**, 47 (1997).
13. P. D. Townsend, Elec. Lett. **30**, 809 (1994).
14. J. D. Franson and H. Ilves, Appl. Opt. **33**, 2949 (1994).
15. A. Muller, H. Zbinden, and N. Gisin, Nature **378**, 449 (1995).
16. H. Zbinden, J. D. Gautier, N. Gisin et al., Electron. Lett. **33**, 586 (1997).
17. A. Muller, T. Herzog, B. Huttner et al., Appl. Phys. Lett. **70**, 793 (1997).
18. D. Stucki, N. Gisin, O. Guinnard et al., New J. of Phys. **4**, 41.1 (2002).
19. D. S. Bethune and W. P. Risk, *An Autocompensating Quantum Key Distribution System using Polarization Splitting of Light*, IQEC'98 Digest of Postdeadline Papers, vol. QPD12-2, May, 1998.
20. D. S. Bethune and W. P. Risk, IEEE J. of Quantum Elecr. **36**, 340 (2000).
21. D. S. Bethune, M. Navarro, and W. P. Risk, arXiv:quant-ph/0104089.
22. C. Elliott, D. Pearson, and G. Troxel, arXiv:quant-ph/0307049.
23. C. Elliott, A. Colvin. D. Pearson et al., arXiv:quant-ph/0503058; C. Elliot, New J. of Phys. **4**, 46.1 (2002).
24. Y. Nambu, T. Hatanaka, H. Yamazaki, and K. Nakamura, arXiv:quant-ph/0404015.
25. T. Kimura, Y. Nambu, T. Hatanaka et al., arXiv:quant-ph/0603041.
26. Y. Nambu, K. Yoshino, and A. Tomita, arXiv:quant-ph/0403104.
27. M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2001 (М. Нильсен, И. Чанг, *Квантовые вычисления и квантовая информация*, М.: Мир, 2006).