PACS 03.67.Dd; 03.67.Pp

Анализ предельно возможных информационных характеристик протоколов квантовой криптографии

Д.В.Сыч, Б.А.Гришанин, В.Н.Задков

Исследуется вопрос об увеличении критического уровня допустимых ошибок протоколов квантовой криптографии за счет варьирования набора букв в квантовом алфавите при фиксированной размерности пространства. Рассматриваются квантовые алфавиты, образующие правильные многогранники на сфере Блоха, и континуальный алфавит, равноправно включающий все квантовые состояния. Показано, что из рассмотренных протоколов наивысшим критическим уровнем ошибок до согласования базисов обладает протокол с алфавитом в виде тетраэдра, а после согласования базисов – протокол с континуальным алфавитом.

Ключевые слова: *оптическая обработка квантовой информации, квантовая криптография.*

1. Введение

С момента появления идеи квантовой криптографии (КК) [1] и до настоящего времени было предложено несколько реализующих ее протоколов [2 – 5]. Все они основаны на принципе некопируемости произвольных квантовых состояний [6], благодаря которому невозможно создать наряду с оригиналом точную копию произвольного сообщения, передаваемого по квантовому каналу, если в качестве букв для него используются взаимно неортогональные состояния некоторого квантового носителя информации, например фотона. Более того, любая попытка подслушивания неизбежно вызовет ошибки в передаваемом сообщении, анализируя которые можно не только обнаружить сам факт подслушивания, но и рассчитать максимально возможный при имеющихся данных информационного обмена объём подслушанной информации.

Напомним основные шаги стандартных протоколов КК, используя общепринятую терминологию: Алиса — передатчик информации, Боб – приемник и Ева – подслушиватель. Различные протоколы КК имеют похожие алгоритмы работы и фактически различаются лишь своими алфавитами, т. е. наборами квантовых состояний, играющих роль букв, из которых строится сообщение. Первый шаг состоит в выборе алфавита, т.е. в кодировании классической информации, которую Алиса хочет передать Бобу, квантовыми состояниями, при этом логической паре битов «0» и «1» сопоставляется набор из нескольких взаимно неортогональных друг другу, но внутренне ортогональных пар состояний. Так, например, в первом протоколе КК, названном по имени создателей BB84, алфавит состоит из четырех состояний: $\{|0\rangle, \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |1\rangle, \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$. Здесь первым двум состояниям соответствует «0», а вторым – «1», причем для кодирования конкретного бита конкретное состояние выбирается из этого набора случайно, например строке «0, 0, 0, 1, 1, 1» может соответствовать последовательность «$|0\rangle, \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |0\rangle, \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), |1\rangle$». Закодированную таким образом последовательность битов Алиса отправляет Бобу. Для извлечения классической информации Боб измеряет полученное состояние в базисе, случайно выбранном из общего с Алисой алфавита, и по результату измерения восстанавливает передаваемый классический бит. В случае, если он угадал «правильный» базис, т. е. измерил состояние в том базисе, в котором оно было закодировано, он должен безошибочно восстановить классический бит. В случае же «неугадывания» вероятность правильного восстановления классического бита равна $1/2$ (для рассматриваемого протокола BB84). Таким образом, на стороне Боба формируется так называемый «сырой ключ» – последовательность классических битов, в котором неизбежно будут ошибки.

Далее выполняется процедура согласования базисов: сообщив по открытому классическому каналу, в каком именно базисе проводилось измерение (но не сообщив его результат), Алиса и Боб отберут только ту часть сообщений, для которой Боб «угадал» базис. В полученном «просеянном» ключе данные на стороне Алисы и Боба должны совпадать, т. к. наличие взаимно неортогональных состояний гарантирует невозможность незаметного подслушивания. Однако реально всегда есть дополнительные ошибки, связанные с естественными шумами в канале передачи, с несовершенством оборудования и т. п. Поэтому после получения просеянного ключа Алиса и Боб выполняют дополнительные классические процедуры коррекции ошибок и усиления безопасности [7].

Общей чертой всех протоколов КК является наличие некоторого *критического* уровня ошибок, выше которого протокол не гарантирует возможности установления секретного сообщения. Существование этого критического уровня ограничивает дальность секретной передачи информации из-за наличия естественных шумов в канале

Д.В.Сыч, Б.А.Гришанин, В.Н.Задков. Московский государственный университет им. М.В.Ломоносова, физический факультет; Международный учебно-научный лазерный центр МГУ им. М.В.Ломоносова, Россия, 119992 Москва, Воробьевы горы;
e-mail: sych@comsim1.phys.msu.ru; grishan@comsim1.phys.msu.ru; zadkov@comsim1.phys.msu.ru

Поступила в редакцию 22 сентября 2004 г.

передачи. В настоящее время максимальная дальность секретной передачи информации по открытому воздуху составляет примерно 100 км [7].

Одной из целей разработки новых протоколов КК является увеличение критического уровня ошибок, что делает протокол более помехозащищенным и устойчивым против как потенциальных атак подслушивателя, так и естественных шумов в экспериментальной установке и информационном канале, что позволяет осуществлять секретную передачу данных на бóльшие расстояния. Увеличения критического уровня ошибок можно достичь варьированием алфавита, а также размерности пространства состояний. Широко распространено мнение (хотя и не доказанное), что в двумерном случае наивысшим критическим уровнем ошибок обладает протокол с алфавитом из трех взаимно-несмещённых базисов – протокол six-state [4, 8, 9]. Дальнейшее увеличение критического уровня ошибок обычно связывается только с увеличением размерности пространства состояний [10–12].

В настоящей работе рассматривается вопрос о возможности увеличения критического уровня ошибок выше уровня протокола six-state за счет варьирования алфавита в двумерном пространстве.

Заметив, что набор из шести букв протокола six-state образует октаэдр на сфере Блоха (в некоторых работах сфера Блоха называется также сферой Пуанкаре [13]), мы рассмотрим алфавиты, буквы которых образуют на сфере Блоха остальные правильные многогранники: тетраэдр, куб, икосаэдр и додекаэдр, имеющие 4, 8, 12 и 20 вершин соответственно, и, как предельный случай многогранника с бесконечным числом вершин, континуальный алфавит, равноправно включающий в себя все квантовые состояния. Протоколы, в которых используются такие алфавиты, повторяют все основные шаги стандартных протоколов КК, например протокола BB84 [1] (формирование сырого ключа, согласование базисов, усиление безопасности и т.д.). Некоторыми особенностями будут обладать только протокол с континуальным алфавитом (п.2) и протокол с алфавитом в виде тетраэдра (п.3). В остальном информационный анализ этих протоколов можно выполнить по стандартной схеме, основанной на расчете взаимной информации в двухчастичных подсистемах трехчастичной системы Алиса – Ева – Боб [14].

2. Особенности протокола с континуальным алфавитом

С практической точки зрения основное отличие протокола с континуальным алфавитом от протоколов с дискретным алфавитом заключается в процедуре согласования базисов. Для дискретных алфавитов выполняется точное согласование базисов, т. е. Алиса и Боб отбирают только ту часть сообщений, для передачи и приема которой они использовали одинаковые базисы. Для континуального алфавита процедуру точного согласования базисов выполнить невозможно, т. к. количество информации о точке из континуума равно бесконечности. Поэтому для континуального алфавита мы предлагаем проводить *приблизительное* согласование базисов. Для этого разобьем все пространство состояний на несколько областей с примерно одинаковыми состояниями и при согласовании базисов будем передавать информацию о номере области, которой принадлежит базис. Будем считать базисы совпавшими, если они попали в одну и ту же область.

Понятно, что такая процедура вызовет дополнительные ошибки, связанные с ненулевой проекцией вектора состояния, кодирующего сообщение «0» в одном базисе $\{|v\rangle, |\tilde{v}\rangle\}$, на вектор состояния, кодирующий сообщение «1» в другом базисе $\{|\mu\rangle, |\tilde{\mu}\rangle\}$, даже если эти базисы попали в одну и ту же область. Рассчитаем количество информации I в одном кубите при приблизительном согласовании базисов:

$$I = 1 + \int |\langle\mu|v\rangle|^2 \log_2 |\langle\mu|v\rangle|^2 \mathrm{d}V_v \mathrm{d}V_\mu \Big/ \int |\langle\mu|v\rangle|^2 \mathrm{d}V_v \mathrm{d}V_\mu, \quad (1)$$

где интегрирование проводится по выбранной области согласования базисов, в которую попадают $|v\rangle$ и $|\mu\rangle$; $\mathrm{d}V_v$, $\mathrm{d}V_\mu$ – дифференциалы объёма на сфере Блоха. Будем считать для простоты, что области, на которые разбивается сфера Блоха, будут круглыми с радиусом R и что $2N^2$ кругами с радиусами $\pi/2N$ заведомо можно покрыть всю сферу Блоха (с единичным радиусом). Тогда для количества информации в одном кубите получаем зависимость, представленную в табл. 1.

Табл.1. Количество информации в одном кубите в зависимости от числа областей при приблизительном согласовании базисов.

Число областей	2	8	18	32	50	72	98
Количество информации (бит)	0.469	0.801	0.906	0.946	0.965	0.976	0.982

С увеличением числа областей и, следовательно, уменьшением размера каждой области информация в одном кубите увеличивается с примерно 0.47 бита при двух областях до 1 бита в пределе бесконечно большого числа областей. Заметим, что увеличение числа областей приводит к пропорциональному увеличению объема дополнительной информации о номере области при согласовании базисов, а также к пропорциональному уменьшению количества отобранных после согласования базисов сообщений.

Другой особенностью протокола с континуальным алфавитом является количественная мера оценки вмешательства подслушивателя. Одной из самых распространенных характеристик является уровень ошибок Q в квантовом бите – QBER (quantum bit error rate): $Q = 1 - N/N_{\max}$, где N – число правильно переданных букв и $N_{\max}$ – общее число переданных букв. Использование QBER как меры вмешательства подслушивателя неявно предполагает его равенство нулю в отсутствие подслушивания. Действительно, в идеальном квантовом канале после точного согласования базисов ошибок в переданном сообщении нет. Однако в случае протокола с континуальным алфавитом точного согласования базисов осуществить не удастся, и QBER не равен нулю даже при отсутствии подслушивания, так что он, очевидно, не отражает реального уровня вмешательства подслушивателя.

Для разрешения данного противоречия мы предлагаем считать точностью передачи не относительное число правильно переданных букв, а относительное количество правильно переданной информации. Тогда уровень ошибок может быть определен как $\tilde{Q} = 1 - I/I_{\max}$, где I – количество информации в одном кубите при наличии

подслушивания, а $I_{\max}$ – её максимально возможная величина в отсутствие подслушивания. По аналогии с QBER эту меру ошибок можно назвать MIER (mutual information error rate) – уровень ошибок во взаимной информации. Видно, что MIER корректно отражает уровень вмешательства подслушивателя даже для протокола с континуальным алфавитом при приблизительном согласовании базисов. Далее удобно использовать обе этих характеристики – QBER и MIER, по умолчанию считая, что при использовании QBER имеет место предельный случай точного согласования базисов.

3. Стратегия перехвата-пересылки

Самой простой стратегией подслушивания является измерение Евой передаваемого кубита в некотором базисе и последующая отправка результата измерения Бобу – так называемая стратегия перехвата-пересылки. Понятно, что в таком случае Ева точно знает, что получает Боб, и установление секретного сообщения между Алисой и Бобом невозможно. Следовательно, максимальный уровень ошибок, при котором секретная связь возможна, не превышает уровня ошибок, вызванных стратегией подслушивания типа перехвата-пересылки, т.е. расчет этих ошибок дает верхнюю границу эффективности протоколов КК.

Предположим, что Алиса передала Бобу некоторое состояние $|\alpha\rangle$, а Ева при его перехвате использовала базис $\{|\psi\rangle, |\psi_\perp\rangle\}$. Тогда Ева получила результат $|\psi\rangle$ с вероятностью $|\langle\psi|\alpha\rangle|^2$ либо $|\psi_\perp\rangle$ с вероятностью $|\langle\psi_\perp|\alpha\rangle|^2$ и отправила полученный результат Бобу. После измерения Бобом передаваемых состояний $|\psi\rangle$ и $|\psi_\perp\rangle$ в базисе $\{|\alpha\rangle, |\alpha_\perp\rangle\}$ он получит правильный результат – состояние $|\alpha\rangle$ – с вероятностями $|\langle\psi|\alpha\rangle|^2$ и $|\langle\psi_\perp|\alpha\rangle|^2$ и неправильный результат – состояние $|\alpha_\perp\rangle$ – с вероятностями $|\langle\psi|\alpha_\perp\rangle|^2$ и $|\langle\psi_\perp|\alpha_\perp\rangle|^2$. Общая вероятность получения правильного результата Бобом равна $|\langle\psi|\alpha\rangle|^4 + |\langle\psi_\perp|\alpha\rangle|^4$ и соответственно вероятность возникновения ошибки $Q_{\alpha\psi} = 1 - |\langle\psi|\alpha\rangle|^4 - |\langle\psi_\perp|\alpha\rangle|^4$.

Для расчета QBER необходимо усреднить $Q_{\alpha\psi}$ по всем базисам Алисы $\{\alpha\}$ и минимизировать результат усреднения по базисам Евы $\{\psi\}$:

$$Q = \sum_{\{\alpha\}} \sum_{\{\psi\}} Q_{\alpha\psi}/(N_\alpha N_\psi),$$

где N_α и N_ψ – число базисов в алфавитах Алисы и Евы. Для протокола с континуальным алфавитом вместо суммирования выполняется соответствующее интегрирование. Результаты расчетов приведены в табл.2. Максимально возможным критическим уровнем ошибок, равным 1/3, обладают протоколы с алфавитами, включающими 6 и 8 букв, и протокол с континуальным алфавитом. Несколько меньшей эффективностью обладают протоколы с 12 и 20 буквами, для которых уровень ошибок равен $74/225 \simeq 0.329$. Отметим одну особенность отсутствующего в табл.2 четырёхбуквенного протокола с алфавитом в виде тетраэдра. Поскольку у тетраэдра нет центральной симметрии, то буквы в таком алфавите не образуют наборы ортогональных базисов и процедура согласования базисов в стандартном виде для такого протокола не выполняется.

Табл.2. Уровень ошибок QBER, вызванный стратегией подслушивания типа перехвата-пересылки.

Число букв в алфавите	6	8	12	20	∞
Уровень ошибок, QBER	0.333	0.333	0.329	0.329	0.333

4. Стратегия оптимального подслушивания

Было доказано [15], что безопасное соединение между Алисой и Бобом возможно, если Боб получает от Алисы больше информации, чем Ева от Алисы или от Боба:

$$I_{\rm AB} > \max(I_{\rm AE}, I_{\rm BE}).$$

Рассмотрим стратегию оптимального подслушивания, когда Ева извлекает из подслушиваемого сообщения максимум информации при заданном уровне вмешательства, вызывающем соответствующий уровень ошибок, что можно записать как

$$I_{\rm AE,BE} = \max_{I_{\rm AB}=\rm const} I_{\rm AE,BE}.$$

Заметим, что эта стратегия может отличаться от оптимального клонирования [16].

Без ограничения общности можно считать, что при оптимальном подслушивании Ева выполняет унитарное преобразование $U_{\rm BE}$ над передаваемым от Алисы к Бобу состоянием $|\beta\rangle_{\rm B}$ и присоединенным к информационному каналу пробным состоянием Евы $|0\rangle_{\rm E}$ (если преобразование Евы является неунитарным, то оно соответствует некоторому унитарному преобразованию в расширенной системе с последующим усреднением по части переменных, что не добавляет ей какой-либо информации и не создаёт никаких дополнительных проблем для Алисы и Боба). Действие этого унитарного преобразования на базисные элементы выглядит следующим образом:

$$\begin{aligned} |0\rangle_{\rm B}|0\rangle_{\rm E} &\xrightarrow{U_{\rm BE}} |0\rangle_{\rm B}|\Phi_{00}\rangle_E + |1\rangle_{\rm B}|\Phi_{01}\rangle_{\rm E}, \\ |1\rangle_{\rm B}|0\rangle_{\rm E} &\xrightarrow{U_{\rm BE}} |0\rangle_{\rm B}|\Phi_{10}\rangle_E + |1\rangle_{\rm B}|\Phi_{11}\rangle_{\rm E}. \end{aligned} \tag{4}$$

Унитарность предполагает наложение ограничений, вытекающих из условий сохранения ортогональности $\langle\Phi_{00}|\Phi_{10}\rangle + \langle\Phi_{01}|\Phi_{11}\rangle = 0$ и нормировки $|\Phi_{00}|^2 + |\Phi_{01}|^2 = |\Phi_{10}|^2 + |\Phi_{11}|^2 = 1$.

Учитывая эти ограничения, набор всех состояний $|\Phi_{ij}\rangle$ можно представить в форме суперпозиции всего двух базисных состояний:

$$\begin{pmatrix} |\Phi_{00}\rangle \\ |\Phi_{01}\rangle \\ |\Phi_{10}\rangle \\ |\Phi_{11}\rangle \end{pmatrix} = \begin{pmatrix} \gamma_{00} & \gamma_{01} \\ \gamma_{10} & \gamma_{11} \\ \gamma_{11} & \gamma_{10} \\ \gamma_{01} & \gamma_{00} \end{pmatrix} \begin{pmatrix} |0\rangle_{\rm E} \\ |1\rangle_{\rm E} \end{pmatrix}, \tag{5}$$

где все коэффициенты преобразования (5) определяются через два параметра (θ и φ), контролируемых Евой: $\gamma_{mn} = (-1)^{mn}\cos(\theta - m\pi/2)\cos(\varphi - n\pi/2)$.

Начальная матрица плотности системы Боб – Ева $\hat\rho_{\rm EB}^{(1)}(\alpha) = |0\rangle_{\rm E}\langle 0|_{\rm E} \otimes |\alpha\rangle_{\rm B}\langle\alpha|_{\rm B}$ после преобразования (4) переходит в конечную матрицу $\hat\rho_{\rm EB}^{(2)}(\alpha)$, на основе которой получаем совместное трёхчастичное распределение вероятностей

$$P_{\mathrm{ABE}}(\alpha,\beta,\varepsilon)=\mathrm{Tr}_{\mathrm{BE}}[(|\varepsilon\rangle_{\mathrm{E}}\langle\varepsilon|_{\mathrm{E}}\otimes|\beta\rangle_{\mathrm{B}}\langle\beta|_{\mathrm{B}})\hat{\rho}^{(2)}_{\mathrm{EB}}(\alpha)]\mathrm{d}V_{\mathrm{E}}\mathrm{d}V_{\mathrm{B}}. \quad (6)$$

Естественной характеристикой для расчета количества информации является стандартный информационный функционал Шеннона:

$$I_{XY}[P_{XY}]=S[P_X]+S[P_Y]-S[P_{XY}], \quad (7)$$

где $S[P]$ – классическая энтропия Шеннона [17], заданная на совместном ($P=P_{XY}$) и парциальных ($P=P_X, P_Y$) распределениях вероятностей. Усредняя (6) по третьей системе, получаем двухчастичные распределения вероятностей и, на основе (7), соответствующие зависимости информации I_{AB}, I_{AE}, I_{BE} в системах Алиса – Боб, Алиса – Ева и Боб – Ева от параметров θ и φ.

Из сравнения описанных зависимостей следует, что при любых значениях этих параметров выполняется условие $I_{\mathrm{AE}}\geqslant I_{\mathrm{BE}}$. Поэтому далее зависимость информации I_{BE} рассматривать нет необходимости и условие безопасности (2) преобразуется в соотношение $I_{\mathrm{AB}}>I_{\mathrm{AE}}$.

Анализ условия оптимальности подслушивания (3) показывает, что оно выполняется в области значений параметров $\theta=\pi/4-\varphi$. С учётом того, что зависимости I_{AE} и I_{AB} симметричны относительно $\theta=\varphi$, на рис.1 представлены лишь однопараметрические зависимости $I_{\mathrm{AB}}(\theta)$ при выполнении условия оптимального подслушивания (3).

Условие безопасности $I_{\mathrm{AB}}>I_{\mathrm{AE}}$ в силу симметрии $I_{\mathrm{AB}}(\theta,\varphi)=I_{\mathrm{AE}}(\varphi,\theta)$ и условия оптимальности $\theta=\pi/4-\varphi$ выполняется вплоть до критического значения $\theta_0=\pi/8$, при котором информация, перехваченная Евой, равна информации, полученной Бобом. Критические значения ошибок $\tilde{Q}_0$ для рассматриваемых протоколов представлены в табл.3, из которой следует, что без согласования базисов наивысшим критическим уровнем ошибок обладает протокол с алфавитом в виде тетраэдра.

Табл.3. Критический уровень ошибок $\tilde{Q}_0$ до согласования базисов.

Число букв в алфавите	4	6	8	12	20	∞
Критический уровень ошибок, MIER	0.650	0.630	0.607	0.597	0.589	0.600

Заметим, что расчет количества информации напрямую не связан с ее *кодированием*. Наиболее часто используется двоичное кодирование, когда одному состоянию из ортогональной пары сопоставляется «0», а другому – «1», что связано с процедурой согласования базисов. Кодирование в континуальном алфавите аналогично стандартным протоколам КК, т. к. для любой буквы из континуального алфавита существует ортогональная ей буква. Способ разделения сферы Блоха на ортогональные пары произволен, надо лишь учитывать разделение на области при приблизительном согласовании базисов. Можно, например, разделить ее на верхнюю часть, кодирующую «0», и нижнюю, кодирующую «1».

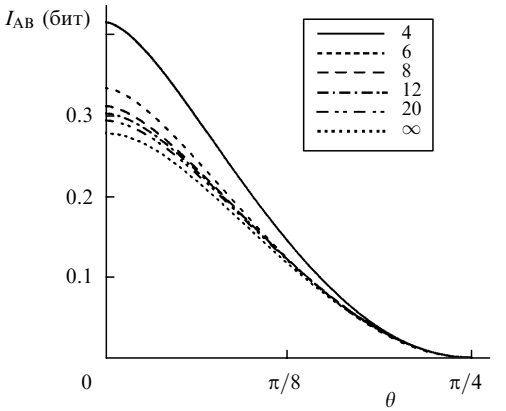

Рис.1. Зависимость количества информации I_{AB} в системе Алиса – Боб от параметра θ для протоколов, использующих 4, 6, 8, 12, 20 букв, и протокола с континуальным алфавитом (бесконечное число букв).

Буквы тетраэдрального алфавита ортогональных пар не образуют, поэтому для них следует использовать другое кодирование, где двум произвольным буквам сопоставляется «0», а двум оставшимся – «1».

Рассмотрим теперь роль согласования базисов. Будем предполагать, что Алиса и Боб выполняют *безопасное* согласование базисов, т. е. Ева не влияет на отбор данных, не вносит ложных сообщений в открытый канал связи и не использует дополнительных преобразований над своим пробным состоянием после согласования базисов, т. е. ее информация после согласования базисов не увеличивается.

Информация I_{AB}, получаемая Бобом от Алисы после согласования базисов, пропорционально увеличивается по сравнению со случаем без согласования, достигая максимального значения 1 бит на одно сообщение (подразумевается точное согласование базисов для протокола с континуальным алфавитом). Условие безопасности $I_{\mathrm{AB}}>I_{\mathrm{AE}}$ теперь выполняется вплоть до других (по сравнению со случаем отсутствия согласования базисов) значений θ_0, зависящих от конкретного протокола. Критический уровень ошибок при этом также увеличивается (см. табл.4).

Табл.4. Критический уровень ошибок $\tilde{Q}_0$ после согласования базисов

Число букв в алфавите	6	8	12	20	∞
Критический уровень ошибок, MIER	0.806	0.805	0.804	0.805	0.811

После согласования базисов наивысшим критическим уровнем ошибок обладает протокол с континуальным алфавитом, что справедливо в предельном случае точного согласования базисов. Для алфавита в виде тетраэдра процедура согласования базисов в стандартном виде не выполняется, поэтому в табл.4 нет соответствующего результата.

5. Экспериментальная реализация

На рис.2 приведена экспериментальная схема реализации рассмотренных выше протоколов квантовой криптографии, где буквы кодируются поляризацией фотонов.

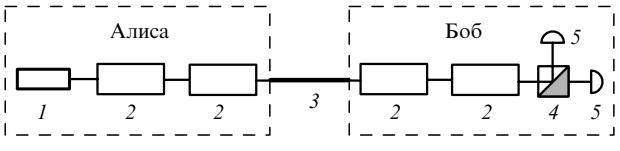

Рис.2. Экспериментальная схема реализации протоколов квантовой криптографии:
1 – источник единичных фотонов; *2* – ячейка Поккельса; *3* – квантовый канал; *4* – поляризационный делитель; *5* – счетчик фотонов.

На стороне Алисы генерируются фотоны с произвольным квантовым поляризационным состоянием. Это можно реализовать с помощью источника единичных фотонов *1* с фиксированной поляризацией, например лазера, работающего в режиме генерации единичных фотонов. Набор букв, составляющих алфавит реализуемого протокола, задается набором точек на сфере Блоха и определяется набором углов поворота поляризационного базиса, например с помощью двух ячеек Поккельса *2*, где первая ячейка поворачивает вертикальную составляющую поляризации, а вторая – горизонтальную. Вместо ячеек Поккельса можно также использовать четвертьволновые поляризационные пластинки, поворачивая их на углы, соответствующие выбранному алфавиту. Алфавитам с конечным дискретным набором букв будет соответствовать конечный дискретный набор углов поворота поляризации, а континуальному алфавиту – непрерывное множество углов поворота поляризации.

Полученный фотон с произвольным поляризационным состоянием далее передается Бобу по квантовому каналу *3*, сохраняющему поляризацию, например по открытому пространству. На стороне Боба поляризация каждого фотона преобразуется согласно заданному алфавиту аналогично тому, как это делается на стороне Алисы, но в обратном порядке, так, чтобы после преобразования фотон находился в фиксированном поляризационном базисе, в котором он измеряется при помощи поляризационного делителя *4* и счетчиков фотонов *5*.

В описанную схему, предназначенную для передачи квантовых букв, следует ещё добавить классический несекретный канал связи, с помощью которого Алиса и Боб обмениваются несекретной информацией для реализации открытых этапов передачи квантового ключа, например для вычисления уровня ошибок, согласования базисов, проверки условия безопасности и т. д.

6. Заключение

Итак, результаты проведённого анализа показывают, что даже при использовании двумерного пространства квантовых состояний можно с помощью варьирования применяемого алфавита превысить критический уровень ошибок протокола six-state. В отсутствие согласования базисов более высоким критическим уровнем ошибок, чем у протокола six-state, обладает протокол с алфавитом в виде тетраэдра, а при использовании согласования базисов – протокол с континуальным алфавитом.

Работа частично поддержана грантами РФФИ № 02–03–32200, 04–02–17554 и грантом INTAS INFO 00–479.

1. Bennett Ch.H. Brassard G., in *Proc. IEEE Intern. Conf. on Computer, System Signal Processing* (New York: IEEE, 1984, p. 175).
2. Ekert A.K. *Phys. Rev. A*, **67**, 661 (1991).
3. Bennett Ch.H. *Phys. Rev. Lett.,* **68**, 3121 (1992).
4. Bruss D. *Phys. Rev. Lett*., **81**, 3018 (1998).
5. Grosshans F. Grangier P. *Phys. Rev. Lett*., **88**, 057902 (2002).
6. Wootters W.K., Zurek W.H. *Nature (Ldn)*, **299**, 802 (1982).
7. Stucki D., Gisin N., Guinnard O., Ribordy G., Zbinden H. *New J. Phys*., **4**, 41.1 (2002).
8. Bechmann-Pasquinucci H., Gisin N. *Phys. Rev. A*, **59**, 4238 (1999).
9. Gottesman D. Lo H.-K. *IEEE Trans. Inf. Theory*, **49**, 457 (2003).
10. Bechmann-Pasquinucci H., Tittel W. *Phys. Rev. A*, **61,** 062308 (2000).
11. Bourennane M., Karlsson A., Bjork G. *Phys. Rev. A*, **64,** 012306 (2001).
12. Cerf N. J., Bourennane M., Karlsson A., Gisin N. *Phys. Rev. Lett*., **88**, 127902 (2002).
13. Борн М., Вольф Э. *Основы оптики* (М.: Наука, 1973, с. 50).
14. Gisin N., Ribordy G., et al. *Rev. Mod. Phys*., **74**, 145 (2002).
15. Bennett C.H., Brassard G., Robert J. M. *SIAM J. Comput*., **17**, 210 (1988).
16. Fuchs C.A., Gisin N., Griffiths R.B., Niu C.-S., Peres A. *Phys. Rev. A*, **56**, 1163 (1997).
17. Gallagher, R.G. *Information Theory Reliable Communication* (New York: John Wiley and Sons, 1968).