

К ВОПРОСУ ОБ ИСПОЛЬЗОВАНИИ КУКВАРТОВ ДЛЯ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧА

С. П. Кулик, А. П. Шурупов*

*Московский государственный университет им. М. В. Ломоносова
119899, Москва, Россия*

Поступила в редакцию 29 декабря 2006 г.

Проведен сравнительный анализ протокола квантового распределения ключа при использовании кубитов и куквартов в качестве носителей информации. Рассмотрены различные схемы некогерентных атак, которые могут использоваться злоумышленником для получения секретной информации. Проанализированы вносимые подслушивателем ошибки для различных протоколов используемых при распределении ключа.

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

Квантовое распределение ключа (квантовая криптография) позволяет организовать секретную передачу ключа таким образом, что можно гарантировать его секретность на уровне фундаментальных законов природы — квантовой механики [1–3].

1. ОБОБЩЕННЫЕ ПРОТОКОЛЫ *VB84*

Впервые идея протокола квантового распределения ключа (КРК) на состояниях размерности $D > 2$, была высказана в работе [4]. Предложенный авторами этой работы протокол квантового распределения ключа является обобщением на трехуровневые системы известного кубитового протокола *VB84* [2]. Согласно [4], квантовые состояния, в которых кодируется информация, принадлежат четырем взаимно несмещенным базисам, каждый из которых является ортонормированным и состоит из тройки векторов. По определению векторы, принадлежащие семейству взаимно несмещенных базисов, удовлетворяют следующим условиям (D — размерность гильбертова пространства)

1. $|\langle e_i | e_j \rangle|^2 = \frac{1}{D}$, если векторы $|e_i\rangle$, $|e_j\rangle$ принадлежат разным базисам;

2. $|\langle e_i | e_j \rangle|^2 = 0$, $i \neq j$ и $|\langle e_i | e_i \rangle|^2 = 1$, если векторы принадлежат одному базису.

Можно показать [5], что существует набор $M = D + 1$ взаимно несмещенных базисов, если

*E-mail: Sergei.Kulik@gmail.com

только размерность пространства D удовлетворяет условию $D = p^k$, где p — простое число, а k — целое. Так, для $D = 3$ и 4 число базисов составляет $M_3 = 4$ и $M_4 = 5$. Соответствующие базисные квантовые состояния называются кутритами и куквартами. Полное число используемых состояний равно $m = MD$; для трехуровневых систем протокол строится на 12 состояниях, для четырехуровневых систем — на 20 состояниях.

С геометрической точки зрения среди векторов, принадлежащих взаимно несмещенным базисам, нет выделенных: проекция выбранного вектора из числа $m = MD$ возможных на любой вектор, принадлежащий другому базису и, следовательно, неортогональный ему, имеет одну и ту же величину. Именно это свойство и используется при построении ряда протоколов квантового распределения ключа.

Распределение ключа при помощи квантовых состояний высокой размерности, по сути, не отличается от сценария обычных кубитовых протоколов. Случайная строка символов соответствующей размерности (например, 0, 1, 2, 3, если $D = 4$) кодируется в последовательности m неортогональных состояний из M случайно выбранных, но заранее заданных базисов.

При дальнейшем обобщении можно построить протокол, использующий бесконечномерное гильбертово пространство и, соответственно, бесконечное число базисов [6].

Оказывается, что в случае $D = 4$ возможно от-

носителем просто приготовить 12 состояний, являющихся элементами трех взаимно несмещенных базисов [7, 8]. Учитывая это обстоятельство, в данной работе подробно исследован расширенный протокол *BB84* на куквартах, в котором используются три ($M = 3$) из пяти возможных взаимно несмещенных базисов.

2. АНАЛИЗ ПОДСЛУШИВАНИЯ

Для определения попыток вторгнуться в квантовый канал связи¹⁾ во время передачи данных легитимные пользователи (традиционно, Alice — для передающей станции и Bob — для принимающей) раскрывают часть ключа для сравнения. По результатам сравнения оценивается величина ошибки, вызванной наличием физического шума и/или подслушивания в канале связи.

Если Eve каждый раз взаимодействует только с одним передаваемым состоянием (или квантовой системой), то такая атака называется некогерентной. Иногда злоумышленнику выгоднее, чтобы его атака была симметричной, тогда создаваемое им возмущение не будет статистически отличаться от физического шума.

Далее мы будем использовать символы ψ , ϕ , φ для обозначения трех взаимно несмещенных базисов в четырехмерном гильбертовом пространстве.

2.1. Перехват/пересылка

Простейшая стратегия подслушивания — перехват/пересылка. Согласно этой стратегии, Eve перехватывает состояние, которое Alice послала Bob, проводит его измерение и отправляет в приемную станцию состояние, являющееся копией измеренного. Такое действие не нарушает теорему о запрете клонирования неизвестных квантовых состояний [3], поскольку Eve в точности знает состояние, которое она приготавливает, но не знает состояние, которое измеряет. Далее будем считать, что Alice и Bob используют одинаковые базисы, т. е. будем учитывать состояния, оставленные после процедуры сравнения базисов.

Рассмотрим протокол на куквартах. Предположим, что Alice посылает состояние $|\psi_\alpha\rangle$. Если Eve проводит измерение в ψ -базисе (этот базис выбирается случайно, с вероятностью $1/3$), она измерит со-

стояние $|\psi_\alpha\rangle$, приготовит его невозмущенную копию и перешлет ее Bob. Таким образом, Eve знает правильное состояние, и, следовательно, Bob тоже измерит правильное состояние. В этом случае Eve получила 100% информации о передаваемом состоянии и не внесла ошибку своими действиями. Если же Eve проводила измерение в ϕ - или φ -базисе, то она с равной вероятностью $1/4$ измерит одно из базисных состояний. Это означает, что Eve не получила никакой информации об исходном состоянии. Любое состояние, посланное Eve в ϕ - или φ -базисах и измеренное Bob в ψ -базисе, даст правильное состояние $|\psi_\alpha\rangle$ лишь с вероятностью $1/4$. Таким образом, Bob с вероятностью $3/4$ регистрирует неправильное состояние. Суммарная ошибка будет определяться произведением вероятностей ошибки у Eve и Bob и составит $2/3 \cdot 3/4 = 1/2$.

В общем случае информация по Шеннону определяется выражением

$$I = \log_2(D) + H_D(p_1, \dots, p_D), \quad (1)$$

где $H_D(p_1, \dots, p_D)$ — функция энтропии, определенная как

$$H_D(p_1, \dots, p_D) = p_1 \log_2 p_1 + \dots + p_D \log_2 p_D,$$

p_1, \dots, p_D — вероятности различных исходов, D — размерность пространства.

При стратегии «прием/пересылка» Eve имеет доступ к $1/3$ передаваемой информации. Действительно, используя формулу (1), получаем

$$I_{3-basis}^{(4D)} = 0.666,$$

т. е. в среднем $2/3$ бита, или $1/3$ от передаваемой информации.

Для сравнения приведем данные, полученные при использовании двухбазисного протокола в четырехмерном пространстве:

$$I_{2-basis}^{(4D)} = 1,$$

что составляет половину передаваемой информации. В этом случае вероятность ошибки у Bob составляет $3/8$.

Для протокола *BB84* на кубитах [2] ошибка Bob составляет $1/4$, а информация Eve $I^{(2D)} = 1/2$ бита, т. е. равна половине полной информации.

Для уменьшения вносимой ошибки Eve может проводить измерения только части передаваемых состояний. Тогда и ее информация, и вносимое возмущение уменьшаются в соответствующее число раз.

¹⁾ Действия злоумышленника (Eve) по вторжению в канал связи с целью извлечения информации о передаваемых данных принято называть «подслушиванием».

2.2. Промежуточный базис

Вместо использования базисов Alice и Bob, Eve может проводить измерения в промежуточном базисе [9]. Подслушивание с использованием промежуточного базиса — простейшая стратегия, дающая вероятностную информацию.

В обобщенном протоколе BB84 промежуточный базис θ удовлетворяет следующим условиям:

$$\begin{aligned} |\langle \theta_i | \psi_i \rangle| &= |\langle \theta_i | \phi_i \rangle| = |\langle \theta_i | \varphi_i \rangle| = \max, \\ |\langle \theta_i | \psi_j \rangle| &= |\langle \theta_i | \phi_j \rangle| = |\langle \theta_i | \varphi_j \rangle| = \min, \quad i \neq j. \end{aligned} \quad (2)$$

Если для передачи информации используются только два базиса, то элементы промежуточного θ -базиса могут быть получены просто:

$$|\theta_i\rangle = N (|\psi_i\rangle + |\phi_i\rangle), \quad (3)$$

где N выбирается из условий нормировки. Таким образом, элемент $|\theta_i\rangle$ лежит в гиперплоскости, образованной векторами $|\psi_i\rangle$ и $|\phi_i\rangle$.

В случае куквартов величина перекрытия составляет

$$|\langle \theta_i | \psi_i \rangle| = |\langle \theta_i | \phi_i \rangle| = \frac{3}{2\sqrt{3}}, \quad (4a)$$

$$|\langle \theta_i | \psi_j \rangle| = |\langle \theta_i | \phi_j \rangle| = \frac{1}{2\sqrt{3}}. \quad (4b)$$

Пусть Alice посылает состояние $|\psi_\alpha\rangle$, а Eve проводит измерения в указанном промежуточном базисе. Тогда вероятности получить в результате измерения правильный результат равны

$$P(\theta_\alpha) = 3/4, \quad P(\theta_\beta) = P(\theta_\chi) = P(\theta_\delta) = 1/12.$$

Отсюда следует, что шенноновская информация у Eve

$$I^{(4D)} = 2 + \frac{3}{4} \log_2 \frac{3}{4} + 3 \cdot \frac{1}{12} \log_2 \frac{1}{12} \approx 0.792,$$

т. е. составляет 0.396 от всей информации. Величина вносимого возмущения есть

$$E_{Bob}^{(4D)} = 5/12.$$

Для аналогичного случая с кубитами эти величины, соответственно, равны

$$I^{(2D)} \approx 0.399, \quad E_{Bob}^{(2D)} \approx 1/4.$$

Если при передаче информации используются кукварты в трех несмещенных базисах, то элементы промежуточного базиса (если он существует) можно

искать по следующему алгоритму. Первый элемент этого базиса должен иметь вид

$$|\theta_\alpha\rangle = a|\psi_\alpha\rangle + \sum_{j=\beta,\chi,\delta} \sqrt{\frac{1-a^2}{3}} e^{i\Gamma_j} |\psi_j\rangle. \quad (5)$$

Остальные векторы получаются аналогично. В соответствии с формулой (1), вероятность правильного угадывания передаваемого состояния есть a^2 , а неправильного — $(1-a^2)/3$.

Однако система (2) при учете формул (4) с указанными состояниями (5) не имеет решений, а, следовательно, промежуточного базиса для указанного протокола передачи информации не существует. Следовательно, данный тип атаки на протокол на куквартах в трех взаимно несмещенных базисах не осуществим.

В работе [10] строго доказано отсутствие такого базиса для случая использования всех пяти взаимно несмещенных базисов.

2.3. Оптимальный алгоритм

В работах [11, 12] была предложена стратегия, при которой Eve получает максимальное значение информации при минимальном вносимом возмущении.

Предположим обычную схему подслушивания, при которой злоумышленник перехватывает квантовую систему в процессе ее распространения от Alice к Bob. Далее путем унитарного преобразования связывает ее со вспомогательной системой и после этого отправляет Bob исходную, но теперь уже возмущенную, систему, оставляя себе вспомогательную. Предположим, что Eve может сохранять все вспомогательные системы до момента публичного оглашения Bob базисов, в которых он производил измерения.

Количество информации, которое в итоге получает Eve, определяется величиной воздействия на передаваемые состояния и способом измерения вспомогательных систем. Чем сильнее воздействие, тем больше информации доступно Eve, но при этом увеличивается и вносимое ею возмущение.

Наиболее общая симметричная стратегия подслушивания для куквартов выглядит следующим образом:

$$\begin{aligned}
 U|\psi_0\rangle|E\rangle &= \sqrt{D-1}|\psi_0\rangle|E_{00}\rangle + \sqrt{D/3}|\psi_1\rangle|E_{01}\rangle + \\
 &+ \sqrt{D/3}|\psi_2\rangle|E_{02}\rangle + \sqrt{D/3}|\psi_3\rangle|E_{03}\rangle, \\
 U|\psi_1\rangle|E\rangle &= \sqrt{D/3}|\psi_0\rangle|E_{10}\rangle + \sqrt{D-1}|\psi_1\rangle|E_{11}\rangle + \\
 &+ \sqrt{D/3}|\psi_2\rangle|E_{12}\rangle + \sqrt{D/3}|\psi_3\rangle|E_{13}\rangle, \\
 U|\psi_2\rangle|E\rangle &= \sqrt{D/3}|\psi_0\rangle|E_{20}\rangle + \sqrt{D/3}|\psi_1\rangle|E_{21}\rangle + \\
 &+ \sqrt{D-1}|\psi_2\rangle|E_{22}\rangle + \sqrt{D/3}|\psi_3\rangle|E_{23}\rangle, \\
 U|\psi_3\rangle|E\rangle &= \sqrt{D/3}|\psi_0\rangle|E_{30}\rangle + \sqrt{D/3}|\psi_1\rangle|E_{31}\rangle + \\
 &+ \sqrt{D/3}|\psi_2\rangle|E_{32}\rangle + \sqrt{D-1}|\psi_3\rangle|E_{33}\rangle,
 \end{aligned}
 \tag{6}$$

где D — вносимое Eve возмущение, а $F = 1 - D$ — мера соответствия приходящего к Bob состояния переданному Alice после возмущения, внесенного Eve. Мы обозначили за $|E\rangle$ исходное состояние системы у Eve, а состояния после взаимодействия $|E_{00}\rangle, |E_{01}\rangle \dots$ считаем нормированными. Отметим, что размерность Гильбертова пространства, относящегося к системам Eve, не фиксирована.

Требования симметрии и унитарности значительно снижают сложность анализа, так как уменьшается число параметров, необходимых для описания стратегии наиболее общего вида.

Данная стратегия была проанализирована для протоколов на куквартах, использующих только два [12] или все пять [11] взаимно несмещенных базиса.

Рассмотрим эту стратегию для протокола, в котором используются три взаимно несмещенных базиса. Взаимные информации между Alice–Eve и Alice–Bob сравниваются, и, следовательно, протокол теряет секретность при критическом значении возмущения $D_c^{(3)} = 0.2658$. Для сравнения приведем цифры, полученные в указанных выше работах: $D_c^{(2)} = 0.25$, $D_c^{(5)} = 0.2666$. Как и ожидалось, с увеличением числа взаимно несмещенных базисов увеличивается и значение критического возмущения D_c . Это увеличение, однако, незначительно. С другой стороны, следует отметить, что с увеличением числа базисов уменьшается и скорость генерации ключа, что ограничивает практическое использование таких протоколов.

Полученные критические значения возмущения определяют величину ошибок, вносимых квантовым каналом связи, при которой оставшаяся часть ключа может считаться все еще секретной. Ошибки в канале связи могут быть связаны как с физическим шумом, так и с действиями злоумышленника при попытке подслушивания в канале. Следовательно, более высокое значение возмущения для протокола распределения ключа позволяет использовать канал связи с более высоким шумом.

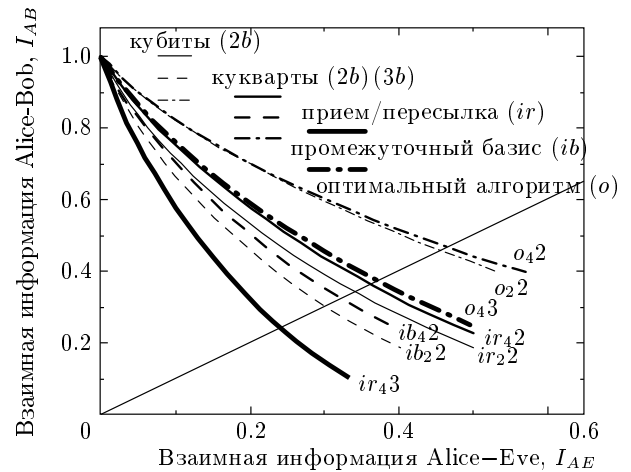


Рис. 1. Эффективность различных стратегий подслушивания: взаимная информация легитимных пользователей в зависимости от информации, доступной злоумышленнику. Протокол остается секретным до тех пор, пока взаимная информация легитимных пользователей больше информации, доступной злоумышленнику

Сравним полученные результаты с теми, которые получаются при использовании универсальной клонирующей машины [13]. Аналитически случай пяти базисов был разобран в работе [14]. Аналогичные рассуждения, проведенные для кутритов, были подтверждены численными расчетами в модели универсальной клонирующей машины [11, 15]. Полученный результат полностью совпадает с результатами оптимального подслушивания.

На рис. 1 представлен график, отображающий эффективности различных стратегий подслушивания.

До тех пор, пока взаимная информация у легитимных пользователей больше, чем взаимная информация пользователь–подслушиватель, рассмотренные протоколы являются секретными. Это означает, что в результате процедур чистки и усиления секретности у Alice и Bob возникнет абсолютно секретная строка битов. Как только величина информации у злоумышленника превысит величину информации между легитимными пользователями, гарантировать секретность полученного ключа становится невозможным. Прямая $I_{AB} = I_{AE}$ отделяет на графике соответствующие области.

Пусть Alice и Bob сначала выбирают протокол, с помощью которого будет проводиться распределение ключа (последняя цифра в обозначении кривых). Eve же в силу своих технических способностей

выбирает стратегию подслушивания (буквы в обозначении кривых). Предположим, что выбран расширенный протокол *BB84* в четырехмерном пространстве с использованием двух взаимно несмещенных базисов (N_42 , $N = o, ir, ib$). Пусть Eve пытается получить фиксированное значение величины информации, например, 40%. Из рис. 1 видно, что использование стратегий приема-пересылки и подслушивания в промежуточном базисе приведет к такому возмущению информации у легитимных пользователей, что секретность протокола уже нельзя будет гарантировать. Однако же если Eve сможет реализовать стратегию оптимального подслушивания, то, получив 40% информации, она не внесет фатальной ошибки, при которой протокол потеряет секретность — его по-прежнему можно будет использовать легитимным пользователям. Как было отмечено выше, использование оптимальной стратегии дает возможность подслушивателю (при индивидуальной атаке) получить максимально возможную информацию, внося минимальный уровень ошибок. Величины ошибок, при которых протоколы перестают быть секретными, получаются из равенства величин информации у легитимных пользователей и злоумышленника, в тот момент, когда скорость распределения ключа становится равной нулю.

2.4. Скорость распределения ключа

Скорость распределения ключа определяется как отношение разности взаимных информаций Alice–Bob и Alice–Eve к числу используемых базисов M :

$$R_{AB} = \frac{1}{M} (I_{AB} - I_{AE}). \quad (7)$$

Действительно, с увеличением числа базисов вероятность их совпадения у легитимных пользователей уменьшается, доля отбрасываемых исходов измерения растет, следовательно, число исходов, используемых для генерации ключа, уменьшается. В то же время доля извлекаемой информации, очевидно, пропорциональна разности $(I_{AB} - I_{AE})$, I_{AB} — взаимная информация Alice–Bob — может быть вычислена через величину возмущения, вносимого каналом связи и/или Eve:

$$I_{AB} = \log_2 N + (1 - E_{Bob}) \log_2(1 - E_{Bob}) + E_{Bob} \log_2 \frac{E_{Bob}}{N - 1}.$$

На рис. 2 показаны зависимости скорости распределения ключа (битов за одну посылку) для раз-

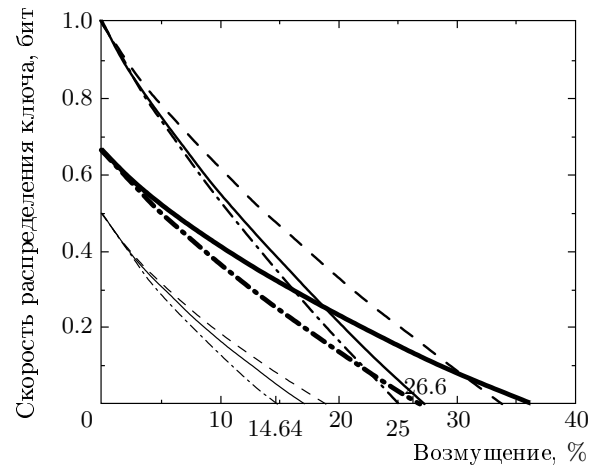


Рис. 2. Скорость распределения ключа (битов за одну посылку) как функция величины вносимого возмущения. Пересечению кривых с осью абсцисс отвечают предельно допустимые уровни возмущений. Обозначения кривых такие же, как на рис. 1

личных стратегий подслушивания от величины вносимого возмущения. Из представленных графиков видно, что с повышением размерности пространства увеличивается и величина критического возмущения, при котором протокол еще остается секретным. В пределе бесконечной размерности пространства величина допустимого возмущения асимптотически стремится к единице [6]. Этот факт показывает, что «физический» метод борьбы с шумами в виде использования квантовых систем высокой размерности гильбертова пространства представляется более перспективным, чем традиционные протоколы на двухуровневых системах. Основным препятствием на этом пути является сложность манипуляций с квантовыми состояниями высокой размерности — процедуры приготовления и измерения квантовых оптических состояний высокой размерности не достаточно хорошо отработаны. Одним из немногих исключений являются поляризационные состояния двухфотонного поля (бифотонов), получаемые в процессе спонтанного параметрического рассеяния света [7].

3. ОБСУЖДЕНИЕ

3.1. Пара кубитов или кукварт?

Рассмотрим совместные состояния двух кубитов

$$\Psi_1 = a_1|0\rangle + b_1|1\rangle, \quad \Psi_2 = a_2|0\rangle + b_2|1\rangle,$$

такие что

$$\Psi = \Psi_1 \otimes \Psi_2 = a_1 a_2 |00\rangle + a_1 b_2 |01\rangle + b_1 a_2 |10\rangle + b_1 b_2 |11\rangle. \quad (8)$$

Очевидно, что в общем случае произвольное чистое состояние четырехуровневой системы не факторизуется, т. е. представляет собой перепутанное состояние двух кубитов:

$$\Psi = c_1 |00\rangle + c_2 |01\rangle + c_3 |10\rangle + c_4 |11\rangle \neq \Psi_1 \otimes \Psi_2. \quad (9)$$

Критерием факторизуемости состояния (9) служит соотношение

$$c_1 c_4 = c_2 c_3. \quad (10)$$

Действительно, редуцированная одночастичная (например, для второго фотона пары) матрица плотности (9) имеет вид

$$\rho_2 = S_{P1} \rho = \begin{pmatrix} |c_1|^2 + |c_3|^2 & c_1 c_2^* + c_3 c_4^* \\ c_2 c_1^* + c_4 c_3^* & |c_2|^2 + |c_4|^2 \end{pmatrix}. \quad (11)$$

Здесь $\rho \equiv |\Psi\rangle\langle\Psi|$, а нижний индекс «1» в обозначении следа матрицы, как обычно, указывает на суммирование по индексам подсистемы 1. Из выражения (11) следует, что собственные значения ρ_2 оказываются равными $\lambda_{1,2}^{(2)} = 0, 1$ только при выполнении условия (10). Это означает, что состояния подсистем(ы) — чистое и общая волновая функция (9) факторизуется.

С практической точки зрения приготовление и измерение заданных перепутанных состояний двух кубитов гораздо сложнее, чем приготовление и измерение двух независимых кубитов. Поэтому в работах [7, 8] был предложен достаточно простой метод получения двенадцати состояний куквартов, принадлежащих трем взаимно несмещенным базисам. Эти состояния представляют собой факторизованные состояния пары поляризационных фотонов-кубитов, полученных в результате спонтанного параметрического рассеяния света в нецентросимметричных кристаллах. Первый базис является горизонтально-вертикальным, а состояния в нем выражаются в виде линейных комбинаций векторов горизонтальной $|H\rangle$ и вертикальной $|V\rangle$ поляризаций фотонов:

$$\begin{aligned} |\psi_\alpha\rangle &= |H_1, H_2\rangle, & |\psi_\beta\rangle &= |H_1, V_2\rangle, \\ |\psi_\chi\rangle &= |V_1, H_2\rangle, & |\psi_\delta\rangle &= |V_1, V_2\rangle. \end{aligned} \quad (12a)$$

Здесь индексы «1» и «2» относятся к разным фотонам, составляющим бифотон и отличающимся, например, частотами. Оставшиеся два базиса — диагональный

$$\begin{aligned} |\psi_\beta\rangle &= |D_1, D_2\rangle, & |\psi_\beta\rangle &= |D_1, A_2\rangle, \\ |\psi_\beta\rangle &= |A_1, D_2\rangle, & |\psi_\beta\rangle &= |A_1, A_2\rangle \end{aligned} \quad (12б)$$

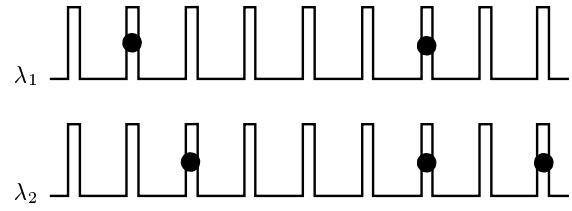


Рис. 3. Независимые однофотонные пакеты со средним числом фотонов $\mu \sim 0.1$



Рис. 4. Бифотонные пакеты со средним числом бифотонов в импульсе $\mu \sim 0.1$

и циркулярный

$$\begin{aligned} |\psi_\gamma\rangle &= |R_1, R_2\rangle, & |\psi_\gamma\rangle &= |R_1, L_2\rangle, \\ |\psi_\gamma\rangle &= |L_1, R_2\rangle, & |\psi_\gamma\rangle &= |L_1, L_2\rangle \end{aligned} \quad (12в)$$

получаются при помощи $SU(2)$ -вращений состояний отдельных фотонов и легко осуществимы в поляризационной оптике.

Составляющие базисы (12) состояния выражаются через линейные комбинации векторов $|H\rangle$ и $|V\rangle$ для первого и второго фотонов пары:

$$\begin{aligned} | + 45^\circ \rangle &\equiv |D\rangle = \frac{1}{\sqrt{2}} (|H\rangle + |V\rangle), \\ | - 45^\circ \rangle &\equiv |A\rangle = \frac{1}{\sqrt{2}} (|H\rangle - |V\rangle), \end{aligned} \quad (13)$$

$$\begin{aligned} |R\rangle &= \frac{1}{\sqrt{2}} (|H\rangle + i|V\rangle), \\ |L\rangle &= \frac{1}{\sqrt{2}} (|H\rangle - i|V\rangle). \end{aligned} \quad (14)$$

Однако, как указано выше, при таком выборе базисов базисные состояния факторизуются на произведение соответствующих состояний каждого из фотонов без какого-либо перепутывания между ними — критерий (10) выполняется.

Возникает вопрос, можно ли при таком выборе базисных состояний вместо бифотона использовать два однофотонных состояния, полученных независимо, но распространяющихся, например, в одной пространственной моде. На рис. 3 и 4 для сравнения показаны временные диаграммы, иллюстрирующие распределение пары независимых (рис. 3) и пары

коррелированных (рис. 4) фотонов. Нетрудно показать, что такой способ распределения ключа сводится к работе двух независимых протоколов *BB84*. Такой прием может быть использован для увеличения скорости генерации ключа (по сравнению с одним протоколом), но никакого выигрыша в увеличении секретности нет.

Измерение поляризационных состояний света, принадлежащих гильбертову пространству размерности $D = 4$, сводится к регистрации парных совпадений фотоотсчетов двух детекторов [7]. В этом смысле пара независимых фотонов и бифотон являются эквивалентными — с точностью, определяемой окном времени совпадений T_c . Следует отметить, что на данном этапе развития экспериментальной техники нет возможности с высокой вероятностью создать ровно один фотон в определенном достаточно малом временном окне. Следовательно, нельзя приготовить двухфотонное состояние, иначе как используя процесс спонтанного параметрического рассеяния света. Это обстоятельство делает непригодным использование такой пары для квантового распределения ключа в четырехмерном пространстве.

При использовании бифотонов в качестве квантовых систем для протокола квантового распределения ключа удастся повысить скорость генерации ключа а также устойчивость протокола по отношению к возможным атакам.

3.2. Схема парных совпадений

При использовании в качестве носителей информации бифотонов (поляризационное состояние каждого бифотона рассматривается как кукварт), следует сделать несколько замечаний по поводу схемы их регистрации. В качестве однофотонных детекторов удобнее использовать лавинные фотодиоды. При работе лавинных фотодиодов в стробируемом режиме напряжение смещения поддерживается ниже напряжения пробоя и увеличивается только на короткое время τ в момент прихода фотона, который считается известным. В самом грубом приближении лавинные фотодиоды можно охарактеризовать только двумя параметрами: квантовой эффективностью η и вероятностью p появления шумового отсчета за время τ .

Стандартная схема измерения поляризационного состояния бифотона $|H_1V_2\rangle$, принадлежащего горизонтально-вертикальному базису, представлена на рис. 5. Она представляет собой поляризационный светоделитель, пропускающий свет с горизонтальной поляризацией и отражающий с вертикальной по-

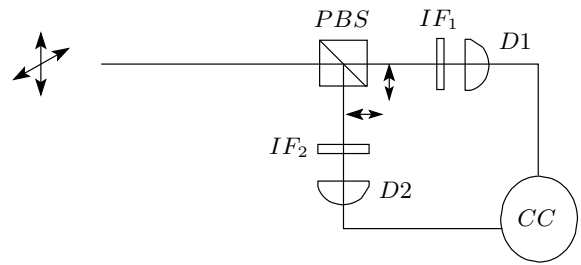


Рис. 5. Схема измерения базисного поляризационного состояния бифотона $|H_1V_2\rangle$. *PBS* — поляризационный светоделитель, пропускающий свет с горизонтальной поляризацией и отражающий свет с вертикальной поляризацией; *CC* — схема совпадений, *IF*₁, *IF*₂ — интерференционные фильтры, выделяющие длины волн λ_1 и λ_2 ; *D*₁, *D*₂ — счетчики фотонов

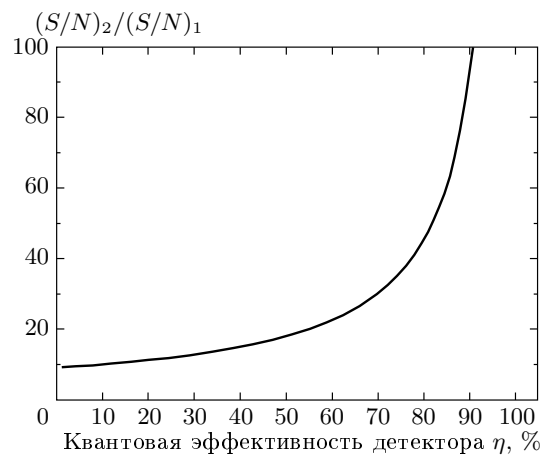


Рис. 6. Частное отношений сигнал-шум в случае двухфотонной и однофотонной схем регистрации для $\mu \sim 0.1$

ляризацией, и два детектора, работающие в режиме счета фотонов. Выходы детекторов объединены на схеме совпадений. Для однозначной идентификации состояния перед детекторами установлены интерференционные фильтры, каждый из которых пропускает одну из двух длин волн. В качестве схемы совпадений выступает логический элемент «И», который на выходе будет давать отсчет лишь в случае, когда за время одного и того же строба в обоих фотодиодах произошел фотоотсчет.

Моменты рождения бифотонов подчинены статистике Пуассона

$$P(n, \mu) = \frac{\mu^n}{n!} e^{-\mu},$$

поэтому для уменьшения вероятности нахождения двух бифотонов ($n = 2$) в одной посылке τ , необходимо уменьшать среднее число бифотонов за строб μ (см. рис. 3 и 4). В практической квантовой криптографии, где «однофотонные» состояния готовятся путем ослабления мощности лазерных импульсов, среднее число фотонов в импульсе обычно устанавливается на уровне $\mu = 0.1$ [16].

Суммируя сказанное выше, можно сделать несколько оценок.

1. Вероятность зарегистрировать бифотон равна $P_S = \mu\eta^2$.

2. Вероятность получить отсчет схемы совпадений, обусловленный появлением шумовых фотоотчетов одновременно в обоих диодах во время одного строба, равна

$$P_{NN} = (1 - \mu)p^2.$$

Поскольку в стробируемом режиме величина p для низкошумящих детекторов составляет порядка 10^{-4} – 10^{-5} в расчете на один строб, то в выражении для P_{NN} квадратичной по p поправкой можно пренебречь.

3. Вероятность получить отсчет схемы совпадений, обусловленный регистрацией одного из фотонов пары одним детектором и шумового отсчета — другим детектором (т. е. один из фотодиодов с вероятностью η регистрирует один из фотонов, а во втором диоде регистрация фотона не происходит, $(1 - \eta)$), но появляется шумовой отсчет, p) равна

$$P_{SN} = \mu\eta(1 - \eta)p(1 - p) \approx \mu\eta(1 - \eta)p.$$

Данный исход нельзя назвать полностью шумовым, так как информация об одном из фотонов, составляющих бифотон все-таки извлекается. Тем не менее, будем считать, что этот исход является шумовым.

Оценим величину отношения сигнал–шум. Для указанной двухфотонной схемы она равна

$$\left(\frac{S}{N}\right)_2 \approx \frac{P_S}{P_{SN}} = \frac{\eta}{(1 - \eta)p}.$$

В то же время для однофотонной схемы это отношение составляет

$$\left(\frac{S}{N}\right)_1 \approx \frac{\mu\eta}{(1 - \mu)p}.$$

Таким образом, отношение сигнал–шум для двухфотонной схемы превосходит такое же отношение для однофотонного режима в

$$\frac{1 - \mu}{\mu} \frac{1}{1 - \eta} \text{ раз.}$$

График этой зависимости при фиксированном среднем числе μ фотонов (бифотонов) схемы приведен на рис. 6. При типичных значениях величин $\mu = 0.1$ и $\eta = 0.1$ (для лавинных InGaAs-фотодиодов, $\lambda = 1.5$ мкм) эта разница достигает порядка величины.

3.3. Отображение в двумерный ключ

Следуя работе [17], представим алфавит высокой размерности в виде кодированной последовательности битов. Например, обозначим

$$\alpha = 00, \quad \beta = 01, \quad \chi = 10, \quad \delta = 11. \quad (15)$$

Alice и Bob также могут использовать последовательность битов для представления алфавита высокой размерности. Однако пример, приведенный ниже, показывает, что они должны правильно выбрать момент, когда наиболее выгодно переходить к такому представлению. Предположим, что для передачи использовались два взаимно несмещенных базиса, а подслушатель применял атаку в промежуточном базисе. Тогда он угадывает кварталы с вероятностью $3/4$, т. е. каждые три из четырех кварталов. Пусть секретная строка кварталов у Alice:

$$\alpha\delta\beta\alpha\chi\delta\delta\beta\gamma\alpha\beta\delta \dots$$

Строка же у Eve окажется, к примеру, такой:

$$\alpha\delta\chi\alpha\chi\beta\delta\beta\gamma\alpha\alpha\delta \dots$$

Видно, что три кварта из 12 получены с ошибкой, т. е. доля ошибок составляет $1/4$.

Однако при переходе к представлению ключа в битах оказывается следующее:

<i>Alice</i>	00	11	01	00	10	11	11	01	10	00	01	10
<i>Eve</i>	00	11	10	00	10	01	11	01	10	00	00	10

Видно, что теперь Eve ошиблась только в четырех битах из 24, т. е. $1/6$ битов оказывается ошибочным. Уменьшение числа ошибочных битов по сравнению с предыдущим случаем произошло потому, что ошибки в строке Eve перестали быть независимыми, они стали поблочно-независимы.

Приведенный пример указывает на нецелесообразность представления алфавита высокой размерности в виде битовой строки до проведения процедур чистки ошибок и усиления секретности. Также следует отметить, что правило перевода (15) не должно разглашаться, так как, зная это правило, злоумышленник может начать разрабатывать оптимальную стратегию, например, измеряя входные состояния с разными весами. Отметим, что обсуждению сравнения защищенности протоколов квантового распределения ключа, построенных на кубитах и кудитах — квантовых системах произвольной размерности ($D > 2$), посвящена работа [18].

В заключение хотелось бы подчеркнуть, что использование квантовых состояний, принадлежащих гильбертову пространству высокой размерности, рассматривается как физический способ преодоления традиционных проблем квантовой криптографии. Анализ секретности расширенных протоколов квантового распределения ключа свидетельствует об увеличении стойкости таких протоколов по отношению к различным атакам на ключ и/или воздействию шума. При этом неизбежное уменьшение скорости генерации ключа, связанное с ростом размерности пространства и, следовательно, увеличение доли отбрасываемых исходов в ходе обмена информацией по открытому каналу связи, можно компенсировать путем использования редуцированного набора взаимно несмещенных базисов. Разработанные на сегодняшний день методы приготовления, преобразования и измерения класса двухфотонных поляризационных состояний позволяют оценивать его как возможного кандидата для практической реализации квантовых криптографических систем будущего.

Авторы выражают благодарность Х. Збиндену (H. Zbinden), Х. Вайнфуртеру (H. Weinfurter), С. Н. Молоткову и Д. Хорошко за полезные обсуждения результатов работы.

Работа выполнена при финансовой поддержке РФФИ (гранты №№ 06-02-16769, 07-02-01041-а) и Программы поддержки ведущих научных школ (грант № НШ-4586.2006.2).

ЛИТЕРАТУРА

1. S. Wiesner, SIGACT News **15**, 78 (1983).
2. C. H. Bennett and G. Brassard, Int. Conf. on Computers, Systems and Signal Processing, Bangalore, India IEEE, New York (1984), p. 175.
3. W. K. Wootters and W. H. Zurek, Nature **299**, 802 (1982).
4. H. Bechmann-Pasquinucci and A. Peres, Phys. Rev. Lett. **85**, 3313 (2000).
5. W. K. Wootters and B. D. Fields, Ann. Physics **191**, 363 (1989).
6. D. V. Sych, B. A. Grishanin, and V. N. Zadkov, Laser Physics **14**, 1314 (2004).
7. С. П. Кулик, Г. А. Масленников, Е. В. Морева, ЖЭТФ **129**, 814 (2006).
8. Yu. I. Bogdanov, E. V. Moreva, G. A. Maslennikov, R. F. Galeev, S. S. Straupe, and S. P. Kulik, Phys. Rev. A **73**, 063810 (2006).
9. C. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, J. Cryptology **5**, 3 (1992).
10. R. Asplund, G. Bjork, and M. Bourenanne, J. Opt. B: Quantum Semiclass. Opt. **3**, 163 (2001).
11. D. Bruß and C. Macchiavello, Phys. Rev. Lett. **88**, 127901 (2002).
12. F. Caruso, H. Bechmann-Pasquinucci, and C. Macchiavello, Phys. Rev. A **72**, 032340 (2005).
13. V. Bužek and M. Hillery, Phys. Rev. Lett. **81**, 5003 (1998).
14. N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002).
15. T. Durt, N. J. Cerf, N. Gisin, and M. Zukowski, Phys. Rev. A **67**, 012311 (2003).
16. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
17. H. Bechmann-Pasquinucci and W. Tittel, Phys. Rev. A **61**, 062308 (2000).
18. Д. В. Хорошко, С. Я. Килин, Опт. и спектр. **94**, 691 (2003).