Письма в ЖЭТФ, том 99, вып. 12, с. 832 – 836 © 2014 г. 25 июня

О стойкости квантовой криптографии со смещенными базисами на композитных фотонах – поляризационных кутритах

С. Н. Молотков[1)]

Институт физики твердого тела РАН, 142432 Черноголовка, Россия

Академия криптографии РФ, 121552 Москва, Россия

Факультет вычислительной математики и кибернетики, МГУ им. Ломоносова, 119991 Москва, Россия

Поступила в редакцию 12 мая 2014 г.

Ранее была предложена экспериментальная схема приготовления и измерения коррелированных пар фотонов – поляризационных кутритов. В данной работе приводится анализ стойкости квантового распределения ключей на поляризационных кутритах. Совместное использование несмещенных и смещенных базисов позволяет существенно увеличить критическую ошибку по сравнению с другими протоколами.

DOI: 10.7868/S0370274X14120108

Введение. В последнее время многоуровневые квантовые системы вызывают интерес в связи с задачами квантовой криптографии [1, 2]. Квантовая криптография (квантовое распределение секретных ключей), пожалуй, единственный раздел квантовой информатики, который доведен до реальных практических применений. Основным параметром любой системы квантовой криптографии является критическая ошибка, до которой гарантируется секретное распределение ключей. Типичное значение критической ошибки в однофотонном случае в пределе бесконечно длинных передаваемых последовательностей, например для одного из базовых протоколов BB84 [3], составляет $Q_c \approx 11\,\%$ [4] (Q_c – корень уравнения $1 = 2h(Q_c)$, $h(Q)$ – бинарная энтропийная функция). В случае квазиоднофотонного состояния (ослабленного лазерного излучения) ошибка становится еще меньше. При этом в последнем случае критическая ошибка даже до конца не известна. Чем больше допустимая ошибка, тем большую дальность передачи ключей можно обеспечить.

Одним из направлений исследований является использование многоуровневых систем. Поскольку доказательство стойкости протоколов квантовой криптографии при больших размерностях пространства состояний квантовой системы оказывается достаточно сложной задачей, приходится рассматривать наборы информационных состояний, которые обладают определенными свойствами симметрии. Одним из разрабатываемых направлений являются системы с несмещенными базисами [5–7]. Набор состояний $\{|e_i^j\rangle\}$ (где $j = 1, \ldots, b_d$ – индекс базиса, i – номер внутри одного базиса) в пространстве состояний $\mathcal{H}_d$ называется несмещенным, если модули скалярных произведений (“углы”) любой пары состояний из разных базисов одинаковы, $|\langle e_i^j | e_{i'}^{j'}\rangle| = 1/\sqrt{d}$, а внутри одного базиса состояния ортогональны. Такое свойство симметрии является достаточно сильным, что облегчает анализ стойкости. Данное направление развивается по двум ветвям. Первая, чисто математическая, сводится к исследованию максимально возможного количества несмещенных базисов в пространстве данной размерности d. В этом направлении получен ряд интересных результатов [8–14]. Вторая ветвь – это использование в квантовой криптографии состояний с несмещенными базисами [5–7]. Надежды в этом направлении связаны с увеличением критической ошибки протоколов. В работе [7] была вычислена критическая ошибка протоколов квантового распределения ключей с несмещенными базисами вплоть до 20 базисов. В таком случае критическая ошибка дотягивает до $Q_c \approx 33\,\%$. Как теоретический результат это выглядит привлекательно. Вопрос состоит в том, где взять квантовые системы с такой размерностью пространства состояний. Реально можно использовать только фотоны. Пространство поляризационных степеней свободы имеет размерность $d = 2$, что недостаточно для реализации подобных протоколов.

Для достижения больших размерностей необходимо использовать состояния со сложной пространственно-временной структурой. Кроме того, при большом числе базисов процедура согласования (совпадения) базисов при передаче ключей

1) e-mail: sergei.molotkov@gmail.com

на приемной и передающей сторонах снижает эффективность протокола. При числе базисов $b = 11$, вероятность совпадения базисов $1/b^2 \approx 1\,\%$.

Хотелось бы иметь протокол, который обеспечил бы большую критическую ошибку, используя поляризационные степени свободы фотонов. Кроме того, протокол должен обеспечивать не абстрактную, а технически реализуемую процедуру приготовления и измерения квантовых состояний. Экспериментально реализуемый метод приготовления и измерения поляризационных состояний кутритов был предложен в работе [15]. Использование поляризационных состояний составных (композитных) фотонов (поляризационных кутритов) позволяет при размерности пространства состояний $d = 3$ получить большую критическую ошибку.

Информационные состояния поляризационных кутритов. Один из способов увеличения размерности пространства поляризационных степеней свободы состоит в использовании запутанных (коррелированных) пар фотонов. Пары коррелированных фотонов возникают в процессах спонтанного параметрического рассеяния (конверсии) фотонов вниз по энергии. Такой процесс генерации бифотонов был впервые предсказан теоретически Д.Н. Клышко [16], а затем экспериментально исследован в группе А.Н. Пенина [17]. Состояние пары фотонов в частотно-вырожденном случае, когда их частоты и направления распространения совпадают, может быть представлено в виде

$$|\Psi\rangle = c_1|HH\rangle + c_2|HV\rangle + c_3|VV\rangle, \tag{1}$$

где пространство состояний поляризации (вертикальной $|V\rangle$ и горизонтальной $|H\rangle$) $\dim(\mathcal{H}_d) = \dim(\mathrm{Sym}(\mathcal{H}_2 \otimes \mathcal{H}_2)) = 3$ представляет собой симметризованное тензорное произведение (следствие симметрии относительно перестановки частиц), а $\mathcal{H}_2$ – двумерное пространство состояний поляризационных степеней свободы.

Информационные состояния кутритов имеют вид

$$\begin{gathered}
\text{базис} \quad H+ \begin{cases} |0_{H+}\rangle_B = \frac{1}{\sqrt{2}}(|HH\rangle_B + |HV\rangle_B), \\ |1_{H+}\rangle_B = \frac{1}{\sqrt{2}}(|HH\rangle_B - |HV\rangle_B); \end{cases} \\
\text{базис} \quad V+ \begin{cases} |0_{V+}\rangle_B = \frac{1}{\sqrt{2}}(|VV\rangle_B + |HV\rangle_B), \\ |1_{V+}\rangle_B = \frac{1}{\sqrt{2}}(|VV\rangle_B - |HV\rangle_B); \end{cases} \\
\text{базис} \quad H\times \begin{cases} |0_{H\times}\rangle_B = \frac{1}{\sqrt{2}}(|HH\rangle_B + i|HV\rangle_B), \\ |1_{H\times}\rangle_B = \frac{1}{\sqrt{2}}(|HH\rangle_B - i|HV\rangle_B); \end{cases} \\
\text{базис} \quad V\times \begin{cases} |0_{V\times}\rangle_B = \frac{1}{\sqrt{2}}(|VV\rangle_B + i|HV\rangle_B), \\ |1_{V\times}\rangle_B = \frac{1}{\sqrt{2}}(|VV\rangle_B - i|HV\rangle_B). \end{cases}
\end{gathered} \tag{2}$$

На передающей стороне случайно и равновероятно выбирается один из базисов, H или V. Далее внутри базиса также равновероятно выбирается подбазис "+" или "$\times$". И наконец, выбирается 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:

$$\begin{aligned}
I &= |HH\rangle\langle HH| + |HV\rangle\langle HV| + |VV\rangle\langle VV| = \\
&= |0_{H+}\rangle\langle 0_{H+}| + |1_{H+}\rangle\langle 1_{H+}| + |VV\rangle\langle VV| = \\
&= |0_{H\times}\rangle\langle 0_{H\times}| + |1_{H\times}\rangle\langle 1_{H\times}| + |VV\rangle\langle VV| = \\
&= |0_{V+}\rangle\langle 0_{V+}| + |1_{V+}\rangle\langle 1_{V+}| + |HH\rangle\langle HH| = \\
&= |0_{V\times}\rangle\langle 0_{V\times}| + |1_{V\times}\rangle\langle 1_{V\times}| + |HH\rangle\langle HH|.
\end{aligned} \tag{3}$$

Каждое разложение единицы (3) описывает *отдельное измерение* в соответствующем базисе. Состояния из разных базисов попарно-неортогональны, т.е. достоверно не различимы.

Важно отметить (см.(2), (3)), что, например, при выборе состояний в базисе $H+, \times$ на передающей стороне на приемной стороне в отсутствие подслушивателя никогда не будет исходов в канале измерений $|VV\rangle\langle VV|$. Данные исходы являются дополнительными контрольными исходами.

Внутри базисов $H+$ и $V+$ состояния являются несмещенными, а между базисами они "смещены" (перекрываются по компоненте $|HV\rangle$). Под несмещенными состояниями понимаются базисные состояния, между которыми модуль скалярного произведения одинаков для любой пары состояний. Именно такая ситуация имеет место для состояния внутри базисов H и V. Состояния из базисов H и V удобно называть смещенными, поскольку модуль скалярного произведения любой пары состояний из этих базисов отличается от модуля скалярных произведений внутри самих базисов. Именно это зацепление состояний из разных несмещенных базисов и приводит к тому, что протокол становится двухпараметрическим. Длина секретного ключа зависит от двух параметров: ошибки Q в информационной последовательности бит и дополнительного контрольного параметра δ. Этот параметр связан с тем, что подслушиватель не может достоверно различить состояния из разных смещенных базисов $|H+,\times\rangle$ и $|V+,\times\rangle$ (дополнительно к невозможности достоверно различить состояния из несмещенных базисов $|H+\rangle$ и $|H\times\rangle$ и, соответственно, $|V+\rangle$ и $|V\times\rangle$).

Унитарная атака подслушивателя. Для того чтобы не усложнять выкладки, исследуем стойкость в асимптотическом пределе бесконечно длинных передаваемых последовательностей. Наиболее общая атака подслушивателя на передаваемый ключ может быть описана следующим образом. Подслушиватель в каждой посылке независимо использует вспомогательное квантовое состояние $|E\rangle$, которое запутывается при помощи унитарного преобразования U_{BE}, находящегося в руках подслушивателя. Модифицированное информационное состояние передается на приемную сторону. Вспомогательную подсистему подслушиватель сохраняет в квантовой памяти. После передачи всей последовательности и измерений на приемной стороне подслушиватель производит коллективные измерения над всей квантовой памятью. Такая атака является самой общей [18, 19]. Достаточно выяснить действие унитарного оператора на базисные состояния. Затем по линейности можно получить его действие на любые линейные комбинации базисных состояний:

$$|\Psi_i\rangle_{BE} = U_{BE}\left(|i\rangle_B \otimes |E\rangle_E\right) = \sum_{j=1}^{3} |i\rangle_B \otimes |e_i^j\rangle_E, \tag{4}$$
$$|1\rangle_B = |HH\rangle, \quad |2\rangle_B = |HV\rangle, \quad |3\rangle_B = |VV\rangle,$$

что фактически является разложением Шмидта. Оператор U_{BE} должен удовлетворять условию унитарности. С учетом симметрии внутри несмещенных базисов $H+,\times$ и $V+,\times$, а также симметрии между смещенными базисами $H+,\times$ и $V+,\times$ унитарный оператор может быть параметризован следующим образом:

$${}_E\langle e_i^i|e_i^i\rangle_E = 1-\delta, \quad i=1,2,3, \tag{5}$$

$${}_E\langle e_j^i|e_j^i\rangle_E = \frac{\delta}{2}, \quad i=2,3,\ j=1,2,3,\ i\neq j, \tag{6}$$

$$\begin{gathered} {}_E\langle e_1^1|e_2^2\rangle_E = {}_E\langle e_2^2|e_3^3\rangle_E = (1-\delta)(1-2Q), \\ {}_E\langle e_1^2|e_2^1\rangle_E = {}_E\langle e_3^2|e_2^3\rangle_E = (1-\delta)(1-2Q). \end{gathered} \tag{7}$$

Поскольку базисы H и V и состояния внутри них выбираются равновероятно, симметрия между базисами означает, что модули скалярных произведений в (5)–(7) не должны меняться при замене индексов H на V, а также $\times$ на $+$. Функции, удовлетворяющие соотношениям (5)–(7), удобно представить в виде

$$\begin{gathered} |e_1^1\rangle_E = \sqrt{1-\delta}|\mu_1\rangle_E,\ |e_1^2\rangle_E = \sqrt{\frac{\delta}{2}}|\mu_2\rangle_E, \\ |e_1^3\rangle_E = \sqrt{\frac{\delta}{2}}|\mu_3\rangle_E, \end{gathered} \tag{8}$$

$$|e_2^1\rangle_E = \sqrt{\frac{\delta}{2}}(c_\alpha|\mu_2\rangle_E + s_\alpha|\mu_4\rangle_E),\ |e_3^1\rangle_E = \sqrt{\frac{\delta}{2}}|\mu_5\rangle_E, \tag{9}$$

$$\begin{gathered} |e_2^2\rangle_E = \sqrt{1-\delta}(c_\alpha|\mu_1\rangle_E + s_\alpha|\mu_5\rangle_E), \\ |e_3^2\rangle_E = \sqrt{1-\delta}|\mu_6\rangle_E, \end{gathered} \tag{10}$$

$$|e_2^3\rangle_E = \sqrt{\frac{\delta}{2}}(c_\alpha|\mu_6\rangle_E + s_\alpha|\mu_7\rangle_E),\ |e_3^3\rangle_E = \sqrt{\frac{\delta}{2}}|\mu_1\rangle_E, \tag{11}$$

где $|\mu_k\rangle_E$ ($k=1,\ldots,7$) – ортонормированный базис в $\mathcal{H}_E$ (пространстве состояний вспомогательной квантовой системы подслушивателя).

Действие унитарного оператора на информационные состояния имеет вид

$$\begin{gathered} |\Psi_{0_{H+}}\rangle_{BE} = |0_{H+}\rangle_B \otimes \frac{|E_+^+\rangle_E + |D_+^+\rangle_E}{2} + \\ + |1_{H+}\rangle_B \otimes \frac{|E_+^-\rangle_E - |D_+^-\rangle_E}{2} + |3\rangle_B \otimes \frac{|C_+^+\rangle_E}{\sqrt{2}}, \end{gathered} \tag{12}$$

$$\begin{gathered} |\Psi_{1_{H+}}\rangle_{BE} = |1_{H+}\rangle_B \otimes \frac{|E_+^+\rangle_E - |D_+^+\rangle_E}{2} + \\ + |0_{H+}\rangle_B \otimes \frac{|E_+^-\rangle_E + |D_+^-\rangle_E}{2} + |3\rangle_B \otimes \frac{|C_+^-\rangle_E}{\sqrt{2}}. \end{gathered} \tag{13}$$

Аналогично для состояний в базисах $|0_{H\times}\rangle, |1_{H\times}\rangle$ и $|0_{V+,\times}\rangle, |1_{V+,\times}\rangle$.

Функции в (12), (13) определены как

$$\begin{gathered} |E_+^\pm\rangle_E = |e_1^1\rangle_E \pm |e_2^2\rangle_E, \\ |D_+^\pm\rangle_E = |e_1^2\rangle_E \pm |e_2^1\rangle_E, \\ |C_+^\pm\rangle_E = |e_2^3\rangle_E \pm |e_1^3\rangle_E. \end{gathered} \tag{14}$$

Матрица плотности на приемной стороне получается взятием частичного следа по подсистеме подслушивателя E:

$$\rho_{0_{H+}}^B = \mathrm{Tr}_E\{|\Psi_{0_{H+}}\rangle_{BE\,BE}\langle\Psi_{0_{H+}}|\} = \tag{15}$$
$$= |0_{H+}\rangle_{BB}\langle 0_{H+}|\frac{{}_E\langle E_+^+|E_+^+\rangle_E + {}_E\langle D_+^+|D_+^+\rangle_E}{4} +$$
$$+ |1_{H+}\rangle_{BB}\langle 1_{H+}|\frac{{}_E\langle E_+^-|E_+^-\rangle_E + {}_E\langle D_+^-|D_+^-\rangle_E}{4} +$$
$$+ |3\rangle_{BB}\langle 3|\frac{{}_E\langle C_+^+|C_+^+\rangle_E}{2},$$

$$\rho_{1_{H+}}^B = \mathrm{Tr}_E\{|\Psi_{1_{H+}}\rangle_{BE\,BE}\langle\Psi_{1_{H+}}|\} = \tag{16}$$
$$= |1_{H+}\rangle_{BB}\langle 1_{H+}|\frac{{}_E\langle E_+^+|E_+^+\rangle_E + {}_E\langle D_+^+|D_+^+\rangle_E}{4} +$$
$$+ |0_{H+}\rangle_{BB}\langle 0_{H+}|\frac{{}_E\langle E_+^-|E_+^-\rangle_E + {}_E\langle D_+^-|D_+^-\rangle_E}{4} +$$
$$+ |3\rangle_{BB}\langle 3|\frac{{}_E\langle C_+^-|C_+^-\rangle_E}{2}.$$

Критическая ошибка протокола и длина секретного ключа. Для вычисления длины секретного ключа удобно воспользоваться следующим критерием [18]. (Отметим, что возможны и другие критерии [19], которые, впрочем, в асимптотическом пределе эквиваленты используемому ниже.) Наиболее экономный и короткий способ сводится к вычислению разницы информации Холево [20] для легитимного пользователя на приемной стороне и информации Холево для подслушивателя. Информация Холево представляет собой максимально достижимую величину классической информации, которая может быть получена из квантового ансамбля. Из-за симметрии по отношению к базисам достаточно вычислить информацию Холево в одном базисе ($H+$). Поскольку информационные состояния выбираются равновероятно, квантовый ансамбль есть $\{\rho^B_{0_{H+}}, \rho^B_{1_{H+}}\}$ с вероятностями $\{\Pr(0_{H+}) = \Pr(1_{H+}) = 1/2\}$. С учетом (15), (16) для матриц плотности находим

$$\rho^B_{0_{H+}} = (1-\delta)(1-Q)|0_{H+}\rangle_{BB}\langle 0_{H+}| + \\ + (1-\delta)Q|1_{H+}\rangle_{BB}\langle 1_{H+}| + \delta|3\rangle_{BB}\langle 3|, \tag{17}$$

$$\rho^B_{0_{H+}} = (1-\delta)(1-Q)|1_{H+}\rangle_{BB}\langle 1_{H+}| + \\ + (1-\delta)Q|0_{H+}\rangle_{BB}\langle 0_{H+}| + \delta|3\rangle_{BB}\langle 3|. \tag{18}$$

Информация Холево для легитимного пользователя на приемной стороне по определению равна

$$\chi(\rho_B) = S\left(\frac{\rho^B_{0_{H+}} + \rho^B_{1_{H+}}}{2}\right) - \frac{1}{2}\left[S(\rho^B_{0_{H+}}) + S(\rho^B_{1_{H+}})\right], \tag{19}$$

где $S(\rho) = -\mathrm{Tr}\{\rho\log\rho\}$ – энтропия фон Неймана. Аналогично информация Холево для подслушивателя есть

$$\chi(\rho_E) = S\left(\frac{\rho^E_{0_{H+}} + \rho^E_{1_{H+}}}{2}\right) - \frac{1}{2}\left[S(\rho^E_{0_{H+}}) + S(\rho^E_{1_{H+}})\right], \tag{20}$$

где частичная матрица плотности подслушивателя $\rho^E_{0,1_{H+}} = \mathrm{Tr}_B\{|\Psi_{0,1_{H+}}\rangle_{BEBE}\langle\Psi_{0,1_{H+}}|\}$. Поскольку ненулевые собственные числа частичных матриц плотности подслушивателя и легитимного пользователя совпадают, имеем

$$S(\rho^B_{0,1_{H+}}) = S(\rho^E_{0,1_{H+}}) \tag{21}$$

и длина секретного ключа равна

$$r_{\mathrm{secr}} = \chi(\rho_B) - \chi(\rho_E) = \\ = S\left(\frac{\rho^B_{0_{H+}} + \rho^B_{1_{H+}}}{2}\right) - S\left(\frac{\rho^E_{0_{H+}} + \rho^E_{1_{H+}}}{2}\right). \tag{22}$$

Для суммарной матрицы плотности с учетом (17), (18) находим

$$\rho^B = \frac{\rho^B_{0_{H+}} + \rho^B_{1_{H+}}}{2} = \frac{1-\delta}{2}|0_{H+}\rangle_{BB}\langle 0_{H+}| + \\ + \frac{1-\delta}{2}|1_{H+}\rangle_{BB}\langle 1_{H+}| + \delta|3\rangle_{BB}\langle 3|. \tag{23}$$

Энтропия фон Неймана $S(\rho^B)$ есть

$$S\left(\frac{\rho^B_{0_{H+}} + \rho^B_{1_{H+}}}{2}\right) = 1 + h(\delta), \\ h(\delta) = -\delta\log(\delta) - (1-\delta)\log(1-\delta). \tag{24}$$

Соответствующая суммарная матрица плотности подслушивателя с учетом (12), (13) равна

$$\rho^E = \frac{1}{2}\big(|e^1_1\rangle_{EE}\langle e^1_1| + |e^2_2\rangle_{EE}\langle e^2_2| + |e^2_1\rangle_{EE}\langle e^2_1| + \\ + |e^1_2\rangle_{EE}\langle e^1_2|\big) + \frac{1}{2}\left(|e^2_3\rangle_{EE}\langle e^2_3| + |e^3_1\rangle_{EE}\langle e^3_1|\right). \tag{25}$$

Собственные числа (25) удобно представить в виде

$$\lambda_1 = (1-\eta)(1-\delta)(1-Q), \quad \lambda_2 = (1-\eta)(1-\delta)Q, \tag{26}$$
$$\lambda_3 = \eta(1-\delta)(1-Q), \quad \lambda_4 = \eta(1-\delta)Q,$$
$$\lambda_{5,6} = \frac{\delta}{2}, \quad \eta = \frac{\delta}{1-\delta}.$$

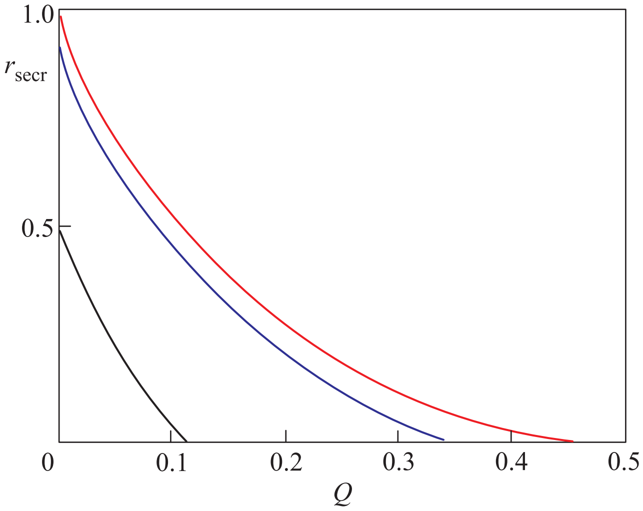
Энтропия фон Неймана $S(\rho^E)$ есть

$$S\left(\frac{\rho^E_{0_{H+}} + \rho^E_{1_{H+}}}{2}\right) = -\sum_{i=1}^{6}\lambda_i\log\lambda_i = \\ = (1-\delta)[h(\eta) + h(Q)] + h(\delta) + \delta. \tag{27}$$

Принимая во внимание (22), (24) и (27), для длины секретного ключа находим

$$r_{secr} = (1-\delta)[1 - h(\eta) - h(Q)]. \tag{28}$$

Интерпретация результатов. Использование комбинации несмещенных и смещенных базисов даже при минимальной размерности пространства состояний поляризационных степеней свободы $\dim\mathcal{H}_d = 3$ позволяет увеличить критическую ошибку протокола вплоть до 50 % (при значениях контрольного параметра $\delta \to 0$). Неформально это связано со следующим свойством информационных состояний. Состояния из смещенных базисов перекрываются по компоненте состояний $|HV\rangle$. Поскольку приемная и передающая стороны выбирают базисы $H+, \times$ и $V+, \times$ случайно и после передачи состояний оставляют только те посылки, где выбор базисов совпадал, в отсутствие подслушивателя



Длина секретного ключа как функция наблюдаемой ошибки Q на приемной стороне при различных значениях контрольного параметра δ: $\delta = 0.001$ (*1*), 0.01 (*2*) и 0.1 (*3*)

отсчетов в канале измерений $|VV\rangle$ при выборе базисов $|H+,\times\rangle$ никогда не будет. Аналогично не будет отсчетов в канале измерений $|HH\rangle$ при выборе базисов $|V+,\times\rangle$. Так как подслушивателю неизвестен выбор одного из несмещенных базисов, $H+,\times$ или $V+,\times$, это неизбежно приведет к тому, что подслушиватель будет ошибаться. Ошибка подслушивателем в выборе смещенных базисов $H+,\times$ или $V+,\times$ будет приводить к появлению отсчетов в контрольных каналах измерений $|VV\rangle$ (при выборе базисов $|H+,\times\rangle$) и $|HH\rangle$ (при выборе базисов $|V+,\times\rangle$). Вероятность δ отсчетов в контрольных каналах измерений зависит от унитарного оператора U_{BE}, управляемого подслушивателем.

Неортогональность, а значит, и достоверная неразличимость состояний из разных несмещенных базисов $H+$ и $H\times$ (или $V+$ и $V\times$) будет приводить к ошибкам, производимым подслушивателем в информационных каналах измерений $|0,1_{H+}\rangle$ и $|0,1_{H\times}\rangle$ (или $|0,1_{V+}\rangle$ и $|0,1_{V\times}\rangle$). Вероятность данной ошибки Q также регулируется действиями подслушивателя.

Легитимные пользователи могут прерывать протокол, если величина δ (доля контрольных отсчетов) превышает, например, значение $\delta = 0.001$. В этом случае подслушиватель может действовать лишь таким образом, чтобы вносить ошибку Q в информационную битовую последовательность. В результате критическая ошибка Q_C превышает 40 %. Фактически использование смещенных базисов в дополнение к несмещенным “размазывает” ошибку подслушивателя на информационные и контрольные отсчеты, что увеличивает критическую ошибку Q_c.

1. H. Bechmann-Pasquinucci and N. Gisin, Phys. Rev. A **59**, 4238 (1999).
2. N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002).
3. C. H. Bennett and G. Brassard, *Proc. of IEEE Int. Conf. on Comput. Sys. and Sign. Proces.*, Bangalore, India (1984), p. 175.
4. P. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
5. N. J. Cerf, M. Bourennane, 3. A.Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902-1 (2002).
6. F. Caruso, H. Bechmann-Pasquinucc, and C. Macchiavello, Phys. Rev. A **72**, 032340-1 (2005).
7. L. Sheridan and V. Scarani, Phys. Rev. A **82**, 030301(R) (2010).
8. I. D. Ivanovic, J. Phys. A **14**, 3241 (1981).
9. W. K. Wootters and B. D. Fields, Ann. Phys. **191** 363 (1989).
10. A. Klappenecker and M. Roetteler, *Constructions of Mutually Unbiased Bases*, Springer-Verlag, Berlin (2004).
11. M. Grassl, quant-ph/0406175.
12. C. Archer, J. Math. Phys. **46**, 022106 (2005); quant-ph/0312204.
13. I. Bengtsson, W. Bruzda, A. Ericsson, J.-A. Larsson, W. Tadej, and K. Zyczkowski, quant-ph/0610161.
14. P. Wocjan and T. Beth, quant-ph/0407081.
15. С. П. Кулик, С. Н. Молотков, И. В. Радченко, Письма в ЖЭТФ, **96**, 367 (2012).
16. Д. Н. Клышко, *Когерентный распад фотонов в нелинейной среде. Докл. на Всесоюзном совещании по нелинейным свойствам сред*, Черноголовка (1966); Д. Н. Клышко, Письма в ЖЭТФ **6**, 4902 (1967).
17. Д. Н. Клышко, А. Н. Пенин, Б. Ф. Полковников, Письма в ЖЭТФ **2**, 11 (1970).
18. M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*, Cambridge Univ. Press, Cambridge (2000).
19. R. Renner, *Security of Quantum Key Distribution*, PhD Thesis, ETH Zürich, Dec. 2005.
20. А. С. Холево, *Квантовые системы, каналы, информация*, МЦМО, М. (2010), с. 327.