Письма в ЖЭТФ, том 85, вып. 6, с. 354 – 359 © 2007 г. 25 марта

Комбинированный фазово-временной метод кодирования в квантовой криптографии

С. П. Кулик, С. Н. Молотков[+*▽], *А. П. Маккавеев*[▽]

Физический факультет МГУ им. М.В. Ломоносова, 119899 Москва, Россия

[+] *Институт физики твердого тела РАН, 142432 Черноголовка, Московская обл., Россия*

[*] *Академия Криптографии РФ, 121552 Москва, Россия*

[▽] *Факультет вычислительной математики и кибернетики, МГУ им. М.В. Ломоносова, 119899 Москва, Россия*

Поступила в редакцию 15 февраля 2007 г.

Предложен новый комбинированный фазово-временной метод кодирования для оптоволоконных систем квантовой криптографии. Сделаны предварительные оценки вероятности критической величины ошибки, до которой возможно распределение криптографических ключей.

PACS: 03.65.Bz, 03.67.Db

Квантовая криптография – распределение криптографических ключей по открытым каналам связи – основана на фундаментальных физических законах квантовой механики. Любое измерение над квантовой системой, вообще говоря, изменяет ее состояние. Данное обстоятельство позволяет детектировать попытки подслушивания в канале связи. Более формально, если квантовая система находится в одном из двух неортогональных состояний, то в принципе не существует измерений, которые бы с достоверностью позволяли различать эти состояния. Достоверная неразличимость неортогональных состояний является следствием соотношения неопределенностей Гайзенберга, или более формально, следствием того, что пара некоммутирующих операторов, отвечающая наблюдаемым, не может иметь общей системы собственных векторов.

Детектирование попыток подслушивания на приемной стороне происходит по изменению статистики измерений по сравнению со статистикой на невозмущенных состояниях. Принципиально невозможно отличить изменения статистики измерений, вызванное действием подслушивателя, от изменения статистики, вызванной неидеальностями системы (шумами в канале связи, темновых отсчетов фотодетекторов и т.д.). Поэтому все изменения статистики измерений и, соответственно, ошибки в первичных ключах приходится относить на действия подслушивателя.

Если бы квантовая криптография позволяла лишь детектировать попытки подслушивания, то этого было бы недостаточно для распределения ключей. Квантовая криптография позволяет не только детектировать попытки подслушивания, но и гарантировать секретность передаваемых ключей, если изменение статистики (величина ошибки в первичных ключах) не превышает некоторой критической величины.

Квантовый криптографический протокол тем устойчивей к подслушиванию и различного рода шумам, чем больше допустимая критическая ошибка, до которой гарантируется секретность распространения ключей. Наиболее изученным протоколом является так называемый протокол BB84 [1]. Критическая величина ошибки для него составляет $\sim 11\%$ [2–4]. Кроме того, данный протокол может быть реализован различными способами для оптоволоконных систем квантовой криптографии. Теоретически были предложены и другие протоколы распространения ключей, которые имеют большую критическую ошибку, чем BB84 [2–4]. Однако такие протоколы используют, как правило, многоуровневые квантовые системы с размерностью пространства состояний больше двух [5]. В силу этого экспериментальная реализация таких протоколов для оптоволоконных систем крайне сложна и не практична. Например, реализация протокола [6] требует использования четырехплечевого интерферометра Маха-Цандера на приемной и передающей станциях, для которого чрезвычайно сложно добиться долговременной оптической стабильности.

В данной работе предлагается новый протокол распространения ключей, который, по нашим предварительным оценкам, имеет большую величину критической ошибки по сравнению с существующими, является технически реализуемым, причем достаточно небольшой модификацией уже существующих систем квантовой криптографии. Данный протокол

является комбинированным фазово-временным способом кодирования однофотонных состояний для распределения ключей. В определенном смысле, данный метод кодирования представляет собой комбинацию двух квантовых криптографических протоколов BB84 [1] и B92 [7].

Опишем сначала формальный протокол, а затем его оптоволоконную реализацию.

В протоколе в качестве информационных состояний используется 8 состояний, по два состояния в каждом из 4 базисов, которые будем обозначать как $+L$, $\times L$, $+R$ и $\times R$. Состояния в базисе $+L$

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

в базисе $\times L$

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

в базисе $+R$

$$|0_{+R}\rangle = \frac{1}{\sqrt{2}}(|1\rangle + |2\rangle), \quad |1_{+R}\rangle = \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle), \quad (3)$$

в базисе $\times R$

$$|0_{\times R}\rangle = \frac{1}{\sqrt{2}}(|1\rangle + i|2\rangle), \quad |1_{\times R}\rangle = \frac{1}{\sqrt{2}}(|1\rangle - i|2\rangle). \quad (4)$$

Здесь $|0\rangle$, $|1\rangle$ и $|2\rangle$ – ортонормированные базисные векторы (забегая вперед, отметим, что данные базисные векторы отвечают локализованным во времени однофотонным состояниям, попарно сдвинутым во времени на определенную величину). Формально пространство состояний H является трехмерным. Состояния внутри одного базиса ортогональны аналогично протоколу BB84 [1], а из разных базисов попарно неортогональны как в протоколе B92 [7].

Формально протокол выглядит следующим образом.

Алиса на передающей станции равновероятно выбирает одно из 8 состояний и направляет на приемную станцию Бобу.

Боб независимо от Алисы случайно и равновероятно выбирает один из 4 базисов для измерений. Т.е. более точно, Боб использует случайно одно из 4-х измерений, которые описываются следующими разложениями единицы I в H:

$$I = |0_{+L}\rangle\langle 0_{+L}| + |1_{+L}\rangle\langle 1_{+L}| + |2\rangle\langle 2| - \text{измерение в базисе } +L, \quad (5)$$

$$I = |0_{\times L}\rangle\langle 0_{\times L}| + |1_{\times L}\rangle\langle 1_{\times L}| + |2\rangle\langle 2| - \text{измерение в базисе } \times L, \quad (6)$$

$$I = |0\rangle\langle 0| + |1_{+R}\rangle\langle 1_{+R}| + |2_{+R}\rangle\langle 2_{+R}| - \text{измерение в базисе } +R, \quad (7)$$

$$I = |0\rangle\langle 0| + |1_{\times R}\rangle\langle 1_{\times R}| + |2_{\times R}\rangle\langle 2_{\times R}| - \text{измерение в базисе } \times R. \quad (8)$$

Боб сообщает только сам факт получения состояния.

После проведения серии посылок и измерений Алиса раскрывает базисы, но не раскрывает сами состояния.

Боб открыто сообщает номера посылок, где базисы не совпадали. Данные посылки отбрасываются. Результаты измерений в тех посылках, в которых базисы совпадали, Боб интерпретирует как 0 или 1. В отсутствие подслушивателя и шума измерения при совпадающих базисах позволяют однозначно интерпретировать полученные состояния.

Дальнейшие действия аналогичны другим протоколам. Производится оценка вероятности ошибки путем раскрытия случайной части полученной битовой последовательности (раскрытая часть в дальнейшем отбрасывается). Далее происходит распределенная коррекция ошибок в оставшейся части, если вероятность ошибки не превышает критической величины. Затем производится сжатие очищенного ключа (усиление секретности – privacy amplification).

Сделаем предварительную оценку величины критической ошибки для данного протокола для простейших стратегий подслушивания. Параллельно проведем сравнение с протоколом BB84 [1].

Первая простейшая стратегия – прием – перепосыл с угадыванием базиса. Для стандартного протокола BB84 данная стратегия сводится к следующему. Подслушиватель пытается угадать базис, затем производит измерения в этом базисе. Вероятность правильно угадать базис равна 1/2. Если базис угадан правильно, то состояния из-за их ортогональности идентифицируются в этом базисе с достоверностью. Поэтому для половины передаваемой последовательности подслушиватель знает все передаваемые состояния. Для второй половины, где базис не угадан, измерения в неправильном базисе дают вероятность ошибки для подслушивателя, равную 1/2. Взаимная

информация подслушивателя о передаваемой последовательности, после раскрытия базисов легитимными пользователями, равна $I_{AE} = 1/2$ в пересчете на посылку. Ошибка на приемной стороне, которая возникает при данной стратегии подслушивателя, равна $Q = 25\%$, поскольку только половина состояний из той части (половины) последовательности, где базис был угадан неправильно, при перепосылке состояний из неправильного базиса, даст ошибку на приемном конце.

Для данного протокола вероятность угадывания правильного базиса составляет $1/4$. С вероятностью $1/2$ угадывается базис L или R, и с вероятностью $1/2$, при выбранном L или R, базис $+$ или $\times$. Поэтому подслушиватель знает с достоверностью, после раскрытия базисов легитимными пользователями, $1/4$ долю бит в передаваемой последовательности. Для остальной $3/4$ последовательности вероятность ошибки для подслушивателя составляет, как следует из (5)–(8), $1/2$. Соответственно, взаимная информация подслушивателя равна $I_{AE} = 1/4$ в пересчете на посылку для всей последовательности. Для вероятности ошибки от перепосыла состояний для той половины последовательности, для которой базис L или R угадан правильно, рассуждения аналогичны предыдущему случаю, как для протокола BB84. Вероятность ошибки на приемной стороне равна $\frac{1}{4}\frac{1}{2}$. Для второй половины, для которой базис L или R угадан неправильно перепосыл состояний приведет к вероятности ошибки на приемной стороне, равной $\frac{1}{2}\frac{1}{2}$. Суммарная вероятность ошибки $Q = 37.5\%$ при взаимной информации $I_{AE} = 1/4$. Таким образом, при подобной стратегии подслушивания взаимная информация в два раза меньше, а вероятность производимой ошибки при этом в полтора раза больше, чем для протокола BB84.

Следующая стратегия типа прием – перепосыл для обычного протокола BB84 сводится к измерению состояний в так называемом промежуточном симметричном базисе (Breidbart basis) [8] в двумерном пространстве состояний. В этом базисе углы между базисными векторами и информационными состояниями $\frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ и $\frac{1}{\sqrt{2}}(|0\rangle \pm i|1\rangle)$ составляют $\pi/8$ и $5\pi/8$. В этом базисе вероятность правильной идентификации p бита 0 или 1 есть (например, для базисов $+, \times L$)

$$p = |\langle 0_{+L}|0_{Br}\rangle|^2 = |\langle 1_{+L}|1_{Br}\rangle|^2 = |\langle 0_{\times L}|0_{Br}\rangle|^2 = \\ = |\langle 1_{\times L}|1_{Br}\rangle|^2 = \cos^2\left(\frac{\pi}{8}\right) = \frac{1}{2}\left(1 + \frac{1}{\sqrt{2}}\right) \approx 85\%, \quad (9)$$

соответственно, вероятность ошибки $1 - p$ (вероятность перепослать 0 к Бобу, когда реально Алиса посылала 1, и наоборот) есть

$$1 - p = |\langle 0_{+L}|1_{Br}\rangle|^2 = |\langle 1_{+L}|0_{Br}\rangle|^2 = \\ = |\langle 0_{\times L}|1_{Br}\rangle|^2 = |\langle 1_{\times L}|0_{Br}\rangle|^2 = \\ = 1 - \cos^2\left(\frac{\pi}{8}\right) = \frac{1}{2}\left(1 - \frac{1}{\sqrt{2}}\right) \approx 15\%. \quad (10)$$

Здесь $|0_{Br}\rangle$, $|1_{Br}\rangle$ – промежуточный базис. Взаимная информация подслушивателя о битовой строке после раскрытия базисов фактически ограничена пропускной способностью бинарного симметричного канала связи с вероятностью ошибки $1 - p$:

$$I_{AE} = 1 + p\log p + (1 - p)\log(1 - p) \approx 0.4. \quad (11)$$

В отличие от предыдущей стратегии информация подслушивателя о каждом передаваемом бите является вероятностной. Как известно, секретная передача ключей возможна [9], если взаимная информация о битовой строке между Алисой и Бобом I_{AB} больше, чем взаимная информация между Алисой и подслушивателем

$$I_{AB} > I_{AE}. \quad (12)$$

Поскольку состояния подслушивателем идентифицируются с ошибкой, то это приводит к появлению ошибки Q на приемной стороне. Взаимная информация I_{AB} определяется пропускной способностью симметричного бинарного канала связи с вероятностью ошибки Q:

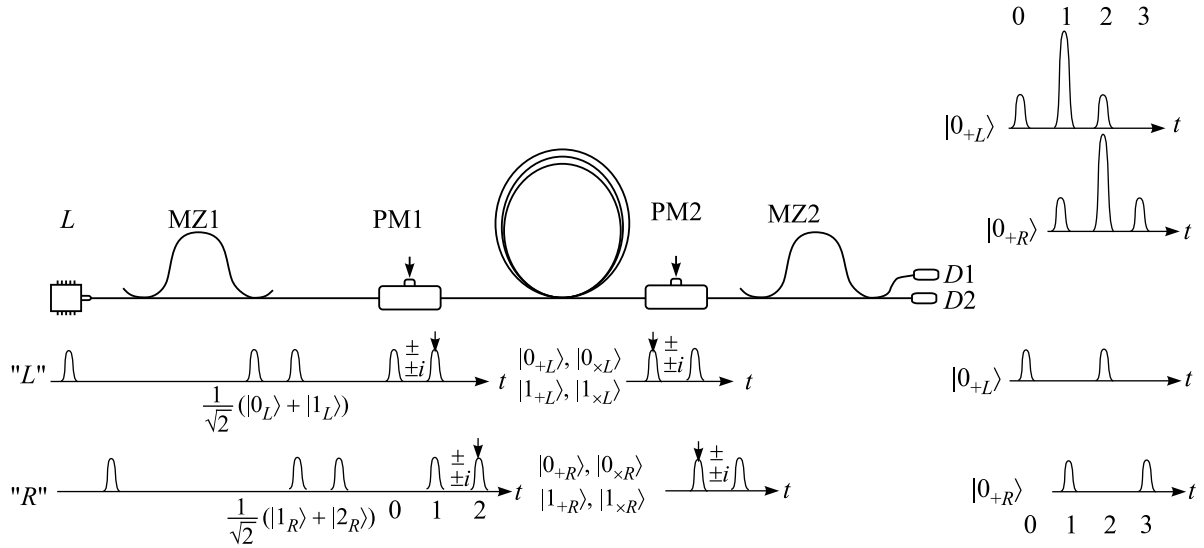
$$I_{AB} = 1 + Q\log Q + (1 - Q)\log(1 - Q). \quad (13)$$

Условие (12) дает критическую ошибку на приемной стороне, до которой возможно распространение секретных ключей (при данной стратегии подслушивания):

$$I_{AB} = I_{AE} \approx 0.4, \quad Q \approx 15\%. \quad (14)$$

Таким образом, стратегия подслушивания с измерением в промежуточном симметричном базисе оказывается более эффективной для подслушивателя, чем стратегия с простым угадыванием базисов.

Перейдем к обсуждению аналогичной стратегии для нашего протокола. Оказывается, что промежуточного симметричного базиса, который минимизирует ошибку по всем состояниям для случая, когда $M = N + 1$ (M – число базисов, в нашем случае $M = 4$, $N = 3$ – размерность пространства состояний), не существует [10]. Поэтому сначала подслушиватель должен угадать базис L или R (это имеет место с вероятностью $1/2$), а затем использовать



Оптоволоконная схема квантовой криптографии с фазово-временным кодированием. MZ1 и MZ2 – разбалансированные интерферометры Маха-Цандера, PM1 и PM2 – фазовые модуляторы, L – лазер, $D1$, $D2$ – лавинные фотодетекторы, 0, 1, 2, 3 – временные окна

промежуточный базис. Базис L или R правильно угадывается только для половины последовательности, например, L, а затем производятся измерения в промежуточном базисе, которые описываются разложением единицы

$$I = |0_{Br}\rangle\langle 0_{Br}| + |1_{Br}\rangle\langle 1_{Br}| + |2\rangle\langle 2|. \qquad (15)$$

В этом случае для половины последовательности, для которой базис, например, L, был угадан правильно, справедливы рассуждения, аналогичные предыдущему случаю. Взаимная информация подслушивателя есть

$$I_{AE} = \frac{1}{2}(1 + p\log p + (1-p)\log(1-p)) \approx 0.2. \qquad (16)$$

Для второй половины последовательности, для которой базис, например, L, угадан неверно, взаимная информация подслушивателя, как видно из структуры состояний (1)–(4) и измерения (15), равна нулю. Производимая подслушивателем ошибка на приемной стороне при этом равна

$$Q = \frac{15\%}{2} + \frac{1}{4}\frac{1}{2}\frac{1}{2} \approx 32.5\%. \qquad (17)$$

Таким образом, предварительные оценки показывают, что производимая подслушивателем ошибка больше, а извлекаемая информация при этом меньше, чем в протоколе BB84. Это связано с тем, что различимость состояний для подслушивателя эффективно меньше не только за счет неортогональности состояний внутри разных базисов $(+L, \times L)$ и $(+R, \times R)$, но и за счет попарной неортогональности состояний из разных базисов L и R.

Опишем теперь оптоволоконную реализацию данного протокола. Оптоволоконная реализация представлена на рисунке. Система состоит из лазера, двух разбалансированных оптоволоконных интерферометров Маха-Цандера с разностью длин плеч по времени T, двух фазовых модуляторов и двух лавинных фотодетекторов, работающих в стробируемом режиме. На рисунке не показан лазер, который генерирует короткие классические импульсы, используемые для синхронизации (привязке по времени) однофотонных состояний в каждой посылке, и аттенюатор.

Приготовление информационных состояний. Алиса запускает лазер, который генерирует короткие импульсы в каждой посылке. При этом случайно и равновероятно генерируется одно из двух состояний, сдвинутых по времени на величину T, равную разности длинного и короткого плеча интерферометра Маха-Цандера. На данной стадии Алиса, по существу, выбирает базис L или R. Обозначим данную пару состояний как $|0_L\rangle$ и $|1_R\rangle$. Состояния $|0_L\rangle$ и $|1_R\rangle$ отличаются друг от друга лишь на сдвиг по времени на величину T ($|1_R\rangle = U(T)|0_L\rangle$, $U(T)$ – оператор трансляции по времени на T). Далее, как несложно убедиться, после прохождения через интерферометр Маха-Цандера на одном из его выходов данные состояния преобразуются в следующую пару состояний:

$$|0_L\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |1_R\rangle \to \frac{1}{\sqrt{2}}(|1\rangle + |2\rangle). \qquad (18)$$

Таблица 1

Bit value	Alice phase ϕ_A	State in basis L	State in basis R	Bob phase ϕ_B
0	0	$\|0_{+L}\rangle$	$\|0_{+R}\rangle$	0
1	π	$\|1_{+L}\rangle$	$\|1_{+R}\rangle$	0
0	$\pi/2$	$\|0_{\times L}\rangle$	$\|0_{\times R}\rangle$	$\pi/2$
1	$3\pi/2$	$\|1_{\times L}\rangle$	$\|1_{\times R}\rangle$	$\pi/2$

Каждое состояние в (18) представляет собой суперпозицию состояний $|0\rangle$, $|1\rangle$ и $|1\rangle$, $|2\rangle$, локализованных во временных окнах 0, 1, 2, соответственно (рисунок). Временные окна 0, 1, 2 последовательно отстоят друг от друга на временной интервал T, равный разности длинного и короткого плеч интерферометра Маха-Цандера.

Далее, при прохождении состояний (18) через фазовый модулятор Алиса прикладывает на короткое время напряжение к модулятору, которое приводит к появлению дополнительной разности фаз между "половинками" состояний в суперпозиции $-\frac{1}{\sqrt{2}}(|0\rangle + + e^{i\phi_A}|1\rangle)$, $\frac{1}{\sqrt{2}}(|1\rangle + e^{i\phi_A}|2\rangle)$. Физически приложение напряжения к фазовому модулятору на время, когда в нем присутствует одна из "половинок" состояния, представляющего суперпозицию локализованных во временных окнах состояний, изменяет показатель преломления среды, что и приводит к появлению дополнительной разности фаз между "половинками" в суперпозиции. Такое включение фазовых модуляторов было использовано в работе [11] (предыдущих оптоволоконных реализациях протокола BB84 фазовые модуляторы включались в длинные плечи интерферометра Маха-Цандера на приемном и передающем конце). Возможны два варианта приложения напряжения, которые с точки зрения квантового криптографического протокола эквивалентны, поскольку имеет смысл только относительная разность фаз между "половинками" в суперпозиции. В первом варианте напряжение прикладывается во временном окне 1 (к передней "половинке" в случае $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ (18), и к задней, в случае состояния $\frac{1}{\sqrt{2}}(|1\rangle + |2\rangle)$ (18)). Во втором варианте напряжение на модулятор прикладывается во временном окне 1, если Алиса генерирует состояние $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, и во временном окне 2, если Алиса генерирует состояние $\frac{1}{\sqrt{2}}(|1\rangle + |2\rangle)$. Для определенности будем считать, что Алиса действует по второму варианту и выбирает случайно и равновероятно напряжение на модуляторе, которое приводит к относительной разности фаз в соответствии с табл.1.

Далее, после ослабления состояния посылаются в канал связи. На приемной стороне Боб случайно равновероятно и независимо от Алисы прикладывает напряжения на фазовый модулятор, которые приводят к дополнительной относительной разности фаз $\phi_B = 0$ или $\phi_B = \pi/2$. Способ подачи напряжения на модулятор такой же, как на передающей стороне. Перед входом в интерферометр Маха-Цандера на приемной стороне состояния после фазового модулятора имеют вид

$$\frac{1}{\sqrt{2}}(|0\rangle + e^{i(\phi_A - \phi_B)}|1\rangle) - \quad \text{базис } L, \tag{19}$$

$$\frac{1}{\sqrt{2}}(|1\rangle + e^{i(\phi_A - \phi_B)}|2\rangle) - \quad \text{базис } R. \tag{20}$$

Далее происходит согласование базисов по открытому каналу связи. Алиса сообщает базисы для каждой посылки, которые она использовала, но не сообщает значения бита. В каждом базисе имеются два значения бита, которые не раскрываются публично. Боб оставляет измерения только в тех посылках, где базисы совпадали. Соответствие базисов (относительной фазы в суперпозиции) у Алисы и Боба приведено в табл.1.

Для не отбрасываемых посылок, в которых базисы совпадают, на детекторы ($D1$ и $D2$) поступают состояния, приведенные в табл.2.

Таблица 2

Bit value	Alice's state	Bob's state	Bob's detector
0	$\|0_{+L}\rangle$	$\frac{1}{8}(\|0\rangle + 2\|1\rangle + \|2\rangle)$	$D1$
1	$\|1_{+L}\rangle$	$\frac{1}{8}(\|0\rangle + \|2\rangle)$	$D2$
0	$\|0_{\times L}\rangle$	$\frac{1}{8}(\|0\rangle + \|2\rangle)$	$D1$
1	$\|1_{\times L}\rangle$	$\frac{1}{8}(\|0\rangle + 2\|1\rangle + \|2\rangle)$	$D2$
0	$\|0_{+R}\rangle$	$\frac{1}{8}(\|1\rangle + \|3\rangle)$	$D1$
1	$\|1_{+R}\rangle$	$\frac{1}{8}(\|1\rangle + \|3\rangle)$	$D2$
0	$\|0_{\times R}\rangle$	$\frac{1}{8}(\|1\rangle + 2\|2\rangle + \|3\rangle)$	$D1$
1	$\|1_{\times R}\rangle$	$\frac{1}{8}(\|1\rangle + 2\|2\rangle + \|3\rangle)$	$D2$

Измерения проводятся путем стробирования детекторов $D1$ и $D2$ во временных окнах 1 и 2, которые выбираются случайно. После стадии согласования базисов по открытому каналу связи между Алисой и Бобом Боб однозначно может идентифицировать передаваемые значения битов. Например, в отсутствие

подслушивателя, если передавалось состояние $|0_{+L}\rangle$, то отсчеты для состояний в базисе $+L$ будут иметь место только во временном окне 1 в детекторе $D1$ и никогда в окне 1 в детекторе $D2$. Фактически, преобразование состояний при помощи фазового модулятора и интерферометра на приемной стороне, измерение в определенных временных окнах детекторами $D1$, $D2$ эквивалентно использованию измерений (5)–(8) в смысле различимости состояний.

В заключение отметим, что точная величина критической ошибки для данного протокола на сегодняшний день неизвестна. Предварительные оценки для простейших стратегий подслушивания типа прием – перепосыл дают надежду, что предложенный протокол потенциально имеет большую критическую величину ошибки, чем стандартный и наиболее исследованный протокол BB84. Предложенный протокол допускает обобщение (усиление в смысле величины критической ошибки), если сделать пару состояний в каждом из базисов $+L$, $\times L$ (аналогично в $+R$, $\times R$) попарно неортогональными путем соответствующего выбора фаз. Такая конструкция приводит к так называемому протоколу BB84 4+2 [12], который устойчив к PNS-атаке (Photon Number Splitting attack). В нашем случае, это приводит к новому, еще более устойчивому протоколу, чем BB84 4+2, который будет представлен отдельно.

Один из авторов (С.Н.М.) благодарит Академию криптографии РФ за поддержку. Работа поддержана проектами Российского фонда фундаментальных исследований # 05-02-08306-офи-а, # 05-02-17387, # 06-02-16769.

1. C. H. Bennett and G. Brassard, *Quantum Cryptography: Public Key Distribution and Coin Tossing*, Proc. of IEEE Int. Conf. on Comput. Sys. and Sign. Proces., Bangalore, India, December 1984, p. 175.
2. D. Mayers and A. Yao, arXiv:quant-ph/9802025.
3. E. Biham, M. Boyer, P. O. Boykin et al., arXiv:quant-ph/9912053.
4. P. W. Shor and J. Preskill, arXiv:quant-ph/0003004.
5. H. Bechmann-Pasquinucci and A. Peres, Phys. Rev. Lett. **85**, 3313 (2000).
6. H. Bechmann-Pasquinucci and W. Tittel, Phys. Rev. A **61**, 062308 (2000).
7. C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
8. C. H. Bennett, F. Bessette, G. Brassard et al., **5**, 53 (1992).
9. I. Csiszár and J. Körner, IEEE Trans. Inf. Theory **24**, 339 (1978).
10. M. Bourennane, A. Karlsson, and G. Björk, Phys. Rev. A **64**, 012306-1 (2001); R. Asplund, M. Bourennane, and G. Björk, arXiv:quant-ph/0011037.
11. Y. Nambu, K. Yoshino, and A. Tomita, arXiv:quant-ph/0603041.
12. V. Scarani, A. Acin, G. Ribordy, and N. Gisin, Phys. Rev. Lett. **92**, 057901-1 (2004); A. Acin, N. Gisin, and V. Scarani, arXiv:quant-ph/0302037.