ЖЭТФ, 2020, том 157, вып. 2, стр. 195–205

О ПРОСТОМ СПОСОБЕ ЗАЩИТЫ ОТ АТАКИ "DETECTORS MISMATCH" В КВАНТОВОЙ КРИПТОГРАФИИ: ПРОТОКОЛ BB84

К. А. Балыгин [a,e], ***И. Б. Бобров*** [a,e], ***А. Н. Климов*** [a,e],

С. Н. Молотков [b,c,d,e*], ***М. И. Рыжкин*** [b]

[a] *Физический факультет, Московский государственный университет им. М. В. Ломоносова 119899, Москва, Россия*

[b] *Институт физики твердого тела Российской академии наук 142432, Черноголовка, Московская обл., Россия*

[c] *Академия криптографии Российской Федерации 121552, Москва, Россия*

[d] *Факультет вычислительной математики и кибернетики, Московский государственный университет им. М. В. Ломоносова 119899, Москва, Россия*

[e] *Центр квантовых технологий, Московский государственный университет им. М. В. Ломоносова 119899, Москва, Россия*

Поступила в редакцию 1 июля 2019 г.,
после переработки 26 августа 2019 г.
Принята к публикации 28 августа 2019 г.

Системы квантовой криптографии являются открытыми системами, поэтому возможно активное зондирование, а также навязывание нештатной работы элементов приемной и передающей аппаратуры, которое, как было продемонстрировано экспериментально, может приводить к компрометации секретности системы. Разработка систем, которые гарантируют обнаружение таких атак и секретность передаваемых ключей не на уровне отдельных технических решений, а на уровне физических принципов, является актуальной задачей. В работе предложен простой, физически интуитивно понятный принцип защиты от атаки активного зондирования — Detectors Mismatch, который требует лишь минимальных изменений в имеющихся системах, использующих протокол квантового распределения BB84.

DOI: 10.31857/S0044451020020017

1. ВВЕДЕНИЕ

Квантовая криптография [1], синоним квантового распределения ключей, решает центральную проблему симметричной криптографии, а именно, проблему распределения криптографических ключей, представляющих собой случайную идентичную последовательность нулей и единиц на передающей и принимающей сторонах, неизвестную третьей стороне. Распределение ключей происходит путем согласования — синхронизации двух независимых случайных последовательностей на передающей и приемной сторонах посредством передачи между ними серии квантовых состояний через открытый и доступный для вторжения квантовый канал связи (оптическое волокно или атмосферный канал).

Квантовая криптография обеспечивает безусловную секретность ключей. Под этим понимается тот факт, что секретность ключей гарантируется фундаментальными запретами квантовой механики на различимость квантовых состояний, а не техническими или вычислительными ограничениями подслушивателя. Таким фундаментальным запретом является теорема *no cloning* [2], которая есть следствие соотношений неопределенностей

* E-mail: sergei.molotkov@gmail.com

Гайзенберга – Робертсона [3, 4] для двух некоммутирующих наблюдаемых — эрмитовых операторов. Некоммутирующие эрмитовы операторы не могут иметь общей системы собственных векторов. Это означает, что не существует общего измерения, которое могло бы без ошибки различать собственные состояния одного и другого эрмитовых операторов. Набор собственных векторов каждого эрмитова оператора образует полный ортонормированный базис.

Применительно к квантовой криптографии это означает следующее. Если в качестве информационных состояний выбираются состояния внутри одного или другого базиса случайно в соответствии со случайной последовательностью на передающей стороне, то у подслушивателя принципиально не существует измерений, которые позволяли бы без ошибок различать один или другой набор состояний. Как следствие, любые попытки измерений передаваемых квантовых состояний приведут к ошибкам на приемной стороне.

Выбор базиса измерений на приемной стороне проводится в соответствии со случайной последовательностью, независимой от последовательности на передающей стороне. Посылки, в которых базисы не совпадали, впоследствии легитимными пользователями отбрасываются посредством обмена информацией через открытый классический аутентичный канал связи. Поскольку внутри базиса состояния ортогональны, в посылках, где базисы приготовления и измерения состояний совпадали, можно однозначно идентифицировать передаваемые состояния, если не было вторжений в квантовый канал связи. Вторжение в квантовый канал связи из-за фундаментальных ограничений квантовой механики неизбежно приводит к ошибкам на приемной стороне. Оценка вероятности ошибки происходит через открытый классический канал связи. Квантовая теория информации позволяет получить через энтропийные соотношения неопределенностей [5–8] фундаментальную верхнюю границу утечки информации к подслушивателю при данной наблюдаемой вероятности ошибки.

После коррекции ошибок через открытый классический канал связи возникает одинаковая битовая строка на передающей и принимающей сторонах — просеянный ключ, о котором подслушиватель имеет частичную информацию, которую он получил при вторжении в квантовый канал связи и исправлении ошибок. «Изъятие» частичной информации подслушивателя о просеянном ключе происходит сжатием (хешированием) битовой строки через открытый канал связи — процедура усиления секретности [9, 10] с использованием универсальных хеш-функций второго порядка. В результате возникает общий секретный ключ, о котором подслушиватель не имеет никакой информации.

Действительно, квантовая криптография гарантирует безусловную секретность ключей [11, 12], если учитывать только атаки на передаваемые квантовые состояния, когда подслушиватель не имеет ни прямого, ни косвенного доступа к передающей (Алиса) и принимающей (Боб) станциям. В реальности системы квантовой криптографии являются открытыми системами, в том смысле, что подслушиватель (Ева) может иметь косвенный доступ к приемо-передающей аппаратуре, используя зондирующее излучение. Обычно такие атаки называются Trojan-horse attacks [13–19].

Все атаки на системы квантовой криптографии можно разделить на три класса.

1. Атаки непосредственно на информационные квантовые состояния в квантовом канале связи.

2. Пассивные атаки, использующие детектирование побочного электромагнитного излучения от аппаратуры приемной и передающей станций.

3. Активные атаки, использующие зондирование внешним излучением состояния элементов аппаратуры — фазовых модуляторов, лавинных детекторов, а также атаки с модификацией работы элементов системы, например, атака с ослеплением лавинных детекторов [13–16] и атака Detectors Mismatch [18, 19].

Первый класс атак подразумевает, что подслушиватель не имеет ни прямого, ни косвенного доступа к приемо-передающей аппаратуре. Секретность ключей при таких атаках гарантируется фундаментальными ограничениями квантовой теории на различимость квантовых состояний.

Второй класс атак связан с пассивным детектированием побочных сигналов от работы элементов приемной и передающей аппаратуры — излучения от фазовых модуляторов, генераторов случайных чисел, стробирования лавинных детекторов, обратного переизлучения лавинных детекторов при их срабатывании.

Третий класс атак использует активное зондирование через волоконную линию связи состояния активных элементов системы, например, фазовых модуляторов, которые несут информацию о передаваемом ключе. Возможны атаки, при которых изменяется штатная работа элементов системы, например, лавинных детекторов [13–16].

Без устойчивости системы к таким атакам невозможно всерьез говорить о секретности распределяемых ключей. Требуется исследование секретности ключей с учетом подобных атак.

Принципиально важно обеспечить защиту систем квантовой криптографии от атак второго и третьего типа не техническими средствами, добавлением дополнительных сторожевых детекторов и других технических контрольных элементов, а на уровне фундаментальных физических принципов. В противном случае квантовая криптография из разряда систем, обеспечивающих безусловную секретность ключей, гарантируемую фундаментальными законами физики, будет переведена в разряд систем, которые обеспечивают секретность лишь техническими средствами. Поэтому важно найти такие способы приготовления и регистрации квантовых состояний, которые гарантировали бы на физическом уровне детектирование изменения работы элементов системы. При этом желательно не вносить существенных изменений в конструкцию системы. Ниже будем рассматривать системы с фазовым кодированием. В этих системах приготовление информационных квантовых состояний в разных базисах происходит при помощи интерферометра Маха – Цандера, который приводит к «размазыванию» во времени исходного лазерного импульса — сильно ослабленного когерентного состояния. На приемной стороне измерение также реализуется при помощи интерферометрических преобразований на интерферометре Маха – Цандера. Фактически интерферометр обеспечивает конструктивную на одном выходе и деструктивную интерференцию на другом выходе входных квантовых состояний. Конструктивная и деструктивная интерференция обеспечивается выбором фазового сдвига между состояниями в разных временных окнах.

Ниже будет показано, что введение дополнительного случайного выбора фазы внутри каждого базиса гарантирует детектирование атаки Detectors Mismatch. При этом детектирование такой атаки фактически гарантируется нарушением интерференционной картины подслушивателем, поскольку Еве неизвестен случайный выбор фаз на приемной станции, который отвечает максимуму интерференционной картины. С физической точки зрения картина разрушения интерференции и неизбежное возникновение ошибок при детектировании, полностью аналогична разрушению интерференции на двух щелях, если положение щелей выбирается случайно из двух вариантов, неизвестных подслушивателю. Ниже будет подробно разобрана данная ситуация защиты, которая основана на очень простой и физически интуитивно понятной идее. Причем реализация защиты не требует сколь-нибудь существенных изменений в конструкции системы.

Ранее было показано, что для систем с фазовым кодированием атаки с ослеплением оказываются неэффективными и приводят к детектированию атаки [20, 21]. Причем детектирование такой атаки также отвечает разрушению распределенной интерференционной картины на приемной стороне. Других модификаций атаки с ослеплением детекторов с тех пор еще не было предложено.

Ниже пойдет речь о так называемой атаке Detectors Mismatch [18, 19]. При такой атаке подслушиватель навязывает отсчеты лавинным фотодетекторам и в результате может знать весь ключ, не производя ошибок на приемной стороне. Система без защиты от такой атаки не может обеспечить секретность ключей. Более точно, если такая атака не детектируется легитимными пользователями, то система не обеспечивает секретность ключей. Если атака детектируется, т. е. система устроена таким образом, что атака неизбежно приводит к наблюдаемым ошибкам на приемной стороне, то обнаружение атаки позволяет защититься от нее. Иначе говоря, обнаружение атаки автоматически ведет к защите от нее, в том смысле, как было сказано выше.

Ниже предлагается простой способ защиты от этой атаки применительно к протоколу квантового распределения ключей BB84 [1], который является широко используемым базовым протоколом. Предлагаемый в работе простой и эффективный способ защиты от данной атаки основан не на технических «заплатках», а на физических принципах реализации самого протокола квантового распределения ключей — способа приготовления и измерения квантовых состояний.

Нужно отметить, как будет видно ниже, сама по себе атака Detectors Mismatch является нетривиальной, поскольку Ева получает информацию о ключе и при этом скрывает от измерений на приемной стороне разрушение исходной интерференционной картины. Цель данной работы — предложить простой способ модификации измерений квантовых состояний, при котором гарантированно такая атака будет детектироваться. На наш взгляд, подробный разбор ситуации *pro et contra* является с физической точки зрения вполне интересным.

2. АТАКА DETECTORS MISMATCH

Атака Detectors Mismatch применима к системам квантовой криптографии, как с фазовым, так и с поляризационным кодированием, использующим два однофотонных детектора. Кривые чувствительности двух разных детекторов могут быть различными. Это значит, что могут быть временные интервалы, в которых один детектор имеет эффективность регистрации фотонов, отличную от нуля, а чувствительность другого детектора равна нулю (рис. 1), и наоборот. В таком случае злоумышленник может послать на приемную сторону импульс, который попадал бы в тот временной интервал, в котором чувствительность одного детектора равна нулю, а другого не равна.

Таким образом, злоумышленник может навязывать срабатывания нужного ему детектора. При штатной работе системы положение по времени и длительность квантовых состояний выбирается так, чтобы они попадали в область чувствительности по времени обоих детекторов (рис. 1). Подслушиватель в каждой посылке или части посылок может подменять истинные квантовые состояния своими состояниями (fake states) с меньшей длительностью и другим положением по времени относительно кривых чувствительности детекторов, тем самым может навязывать отсчет или его отсутствие в одном из детекторов.

Предлагаемый способ обнаружения и защиты от атаки, использующей разную по времени зависимость чувствительности однофотонных детекторов, применим для систем квантовой криптографии с фазовым кодированием и поляризационным кодированием.

Прежде чем описать способ защиты, приведем описание работы системы квантового распределения ключей в отсутствие атаки и саму атаку Detectors Mismatch, использующую разные временные зависимости чувствительности однофотонных детекторов [18, 19].

Приведем необходимое для дальнейшего описание атаки на системы квантового распределения ключей с фазовым кодированием на примере протокола BB84, который является базовым протоколом. Для систем с поляризационным кодированием и других протоколов атака проводится аналогично.

В стандартной общепринятой версии протокола BB84 используется два базиса + и ×, которые на передающей стороне выбираются случайно и равновероятно в соответствии со случайной последовательностью 0 и 1. Внутри каждого базиса случайно и равновероятно также в соответствии со случайной последовательностью, выбирается одно из двух значений фазы. Значение фазы однозначно сопоставляется с квантовым состоянием, приготавливаемым на передающей стороне. В системах квантовой криптографии с фазовым кодированием каждое квантовое состояние представляет собой пару квазиоднофотонных когерентных состояний (рис. 1, 2), локализованных во временных окнах 1 и 2,

$$|\alpha\rangle_1 \otimes |e^{i\varphi_A}\alpha\rangle_2, \tag{1}$$

где α — амплитуда квазиоднофотонного когерентного состояния, индексы 1 и 2 обозначают временные окна (рис. 1), выбор базиса и состояний внутри каждого базиса фиксируется выбором относительной фазы между квазиоднофотонными состояниями внутри пары (рис. 1, 2), относительная фаза когерентных состояний, локализованных во временных окнах 1 и 2 в базисах + и ×, имеет вид

$$\begin{cases} 0^+ \to \varphi_A = 0, \\ 1^+ \to \varphi_A = \pi, \end{cases} \qquad \begin{cases} 0^\times \to \varphi_A = \dfrac{\pi}{2}, \\ 1^\times \to \varphi_A = \dfrac{3\pi}{2}. \end{cases} \tag{2}$$

Зависимости чувствительности двух однофотонных детекторов по времени могут различаться (рис. 1, 2). При штатном режиме работы длительность квантовых состояний и их положение по времени выбираются таким образом, чтобы состояния попадали в общую область по времени зависимости чувствительности обоих однофотонных детекторов D1 и D2 (рис. 1, 2). Перед детектированием состояний на передающей стороне в системах квантовой криптографии с фазовым кодированием состояния, поступающие из квантового канала связи, подвергаются преобразованию на интерферометре Маха–Цандера (рис. 1, 2). На принимающей стороне выбор базиса измерения — либо +, либо × — проводится случайно и равновероятно в соответствии со случайной последовательностью на принимающей стороне. В базисе + выбирается значение фазы $\varphi_B = 0$, в базисе × — значение $\varphi_B = \pi/2$ для компенсации фаз передающей стороны (формула (2)). Выбор фазы проводится наложением напряжения на фазовый модулятор в плече интерферометра Маха–Цандера (рис. 1, 2).

Вероятность отсчета на детекторах в центральном временном окне 2 (рис. 1*a*) определяется разностью фаз передающей и принимающей сторон, и на детекторе D1, пропорциональна

$$\cos^2\left(\frac{\varphi_A - \varphi_B}{2}\right), \tag{3}$$

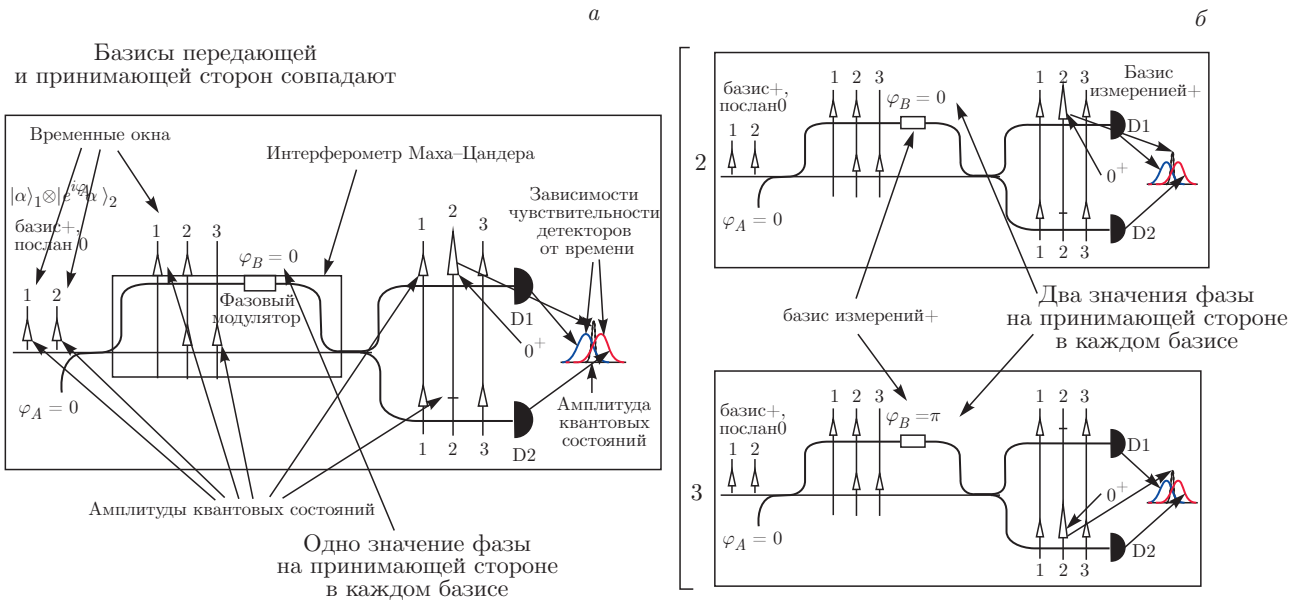

Рис. 1. Схематическое изображение приемной части. Показано распространение информационных состояний через оптический тракт на принимающей стороне и их детектирование для случая, когда базисы принимающей и передающей сторон совпадают. Для примера выбран базис +. В правых частях рисунков также показаны различные временные зависимости чувствительности лавинных детекторов. *а*) Стандартная версия протокола BB84. Показано детектирование состояния 0 в базисе +. Фаза на передающей стороне равна $\varphi_A = 0$, фаза на принимающей стороне в базисе + равна $\varphi_B = 0$. При штатной работе отсчет должен быть на детекторе D1. *б*) Новая версия протокола. Показано детектирование состояния 0 в базисе +. Фаза на передающей стороне равна $\varphi_A = 0$, фаза на принимающей стороне в базисе + выбирается случайно и равновероятно из двух значений $\varphi_B = 0$ и $\varphi_B = \pi$. При $\varphi_B = 0$ отсчет возникает на детекторе D1, при $\varphi_B = \pi$ — на детекторе D2

а на детекторе D2 пропорциональна

$$\sin^2\left(\frac{\varphi_A - \varphi_B}{2}\right). \qquad (4)$$

Если базисы передающей и принимающей сторон совпадают (см. рис. 1, 2, а также формулы (3), (4)), то при разности фаз состояний, выбранных передающей стороной и принимающей стороной $\varphi_A - \varphi_B = 0$, конструктивная интерференция имеет место на входе детектора D1 (рис. 1*а* отвечает ситуации, когда посылался 0 в базисе +, рис. 2 отвечает ситуации, когда посылалась 1 в базисе +), что будет приводить к отсчету в детекторе D1 в центральном временном окне 2. Иначе говоря, при совпадении базисов, например, при базисе +, когда и передающая, и принимающая стороны выбирают фазу 0, после преобразований входных состояний на интерферометре Маха–Цандера конструктивная интерференция будет иметь место на детекторе D1. Из-за деструктивной интерференции на детекторе D2 срабатывания детектора не будет (рис. 1*а*). Отсчет детектора D1 интерпретируется как логический 0 (рис. 1*а*). Если передающая сторона посылала 1 в базисе + (рис. 2*а*), что отвечает выбору фазы π, то на детекторе D2 будет конструктивная интерференция, которая приведет к срабатыванию детектора D2. Из-за деструктивной интерференции на детекторе D1 срабатывания детектора D1 не будет (рис. 2*а*). Отсчет детектора D2 интерпретируется как логическая 1.

При несовпадающих базисах передающей и принимающей сторон полной конструктивной или деструктивной интерференции на детекторах D1 и D2 не происходит (рис. 3). Вероятность детектирования на обоих детекторах D1 и D2 независимо от посланного состояния (рис. 3), соответственно выбора фаз в несовпадающих базисах, будет пропорциональна

$$\sin^2\left(\frac{\varphi_A - \varphi_B}{2}\right) = \cos^2\left(\frac{\varphi_A - \varphi_B}{2}\right) = \frac{1}{2}, \qquad (5)$$

если фазы φ_A и φ_B выбираются из разных базисов, причем независимо от самого выбора фаз. Отсчет будет иметь место на обоих детекторах D1 и D2 (рис. 3) с одинаковой вероятностью независимо от того, какую фазу состояний выбрали передающая и принимающая стороны.

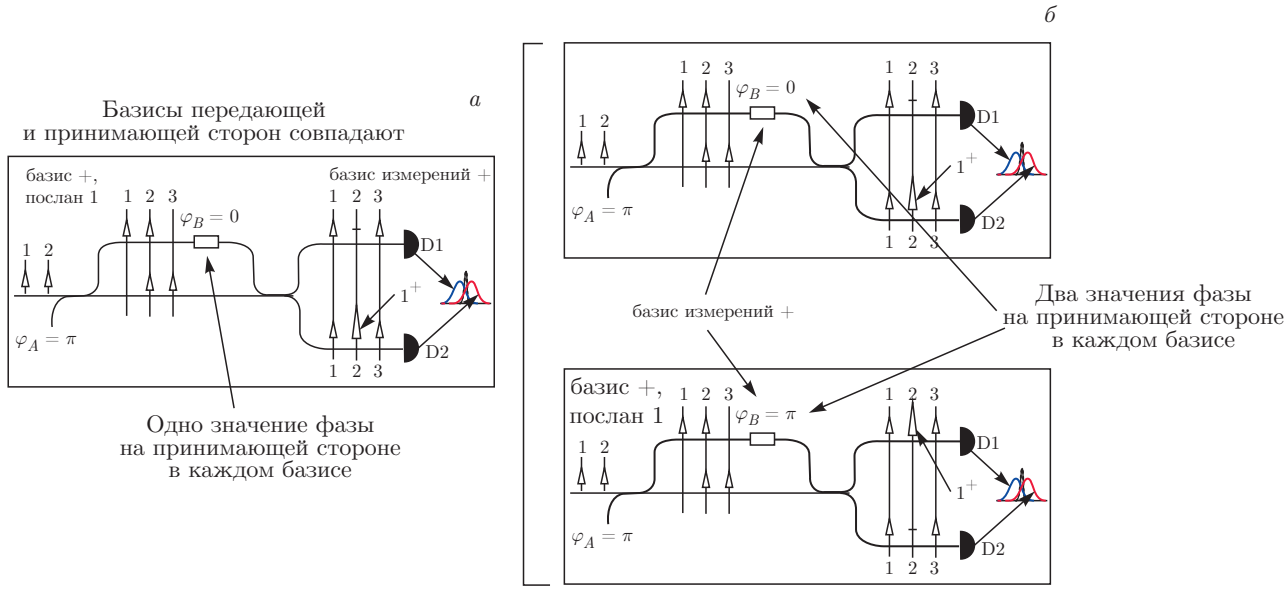

Рис. 2. Схематическое изображение приемной стороны, аналогичное рис. 1. Показано распространение информационных состояний через оптический тракт на принимающей стороне и их детектирование для случая, когда базисы принимающей и передающей сторон совпадают. Для примера выбран базис +. Показаны также различные временные зависимости чувствительности лавинных детекторов. *а*) Стандартная версия протокола BB84. Показано детектирование состояния 1 в базисе +. Фаза на передающей стороне равна $\varphi_A = \pi$, фаза на принимающей стороне в базисе + равна $\varphi_B = 0$. При штатной работе отсчет должен быть на детекторе D2. *б*) Новая версия протокола. Показано детектирование состояния 1 в базисе +. Фаза на передающей стороне равна $\varphi_A = \pi$, фаза на принимающей стороне в базисе + выбирается случайно и равновероятно из двух значений $\varphi_B = 0$ и $\varphi_B = \pi$. При $\varphi_B = 0$ отсчет возникает на детекторе D2, при $\varphi_B = \pi$ — на детекторе D1

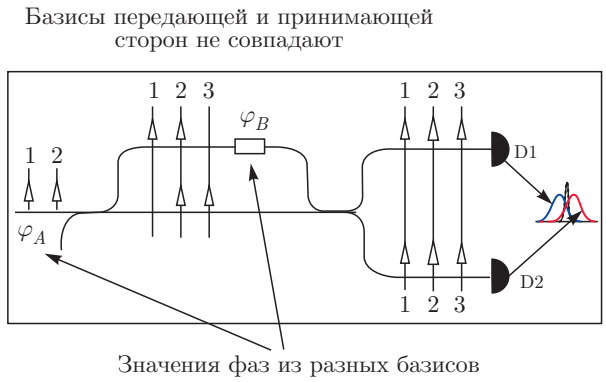

Рис. 3. Иллюстрация эволюции квантовых состояний на принимающей стороне и их детектирования на приемной части для случая, когда базис информационных состояний и базис передающей части не совпадают

Атака Detectors Mismatch является атакой прием–перепосыл: подслушиватель разрывает квантовый канал связи и проводит измерение в своем случайно выбранном базисе и перепосылает свои состояния в зависимости от результата измерений. При описании атаки возникают ситуации, когда базисы перепосланного состояния подслушивателя, принимающей и передающей сторон совпадают (рис. 1, 2), эволюция состояний и их детектирование представлены на рис. 1, 2. Однако возможны ситуации, когда базис перепосланного состояния и базис измерений принимающей стороны не совпадают, данная ситуация показана на рис. 3 для стандартной версии протокола BB84.

Получив результат, подслушиватель готовит состояние, которое противоположно измеренному состоянию в противоположном базисе и во временном окне, в котором детектор, который должен был бы регистрировать измеренные состояния, является чувствительным, а детектор, который должен был бы регистрировать противоположные измеренным состояния, был бы неактивен, т. е. состояния не попадали бы в область чувствительности по времени. То есть в соответствии с результатом своих измерений подслушиватель перепосылает состояние, которое вызовет срабатывание на приемной стороне того же детектора, что сработал у подслушивателя, при условии совпадения базисов подслушивателя и приемной стороны.

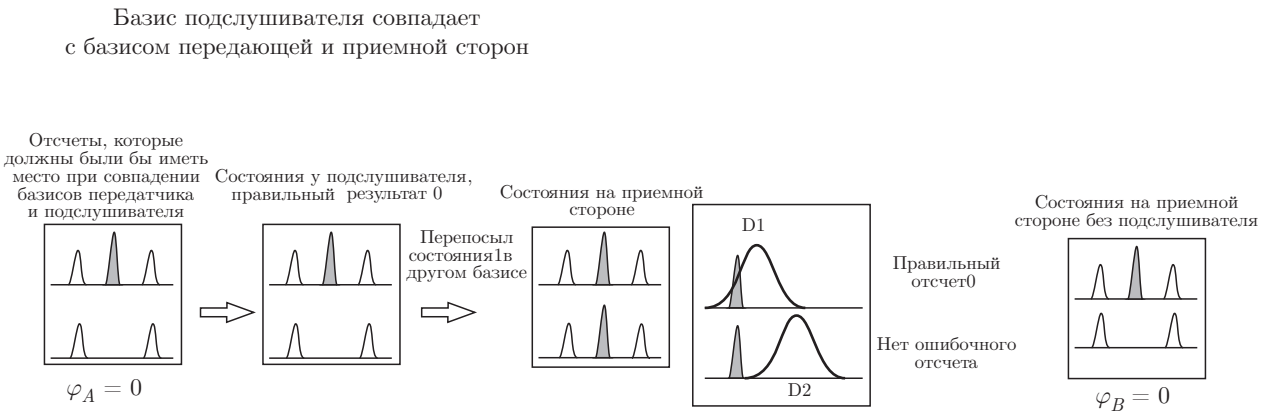

Рис. 4. Иллюстрация детектирования и перепосыла состояний подслушивателем при атаке Detectors Mismatch в стандартной версии протокола BB84 для ситуации, когда базис измерений подслушивателя совпадает с базисом принимающей и передающей сторон

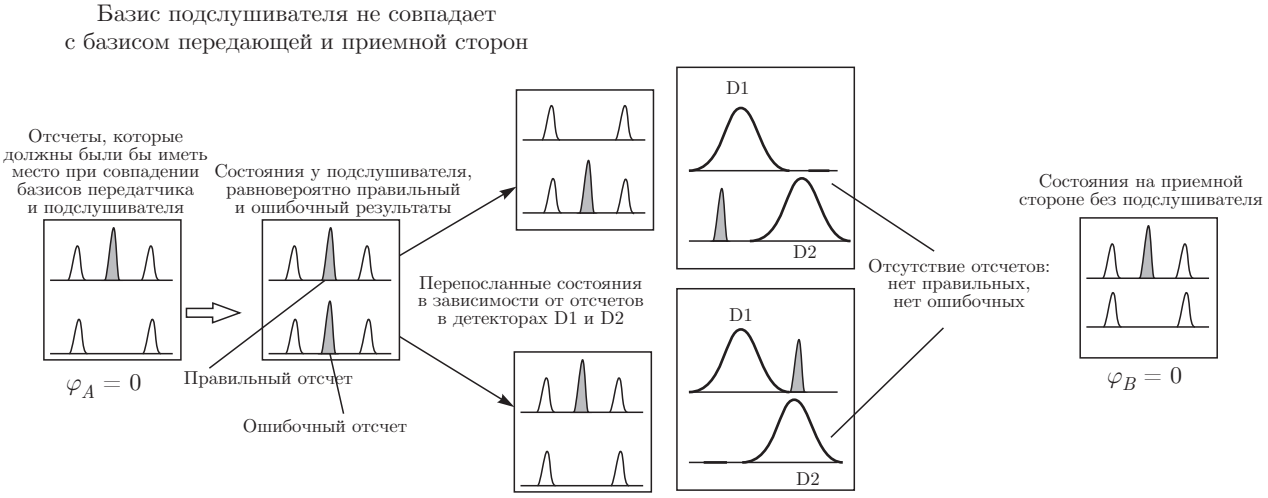

Рис. 5. Иллюстрация эволюции состояний и их детектирование на приемной стороне при атаке Detectors Mismatch в стандартной версии протокола BB84 для случая, когда базис подслушивателя не совпадает с базисом легитимных пользователей

Таким образом, принципиальный момент стратегии подслушивателя состоит в том, что длительность и положение по времени подменного состояния (fake state) всегда выбираются так, чтобы оно не попадало в область чувствительности по времени того однофотонного детектора, который не должен был бы регистрировать перепосланное квантовое состояние в данном базисе, т. е. в базисе, в котором подменное состояние перепосылается (рис. 4). Такая стратегия позволяет подслушивателю не производить ошибок на приемной стороне, если было перепослано неправильное состояние.

Для пояснения рассмотрим пример. Пусть подслушиватель проводил измерение в базисе + и получил значение 0, тогда он перепосылает состояние, отвечающее значению 1 в базисе $\times$, во временном интервале, в котором будет чувствителен детектор D1, а детектор D2 будет неактивен — будет «слеп». Тогда, если Алиса и Боб выбрали базис $\times$, то конструктивная интерференция будет в плече интерферометра, где детектор D2, но в том временном интервале, в котором детектор неактивен — «слеп». Детектор не сработает. Если Алиса и Боб выбрали базис +, то квантовое состояние «делится» пополам после прохождения интерферометра между детекторами D1 и D2 и будет локализовано в том временном интервале, в котором детектор D1 чувствителен, а детектор D2 неактивен. Поскольку передающая и принимающая стороны оставляют только те посылки, в которых базисы совпадали, при атаке подслушивателя возможны две ситуации.

1. Приемная сторона выбрала базис $\times$, тогда на входе детектора D2 будет конструктивная интерференция, а на входе детектора D1 — деструктивная (рис. 5). Сигнал будет расположен во временном окне, в котором детектор D2 слеп. Ни один из детекторов не сработает. Отсутствие отсчетов не есть ошибка.

2. Приемная сторона выбрала базис $+$. Состояние «делится» пополам между детекторами D1 и D2, но будет находиться в области чувствительности только детектора D1 (рис. 4). Сработает детектор D1, Боб запишет значение 1. При этом также возможны две ситуации.

2.1. Если передающая сторона приготовила состояние в базисе $+$, то при согласовании базисов отсчет сохранится и пойдет в ключ. Приемная и передающая стороны и подслушиватель будут иметь одинаковые значения.

2.2. Передающая сторона приготовила состояние в базисе $\times$, тогда при согласовании базисов данная посылка будет выброшена, так как базисы Алисы и Боба не совпадают.

В результате атаки подслушиватель знает весь передаваемый ключ, не производит ошибок на принимающей стороне — ошибочные отсчеты отсутствуют, и не детектируется. Система не обеспечивает секретность ключей. Аналогичная ситуация имеет место и в системах с поляризационным кодированием.

3. ДЕТЕКТИРОВАНИЕ И ЗАЩИТА ОТ АТАКИ

Для обнаружения и защиты от атаки, использующей разную по времени зависимость чувствительности однофотонных детекторов, в системах квантовой криптографии с фазовым и поляризационным кодированием, при которой подслушиватель знает весь криптографический ключ и не обнаруживается, предлагается следующий способ.

Наша идея детектирования и защиты от атаки Detectors Mismatch состоит в следующем. Принимающая сторона в каждом базисе выбирает не одно значение фазы: 0 в базисе $+$ и $\pi/2$ базисе $\times$, как имеет место в известных системах квантовой криптографии с протоколом BB84, а в каждом базисе случайно выбирает два значения фазы: 0 и π в базисе $+$ и $\pi/2$ и $3\pi/2$ в базисе $\times$. При таком выборе фаз при атаке подслушивателя, использующей разную по времени зависимость чувствительности однофотонных детекторов, неизбежно возникают ошибки на принимающей стороне. По наличию ошибок происходит обнаружение подслушивателя и проводится оценка утечки информации к нему.

Модификация протокола представлена на рис. 6. В базисе $+$ выбор одного значения фазы приводит к тому, что состояние 0^+, поступающее на приемную сторону, приводит к конструктивной интерференции на детекторе D1 и отсчету на нем. Отсчет на детекторе D2 отсутствует из-за деструктивной интерференции на нем (рис. 6). Если в базисе $+$ выбираются два значения фазы, то отсчет в детекторе D1 или в детекторе D2 от полученного состояния 0^+ будет иметь место в зависимости от выбора фазы на принимающей стороне: при выборе фазы 0 отсчет в детекторе D1, при выборе фазы π отсчет в детекторе D2 (рис. 6). Аналогично, если на детектор поступает состояние 1^+, то при одном выборе фазы, равной 0, отсчет будет иметь место на детекторе D2. При двух случайных выборах значений фазы на принимающей стороне отсчет будет иметь место на обоих детекторах в зависимости от выбора фазы. При выборе фазы π отсчет от состояния 1^+ будет на детекторе D1 (рис. 1), при выборе фазы 0 отсчет будет иметь место на детекторе D2 (рис. 6).

Таким образом, на принимающей стороне при двух случайных значениях фаз внутри базиса состояния, отвечающие 0^+ и 1^+, дают отсчеты в обоих детекторах в зависимости от выбора фазы. Аналогичная ситуация имеет место в базисе $\times$. Случайный выбор двух значений фаз внутри каждого базиса приводит к тому, что подслушиватель неизбежно будет производить ошибки на принимающей стороне и будет детектироваться.

Обсудим ситуацию более детально. Достаточно рассмотреть случай, когда базис подслушивателя не совпадает с базисом передающей и принимающей сторон, чтобы убедиться в том, что атака приведет к появлению ошибок на приемной стороне — обнаружению подслушивателя. Ситуация совпадающих базисов у всех участников протокола рассматривается аналогично.

Пусть передающая сторона посылала 0 в базисе $+$ (рис. 6). Если базис измерений подслушивателя не совпадает с базисом передающей и принимающей сторон — подслушиватель выбрал базис $\times$, то подслушиватель будет равновероятно получать правильный и ошибочный результаты.

1. Правильный отсчет у подслушивателя (рис. 6). Отсчет у подслушивателя в детекторе D1 (интерпретируется как логический 0) — правильный результат (рис. 6). Результат — отсчет на детекторе D1 — интерпретируется как $0^\times$. В этом случае подслуши-

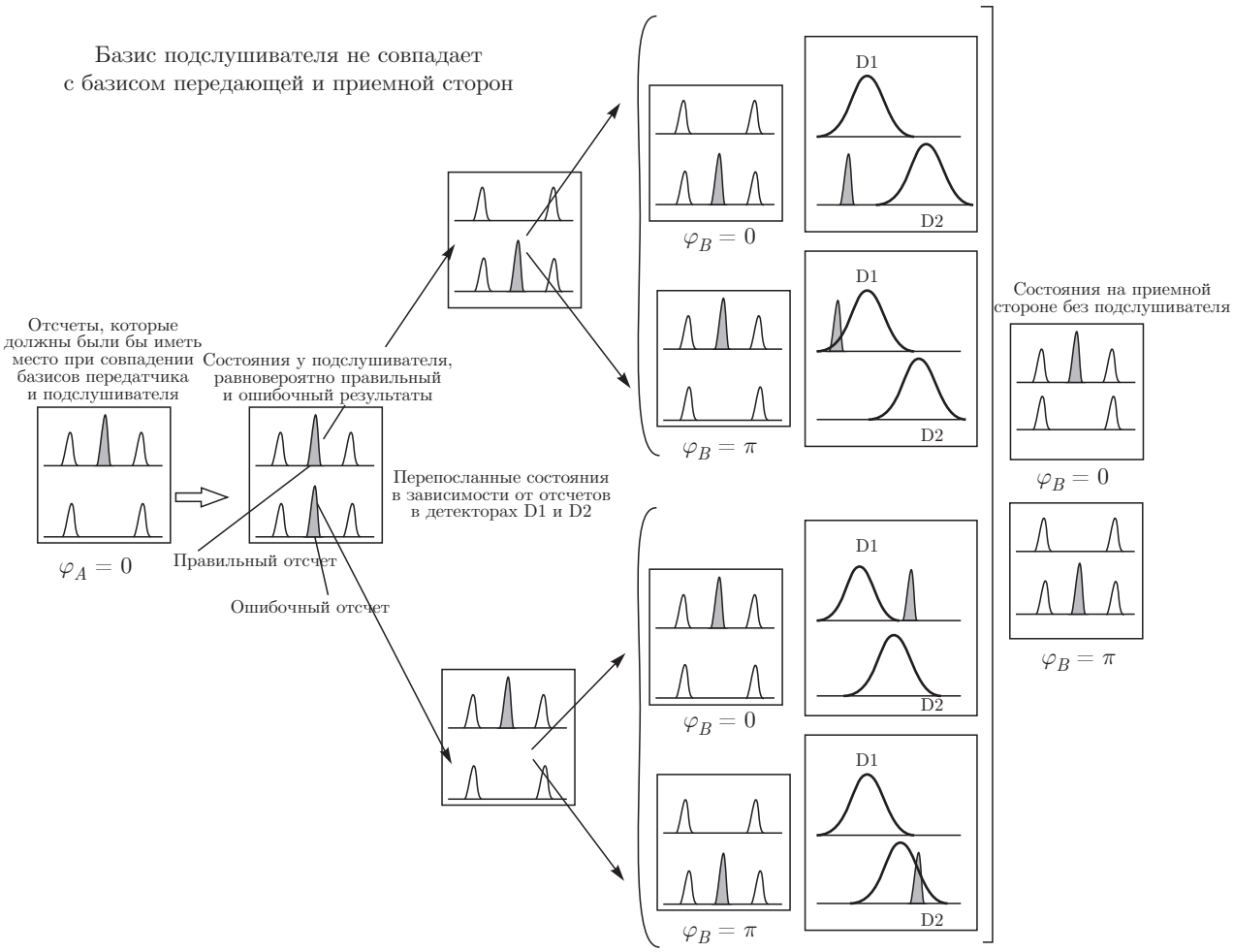

Рис. 6. Иллюстрация эволюции состояний и их детектирование на приемной стороне при атаке Detectors Mismatch в модифицированной версии протокола BB84 для случая, когда базис подслушивателя не совпадает с базисом легитимных пользователей

ватель перепосылает состояние в противоположном базисе 1^+, сдвинутое по времени так, чтобы не попадать в кривую по времени чувствительности детектора D2, т. е. блокирует отсчет в детекторе D2 (рис. 6). В этом случае перепосланное состояние не произведет ошибочный отсчет в детекторе D2 при условии, что принимающая сторона выбрала фазу 0 в базисе +. Однако, если принимающая сторона выбрала фазу π, то состояние 1^+ даст конструктивную интерференцию на детекторе D1 (рис. 6) и ошибочный отсчет на нем, поскольку при истинном состоянии 0^+ и выборе фазы π отсчета от истинного состояния 0^+ на детекторе D1 не должно быть. Должен быть отсчет только на детекторе D2 (рис. 6).

2. У подслушивателя возник ошибочный отсчет (рис. 6). Отсчет у подслушивателя в детекторе D2 (интерпретируется как логическая 1) — ошибочный результат (рис. 6). Результат — отсчет на детекторе D2 — интерпретируется как $1^\times$. В этом случае подслушиватель перепосылает состояние в противоположном базисе 0^+, сдвинутое по времени так, чтобы не попадать в кривую по времени чувствительности детектора D1, т. е. блокирует отсчет в детекторе D1 (рис. 6). В этом случае перепосланное состояние не произведет ошибочный отсчет в детекторе D1 при условии, что принимающая сторона выбрала фазу 0 в базисе +. Если принимающая сторона выбрала фазу π, то состояние 0^+ даст конструктивную интерференцию на детекторе D2 (рис. 6), как и должно быть, поскольку при истинном состоянии 0^+ и выборе фазы π отсчет от истинного состояния 0^+ должен быть на детекторе D2 (рис. 6).

Аналогичная ситуация имеет место, если передающей и принимающей сторонами выбран базис $\times$.

Таким образом, в предложенной модификации протокола BB84, когда принимающая сторона в каждом базисе измерений выбирает не одно значение фазы, как имело место в известных системах, а в каждом базисе случайно выбирает два значения фазы: фазу 0 или π в одном базисе и случайно фазу $\pi/2$ или $-\pi/2$ в другом базисе, подслушиватель при атаке Detector Mismatch неизбежно производит ошибки на приемной стороне и обнаруживается.

4. ОЦЕНКА ВЕРОЯТНОСТИ ОШИБКИ

Проведем оценку вероятности ошибки, которую будет производить подслушиватель при атаке Detectors Mismatch, если используется предложенный способ защиты от данной атаки.

Сделаем консервативные предположения в пользу подслушивателя. Пусть подслушиватель атакует каждую посылку квантовых состояний. Пусть подслушиватель может обеспечить перепосыл достаточно коротких по времени состояний, чтобы они точно не попадали в кривую чувствительности одного по времени соответствующего детектора, который не должен делать отсчет при регистрации перепосланных состояний.

В асимптотическом пределе длинных последовательностей, которым мы ограничимся, базис подслушивателя в половине посылок совпадает с базисом легитимных пользователей — вероятность совпадения базисов $\frac{1}{2}$. В этих посылках подслушиватель не производит ошибок. В половине посылок базис подслушивателя не совпадает с базисом легитимных пользователей – вероятность несовпадения базисов $\frac{1}{2}$.

Как следует из предыдущего анализа (см. также рис. 6), в половине этих посылок подслушиватель получит правильный отсчет — вероятность $\frac{1}{2} \cdot \frac{1}{2}$, а в половине ошибочный — вероятность $\frac{1}{2} \cdot \frac{1}{2}$. Далее, из половины посылок, где был правильный отсчет у подслушивателя, половина посылок попадет в ситуацию, когда была выбрана фаза $\varphi_B = 0$ (рис. 6), при этом отсчета не будет, а половина посылок попадет в ситуацию, когда была выбрана фаза $\varphi_B = \pi$ (рис. 6), и будут правильные отсчеты у легитимных пользователей. В итоге, при не совпадающих базисах подслушивателя и легитимных пользователей вероятность правильных отсчетов есть $\frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{2}$.

Далее, в половине посылок, где у подслушивателя был ошибочный отсчет (рис. 6), в половине посылок у легитимных пользователей отсчетов не будет ($\varphi_B = 0$, рис. 6), а в половине посылок ($\varphi_B = \pi$, рис. 6) будет ошибочный отсчет.

Окончательно вероятность правильных отсчетов (пока ненормированная) есть

$$\Pr_{OK} = \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{2}, \tag{6}$$

а вероятность ошибочных отсчетов (тоже пока ненормированная) —

$$\Pr_{Err} = \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{2}. \tag{7}$$

Соответственно вероятность ошибки на приемной стороне равна

$$Q = \frac{\Pr_{Err}}{\Pr_{Err} + \Pr_{OK}} = \frac{1}{6} \approx 16.7\,\%, \tag{8}$$

что превышает критическую ошибку 11 % протокола BB84 в однофотонном случае. Разумеется, данная оценка носит иллюстративный характер и приведена лишь для того, чтобы показать чувствительность предложенного метода к обнаружению атаки Detectors Mismatch.

5. ЗАКЛЮЧЕНИЕ

Предложен простой, физически и интуитивно понятный метод защиты от атаки Detectors Mismatch, который требует лишь минимальной модификации управляющей электроники и программного обеспечения систем квантовой криптографии, использующих распространенный протокол BB84. Иначе говоря, при такой простой модификации протокола атака Detectors Mismatch всегда обнаруживается — детектируется. Сжатие очищенного ключа в зависимости от наблюдаемого процента ошибок на приемной стороне приводит к «изъятию» информации, которую подслушиватель может получить при такой атаке.

Благодарности. Выражаем благодарность коллегам по Академии криптографии Российской Федерации, С. П. Кулику за предложение заняться данной важной темой, многочисленные полезные обсуждения и поддержку.

Финансирование. Работа поддержана Российским научным фондом (проект № 16-12-00015 (продолжение)).

ЛИТЕРАТУРА

1. C. H. Bennett and G. Brassard, in *Proc. IEEE Int. Conf. on Comp., Sys. and Signal Process.*, pp. 175–179, Bangalore, India (1984).

2. W. K. Wooters and W. H. Zurek, Nature **299**, 802 (1982).

3. W. Heisenberg, Z. Phys. **43**, 172 (1927).

4. H. P. Robertson, Phys. Rev. **34**, 163 (1929).

5. D. Deutsch, Phys. Rev. Lett. **50**, 631 (1983).

6. H. Maassen and J. B. M. Uffink, Phys. Rev. Lett. **60**, 1103 (1988).

7. K. Kraus, Phys. Rev. D **35**, 3070 (1987).

8. M. Tomamichel and R. Renner, Phys. Rev. Lett. **106**, 110506 (2011).

9. C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, IEEE Trans. Inf. Theory **41**, 1915 (1995).

10. R. Renner, PhD Thesis, ETH Zürich (2005); arXiv: 0512258.

11. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

12. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).

13. A. Vakhitov, V. Makarov, and D. R. Hjelme, J. Mod. Opt. **48**, 2023 (2001).

14. N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Phys. Rev. A **73**, 022320 (2006).

15. N. Jain, E. Anisimova, I. Khan, V. Makarov, Ch. Marquardt, and G. Leuchs, *Talk presented at the Central European Workshop on Quantum Optics*, Brussels, June, 2327 (2014).

16. L. Lydersen, C. Wiechers, Ch. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nature Photonics **4**, 686 (2010); arXiv:1008.4593.

17. Z. L. Yuan, J. F. Dynes, and A. J. Shields, Nature Photonics **4**, 800 (2010).

18. V. Makarov, A. Anisimov, and J. Skaar, Phys. Rev. A **74**, 022313 (2006), arXiv:0511032.

19. V. Makarov and J. Skaar, Quant. Inf. Comp. **8**, 0622 (2008); arXiv:0702262.

20. K. A. Balygin, A. N. Klimov, I. B. Bobrov, K. S. Kravtsov, S. P. Kulik, and S. N. Molotkov, Laser Phys. Lett. **15**, 095203 (2018).

21. K. A. Balygin, A. N. Klimov, I. B. Bobrov, K. S. Kravtsov, S. P. Kulik, and S. N. Molotkov, Laser Phys. Lett. **16**, 019402 (2019).