ЖЭТФ, 2010, том 137, вып. 4, стр. 637–645

О ПАССИВНОМ ЗОНДИРОВАНИИ ВОЛОКОННО-ОПТИЧЕСКИХ ЛИНИЙ КВАНТОВОЙ СВЯЗИ

А. В. Корольков [a], ***К. Г. Катамадзе*** [b], ***С. П. Кулик*** [b*], ***С. Н. Молотков*** [a,c,d]

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

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

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

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

Поступила в редакцию 4 сентября 2009 г.

Лавинные фотодетекторы на основе InGaAs:P являются наиболее чувствительными и единственными на сегодняшний день детекторами, работающими в телекоммуникационном диапазоне длин волн 1.3–1.55 мкм в оптоволоконных системах квантовой криптографии, которые способны работать в режиме счета отдельных фотонов. В отличие от широко используемых кремниевых фотодетекторов в диапазоне длин волн до 1 мкм, работающих в ждущем режиме, данные детекторы всегда работают в режиме стробирования. При рождении электрон-дырочной пары при поглощении фотона, затем появлении лавины носителей возможен обратный процесс — рекомбинации и излучения фотонов. Такое обратное излучение может представлять потенциально серьезную проблему для стойкости волоконно-оптических систем квантовой криптографии при пассивном зондировании. Приводятся результаты исследования по регистрации обратного излучения. Приведена оценка для вероятности такого излучения.

1. ВВЕДЕНИЕ

За последнее десятилетие передача конфиденциальной информации[1)] при помощи квантовых состояний была доведена от достаточно абстрактных теоретических идей до конкретных технических решений и в ряде случаев до технологий [1–3]. Секретность ключей в квантовой криптографии основана не на технических или вычислительных ограничениях, а на фундаментальных запретах, диктуемых квантовой механикой. В квантовой криптографии считается, что контролируются только передающий и принимающий узел связи, а квантовый канал связи[2)], по которому передаются квантовые состояния, не контролируется и доступен для любых активных манипуляций и модификаций подслушивателем, вплоть до его замены другой более совершенной линией связи. Кроме того, подразумевается, что действия подслушивателя не ограничены никакими техническими возможностями, а лимитируются только фундаментальными законами квантовой механики, связанными с ограничениями на разли-

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

1) Более точно, квантовая криптография позволяет передавать секретные ключи, при помощи которых затем можно передавать конфиденциальную информацию.

2) Реально квантовый канал связи представляет собой обычное одномодовое волокно, по которому передаются квантовые однофотонные (или квазиоднофотонные) состояния. Если передается классический оптический сигнал, например, импульсы синхронизации, то та же самая линия связи работает как классический канал связи.

чимость неортогональных квантовых состояний[3]. Любое вторжение в линию связи с целью получить информацию о передаваемом квантовом состоянии приводит к его возмущению и появлению ошибок на приемной стороне. В реальных системах неидеальности приводят к ошибкам на приемной стороне даже в отсутствие подслушивателя. Для каждого протокола квантового распределения ключей существует критическая ошибка, до которой можно передавать ключи и гарантировать их секретность. Поскольку ошибки, возникающие от собственных шумов, и ошибки от подслушивателя принципиально неотличимы, все ошибки приходится списывать на действия подслушивателя. В оптоволоконных системах квантовой криптографии источник квантовых состояний не является строго однофотонным[4], линия связи не является идеальной и имеет потери, лавинные фотодетекторы имеют собственные темновые шумы и конечную квантовую эффективность ($< 100\,\%$). Длительные и детальные исследования показали [1–3], что даже в таких условиях, когда подслушиватель имеет доступ только к линии связи, квантовая криптография обеспечивает секретность передаваемых ключей, если длина линии связи не превышает некоторой критической величины. При этом подразумевается, что возможности аппаратуры легитимных пользователей ограничены сегодняшним технологическим уровнем, а подслушиватель не ограничен никакими техническими возможностями. Например, он может иметь еще не реализованную долговременную квантовую память, идеальные фотодетекторы без темновых шумов и со $100\,\%$-й квантовой эффективностью, может заменить существующую неидеальную квантовую линию связи на свою идеальную, делать неразрушающее измерение числа фотонов в канале связи[5]. Даже в таких неравных по техническому уровню условиях, когда подслушиватель не имеет доступа к передающей и принимающей станции, а имеет доступ только к линии связи, квантовая криптография обеспечивает секретность передаваемых ключей.

[3] С формальной точки зрения, секретность в квантовой криптографии базируется на простом математическом факте, что пара некоммутирующих наблюдаемых — эрмитовых операторов — не может иметь общей системы собственных векторов, что является фактически переформулировкой соотношений неопределенностей Гейзенберга.

[4] В качестве такого источника используется сильно ослабленное лазерное излучение, которое представляет собой когерентное состояние с пуассоновской статистикой по числу фотонов.

[5] Неразрушающие и невозмущающие (nondemolition) измерения со $100\,\%$-й эффективностью числа фотонов, но не их состояния, не запрещены в квантовой механике. Хотя такие измерения на сегодняшний день еще не реализованы экспериментально.

2. ВИДЫ АТАК НА ПЕРЕДАВАЕМЫЙ КЛЮЧ

Возможны два вида атак: активные и пассивные. При активных атаках подслушиватель либо модифицирует сами передаваемые квантовые состояния, либо активным образом посредством своего сигнала зондирует состояния передающего и принимающего узлов. При пассивных атаках подслушиватель не использует собственные зондирующие сигналы.

Прямой доступ к линии связи. Если подслушиватель имеет доступ только к линии квантовой связи, по которой передаются квантовые состояния, то для каждого протокола квантового распределения ключей имеется оптимальная для подслушивателя атака, связанная с модификацией квантовых состояний. Оптимальной такая атака считается в том смысле, что она дает максимум информации для подслушивателя при наблюдаемой на приемной стороне ошибке. Для реализации оптимальной в этом смысле атаки подслушивателю необходимо иметь квантовую память и уметь делать коллективные измерения над целой последовательностью квантовых состояний. В полной мере такая атака до сих пор экспериментально не реализована. Имеются лишь частичные результаты [4]. Данная атака относится к активному типу атак на передаваемый ключ, причем неизбежно происходит модификация и возмущение передаваемых квантовых состояний, которые детектируются на приемной стороне.

Косвенный доступ к приемной и передающей станциям. В реальных условиях сами передающая и приемная станции не являются полностью изолированными от внешнего мира. Напрямую они недоступны подслушивателю, но могут быть доступны косвенно через квантовый канал связи (оптоволокно). Возможны как активные, так и пассивные виды атак. Такие атаки не связаны с модификацией и измерением передаваемых квантовых состояний, тем самым, не приводят к ошибкам в информационной последовательности.

Один из видов активных атак связан с активным зондированием передающей аппаратуры. Приготовление квантовых состояний на передающей стороне, например, для систем квантовой криптографии, с наиболее часто применяемым фазовым методом кодирования [2] использует активный оптоволоконный элемент — фазовый модулятор (рис. 1). Поэтому, ес-

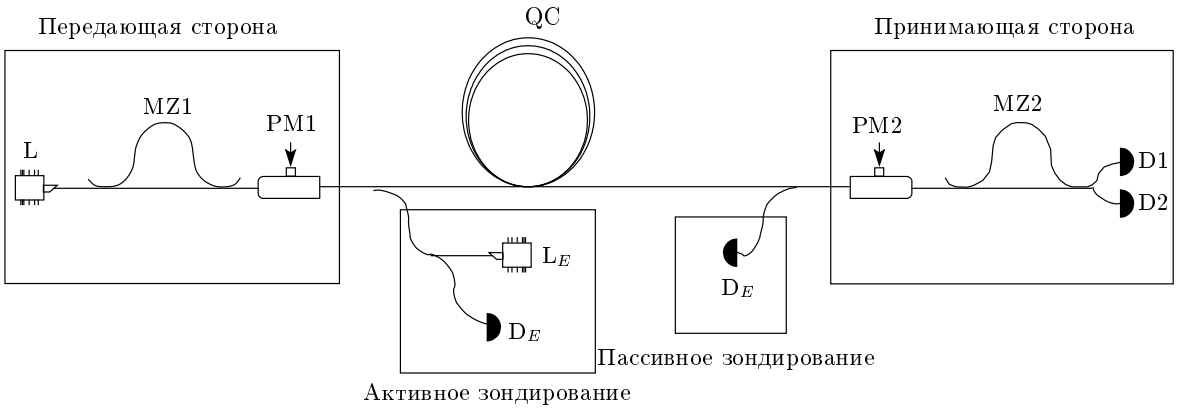

Рис. 1. Типичная схема оптоволоконной системы квантовой криптографии. MZ1 и MZ2 — разбалансированные интерферометры Маха – Цандера, PM1 и PM2 — фазовые модуляторы, L — лазер, D1, D2 — лавинные фотодетекторы, QC — квантовый канал связи, L_E и D_E — лазер и фотодетекторы подслушивателя

ли известно состояние фазового модулятора в каждой посылке, то фактически известно передаваемое квантовое состояние и соответствующий бит ключа. Фазовая модуляция осуществляется путем приложения напряжения на фазовый модулятор, который при этом изменяет оптическую длину, что приводит к появлению дополнительной разности фаз в суперпозиции квантовых состояний, локализованных в разных временны́х окнах (рис. 1). Изменение оптической длины фазового модулятора может быть обнаружено посредством измерения отраженного внешнего зондирующего излучения (рис. 1) так же, как это происходит в методе оптической рефлектометрии с временны́м или фазовым разрешением. Такое активное зондирование состояния передающего узла не приводит к возмущению передаваемых квантовых состояний и ошибкам на приемной стороне. Однако данная атака детектируется добавлением контрольного детектора на передающей стороне. Возможны также другие способы блокирования такой активной атаки.

Аналогичным способом возможно активное зондирование состояния фазового модулятора на приемной стороне. Такое зондирование, как несложно понять, при любой интенсивности зондирующего импульса (от однофотонного до многофотонного) уже будет приводить к ошибкам на приемной стороне, причем при любом уровне зондирующего сигнала. Это легко понять, поскольку при любой интенсивности зондирующего сигнала имеется вероятность его прохождения на лавинные детекторы и его регистрации. Поскольку зондирующий сигнал никак не связан с передающими состояниями, неизбежно возникнут ошибки в информационной последовательности[6)].

Одним из видов активного зондирования является техника «ослепления» (blinding) лавинных фотодетекторов [5]. Однако такое зондирование также легко обнаруживается с помощью контрольного классического детектора на принимающей стороне.

Кроме активных атак, когда используется внешний зондирующий оптический сигнал, возможно также пассивное зондирование. Именно такое пассивное зондирование будет рассмотрено ниже. Оно связано с регистрацией излучения от активных оптических элементов на приемной станции.

Во всех действующих оптоволоконных системах квантовой криптографии в качестве однофотонных детекторов в оптическом диапазоне длин волн 1.3–1.55 мкм в оптоволоконных системах квантовой криптографии используются лавинные детекторы, представляющие собой определенную мезагетероструктуру на основе InGaAs:P.

Важно отметить, что данный тип детекторов является пока единственным типом детекторов, приемлемых для оптоволоконных систем квантовой криптографии. Поэтому исследование пассивного зондирования — обратного излучения при регистрации фотонов — является крайне важным для криптографической стойкости оптоволоконных систем квантовой криптографии. Важно и необходимо иметь оценку верхней границы для вероятности обратно-

[6)] Возможны более изощренные ситуации, когда вид зондирующего излучения связан с частичной информацией, полученной о передаваемом квантовом состоянии. Здесь такие атаки не рассматриваются.

го излучения. Секретность ключей все равно будет обеспечена, лишь бы вероятность обратного излучения была меньше единицы (акт обратного излучения имеет место не при каждом акте регистрации фотона). Верхняя граница вероятности обратного излучения дает величину дополнительного сжатия ключей по сравнению с тем случаем, когда такое излучение отсутствует. Еще раз отметим, что секретность все равно обеспечивается при любой вероятности обратного излучения, меньшей единицы.

Поглощение фотона приводит к рождению электрон-дырочной пары, которая затем ускоряется внутри структуры за счет приложенного напряжения и порождает лавину носителей, приводящую к импульсу тока на выходе, который и регистрируется. Важно отметить, что детекторы в телекоммуникационном диапазоне длин волн 1.3–1.55 мкм, используемые в системах квантовой криптографии, для уменьшения темновых шумов работают в стробируемом режиме.

Возможен и обратный процесс переизлучения за счет рекомбинации носителей из лавины. Данное излучение может быть зарегистрировано за пределами принимающей станции через квантовый оптоволоконный канал связи. Поскольку в реальных системах квантовой криптографии используется пара лавинных фотодетекторов (рис. 1), излучение из них может слегка отличаться (например, по спектральному составу), и детектирование такого излучения даст некоторую информацию о передаваемом ключе.

Такая атака является пассивной, не приводит к ошибкам на приемной стороне и, вообще говоря, никакими средствами не может быть зарегистрирована, поэтому потенциально является крайне опасной.

Однофотонный лавинный детектор в телекоммуникационном диапазоне длин волн 1.3–1.55 мкм на сегодняшний день представляет собой уникальное и сложное устройство. Такое исследование пассивного зондирования квантовых линий связи является достаточно сложной и деликатной задачей и, насколько нам известно, до сих пор не проводилось[7)].

Известны лишь эксперименты по детектированию обратного свечения на Si-фотодетекторах в диапазоне 0.8 мкм. Такое свечение было обнаружено, причем использовалась специальная оптическая схема в «воздушном» (не оптоволоконном) варианте для сбора обратного излучения [8].

3. ПАССИВНОЕ ЗОНДИРОВАНИЕ ЛАВИННЫХ ДЕТЕКТОРОВ

В экспериментах были использованы однофотонные лавинные фотодетекторы собственной разработки [9] (рис. 2, 3). Схема эксперимента представлена на рис. 2; один детектор был ведущим, второй — ведомым. Детекторы были синхронизированы от общего внешнего генератора с частотой 1 МГц (конструктивно возможен также запуск импульса строба от внутреннего генератора). Длительность импульса строба была выбрана 5 нс (возможный диапазон длительностей строба 1.8–12 нс) с амплитудой до 7 В. Типичное напряжение пробоя для данных структур серии 547NT (фирмы JDSU) 62 В. Для отсечки паразитных электронных шумов используется дискриминация выходного сигнала с лавинного детектора, диапазон напряжений дискриминатора 0–400 мВ. Диапазон задержек импульса стробирования относительно импульса синхронизации составлял 0–12 нс. Оптические входы детекторов были соединены напрямую стандартным пэтчкордом волокна SMF-28 длиной 1.14 см. Для избежания паразитных засветок для ведомого фотодетектора лавинный фотодиод ведущего детектора засвечивался непосредственно через оплетку присоединенного (pigtailed) к детектору оптоволокна. Задержка выработки строба на ведомом детекторе относительно строба на ведущем была подобрана таким образом, чтобы фотон, испущенный в окне стробирования в ведущем детекторе, приходил на ведомый детектор точно в момент выработки строба[8)]. Кроме того, дополнительно для устранения паразитных засветок ведомого детектора он был затемнен. Оптическая изолированность ведомого детектора от засветки ве-

[7)] Активно ведется разработка сверхпроводящих детекторов на основе NbN [6]. У них есть ряд потенциальных преимуществ: нет афтерпалсинга (afterpulsing), более высокие рабочие частоты (рекорды до 40 ГГц). Однако стоит отметить, что на сегодняшний день с учетом новой схемотехники [7] лавинные фотодиоды «дотянулись» до частот регистрации сигнала в 10 ГГц (с активным подавлением афтерпалсинга), поэтому преимущество по частотам нивелировано, а удобство, в смысле того, что не требуются низкие температуры, осталось.

[8)] В отличие от экспериментов [8] на кремниевых фотодетекторах, которые работают не в стробируемом, а ждущем режиме, схема совпадения не требуется, поскольку все отсчеты обоих фотодетекторов привязаны к импульсам синхронизации. Поэтому для обнаружения дополнительного сигнала, связанного с регистрацией излучения от ведущего детектора, достаточно зарегистрировать изменение среднего числа отсчетов при засветке и без засветки ведущего детектора. Для экспериментов [8] с кремниевыми детекторами, работающими в ждущем режиме, для надежной привязки событий излучения-регистрации двумя детекторами требуется схема совпадения.

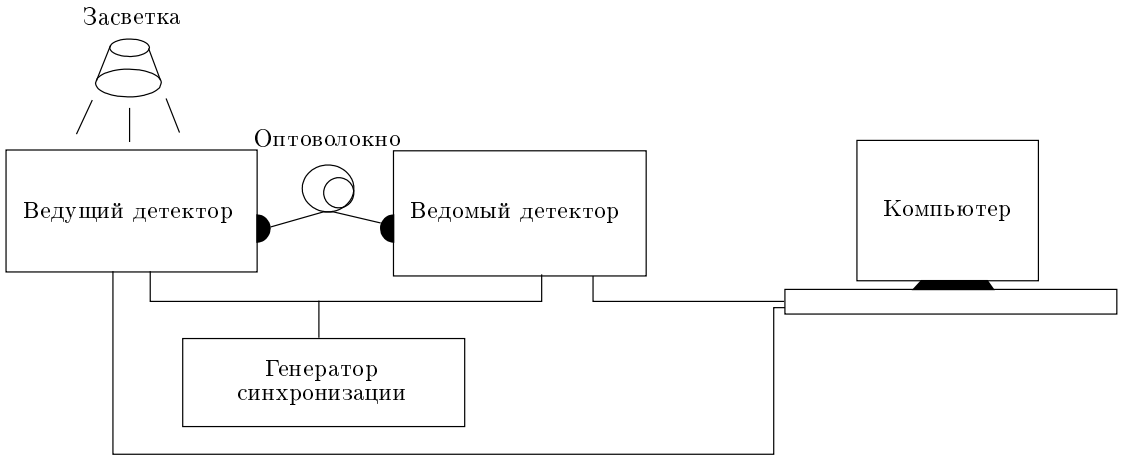

Рис. 2. Схема эксперимента

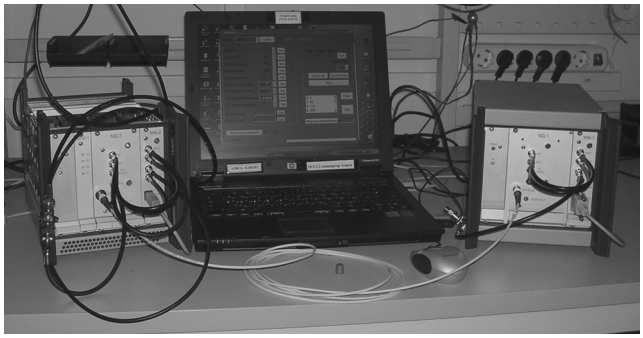

Рис. 3. Экспериментальная аппаратура для исследования пассивного зондирования

дущего проверялась при включенной и выключенной засветке ведущего детектора. Сам ведущий детектор при этом был выключен.

Было проведено несколько серий экспериментов с целью выяснения взаимного влияния всех возможных факторов.

4. ПАССИВНОЕ ЗОНДИРОВАНИЕ

4.1. Сканирование по задержке

Для ведущего детектора напряжение смещения было выбрано таким, чтобы при засветке обеспечить достаточно большое число фотоотсчетов, но при этом еще избежать ослепления детектора. Рабочие параметры детекторов приведены в табл. 1. Проводилось сканирование по задержке ведомого детектора. Время усреднения 1 с. Общее время измерения 17 мин. Программно выставлялись три значения задержки на ведомом детекторе каждые 13 с. Значение 6.5 нс отвечает условию полного согласования момента стробирования ведомого детектора и момента прихода излученных фотонов с ведущего детектора. Далее для краткости будем называть условием полного совпадения моментов наложения строба и момента возможного прихода фотона условием синхронизма. Два других значения задержки 2 нс и 13 нс соответствовали выводу из режима синхронизма.

В таблицах в скобках указано число отсчетов без засветки. Число темновых отсчетов ведущего детектора составляло $2 \cdot 10^{-4}$ отсч./строб при квантовой эффективности детекторов 20–25 %. Результаты представлены в табл. 2. Из табл. 2 видно, что максимум числа отсчетов наблюдается в условиях синхронизма, однако превышение находится в пределах статистической погрешности.

В следующей серии экспериментов также проводилось сканирование по задержке ведущего детектора. Параметры приведены в табл. 3. Скорость темновых отсчетов у ведущего детектора была понижена за счет уменьшения напряжения смещения до уровня $3 \cdot 10^{-5}$ отсч./строб.

Проводилось сканирование при двух значениях задержки: 6.5 нс, условие синхронизма, 11 нс, отсутствие синхронизма (рассогласование по задержкам), каждое по 500 с, общее время измерений 59 мин. Результаты измерений представлены в табл. 4, из которой видно, что максимум числа отсчетов наблюдается в условиях синхронизма, однако превышение находится в пределах статистической погрешности.

Таблица 1

Параметры	Ведущий детектор	Ведомый детектор
Длительность строба	5 нс	5 нс
Порог дискриминации	258 мВ	257 мВ
Напряжение смещения	55 В	53.9 В
Число отсчетов	530000 (10) $с^{-1}$	200 $с^{-1}$
Температура фотодиода	228 К	228 К

Таблица 2

Задержка ведущего детектора	Нет синхронизма, 2 нс	Синхронизм, 6.5 нс	Нет синхронизма, 13 нс
Среднее число отсчетов, $с^{-1}$	206.0059	207.0296	206.2870
Среднеквадратичное отклонение	0.96426	0.94652	0.95905

4.2. Сканирование по напряжению смещения ведущего детектора

Приведем также две серии экспериментов со сканированием по напряжению смещения ведущего детектора. При понижении напряжения смещения можно добиться полного «выключения» ведущего детектора — темновые отсчеты и отсчеты при засветке отсутствуют (детектор не активен). Напряжение отсечки было выбрано 49 В, в этом случае при стробировании детектора отсчеты отсутствуют, нет рождения лавины носителей при поглощении фотона и, соответственно, должно отсутствовать обратное свечение. Задержка на ведомом детекторе составляла 6.5 нс, т. е. детекторы находились в условиях синхронизма. Собственная скорость темновых отсчетов на ведомом детекторе составляла $1 \cdot 10^{-4}$ отсч./строб.

На рис. 4 приведены типичные данные числа отсчетов от времени. Измерения проводились с чередованием по 500 с с напряжением смещения 55 В (ведущий детектор активен) и 49 В (детектор не активен). Общее время измерений 33 мин. Из табл. 5 видно, что превышение находится в пределах погрешности.

Наконец, приведем результаты последней серии измерений. Было повышено напряжение смещения на ведомом детекторе для увеличения квантовой эффективности. Скорость темновых отсчетов при этом составила $2 \cdot 10^{-4}$ отсч./строб. Остальные параметры оставались такими же. Проводилось чередование

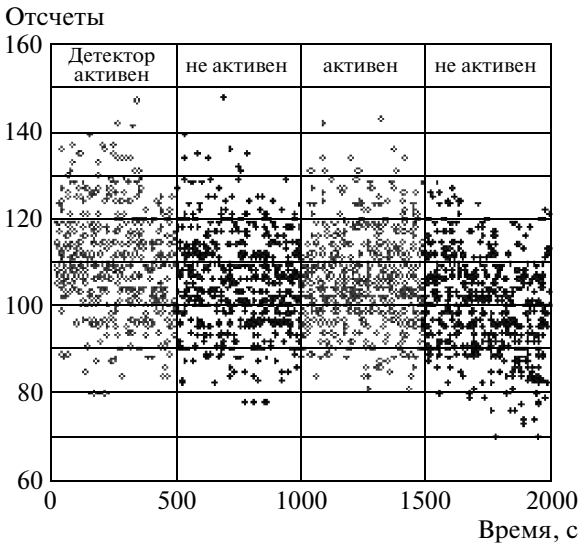

Рис. 4

включения и выключения ведущего детектора путем приложения напряжения смещения 55 В (активен) и 49 В (не активен) через 500 с. Средние значения за каждые 50 с приведены на рис. 5. Окончательные данные, усредненные по всей серии, приведены в табл. 6.

Из полученных данных можно оценить вероятность излучения фотона (P_{radiat}) при регистрации ведущим детектором за время строба. Разумеется,

Таблица 3

Параметры	Ведущий детектор	Ведомый детектор
Длительность строба	5 нс	5 нс
Порог дискриминации	258 мВ	257 мВ
Напряжение смещения	55 В	53 В
Число отсчетов	530000 (10) $с^{-1}$	30 $с^{-1}$
Температура фотодиода	228 К	228 К

Таблица 4

Задержка ведущего детектора	Синхронизм, 6.5 нс	Нет синхронизма, 11 нс
Среднее число отсчетов, $с^{-1}$	31.71657	30.1171
Среднеквадратичное отклонение	2.09737	1.57523

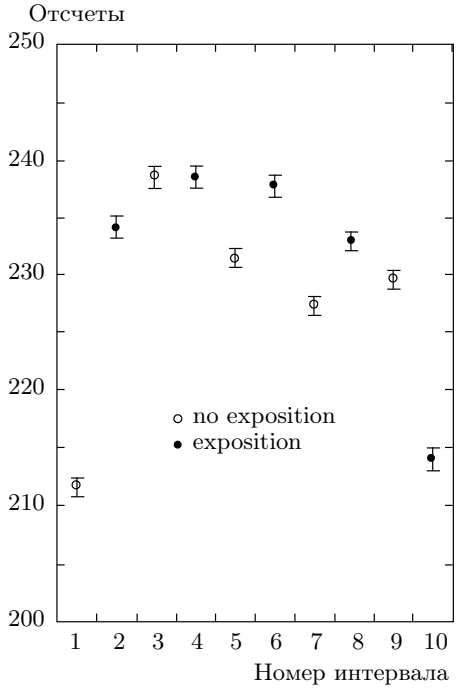

Рис. 5. Среднее число отсчетов за интервал 50 с; ○ — детектор не активен, • — активен

данная вероятность включает в себя не только вероятность испускания, но также и вероятность попадания в оптоволокно и вероятность прохождения фотона к ведомому детектору по оптоволокну:

$$P_{radiat} f \eta = N_{count}^{light} - N_{count}^{no\ light}. \qquad (1)$$

Здесь f — частота стробирующих импульсов (1 МГц), η — квантовая эффективность ведомого детектора, N_{count}^{light}, $N_{count}^{no\ light}$ — число отсчетов ведомого детектора при засветке и в отсутствие засветки ведущего. При типичной разнице $N_{count}^{light} - N_{count}^{no\ light} \approx 1$ (см. табл. 2, 4, 6) и $\eta \approx 25\,\%$ для вероятности обратного излучения получаем

$$P_{radiat} \approx \frac{1}{0.25 \cdot 10^6} = 4 \cdot 10^{-6} \frac{1}{\text{строб}}. \qquad (2)$$

Данная величина сравнима со скоростью собственных темновых отсчетов детектора при длительности строба 5 нс.

5. ОБСУЖДЕНИЕ РЕЗУЛЬТАТОВ

Таким образом, атака с пассивным зондированием, связанная с регистрацией подслушивателем обратного излучения, является единственной атакой, которая никаким образом не может быть обнаружена легитимными пользователями. Тем не менее, важно еще раз отметить, что такое пассивное зондирование не приводит к потере секретности передаваемых ключей.

Потенциально обратное излучение может приводить к получению дополнительной информации подслушивателя о передаваемом ключе. Причем получение этой дополнительной информации не приво-

Таблица 5

Напряжение смещения ведущего детектора	Активен, 54.5 В	Не активен, 49 В
Среднее число отсчетов, $с^{-1}$	132.5269	127.1517
Среднеквадратичное отклонение	0.5930	0.5930

Таблица 6

Напряжение смещения ведущего детектора	Активен, 55 В	Не активен, 49 В
Среднее число отсчетов, $с^{-1}$	231.483	227.683
Среднеквадратичное отклонение	4.4658	4.4256

дит к появлению ошибок на приемной стороне и не детектируется. Однако эта информация может быть «изъята» у подслушивателя путем дополнительного сжатия ключа на стадии усиления секретности (privacy amplification) [10] при помощи универсальных хэш-функций второго порядка [11]. Например, для протокола квантового распределения ключей BB84 [1] при наблюдаемой ошибке на приемной стороне Q длина секретного ключа, который может быть получен из последовательности длины n, составляет

$$\frac{r}{n} = 1 - 2h(Q) - P_{radiat}, \qquad (3)$$

где

$$h(Q) = -Q\log_2 Q - (1-Q)\log_2(1-Q)$$

— бинарная энтропийная функция. Даже при отсутствии подслушивателя ошибки за счет собственных неидеальностей системы (разбалансировка интерферометра, темновые шумы) дают в совокупности ошибку Q в несколько процентов. Поэтому дополнительное сжатие ключа на величину $P_{radiat}n$ представляет собой лишь ничтожно малую величину. Например, при длине последовательности 10^6 бит требуется дополнительное эффективное сжатие на несколько битов даже при условии, что подслушиватель будет регистрировать обратное излучение идеальными детекторами со 100 %-й квантовой эффективностью и без собственных темновых шумов.

Таким образом, в работе экспериментально рассмотрено влияние обратного излучения на секретность ключей в оптоволоконных системах квантовой криптографии. Найдена верхняя граница вероятности обратного излучения, которая определяет степень дополнительного сжатия ключей, чтобы гарантировать их секретность.

Выражаем благодарность Академии криптографии РФ за поддержку данной работы. Работа также выполнена при частичной финансовой поддержке РФФИ (грант № 08-02-00559).

ЛИТЕРАТУРА

1. C. H. Bennett and G. Brassard, Proc. IEEE Int. Conf. on Comput. Sys. and Sign. Proces., Bangalore, India (1984), p. 175.

2. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, arXiv:quant-ph/0101098; Rev. Mod. Phys. **74**, 145 (2002); D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten, arXiv:quant-ph/0903.3907.

3. R. Alleaume, J. Bouda, C. Branciard, T. Debuisschert, M. Dianati, N. Gisin, M. Godfrey, P. Grangier, T. Langer, A. Leverrier, N. Lutkenhaus, P. Painchault, M. Peev, A. Poppe, T. Pornin, J. Rarity, R. Renner, G. Ribordy, M. Riguidel, L. Salvail, A. Shields, H. Weinfurter, and A. Zeilinger, arXiv:quant-ph/0701168; R. Ursin, T. Jennewein, J. Kofler, J. M. Perdigues, L. Cacciapuoti, C. J. de Matos, M. Aspelmeyer, A. Valencia, T. Scheidl, A. Fedrizzi, A. Acin, C. Barbieri, G. Bianco, C. Brukner, J. Capmany, S. Cova, D. Giggenbach, W. Leeb, R. H. Hadfield, R. Laflamme, N. Lutkenhaus,

G. Milburn, M. Peev, T. Ralph, J. Rarity, R. Renner, E. Samain, N. Solomos, W. Tittel, J. P. Torres, M. Toyoshima, A. Ortigosa-Blanch, V. Pruneri, P. Villoresi, I. Walmsley, G. Weihs, H. Weinfurter, M. Zukowski, and A. Zeilinger, arXiv:quant-ph/0806.0945; W. Mauerer, W. Helwig, and C. Silberhorn, arXiv: quant-ph/0712.0517; V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus, and M. Peev, arXiv:quant-ph/0802.4155.

4. T. Kim, I. Stork, genannt Wersborg, F. N. C. Wong, and J. H. Shapiro, arXiv:quant-ph/0611235.

5. V. Makarov, arXiv:quant-ph/0707.3987.

6. Book of Abstracts, *Single-Photon Workshop 2007, Source, Detectors, Applications and Measurements Methods*, INRIM, Torino, Italy (2007).

7. Z. L. Yuan, A. R. Dixon, J. F. Dynes, A. W. Sharpe, and A. J. Shields, New J. Phys. **11**, 045019 (2009).

8. C. Kurtsifier, P. Zarda, S. Mayer, and H. Weinfürter, J. Mod. Opt. **48**, 2039 (2001).

9. С. Н. Молотков, С. П. Кулик, А. И. Климов, *Устройство для регистрации слабых оптических импульсов*, Патент РФ №2339919, приоритет от 15.06.2007.

10. C. H. Bennett, G. Brassard, C. Crépeau, and U. Maurer, *Generalized Privacy Amplification*, IEEE Trans. Inf. Theory **41**, 1915 (1995).

11. J. L. Carter and M. N. Wegman, J. Comp. Syst. Sci. **18**, 143 (1979).