Письма в ЖЭТФ, том 105, вып. 9, с. 570 – 576

Практическая квантовая криптография

К. А. Балыгин[a], *В. И. Зайцев*[a], *А. Н. Климов*[a,b], *А. И. Климов*[a], *С. П. Кулик*[a], *С. Н. Молотков*[c,d,e1)]

[a] *Физический факультет МГУ им. М.В. Ломоносова, 119991 Москва, Россия*

[b] *Институт общей физики им. А.М. Прохорова РАН, 119991 Москва, Россия*

[c] *Академия Криптографии Российской Федерации, 121522 Москва, Россия*

[d] *Институт физики твердого тела РАН, 142432 Черноголовка, Россия*

[e] *Факультет вычислительной математики и кибернетики МГУ им. М.В. Ломоносова, 119991 Москва, Россия*

Поступила в редакцию 27 марта 2017 г.

После переработки 4 апреля 2017 г.

Проведен комплекс экспериментов, в которых апробируется система квантовой криптографии на основе 4-базисного протокола с геометрически однородными состояниями. Представлены результаты по приготовлению, преобразованию и измерению квантовых состояний света, передаваемых по реальным оптоволоконным линиям связи в условиях неконтролируемых внешних воздействий на расстоянии 32 км. Показано, что выбранные алгоритмы обработки квантовой информации адекватны и являются основой практических устройств защищенных линий связи.[2)]

DOI: 10.7868/S0370274X17090119

Введение. Практически все современные системы передачи и обработки информации используют криптографические средства защиты информации. При обмене информацией между центрами обработки данных (ЦОД), объектами критической инфраструктуры и отдельными пользователями используется шифрование данных. Для защиты критической информации применяется симметричное шифрование, которое требует наличие секретных ключей у легитимных сторон обмена информацией. Поскольку шифрование на одном и том же ключе имеет ограничение по объему шифруемой информации, то при увеличении потока данных требуется все более частая смена ключей между удаленными сторонами обмена. На сегодняшний день смена ключей так или иначе связана с их физическим переносом и последующим хранением, что требует специальных мероприятий, где всегда присутствует человеческий фактор. Также это затратно экономически.

Квантовая криптография позволяет решить проблему распределения ключей, исключить человеческий фактор и обеспечить требуемую частоту смены ключей. Причем секретность распределяемых ключей гарантируется фундаментальными законами квантовой механики.

Конечной целью работ по квантовой криптографии является создание глобальной инфраструктуры распределения ключей, использующей как волоконные линии связи, так и открытое пространство, включая оптические соединения между низкоорбитальными спутниками. Работы по созданию такой инфраструктуры уже давно ведутся во всех технологически развитых странах как в лабораторных условиях, так и на реальных волоконных линиях связи, а также через открытое пространство. Упомянем некоторые из них: Европа [1], Китай [2], США [3], Япония [4], Англия [5]. В отличие от квантовых вычислений, где пока никаких заметных практических достижений не продемонстрировано, в квантовой криптографии уже существуют впечатляющие практические успехи.

На сегодняшний день значительный объем передачи данных происходит по волоконным линиям связи. Однако из-за технологических ограничений гарантировать секретность ключей, распределяемых в системах квантовой криптографии по волоконным линиям, можно только до определенной длины линии связи, которая определяется используемым протоколом квантовой криптографии и его технической реализацией. Говоря о реализации, выделим как неотъемлемую часть элементы инженерии квантовых состояний, которые представляют наиболее сложную часть системы квантового распределения ключей (КРК) – в силу крайней чувствитель-

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

[2)] Пресс-релизы: http://fpi.gov.ru/press/news/2016100602; http://www.phys.msu.ru/rus/news/archive/201610051173.

ности к воздействиям внешних факторов, неидеальностям аппаратуры и др.: 1) генерация квантовых состояний; 2) их преобразование согласно протоколу и последующая передача через оптоволоконную линию связи; 3) измерение квантовых состояний, также включающее предварительное преобразование. Если первый и третий элементы можно считать относительно хорошо проработанными и составляющими инструментарий квантовой оптики, то наиболее существенным – в контексте влияния внешних факторов – является второй элемент, который принципиально усложняется по сравнению с реализацией системы КРК в лабораторных условиях. Другой блок любой системы КРК – это те элементы, которые осуществляют контроль и мониторинг за работой компонентов системы в целом, включая протокол обмена по классическому (открытому) каналу связи. Здесь важное значение отводится реализации обратной связи, призванной обеспечивать функционирование системы в автоматическом режиме и подстраивать критические параметры для минимизации технических ошибок, которые связаны с неидеальностью аппаратуры, присутствуют в любой системе КРК и должны быть минимизированы на аппаратном уровне.

Все известные системы используют различные протоколы квантовой криптографии, а также имеющуюся инфраструктуру волоконных линий связи, или специально создаваемую для этих целей. Поскольку различные системы используют очень разнородные протоколы квантовой криптографии, были попытки упорядочить данный процесс и выработать единые требования по криптостойкости таких систем. Однако даже в рамках ЕС этот процесс, инициированный ETSI (European Telecommunications Standards Institute), был начат, но не завершен до сих пор [6]. Это связано не только с организационными вопросами, но и с большим разнообразием квантовых протоколов и рядом вопросов, связанных с криптостойкостью самих протоколов и их конкретных реализаций. Кроме того, требования по криптостойкости в разных странах различаются.

Реализация системы. Финальным продуктом любой системы КРК являются секретные ключи. Для реального применения их секретность должна быть строго доказана. Поскольку система квантовой криптографии является распределенным устройством, то кроме атак на передаваемые квантовые состояния по линии связи, возможны атаки активного зондирования по линии связи на приемную и передающую аппаратуры, к которым подслушиватель не имеет прямого доступа (например, могут считываться состояния фазовых модуляторов, что дает однозначную информацию о передаваемом состоянии).

Таким образом, секретность ключей достигается, как выбором квантового протокола, так и технической реализацией системы, т.е. протокол должен обеспечивать секретность ключей при атаках на квантовый канал связи – без прямого и косвенного доступа к передающей и приемной аппаратуре. С другой стороны, система квантовой криптографии должна обеспечивать защиту и от атак на аппаратуру через канал. Отметим, что многие известные системы уязвимы при атаках активного зондирования [7].

В данном сообщении представлены результаты экспериментов по КРК при помощи двухпроходной волоконной системы квантовой криптографии, защищенной в обоих смыслах. Практическая реализация, используемый протокол КРК, а также методы обработки сырых ключей и получение финальных ключей были описаны ранее (см. [8]). Система позволяет распределять ключи в сетевом варианте в конфигурации типа “звезда” с числом узлов до 32. Однако это количество может быть легко увеличено, так как оно определяется только числом выходов программно управляемого волоконного коммутатора. В системе также реализована защита от активного зондирования как сервера, так и клиента. Защита клиентской станции от подмены состояний более яркими состояниями была представлена в [8]. Данная система априори устойчива к атакам с ослеплением детектора [9], поскольку в ней используется только один однофотонный лавинный детектор [8], а атака с ослеплением эффективна только при использовании двух лавинных детекторов [9]. По этой же причине система устойчива к атаке detector mismatch [9], которая строится на различной квантовой эффективности двух лавинных детекторов на выходе приемного интерферометра Маха–Цандера. Подробное изложение реализации защиты от активного зондирования требует большего места и будет приведено отдельно. Ниже кратко приедем обоснование выбора протокола, используемого в системе.

Выбор протокола. На сегодняшний день все системы квантовой криптографии в качестве источника информационных состояний используют ослабленное до квазиоднофотонного уровня лазерное излучение. Если говорить только об атаках на квантовый канал связи, то оказывается, что в этих условиях многие используемые протоколы страдают недоказанностью. Проблемы возникают из-за совместного действия двух факторов: потерь в квантовом канале связи и не строгой однофотонности источника ин-

формационных состояний. Существующие протоколы BB84, SARG [10, 11] при использовании ослабленного лазерного излучения не могут гарантировать секретность ключей при длине линии связи больше некоторого критического размера, соответственно при потерях больше критических.

Информационные состояния ослабленного лазерного излучения – квазиоднофотонные когерентные состояния – являются линейно независимыми, что приводит к атаке с UM (USD) (Unambiguous Measurements или Unambiguous State Discrimination) измерениями [10], или PNS-атаке (Photon Number Splitting Attack) [10], которая является частным случаем UM-измерений. Поэтому любой используемый протокол должен быть устойчив по отношению к данной атаке. Протокол заведомо становится несекретным, если вероятность неуспеха (ошибки) при различении подслушивателем квантовых состояний $\Pr(?) = 1 - \Pr(\mathrm{OK})$ становится меньше вероятности потерь в линии связи $\Pr(\mathrm{Loss}) = 1 - \Pr(\mathrm{Trans})$.

Нами был выбран протокол на геометрически однородных состояниях с 4-мя базисами [8] по изложенным ниже причинам. Информационными состояниями являются геометрически однородные когерентные состояния $|\alpha_j\rangle$, которые получаются унитарным поворотом U^j, $U^N = I - |\alpha_j\rangle = U^j|\alpha\rangle$ (I – единичный оператор), где $\alpha_j = e^{i\frac{2\pi}{2\cdot N_{\mathrm{basis}}}j}\alpha$ ($j = 0, 1, ...2 \cdot N_{\mathrm{basis}} - 1$). В протоколе используются $N_{\mathrm{basis}} = 4$ базиса, в каждом из них имеется пара неортогональных состояний с $|\alpha_j\rangle$ и $|\alpha_{j+1}\rangle$, отвечающих 0 и 1. Для геометрически однородных состояний вероятность успеха $\Pr(\mathrm{OK}) = 1 - \Pr(?)$ при различении квантовых состояний при UM атаке имеет точное аналитическое выражение (см. [12])

$$\Pr(?) = 1 - N \min_r \left(\frac{1}{N} \sum_{j=0}^{N-1} e^{\mu(e^{i\frac{2\pi j}{N}}-1)} e^{-i\frac{2\pi jr}{N}} \right),$$

$$N = 2 \cdot N_{\mathrm{basis}} = 8.$$

При среднем числе фотонов в информационном когерентном состоянии $\mu = 0.4$ вероятность успеха при различении состояний $\Pr(\mathrm{OK}) = 1.76 \cdot 10^{-6}$, для BB84 данная вероятность существенно выше $\Pr(\mathrm{OK}) = 2.9 \cdot 10^{-2}$ (для протокола SARG [10, 11] вероятность имеет тот же масштаб). Потери в линии длиной 100 км для стандартного одномодового волокна $\Pr(\mathrm{Loss}) = 1 - 10^{-2} = 0.99$. Удобнее рассуждать в терминах вероятности прохождения через канал связи $\Pr(\mathrm{Trans}) = 10^{-2}$. Протокол перестает быть секретным, если $\Pr(\mathrm{OK}) > \Pr(\mathrm{Trans})$. Для протокола на геометрически однородных состояниях, чтобы протокол перестал быть секретным, вероятность прохождения через канал связи должна упасть до уровня $\Pr(\mathrm{Trans}) \approx \Pr(\mathrm{OK}) = 1.76 \cdot 10^{-6}$, что эквивалентно длине линии в 300 км. На таких длинах уже более существенны темновые шумы детектора. В силу этого был выбран данный протокол. Для величины $\Pr(\mathrm{OK})$ в этом протоколе имеется точное решение. Таким образом решается проблема не строго однофотонного источника и потерь в линии связи.

В других протоколах проблема UM (USD) и PNS измерений решается другим способом за счет распределенного кодирования. Однако распределенный характер квантовых состояний приводит к усложнению анализа секретности протокола, которое до сих пор не получено, и секретность протоколов остается в значительной степени вопросом веры. Для протокола DPS (Differential Phase Shift) [13] и COW (Coherent One Way) [14] из-за распределенного кодирования до сих пор нет внятного доказательства их секретности. Кроме того, доказательства секретности в строго однофотонном случае дают оценку критической ошибки $\approx 4.12\,\%$ [15], которая при использовании ослабленного лазерного излучения вряд ли будет больше. Протокол Decoy State [16] явно использует предположения о свойствах лавинных однофотонных детекторов, так как в протоколе требуется отличать состояния ослабленного лазерного излучения с разным средним числом фотонов, что неприемлемо, поскольку свойства детектора, например, квантовая эффективность, могут флуктуировать в процессе регистрации квантовых состояний, т.е. в формулу для длины секретного ключа напрямую входят квантовая эффективность однофотонных детекторов, что неприемлемо, поскольку квантовая эффективность флуктуирует со временем.

Результаты экспериментов. Основной целью экспериментов была проверка работы системы квантового распределения ключей полностью в автоматическом режиме без участия оператора. Это означает, что система должна работать в непрерывном, круглосуточном режиме и автоматически подстраивать, если необходимо, свои внутренние параметры под изменения внешней среды: в основном, речь идет об управлении вторым этапом эволюции квантовых состояний (см. раздел Введение).

Действительно, секретность распределяемых ключей гарантируется, если уровень ошибки и уровень потерь не превышают некоторого критического значения, которое зависит от используемого протокола и длины линии. Внутренними критическими параметрами системы являются уровень

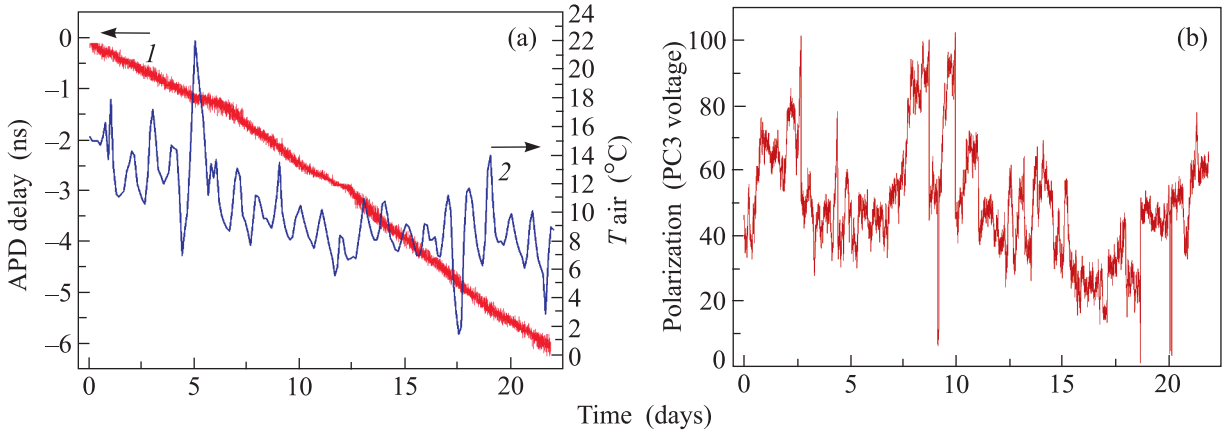

Рис. 1. (Цветной онайн) (a) – Зависимость изменения задержки строба лавинного фотодетектора (APD) от времени (кривая *1*), температуры внешней среды от времени (кривая *2*). (b) – Зависимость напряжения на одном из каналов управления контроллером поляризации, которое отражает изменение состояния поляризации состояний при прохождении через линию связи от времени

собственных темновых шумов лавинного однофотонного детектора и видность интерференционной картины. Внешними важными величинами являются потери в линии связи, изменение поляризации посылаемых состояний, показателя преломления и длины линии в зависимости от температуры и прочих внешних условий. Например, оптическая длина 10-километровой линии изменяется на ≈ 1 м при изменении температуры на 10 °C. Поскольку лавинный детектор работает в стробируемом (гейгеровском) режиме при длительности строба порядка 0.5 нс (соответствующий пространственный масштаб 10 см), то требуется непрерывная подстройка всех внутренних задержек в зависимости от актуальной длины линии, иначе система перестанет регистрировать (информационные) квантовые состояния и станет неработоспособной.

В данной реализации ключи генерируются в пакетном режиме. Перед посылкой каждой серии информационных состояний система проверяет все контрольные параметры: темновые шумы лавинного однофотоного детектора, видность интерференционной картины интерферометра Маха–Цандера, потери в канале, подстраивает задержки, поляризацию и т.д. По измеренным параметрам оценивается ожидаемая ошибка в первичных ключах и длина серии информационных состояний, которую необходимо послать, чтобы получить необходимую длину секретного ключа.

Эксперименты проводились в период сентября–октября 2016 г. на реальной линии ПАО "Ростелеком" между двумя городами в Московской области (Павловский Посад и Ногинск). Было выделено отдельное темное волокно в общем кабеле из 12 волокон. Остальные волокна использовали по прямому назначению – по ним передавалась телекоммуникационная информация. Длина линии составляла 32 км 51 м. Предварительно измеренный коэффициент потерь в линии составлял $\delta = 0.22$ дбит/км.

Эксперименты проводили на той линии и в течении того времени, на которое линия была предоставлена. В автоматическом непрерывном режиме без сбоев система работала в течении 22 дней. Далее приводятся зависимости критических параметров системы в зависимости от времени. На рис. 1a (кривая *1*) показана зависимость изменения задержки времени строба лавинного детектора, связанная с изменением длины линии связи от времени, а также изменение температуры окружающей среды от времени (кривая *2*); график взят по данным [https://rp5.ru/]. В этот период происходило постепенное похолодание, что привело к постоянному изменению длины линии связи. Изменение длины линии отслеживалось системой в автоматическом режиме. На рис. 1b приведено изменение состояния поляризации в канале связи, точнее напряжения на одном из каналов управления контроллером поляризации, отражающее изменение состояния поляризации, которое на входе клиента (выходе из линии) непрерывно компенсируется контроллером поляризации для достижения максимальной эффективности генерации ключей. Ключевыми параметрами, определяющими работу системы, в том числе наблюдаемую ошибку на приемной стороне и секретность ключей, являются видность интерференционной картины и уровень темновых шумов лавинного детектора. В системах бы-

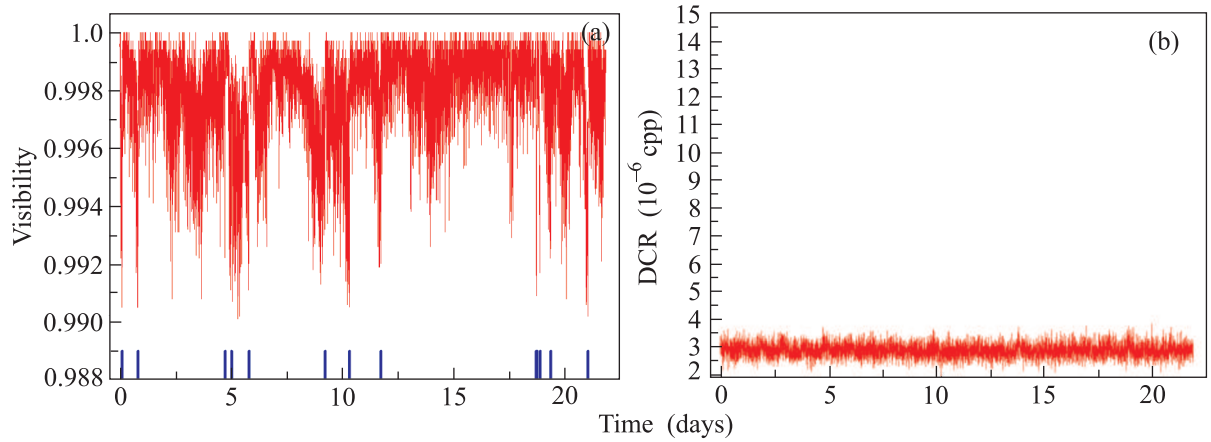

Рис. 2. (Цветной онлайн) (a) – Зависимость видности интерференционной картины (V) от времени. (b) – Зависимость вероятности темновых шумов на строб от времени (длительность строба $\tau = 670$ ps)

ла применена активная стабилизация интерферометра [8], которая позволяет достичь видности, близкой к идеальной. Система проверяет видность интерференционной картины перед каждой посылкой серии информационных состояний. Если видность оказывается меньше $V = 0.99$, то система автоматически производит подстройку интерферометра. Синими барами на рис. 2 показаны моменты времени, в которые система подстраивала интерферометр. Как видно из рис. 2a, такие события из-за хорошей термостабилизации интерферометра и двухпроходной реализации системы происходили в среднем один раз в несколько суток.

Другим критическим параметром являются темновые шумы однофотонного лавинного детектора. На рис. 2b приведены зависимости вероятности темновых шумов на строб от времени. Как видно из рис. 2b, система держит темновые шумы на постоянном уровне в течении всего времени проведения экспериментов. Известные перед посылкой каждой серии информационных состояний видность интерференционной картины, уровень темновых шумов и потери в линии связи позволяют довольно точно оценивать ожидаемую ошибку в первичных ключах, что требуется при последующей коррекции ошибок. Это дает возможность не раскрывать часть сырого ключа для оценки вероятности ошибки, которая затем отбрасывается. Такая процедура позволяет экономить сырой ключ. Величина утечки информации при коррекции ошибок устанавливается по фактически раскрытому числу бит при коррекции ошибок [8].

На рис. 3a показана измеренная эффективность – отношение числа зарегистрированных состояний к посланному для общего числа отсчетов (кривая *1*), числа отсчетов по сырым ключам – в совпадающих базисах (кривая *2*) и по секретным ключам (кривая *3*), как функции времени. На рис. 3b приведена зависимость вероятности ошибки в сырых ключах как функция времени. В системе длину секретного ключа вычислялись по протоколу [8].

Интересно сравнить ожидаемую эффективность (вероятность) по отсчетам с реально наблюдаемой. Вероятность отсчетов в совпадающих базисах есть

$$Eff = \frac{1}{4\cdot 2}(1 - e^{-\mu\eta \sin^2(\frac{\Delta\varphi}{2})T_{\rm ch}(L)T_{\rm sys}}) \approx$$
$$\approx \frac{1}{4\cdot 2}\mu\eta \sin^2\left(\frac{\Delta\varphi}{2}\right) T_{\rm ch}(L)T_{\rm sys}, \qquad (1)$$

где μ – среднее число фотонов, $\eta = 0.2$ – квантовая эффективность лавинного детектора, $T_{\rm ch}(L) = 10^{-\frac{\delta\cdot L}{10}} = 0.198$ – вероятность прохождения через линию связи, ($L = 32$ км – длина линии, $\delta = 0.22$ дбит/км – коэффициент потерь в данной линии), $T_{\rm sys} = \frac{1}{5.1}$ – вероятность прохождения через приемную сторону за счет внутренних потерь (потери при прохождении через систему защиты от активного зондирования, фазовый модулятор, светоделители и т.д.), коэффициент $1/4$ отвечает за то, что из полного числа посылок в совпадающих базисах будет только $1/4$ (4 – число базисов), коэффициент $1/2$ означает, что при одном детекторе из двух значений и уже при совпадающих базисах каждая из сторон, приемная и передающая, выбирает случайно из двух значений и независимо выставляет фазу на фазовом модуляторе, причем отсчет в детекторе на одном из выходов интерферометра Маха–Цандера будет только в случае, если фазы отличаются на $\Delta\varphi = \frac{\pi}{2}$, $\sin^2(\frac{\pi}{4}) = \frac{1}{2}$. В остальной половине случаев формально должен бы быть отсчет на детекторе на втором выходе интерферометра, который

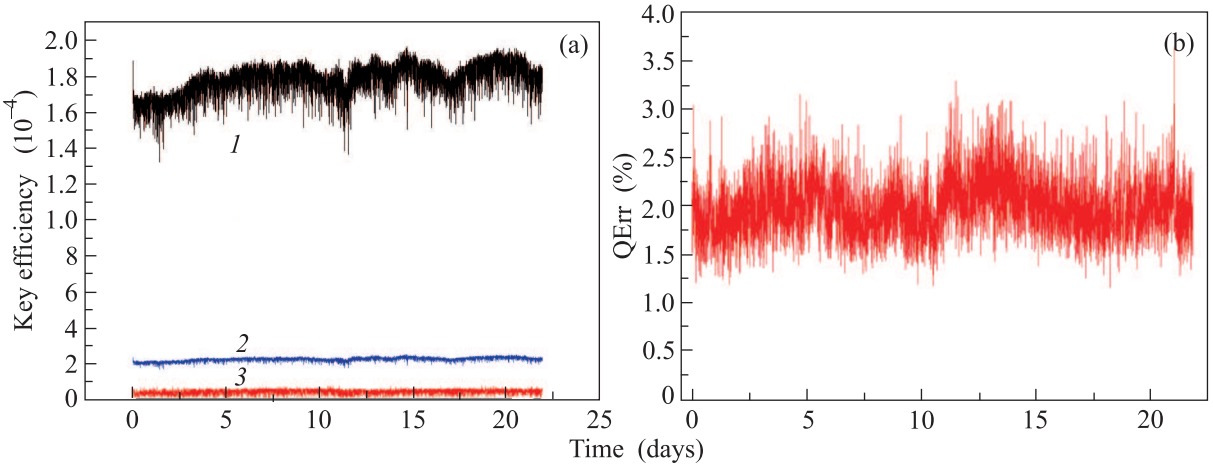

Рис. 3. (Цветной онлайн) (a) – Зависимости вероятности фотоотсчетов лавинного однофотонного детектора от времени: *1* – вероятность общего числа фотоотсчетов; *2* – вероятность отсчетов в совпадающих базисах. Данная последовательность является сырым (неочищенным) ключом – sifted key. Кривая *3* – вероятность отсчетов по секретному ключу – после исправления ошибок и усиления секретности (хэширования). Усредненное значение этой вероятности составляет $4.2 \cdot 10^{-5}$. (b) – Зависимость вероятности ошибки в сырых ключах от времени

отсутствует по причинам, упомянутым во Введении. В итоге вероятность отсчета в совпадающих базисах после разложения экспоненты в ряд равна

$$Eff = \frac{0.4 \cdot 0.2\frac{1}{2}0.198\frac{1}{5.1}}{4 \cdot 2} \approx 2 \cdot 10^{-4},$$

что прекрасно совпадает с измеренным значением (рис. 3a, кривая *2*).

Наконец, на рис. 4 показана зависимость длины секретного ключа как функция времени. Система перед посылкой каждой серии, после измерений контрольных параметров, описанных выше, определяла длину серии информационных состояний, необходимую для получения требуемого количества секретных ключей. Минимально требовалось, чтобы в результате передачи серии квантовых состояний возникал один секретный ключ длиной 256 бит – длина ключа для российских стандартов шифрования. Среднее число секретных бит составляло ≈ 1000 бит (≈ 4 ключа).

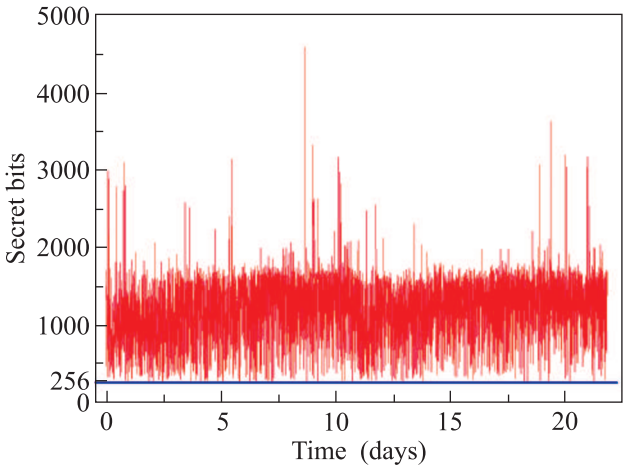

Рис. 4. (Цветной онлайн) Зависимость числа бит в секретном ключе как функции времени

Таким образом, показано, что физическая реализация 4-базисного протокола на геометрически однородных квантовых состояниях света является адекватной и может составить основу для построения практических систем квантового распределения ключей. Проведенные эксперименты системы КРК показали устойчивую работу в автоматическом непрерывном режиме – с подстройкой всех критических параметров на реальной оптоволоконной линии связи длиной 32 км в течении 22 суток без единого сбоя.

Авторы благодарят А.И. Исаева за неоценимую помощь в организации испытаний, А.В. Королькова за постоянный интерес и поддержку, главного архитектора по стратегии безопасности сетевых и облачных решений ПАО “Ростелеком” М.А. Меджлумова, ПАО “Ростелеком” за предоставленную возможность использовать волоконную линию. Авторы благодарят Фонд Перспективных Исследований за поддержку при разработке системы. Часть системы, связанная с защитой от активного зондирования, выполнена при поддержке РНФ (грант 16-12-00015).

1. A. Muller, H. Zbinden, and N. Gisin, Nature **378**, 449 (1995); D. Stucki, N. Gisin, O. Guinnard,

G. Ribordy, and H. Zbinden, New J. Phys. **4**, 411 (2002); P. Jouguest, S. Kunz-Jacques, T. Debuisschert, S. Fossier, E. Diamanti, R. Alleaume, R. Tualle-Brouri, P. Grangier, A. Leverrier, P. Pache, and P. Painchault, Opt. Express **20**, 14030 (2012); A. Ciurana, J. Martinez-Mateo, M. Peev, A. Poppe, N. Walenta, H. Zbinden, and V. Martin, Opt. Express **22**, 1576 (2014); A. Poppe, M. Peev, and O. Maurhart, Int. J. Quantum Inf. **6**, 209 (2008); M. Peev, C. Pacher, R. Alleaume et al. (Collaboration), New J. Phys. **11**, 075001 (2009); D. Stucki, M. Legre, F. Buntschu et al. (Collaboration), New J. Phys. **13**, 123001 (2011); D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten, New J. Phys. **11**, 075003 (2009); S. Nauerth, F. Moll, M. Rau, C. Fuchs, J. Horwath, S. Frick, and H. Weinfurter, Nature Photon. **7**, 382 (2013); B. Korzh1, C. C. W. Lim, R. Houlmann, N. Gisin1, M.J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, Nature Photon. **9**, 163 (2015).

2. X. F. Mo, B. Zhu, Z. F. Han, Y. Z. Gui, and G. C. Guo, Opt. Lett. **30**, 2632 (2005); L. J. Ma, H. Xu, and X. Tang, Proc. SPIE **6305**, 630513 (2006); T. Zhang, X. F. Mo, Z. F. Han, and G. C. Guo, Phys. Lett. A **372**, 3957 (2008); S. Wang, W. Chen, Z. Q. Yin et al. (Collaboration), Opt. Lett. **35**, 2454 (2010); W. Chen, Z. F. Han, T. Zhang, H. Wen, Z. Q. Yin, F. X. Xu, Q. L. Wu, Y. Liu, Y. Zhang, X. F. Mo, Y. Z. Gui, G. Wei, and G. C. Guo, IEEE Photonics Tech. Lett. **21**, 575 (2009); F. X. Xu, W. Chen, S. Wang, Z. Q. Yin, Y. Zhang, Y. Liu, Z. Zhou, Y. B. Zhao, H. W. Li, D. Liu, Z. F. Han, and G. C. Guo, Chinese Sci. Bull. **54**, 2991 (2009); T. Y. Chen, H. Liang, Y. Liu, W. Q. Cai, L. Ju, W. Y. Liu, J. Wang, H. Yin, K. Chen, Z. B. Chen, C. Z. Peng, and J. W. Pan, Opt. Express **17**, 6540 (2009); T. Y. Chen, J. Wang, H. Liang, Opt. Express **18**, 27217 (2010); S. Wang, W. Chen, J. F. Guo, Z. Q. Yin, H. W. Li, Z. Zhou, G. C. Guo, and Z. F. Han, Opt. Lett. **37**, 1008 (2012).
3. R. J. Hughes, G. L. Morgan, and C. G. Peterson, J. Mod. Opt. **47** 533 (2000); P. Toliver, R. J. Runser, T. E. Chapuran, J. L. Jackel, T. C. Banwell, M. S. Goodman, R. J. Hughes, C. G. Peterson, D. Derkacs, J. E. Nordholt, L. Mercer, S. McNown, A. Goldman, and J. Blake, IEEE Photon. Technol. Lett. **15**, 1669 (2003); C. Elliott, New J. Phys. **4**, 46.1 (2002); C. Elliott, *in Quantum Information and Computation III, Proc. SPIE* **5815**, 138 (2005); T. E. Chapuran, P. Toliver, N. A. Peters, J. Jackel, M. S. Goodman, R. J. Runser, S. R. McNown, N. Dallmann, R. J. Hughes, K. P. McCabe, J. E. Nordholt, C. G. Peterson, K. T. Tyagi, L. Mercer, and H. Dardy, New J. Phys. **11**, 105001 (2009).
4. M. Sasaki, M. Fujiwara, H. Ishizuka et al. (Collaboration), Opt. Express **19**, 10387 (2011); A. Tanaka, M. Fujiwara, K. Yoshino, S. Takahashi, Y. Nambu, A. Tomita, S. Miki, T. Yamashita, Z. Wang, M. Sasaki, and A. Tajima, IEEE J. Quantum Electron. **48**, 542 (2012).
5. P. D. Townsend, S. J. D. Phoenix, K. J. Blow, and S. M. Barnett, Electron Lett. **30**, 1875 (1994); J. F. Dynes, I. Choi, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, M. Fujiwara, M. Sasaki, and A. J. Shields, Opt. Express **20**, 16339 (2012); P. D. Townsend, Electron. Lett. **33**, 188 (1997); P. D. Townsend, Nature **385**, 47 (1997); Z. L. Yuan and A. J. Shields, Opt. Express **13**, 660 (2005); B. Fröhlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, Z. L. Yuan, and A. J. Shields, Nature **501**, 69 (2013); K. A. Patel, J. F. Dynes, I. Choi, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields, Phys. Rev. X **2**, 041010 (2012); K. A. Patel, J. F. Dynes, M. Lucamarini, I. Choi, A. W. Sharpe, Z. L. Yuan, R. V. Penty, and A. J. Shields, Appl. Phys. Lett. **104**, 051123 (2014).
6. T. Langer and G. Lenhart, New J. Phys. **11**, 055051 (2009); G. Lenhart, AIP Conference Proc. **1469**, 50 (2012).
7. S. Sajeed, I. Radchenko, S. Kaiser, J.-Ph. Bourgoin, A. Pappa, L. Monat, M. Legré, and V. Makarov, Phys. Rev. A **91**, 032326 (2015); arXiv:1412.8032 [quant-ph].
8. С. Н. Молотков, Письма в ЖЭТФ **101**, 637 (2015); К. А. Балыгин, А. Н. Климов, С. П. Кулик, С. Н. Молотков, Письма в ЖЭТФ **103**, 469 (2016); К. А. Балыгин, А. Н. Климов, С. П. Кулик, С. Н. Молотков, Письма в ЖЭТФ **104**, 349 (2016); К. А. Балыгин, А. Н. Климов, А. В. Корольков, С. П. Кулик, С. Н. Молотков, Письма в ЖЭТФ **103**, 883 (2016).
9. V. Makarov, A. Anisimov, and J. Skaar, Phys. Rev. A **74**, 022313 (2006); A. Vakhitov, V. Makarov, and D. R. Hjelme, J. Mod. Opt. **48**, 2023?2038 (2001); L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, arXiv:1009:2663 [quant-ph].
10. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
11. A. Acin, N. Gisin, and V. Scarani, Phys. Rev. A **69**, 012309 (2004); V. Scarani, A. Acin, G. Ribordy, and N. Gisin, Phys. Rev. Lett. **92**, 057901 (2004).
12. A. Chefles, arXiv/quant-ph: 9807022; A. Chefles and S. M. Barnett, arXiv/quant-ph: 9807023.
13. K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. Lett. **89**, 037902 (2002).
14. N. Gisin, G. Ribordy, H. Zbinden, D. Stucki, N. Brunner, and V. Scarani, arXiv:quant-ph/0411022; D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, Appl. Phys. Lett. **87**, 194108 (2005).
15. K. Wen, K. Tamaki, and Y. Yamamoto, arXiv:0806.2684.
16. W. Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003); X. B. Wang, Phys. Rev. Lett. **94**, 230503 (2005); H. K. Lo, X. F. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).