Письма в ЖЭТФ, том 106, вып. 2, с. 108 – 114 

# Управление распределенной интерференцией в однопроходной системе квантовой криптографии

*К. А. Балыгин*[a], *А. Н. Климов*[a,b], *С. П. Кулик*[a 1)], *С. Н. Молотков*[c,d,e 1)]

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

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

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

[d] *Академия Криптографии Российской Федерации, 121552 Москва, Россия*

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

Поступила в редакцию 26 мая 2017 г.
После переработки 19 июня 2017 г.

Продемонстрировано управление интерференцией в двух разнесенных волоконных интерферометрах Маха–Цандера и поддержание видности на уровне, близком к идеальному, в однопроходной системе квантовой криптографии непосредственно в процессе распределения ключей при длине линии в 50 км. Показано, что отклонение видности от идеальной однозначно связано с регистрируемой разностью числа нулей и единиц в сыром (просеянном) ключе. Это позволяет осуществлять балансировку интерферометра только в квазиоднофотонном режиме без прерывания передачи ключей, используя разность числа нулей и единиц в сыром ключе, как сигнал ошибки. Предложенный подход сокращает время балансировки и, кроме того, не требует дополнительных обменов по открытому каналу связи.

DOI: 10.7868/S0370274X17140107

**Введение.** Условно все способы распределения ключей можно разделить на два класса. В первом – секретность распределяемых ключей обеспечивается техническими средствами защиты контейнера с ключами, фактически, в том или ином виде, доставкой ключей курьерами. При этом сам физический носитель ключевой информации не важен. Такой способ распределения ключей не является безусловно секретным, так как секретность обеспечивается техническими мероприятиями, а не фундаментальными законами природы [1, 2].

Вторым классом является квантовое распределение ключей (КРК), в котором секретность получаемых ключей базируется на фундаментальных законах квантовой механики. Носителем ключевой информации является квантовое состояние, которое передается по открытым и доступным для прослушивания каналам связи (оптоволоконным линиям или через открытое пространство). Квантовая природа носителя ключевой информации оказывается принципиально важной и при соблюдении определенных условий обеспечивает секретность ключей. Квантовая механика запрещает с достоверностью копировать неизвестное квантовое состояние, а также гарантирует, что любые измерения неортогональных квантовых состояний будут приводить к их возмущению. Возмущение квантовых состояний неизбежно приводит к ошибкам на приемной стороне и обнаруживается. Законы квантовой механики позволяют установить фундаментальную верхнюю границу утечки информации к подслушивателю по наблюдаемой ошибке на приемной стороне. Если наблюдаемая ошибка (соответственно, утечка информации к подслушивателю) на приемной стороне меньше некоторого критического значения, то можно извлечь ключ и гарантировать его секретность [1, 2].

Ошибки могут возникать и от неидеальностей системы. Поскольку ошибки от подслушивания и собственные шумы неотличимы, то все наблюдаемые ошибки приходится списывать на подслушивателя. *Поэтому главная практическая задача квантовой криптографии – обеспечить стабильную работу распределенной системы с параметрами, предписываемыми квантовым протоколом, и с минимальными собственными шумами, приводящими к ошибкам.* В волоконных системах квантовой криптографии используются как фазовое кодирование – биты ключа кодируются в относительную фазу двух когерентных разделенных во времени квазиоднофотонных состо-

1) e-mail: sergei.molotkov@gmail.com, sergei.kulik@physics.msu.ru

яний, так и кодирование битов ключа в состояние поляризации [1, 2]. Оптическое волокно не сохраняет состояние поляризации, поэтому при прохождении через канал связи поляризация неконтролируемым способом изменяется. Хотя эти изменения достаточно медленные, все равно необходима активная стабилизация. Попытки реализовать такие системы были, но не получили дальнейшего развития по ряду технических причин [3].

Волоконные системы с фазовым кодированием можно разделить на два класса: двухпроходные и однопроходные [1]. В тех и других системах при детектировании квантовых состояний использован интерферометр Маха–Цандера (МЦ), на котором "сбивается" пара пространственно разнесенных квазиоднофотонных когерентных состояний с различной относительной фазой.

В двухпроходных схемах приготовление пары состояний и их "сбивка" происходит на одном и том же интерферометре МЦ, поэтому видность интерференционной картины обладает стабильностью. *Однако основной недостаток таких схем связан с их большей уязвимостью по отношению к атакам с активным зондированием и подменой состояний более яркими (см., например, [4]), что требует дополнительных мер защиты [5].*

В однопроходных схемах используется пара разнесенных независимых интерферометров МЦ на передающей и приемной сторонах и видность интерференционной картины зависит от относительной разности хода в двух интерферометрах. Это приводит к гораздо большей нестабильности интерференции, чем в двухпроходной системе.

**Различные способы взаимной балансировки интерферометров Маха–Цандера.** Покажем необходимость балансировки интерферометра. Оценим масштабы величин. На стабильность интерференции влияет изменение длины волны лазера, температура интерферометра, механические вибрации и проч. Даже аккуратная термостабилизация интерферометра не позволяет держать постоянной температуру волоконного интерферометра в течении длительного времени. Температурное изменение оптической длины волокна связано с двумя механизмами: первый связан с изменением непосредственно длины волокна за счет изменения температуры; второй – с изменением показателя преломления за счет температурного изгиба и кручения. Коэффициент теплового расширения волокна $\delta_L \approx 10^{-6}\frac{1}{^\circ\mathrm{C}}$. Коэффициент температурного изменения показателя преломления $\delta_R \approx 10^{-5}\frac{1}{^\circ\mathrm{C}}$. Оценим изменение температуры, приводящее к уменьшению видности и ошибкам в ключах. Рабочая длина волны лазера $\lambda = 1.55\cdot 10^{-4}$ см. Разность длин плеч интерферометра $\Delta L \approx 10^2$ см. Пусть $\Delta T$ изменение температуры, которое приводит к изменению разности хода в верхнем и нижнем плече на один процент от длины волны, при этом возникающая в ключах ошибка $Q \approx 1\,\%$. Такая ошибка достигается при изменении температуры на

$$
\begin{gathered}
(\Delta T)_L = \frac{1\,\%\lambda}{\delta_L \Delta L} \approx 0.01\,^\circ\mathrm{C}, \\
(\Delta T)_R = \frac{1\,\%\lambda}{\delta_R \Delta L} \approx 0.001\,^\circ\mathrm{C}.
\end{gathered}
\tag{1}
$$

Наиболее существенна ошибка от изменения показателя преломления, связанная с изгибом и кручением. Изменение разности температур интерферометров на $0.001^\circ$ уже приводит к ошибке в $1\,\%$. При хорошей пассивной термостабилизации такое изменение происходит за несколько секунд, поэтому требуется постоянная стабилизация видности по ходу генерации ключей.

*Отметим, что любые способы балансировки предполагают прерывание передачи ключей в режиме квазиоднофотонных состояний, перевод системы в классический режим (путем увеличения мощности лазера, см. например, [6, 7]) и посылки одинаковых состояний для того, чтобы сбалансировать интерферометр. Классические состояния выбираются так, чтобы сигнал интерференции давал максимальную (или минимальную) видность при регистрации. Наше наблюдение состоит в том, что отклонение видности от идеальной однозначно связано с регистрируемой разностью числа нулей и единиц в сыром (просеянном) ключе, т.е. в совпадающих базисах. Поэтому можно осуществлять балансировку только в квазиоднофотонном режиме, используя разность числа нулей и единиц в сыром ключе, как сигнал ошибки. Это сокращает время балансировки и, кроме того, не требует дополнительного обмена по открытому каналу связи.*

Возможны несколько способов компенсации относительной разности хода в интерферометре: (i) компенсация разности фаз изменением длины волны лазерного излучения на передающей станции, (ii) механическим изменением физической длины одного из плеч интерферометра на приемной станции, (iii) изменением фазы фазовым модулятором на приемной станции.

Изменение длины волны лазера приводит к изменению фазы при одной и той же разности хода, что позволяет добиться высокой видности. Регулировка длины волны лазера обычно происходит за счет изменения тока накачки или температуры лазера. Такой способ использован, например, в работе [6]. Поскольку измерения происходят на приемной стороне, а изменение длины волны лазера на передающей стороне, то данный способ требует обмена по открытому каналу связи, что неудобно и расточительно по времени.

Второй способ не требует большого числа обменов по открытому каналу связи, но имеет ряд технических недостатков, связанных с механическим изменением длины одного из плеч интерферометра. Кроме того, у пьезоэлемента присутствует, хоть и незначительный, гистерезис и время релаксации к равновесному положению при изменении напряжения.

Третий способ наиболее удобен и не обладает недостатками двух предыдущих, и сводится к наложению базового смещения фазы для компенсации разности длин плеч интерферометра.

**Преобразование состояний. Основная идея балансировки.** Для дальнейшего нам понадобятся выражения вероятности отсчетов для когерентных квазиоднофотонных состояний в зависимости от относительной фазы состояний и относительной разности хода в интерферометрах. Рассмотрим преобразование состояний через оптический тракт в однопроходной системе (рис. 1). Состояния на входе в канал связи после последовательного преобразования когерентных состояний через передающий оптический тракт (Alice) – интерферометр МЦ, фазовый модулятор, аттенюатор, могут быть представлены в виде

$$|\alpha\rangle \to |\alpha\rangle_1 \otimes |e^{i\Delta L_A}\alpha\rangle_2 \to |e^{i\varphi_A}\alpha\rangle_1 \otimes |e^{i\Delta L_A}\alpha\rangle_2. \quad (2)$$

Индексы 1 и 2 отвечают пространственно разделенным состояниям после прохождения интерферометра. Поскольку весь тракт выполнен из PM-волокон, состояние поляризации сохраняется, следовательно, индекс поляризации в когерентных состояниях всюду ниже, его для краткости опускаем. Преобразование на интерферометре МЦ на приемной станции (Bob) имеет вид (см. рис. 1)

$$\begin{pmatrix} |e^{i(\varphi_A-\varphi_B)}\frac{\alpha}{\sqrt{2}}\rangle_1 \otimes |e^{i\Delta L_A}\frac{\alpha}{\sqrt{2}}\rangle_2 \\ \\ |-e^{i(\varphi_A-\varphi_B)}\frac{\alpha}{\sqrt{2}}\rangle_1 \otimes |-e^{i\Delta L_A}\frac{\alpha}{\sqrt{2}}\rangle_2 \end{pmatrix}. \quad (3)$$

Состояния перед вторым светоделителем в верхнем и нижнем плечах интерферометра МЦ (см. рис. 1) равны

$$\begin{pmatrix} |vac\rangle_1 \otimes |e^{i(\varphi_A-\varphi_B)}\frac{\alpha}{\sqrt{2}}\rangle_2 \otimes |e^{i\Delta L_A}\frac{\alpha}{\sqrt{2}}\rangle_3 \\ \\ |-e^{i(\varphi_A-\varphi_B-\Delta L_B)}\frac{\alpha}{\sqrt{2}}\rangle_1 \otimes \\ \otimes|-e^{i(\Delta L_A-\Delta L_B)}\frac{\alpha}{\sqrt{2}}\rangle_2 \otimes |vac\rangle_3 \end{pmatrix}, \quad (4)$$

а состояния на выходе интерферометра МЦ приемной станции есть

$$\begin{pmatrix} |-e^{i(\varphi_A-\varphi_B-\Delta L_B)}\frac{\alpha}{2}\rangle_1 \otimes \\ \otimes|(e^{i(\varphi_A-\varphi_B)} + e^{-i\Delta L_{AB}})\frac{\alpha}{2}\rangle_2 \otimes |e^{i\Delta L_A}\frac{\alpha}{2}\rangle_3 \\ \\ |-e^{i(\varphi_A-\varphi_B-\Delta L_B)}\frac{\alpha}{2}\rangle_1 \otimes \\ \otimes|(e^{i(\varphi_A-\varphi_B)} - e^{-i\Delta L_{AB}})\frac{\alpha}{2}\rangle_2 \otimes |e^{i\Delta L_A}\frac{\alpha}{2}\rangle_3 \end{pmatrix}, \quad (5)$$

где $\Delta L_{AB} = -(\Delta L_A - \Delta L_B)$.

Детектирование информационных состояний однофотонным детектором (SPAD, на рис. 1) происходит в центральном временно́м окне (состояния с индексом 2). При малом среднем числе фотонов в информационном состоянии $\mu = |\alpha|^2$ вероятность детектирования пропорциональна $\eta|(e^{i(\varphi_A-\varphi_B)} - e^{-i\Delta L_{AB}})\frac{\alpha}{2}|^2$, $\eta$ – квантовая эффективность однофотонного детектора.

Нами использован протокол квантовой криптографии на геометрически однородных когерентных состояниях, который гарантирует доказуемую секретность ключей [8]. В протоколе используется 4 базиса, в каждом базисе пара неортогональных состояний с фазами 0 и $\frac{\pi}{2}$ – отвечают битам 0 и 1. В остальных 3-х базисах состояния получаются унитарным поворотом двух состояний на угол $\frac{\pi}{4}$ [8]. Далее приведена таблица кодирования для фаз на передающей и приемной сторонах в одном из базисов (табл. 1).

**Таблица 1**

| | $\varphi_A$ | $\varphi_B$ |
|---|---|---|
| 0 | 0 | $\frac{\pi}{2}$ |
| 1 | $\frac{\pi}{2}$ | 0 |

Если отличие от табличной разности фаз, вызванное разбалансировкой интерферометра, обозначить $x$, то вероятность правильной интерпретации битов 0 и 1 равна

$$\Pr(0_B|0_A) = \sin^2\left(\frac{\Delta\varphi_{AB}}{2} + x\right),$$
$$\Pr(1_B|1_A) = \sin^2\left(\frac{\Delta\varphi_{AB}}{2} - x\right), \quad (6)$$
$$\Delta\varphi_{AB} = \varphi_A - \varphi_B = \frac{\pi}{2}.$$

Вероятность ошибочной интерпретации из-за неточной балансировки интерферометров, когда был послан 0 – выбрана фаза $\varphi_B^1$, и наоборот, послан 1, а выбрана фаза $\varphi_B^0$, имеет вид

$$\Pr(1_B|0_A) = \sin^2(x), \quad \Pr(0_B|1_A) = \sin^2(x). \quad (7)$$

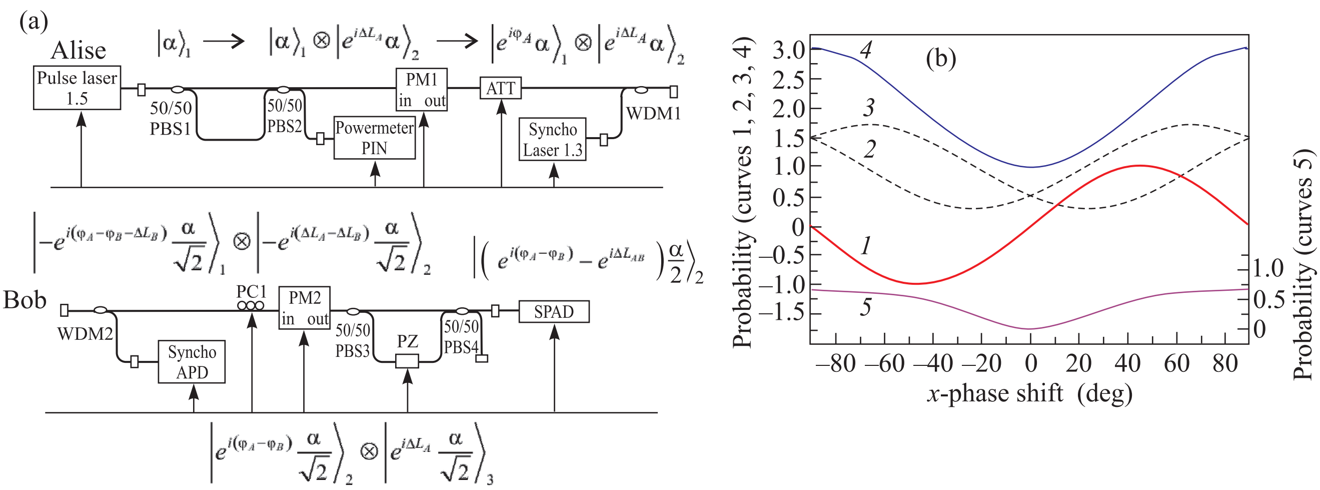


Рис. 1. (Цветной онлайн) (a) – Упрощенная функциональная схема передающей (Алиса) и приемной (Боб) частей системы. Интерферометры МЦ выполнены на поляризационно-сохраняющем волокне. Приняты следующие обозначения. Pulse Laser 1.5 – лазер с рабочей длиной волны 1.5 мкм для формирования одиночных импульсов с определенной тактовой частотой. PBS1, PBS2, PBS3, PBS4 – светоделители 50/50 на поляризационно-сохраняющих волокнах. MZ – интерферометры Маха–Цандера на поляризационно-сохраняющих волокнах. Powermeter PIN – детектор для контроля выходной мощности лазера. PM1, PM2 – фазовый модулятор для кодирования состояний. ATT – электронно-управляемый аттенюатор. WDM1, WDM2 – разделители по длинам волн 1.55/1.3 мкм (Wave Length Demultiplexor). Synchro Laser 1.3 – лазер с рабочей длиной волны 1.3 мкм для выработки синхроимпульсов. Synchro APD – классический телекоммуникационный лавинный детектор для выработки электрических импульсов синхронизации по оптическим импульсам на длине волны 1.3 мкм. PC1 – контроллер поляризации для выравнивания поляризации входных состояний из линии связи. PZ – электронно-управляемый пьезоэлемент для механического удлинения одного из плеч интерферометра МЦ. SPAD – однофотонный лавинный детектор для регистрации квазиоднофотонных информационных оптических импульсов. (b) – Вероятности (ненормированные), кроме кривой *5*. Кривые отвечают зависимостям: *1* – $\Delta(x)$, формула (8), разница нулей и единиц; *2* – формула (6), количество нулей; *3* – формула (6), количество единиц; *4* – $\Pr(0_B|0_A)+\Pr(0_B|1_A)+\Pr(1_B|1_A)+\Pr(1_B|0_A)$, полное количество бит в ключе; *5* – формула (9), вероятность ошибки в ключе

Итоговая вероятность (ненормированная, но это не важно) обнаружить разное количество 0 и 1 есть

$$\begin{gathered}\Delta(x) = \Pr(0_B|0_A) + \Pr(0_B|1_A) - \\ - \Pr(1_B|1_A) - \Pr(1_B|0_A) = \\ = \sin^2\left(\frac{\Delta\varphi_{AB}}{2}+x\right) - \sin^2\left(\frac{\Delta\varphi_{AB}}{2}-x\right) = \\ = \sin^2\left(\frac{\pi}{4}+x\right) - \sin^2\left(\frac{\pi}{4}-x\right), \quad x = \frac{\Delta L_{AB}}{2}. \qquad (8)\end{gathered}$$

Вероятность наблюдаемой ошибки в ключе на приемной стороне, вызванной разбалансировкой интерферометра

$$Q(x) = \frac{2\sin^2(x)}{2\sin^2(x)+\sin^2\left(\frac{\pi}{4}+x\right)+\sin^2\left(\frac{\pi}{4}-x\right)}. \qquad (9)$$

Зависимости, представленные формулами (6)–(9), показаны на рис. 1b. *Важно отметить, что в наблюдаемую ошибку $Q$, кроме вклада от неточности балансировки интерферометра, вносят вклад и другие факторы, например, темновые шумы и резкие изменения поляризации в канале связи, вызванные внешними причинами. В отсутствии упомянутых факторов ошибка $Q$ однозначно определяется видностью $Q = \frac{1-V}{2}$.*

*Таким образом, каждый раз после формирования сырого ключа, величина $\Delta(x)$, пропорциональная разности нулей и единиц в нем, может использоваться как сигнал ошибки для регулировки разности фаз одним из указанных выше методов. Важно, что для этого не требуется дополнительный обмен с передающей стороной.*

**Регулятор для балансировки интерферометра.** Поскольку видность интерференционной картины определяется только относительной разностью длин плеч интерферометров на передающей и приемной стороне, то достаточно регулировать только один из интерферометров. Так как измерения происходят на приемной стороне, то естественно там же осуществлять регулировку интерферометра. В работе [6] использована регулировка при помощи изменения длины волны лазера на передающей

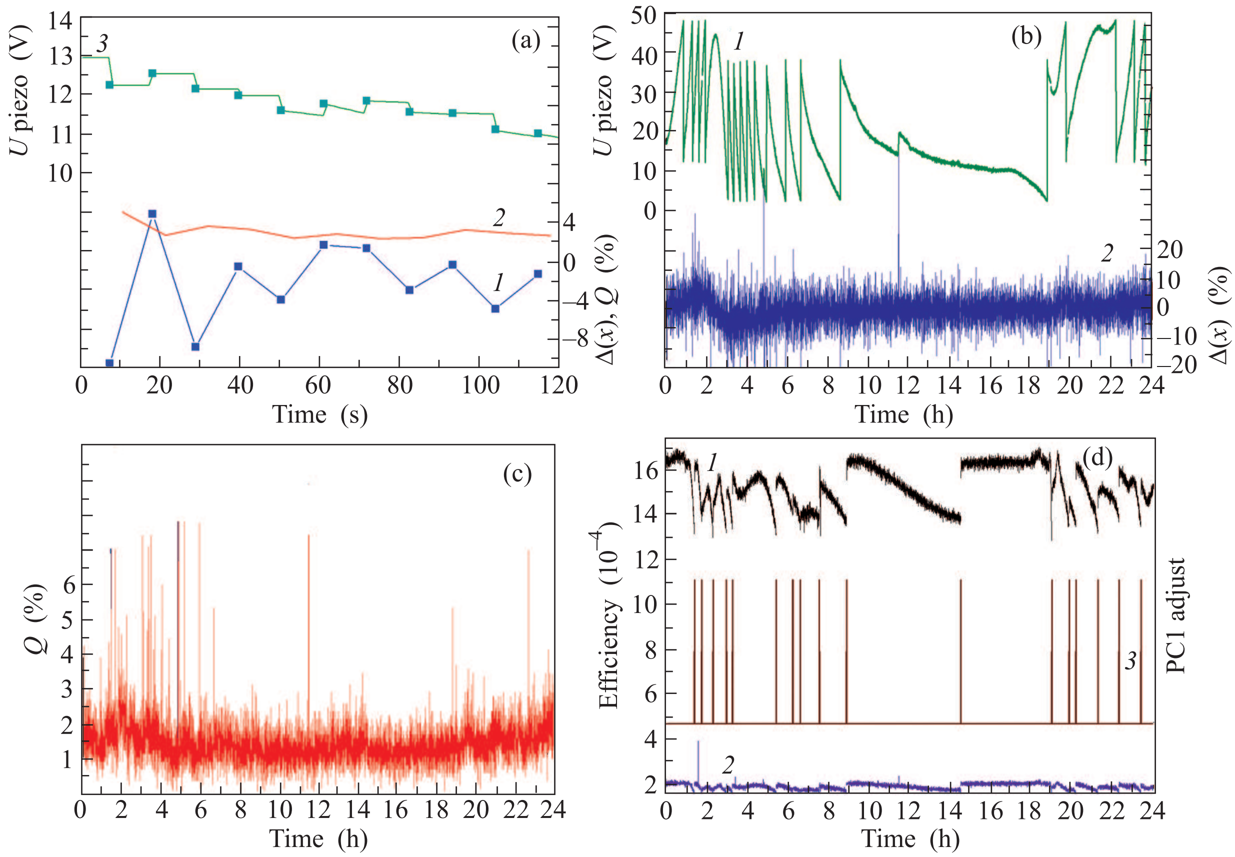


Рис. 2. (Цветной онлайн) Баланс интерферометра при помощи пьезоэлемента. (a) – Процесс регулировки. Кривая *1* – сигнал ошибки для ПИД-регулятора (разница 0 и 1 по отношению к полному числу зарегистрированных 0 и 1 ($\Delta(x)$) в сыром ключе. Кривая *2* – ошибка в сыром ключе. Кривая *3* – изменение напряжения на пьезоэлементе. Точками показаны значения, вычисленные ПИД-регулятором. Первые 50 с управление осуществлялось без учета скорости изменения фазы, затем – между моментами регулировки напряжение менялось с учетом усредненной скорости. (b) – Зависимости напряжения на пьезоэлементе (кривая *1*) и сигнала ошибки (кривая *2*) от времени при работе системы в течение суток. Изменение напряжения на пьезоэлементе на 36 В отвечает изменению фазы на $2\pi$. (c) – Зависимости ошибки $Q$ в сыром ключе от времени. (d) – Зависимости эффективности по всем отсчетам однофотонного детектора (кривая *1*) и по сырым ключам (кривая *2*) от времени. Эффективность определяли как отношение числа зарегистрированных состояний (всех или в совпадающих базисах) к числу посланных состояний. Среднее число фотонов на входе в линию связи $\mu = 0.4$. Вероятность темновых шумов однофотонного лавинного детектора собственной разработки составляла $p_d = 3 \cdot 10^{-6}$ отсчетов/строб, длительность строба $\tau = 630$ пс. На кривой *3* вертикальными линиями показаны моменты времени, в которых производилась автоматическая регулировка состояния поляризации на входе в приемную станцию для поддержания максимального прохождения через канал связи

стороне. Такой способ требует изменения уровня сигнала с квазиоднофотонного до классического, дополнительного времени на проведение измерений и большего числа обменов по открытому каналу связи, так как результат регулировки – видность, измеряется на одном конце линии, а параметр, управляющей этим – на другом (передающей стороне).

В нашем случае, одновременно с получением сырого ключа, получается сигнал ошибки (пропорциональный разности нулей и единиц в ключе), который используется ПИД (Пропорциональным Интегро-Дифференциальным) регулятором для управления пьезоэлементом PZ, либо фазовым модулятором PM2 (см. рис. 1a).

Как показали эксперименты, время разбалансировки интерферометров на величину, дающую чувствительный вклад в ошибку ключа, иногда оказывается сравнимым со временем его генерации. Это означает, что регулировка фазы должна производиться чаще, чем вырабатывается сигнал ошибки (сырой ключ). Для этого определялась усредненная за некоторое время скорость изменения фазы, и в промежутках между моментами регулирования фаза

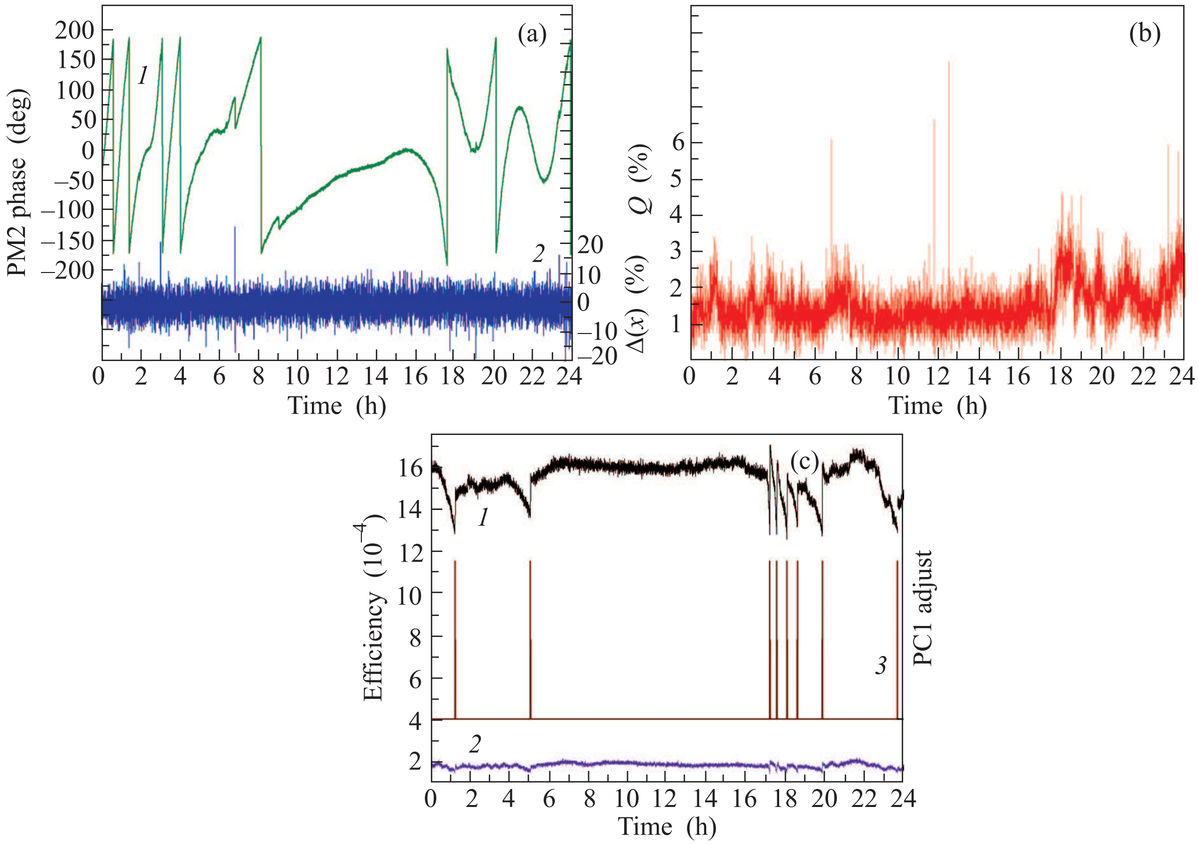


Рис. 3. (Цветной онлайн) Баланс интерферометра при помощи фазового модулятора. (a) – Зависимости фазового сдвига на фазовом модуляторе (кривая *1*) и сигнала ошибки для ПИД-регулятора (разница 0 и 1 по отношению к полному числу зарегистрированных 0 и 1 ($\Delta(x)$) в сыром ключе) (кривая *2*) от времени при работе системы в течение суток. (b) – Зависимости ошибки $Q$ в сыром ключе от времени. (c) – Зависимости эффективности по всем отсчетам однофотонного детектора (кривая *1*) и по сырым ключам (кривая 2) от времени. Эффективность определялась как отношение числа зарегистрированных состояний (всех или в совпадающих базисах) к числу посланных состояний. Среднее число фотонов на входе в линию связи $\mu = 0.4$. На кривой *3* вертикальными линиями показаны моменты времени, в которых проводилась автоматическая регулировка состояния поляризации на входе в приемную станцию для поддержания максимального прохождения через канал связи

изменялась с этой скоростью. На рис. 2a показана регулировка без и с учетом скорости изменения фазы. Учет скорости позволил поддерживать видность интерференции и уровень ошибок в ключах на уровне, близком к теоретическому, при изменении периода генерации ключа в широких пределах.

**Балансировка при помощи пьезоэлемента.** Передача ключей и соответственно измерения проходили в непрерывном автоматическом режиме в течении суток на длине линии 50 км. На рис. 2 приведены результаты экспериментальной реализации активной стабилизации интерферометра при помощи пьезоэлемента, встроенного в длинное плечо интерферометра на приемной стороне системы. На рис. 2a представлены зависимости от времени нормированной разности числа 0 и 1 с соответствующими регулировками ПИД-регулятором длины одного из плеч интерферометра. На рис. 2b показаны зависимости наблюдаемой ошибки $Q$ от времени, на рис. 2c – зависимости от времени эффективности по сырым ключам с отмеченными моментами автоматической подстройки входной поляризации на приемной станции для обеспечения максимальной эффективности передачи и регистрации квантовых состояний при изменениях состояния поляризации в линии. Отметим, что данные изменения являются довольно медленными.

**Балансировка при помощи фазового модулятора.** Компенсацию разности хода в (8) можно достигнуть дополнительным смещением фазы $\Delta\varphi_B$. Данное смещение не влияет на криптографические свойства, поскольку относительная разность фаз для различных состояний, кодирующих 0 и 1, не меняется ($\varphi_B^0 + \Delta\varphi_B - (\varphi_B^1 + \Delta\varphi_B) = \varphi_B^0 - \varphi_B^1$). На рис. 3a приведены зависимости относительной разности числа 0 и 1 как функции времени. На том же рисунке изображены зависимости регулирующих значений фазы $\Delta\varphi_B$. Отметим, что как следует из рис. 2d и рис. 3c в ночное время (на графиках интервал времени от 8 до 16) требуется менее частая подстройка поляризации в линии, чем в дневное время, что связано с температурой внешней среды.

**Заключение.** Таким образом, продемонстрирована активная стабилизация интерференционной картины в однопроходной системе квантовой криптографии, работающей в автоматическом режиме. Длина линии составляла 50 км. В отличии от других методов наш способ не требует прерывания генерации ключей, активная подстройка происходит непосредственно в процессе распределения ключей, и отсутствует необходимость увеличения числа обменов по открытому каналу связи. Приведены два метода активной стабилизации при помощи пьезоэлемента и фазового модулятора. Оба метода работают одинаково хорошо и устойчиво. При этом нет никаких сомнений, что система в режиме автоматической автоподстройки будет поддерживать рабочие параметры в течении сколь угодно продолжительного времени. Предложенный и реализованный метод позволяет отрабатывать все существенные изменения физических факторов, влияющих на интерференционную стабильность.

Выражаем благодарность коллегам из Академии Криптографии Российской Федерации за обсуждения и поддержку. К.А.Б., А.Н.К. и С.Н.М. благодарят РНФ (проект 16-12-00015) за поддержку работ по разработке управляющей электроники и протокола квантового распределения ключей. С.П.К. благодарен за финансовую поддержку работ по проекту Минобрнауки РФ (проект 03.625.31.0254), в рамках которого была разработана и протестирована система ПИД-регулятора.

1. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
2. V. Scarani, V. H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81** 1301 (2009).
3. G. B. Xavier, N. Walenta, G. Vilela de Faria1, G. P. Temporao, N. Gisin, H. Zbinden, and J. P. von der Weid, New. J. Phys. **11**, 045015 (2009).
4. S. Sajeed, I. Radchenko, S. Kaiser, J.-Ph. Bourgoin, A. Pappa, L. Monat, M. Legré, and V. Makarov, Phys. Rev. A **91**, 032326 (2015).
5. К. А. Балыгин, А. Н. Климов, А. В. Корольков, С. П. Кулик, С. Н. Молотков, Письма в ЖЭТФ **103**, 883 (2016).
6. D. Stucki, C. Barreiro, S. Fasel, J.-D. Gautier, O. Gay, N. Gisin, R. Thew, Y. Thoma, P. Trinkler, F. Vannel, and H. Zbinden, Opt. Expr. **17**, 13326 (2009).
7. D. Rosenberg, C. G. Peterson, J. W. Harrington1, P. R. Rice, N. Dallmann, K. T. Tyagi, K. P. McCabe, S. Nam, B. Baek, R. H. Hadfield, R. J. Hughes, and J. E. Nordholt, New J. Phys. **11** 045009 (2009).
8. С. Н. Молотков, Письма в ЖЭТФ **101**, 637 (2015).