Письма в ЖЭТФ, том 103, вып. 6, с. 469 – 474 © 2016 г. 25 марта

Активная стабилизация оптической части в волоконной квантовой криптографии

К. А. Балыгин[+], *А. Н. Климов*[+*], *С. П. Кулик*[+], *С. Н. Молотков*[×∘∇1)]

[+]*Физический факультет МГУ им. Ломоносова, 119991 Москва, Россия*

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

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

[∘]*Академия криптографии РФ, 121552 Москва, Россия*

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

Поступила в редакцию 8 февраля 2016 г.

Предложен и реализован метод активной стабилизации поляризации и других параметров оптической части двухпроходной волоконной системы квантовой криптографии. Метод позволил реализовать полностью автоматическое поддержание видности интерференции, близкой к идеальной ($V \geq 0.99$), и снизить вклад аппаратуры в ошибку в первичных ключах (QBER) до 0.5 %.

DOI: 10.7868/S0370274X16060114

1. Введение. Существующие волоконные системы квантовой криптографии используют фазовый принцип кодирования: информация о битах ключа кодируется в относительную фазу квантовых состояний. Для приготовления и измерения квантовых состояний применяется интерференционный принцип. Стабильность интерференционной картины является решающим фактором, обеспечивающим долговременную устойчивую работу систем квантовой криптографии. Видность интерференции V ($V = (I_{\rm up} - I_{\rm down})/(I_{\rm up} + I_{\rm down})$, где $I_{\rm up,down}$ – интенсивности конструктивной и деструктивной интерференции) напрямую связана с ошибкой в первичных ключах $Q = (1 - V)/2$. Поскольку все ошибки принципиально списываются на действия подслушивателя, видность определяет не только скорость генерации, но и секретность ключей.

В однопроходных системах квантовой криптографии обычно используется пара интерферометров Маха–Цандера, один на передающей, второй – на приемной стороне. Поскольку приготовление и измерение состояний происходят на разных интерферометрах, периодически необходимо балансировать интерферометры для устойчивой интерференционной картины. Двухпроходные схемы являются более устойчивыми, т.к. интерференция происходит на одном и том же интерферометре. Стандартное одномодовое волокно не сохраняет поляризацию и имеет наведенное двулучепреломление [1]. Поэтому состояния, прошедшие в интерферометре по разным путям, имеют разную поляризацию и изменяющуюся со временем относительную фазу. Таким образом, и в двухпроходных схемах требуется подстройка интерферометра. Кроме того, состояние канала связи также постоянно меняется. Существует известное решение по устранению изменения состояния поляризации в канале связи в двухпроходных системах. Отражение от фарадеевского зеркала [2, 3] переставляет состояния двух ортогональных компонент поляризации, что приводит к самокомпенсации искажения поляризации, связанного с двулучепреломлением. Данные схемы также не лишены недостатков. Стандартный волоконный модулятор является поляризационно-чувствительным элементом. Разные состояния поляризации модулируются по-разному. Для компенсации данного эффекта приходится дважды модулировать проходящие состояния. Из-за этого модулятор долго находится в активном состоянии, что понижает криптостойкость системы при активном зондировании. Кроме того, приходится разделять в интерферометре различные состояния поляризации. Это достигается механической фиксацией положения оптических разъемов, что может требовать периодической ручной проверки. И наконец, идея пассивной самокомпенсации с фарадеевскими зеркалами защищена патентом, что исключает ее коммерческое использование. *Предлагаемый нами подход состоит в ис-*

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

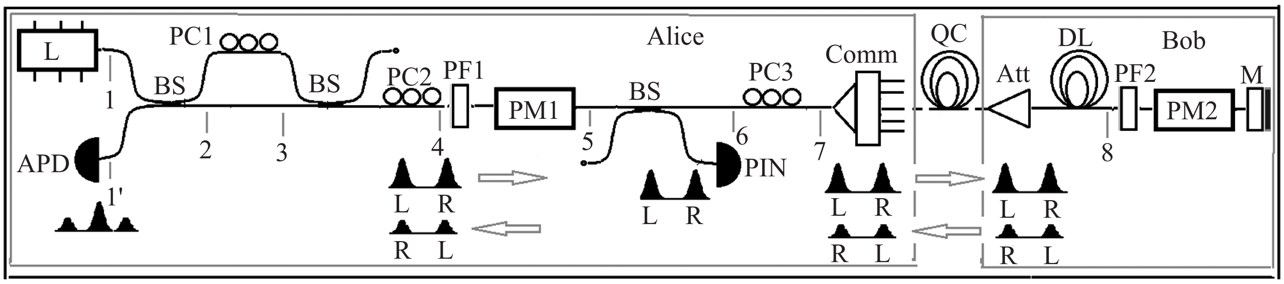

Рис. 1. Функциональная схема двухпроходной системы квантовой криптографии: L – лазер, BS – светоделители, PC1–PC3 – трехканальные контроллеры поляризации, PF1, PF2 – поляризационные фильтры, PM1, PM2 – фазовые модуляторы, APD – однофотонный лавинный детектор, PIN – классический фотодетектор, M – волоконное зеркало, Att – электронно-управляемый аттенюатор, QC – волоконная линия связи, DL – линия задержки, Comm – волоконный коммутатор для переключения между передающей станцией (Alice) и различными клиентами (Bob)

пользовании активной стабилизации интерферометра.

2. Идеология метода активной стабилизации. Интерференция определяется как состоянием поляризации, так и фазовыми соотношениями состояния поля. Как будет показано ниже, для обеспечения стабильной интерференции достаточно измерения интегральных характеристик поля на ходу. Сами по себе интегральные характеристики, такие, как интенсивность отклика детектора, нечувствительны к фазовым соотношениям и состоянию поляризации. Однако в комбинации с другими поляризационно-чувствительными элементами системы, поляризационными фильтрами и фазовыми модуляторами, можно доказуемо гарантировать управление интерференцией на ходу. При этом на выходе интерферометра получается пара одинаковых состояний, отличающихся только сдвигом по времени. Дальнейшая унитарная эволюция пары состояний в канале связи происходит одинаково. Эволюция в обратном направлении, как известно, описывается не обратным унитарным оператором, а транспонированным (в той же системе координат) [4, 5]. Поэтому в общем случае не гарантируется, что пара одинаковых состояний на обратном проходе обеспечит идеальную интерференционную картину. Ниже будет продемонстрировано, что наличие поляризационно-чувствительных элементов позволяет преодолеть данное обстоятельство и обеспечить стабильную интерференцию с видностью, близкой к идеальной. Сначала покажем, что *возможна локальная балансировка интерферометра только посредством измерений интенсивности каждого из пары состояний на его выходе. При этом еще нет никакой интерференции между данной парой состояний, прошедших по верхнему и нижнему плечам интерферометра* (рис. 1). Поскольку оптический тракт линеен и частотной дисперсией при наносекундной длительности импульсов можно пренебречь, то для краткости можно использовать состояния только одной частотной моды. На произвольные состояния, например пакеты, данные преобразования переносятся по линейности [1].

3. Эволюция на стороне Алисы, прямой проход. Состояние поля на выходе лазера (сечение 1 на рис. 1) в базисе состояний поляризации есть $|\hat{E}_{\rm in}(1)\rangle = \begin{pmatrix} \hat{\alpha} \\ \hat{\beta} \end{pmatrix}$, где $\hat{\alpha}, \hat{\beta}$ – компоненты поля для поляризации вверх и вниз. Далее, состояние поля в сечении 2 в верхнем и нижнем плечах интерферометра после симметричного светоделителя равно $\frac{1}{\sqrt{2}}\left(|\hat{E}_{\rm in}(2)\rangle, |\hat{E}_{\rm in}(2)\rangle\right)$. Для поля в сечении 3 в верхнем и нижнем плечах интерферометра с точностью до нормировки имеем

$$|\hat{E}_{\rm L}(3)\rangle = \hat{U}_{\rm PC1}(3,2)|\hat{E}_{\rm in}(2)\rangle,$$

$$|\hat{\rm E}_{R}(3)\rangle = \hat{U}_{\rm down}(3,2)|\hat{E}_{\rm in}(2)\rangle.$$

Стандартное одномодовое волокно не сохраняет поляризацию. Поэтому состояния $|\hat{E}_{\rm L}(3)\rangle$ и $|\hat{E}_{\rm R}(3)\rangle$, прошедшие по верхнему и нижнему путям, *отличаются не только на разность хода* (*относительной фазой*), *но и состоянием поляризации.* Здесь $\hat{U}_{\rm PC1}(3,2)$, $\hat{U}_{\rm down}(3,2)$ – операторы эволюции по верхнему и нижнему путям между сечениями 2 и 3. Волоконный контроллер поляризации позволяет получить из любого входного состояния поля любое выходное. Оператор эволюции PC1 описывается $SU(2)$-матрицей с тремя параметрами, управляемыми внешними напряжениями, которые приводят к деформации трех пьезоэлементов и изменению параметров волокна. Эволюция вне PC1 включена в оператор $\hat{U}_{\rm PC1}$. Поле в сечении 4 после PC2 есть

$$|\hat{E}(4)\rangle = \hat{U}_{\rm PC2}|\hat{E}_{\rm L}(3)\rangle + \hat{U}_{\rm PC2}|\hat{E}_{\rm R}(3)\rangle.$$

Первое слагаемое здесь описывает задний фронт, второе – передний, которые сдвинуты на разность хода длин плеч интерферометра. Поляризационный фильтр PF1 и фазовый модулятор являются поляризационно-чувствительными элементами. Поляризационный фильтр выполняет роль проектора на определенное состояние поляризации. Оси пропускания определенного состояния поляризации фазового модулятора и фильтра всегда согласованы. В базисе состояний поляризации в направлении оси пропускания фильтра имеем $\hat{U}_{\mathrm{PM1}}\hat{P}_{\mathrm{PF1}} = \begin{pmatrix} e^{i\varphi_A} & 0 \\ 0 & 0 \end{pmatrix}$.

Значение относительной фазы φ_A изменяется подачей импульса напряжения на фазовый модулятор во время прохождения одного из состояний L (или R). На прямом проходе фаза $\varphi_A = 0$. Оператор эволюции по двум путям в интерферометре (сечение 5) может быть представлен как пара проекторов на ортогональные подпространства состояний поляризации:

$$\hat{\hat{\hat{U}}}_{\mathrm{down}}(1 \to 5) = \hat{U}_{\mathrm{PM1}}\hat{P}_{\mathrm{PF1}}\hat{U}_{\mathrm{PC2}}\hat{U}_{\mathrm{down}}(2,3) =$$

$$= |\hat{E}^A_{\parallel}(5)\rangle_{\mathrm{LL}}\langle\hat{E}_{\mathrm{in}}(1)| + |\hat{E}^A_{\perp}(5)\rangle_{\mathrm{LL}}\langle\hat{E}^{\perp}_{\mathrm{in}}(1)|,$$

$$\hat{\hat{\hat{U}}}_{\mathrm{up}}(1 \to 5) = \hat{U}_{\mathrm{PM1}}\hat{P}_{\mathrm{PF1}}\hat{U}_{\mathrm{PC2}}\hat{U}_{\mathrm{PC1}}(2,3) =$$

$$= |\hat{E}^A_{\parallel}(5)\rangle_{\mathrm{RR}}\langle\hat{E}_{\mathrm{in}}(1)| + |\hat{E}^A_{\perp}(5)\rangle_{\mathrm{RR}}\langle\hat{E}^{\perp}_{\mathrm{in}}(1)|,$$

где $|\hat{E}^A_{\parallel}(5)\rangle_{\mathrm{L,R}}$ и $|\hat{E}^A_{\perp}(5)\rangle_{\mathrm{L,R}}$ – состояния во временных окнах L и R (рис. 1) с направлением вдоль оси PC2 и перпендикулярно ей. Условие унитарности дает

$$\hat{\hat{\hat{U}}}_{\mathrm{down,up}}(1 \to 5)\hat{\hat{\hat{U}}}^{+}_{\mathrm{down,up}}(1 \to 5) =$$

$$= |\hat{E}^A_{\parallel}(5)\rangle_{\mathrm{L,RL,R}}\langle\hat{E}^A_{\parallel}(5)| + |\hat{E}^A_{\perp}(5)\rangle_{\mathrm{L,RL,R}}\langle\hat{E}^A_{\perp}(5)| = \hat{I}.$$

Далее состояния поступают на PIN-детектор, который измеряет интенсивность импульсов в нужном временном окне. Сначала, изменяя три параметра PC2, добиваемся максимума отклика в окне L ($\max_{\mathrm{PC2}} |||\hat{E}^A_{\parallel}(5)\rangle_{\mathrm{L}}||$) для состояния, прошедшего по нижнему пути. Максимум означает, что поляризация состояния $|\hat{E}^A_{\parallel}(5)\rangle_{\mathrm{L}} = \hat{\hat{\hat{U}}}_{\mathrm{down}}(1 \to 5)|\hat{E}_{\mathrm{in}}(1)\rangle_{\mathrm{L}} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$. Затем изменением трех управляющих параметров PC1 добиваемся максимума отклика детектора ($\max_{\mathrm{PC1}} |||\hat{E}^A_{\parallel}(5)\rangle_{\mathrm{R}}||$) во временном окне R для состояния, прошедшего по верхнему пути. Максимум будет означать, что $|\hat{E}^A_{\parallel}(5)\rangle_{\mathrm{R}} = \hat{\hat{\hat{U}}}_{\mathrm{up}}(1 \to 5)|\hat{E}_{\mathrm{in}}(1)\rangle_{\mathrm{R}} = e^{i\theta}\begin{pmatrix} 1 \\ 0 \end{pmatrix}$, где θ – некоторая постоянная фаза, к которой детектор не чувствителен. После этого состояния в окнах L и R с точностью до фазы одинаковы, $|\hat{E}^A_{\parallel}(5)\rangle_{\mathrm{R}} = e^{i\theta}|\hat{E}^A_{\parallel}(5)\rangle_{\mathrm{L}}$.

4. Эволюция через канал связи (QC), прямой и обратный проходы. Состояния поля перед PC3 в сечении 6 с точностью до нормировки совпадают с состояниями в сечении 5 и одинаковы с точностью до фазового множителя $e^{i\theta}$. При прохождении через канал связи состояния в окнах L и R испытывают одинаковую эволюцию. Эволюция через канал связи (сечения 7, 8), прохождение через поляризационный фильтр, фазовый модулятор, отражение на зеркале и прохождение обратно до сечения 7, дает (индекс "B" относится к состояниям на обратном проходе от станции Боба, см. рис. 1)

$$|\hat{E}^B_{\parallel}(5)\rangle_{\mathrm{L}} + e^{i\varphi_B}|\hat{E}^B_{\parallel}(5)\rangle_{\mathrm{R}} =$$

$$= \hat{U}^T_{\mathrm{PC3}}\hat{U}^T_{\mathrm{ch}}(8,7)\hat{U}_{\mathrm{PF2}}\hat{U}_{\mathrm{PM2}}\hat{U}_{\mathrm{M}}\hat{U}_{\mathrm{PM2}}\hat{P}_{\mathrm{PF2}}\hat{U}_{\mathrm{ch}}(7,8) \times$$

$$\times \hat{U}_{\mathrm{PC3}}(|\hat{E}^A_{\parallel}(6)\rangle_{\mathrm{L}} + |\hat{E}^A_{\parallel}(6)\rangle_{\mathrm{R}}).$$

На обратном проходе после PM1 и PF1 (сечение 4) состояния с точностью до нормировки становятся равными $|\hat{E}^A_{\parallel}(5)\rangle_{\mathrm{L}} + e^{i(\varphi_B-\varphi_A)}|\hat{E}^A_{\parallel}(5)\rangle_{\mathrm{R}}$. При этом задний фронт L → R становится передним, а передний фронт R → L – задним. Таким образом, на обратном проходе $|\hat{E}^A_{\parallel}(5)\rangle_{\mathrm{R}} + e^{i(\varphi_B-\varphi_A)}|\hat{E}^A_{\parallel}(5)\rangle_{\mathrm{L}}$. Соответственно унитарные операторы допускают представление

$$(\hat{\hat{\hat{U}}}_{\mathrm{down}})^{\mathrm{T}}(1' \leftarrow 5) =$$

$$= |\hat{E}^{A*}_{\mathrm{in}}(1')\rangle_{\mathrm{LL}}\langle\hat{E}^*_{\parallel}(5)| + |\hat{E}^{*A\perp}_{\mathrm{in}}(1')\rangle_{\mathrm{LL}}\langle\hat{E}^*_{\perp}(5)|,$$

$$(\widetilde{U}_{\mathrm{up}})^{\mathrm{T}}(1' \leftarrow 5) =$$

$$= |\hat{E}^{A*}_{\mathrm{in}}(1')\rangle_{\mathrm{RR}}\langle\hat{E}^*_{\parallel}(5)| + |\hat{E}^{*A\perp}_{\mathrm{in}}(1')\rangle_{\mathrm{RR}}\langle\hat{E}^*_{\perp}(5)|,$$

Поскольку пространство состояний поляризации двумерно, базисные векторы $|\hat{E}^A_{\parallel}(5)\rangle$ и $|\hat{E}^A_{\perp}(5)\rangle$ (в базисе, в котором один базисный вектор направлен вдоль оси пропускания поляризационного фильтра и оси фазового модулятора, индекс $\parallel$) всегда можно выбрать действительными: $|\hat{E}^A_{\parallel}(5)\rangle = |\hat{E}^{*A}_{\parallel}(5)\rangle$ и $|\hat{E}^A_{\perp}(5)\rangle = |\hat{E}^{*A}_{\perp}(5)\rangle$.

Интерференции подвержены состояния, прошедшие на прямом проходе по короткому плечу, и состояния, прошедшие по длинному плечу интерферометра (рис. 1). Фазовый множитель $e^{i\theta}$, который набирало состояние R, теперь будет набирать состояние L:

$$e^{i\theta}(e^{i(\varphi_B-\varphi_A)} \pm 1)|\hat{E}^{A*}_{\mathrm{in}}(1,1')\rangle =$$

$$= (\widetilde{U}_{\mathrm{up}})^{\mathrm{T}}e^{i(\varphi_B-\varphi_A)}|\hat{E}^A_{\parallel}(1,1')\rangle_{\mathrm{L}} + (\widetilde{U}_{\mathrm{down}})^{\mathrm{T}}|\hat{E}^A_{\parallel}(1,1')\rangle_{\mathrm{R}}.$$

Знак "$\pm$" отвечает полю на выходах 1 и $1'$ соответственно. Отсчет на лавинном детекторе пропорционален разности фаз на сторонах Алисы и Боба: $\propto \sin^2\left(\frac{\varphi_B-\varphi_A}{2}\right)|||\hat{E}^{A*}_{\rm in}(1')\rangle||^2$.

Контроллер поляризации PC3 позволяет компенсировать искажения поляризации в канале связи. Регулировкой трех управляющих напряжений обеспечивается максимум сигнала (см. ниже) на лавинном детекторе (APD на рис. 1).

5. Экспериментальная реализация метода активной стабилизации. *5.1. Локальная балансировка интерферометра.* Представленные выше вычисления дают уверенность в том, что локальная балансировка гарантирует идеальную интерференцию для состояний, возвращающихся обратно из канала связи. Для реализации произвольного $SU(2)$-преобразования каждый контроллер поляризации (PC1, PC2) имеет три управляющих параметра, которые регулируются напряжениями в трех каналах. Поиск максимума сигнала PIN-диода, зависящего от нескольких параметров и имеющего хоть и незначительную, но шумовую составляющую, является нетривиальной задачей. Кроме того, управляющая пьезокерамика контроллеров имеет гистерезис и параметры управления не являются полностью независимыми. В результате исследований было установлено, что наиболее быстрой и устойчивой процедурой, выполняемой автоматически при инициализации системы, является следующая.

1. По каждому каналу независимо и при нулевых значениях в двух других напряжение изменяется с шагом 1 В на полный диапазон (≈ 60 В), что отвечает изменению на полный диапазон трех параметров в $SU(2)$-матрице в базисе горизонтальной и вертикальной поляризаций, описывающей любой линейный оптический элемент. Последняя может быть представлена в виде $SU(2,\varphi,\delta,\theta) = \begin{pmatrix} \cos(\varphi) & -\sin(\varphi) \\ \sin(\varphi) & \cos(\varphi) \end{pmatrix} \times$ $\times \begin{pmatrix} e^{i\delta} & 0 \\ 0 & e^{-i\delta} \end{pmatrix} \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$. Правая матрица преобразований является матрицей поворота, приводящей выбранный общий базис для всей оптической схемы к главным осям части тракта. Вторая матрица после приведения к главным осям описывает двулучепреломление (компоненты с разной поляризацией распространяются с разной скоростью и набирают различные дополнительные фазы $\pm\delta$). Левая матрица описывает обратный поворот от главных оптических осей данной части тракта к общей системе координат всей схемы. Выбирается тот канал, который дает максимальное значение сигнала. Напряжение в этом канале, отвечающее максимуму сигнала, фиксируется. Сканируется напряжение в окрестности этого значения с шагом 0.5 В. Находится максимум и напряжение фиксируется.

2. Процедура, описанная в п. 1, выполняется для двух оставшихся каналов. Напряжение, отвечающее максимуму сигнала в текущем канале, фиксируется. Напряжения, найденные для предыдущих каналов, держатся фиксированными.

3. Осуществляется тонкая подстройка максимума с шагом 0.5 В вблизи выбранных значений по всем трем каналам регулировки. Финальные напряжения фиксируются. Балансировка интерферометра завершена.

Процесс локальной балансировки интерферометра при включении системы занимает 4–6 мин. Эксперименты показали, что использование описываемых алгоритмов позволяет системе (рис. 1) автоматически настраиваться и поддерживать требуемые параметры в течение недели и более (см. рис. 2а–с). Система автоматически начинает балансировку, когда видность уменьшается до уровня $V = 0.99$ (напомним, что идеальная видность $V = 1.0$). Вклад в ошибку (QBER) от неидеальной видности при этом составляет $Q = (1 - 0.99)/2 = 0.5\,\%$. На работающей системе нет необходимости выполнять все шаги балансировки с самого начала. Достаточно выполнить шаг 3, что занимает существенно меньше времени. Зависимость видности от времени приведена на рис. 2а. На рис. 2b представлена временная зависимость ошибки в первичных ключах для реально работающего протокола распределения ключей (длина линии в двухпроходной схеме ≈ 25 км). Основной вклад в ошибку дают темновые шумы лавинного детектора. Эффективность генерации просеянных ключей приведена на рис. 2с.

5.2. Настройка максимального пропускания канала и измерение видности интерференции. Однофотонный лавинный детектор (APD на рис. 1) работает в стробируемом режиме (длительность строба ≈ 0.6 нс). Для корректного измерения сигнала строб должен по времени точно совпадать с приходящим световым импульсом. Однако из-за изменения длины линии и коэффициента преломления в зависимости от внешних факторов, в основном от температуры, происходит неконтролируемое изменение задержки. Кроме того, из-за внешних факторов в линии связи на основе стандартного одномодового волокна происходят искажения поляризации распространяющегося света, что приводит к неконтролируемой модуляции пропускания канала. Для их компенсации используется контроллер поляризации PC3. Настрой-

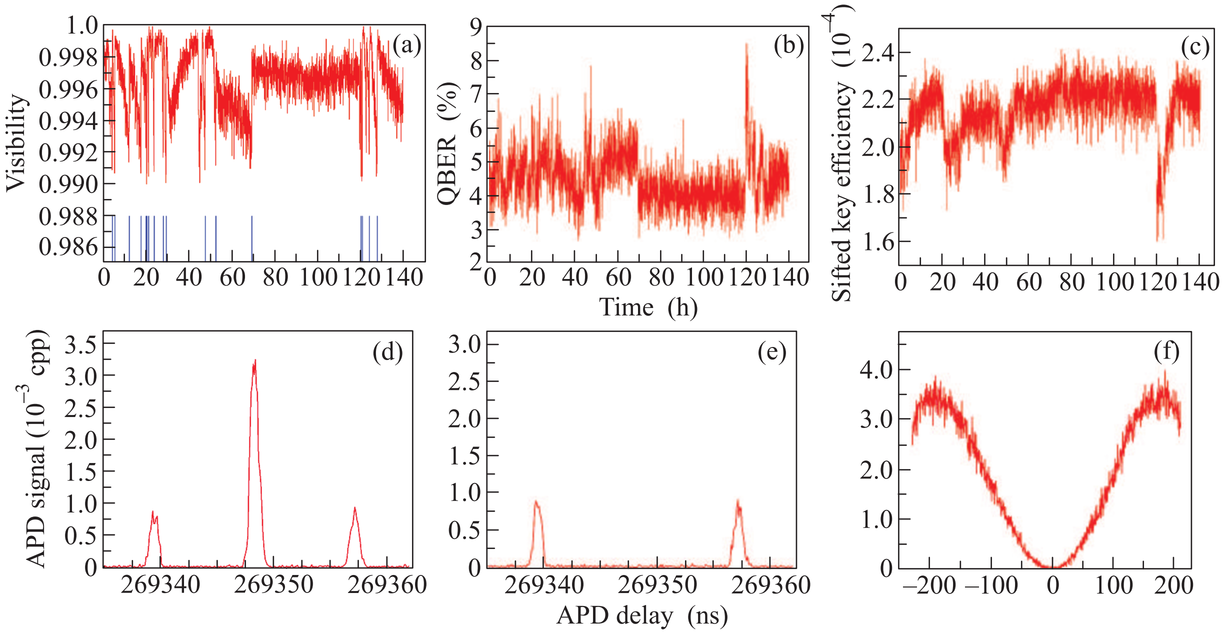

Рис. 2. (Цветной онлайн) a) – Зависимости видности от времени. Короткие вертикальные линии – моменты балансировки при уменьшении видности до критического уровня $V = 0.99$. (b) – Зависимость ошибки (QBER) от времени. (c) – Зависимости эффективности генерации просеянного ключа от времени. Для примера использовался протокол на геометрически однородных состояниях с 4 базисами [6]. Скачки на графиках связаны с изменениями температуры, а также балансировкой интерферометра, переводящей его в состояние с бо́льшей видностью. (d, e) – Зависимости темпа отсчетов на однофотонном детекторе APD при конструктивной (d) и деструктивной (e) интерференции от задержки строба. (f) – Зависимость темпа отсчетов на APD от разности фаз $\varphi_A - \varphi_B$. Задержка строба отсчитывается от импульса лазера. Среднее число фотонов на выходе станции Боба $\mu = 0.4$. Потери в линии связи $\mathrm{Loss} = 10^{-\delta\cdot L/10}$ ($L = 25$ км, $\delta = 0.2$ дб/км). Полные потери Алисы в данной системе 5.07 раз. Среднее число фотонов в когерентном состоянии в одном боковом окне составляет 1/4 от среднего числа фотонов в окне L (или R, см. рис. 1). Квантовая эффективность APD $\eta = 20\,\%$. Число отсчетов в боковом окне $\mathrm{Loss}\cdot(1/5.07)\cdot\eta\cdot\mu\cdot(1/4) = 1.2\cdot10^{-3}$. В центральном окне при сбалансированном интерферометре число отсчетов в 4 раза больше, чем в боковых, что соответствует теоретической оценке

ка максимального пропускания канала проводится автоматически при снижении эффективности генерации ключа. Процедура настройки максимального пропускания канала и измерения видности интерференции состоит из следующих шагов.

1. Открывается аттенюатор до уровня отсчетов APD $\leq 0.1{-}0.2$ на импульс для сохранения линейности. Фаза φ_A модулятора PM1 выставляется равной 0, а фаза φ_B модулятора PM2 – π, чтобы обеспечить максимум сигнала в центральном временном окне на выходе $1'$ (рис. 1).

2. Прописывается зависимость сигнала APD от задержки строба. Уточняется положение центрального временного окна. Запоминается максимальная интенсивность I_{up}.

3. Устанавливаются фазы $\varphi_A = \varphi_B = 0$. При этом отсчеты в центральном временном окне обусловлены только шумами и несбалансированностью интерферометра. Запоминается минимальная интенсивность I_{down}. Рассчитывается видность.

4. Затем, если это необходимо, при помощи контроллера поляризации PC3 производится настройка на максимум пропускания канала (максимум сигнала на центральном пике при $\varphi_A = 0$, $\varphi_B = \pi$). Процедура аналогична процедуре, используемой при локальной балансировке интерферометра.

На рис. 2d и e приведено число отсчетов на лавинном детекторе при разных положениях строба относительно светового импульса при реальных рабочих параметрах, используемых в протоколе, а на рис. 2f представлена зависимость числа отсчетов в центральном временном окне от относительной фазы $\varphi_A - \varphi_B$. Как видно из рис. 2d и e, имеет место практически идеальная видность (не хуже 0.99) при конструктивной и деструктивной интерференции.

6. Заключение. Таким образом, разработан и реализован патентно-чистый метод активной балансировки оптической части двухпроходного варианта системы квантовой криптографии, который позволяет осуществлять компенсацию всех поляризационных и фазовых искажений. Метод переносится и на однопроходные системы. Реализация метода в волоконных системах квантового распределения ключей необходима для поддержания в автоматическом режиме видности интерференционной картины на уровне не менее $V \geq 0.99$ (QBER $\leq 0.5\,\%$). Такой режим работы квантово-криптографических систем отвечает существующим требованиям по автономной (без участия оператора) работе систем связи.

Работа выполнена при поддержке гранта РНФ # 16-12-00015.

1. C. Tsao, *Optical fibre waveguide analysis*, Oxford Science Publ. (1992).
2. D. S. Bethune and W. P. Risk, New J. Phys. **4**, 42.1 (2002).
3. A. Müller, T. Herzog, B. Hüttner, W. Tittel, H. Zbinden, and N. Gisin, Appl. Phys. Lett. **70**, 793 (1997).
4. E. Brinkmeyer, Optics Lett. **6**, 575 (1981).
5. A. Mecozzi and C. Antonelli, J. Lightwave Techn. **29**, 642 (2011).
6. С. Н. Молотков, Письма в ЖЭТФ **101**, 637 (2015).