ЖЭТФ, 2013, том 143, вып. 5, стр. 820–830 

# О ДВУХПРОХОДНОЙ СХЕМЕ БЕЗ ФАРАДЕЕВСКОГО ЗЕРКАЛА ДЛЯ РЕЛЯТИВИСТСКОЙ КВАНТОВОЙ КРИПТОГРАФИИ В ОТКРЫТОМ ПРОСТРАНСТВЕ

***К. С. Кравцов*** [a,b], ***И. В. Радченко*** [a,b], ***А. В. Корольков*** [c], ***С. П. Кулик*** [b*], ***С. Н. Молотков*** [c,d,e**]

[a] *Институт общей физики им. А. М. Прохорова Российской академии наук 119991, Москва, Россия*

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

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

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

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

Поступила в редакцию 6 ноября 2012 г.

Стабильность деструктивной интерференции независимо от входного состояния и состояния квантового канала связи в волоконных оптических схемах, используемых в квантовой криптографии, играет принципиальную роль в обеспечении секретности передаваемых ключей. Предложена новая оптическая схема, которая может использоваться как для релятивистской квантовой криптографии при передаче ключей через открытое пространство, так и для передачи по оптоволоконным линиям. Схема обеспечивает стабильность деструктивной интерференции и допускает простую автоматическую балансировку волоконного интерферометра.

**DOI**: 10.7868/S0044451013050017

## 1. ВВЕДЕНИЕ

В квантовой криптографии — в системах квантового распределения ключей — детектирование попыток подслушивания происходит по потоку ошибок при измерениях квантовых состояний на приемной стороне [1]. Любая система квантовой криптографии гарантирует секретность передаваемых ключей только в том случае, если наблюдаемая ошибка на приемной стороне не превышает некоторого критического значения, которое является фундаментальной величиной для каждого протокола. Принципиально невозможно отличить ошибки, возникающие от вторжения в квантовый канал связи, от собственных ошибок (шумов) аппаратуры. Поэтому все ошибки приходится списывать на действия подслушивателя. Собственные источники ошибок можно условно разделить на три типа: 1) темновые шумы однофотонных лавинных детекторов, 2) нестабильности оптических частей схемы на приемной и передающей сторонах, 3) оптическая нестабильность квантового канала связи. В качестве квантового канала связи может выступать как оптоволоконная линия, так и открытое пространство.

Наша основная цель — использование результатов данной работы для систем релятивистской квантовой криптографии в открытом пространстве. Релятивистская квантовая криптография была пред-

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

ложена в работах [2, 3]. В отличие от других систем квантовой криптографии, где секретность ключей базируется только на запретах квантовой механики на различимость состояний, в релятивистской квантовой криптографии секретность ключей гарантируется как запретами квантовой механики, так и ограничениями специальной теории относительности. Данные системы, в отличие от всех других систем, обеспечивают секретность ключей при больших потерях (теоретически при сколь угодно больших потерях) в канале связи и не строго однофотонном источнике состояний. Неидеальность квантового канала связи — деформации оптоволокна и флуктуации в атмосфере — приводят как к искажениям квантовых состояний, так и к их потере. Было потрачено немало усилий и предложены различные оптические схемы для систем квантовой криптографии для решения проблемы нестабильности квантового канала связи [1]. Однако до сих пор проблема в полном объеме так и не решена. Потери в канале напрямую не приводят к ошибкам на приемной стороне, но влияют косвенно — уменьшая долю реальных отсчетов и, соответственно, увеличивая долю темновых отсчетов, приводящих к ошибкам. Сама идея квантового распределения ключей предполагает исключение участия оператора в процессе генерации ключей. Системы квантовой криптографии представляют собой, по существу, распределенное аналоговое физическое устройство, неизбежно требующее периодической балансировки оптической части. Исключение оператора из работы системы также предполагает, что система должна допускать простую автоматическую балансировку оптической части.

Распространение состояний через канал связи приводит к вращению поляризации и изменению фазовых соотношений между компонентами с разной поляризацией. Причем эти изменения невозможно контролировать. В оптоволоконном канале связи данная проблема является еще более острой, потому что стандартное одномодовое волокно SMF-28 в принципе не сохраняет поляризацию. Использовать для канала связи волокно, сохраняющее поляризацию, PM-волокно, на сегодняшний день достаточно дорого. Используемые практически во всех схемах электрооптические фазовые модуляторы являются поляризационно-избирательными, в результате неконтролируемые изменения поляризации в канале связи приводят к ошибкам. В идеале хотелось бы иметь оптическую схему, которая была бы нечувствительна к таким изменениям, точнее говоря, чтобы изменения поляризации в канале связи напрямую не приводили к ошибкам детектирования. Отсутствие ошибок детектирования при любом состоянии канала связи с физической точки зрения эквивалентно стабильности деструктивной интерференции (гашению интерференции) при фотодетектировании независимо от состояния канала связи. Ниже будем иметь в виду системы квантовой криптографии с фазовым кодированием (см., например, [1]). Схемы с фазовым кодированием как однопроходные, так и двухпроходные содержат в том или ином виде волоконно-оптический интерферометр Маха–Цандера (MZ). При этом технически удобно приготавливать квантовые состояния, используя волоконные интерферометры независимо от того, какой квантовый канал связи используется — волоконная линия или открытое пространство.

## 2. ОПТИЧЕСКАЯ СХЕМА

Для дальнейшего нам потребуются две оптические схемы. Оказывается, что возникают два решения. Для иллюстрации первого решения используется схема без поляризационно-избирательных элементов (рис. 1), вторая схема содержит такие элементы и приведена на рис. 2.

Рассмотрим схему рис. 1. На выходе из лазера отдельное состояние после прохождения интерферометра с разной длиной плеч преобразуется в пару состояний, прошедших по короткому верхнему (up) и нижнему длинному (down) путям. После прохождения канала связи, отражения от зеркала состояния up и down меняются местами. На обратном проходе пара состояний, сдвинутых по расстоянию, снова поступает на интерферометр MZ, где пары состояний по верхнему и нижнему путям опять сдвигаются относительно друг друга. На выходе MZ состояние up, прошедшее по верхнему пути интерферирует с состоянием down, прошедшим по нижнему пути. В зависимости от относительной фазы состояний up и down имеет место либо деструктивная интерференция — отсутствие отсчета на детекторе, либо конструктивная, приводящая к отсчету.

Рассмотрим схему рис. 2. Классические интенсивные импульсы лазера поступают на интерферометр MZ с разной длиной плеч. В длинном плече встроен управляемый контроллер поляризации PC1. Далее пара импульсов через контроллер поляризации PC2 поступает на фазовый модулятор PM1. На прямом проходе модулятор не активен. На обратном проходе на модулятор во время прохождения перед-

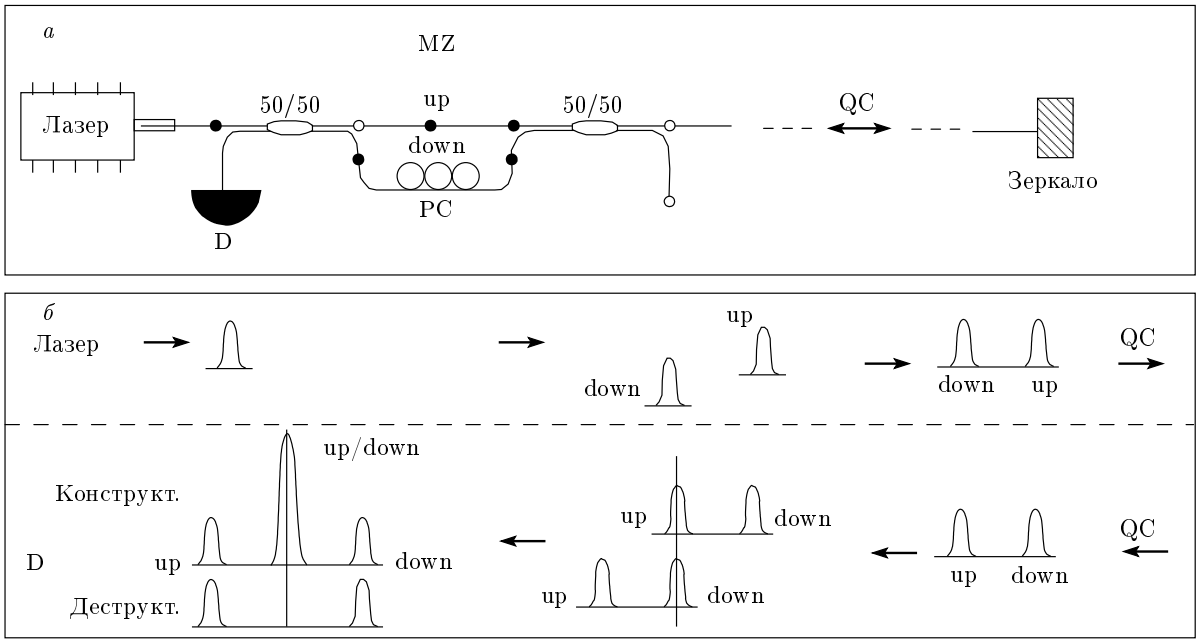


**Рис. 1.** *а*) Оптическая схема без поляризационно-избирательных элементов: MZ — интерферометр Маха – Цандера, PC — контроллер поляризации, D — детектор, 50/50 — симметричные светоделители, QC — канал связи. *б*) Эволюция состояния на прямом (сверху) и обратном (снизу) проходах по оптической системе

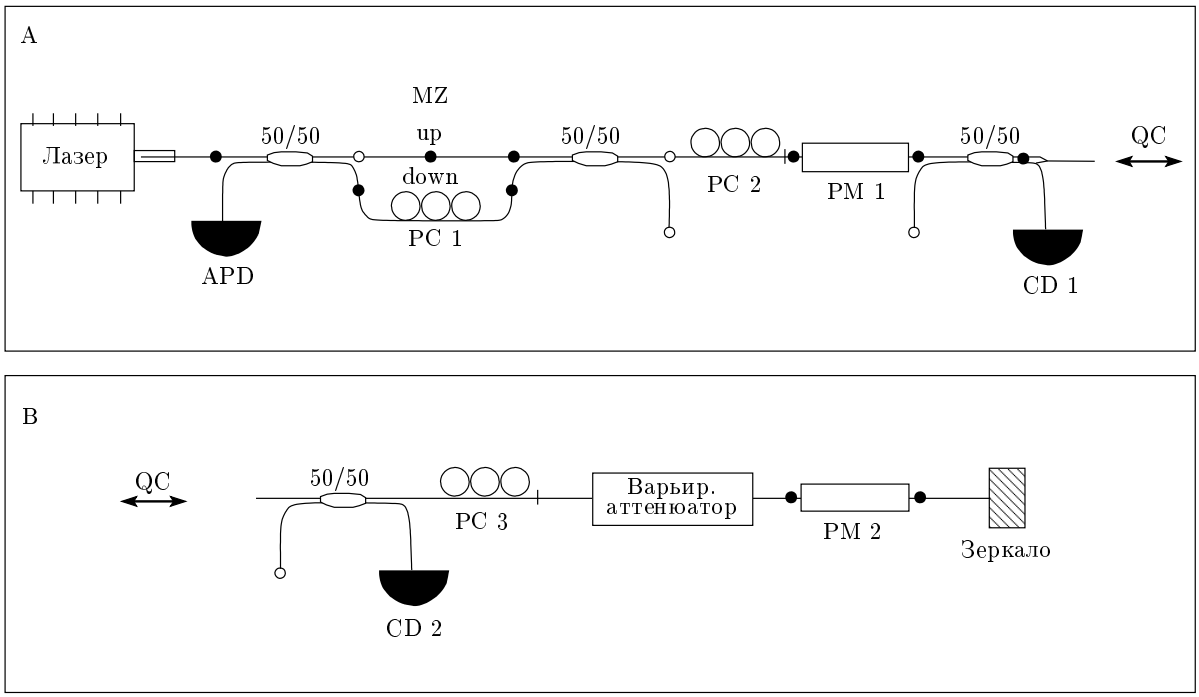


**Рис. 2.** Оптическая схема с поляризационно-избирательными элементами: MZ — интерферометр Маха – Цандера, PC1, PC2, PC3 — контроллеры поляризации, PM1, PM2 — фазовые модуляторы, CD1, CD2 — фотодетекторы, APD — однофотонный лавинный детектор

него состояния прикладывается импульс напряжения для изменения относительной фазы между двумя состояниями, сдвинутыми во времени. Классический фотодетектор CD1 на прямом проходе используется для измерения интенсивности каждого из состояний (на рис. 1 — up и down) при балансировке интерферометра MZ. На приемной стороне пара классических состояний поступает частично на фотодетектор CD2, используемый для синхронизации, затем через управляемый контроллер поляризации PC3 на варьируемый аттенюатор, на котором происходит ослабление сигнала до такого уровня, чтобы после отражения от зеркала и обратного прохождения на стороне B в канал связи поступил квазиоднофотонный сигнал. На фазовый модулятор PM2 прикладывается импульс напряжения на обратном проходе, чтобы изменить относительную фазу между состояниями up и down. При обратном проходе интерферометра за счет сдвига пары состояний во времени имеет место интерференция в центральном временно́м окне — между состояниями up и down (нижняя часть рис. 1), — которая, в зависимости от относительных фаз на состояниях up и down, приводит либо к отсчету, либо к его отсутствию — гашению интерференции.

Общая идея фазового кодирования сводится к следующему. При прохождении состояний туда и обратно на стороне A и B системой проводится изменение относительной фазы между состояниями up и down (см. рис. 2). Фазы на обеих сторонах выбираются независимо и случайно из наборов $\{\varphi_{i,A}\}$ и $\{\varphi_{i,B}\}$ в зависимости от используемого протокола. При этом при определенных парах фаз, например, при $\varphi_{i,A} = \varphi_{i,B}$, имеет место гашение интерференции на лавинном детекторе. Иначе говоря, в таких посылках в отсутствие подслушивателя не должно быть отсчетов. Появление отсчетов в тех посылках, где их не должно быть, свидетельствует о подслушивании при передаче ключей. Число ошибочных отсчетов зависит как от состояния канала связи, так и от точности балансировки интерферометра MZ. Поэтому принципиально важно, чтобы изменения состояния канала сами по себе не приводили к появлению отсчетов там, где их не должно быть.

Если бы интерферометр MZ был идеальным, то на выходе возникала бы пара одинаковых состояний с одинаковой поляризацией, сдвинутых по времени на величину разности хода по верхнему и нижнему путям. Дальнейшая эволюция пары одинаковых состояний через канал связи была бы также одинаковой[1)]. Главная проблема состоит в том, как сделать так, чтобы прохождение по двум путям интерферометра приводило на выходе к двум одинаковым состояниям. Поскольку волокно имеет деформации, поляризационные состояния выходят разными и требуется балансировка интерферометра. Оказывается, что данная задача имеет красивое и простое (но отнюдь не тривиальное) решение, допускающее техническую реализацию и гарантирующее равенство состояний на выходе интерферометра MZ.

## 3. ОБЩИЙ ВИД МАТРИЦЫ ОПТИЧЕСКОГО ПРЕОБРАЗОВАНИЯ

Для дальнейшего удобно пользоваться дираковскими обозначениями. В этом случае состояния поля в базисе двух поляризаций горизонтальной $H$ и вертикальной $V$ — представляют собой двухкомпонентный столбец:

$$|E\rangle = \alpha|E_H\rangle + \beta|E_V\rangle \to \begin{pmatrix} \alpha \\ \beta \end{pmatrix}, \qquad (1)$$

где $|E_{H,V}\rangle$ — базисные состояния поляризации, $\alpha, \beta$ — комплексные коэффициенты.

Эволюция состояний является унитарной, поэтому общий вид матрицы оптического преобразования есть матрица группы SU(2). Трансфер-матрица общего вида в базисе горизонтальной и вертикальной поляризаций, описывающая любой линейный оптический элемент, может быть представлена в виде [4]

$$\begin{aligned}\hat{U}(\varphi,\delta,\theta) &= \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix} \times \\ &\times \begin{pmatrix} e^{i\delta} & 0 \\ 0 & e^{-i\delta} \end{pmatrix} \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} = \\ &= \begin{pmatrix} T(\varphi,\delta,\theta) & R(\varphi,\delta,\theta) \\ -R^*(\varphi,\delta,\theta) & T^*(\varphi,\delta,\theta) \end{pmatrix}. \qquad (2)\end{aligned}$$

Данное представление имеет прозрачный физический смысл. Правая матрица преобразований является матрицей поворота, которая приводит выбранный общий базис ($HV$) для всей оптической схемы к главным осям элемента. Вторая матрица после приведения к главным осям описывает двойное лучепреломление (компоненты с разной поляризацией рас-

[1)] Деформационные и температурные изменения в канале связи за время, разделяющее состояния up и down, не успевают произойти, поскольку данное время составляет несколько наносекунд.

пространяются с разной скоростью и набирают различные дополнительные фазы $\pm\delta$). Третья (левая) матрица описывает обратный поворот главных оптических осей данного оптического элемента к общей системе координат всей схемы.

## 4. ПРЕОБРАЗОВАНИЕ ПОЛЕЙ В ИНТЕРФЕРОМЕТРЕ МАХА–ЦАНДЕРА И КАНАЛЕ СВЯЗИ

Состояние канала постоянно меняется и каждый раз на интерферометр возвращается разная пара состояний. Прохождение туда и обратно не приводит к компенсации изменений состояний. Формальная причина связана с тем, что если эволюция состояний на прямом проходе описывается некоторой унитарной матрицей $\mathbf{U}$, то обратное прохождение (в той же системе координат) описывается транспонированной унитарной матрицей [5, 6] $\mathbf{U}^T$[2)], поэтому их произведение, описывающее эволюцию туда и обратно не является (при наличии двойного лучепреломления) единичной матрицей $\mathbf{U}^T\mathbf{U} \neq \mathbf{I}$.

Дальнейшая цель — выяснить, при каких условиях после выхода состояния из интерферометра Маха–Цандера и прохождения через канал связи туда и обратно на входе детектора APD независимо от состояния канала связи будет иметь место деструктивная интерференция (гашение состояний), т. е. отсутствие отсчетов независимо от изменения состояния самого канала связи.

1) Сначала покажем, что имеются условия, при которых идеальное гашение интерференции будет иметь место при любых изменениях состояний в канале связи за счет упомянутых факторов. Фактически будет показано, что при определенной балансировке интерферометра деструктивная интерференция не будет зависеть от изменений в канале связи и входного состояния. Однако техническая реализация автоматической балансировки для данного решения является достаточно сложной[3)]. Отметим, что данное решение не использует факт присутствия поляризационно-избирательных элементов.

2) Затем приведем второе решение, обеспечивающее идеальное гашение интерференции независимо от входного состояния и канала связи. Покажем также, что существует простой рецепт автоматической балансировки. Данное решение явно использует неизбежное наличие в оптической схеме поляризационно-избирательных элементов (фазовых модуляторов). Присутствие этих элементов является необходимым атрибутом автоматической балансировки.

Забегая вперед, отметим: данные условия обеспечиваются тем, что если из интерферометра выходят одинаковые квантовые состояния, то дальнейшие их изменения в канале связи также будут одинаковыми. И несмотря на то что на интерферометр возвращаются другие состояния по сравнению с теми, которые были на выходе, все равно гарантируется точное гашение интерференции в центральном временно́м окне и отсутствие ошибок, связанных с изменениями состояния квантового канала связи. Нетривиальность процедуры балансировки заключается в том, что достаточно только одного измерения интегральной интенсивности поля в двух временны́х окнах, прошедшего по верхнему и нижнему пути интерферометра на прямом проходе классическим фотодетектором CD2 в режиме интенсивного сигнала лазера.

Докажем сначала первую часть утверждения, а затем приведем процедуру автоматической балансировки для второго решения. Для этого потребуются матрицы преобразований оптических элементов.

**Матрица преобразования для светоделителя 50/50** имеет вид

$$\hat{\mathbf{U}}^{(1)}_{50/50} = \frac{1}{\sqrt{2}}\begin{pmatrix} \hat{I} & -\hat{I} \\ \hat{I} & \hat{I} \end{pmatrix}, \qquad \hat{\mathbf{U}}^{(2)}_{50/50} = \frac{1}{\sqrt{2}}\begin{pmatrix} \hat{I} & -\hat{I} \\ \hat{I} & \hat{I} \end{pmatrix}. \tag{3}$$

**Матрицы преобразований по различным путям интерферометра.** Трансфер-матрица верхнего (up) и нижнего (down) путей в интерферометре Маха–Цандера записывается как

$$\hat{\mathbf{U}}^{MZ}_{up/down} = \begin{pmatrix} \hat{U}^{MZ}_{up} & 0 \\ 0 & \hat{U}^{MZ}_{down} \end{pmatrix}. \tag{4}$$

Полная трансфер-матрица интерферометра MZ равна

$$\hat{\mathbf{U}}^{MZ} = \hat{\mathbf{U}}^{(2)}_{50/50}\hat{\mathbf{U}}^{MZ}_{up/down} \cdot \hat{\mathbf{U}}^{(1)}_{50/50}. \tag{5}$$

Состояния поля в двух каналах up и down равны

[2)] Физическая причина появления транспонированной матрицы на обратном проходе связана с тем, что положительно-частотные состояния поля с противоположными значениями волнового вектора связаны транспонированной матрицей (см. детали вывода в [6]).

[3)] Описание экспериментальной реализации для данного случая требует большого объема и здесь не приведено.

$$|E_{in}^{up}\rangle = \begin{pmatrix} E_H^{up} \\ E_V^{up} \end{pmatrix}, \quad |E_{in}^{down}\rangle = \begin{pmatrix} E_H^{down} \\ E_V^{down} \end{pmatrix},$$
$$|\hat{\mathbf{E}}_{in}^{up/down}\rangle = \begin{pmatrix} |E_{in}^{up}\rangle \\ |E_{in}^{down}\rangle \end{pmatrix}. \tag{6}$$

Выходное поле

$$|\hat{\mathbf{E}}_{out}^{up/down}\rangle = \begin{pmatrix} |E_{out}^{up}\rangle \\ |E_{out}^{down}\rangle \end{pmatrix} = \hat{\mathbf{U}}^{MZ} \cdot |\hat{\mathbf{E}}_{in}^{up/down}\rangle = \frac{1}{2} \begin{pmatrix} (\hat{U}_{up}^{MZ} - \hat{U}_{down}^{MZ})|E_{in}^{up}\rangle \\ (\hat{U}_{up}^{MZ} + \hat{U}_{down}^{MZ})|E_{in}^{up}\rangle \end{pmatrix}. \tag{7}$$

Для амплитуд поля в верхнем канале на выходе MZ (после отбрасывания холостого выхода) имеем

$$|\hat{\mathbf{E}}_{out}^{up}\rangle = \begin{pmatrix} |E_{out}^{up}\rangle \\ 0 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} (\hat{U}_{up}^{MZ} - \hat{U}_{down}^{MZ})|E_{in}^{up}\rangle \\ 0 \end{pmatrix}. \tag{8}$$

**Матрицы зеркал.** Отражение от зеркала (M) и фарадеевского зеркала (FM) дается матрицами

$$\widehat{MR}^{M} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \widehat{MR}^{FM} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}. \tag{9}$$

Фарадеевское зеркало при отражении меняет компоненты поляризации $H \leftrightarrow V$.

**Матрицы преобразования полей в канале связи.** Пусть трансфер-матрица канала связи есть $\hat{U}_{ch}$. При обратном проходе используются транспонированные матрицы преобразования. После прохождения через канал, отражения от зеркала и обратного прохождения через канал для поля перед входом в интерферометр имеем ($m = M$ или $m = FM$)

$$\hat{U}_{\leftrightarrow} = \hat{U}_{ch}^{T} \cdot \widehat{MR}^{m} \cdot \hat{U}_{ch}. \tag{10}$$

Обратное прохождение через интерферометр дается трансфер-матрицей $(\hat{\mathbf{U}}^{MZ})^T$. Для амплитуд поля па верхнем и нижнем выходах интерферометра находим

$$|\hat{\mathbf{E}}_{back}^{up}\rangle = \begin{pmatrix} |E_{back}^{up}\rangle \\ |E_{back}^{down}\rangle \end{pmatrix} = \frac{1}{4} \begin{pmatrix} \left[(\hat{U}_{up}^{MZ})^T \cdot \hat{U}_{\leftrightarrow} \cdot (\hat{U}_{up}^{MZ} - \hat{U}_{down}^{MZ}) + (\hat{U}_{down}^{MZ})^T \cdot \hat{U}_{\leftrightarrow} \cdot (\hat{U}_{up}^{MZ} - \hat{U}_{down}^{MZ})\right] |E_{in}^{up}\rangle \\ \left[-(\hat{U}_{up}^{MZ})^T \cdot \hat{U}_{\leftrightarrow} \cdot (\hat{U}_{up}^{MZ} - \hat{U}_{down}^{MZ}) + (\hat{U}_{down}^{MZ})^T \cdot \hat{U}_{\leftrightarrow} \cdot (\hat{U}_{up}^{MZ} - \hat{U}_{down}^{MZ})\right] |E_{in}^{up}\rangle \end{pmatrix}. \tag{11}$$

Амплитуда поля в центральном временно́м окне при интерференции состояний up (прямой проход) $\rightarrow$ $\rightarrow$ down (обратный проход) и down (прямой проход) $\rightarrow$ up (обратный проход), имеет вид

$$\frac{1}{4} \begin{pmatrix} \left[(\hat{U}_{up}^{MZ})^T \cdot \hat{U}_{\leftrightarrow} \cdot \hat{U}_{down}^{MZ} + (\hat{U}_{down}^{MZ})^T \cdot \hat{U}_{\leftrightarrow} \cdot \hat{U}_{up}^{MZ}\right] |E_{in}^{up}\rangle \\ \left[(\hat{U}_{up}^{MZ})^T \cdot \hat{U}_{\leftrightarrow} \cdot \hat{U}_{down}^{MZ} - (\hat{U}_{down}^{MZ})^T \cdot \hat{U}_{\leftrightarrow} \cdot \hat{U}_{up}^{MZ}\right] |E_{in}^{up}\rangle \end{pmatrix}. \tag{12}$$

**Решение 1.** Первое решение является более-менее очевидным. Если трансфер-матрицы для состояний поляризации по верхнему и нижнему (с точностью до общего фазового множителя $e^{i\psi_L}$ перед матрицей, связанного с разной длиной плеч, который без ограничения общности, ниже опускаем) путям равны $\hat{U}_{up}^{MZ} = \hat{U}_{down}^{MZ} = \hat{U}^{MZ}$, то равны и транспонированные матрицы $(\hat{U}_{up}^{MZ})^T = (\hat{U}_{down}^{MZ})^T = (\hat{U}^{MZ})^T$. Тогда независимо от входного состояния, состояния канала и типа зеркала имеет место идеальная деструктивная интерференция. Амплитуда состояния на выходе лавинного детектора тождественно равна нулю. Это гарантируется для любого состояния условием равенства матриц преобразований по верхнему и нижнему путям в интерферометре,

$$\hat{U}_{up}^{MZ} = \hat{U}_{down}^{MZ} = \hat{U}^{MZ}, \tag{13}$$

тогда

$$|E_{back}^{down}\rangle = \left[(\hat{U}^{MZ})^T \cdot \hat{U}_{\leftrightarrow} \cdot \hat{U}^{MZ} - (\hat{U}^{MZ})^T \cdot \hat{U}_{\leftrightarrow} \cdot \hat{U}^{MZ}\right] |E_{in}^{up}\rangle \equiv 0. \tag{14}$$

Данное решение является универсальным в том смысле, что обеспечивает идеальное гашение интерференции независимо от присутствия других оптических элементов в схеме (поляризационно-избирательных фазовых модуляторов, контроллеров поляризации и отражающих зеркал). Однако не существует простого алгоритма достичь равенства матриц преобразования по двум путям, используя управляющие элементы — контроллеры поляризации[4)].

**Решение 2. Автоматическая балансировка интерферометра.** Приведем теперь второе решение, обеспечивающее гашение интерференции независимо от входного состояния и состояния самого канала связи. Данное решение явно использует факт присутствия в оптической схеме поляризационно-избирательных элементов — фазовых модуляторов. Фазовые модуляторы на основе ниобата лития технологически устроены таким образом, что пропускают состояния только с одним направлением поляризации, которое зависит от оси ориентации фазового модулятора.

Приведем доказательство утверждения вместе с конструктивной процедурой балансировки.

С формальной точки зрения матрица, описывающая действие фазового модулятора, является проектором на определенное направление поляризации. Пусть состояние, отвечающее направлению поляризации, которое пропускает фазовый модулятор, равно $|E_{1||}\rangle$, а отвечающее перпендикулярному направлению, которое не пропускает фазовый модулятор — $|E_{1\perp}\rangle$. Действие фазового модулятора в отсутствие приложенного напряжения на нем в базисе $\{|E_{1||}\rangle, |E_{1\perp}\rangle\}$ описывается проектором

$$\hat{U}_{PM1} = |E_{1||}\rangle\langle E_{1||}|. \tag{15}$$

Пусть состояния после контроллера поляризации PC2, происходящие из состояний, прошедших по верхнему и нижнему пути интерферометра, имеют вид

$$\begin{aligned} |E^{up}\rangle &= \hat{U}^{PC2}_{up}|E_{in}\rangle = \hat{U}^{PC2}\hat{U}^{MZ}_{up}|E_{in}\rangle, \\ |E^{down}\rangle &= \hat{U}^{PC2}_{down}|E_{in}\rangle = \hat{U}^{PC2}\hat{U}^{MZ}_{down}|E_{in}\rangle, \end{aligned} \tag{16}$$

где $\hat{U}^{PC2}$ — трансфер-матрица, описывающая некоторое текущее состояние контроллера поляризации. Управляя контроллером поляризации, можно получить любой унитарный оператор. На данном шаге матрицы перехода по верхнему (up) и нижнему (down) путям интерферометра MZ фиксированы.

[4)] Этот способ требует отдельного рассмотрения.

*Шаг 1. Регулируя состояние PC2, добиваемся равенства нулю интенсивности на фотодетекторе CD2 во временно́м окне, накрывающем состояние, прошедшее по верхнему (up) пути интерферометра — пути, не содержащем контроллера PC1.*

Такая эволюция описывается унитарным оператором, который в двумерном пространстве может быть представлен в виде

$$\begin{aligned} \hat{U}^{PC2}_{up}(\perp) = \hat{U}^{PC2}(\perp)\hat{U}^{MZ}_{up} = \\ = |E_{1\perp}\rangle\langle E_{in}| + |E_{1||}\rangle\langle E_{in\perp}|, \end{aligned} \tag{17}$$

где $|E_{in\perp}\rangle$ — ортогональное дополнение к $|E_{in}\rangle$, а $\hat{U}^{PC2}(\perp)$ — трансфер-матрица, описывающая состояние контроллера поляризации PC2, при котором отсутствуют отсчеты на фотодетекторе CD2 во временно́м окне, накрывающем состояние, прошедшее по пути up в интерферометре. При такой настройке контроллера поляризации состояния, прошедшие по пути up, полностью не пропускаются фазовым модулятором. Вероятность регистрации детектором CD2 равна

$$|\langle E_{1||}|\hat{U}^{PC2}_{up}(\perp)|E_{in}\rangle|^2 = |\langle E_{1||}|E_{\perp}\rangle|^2 = 0. \tag{18}$$

*Шаг 2. Изменяя состояние контроллера поляризации PC1 в плече интерферометра, добиваемся равенства нулю отсчета во втором временно́м окне, накрывающем состояние, прошедшее по пути down.*

Поскольку контроллер поляризации позволяет перевести любое входное состояние в любое выходное, при фиксированном положении контроллера PC2 всегда можно установить такое состояние PC1, при котором отклик детектора CD2 во временно́м окне, накрывающем состояние, прошедшее по нижнему (down) пути, будет равен нулю. Обозначим трансфер-матрицу по нижнему пути интерферометра MZ, отвечающую упомянутому состоянию контроллера PC1, как $\hat{U}^{PC1MZ}_{down}(\perp)$. Тогда матрица преобразования непосредственно перед фазовым модулятором для состояния, прошедшего по пути down, имеет вид

$$\begin{aligned} \hat{U}^{PC1}_{down}(\perp) = \hat{U}^{PC2}(\perp)\hat{U}(\perp)^{PC1MZ}_{down} = \\ = |E'_{1\perp}\rangle\langle E_{in}| + |E'_{1||}\rangle\langle E^{\perp}_{in}|, \end{aligned} \tag{19}$$

где $\hat{U}(\perp)^{PC1MZ}_{down}$ — трансфер-матрица по пути down и состояния $|E'_{1\perp}\rangle$ и $|E'_{1||}\rangle$ параллельны направлениям $|E_{1\perp}\rangle$ и $|E_{1||}\rangle$. Поскольку пространство состояний для поляризационных степеней свободы двумерно, пары ортогональных состояний $\{|E'_{1\perp}\rangle, |E'_{1||}\rangle\}$

и $\{|E_{1\perp}\rangle, |E_{1||}\rangle\}$, перпендикулярных и параллельных одним и тем же направлениям, могут отличаться только фазовыми множителями.

Иначе говоря, $|E'_{1\perp}\rangle = e^{i\varphi_\perp}|E_{1\perp}\rangle$ и $|E'_{1||}\rangle = e^{i\varphi_{||}}|E_{1||}\rangle$. Действительно, из-за двумерности пространства состояний векторы $|E'_{1\perp}\rangle$ и $|E'_{1||}\rangle$ могут быть разложены по базисным векторам $|E_{1\perp}\rangle$ и $|E_{1||}\rangle$, в результате имеем

$$|E'_{1||}\rangle = \gamma|E_{1\perp}\rangle + \lambda|E_{1||}\rangle, \quad |\gamma|^2 + |\lambda|^2 = 1,$$

и аналогично для $|E'_{1\perp}\rangle$. Тогда равенство нулю отсчета на детекторе CD2 означает, что $\lambda = 0$, так как

$$|\langle E'_{1||}|\hat{U}^{PC1}_{down}(\perp)|E_{in}\rangle|^2 = 0,$$

и из $|\gamma|^2 + |\lambda|^2 = 1$ сразу следует, что $\gamma = e^{i\varphi_\perp}$; аналогично для $\lambda$.

Соответственно, для матрицы перехода имеем

$$\hat{U}^{PC1}_{down}(\perp) = \hat{U}^{PC2}(\perp)\hat{U}^{PC1MZ}_{down}(\perp) = e^{i\varphi_\perp}|E_{1\perp}\rangle\langle E_{in}| + e^{i\varphi_{||}}|E_{1||}\rangle\langle E^\perp_{in}|. \quad (20)$$

При этом отсчет на детекторе CD2 для состояний, прошедших по пути down, также отсутствует:

$$|\langle E_{1||}|\hat{U}^{PC1}_{down}(\perp)|E_{in}\rangle|^2 = |\langle E_{1||}|E_\perp\rangle|^2 = 0. \quad (21)$$

*Шаг 3. Используя контроллер поляризации PC2, при фиксированном положении PC1 добиваемся максимального сигнала на детекторе CD2 от состояний, прошедших по путям up и down в интерферометре.*

После шагов 1 и 2 состояния up и down одинаковы (с точностью до фазового множителя) и ортогональны направлению ||. Теперь вращение поляризации при помощи PC2 действует одинаково на оба состояния. Фактически теперь контроллер поляризации PC2 переводит состояния $|E_{1\perp}\rangle$ перед фазовым модулятором в состояния $|E_{1||}\rangle$, отвечающие максимуму измеряемой интенсивности на детекторе CD2. Имеем для состояний, прошедших по пути up:

$$\hat{U}^{PC2}_{up}(||) = \hat{U}^{PC2}(||)\hat{U}^{MZ}_{up} = |E_{1||}\rangle\langle E_{in}| + |E_{1\perp}\rangle\langle E^\perp_{in}|. \quad (22)$$

Найдем теперь

$$\hat{U}^{PC2}_{down}(||) = \hat{U}^{PC2}(||)\hat{U}^{PC1MZ}_{down}(\perp),$$

при этом положение PC1 остается фиксированным с предыдущего шага 2. Для этого потребуется знать матрицы $\hat{U}^{PC2}(||)$, $\hat{U}^{PC1MZ}_{down}(\perp)$ и $\hat{U}^{MZ}_{up}$.

Действительно, пусть унитарный оператор $\hat{U}^{MZ}_{up}$ имеет вид

$$\hat{U}^{MZ}_{up} = |\overline{E}_\perp\rangle\langle E_{in}| + |\overline{E}_{||}\rangle\langle E^\perp_{in}|, \quad (23)$$

где $|\overline{E}_{||}\rangle$ и $|\overline{E}_\perp\rangle$ — некоторые промежуточные ортогональные состояния, в которые преобразуются состояния $|E_{in}\rangle$ и $|E^\perp_{in}\rangle$ при прохождении по верхнему пути MZ до PC2. Тогда для унитарного оператора, отвечающего за эволюцию состояний при прохождении PC2, из (17) находим

$$\begin{aligned}\hat{U}^{PC2}(\perp) &= |E_{1\perp}\rangle\langle\overline{E}_\perp| + |E_{1||}\rangle\langle\overline{E}_{||}|,\\ \hat{U}^{PC2}(||) &= |E_{1||}\rangle\langle\overline{E}_\perp| + |E_{1\perp}\rangle\langle\overline{E}_{||}|.\end{aligned} \quad (24)$$

С учетом (22)–(24) для $\hat{U}^{PC1MZ}_{down}(\perp)$ из (19) получаем

$$\hat{U}^{PC1MZ}_{down}(\perp) = \left(\hat{U}^{PC2}(\perp)\right)^{-1}\hat{U}^{PC2}_{down}(\perp) = e^{i\varphi_\perp}|\overline{E}_\perp\rangle\langle E_{in}| + e^{i\varphi_{||}}|\overline{E}_{||}\rangle\langle E^\perp_{in}|. \quad (25)$$

Окончательно, учитывая (25), находим

$$\hat{U}^{PC2}_{down}(||) = \hat{U}^{PC2}(||)\hat{U}^{PC1MZ}_{down}(\perp) = e^{i\varphi_\perp}|E_{1||}\rangle\langle E_{in}| + e^{i\varphi_{||}}|E_{1\perp}\rangle\langle E^\perp_{in}|. \quad (26)$$

После фазового модулятора в канал связи в разных временны́х окнах выйдут, с точностью до фазового множителя, одинаковые состояния

$$\begin{aligned}|E_{1||}\rangle &= \hat{U}^{PC2}_{up}(||)|E_{in}\rangle,\\ e^{i\varphi_\perp}|E_{1||}\rangle &= \hat{U}^{PC2}_{down}(||)|E_{in}\rangle.\end{aligned} \quad (27)$$

*Шаг 4. Дальнейшая эволюция состояний через канал связи является одинаковой*:

$$\begin{aligned}&\hat{U}^{Mir}\hat{U}^{PC3}\hat{U}_{ch}|E_{1||}\rangle,\\ &\hat{U}^{Mir}\hat{U}^{PC3}\hat{U}_{ch}e^{i\varphi_\perp}|E_{1||}\rangle.\end{aligned} \quad (28)$$

После прохождения канала состояния поступают на фазовый модулятор PM2, где происходит изменение относительной фазы состояний, локализованных в разных временны́х окнах. На фазовый модулятор прикладывается напряжение только во время прохождения состояния, прошедшего по пути up. Оператор, действующий на состояние up, имеет вид

$$\hat{U}^{PM2}_{up} = e^{i\varphi_B}|E_{2||}\rangle\langle E_{2||}|, \quad (29)$$

где $|E_{2||}\rangle$ — состояние поляризации, параллельное оси пропускания PM2. Соответственно на состояние down напряжение не прикладывается, и фазовый множитель отсутствует:

$$\hat{U}^{PM2}_{down} = |E_{2||}\rangle\langle E_{2||}|. \quad (30)$$

Обратно в канал выходят состояния (с точностью до нормировки)

$$e^{i\varphi_B}|E_{2||}\rangle \leftarrow \hat{U}_{up}^{PM2}\hat{U}^{Mir}\hat{U}^{PC3}\hat{U}_{ch}|E_{1||}\rangle, \qquad (31)$$

$$e^{i\varphi_\perp}|E_{2||}\rangle \leftarrow \hat{U}_{down}^{PM2}\hat{U}^{Mir}\hat{U}^{PC3}\hat{U}_{ch}e^{i\varphi_\perp}|E_{1||}\rangle. \qquad (32)$$

Обратная эволюция через канал дается транспонированными матрицами. При обратном прохождении на фазовый модулятор PM1 подается напряжение и изменяется фаза только второго (down) состояния:

$$\begin{aligned}\hat{U}_{down}^{PM1} &= e^{i\varphi_A}|E_{1||}\rangle\langle E_{1||}|,\\ \hat{U}_{up}^{PM1} &= |E_{1||}\rangle\langle E_{1||}|.\end{aligned} \qquad (33)$$

Состояния на выходе PM1 с точностью до нормировки есть

$$e^{i\varphi_B}|E_{1||}\rangle \leftarrow \hat{U}_{up}^{PM1}\left(\hat{U}_{ch}\right)^T \times \times \left(\hat{U}^{PC3}\right)^T\left(e^{i\varphi_B}|E_{2||}\rangle\right) \qquad (34)$$

и соответственно

$$e^{i\varphi_A}e^{i\varphi_\perp}|E_{1||}\rangle \leftarrow \hat{U}_{down}^{PM1}\left(\hat{U}_{ch}\right)^T \times \times \left(\hat{U}^{PC3}\right)^T\left(e^{i\varphi_\perp}|E_{2||}\rangle\right). \qquad (35)$$

*Шаг 5. Обратная эволюция через интерферометр MZ описывается матрицами*

$$\left(\hat{U}_{up}^{PC2}(||)\right)^T = \left(\hat{U}^{PC2}(||)\hat{U}_{up}^{MZ}\right)^T = = |E_{in}^*\rangle\langle E_{1||}^*| + |E_{in}^{\perp *}\rangle\langle E_{1\perp}^*|, \qquad (36)$$

$$\left(\hat{U}_{down}^{PC2}(||)\right)^T = \left(\hat{U}^{PC2}(||)\hat{U}_{down}^{MZ}\right)^T = = e^{i\varphi_\perp}|E_{in}^*\rangle\langle E_{1||}^*| + e^{i\varphi_{||}}|E_{in}^{\perp *}\rangle\langle E_{1\perp}^*|, \qquad (37)$$

где введены обозначения

$$|E\rangle = \alpha|0\rangle + \beta|1\rangle \quad \text{и} \quad |E^*\rangle = \alpha^*|0\rangle + \beta^*|1\rangle,$$

$$\langle E| = \alpha^*\langle 0| + \beta^*\langle 1| \quad \text{и} \quad \langle E^*| = \alpha\langle 0| + \beta\langle 1|,$$

$|0\rangle, |1\rangle$ — некоторые базисные векторы. Состояния на входе однофотонного лавинного детектора (APD) имеют вид

$$e^{i\varphi_\perp}\left(e^{i\varphi_A} - e^{i\varphi_B}\right)|E_{in}^*\rangle \leftarrow \left(\hat{U}_{up}^{PC2}(||)\right)^T \times \times \left(e^{i\varphi_A}e^{i\varphi_\perp}|E_{1||}\rangle\right) - \left(\hat{U}_{down}^{PC2}(||)\right)^T \times \times \left(e^{i\varphi_B}e^{i\varphi_\perp}|E_{1||}\rangle\right). \qquad (38)$$

При записи (38) было учтено, что $\langle E_{1\perp}^*|E_{1||}\rangle = 0$. Действительно, поскольку пара векторов $\{|E_{1||}\rangle, |E_{1\perp}\rangle\}$ и $\{|E_{1||}^*\rangle, |E_{1\perp}^*\rangle\}$ представляют собой пары ортонормированных базисных векторов, всегда можно выбрать некоторые базисные векторы $\{|0\rangle, |1\rangle\}$ так, чтобы коэффициенты разложения $\{|E_{1||}\rangle, |E_{1\perp}\rangle\}$ по $\{|0\rangle, |1\rangle\}$ были вещественными, т. е.

$$|E_{1||}\rangle = \cos\alpha|0\rangle + \sin\alpha|1\rangle, \quad |E_{1\perp}\rangle = \sin\alpha|0\rangle - \cos\alpha|1\rangle.$$

При таком выборе имеют место равенства

$$\langle E_{1\perp}^*|E_{1||}\rangle = 0, \quad \langle E_{1||}^*|E_{1||}\rangle = 1,$$

из которых сразу следует (38).

Согласно (38) вероятность детектирования пропорциональна

$$|e^{i\varphi_\perp}\left(e^{i\varphi_A} - e^{i\varphi_B}\right)|^2.$$

При совпадении фаз $\varphi_A = \varphi_B$ отсчеты должны отсутствовать независимо от входного состояния и состояния канала связи. Именно по таким посылкам происходит детектирование вторжения в канал связи. В посылках, в которых $\varphi_A \neq \varphi_B$, вероятность отсчета на лавинном детекторе APD пропорциональна $\sin^2((\varphi_A - \varphi_B)/2)$.

Отметим, что в зависимости от состояния канала темп информационных отсчетов может меняться, но при этом отсчетов в посылках, где $\varphi_A = \varphi_B$, все равно не возникает. Изменения темпа информационных отсчетов эффективно эквивалентно изменению потерь в канале связи, однако для релятивистской квантовой криптографии это не важно, так как изменение потерь не влияет на секретность ключей (см. детали в [2, 3]).

Заметим, что независимость от состояния канала связи может быть достигнута в двухпроходной схеме с использованием фарадеевского зеркала. Это следует из условия

$$\widehat{M}^{FM} = (\hat{U}_{ch})^T\widehat{M}^{FM}\hat{U}_{ch}.$$

Данный факт используется в так называемых системах «plug&play» [7, 8], однако это обстоятельство не освобождает от балансировки интерферометра с поляризационно-избирательными светоделителями.

## 5. ЭКСПЕРИМЕНТАЛЬНЫЕ ДАННЫЕ

Для экспериментального подтверждения двух приведенных решений была собрана установка, соответствующая схеме рис. 1. В ней использовался

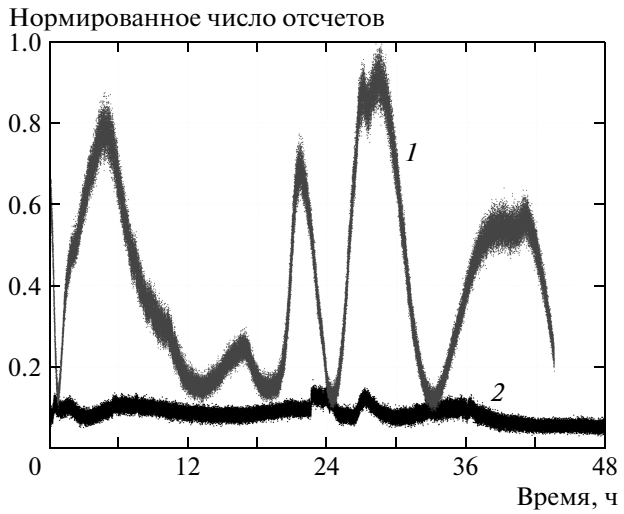


**Рис. 3.** Долговременное измерение интенсивности центрального (интерференционного) пика в схеме без поляризационно-избирательных элементов (рис. 1). Разбалансированный интерферометр (*1*) не обладает долговременной стабильностью из-за различия преобразований $\hat{U}_{up}^{MZ}$ и $\hat{U}_{down}^{MZ}$ в его плечах. После уравнивания преобразований в плечах и сохранении тех же условий эксперимента наблюдается стабильная деструктивная интерференция (*2*), которая не зависит от входного состояния и состояния канала связи

волоконный интерферометр с задержкой 23 нс и три контроллера поляризации для настройки одного из каналов интерферометра, входной поляризации и состояния канала. В качестве канала связи использовалось как открытое пространство с расстоянием передачи в несколько метров, так и одномодовые волокна с длинами от 100 м до нескольких километров. Измерения проводились с помощью стробируемого счетчика фотонов на базе полупроводникового лавинного фотодетектора с длительностью строба 8 нс. Для измерения пропускания интерферометра использовался полупроводниковый лазер с длиной волны 850 нм, генерирующий импульсы длительностью около 4 нс с частотой 125 кГц.

Оптическая установка для проверки решения 1 не включала в себя фазовые модуляторы и, таким образом, не содержала никаких поляризационно-избирательных элементов, что позволило исследовать поведение системы в наиболее общем виде. В первой серии измерений интерферометр был настроен на деструктивную интерференцию в центральном временно́м окне (отсчеты как функция времени показаны на рис. 3 (кривая *2*)). Кривая *1* на рис. 3 отвечает отсчетам в случае, когда интерферометр не был сбалансирован. Точнее говоря, интерферометр в короткий текущий интервал времени был настроен так, чтобы имела место деструктивная интерференция при заданном состоянии канала и заданном входном состоянии лазера (на рис. 3 момент времени близкий к нулю). Однако при этом $\hat{U}_{up}^{MZ} \neq \hat{U}_{down}^{MZ}$. Как видно из рис. 3, в этом случае из-за изменений состояний канала происходит разрушение деструктивной долговременной стабильности интерференции[5)].

Без изменения условий эксперимента интерферометр с помощью итерационной процедуры был перестроен в такое состояние, при котором $\hat{U}_{up}^{MZ} = \hat{U}_{down}^{MZ}$ (с точностью до общего несущественного фазового множителя перед $\hat{U}_{down}^{MZ}$). В этом случае, как видно из рис. 3 (кривая *2*), имеет место долговременная и стабильная деструктивная интерференция, которая не зависит от изменения состояния канала связи. Эксперимент подтверждает возможность, показанную выше теоретически, длительной стабильной деструктивной интерференции, которая имеет место только при условии точного равенства поляризационных преобразований в обоих плечах интерферометра. Настроенный таким образом интерферометр обладал хорошей стабильностью и показал сохранение деструктивной интерференции на протяжении более двух суток (см. рис. 3, кривая *2*).

Для иллюстрации решения 2 в схему были добавлены, как показано на рис. 2, поляризационно-избирательные элементы — электрооптические фазовые модуляторы на основе ниобата лития, являющиеся поляризационными фильтрами. Процедура настройки соответствовала описанной последовательности шагов с использованием классического детектора CD2. После такой настройки на лавинном фотодетекторе в центральном пике наблюдалась деструктивная интерференция, отсутствие сигнала по сравнению с боковыми пиками, которые не зависят от интерференции. Для подтверждения неизменности деструктивной интерференции при изменении параметров канала использовался третий контроллер поляризации PC3, который выполнял в данном случае роль скремблера. При изменении состояния PC3 амплитуда боковых пиков (кривая *1*) изменялась из-за относительного смещения поляризационных осей двух модуляторов, приводящего к модуляции сигнала в канале связи. Однако амплитуда центрального интерференционного пика (кривая *2*) оставалась нулевой и, таким образом, контраст ин-

[5)] При этом, конечно, поддерживается термостабильность самого интерферометра.

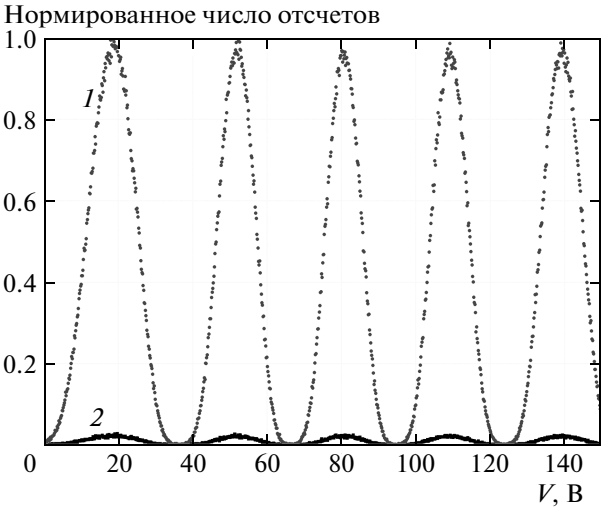


**Рис. 4.** Нормированная интенсивность боковых пиков (*1*) и интерференционного пика (*2*) при изменении состояния канала с помощью контроллера поляризации PC3 (см. рис. 2). V — напряжение, поданное на один из каналов пьезоэлектрического контроллера поляризации; изменению фазы между ортогональными поляризационными компонентами на $\pi$ соответствует напряжение около 16.5 В. Видно сохранение деструктивной интерференции при любом состоянии канала связи

терференции сохранялся (см. рис. 4) в полном соответствии с теоретическими выкладками, представленными выше. Отметим, что при конструктивной интерференции отношение площадей центрального и боковых пиков составляло четыре единицы, что отвечает почти 100 %-й видности. Отношение глубины модуляции (рис. 4) сигнала в центральном временно́м окне к глубине модуляции сигнала в боковых временны́х окнах составляло приблизительно 1/150. Небольшая модуляция в окрестности нуля в центральном временно́м окне связана с неидеальностью фазового модулятора как поляризационного фильтра.

## 6. ЗАКЛЮЧЕНИЕ

Таким образом, предложена оптическая схема, обеспечивающая стабильность деструктивной интерференции и, соответственно, отсутствие ошибок независимо от входного состояния и состояния квантового канала связи. Для практических применений в системах квантовой криптографии принципиально важно, что схема позволяет осуществлять простую автоматическую подстройку.

Один из авторов (С. Н. М) выражает благодарность Д. А. Кронбергу за полезные обсуждения. Работа поддержана грантами Министерства образования и науки РФ (госконтракт № 11.519.11.4009), РФФИ (гранты №№ 12-02-31792, 11-02-00455, 10-02-00204).

## ЛИТЕРАТУРА

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

2. С. Н. Молотков, ЖЭТФ **139**, 429 (2011).

3. С. Н. Молотков, Письма в ЖЭТФ **94**, 504 (2011).

4. C. Tsao, *Optical Fibre Waveguide Analysis*, Oxford Sci. Publ., Oxford (1992).

5. E. Brinkmeyer, Opt. Lett. **6**, 575 (1981).

6. A. Mecozzi and C. Antonelli, J. Lightwave Techn. **29**, 642 (2011).

7. D. S. Bethune and W. P. Risk, New J. Phys. **4**, 42.1 (2002).

8. A. Müller, T. Herzog, B. Hüttner, W. Tittel, H. Zbinden, and N. Gisin, Appl. Phys. Lett. **70**, 793 (1997).