Письма в ЖЭТФ, том 98, вып. 10, с. 700 – 706

Метод балансировки волоконно-оптических интерферометров Маха–Цандера в однопроходной квантовой криптографии

С. П. Кулик[+], *С. Н. Молотков, Т. А. Потапова*[*]

[+]*Физический факультет МГУ им. Ломоносова, 119899 Москва, Россия*

Институт физики твердого тела РАН, 142432 Черноголовка, Россия

Академия криптографии РФ, 103025 Москва, Россия

Факультет вычислительной математики и кибернетики, МГУ им. Ломоносова, 119899 Москва, Россия

[*]*Факультет информационных технологий и вычислительной техники,*
Национальный исследовательский университет "Высшая школа экономики", 109028 Москва, Россия

Поступила в редакцию 19 сентября 2013 г.

Предлагается метод распределенной балансировки для однопроходных систем квантовой криптографии с фазовым кодированием. Данный метод позволяет проводить полностью автоматическую балансировку, является достаточно универсальным и может быть использован в других оптических экспериментах.

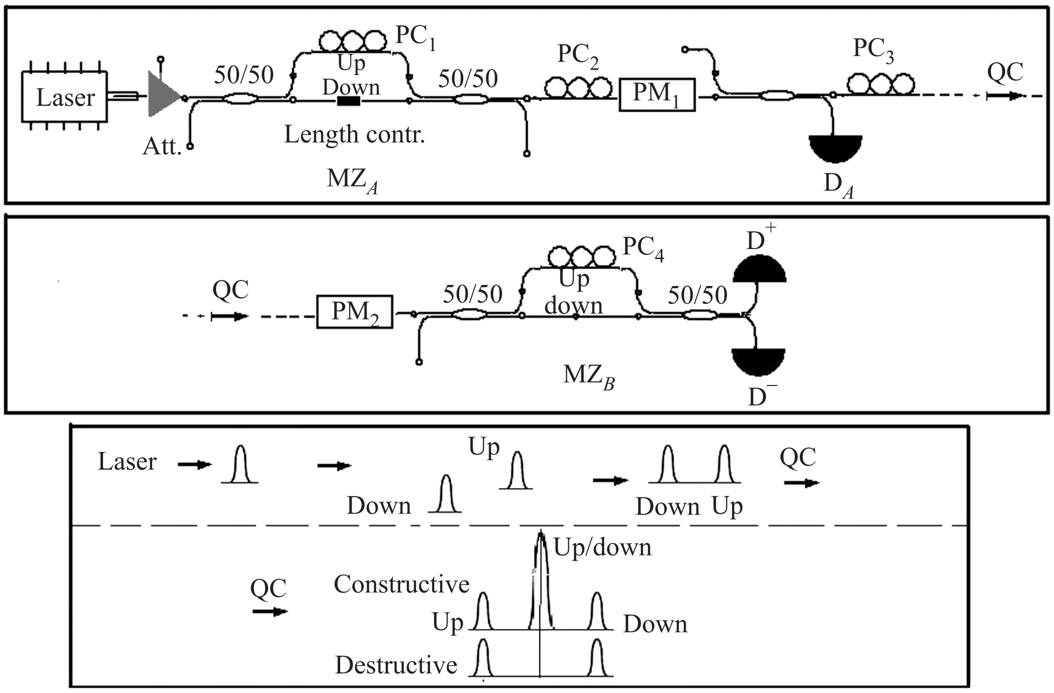
DOI: 10.7868/S0370274X13220098

Введение. Квантовая криптография гарантирует безусловную секретность передаваемых ключей до тех пор, пока наблюдаемая ошибка на приемной стороне не превышает некоторой критической величины. Последняя является фундаментальной величиной для каждого протокола распределения ключей. Если ошибка превышает критическое значение, то нельзя гарантировать секретность ключей. При этом принципиально невозможно отличить ошибку, порождаемую собственными несовершенствами аппаратуры, от ошибки, возникающей от вторжения в канал связи. В квантовой криптографии одним из широко используемых методов является метод фазового кодирования. В этом методе при передаче ключей используется интерференционный принцип в распределенной системе. Для передачи секретных ключей принципиально важным является обеспечение стабильной интерференции, поскольку стабильность интерференционной картины (видность интерференции), напрямую связана с потоком ошибок на приемной стороне (см., например, [1]).

При фазовом кодировании биты ключа кодируются в относительную разность фаз φ (см. [1]). В случае строго однофотонного состояния они кодируются в относительную разность фаз двух "половинок" ($|1\rangle$ и $|2\rangle$) единого квантового состояния, локализованных в разных временных окнах 1 и 2: $|\psi\rangle = (|1\rangle + e^{i\varphi}|2\rangle)/\sqrt{2}$. В случае квазиоднофотонного сильно ослабленного когерентного состояния биты ключа кодируются в относительную разность фаз двух квазиоднофотонных пакетов, локализованных в двух временных окнах: $|\psi_\alpha\rangle = |\alpha_1\rangle \otimes |e^{i\varphi}\alpha_2\rangle$ (где $|\alpha_{1,2}\rangle$ – ослабленные когерентные состояния в двух временных окнах, 1 и 2, $|\alpha_{1,2}|^2 \ll 1$ – среднее число фотонов).

На передающей стороне данная пара состояний получается из одного состояния при помощи волоконного интерферометра Маха–Цандера с разной длиной плеч (см. рисунок). Относительная разность фаз изменяется во время прохождения через фазовый модулятор, который активируется в нужном временном окне (1 или 2). На приемной стороне относительная разность фаз компенсируется аналогичным фазовым модулятором. Состояния, разделенные во времени, "собираются" вместе при помощи точно такого же интерферометра Маха–Цандера. Это дает либо конструктивную интерференцию (в верхнем или нижнем детекторе), либо деструктивную (в нижнем или верхнем детекторе) в центральном временном окне (см. рисунок).

При реализации данного метода используются как однопроходные, так и двухпроходные оптические схемы [2, 3]. Каждый тип систем имеет свои преимущества и недостатки. В двухпроходных схемах проще добиться стабильной интерференции. Однако при этом такие схемы более уязвимы с криптографической точки зрения, поскольку они требуют дополнительного контроля интенсивности лазерных импуль-



Волоконно-оптическая схема однопроходной системы квантовой криптографии с фазовым кодированием

сов на прямом и обратном проходе. *Кроме того, двухпроходные схемы существенно уступают однопроходным по скорости распределения секретных ключей.*

В однопроходных схемах в канал посылаются уже ослабленные до квазиоднофотонного уровня состояния.

Для стабильной интерференции требуется постоянная регулировка независимых и, вообще говоря, разных интерферометров на передающей и приемной стороне для их согласования. Каждый раз эта проблема решается индивидуально [1]. Вместе с тем существует регулярный и универсальный метод подстройки интерферометров, который и предлагается в настоящей работе. Кроме того, данный метод позволяет осуществить полностью автоматическую регулировку.

Рассматриваемый метод существенно использует то обстоятельство, что волоконно-оптические фазовые модуляторы являются поляризационно-чувствительными элементами: они пропускают и модулируют только одно состояние поляризации. Этого факта и двумерности пространства состояний поля, связанного с поляризационными степенями свободы, оказывается достаточном для формулировки универсальной автоматической процедуры балансировки интерферометров Маха–Цандера и достижения устойчивой интерференции.

Линейные оптические элементы. Состояния поля (пакетов) могут быть представлены в виде

$$|\mathrm{E}\rangle = \alpha|\mathrm{E}_H\rangle + \beta|\mathrm{E}_V\rangle, \tag{1}$$

где $|\mathrm{E}_{H,V}\rangle$ – базисные состояния поляризации, α, β – комплексные коэффициенты. Если пакеты локализованы в различных временных окнах i ($i = 1, 2, 3$; см. ниже, а также рисунок), будем отмечать этот факт индексами "i": $|E\rangle_i$. Эволюция состояний является унитарной. Поэтому общий вид матрицы оптического преобразования есть матрица группы SU(2) [4, 5]:

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

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 двоякролучепреломление (компоненты с разной поляризацией распространяются 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.

Любой линейный волоконно-оптический элемент в базисе состояний (1) может быть представлен в виде матрицы из группы SU(2) посредством соответствующего выбора параметров φ, δ, θ. Отметим, что далее речь идет о пакетах поля – состояниях, локализованных во временных окнах. Такие состояния представляют собой интеграл по частотному интервалу $\Delta\omega$: $|\alpha_{1,2}\rangle = \int_{\Delta\omega} f(\omega)|\alpha_\omega\rangle d\omega$ – пакет ослабленных когерентных состояний, локализованных во временных окнах с длительностью $\Delta t \approx \approx 1/\Delta\omega$, где $|\alpha_\omega\rangle$ – монохроматическое когерентное состояние, $f(\omega)$ – функция, описывающая форму пакета. Поскольку данный частотный интервал достаточно узок по сравнению с несущей частотой (запас составляет по крайней мере 6 порядков: несущая частота $\approx 10^{15}$ Гц, а длительность импульсов по времени $\approx 10^{-9}$ с, все элементы не имеют частотной дисперсии в таком диапазоне. Поэтому достаточно рассматривать преобразования одной частотной компоненты, по линейности это справедливо для всех частот в пакете.

Матрица преобразования для светоделителя 50/50 имеет вид

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

где $\hat{\mathrm{I}}$ – единичная матрица 2×2.

Матрица преобразования контроллера поляризации. Данный оптический элемент (см. рисунок) позволяет из любого входного состояния получить любое выходное состояние. Матрица преобразования контролера поляризации имеет вид (2), где параметры φ, δ, θ являются электронно-управляемыми, т.е. путем задания трех различных напряжений на контроллере можно получить любые требуемые значения указанных параметров.

Матрица преобразования фазового модулятора. Данный элемент является поляризационно-чувствительным. С точки зрения поляризации матрица преобразований представляет собой проектор – поляризационный фильтр, который пропускает только одно состояние поляризации. Будем обозначать это состояние как $|\mathrm{PM}^{||}\rangle$, а ортогональное ему состояние поляризации – как $|\mathrm{PM}^{\perp}\rangle$. Кроме того, фазовый модулятор позволяет за счет приложения напряжения во время прохождения через него состояния изменить относительную фазу этого состояния на величину φ_{PM}, которая зависит от приложенного напряжения. Имеем в операторном виде $\hat{\mathbf{U}}(\mathrm{PM}) = e^{i\varphi_{\mathrm{PM}}}|\mathrm{PM}^{||}\rangle\langle\mathrm{PM}^{||}|$, а в матричном виде в базисе состояний $\{|\mathrm{PM}^{||}\rangle, |\mathrm{PM}^{\perp}\rangle\}$

$$\hat{\mathbf{U}}(\mathrm{PM}) = \begin{pmatrix} 0 & e^{i\varphi_{\mathrm{PM}}} \\ 0 & 0 \end{pmatrix}. \tag{4}$$

Общая идея автоматической балансировки. Общая идея автоматической балансировки сводится к тому, чтобы на входе в линию связи, т.е. на выходе передающей станции, возникли два одинаковых (с точностью до относительной разности фаз между ними) состояния, сдвинутых во времени. Данная разность фаз определяется только свойствами интерферометра на передающей стороне.

Процесс балансировки состоит из следующих шагов.

1. Открывается аттенюатор (см. рисунок), что увеличивает интенсивность сигнала до величины, достаточной для устойчивого срабатывания классического детектора D_A, но не приводит к ослеплению лавинных детекторов $\mathrm{D}^{\pm}$ на приемной стороне. При помощи контроллера поляризации PC_2, используя три управляющих напряжения, последовательной регулировкой параметров $\varphi_2, \delta_2, \theta_2$ добиваются того, чтобы сигнал от состояния, прошедшего по нижнему пути интерферометра (без контроллера поляризации PC_1), на фотодетекторе D_A был максимальным. Это гарантирует, что поляризация данного состояния параллельна оси пропускания фазового модулятора.

2. Регулируя параметры $\varphi_1, \delta_1, \theta_1$, добиваются того, чтобы состояние, прошедшее по верхнему пути интерферометра, содержащему контроллер поляризации PC_1, давало максимальный сигнал на фотодетекторе D_A. Регулировка первого контроллера не влияет на состояние, которое прошло по нижнему пути.

3. Два предыдущих шага *гарантируют*, что состояния в двух временных окнах, приходящие на фазовый модулятор, имеют одинаковую поляризацию, но могут отличаться на некоторый фазовый множитель.

При прохождении через линию связи состояния в двух временных окнах остаются одинаковыми с точностью до того же самого фазового множителя. Это связано с тем, что состояния локализованы в разных временных окнах, а значит, модулируются независимо.

4. Регулируя параметры PC_3 $(\varphi_3, \delta_3, \theta_3)$, добиваются максимального сигнала в детекторе D^+, где

должна иметь место конструктивная интерференция, если напряжение на фазовых модуляторах отсутствует.

5. Регулировкой контроллера поляризации PC_4 $(\varphi_4, \delta_4, \theta_4)$ в плече интерферометра на приемной стороне добиваются компенсации общего фазового множителя при помощи гашения интерференции в одном из фотодетекторов (нулевой отклик на D^- и максимальный на D^+).

6. Аттенюатор регулируется так, чтобы сигнал, поступающий в линию, отвечал квазиоднофотонному уровню. Путем задания напряжения на фазовых модуляторах PM_1 и PM_2 в соответствии с протоколом происходит передача ключей. Если из-за большой наблюдаемой ошибки ключи передать нельзя, то передача ключей прерывается и процедура повторяется с п. 1).

Реализация балансировки. Преобразования состояния поля в оптической схеме. Приведем по шагам последовательность преобразования полей в оптическом тракте.

При помощи контроллера поляризации PC_2, используя три управляющих напряжения, последовательной регулировкой параметров $\varphi_2, \delta_2, \theta_2$ добиваются того, чтобы сигнал от состояния, прошедшего по нижнему пути интерферометра (без контроллера поляризации PC_1), на фотодетекторе был равен нулю. Это гарантирует, что поляризация данного состояния ортогональна направлению оси фазового модулятора.

Шаг 1. Фазовый модулятор пропускает только одно направление поляризации, фактически выполняя роль поляризационного фильтра. Исходное состояние поля на выходе лазера локализовано во временном окне. Прохождение по двум плечам интерферометра приводит к разделению поля на две компоненты, сдвинутые по времени на величину, равную разности верхнего и нижнего путей интерферометра, деленной на скорость света в волокне.

Трансфер-матрица для верхнего (up) и нижнего (down) путей интерферометра Маха–Цандера (MZ) имеет вид

$$\hat{\mathbf{U}}^A_{\mathrm{up/down}} = \begin{pmatrix} \hat{\mathrm{U}}^A_{\mathrm{up}} & 0 \\ 0 & \hat{\mathrm{U}}^A_{\mathrm{down}} \end{pmatrix}. \qquad (5)$$

Полная трансфер-матрица интерферометра MZ с учетом (3)–(5) равна

$$\hat{\mathbf{U}}^A = \hat{\mathbf{U}}^{(2)}_{50/50} \hat{\mathbf{U}}^A_{\mathrm{up/down}} \cdot \hat{\mathbf{U}}^{(1)}_{50/50}. \qquad (6)$$

Состояния поля на выходе интерферометра в каналах up и down есть

$$|\mathrm{E}^{\mathrm{up}}_{\mathrm{in}}\rangle = \begin{pmatrix} \mathrm{E}^{\mathrm{up}}_H \\ \mathrm{E}^{\mathrm{up}}_V \end{pmatrix}, \quad |\mathrm{E}^{\mathrm{down}}_{\mathrm{in}}\rangle = \begin{pmatrix} \mathrm{E}^{\mathrm{down}}_H \\ \mathrm{E}^{\mathrm{down}}_V \end{pmatrix}, \\ |\hat{\mathbf{E}}^{\mathrm{up/down}}_{\mathrm{in}}\rangle = \begin{pmatrix} |\mathrm{E}^{\mathrm{up}}_{\mathrm{in}}\rangle \\ |\mathrm{E}^{\mathrm{down}}_{\mathrm{in}}\rangle \end{pmatrix}. \qquad (7)$$

Выходное поле в двух каналах

$$|\hat{\mathbf{E}}^{\mathrm{up/down}}_{\mathrm{out}}\rangle = \begin{pmatrix} |\mathrm{E}^{\mathrm{up}}_{\mathrm{out}}\rangle \\ |\mathrm{E}^{\mathrm{down}}_{\mathrm{out}}\rangle \end{pmatrix} = \\ = \frac{1}{2} \begin{pmatrix} (\hat{\mathrm{U}}^A_{\mathrm{up}} \hat{\mathrm{U}}(\mathrm{PC}_1) - \hat{\mathrm{U}}^A_{\mathrm{down}}) \cdot |\, \mathrm{E}^{\mathrm{up}}_{\mathrm{in}}\rangle \\ (\hat{\mathrm{U}}^A_{\mathrm{up}} \hat{\mathrm{U}}(\mathrm{PC}_1) + \hat{\mathrm{U}}^A_{\mathrm{down}}) \cdot |\, \mathrm{E}^{\mathrm{up}}_{\mathrm{in}}\rangle \end{pmatrix}. \qquad (8)$$

Рабочим является верхний выход интерферометра. Его нижний выход – холостой. Матрица эволюции по верхнему пути интерферометра включает в себя как эволюцию по волокну $(\hat{\mathrm{U}}^A_{\mathrm{up}})$, так и управляемую при помощи контроллера поляризации PC_1 эволюцию $(\hat{\mathrm{U}}(\mathrm{PC}_1))$. По нижнему пути происходит только эволюция по волокну $(\hat{\mathrm{U}}^A_{\mathrm{down}})$.

После прохождения контроллера поляризации PC_2 поле приобретает вид

$$\frac{1}{2}\left(|\mathrm{E}\rangle_{\mathrm{up}} - |\, \mathrm{E}\rangle_{\mathrm{down}}\right) = \\ = \frac{1}{2}\left(\hat{\mathrm{U}}_{\mathrm{up}}(\mathrm{PC}_1)|\, \mathrm{E}^{\mathrm{up}}_{\mathrm{in}}\rangle - \hat{\mathrm{U}}_{\mathrm{down}}(\mathrm{PC}_2)|\mathrm{E}^{\mathrm{up}}_{\mathrm{in}}\rangle\right), \qquad (9)$$

$$\hat{\mathrm{U}}_{\mathrm{up}}(\mathrm{PC}_1) = \hat{\mathrm{U}}(\mathrm{PC}_2)\hat{\mathrm{U}}^A_{\mathrm{up}}\hat{\mathrm{U}}(\mathrm{PC}_1), \\ \hat{\mathrm{U}}_{\mathrm{down}}(\mathrm{PC}_2) = \hat{\mathrm{U}}(\mathrm{PC}_2)\hat{\mathrm{U}}^A_{\mathrm{down}}. \qquad (10)$$

Компоненты $|\mathrm{E}\rangle_{\mathrm{up}}$ и $|\mathrm{E}\rangle_{\mathrm{down}}$ отвечают состояниям поля, разделенным интервалом, равным разности длин верхнего и нижнего плеч интерферометра. При этом состояние компоненты поля $|\mathrm{E}\rangle_{\mathrm{down}}$ регулируется только контроллером поляризации PC_2, а состояние компоненты $|\mathrm{E}\rangle_{\mathrm{up}}$ – как PC_2, так и PC_1 (см. (10)).

Контроллер поляризации позволяет перевести любое входное состояние поля в любое заданное выходное состояние поля. Регулировкой напряжением трех параметров контроллера PC_2 в (10) устанавливается состояние поля на выходе PC_2 с состоянием поляризации, *параллельным* оси пропускания фазового модулятора PM_1. Пусть состояния с поляризацией, параллельной оси пропускания, есть $|\mathrm{PM}_1^{||}\rangle$, а с ортогональной – $|\mathrm{PM}_1^{\perp}\rangle$. Напомним, что квантовые состояния $|\mathrm{PM}_1^{||}\rangle$ и $|\mathrm{PM}_1^{\perp}\rangle$ являются не векторами, а направлениями в пространстве состояний, т.е. они определены с точностью до общего фазового множителя перед состояниями. Поэтому данные фазовые множители мы считаем включенными в эти состояния. Однако относительная фаза между состояниями $|\mathrm{PM}_1^{||}\rangle$ и $|\mathrm{PM}_1^{\perp}\rangle$, прошедшими по верхнему (up) пути, и состояниями с такими же направлениями поляризации, прошедшими по нижнему пути, оказывается принципиально важной (см. ниже).

Унитарный оператор может быть представлен в виде

$$\hat{\mathrm{U}}_{\mathrm{down}}(\mathrm{PC}_2) = |\mathrm{PM}_1^{||}\rangle\langle \mathrm{E}_{\mathrm{in}}^{\mathrm{up}}| + |\mathrm{PM}_1^{\perp}\rangle\langle \mathrm{E}_{\mathrm{in}}^{\mathrm{up}\ \perp}|, \quad (11)$$

где $|\mathrm{E}_{\mathrm{in}}^{\mathrm{up}\ ||}\rangle\langle\ \mathrm{E}_{\mathrm{in}}^{\mathrm{up}\ ||}|$ и $|\mathrm{E}_{\mathrm{in}}^{\mathrm{up}\ \perp}\rangle\langle \mathrm{E}_{\mathrm{in}}^{\mathrm{up}\ \perp}|$ – проекторы на ортогональные дополнения полного пространства состояний квантовой системы, $I = |\mathrm{E}_{\mathrm{in}}^{\mathrm{up}\ ||}\rangle\langle\ \mathrm{E}_{\mathrm{in}}^{\mathrm{up}\ ||}| + |\mathrm{E}_{\mathrm{in}}^{\mathrm{up}\ \perp}\rangle\langle\ \mathrm{E}_{\mathrm{in}}^{\mathrm{up}\ \perp}|$ – единичный оператор в этом пространстве. В нашем случае проекторы имеют единичный ранг. В случае общего унитарного преобразования такое представление унитарного оператора также справедливо, но проекторы не будут проекторами единичного ранга.

Шаг 2. При фиксированном состоянии PC_2 в (10) при помощи PC_1 в плече MZ тремя управляющими напряжениями устанавливается такое состояние PC_1, что

$$\hat{\mathrm{U}}_{\mathrm{up}}(\mathrm{PC}_1) = e^{i\varphi_{||}}|\mathrm{PM}_1^{||}\rangle\langle \mathrm{E}_{\mathrm{in}}^{\mathrm{up}}| + e^{i\varphi_{\perp}}|\mathrm{PM}_1^{\perp}\rangle\langle \mathrm{E}_{\mathrm{in}}^{\mathrm{up}\ \perp}|. \quad (12)$$

В этом случае сигнал на фотодетекторе D_A, который пропорционален норме состояния, будет максимальным для состояний во временных окнах, отвечающих двум путям, up и down, прохождения через интерферометр. Выбор управляющих напряжений осуществляется последовательными итерациями до достижения максимального отклика на детекторе во временном окне сначала для состояния, прошедшего по нижнему пути. Затем итерациями управляющих напряжений на PC_1 достигается максимальный отклик фотодетектора во временном окне для состояния, прошедшего по верхнему пути, содержащему контроллер PC_1.

Важно, что *максимальный отклик детектора в каждом из двух временных окон гарантирует, что компоненты состояния в двух временных окнах перед и на выходе фазового модулятора имеют одинаковые направления поляризации. Они могут отличаться только фазовым множителем. Этот факт является следствием структуры операторов* (11) *и* (12), *что само по себе есть следствие двумерности пространства состояний поля* (см. формулу (1)). *В случае пространства большей размерности максимальный отклик детектора не будет гарантировать равенства состояний, прошедших по верхнему и нижнему пути интерферометра, с точностью до фазового множителя. С математической точки зрения данный факт, возможно, и тривиален. Однако он является ключевым для процедуры балансировки. Неучет данного фазового множителя часто приводит к разбалансировке схемы и росту потока ошибок. Данный множитель устраняется на шаге* 5 *при помощи контроллера поляризации* PC_4 *на приемной стороне.*

Шаг 3. После этого шага оба состояния, прошедшие по верхнему и нижнему пути интерферометра, дадут на фотодетекторе D_A максимальный одинаковый по величине отклик, поскольку

$$\begin{gathered} |\mathrm{PM}_1^{||}\rangle = \hat{\mathrm{U}}_{\mathrm{down}}(\mathrm{PC}_2)|\mathrm{E}_{\mathrm{in}}^{\mathrm{up}}\rangle, \\ e^{i\varphi_{||}}|\mathrm{PM}_1\rangle = \hat{\mathrm{U}}_{\mathrm{up}}(\mathrm{PC}_1)|\mathrm{E}_{\mathrm{in}}^{\mathrm{up}}\rangle, \end{gathered} \quad (13)$$

т.е. поляризация обоих состояний в каждом временном окне параллельна оси пропускания фазового модулятора. Фактически сначала, регулируя три напряжения на PC_2, последовательными итерациями добиваются максимального отклика в одном временном окне. Затем также последовательными итерациями трех напряжений PC_1 добиваются максимума сигнала во втором временном окне. После этого гарантируется, что состояния на входе и выходе PM_1 имеют вид (13), т.е. одинаковы с точностью до относительного фазового множителя. (Отметим, что технически удобнее сначала добиться нулевого отклика на фотодетекторе D_A в двух временных окнах, регулируя последовательно PC_2, а потом PC_1, а затем, регулируя PC_2, вывести сигнал в двух временных окнах на детекторе D_A на максимум. Обе процедуры математически эквивалентны, но описание второй требует несколько большего места.)

Шаг 4. Если на фазовый модулятор не подается импульс управляющего напряжения ($\varphi_A = 0$), то он работает как проектор. На стадии передачи ключей при прохождении компоненты состояния (*down*) в определенном временном окне прикладывается импульс управляющего напряжения, который задает определенное значение φ_A:

$$\hat{\mathrm{U}}(\mathrm{PM}_1) = e^{i\varphi_A}|\mathrm{PM}_1^{||}\rangle_{\mathrm{up}\,\mathrm{up}}\langle \mathrm{PM}_1^{||}|. \quad (14)$$

На стадии балансировки интерферометра $\varphi_A = 0$. После фазового модулятора в двух временных окнах в канал выходят одинаковые с точностью до фазового множителя состояния

$$\frac{1}{2}\left(e^{i\varphi_{||}}|\mathrm{PM}_1^{||}\rangle_{\mathrm{up}} - |\mathrm{PM}_1^{||}\rangle_{\mathrm{down}}\right). \quad (15)$$

Затем управляющими напряжениями устанавливается такое состояние PC_3, чтобы при данном состоянии канала поляризационное состояние поля на приемной стороне B было параллельным оси пропускания фазового модулятора PM_2. Имеем

$$\hat{U}(PC_3)_{ch} = \hat{U}_{ch}\hat{U}(PC_3) = |PM_2^{||}\rangle\langle PM_1^{||}|, \quad (16)$$

где унитарный оператор $\hat{U}_{ch}$ описывает эволюцию состояний в квантовом канале связи.

Шаг 5. В процессе балансировки фазовый модулятор PM_2 также неактивен ($\varphi_B = 0$). В процессе передачи ключей в зависимости от используемого протокола в момент прохождения состояния (up) на фазовый модулятор подается импульс управляющего напряжения, который задает значение φ_B:

$$\hat{U}(PM_2) = e^{i\varphi_B}|PM_2^{||}\rangle_{up\,up}\langle PM_2^{||}| + |PM_2^{||}\rangle_{down\,down}\langle PM_2^{||}|. \quad (17)$$

На входе интерферометра на приемной стороне после прохождения PM_2 (если последний неактивен) получается состояние

$$\frac{1}{2}\left(e^{i\varphi_{||}}|PM_2^{||}\rangle_{up} - |PM_2^{||}\rangle_{down}\right). \quad (18)$$

Отметим, что компоненты состояния в двух временных окнах после прохождения канала имеют *одинаковую поляризацию* (15) *и отличаются только относительным фазовым множителем перед компонентой* up, *на который состояние канала не влияет.* Данный фазовый множитель устраняется при помощи контроллера поляризации PC_4 в одном из плеч интерферометра MZ на приемной стороне.

Преобразование поля при прохождении интерферометра на приемной стороне аналогично предыдущему. Поле на входах лавинных фотодетекторов $D^{\pm}$ имеет вид

$$|D^{\pm}\rangle = \frac{1}{4}\left(\hat{U}^B_{up}(PC_4) \pm \hat{U}^B_{down}\right) \times \times \left(e^{i\varphi_{||}}|PM_2^{||}\rangle_{up} - |PM_2^{||}\rangle_{down}\right), \quad (19)$$

где

$$\hat{U}^B_{up}(PC_4) = \hat{U}(PC_4)\hat{U}^B_{up}. \quad (20)$$

Поскольку интерферируют только компоненты поля, прошедшие по путям up/down и down/up, соответственно, на передающей и приемной сторонах, для компонент поля в центральном временном окне (см. рисунок) имеем

$$\hat{U}^B_{up}(PC_4)|PM_2^{||}\rangle_{down} \pm e^{i\varphi_{||}}\hat{U}^B_{down}|PM_2^{||}\rangle_{up}. \quad (21)$$

Выбором управляющих напряжений на контроллере поляризации PC_4 можно добиться того, чтобы

$$\hat{U}^B_{up}(PC_4) = e^{-i\varphi_{||}}|E^{||}\rangle_{down/up\,up}\langle PM_2^{||}| + + e^{-i\varphi_{\perp}}|E^{\perp}\rangle_{down/up\,up}\langle PM_2^{\perp}|, \quad (22)$$

где прошедшее по верхнему пути состояние

$$|E^{||}\rangle_{down/up} = \hat{U}^B_{down}|PM_2^{||}\rangle_{up}. \quad (23)$$

После этого состояния в центральном временном окне на верхнем и нижнем детекторах становятся равными

$$|D^{\pm}\rangle = \frac{1}{2}\left(|E^{||}\rangle_{down/up} \pm |E^{||}\rangle_{up/down}\right). \quad (24)$$

Индексы компонент состояний $|E^{||}\rangle_{down/up}$ и $|E^{||}\rangle_{up/down}$ отражают только эволюцию при прохождении по разным путям на передающей и приемной сторонах. Сами компоненты состояния поля локализованы в одном и том же временном окне и одинаковы, $|E^{||}\rangle_{down/up} = |E^{||}\rangle_{up/down}$.

Отклик на фотодетекторе пропорционален норме вектора (24). Отклик на верхнем и нижнем детекторах в центральном временном окне с точностью до нормировки есть

$$|\langle D^{\pm}|D^{\pm}\rangle|^2 = \begin{cases} 1, & D^+, \\ 0, & D^-. \end{cases} \quad (25)$$

После этого шага балансировка заканчивается. Отметим, что в MZ_A может быть добавлен пъезоэлемент, изменяющий длину одного из плеч (length contr. на рисунке). Данный элемент посредством приложения напряжения в несколько вольт позволяет изменять длину оптического пути в пределах нескольких длин волн для точного совпадения разности хода по верхнему и нижнему пути в двух независимых интерферометрах, MZ_A и MZ_B. После балансировки можно подрегулировать разность хода в MZ_A по максимуму конструктивного пика интерференции на приемной стороне.

Шаг 6. На стадии распределения ключей на фазовые модуляторы подаются импульсы напряжения, что приводит к добавлению фаз φ_A (PM_1) и φ_B (PM_2). Состояние поля в центральном временном окне на входах фотодетекторов

$$|D^{\pm}\rangle = \frac{1}{2}\left(e^{i\varphi_A}|E^{||}\rangle_{down/up} \pm e^{i\varphi_B}|E^{||}\rangle_{up/down}\right). \quad (26)$$

Вероятность фотоотсчета в детекторах оказывается равной

$$\Pr(\pm) \propto \begin{cases} \cos^2(\frac{\varphi_A - \varphi_B}{2}), & D^+, \\ \sin^2(\frac{\varphi_A - \varphi_B}{2}), & D^-. \end{cases} \quad (27)$$

Передача ключей продолжается до тех пор, пока наблюдаемая ошибка не превысит критической величины. В противном случае передача прекращается, мощность лазера выводится на классический уровень и происходит процесс балансировки.

Заключение. Стабильность интерференционной картины (видность) зависит только от стабильности самих интерферометров и не зависит от состояния канала связи. Таким образом, если время стабильности самих интерферометров больше, чем времена, на которых изменяется состояние канала связи, то это изменение не приведет к ухудшению видности и, соответственно, к увеличению потока ошибок на приемной стороне. Изменение состояния канала приводит только к уменьшению темпа отсчетов (из-за рассогласования состояния поляризации с осью пропускания фазового модулятора PM_2), но не к ошибкам. Обеспечить стабильность интерферометров, например температурную и вибрационную, существенно проще, чем стабильность состояния канала связи, который, согласно идеологии квантовой криптографии, может быть модифицирован подслушивателем и никак не контролируется. Единственным параметром, за которым требуется следить легитимным пользователям, является поток ошибок на приемной стороне.

1. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
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. C. Tsao, *Optical Fibre Waveguide Analysis*, Oxford Science Publ. (1992).
5. A. Mecozzi and C. Antonelli, J. Lightwave Techn. **29**, 642 (2011).