Письма в ЖЭТФ, том 99, вып. 12, с. 837 – 842 © 2014 г. 25 июня

О стабилизации "на ходу" видности интерференции в волоконной квантовой криптографии

С. П. Кулик[+1)], *С. Н. Молотков*

[+]*Физический факультет, МГУ им. Ломоносова, 119992 Москва, Россия*

Институт физики твердого тела РАН, 142432 Черноголовка, Россия

Академия криптографии РФ, 121552 Москва, Россия

Факультет вычислительной математики и кибернетики, МГУ им. Ломоносова, 119992 Москва, Россия

Поступила в редакцию 13 мая 2014 г.

Предложен метод стабилизации видности интерференции в волоконной квантовой криптографии. Он позволяет "на ходу" балансировать пространственно разделенные интерферометры, не прерывая передачи ключей.

DOI: 10.7868/S0370274X1412011X

Введение. Стабильность волоконно-оптической части в системах квантовой криптографии играет принципиальную роль [1]. Дело в тот, что протоколы квантового распределения ключей гарантируют секретность передаваемых ключей, только если ошибка в сырых ключах не превышает некоторой критической величины. Данная величина является фундаментальной константой протокола. Принципиально невозможно отличить ошибки на приемной стороне из-за действий подслушивателя от собственных ошибок, возникающих из-за несовершенства аппаратуры (темновых шумов лавинных детекторов, нестабильности волоконной части и т.д.).

Поскольку волокно не "держит" поляризацию, в волоконных системах квантовой криптографии применяют в основном фазовое кодирование, которое, по сути, сводится к использованию интерференционных эффектов. Видность интерференционной картины V напрямую связана с наблюдаемой ошибкой Q на приемной стороне: $Q = (1 - V)/2$. Чем хуже видность, тем больше внутренняя ошибка, обусловленная неидеальностью интерференционной картины. Применение интерференции осуществляется с помощью интерферометров. Приготовление состояний происходит на передающей стороне при помощи одного интерферометра, а детектирование (регистрация интерференционной картины) на приемной стороне при помощи другого интерферометра.

Обычное оптоволокно (SMF-28) имеет (хотя и слабое) двулучепреломление и не сохраняет поляризацию. Это приводит к тому, что фазовое и поляризационное состояния поля зависят от пути в интерферометре. Кроме того, состояние квантового канала в квантовой криптографии изменяется со временем, что также приводит к изменению фазового и поляризационного состояний поля. Даже если обеспечить стабильность и *согласованность* самих интерферометров, то изменение канала связи все равно будет приводить к ошибкам (разрушению идеальной интерференционной картины).

Для решения данной проблемы применялись двухпроходные схемы с самокомпенсацией. Идея схемы заключается в использовании только одного интерферометра на передающей стороне [2, 3]. Проблема состоит в том, что состояние канала постоянно меняется и каждый раз на интерферометр возвращаются разные состояния. Прохождение туда и обратно не приводит к компенсации изменений состояний. Формальная причина этого связана с тем, что если эволюция состояний на прямом проходе описывается некоторой унитарной матрицей U_{ch}, то обратное прохождение (в той же системе координат) описывается транспонированной унитарной матрицей U_{ch}^{T}, поэтому при наличии двулучепреломления их произведение, описывающее эволюцию туда и обратно, не является единичной матрицей: $U_{ch}^{\mathrm{T}} U_{ch} \neq I$ [4, 5]. В работах [2, 3] было предложено использовать на приемной стороне фарадеевское зеркало, которое при отражении перебрасывает компоненты двух ортогональных состояний поляризации между собой. При обратном прохождении линия связи изменения различных компонент поляризации ком-

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

пенсируются. При этом интерференция происходит на том же самом интерферометре, что обеспечивает стабильность интерференции.

В [6] была продемонстрирована двухпроходная схема без использования фарадеевского зеркала с автоматической самокомпенсацией. В дальнейшем схема применялась в демонстрационном варианте релятивисткой квантовой криптографии для открытого пространства [7].

Двухпроходные схемы с фарадеевским зеркалом имеют серьезные недостатки в смысле криптографической стойкости. Таких недостатков лишены однопроходные схемы. Кроме того, в двухпроходных схемах из-за прохождения состояний туда и обратно приходится использовать пакетную передачу, что снижает скорость генерации ключей.

Однопроходные схемы обеспечивают большую скорость генерации ключей, но обладают меньшей оптической стабильностью. В работе [8] была предложена схема с автоматической подстройкой видности. Однако в ней приходится периодически прерывать передачу ключей, увеличивать интенсивность сигнала до классического уровня, балансировать интерферометры, а затем вновь ослаблять интенсивность до квазиоднофотонного уровня для передачи ключей.

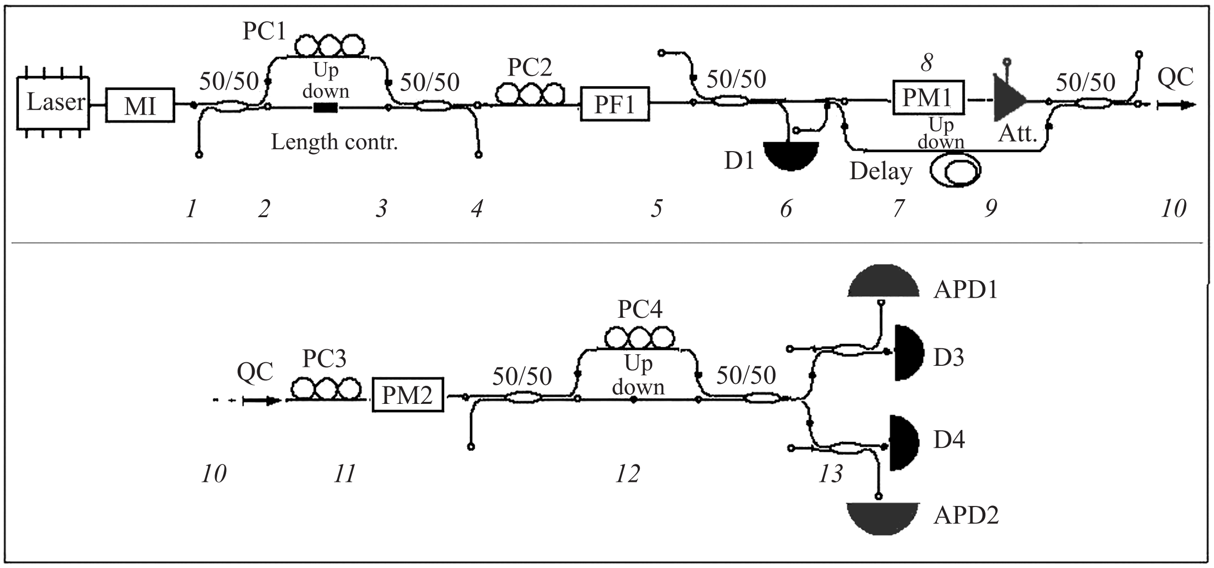
В идеале хотелось бы иметь систему, где балансировка интерферометра происходит перманентно без прерывания передачи ключей и перевода интенсивности лазера в классический режим. В данной работе предложена схема, которая позволяет постоянно подстраивать интерферометры без прерывания передачи ключей.

Идея балансировки "на ходу". Общая идея балансировки видности "на ходу" достаточно проста. В каждом такте передачи (характерные тактовые частоты от 100 кГц до нескольких МГц) из интенсивного классического непрерывного лазерного излучения модулятором интенсивности формируются короткие (порядка наносекунды) импульсы. Далее импульс излучения проходит через интерферометр Маха–Цандера, который формирует пару импульсов, разнесенных во времени на несколько наносекунд. Первая пара импульсов ослабляется до квазиоднофотонного уровня и поступает на фазовый модулятор, на который при прохождении одного из квазиоднофотонных импульсов прикладывается напряжение (кодирование на передающей стороне). Вторая пара интенсивных импульсов отводится в линию задержки. Длина линии задержки превышает расстояние между импульсами (разность хода в плечах интерферометра), но меньше расстояния между импульсами в соседних тактах. В итоге в канал связи поступают две пары импульсов: квазиоднофотонные, несущие информацию о ключе, и интенсивные, используемые для настройки видности.

Обе пары импульсов через канал связи поступают на интерферометр Маха–Цандера на приемной стороне. В момент прихода квазиоднофотонных импульсов при прохождении *только одного из этих квазиоднофотонных импульсов* через фазовый модулятор к нему прикладывается напряжение. Это приводит к изменению относительной фазы между импульсами. Таким образом, происходит декодирование. После прохождения через интерферометр в зависимости от относительной фазы на передающей и приемной стороне происходит либо конструктивная, либо деструктивная интерференция на одном или другом выходе. Состояния на выходе интерферометра через асимметричный светоделитель поступают на классические и однофотонные детекторы, которые активируются только в момент прихода либо интенсивных, либо квазиоднофотонных состояний соответственно. Асимметричный светоделитель нужен для того, чтобы основная часть квазиоднофотонных состояний попадала на лавинные, а не на классические детекторы. Для интенсивных классических сигналов такая асимметрия неважна, т.к. уровня сигнал на классических детекторах достаточно для их работы. Для регистрации сигнала лавинные однофотонные детекторы стробируются только в момент прихода квазиоднофотонных состояний.

Задержанные относительно квазиоднофотонных импульсов интенсивные классические импульсы также проходят через интерферометр. Это приводит к их интерференции, которая регистрируется в момент прихода интенсивных состояний классическими детекторами. Интенсивная пара импульсов не проходит через фазовый модулятор на передающей стороне и не приобретает дополнительной относительной фазы между импульсами. Поэтому интерференция этих импульсов содержит информацию только об относительной фазе, получаемой в плечах двух интерферометров на приемной и передающей стороне. Таким образом, в каждом такте передачи величина сигнала на классических детекторах позволяет сбалансировать (согласовать) разнесенные интерферометры "на ходу", не прерывая передачи ключей.

Эволюция состояний через оптический тракт. Общий вид волоконной части системы приведен на рисунке. Одномодовое состояние излучения лазера описывается когерентным состоянием $|\alpha\rangle$. Ниже речь пойдет о пакетах длительностью порядка наносекунд. При таких длительностях частотная дисперсия не играет роли. Поэтому достаточно



Волоконно-оптическая схема однопроходной системы квантовой криптографии. Верхняя часть относится к передающей станции, нижняя – к приемной. Цифрами на рисунке указаны пункты 1–13 из текста, соответствующие этапам эволюции состояний вдоль оптического тракта. В схеме для выравнивания длин плеч у двух интерферометров на одном из них может использоваться пьезоэлемент (length cotr.)

рассматривать преобразование через линейный оптический тракт для одной моды. Кроме того, для сокращения выкладок и наглядности удобнее рассматривать преобразование амплитуд полей, а не операторов. В таком подходе амплитуда полей, локализованных в разных временных окнах, дается суммой неперекрывающихся амплитуд, а не тензорным произведением. На наш взгляд, это более наглядно и, естественно, не меняет результатов.

1. Общее состояние поля можно представить в виде $|E_{\rm in}\rangle = \alpha|E_H\rangle + \beta|E_V\rangle$, где $|E_{H,V}\rangle$ – базисные состояния поляризации, α, β – комплексные коэффициенты. Состояния на одном из входов Маха-Цандера имеет вид $|\hat{E}_{\rm in}\rangle_1 = \begin{pmatrix} |E_{\rm in}\rangle \\ 0 \end{pmatrix}$. На втором входе (нижний элемент в столбце) поле отсутствует.

2. Матрица симметричного светоделителя имеет стандартный вид: $\hat{U}_{50/50} = \frac{1}{\sqrt{2}}\begin{pmatrix} I & I \\ -I & I \end{pmatrix}$. Состояния поля после светоделителя

$$|\hat{E}\rangle_2 = \hat{U}_{50/50}|\hat{E}_{\rm in}\rangle_1 = \frac{1}{\sqrt{2}}\begin{pmatrix} |E_{\rm in}\rangle \\ |E_{\rm in}\rangle \end{pmatrix}. \qquad (1)$$

3. Эволюция состояний по верхнему и нижнему путям интерферометра дается матрицей $\hat{U}(\mathrm{MZ1}) = \begin{pmatrix} U(\mathrm{PC1})_{\rm up} & 0 \\ 0 & U(\mathrm{MZ1})_{\rm down} \end{pmatrix}$, причем оператор эволюции по верхнему пути включает регулировку состояния контроллером PC1 и задержку (временной сдвиг состояния):

$$|\hat{E}\rangle_3 = \hat{U}(\mathrm{MZ1})|\hat{E}\rangle_2 = = \begin{pmatrix} U(\mathrm{PC1})_{\rm up}|E\rangle_2 & 0 \\ 0 & U(\mathrm{MZ1})_{\rm down}|E\rangle_2 \end{pmatrix} = = \begin{pmatrix} |E\rangle^{\rm up} \\ |E\rangle^{\rm down} \end{pmatrix}. \qquad (2)$$

4. Состояния на выходе второго светоделителя в интерферометре

$$|\hat{E}\rangle_4 = \hat{U}_{50/50}|\hat{E}\rangle_3 = \frac{1}{\sqrt{2}}\begin{pmatrix} |E\rangle_4^{\rm up} + |E\rangle_4^{\rm down} \\ |E\rangle_4^{\rm down} + |E\rangle_4^{\rm up} \end{pmatrix}. \qquad (3)$$

Второй выход светоделителя является холостым. С точностью до нормировки состояния перед контроллером поляризации PC2 имеют вид $\begin{pmatrix} |E\rangle_4^{\rm up} + |E\rangle_4^{\rm down} \\ 0 \end{pmatrix}$.

4. После прохождения через контроллер поляризации $PC2$ состояния становятся равными $|E\rangle_5 = U(\mathrm{PC2})|E\rangle_4^{\rm up} + U(\mathrm{PC2})|E\rangle_4^{\rm down}$. Далее состояния поступают на поляризационный фильтр.

5. Поляризационный фильтр играет роль проектора. Матрица эволюции которого имеет вид (PF1) = $= |E_{||}^{\rm PF1}\rangle\langle E_{||}^{\rm PF1}|$, где $|E_{||}\rangle$ – состояние поля с поляризацией, параллельной оси пропускания фильтра. Состояние поля на выходе фильтра

$$|E\rangle_6 = \langle E_{||}^{\rm PF1}|U({\rm PC2})|E\rangle_4^{\rm up}\cdot|E_{||}^{\rm PF1}\rangle^{\rm up} + \\ + \langle E_{||}^{\rm PF1}|U({\rm PC2})|E\rangle_4^{\rm down}\cdot|E_{||}^{\rm PF1}\rangle^{\rm down}, \qquad (4)$$

где состояния $|E_{||}^{\rm PF1}\rangle^{\rm up}$ и $|E_{||}^{\rm PF1}\rangle^{\rm down}$ одинаковы с точностью до сдвига по времени.

6. Состояния $|E\rangle_6$ с точностью до множителя $1/\sqrt{2}$ оказываются в канале и на фотодетекторе (D_1, см. рисунок). Интенсивности, измеренные во временных окнах "up" и "down", с учетом (4) пропорциональны

$$I_{\rm up} = |^{\rm up}\langle E_{||}^{\rm PF1}|U({\rm PC2})|E\rangle_4^{up}|^2 = \\ = |^{\rm up}\langle E_{||}^{\rm PF1}|U({\rm PC2})\cdot U({\rm PC1})_{\rm up}|E_{\rm in}\rangle|^2, \qquad (5)$$

$$I_{\rm down} = |^{\rm down}\langle E_{||}^{\rm PF1}|U({\rm PC2})|E\rangle_4^{\rm down}|^2 = \\ = |^{\rm down}\langle E_{||}^{\rm PF1}|U({\rm PC2})\cdot U({\rm MZ1})_{\rm down}|E_{\rm in}\rangle|^2. \qquad (6)$$

Контроллер поляризации реализует унитарное преобразование состояния поля самого общего вида, что позволяет любое состояние поля перевести в любое наперед заданное состояние. Формально матрица эволюции PC2 может быть представлена как матрица группы $\mathbf{SU(2)}$. Общий вид матрицы $\mathbf{SU(2)}$ есть

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

Таким образом, регулируя три канала контроллера (параметры φ,δ,θ), можно добиться того, чтобы

$$U({\rm PC2})U_{\rm down}|E_{\rm in}\rangle = |E_{||}^{\rm PF1}\rangle^{\rm down}. \qquad (7)$$

Последнее неформально означает, что состояние, прошедшее по нижнему, короткому пути интерферометра, становится параллельным оси пропускания поляризационного фильтра. При такой ориентации сигнал на фотодетекторе во временном окне состояния "down" максимален. Параметры PC2, регулирующие напряжения, когда сигнал максимален, фиксируются. Далее регулировкой PC1 добиваются того, чтобы сигнал во временном окне для состояния, прошедшего по длинному пути "up", был максимален. Максимум сигнала в этом временном окне означает, что состояние поляризации "up" параллельно оси пропускания поляризационного фильтра:

$$U({\rm PC2})U({\rm PC1})_{\rm up}|e_{\rm in}\rangle = e^{i\varphi}|E_{||}^{\rm PF1}\rangle^{\rm up}. \qquad (8)$$

Важно отметить, что максимум сигналов в двух временных окнах означает, что состояния, прошедшие по верхнему и нижнему пути, параллельны оси пропускания и одинаковы с точностью до относительной фазы φ (см. (5)–(8)). Данная фаза компенсируется при настройке интерферометра на приемной стороне.

7. Теперь в линию задержки и в линию с фазовым модулятором направляются одинаковые состояния

$$\frac{1}{\sqrt{2}}\begin{pmatrix} |E_{||}^{\rm PF1}\rangle^{\rm down} + e^{i\varphi}|E_{||}^{\rm PF1}\rangle^{\rm up} \\ |E_{||}^{\rm PF1}\rangle^{\rm down} + e^{i\varphi}|E_{||}^{\rm PF1}\rangle^{\rm up} \end{pmatrix}. \qquad (9)$$

8. Фазовый модулятор пропускает только состояния с определенной поляризацией, параллельной оси пропускания ($|E_{||}^{\rm PM1}\rangle$). На фазовый модулятор подается короткий импульс напряжения при прохождении состояния в некотором временном окне. Это приводит к изменению относительной фазы состояния. Действие фазового модулятора описывается унитарным оператором

$$U({\rm PM1}) = e^{i\varphi_A}|E_{||}^{\rm PM1}\rangle^{\rm up/down\ \ up/down}\langle E_{||}^{\rm PM1}|. \qquad (10)$$

Здесь индекс "up/down" отражает тот факт, что импульс напряжения может прикладываться либо к состоянию "up", либо к состоянию "down", что приводит к появлению относительной фазы φ_A между этими состояниями.

Состояния на выходе фазового модулятора, поступающие в линию задержки, имеют вид

$$\frac{1}{\sqrt{2}}\begin{pmatrix} |E_{||}^{\rm PM1}\rangle^{\rm down} + e^{i(\varphi+\varphi_A)}|E_{||}^{\rm PM1}\rangle^{\rm up} \\ |E_{||}^{\rm PF1}\rangle^{\rm down} + e^{i\varphi}|E_{||}^{\rm PF1}\rangle^{\rm up} \end{pmatrix}. \qquad (11)$$

9. Пусть операторы эволюции по верхнему и нижнему путям есть $U_{\rm up}^{\rm delay}$ и $U_{\rm down}^{\rm delay}$. Состояния перед светоделителем перед выходом из линии задержки есть

$$\frac{1}{\sqrt{2}}\begin{pmatrix} U_{\rm up}^{\rm delay}\left(|E_{||}^{\rm PM1}\rangle^{\rm down} + e^{i(\varphi+\varphi_A)}|E_{||}^{\rm PM1}\rangle^{\rm up}\right) \\ U_{\rm down}^{delay}\left(|E_{||}^{\rm PF1}\rangle^{\rm down} + e^{i\varphi}|E_{||}^{\rm PF1}\rangle^{\rm up}\right) \end{pmatrix} = \\ = \frac{1}{\sqrt{2}}\begin{pmatrix} |E(\varphi,\varphi_A)\rangle_{\rm delay}^{\rm up} \\ |E(\varphi,\varphi_A)\rangle_{\rm delay}^{\rm down} \end{pmatrix}. \qquad (12)$$

Состояния в верхнем пути проходят через аттенюатор и ослабляются до квазиоднофотонного уровня. В канал связи поступают состояния (с точностью до нормировки) $|E(\varphi,\varphi_A)\rangle_{\rm delay}^{\rm up} + |E(\varphi,\varphi_A)\rangle_{\rm delay}^{\rm down}$.

10. Эволюция состояний в канале (QC, см. рисунок) дается унитарным оператором U_{ch}. Соответственно состояния перед приемной станцией есть $U_{ch}(|E(\varphi,\varphi_A)\rangle_{\rm delay}^{\rm up} + |E(\varphi,\varphi_A)\rangle_{\rm delay}^{\rm down})$. Контроллер поляризации PC3 служит для ориентации квазиоднофотонных информационных состояний

$U_{ch}|E(\varphi,\varphi_A)\rangle^{\rm up}_{\rm delay}$ таким образом, чтобы обеспечить максимальное прохождение через фазовый модулятор PM2, который имеет выделенную ось пропускания $|E^{\rm PM2}_{||}\rangle$. Приводящее к сдвигу относительной фазы напряжение подается на модулятор только в момент прохождения состояния $e^{i(\varphi+\varphi_A)}|E^{\rm PM1}_{||}\rangle^{\rm up}$ (см. (10)–(12)).

11. Регулировка контроллера поляризации приводит к тому, что направление поляризации квазиоднофотонных состояний совпадает с осью фазового модулятора, $U({\rm PC3})U_{ch}\left(|E(\varphi,\varphi_A)\rangle^{\rm up}_{\rm delay}+|E(\varphi,\varphi_A)\rangle^{\rm down}_{\rm delay}\right)$. После выхода фазового модулятора имеем

$$\begin{aligned}&U({\rm PC3})U_{ch}(U^{\rm delay}_{\rm up}(|E^{\rm PM2}_{||}\rangle^{\rm down}+e^{i(\varphi+\varphi_A)}|E^{\rm PM2}_{||}\rangle^{\rm up})+\\&+U^{\rm delay}_{\rm down}(|E^{\rm PM2}_{||}\rangle^{\rm down}+e^{i\varphi}|E^{\rm PM2}_{||}\rangle^{\rm up}))=\\&=|E^{\rm PM2}_{||}\rangle^{\rm down/up}+e^{i(\varphi+\varphi_A+\varphi_B)}|E^{\rm PM2}_{||}\rangle^{\rm up/up}+\\&+a\left(|E^{\rm PM2}_{||}\rangle^{\rm down/down}+e^{i\varphi}|E^{\rm PM2}_{||}\rangle^{\rm up/down}\right),\end{aligned}\qquad(13)$$

где, например,

$$|E^{\rm PM2}_{||}\rangle^{\rm down/up}=U({\rm PC3})U_{ch}U^{\rm delay}_{\rm up}|E^{\rm PM2}_{||}\rangle^{\rm down}.\qquad(14)$$

Здесь индексы “down/up” относятся к состояниям, прошедшим по нижнему пути интерферометра Маха–Цандера на передающей стороне и по нижнему пути по линии задержки. Константа a определяется скалярным произведением интенсивных состояний, прошедших по нижнему пути линии задержки, и состояниями, параллельными оси пропускания фазового модулятора PM2:

$$\begin{aligned}&a=\langle E^{\rm PM2}_{||}|U(PC3)U_{ch}U^{\rm delay}_{\rm down}\times\\&\times\left(|E^{\rm PM2}_{||}\rangle^{\rm down}+e^{i\varphi}|E^{\rm PM2}_{||}\rangle^{\rm up}\right)=\\&=\langle E^{\rm PM2}_{||}|U({\rm PC3})U_{ch}U^{\rm delay}_{\rm down}|E^{\rm PM2}_{||}\rangle^{\rm down}+\\&+\langle E^{\rm PM2}_{||}|U({\rm PC3})U_{ch}U^{\rm delay}_{\rm down}e^{i\varphi}|E^{\rm PM2}_{||}\rangle^{\rm up}.\end{aligned}\qquad(15)$$

12. Эволюция состояний через интерферометр Маха–Цандера на приемной стороне описывается аналогично ситуации на передающей стороне. На двух выходах интерферометра получаем состояния

$$\begin{aligned}&\frac{1}{\sqrt2}\begin{pmatrix}U({\rm PC4})_{\rm up}\left(|E^{\rm PM2}_{||}\rangle^{\rm down/up}+e^{i(\varphi+\varphi_A+\varphi_B)}|E^{\rm PM2}_{||}\rangle^{\rm up/up}+a\left(|E^{\rm PM2}_{||}\rangle^{\rm down/down}+e^{i\varphi}|E^{\rm PM2}_{||}\rangle^{\rm up/down}\right)\right)\\U(MZ2)_{\rm down}\left(|E^{\rm PM2}_{||}\rangle^{\rm down/up}+e^{i(\varphi+\varphi_A+\varphi_B)}|E^{\rm PM2}_{||}\rangle^{\rm up/up}+a\left(|E^{\rm PM2}_{||}\rangle^{\rm down/down}+e^{i\varphi}|E^{\rm PM2}_{||}\rangle^{\rm up/down}\right)\right)\end{pmatrix}+\\&+\frac{1}{\sqrt2}\begin{pmatrix}U({\rm MZ2})_{\rm down}\left(|E^{\rm PM2}_{||}\rangle^{\rm down/up}+e^{i(\varphi+\varphi_A+\varphi_B)}|E^{\rm PM2}_{||}\rangle^{\rm up/up}+a\left(|E^{\rm PM2}_{||}\rangle^{\rm down/down}+e^{i\varphi}|E^{\rm PM2}_{||}\rangle^{\rm up/down}\right)\right)\\-U({\rm PC4})_{\rm up}\left(|E^{\rm PM2}_{||}\rangle^{\rm down/up}+e^{i(\varphi+\varphi_A+\varphi_B)}|E^{\rm PM2}_{||}\rangle^{\rm up/up}+a\left(|E^{\rm PM2}_{||}\rangle^{\rm down/down}+e^{i\varphi}|E^{\rm PM2}_{||}\rangle^{\rm up/down}\right)\right)\end{pmatrix}.\end{aligned}\qquad(16)$$

13. Поскольку интерферируют только те состояния, которые прошли по разным путям в первом интерферометре и по одинаковым путям линии задержки, для квазиоднофотонных информационных состояний имеем

$$\begin{aligned}&U({\rm PC4})_{\rm up}|E^{\rm PM2}_{||}\rangle^{\rm down/up}\pm\\&\pm U({\rm MZ2})_{\rm down}e^{i(\varphi+\varphi_A+\varphi_B)}|E^{\rm PM2}_{||}\rangle^{\rm up/up}.\end{aligned}\qquad(17)$$

Аналогично для интенсивных классических состояний, прошедших по длинному пути линии задержки, имеем

$$\begin{aligned}&a\Big(U({\rm PC4})_{\rm up}|E^{\rm PM2}_{||}\rangle^{\rm down/down}\pm\\&\pm U({\rm MZ2})_{\rm down}e^{i(\varphi)}|E^{\rm PM2}_{||}\rangle^{\rm up/down}\Big).\end{aligned}\qquad(18)$$

Регулируя состояние контроллера поляризации PC4 можно добиться того, чтобы выполнялось

$$\begin{aligned}&U({\rm PC4})_{\rm up}|E^{\rm PM2}_{||}\rangle^{\rm down/down}=\\&=U({\rm MZ2})_{\rm down}e^{i(\varphi)}|E^{\rm PM2}_{||}\rangle^{\rm up/down}.\end{aligned}\qquad(19)$$

Как видно из (17) и (18), структура классических и квазиоднофотонных состояний одинакова (за исключением фазовых множителей $\varphi_{A,B}$, которые кодируют состояния ключа). Интенсивность сигнала на классических фотодетекторах $\rm D_{3,4}$ (см. рисунок) пропорциональна квадрату модуля амплитуды поля во временном окне, отвечающим состояниям, прошедшим по длинному пути линии задержки. В результате имеем

$$I_{\text{clas}}^{\text{up/down}} = |a|^2 \Big| \Big(U(\text{PC4})_{\text{up}} |E_{||}^{\text{PM2}}\rangle^{\text{down/down}} \pm \pm U(\text{MZ2})_{\text{down}} e^{i(\varphi)} |E_{||}^{\text{PM2}}\rangle^{\text{up/down}} \Big) \Big|^2 = \tag{20}$$

$$= |a|^2 \Big| U(\text{PC4})_{\text{up}} |E_{||}^{\text{PM2}}\rangle^{\text{down/down}} \Big|^2 |1 \pm 1|^2 \propto \begin{cases} \text{max}; \\ 0. \end{cases}$$

В данном случае на верхнем классическом детекторе будет наблюдаться максимум сигнала в этом временном окне и/или его отсутствие (нулевой сигнал на нижнем детекторе). С учетом (17) сигнал (отсчеты) на лавинных однофотонных детекторах ($\text{APD}_{1,2}$) в соответствующем временном окне будет иметь место, с вероятностью

$$\text{Pr}_{\text{APD}}^{\text{up/down}} = |U(\text{PC4})_{\text{up}} |E_{||}^{\text{PM2}}\rangle^{\text{down/up}}|^2 |1 \pm e^{i(\varphi_A + \varphi_B)}|^2, \tag{21}$$

что и требуется протоколом: вероятность отсчета в лавинных детекторах зависит только от общей относительной фазы, заданной на приемной и передающей стороне.

Заключительные замечания. Итак, предложенный метод позволяет балансировать как интерферометр на передающей станции, так и, согласованно с ним, интерферометр на приемной станции, не прерывая передачи ключей. На передающей станции балансировка сводится к поддержанию максимального уровня сигнала на классическом фотодетекторе посредством измерения интенсивности в двух временных окнах, отвечающих сигналу, прошедшему по верхнему и нижнему путям интерферометра. Максимум сигнала гарантирует одинаковость сдвинутых по времени состояний с точностью до общего фазового множителя. Данный множитель относительной ‘фазы “проносится” состояниями через весь оптический тракт. Разделение состояний с помощью линии задержки сохраняет данный фазовый множитель как в квазиоднофотонных, так и в интенсивных состояниях. Хотя сами состояния оказываются разными, поскольку проходят разные оптические пути. Однако при приходе на приемную станцию из-за прохождения через фазовый модулятор, играющий также роль поляризационного фильтра, пары классических и квазиоднофотонных состояний приобретают одинаковую поляризационную структуру и имеют *общую и одинаковую относительную фазу*. Измерение сигнала во временном окне, отвечающем классическим состояниям, позволяет устранить указанный фазовый множитель посредством регулировки контроллером поляризации. Такую регулировку можно осуществлять итерационно в каждом такте, не прерывая передачу ключей. Изменение состояния канала может приводить к изменению темпа отсчета, но не к ошибкам детектирования.

Лавинные однофотонные детекторы стробируются только в момент прихода квазиоднофотонных состояний. Это позволяет избежать их засветки “остаточным” излучением от классического сигнала, разнесенного во времени с квазиоднофотонными состояниями. Отметим, что для избежания засветок лавинных детекторов принципиально важно обеспечить достаточную глубину амплитудной модуляции (запирание модулятора интенсивности) для того, чтобы предотвратить проникновение в оптический тракт постоянной компоненты излучения CW-лазера между импульсами света.

Отметим также, что от контроллеров поляризации (кроме PC3) можно избавиться, если использовать сохраняющие поляризацию волокна и светоделители.

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).
6. К. С. Кравцов, И. В. Радченко, А. В. Корольков, С. П. Кулик, С. Н. Молотков, ЖЭТФ **143**, 820 (2013).
7. I. V. Radchenko, K. S. Kravtsov, S. P. Kulik, and S. N. Molotkov, Las. Phys. Lett. **11**, 065203 (2014); arXiv/quant-ph/1403.3122.
8. С. П. Кулик, С. Н. Молотков, Т. А. Потапова, Письма в ЖЭТФ **98**, 700 (2013).