РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2 665 249**(13) **C1**

(51) МПК
H04L 9/08 (2006.01)
G06F 21/72 (2013.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК
***H04L 9/08** (2006.01); **G06F 21/72** (2006.01)*

(21)(22) Заявка: **2017144533, 19.12.2017**

(24) Дата начала отсчета срока действия патента:
19.12.2017

Дата регистрации:
28.08.2018

Приоритет(ы):
(22) Дата подачи заявки: **19.12.2017**

(45) Опубликовано: **28.08.2018** Бюл. № **25**

Адрес для переписки:
127287, Москва, Старый Петровско-Разумовский пр-д, 1/23, стр. 1, Открытое акционерное общество "Информационные технологии и коммуникационные системы"

(72) Автор(ы):
Балыгин Кирилл Алексеевич (RU),
Зайцев Владимир Иванович (RU),
Климов Андрей Николаевич (RU),
Кулик Сергей Павлович (RU),
Молотков Сергей Николаевич (RU)

(73) Патентообладатель(и):
Открытое акционерное общество "Информационные технологии и коммуникационные системы" (RU)

(56) Список документов, цитированных в отчете о поиске: **RU 2622985 C1, 21.06.2017. RU 2507690 C1, 20.02.2014. RU 2015141966 A, 04.04.2017. US 2009/0046857 A1, 19.02.2009.**

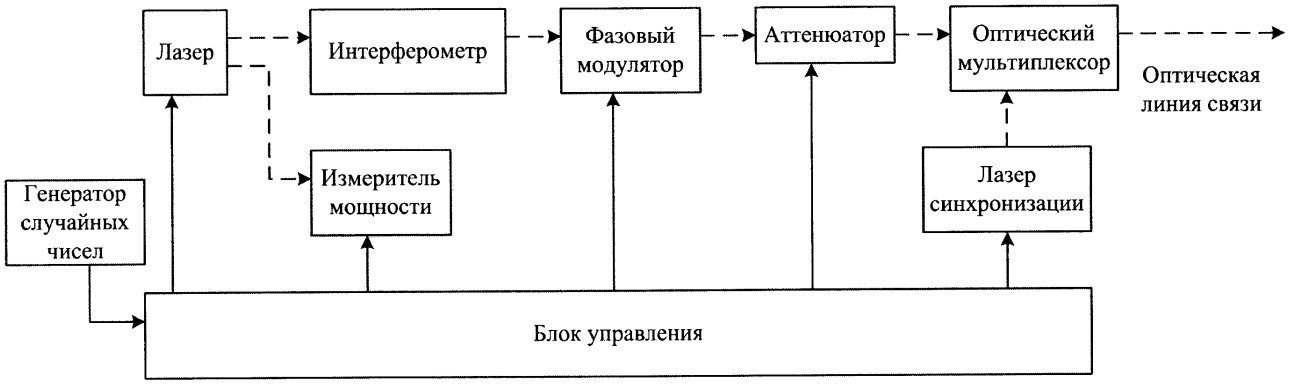
(54) Способ управления интерференционной картиной в однопроходной системе квантовой криптографии

(57) Реферат:

Изобретение относится к области квантовой криптографии. Технический результат – исключение прерывания передачи ключей в режиме квазиоднофотонных состояний для управления интерференционной картиной. Способ заключается в том, что генерируют случайную последовательность нулей и единиц с помощью генератора случайных чисел в передающей части, генерируют на основании последовательности нулей и единиц последовательность квазиоднофотонных состояний в передающей части, разделяют каждое квазиоднофотонное состояние с помощью интерферометра передающей части на пару пространственно разнесенных квазиоднофотонных когерентных состояний, передают полученные пространственно разнесенные квазиоднофотонные когерентные состояния из передающей части в принимающую часть с помощью линии связи, принимают пространственно разнесенные квазиоднофотонные когерентные состояния в принимающей части, получают интерференционную картину от пространственно разнесенных квазиоднофотонных когерентных состояний на выходе интерферометра принимающей части, регистрируют последовательность квазиоднофотонных состояний после прохождения интерферометра принимающей части в фотоприемном блоке в виде последовательности нулей и единиц в зависимости от видности полученной интерференционной картины для каждого квазиоднофотонного состояния, определяют сигнал ошибки в блоке обработки принимающей части на основании сравнения принятой и переданной последовательностей нулей и единиц, при этом в качестве сигнала ошибки применяется величина, пропорциональная числу несовпадений в позициях принятой и переданной последовательностей единиц и нулей, и регулируют видность интерференционной картины, полученной на выходе интерферометра принимающей части, посредством компенсации

RU 2665249 C1

относительной разности хода в интерферометре принимающей части на основании принятого сигнала ошибки. 2 ил.



Фиг. 1

RU 2665249 C1

RU 2665249 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 665 249**(13) **C1**

(51) Int. Cl.
H04L 9/08 (2006.01)
G06F 21/72 (2013.01)

(12) ABSTRACT OF INVENTION

(52) CPC
H04L 9/08 (2006.01); G06F 21/72 (2006.01)

(21)(22) Application: **2017144533, 19.12.2017**

(24) Effective date for property rights:
19.12.2017

Registration date:
28.08.2018

Priority:
(22) Date of filing: **19.12.2017**

(45) Date of publication: **28.08.2018** Bull. № **25**

Mail address:
127287, Moskva, Staryj Petrovsko-Razumovskij pr-d, 1/23, str. 1, Otkrytoe aktsionernoe obshchestvo "Informatsionnye tekhnologii i kommunikatsionnye sistemy"

(72) Inventor(s):
Balygin Kirill Alekseevich (RU),
Zajtsev Vladimir Ivanovich (RU),
Klimov Andrej Nikolaevich (RU),
Kulik Sergej Pavlovich (RU),
Molotkov Sergej Nikolaevich (RU)

(73) Proprietor(s):
Otkrytoe aktsionernoe obshchestvo "Informatsionnye tekhnologii i kommunikatsionnye sistemy" (RU)

RU 2665249 C1

(54) CONTROLLING METHOD OF THE INTERFERENCE IMAGE IN A SINGLE-PASS SYSTEM OF QUANTUM CRYPTOGRAPHY

(57) Abstract:

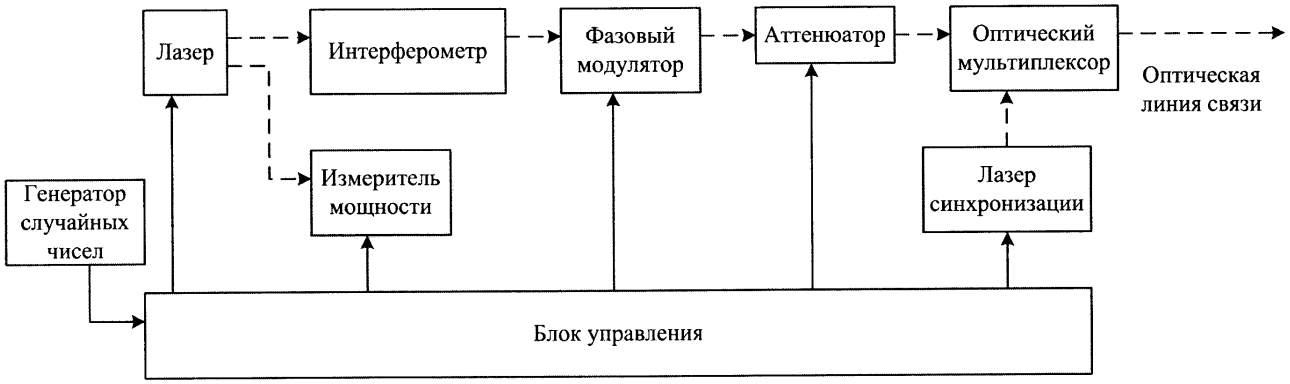
FIELD: cryptography.

SUBSTANCE: invention relates to the field of quantum cryptography. Method consists in generating a random sequence of zeros and ones using a random number generator in the transmitting part, generate on the basis of a sequence of zeros and ones a sequence of quasi-one-photon states in the transmitting part, divide each quasi-one-photon state by means of the interferometer to a pair of spatially separated quasi-one-photon coherent states, transmit the obtained spatially separated quasi-one-photon coherent states from the transmitting part to the receiving part using a communication link, take spatially separated quasi-one-photon coherent states in the receiving part, an interference pattern is obtained from the spatially spaced quasi-one-photon coherent states at the output of the interferometer of the receiving part, register a sequence of quasi-one-photon states after passing the interferometer of the receiving part in the photodetector block in the form of a sequence of zeros and ones depending on the visibility of the obtained interference pattern for each quasi-one-photon state, determining an error signal in the processing unit of the receiving part based on comparing the received and transmitted sequences of zeros and ones, while as the error signal a quantity proportional to the number of mismatches in the positions of the received and transmitted sequences of ones and zeros is applied, and adjust the visibility of the interference pattern obtained at the output of the interferometer of the receiving part by compensating for the relative path difference in the interferometer of the receiving part based on the received error signal.

EFFECT: excluding the interruption of key transfer in the quasi-one-photon state for controlling the interference pattern.

1 cl, 2 dwg

RU 2665249 C1



Фиг. 1

RU 2665249 C1

RU 2665249 C1

Область техники, к которой относится изобретение

Изобретение относится к области квантовой криптографии, а именно, к управлению интерференционной картиной в однопроходной системе квантовой криптографии.

Уровень техники

Цель квантовой криптографии - получение идентичных ключей, представляющих собой последовательность нулей и единиц, на передающей и принимающей частях. Ключи генерируются посредством передачи квазиоднофотонных квантовых состояний из передающей части в принимающую часть. Для достижения этой цели требуется обеспечение стабильной работы оптической части системы с минимальными собственными шумами, приводящими к ошибкам в ключах. Одним из основных источников ошибок в ключах является отклонение интерференционной картины от идеальной.

В настоящем изобретении раскрывается способ обеспечения стабильности волоконной системы квантовой криптографии с фазовым кодированием, т.е. когда биты ключа кодируются в относительную фазу двух когерентных разделенных во времени квазиоднофотонных состояний.

Рассматриваемая система относится к классу однопроходных систем, иными словами, в рассматриваемой системе используется пара разнесенных независимых интерферометров Маха-Цандера на передающей и принимающей сторонах и, видность интерференционной картины, которая определяет уровень собственных ошибок в первичных ключах, зависит от относительной разности хода в двух интерферометрах. Однопроходные система позволяет достигать более высокой скорости генерации ключей, по сравнению с двухпроходными системами, при условии обеспечения «идеальной» видности интерференционной картины, в качестве которой используется величина

$$V = \frac{I_{\max} - I_{\min}}{I_{\max} + I_{\min}},$$

где I_{max} - интенсивность излучения в максимуме интерференционной картины;

I_{min} - интенсивность излучения в минимуме интерференционной картины;

Но использование двух независимых интерферометров в передающей и принимающей частях приводит к существенному снижению стабильности интерференционной картины по сравнению с двухпроходными системами.

На стабильность интерференции влияют изменение длины волны лазера, температура интерферометра, механические вибрации. При этом даже аккуратная термостабилизация интерферометра не позволяет держать постоянной температуру волоконного интерферометра в течение длительного времени.

Температурное изменение оптической длины волокна связано с двумя механизмами: первый связан с изменением непосредственно длины волокна за счет изменения температуры; второй - с изменением показателя преломления за счет температурного изгиба и кручения. Наиболее существенна ошибка от изменения показателя преломления, связанная с изгибом и кручением. Изменение разности температур интерферометров на 0.001° уже приводит к ошибке в 1%. При хорошей пассивной термостабилизации такое изменение происходит за несколько секунд, поэтому требуется постоянная стабилизация видности по ходу генерации ключей.

Известные способы балансировки предполагают прерывание передачи ключей в режиме квазиоднофотонных состояний, перевод системы в классический режим (путем увеличения мощности лазера) и посылку одинаковых состояний для того, чтобы

сбалансировать интерферометр. Классические состояния выбираются так, чтобы сигнал интерференции давал максимальную видность в предположении, что интерферометры идеально сбалансированы. Если интерферометры сбалансированы неидеально, то видность не будет максимальной и отклонение величины видности от максимального значения может быть использовано как сигнал ошибки для регулировки интерферометра принимающей части.

Известен способ управления интерференционной картиной в однопроходной схеме квантовой криптографии (см. «Continuous high speed coherent one-way quantum key distribution)), D. Stucki, C. Barreiro, S. Fasel, J.-D. Gautier, O. Gay, N. Gisin, R. Thew, Y. Thoma, P. Trinkler, F. Vannel, H. Zbinden, Opt. Expr. 17, 13326 (2009)), основанный на регулировке длины волны лазера, которая приводит к изменению фазы при одной и той же разности хода, что, в свою очередь, позволяет добиться высокой видности. Регулировка длины волны лазера обычно происходит за счет изменения тока накачки или температуры лазера. В данном способе измерения происходят на принимающей части, а изменение длины волны лазера на передающей части. Для такой регулировки требуются изменение уровня сигнала с квазиоднофотонного до классического, дополнительное время на проведение измерений и большое число обменов по открытому каналу связи.

Также известен другой способ управления интерференционной картиной в схеме однопроходной схеме квантовой криптографии (см. «Practical long-distance quantum key distribution system using decoy levels», D. Rosenberg, C.G. Peterson, J.W. Harringtonl, P.R. Rice, N. Dallmann, K.T. Tyagi, K.P. McCabe, S. Nam, B. Baek, R.H. Hadfield, R.J. Hughes, J.E. Nordholt, New J. Phys. 11 045009 (2009)), основанный на механическом изменении физической длины одного из плеч интерферометра на принимающей части. Этот способ не требует большого числа обменов по открытому каналу связи, но имеет ряд технических недостатков, связанных с механическим изменением длины одного из плеч интерферометра с использованием пьезоэлемента.

Поскольку у пьезоэлемента присутствует, хоть и незначительный, гистерезис, поэтому необходимо вносить задержки по времени, которые диктуются временем релаксации к положению равновесия пьезоэлемента после приложения напряжения. Кроме того, поскольку изменение длины одного из плеч интерферометра принимающей части происходит за счет механического изменения длины самого пьезоэлемента, то это приводит к механическому износу пьезоэлемента и изменению его свойств. Поэтому при длительной непрерывной работе системы приходится производить дополнительную калибровку зависимости длины пьезоэлемента от приложенного напряжения, что является недостатком известного способа.

Раскрытие изобретения

Техническая проблема, на разрешение которой направлено изобретение, заключается в создании способа, обеспечивающего непрерывную передачу ключей по каналу связи.

Техническим результатом является исключение прерывания передачи ключей в режиме квазиоднофотонных состояний для управления интерференционной картиной за счет компенсации относительной разности хода в интерферометре принимающей части, и минимизации времени, затрачиваемого на эту компенсацию.

Для этого предлагается способ управления интерференционной картиной в однопроходной системе квантовой криптографии, включающей

- передающую часть, содержащую
  - генератор случайных чисел,
  - лазер,
  - интерферометр,

- блок управления;
- принимающую часть, содержащую
  - интерферометр,
  - фотоприемный блок,
  - блок обработки,
  - блок управления;
- линию связи, выполненную в виде одномодового оптического волокна и соединяющую передающую и принимающую части;

способ заключается в том, что

- генерируют случайную последовательность нулей и единиц с помощью генератора случайных чисел в передающей части;
- генерируют на основании последовательности нулей и единиц последовательность квазиоднофотонных состояний в передающей части;
- разделяют каждое квазиоднофотонное состояние с помощью интерферометра передающей части на пару пространственно разнесенных квазиоднофотонных когерентных состояний;
- передают полученные пространственно разнесенные квазиоднофотонные когерентные состояния из передающей части в принимающую часть с помощью линии связи;
- принимают пространственно разнесенные квазиоднофотонные когерентные состояния в принимающей части;
- получают интерференционную картину от пространственно разнесенных квазиоднофотонных когерентных состояний на выходе интерферометра принимающей части;
- регистрируют последовательность квазиоднофотонных состояний после прохождения интерферометра принимающей части в фотоприемном блоке в виде последовательности нулей и единиц, в зависимости от видности полученной интерференционной картины для каждого квазиоднофотонного состояния;
- определяют сигнал ошибки в блоке обработки принимающей части на основании сравнения принятой и переданной последовательностей нулей и единиц, при этом в качестве сигнала ошибки, применяется величина, пропорциональная числу несовпадений в позициях принятой и переданной последовательностей единиц и нулей; и
- регулируют видность интерференционной картины, полученной на выходе интерферометра принимающей части, посредством компенсации относительной разности хода в интерферометре принимающей части на основании принятого сигнала ошибки.

Пусть разность фаз, диктуемая протоколом квантового распределения ключей, равна

$$\Delta\varphi_{AB} = \varphi_A - \varphi_B = \frac{\pi}{2}$$

Тогда вероятность правильной регистрации, т.е. вероятность зарегистрировать на принимающей части 0_B, если с передающей части был послан 0_A, равна

$$\Pr(0_B \mid 0_A) = \sin^2\left(\frac{\Delta\varphi_{AB}}{2} - x\right),$$

где x - рассогласование по фазе из-за неточной балансировки интерферометров на передающей и принимающей частях.

Соответственно, вероятность зарегистрировать на принимающей части 1_B, если с передающей части был послан 1_A, равна

$$\Pr(1_B|1_A)=\sin^2\left(\frac{\Delta\varphi_{AB}}{2}-x\right)$$

Вероятность ошибочной регистрации, когда с передающей части был послан 0_A, а на принимающей части был зарегистрирован 1_B, равна

$$\Pr(1_B|0_A)=\sin^2 x$$

Аналогично, вероятность ошибочной регистрации, когда с передающей части был послан 1_A, а на принимающей части был зарегистрирован 0_B, равна

$$\Pr(0_B|1_A)=\sin^2 x$$

Нули и единицы (O_A и 1_A) посылаются равновероятно, и, следовательно, количество зарегистрированных нулей и единиц (0_B и 1_B) на принимающей части тоже должно быть одинаковым, при условии идеальной балансировки интерферометров на передающей и принимающей частях, т.е. когда x=0.

Неточная балансировка интерферометров на принимающей и передающей частях (x отлично от нуля) приведет к тому, что количество нулей и единиц в принимающей части станет разным. Вероятность зарегистрировать на принимающей части разное количество нулей и единиц в зависимости от неточности балансировки x, равна

$$\begin{aligned}\Delta(x)&=\Pr(0_B|0_A)+\Pr(0_B|1_A)-\Pr(1_B|1_A)-\Pr(1_B|0_A)=\\&=2\sin^2 x+\sin^2\left(\frac{\Delta\varphi_{AB}}{2}+x\right)-\sin^2\left(\frac{\Delta\varphi_{AB}}{2}-x\right)=\\&=2\sin^2 x+\sin^2\left(\frac{\pi}{4}+x\right)-\sin^2\left(\frac{\pi}{4}-x\right)\end{aligned}\qquad(1)$$

Различное количество нулей и единиц на принимающей части приводит к вероятности ошибки на принимающей части системы, которая равна

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

Вероятность ошибки Q(x) однозначно связана с величиной видности V(x)

$$Q(x)=\frac{1-V(x)}{2}\qquad(2)$$

Когда интерферометры идеально сбалансированы (x=0), вероятность ошибки Q(x=0)=0, при этом видность является идеальной - достигает своего максимального значения V(x=0)=1. Вероятность ошибки используется как сигнал регулировки видности. При зарегистрированной (наблюдаемой) вероятности ошибки Q(x), изменяется величина фазового сдвига x так, чтобы вероятность ошибки обращалась в нуль, при таком значении x видность достигнет своего максимального значения равного единице.

Таким образом, каждый раз при формировании "сырого" ключа ("сырой" ключ - это последовательность нулей и единиц, которая еще содержит ошибки на принимающей части), величина Δ(x), пропорциональная разности нулей и единиц в нем, может использоваться как сигнал ошибки для регулировки разности фаз. Важно, что для этого не требуется дополнительный обмен с передающей частью.

Предложенный способ реализуется в однопроходной схеме, в которой используется пара разнесенных интерферометров Маха-Цандера, один из которых находится на передающей стороне, а второй на принимающей стороне. В передающей части (фиг. 1) с помощью лазера и последующего ослабления его излучения генерируется последовательность квазиоднофотонных состояний. Затем каждое квазиоднофотонное состояние с помощью интерферометра передающей части разделяется во времени на два когерентных квазиоднофотонных состояния, относительной фазой которых кодируются биты передаваемого ключа. При этом исходные квантовые состояния, которые отвечают нулям и единицам на передающей станции, посылаются равновероятно.

Полученные пространственно разнесенные квазиоднофотонные когерентные состояния передаются по оптическому волокну от передающей части к принимающей части однопроходной схемы.

Пространственно разнесенные квазиоднофотонные когерентные состояния в принимающей части (фиг. 2) снова поступают на интерферометр Маха-Цандера, на котором пары пространственно разнесенных квазиоднофотонных когерентные состояний с различной фазой совмещаются. После чего оптические импульсы регистрируются однофотонным детектором.

Получаемая интерференционная картина обладает видностью, которая будет «идеальной» (т.е. равной 1) в случае, когда количество единиц и нулей в принятом ключе будет одинаковым (также как и в передаваемом ключе). Отклонение видности от «идеальной» однозначно связано с регистрируемой разностью количества нулей и единиц в ключе. Вероятность обнаружения различного количества нулей и единиц в принятом ключе определяется формулой (1). Величина видности V(x) однозначно связана с ошибкой Q(x) (формула (2)).

Таким образом, величина, пропорциональная разности нулей и единиц в ключе может быть использована как сигнал ошибки для регулировки разности фаз пространственно разнесенных квазиоднофотонных когерентные состояний компенсацией относительной разности хода в интерферометре принимающей части.

Причем для этого не требуется дополнительного обмена с передающей частью, т.е. нет необходимости прерывании передачи ключей в режиме квазиоднофотонных состояний для компенсации относительной разности хода в интерферометре принимающей части, а, следовательно, и для управления интерференционной картиной, и время, затрачиваемое на эту компенсацию, минимизируется.

Краткое описание чертежей

На фиг. 1 показана схема передающей части.

На фиг. 2 показана схема принимающей части.

На схемах пунктирными линиями обозначены пути оптического излучения, сплошными линиями обозначены электрические связи.

Осуществление изобретения

Для реализации предложенного способа сначала необходимо сформировать передающую часть, принимающую часть и линию связи, соединяющую передающую и принимающую части.

Передающая часть содержит генератор случайных чисел, лазер, интерферометр по схеме Маха-Цандера, оптические элементы, формирующие параметры излучения и блок управления (фиг. 1).

В качестве лазера, формирующего информационные состояния, используется полупроводниковый лазерный диод с рабочей длиной волны 1.55 мкм, для формирования одиночных импульсов с определенной тактовой частотой.

В составе интерферометра используются волоконные светоделители на поляризационно-сохраняющих волокнах.

Для контроля работы лазера используется измеритель мощности на основе фотодиода.

После прохождения интерферометра излучение проходит через волоконный фазовый модулятор и аттенюатор, управляемый электронным образом с помощью блока управления.

Затем на выходе излучение проходит через волоконный оптический мультиплексор (разделитель) по длинам волн 1.55/1.3 мкм, на который также подается излучение от лазера синхронизации с длиной волны 1.3 мкм.

Излучение между оптическими элементами передающей части передается через поляризационно сохраняющие оптические волокна.

После оптического мультиплексора излучение попадает линию связи, выполненную в виде одномодового оптического волокна и соединяющую передающую и принимающую части.

Управление и контроль сигналов в целом осуществляются в блоке управления передающей части.

После прохождения линии связи оптический сигнал попадает в принимающую часть на входной волоконный оптический мультиплексор, где разделяется на два потока. Первый сигнальный поток с длиной волны 1.55 мкм проходит к контроллеру поляризации, а второй поток с длиной волны 1.3 мкм попадает в фотоприемник синхронизации, выходной сигнал с которого служит для синхронизации дальнейшей обработки.

После прохождения контроллера поляризации излучение проходит через волоконный фазовый модулятор и попадает в интерферометр, также выполненный по схеме Маха-Цандера. В одно из плеч интерферометра установлен пьезоэлемент для возможности управления оптической длиной пути. Пьезоэлемент жестко прикреплен к оптическому волокну, например, приклеен. Приложение напряжения к пьезоэлементу изменяет его геометрическую длину, что приводит к изменению длины волокна в месте соприкосновения его с пьезоэлементом.

Излучение на выходе из интерферометра попадает в фотоприемный блок, выполненный в виде однофотонного детектора на лавинном фотодиоде, для регистрации квазиоднофотонных информационных оптических импульсов. Выходные сигналы фотоприемного блока обрабатываются в блоке обработки.

Излучение между оптическими элементами принимающей части также передается через поляризационно сохраняющие оптические волокна.

Управление и контроль сигналов в целом осуществляются в блоке управления принимающей части.

После сформирования аппаратной части можно выполнить предложенный способ.

Состояния на выходе лазера передающей части является когерентным состоянием $|\alpha\rangle$.

Последовательные преобразования когерентного состояния в передающий части

при прохождении через интерферометр, фазовый модулятор и аттенюатор могут быть представлены в виде

$$|\alpha\rangle \rightarrow |\alpha\rangle_1 \otimes |\exp(i\Delta L_A)\alpha\rangle_2 \rightarrow |\exp(i\varphi_A)\alpha\rangle_1 \otimes |\exp(i\Delta L_A)\alpha\rangle_2$$

Индексы 1 и 2 отвечают пространственно разделенным состояниям после прохождения интерферометра (фиг. 1). Весь оптический тракт выполнен из поляризационно сохраняющих волокон, состояние поляризации сохраняется, поэтому индекс поляризации в когерентных состояниях всюду ниже для краткости опущен.

Состояния в принимающей части в верхнем и нижнем плече интерферометра после первого светоделителя имеют вид (фиг. 2)

$$\begin{pmatrix} |\exp(i(\varphi_A-\varphi_B)\frac{\alpha}{\sqrt{2}}\rangle_1 \otimes |\exp(i\Delta L_A)\frac{\alpha}{\sqrt{2}}\rangle_2 \\ |-\exp(i(\varphi_A-\varphi_B)\frac{\alpha}{\sqrt{2}}\rangle_1 \otimes |-\exp(i\Delta L_A)\frac{\alpha}{\sqrt{2}}\rangle_2 \end{pmatrix}$$

Состояния перед вторым светоделителем в верхнем и нижнем плечах интерферометра равны

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

Состояния на выходе интерферометра принимающей части равно

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

где $\Delta L_{AB} = -(\Delta L_A - \Delta L_B)$ - разность оптических длин плеч интерферометров в передающей и принимающей приемной частях соответственно.

Детектирование информационных состояний происходит однофотонным детектором. При малом среднем числе фотонов в информационном состоянии $\mu = |\alpha|^2$ вероятность детектирования пропорциональна

$$\left|(\exp(i(\varphi_A-\varphi_B))-\exp(-i(\Delta L_{AB})))\frac{\alpha}{2}\right|^2,$$

пропорциональна

$$\left|(\exp(i(\varphi_A-\varphi_B))-\exp(-i(\Delta L_{AB})))\frac{\alpha}{2}\right|^2 \approx \sin^2\left(\frac{\Delta\varphi_{AB}}{2}+x\right),$$

где $x = \frac{\Delta L_{AB}}{2}$ обозначает отклонение разности фаз от значения, требуемого протоколом квантового распределения ключей, вызванное разбалансировкой интерферометра.

Вероятность правильной регистрации битов 0 и 1 будет равна

$$\Pr(0_B|0_A)=\sin^2\left(\frac{\Delta\varphi_{AB}}{2}+x\right),$$

$$\Pr(1_B|1_A)=\sin^2\left(\frac{\Delta\varphi_{AB}}{2}-x\right),$$

$$\Delta\varphi_{AB}=\varphi_A-\varphi_B=\frac{\pi}{2}$$

Вероятность ошибочной интерпретации из-за неточной балансировки интерферометров, когда был послан 0 -- выбрана фаза φ_B^1 и наоборот, послана 1, а выбрана фаза φ_B^0 будет равно

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

$$\Pr(0_B|1_A)=\sin^2 x$$

Итоговая вероятность обнаружить разное количество 0 и 1 есть

$$\Delta(x)=\Pr(0_B|0_A)+\Pr(0_B|1_A)-\Pr(1_B|1_A)-\Pr(1_B|0_A)=$$

$$=2\sin^2 x+\sin^2\left(\frac{\Delta\varphi_{AB}}{2}+x\right)-\sin^2\left(\frac{\Delta\varphi_{AB}}{2}-x\right)=$$

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

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

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

Вероятность ошибки Q(x) представляет собой отношение разности числа нулей и единиц в последовательности к полной длине последовательности при величине разбалансировки x. Вероятность ошибки Q(x) однозначно связана с величиной видности V(x)

$$Q(x)=\frac{1-V(x)}{2}$$

Когда интерферометры идеально сбалансированы (x=0)), вероятность ошибки Q(x=Q)=0, при этом видность является идеальной - достигает своего максимального значения V(x=0)=1. Вероятность ошибки используется как сигнал регулировки видности. При зарегистрированной (наблюдаемой) вероятности ошибки Q(x) изменяется величина фазового сдвига x так, чтобы вероятность ошибки обращалась в нуль, при таком значении x видность достигнет своего максимального значения равного единице.

Таким образом, каждый раз при формировании "сырого" ключа величина Δ(x) пропорциональная разности нулей и единиц в нем, может использоваться как сигнал ошибки для регулировки разности фаз. Важно, что для этого не требуется дополнительный обмен с передающей стороной.

Полученная величина Δ(x), пропорциональная разности нулей и единиц, преобразуется в блоке обработки в сигнал управления пьезоэлементом для непосредственной регулировки разности фаз в интерферометре принимающей части.

(57) Формула изобретения

Способ управления интерференционной картиной в однопроходной системе квантовой криптографии, включающей

передающую часть, содержащую

генератор случайных чисел,

лазер,

интерферометр,

блок управления;

принимающую часть, содержащую

интерферометр,

фотоприемный блок,

блок обработки,

блок управления;

линию связи, выполненную в виде одномодового оптического волокна и соединяющую передающую и принимающую части;

способ заключается в том, что

генерируют случайную последовательность нулей и единиц с помощью генератора случайных чисел в передающей части;

генерируют на основании последовательности нулей и единиц последовательность квазиоднофотонных состояний в передающей части;

разделяют каждое квазиоднофотонное состояние с помощью интерферометра передающей части на пару пространственно разнесенных квазиоднофотонных когерентных состояний;

передают полученные пространственно разнесенные квазиоднофотонные когерентные состояния из передающей части в принимающую часть с помощью линии связи;

принимают пространственно разнесенные квазиоднофотонные когерентные состояния в принимающей части;

получают интерференционную картину от пространственно разнесенных квазиоднофотонных когерентных состояний на выходе интерферометра принимающей части;

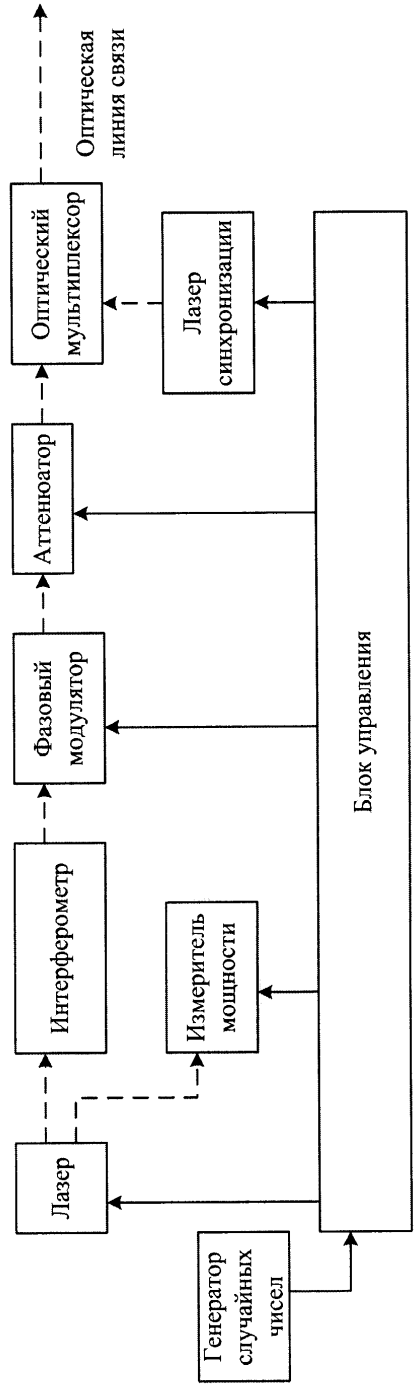
регистрируют последовательность квазиоднофотонных состояний после прохождения интерферометра принимающей части в фотоприемном блоке в виде последовательности нулей и единиц в зависимости от видности полученной интерференционной картины для каждого квазиоднофотонного состояния;

определяют сигнал ошибки в блоке обработки принимающей части на основании сравнения принятой и переданной последовательностей нулей и единиц, при этом в качестве сигнала ошибки применяется величина, пропорциональная числу несовпадений в позициях принятой и переданной последовательностей единиц и нулей; и

регулируют видность интерференционной картины, полученной на выходе интерферометра принимающей части, посредством компенсации относительной разности хода в интерферометре принимающей части на основании принятого сигнала ошибки.

1

Способ управления интерференционной картиной в однопроходной системе квантовой криптографии

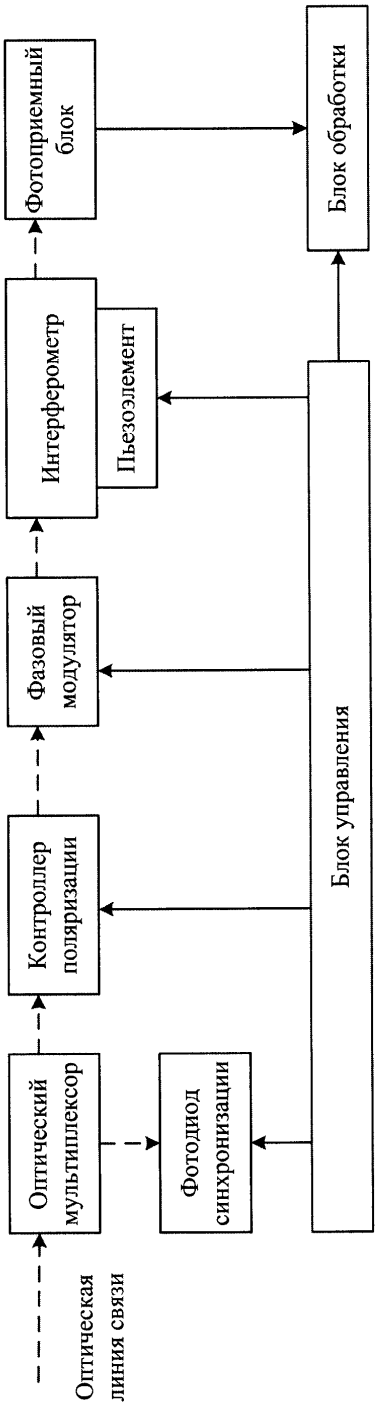


Фиг. 1

- 1 -

2

Способ управления интерференционной картиной в однопроходной системе квантовой криптографии



Фиг. 2