РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 730 554**(13) **C1**

(51) МПК
H04L 9/08 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК
H04L 9/08 (2020.02)

(21)(22) Заявка: **2019138761, 29.11.2019**

(24) Дата начала отсчета срока действия патента:
29.11.2019

Дата регистрации:
24.08.2020

Приоритет(ы):
(22) Дата подачи заявки: **29.11.2019**

(45) Опубликовано: **24.08.2020** Бюл. № **24**

Адрес для переписки:
119234, Москва, ул. Ломоносовский проспект, 27, стр. 1, Московский государственный университет имени М.В. Ломоносова, Фонд "Национальное интеллектуальное развитие"

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

(73) Патентообладатель(и):
Федеральное государственное бюджетное образовательное учреждение высшего образования "Московский государственный университет имени М.В. Ломоносова" (МГУ) (RU)

(56) Список документов, цитированных в отчете о поиске: **RU 2667755 C1, 24.09.2018. US 2011/0126011 A1, 26.05.2011. US 2014/0119537 A1, 01.05.2014. US 2016/0134420 A1, 12.05.2016. US 2017/0026175 A1, 26.01.2017.**

(54) СПОСОБ ВЫЯВЛЕНИЯ АТАКИ НА КВАНТОВЫЕ СОСТОЯНИЯ В КВАНТОВОМ КАНАЛЕ СВЯЗИ

(57) Реферат:

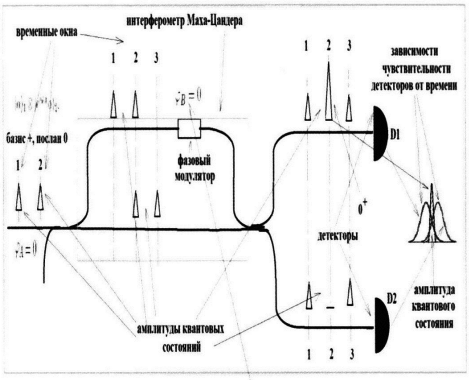
Изобретение относится к области квантовой криптографии. Технический результат заключается в обеспечении выявления в системах квантовой криптографии с фазовым и поляризационным кодированием ложных квантовых состояний в квантовом канале связи, сгенерированных злоумышленником. Технический результат достигается за счет того, что на этапе передачи серии посылок задают длину серии посылок и для каждой посылки в серии выполняют подготовку передающей и принимающей сторон, передачу посылки передающей стороной и прием посылки принимающей стороной, при этом подготовка передающей стороны включает выбор случайно и равновероятно одного из двух базисов передающей стороны, выбор случайно и равновероятно одного из двух значений фазы в выбранном базисе, синхронизацию общего времени между передающей и принимающей сторонами и приготовление передающей стороной квантового состояния, однозначно соответствующего выбранному значению фазы. 2 з.п. ф-лы, 6 ил.

RU 2730554 C1

RU 2730554 C1

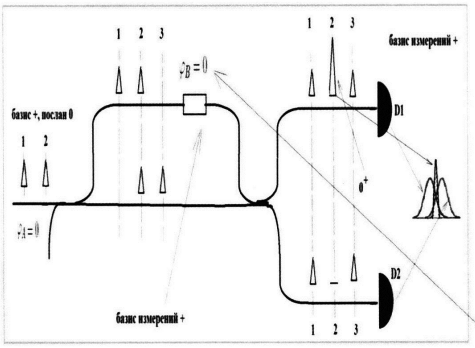
RU 2730554 C1

базисы передающей и принимающей сторон совпадают

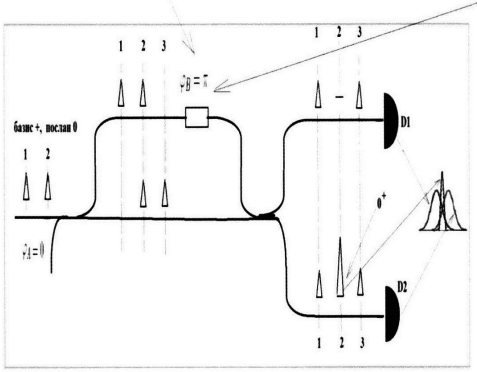


одно значение фазы на принимающей стороне в каждом базисе

2



3



два значения фазы на принимающей стороне в каждом базисе

RU 2730554 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 730 554**(13) **C1**

(51) Int. Cl.
H04L 9/08 (2006.01)

(12) ABSTRACT OF INVENTION

(52) CPC
H04L 9/08 (2020.02)

(21)(22) Application: **2019138761, 29.11.2019**

(24) Effective date for property rights:
29.11.2019

Registration date:
24.08.2020

Priority:
(22) Date of filing: **29.11.2019**

(45) Date of publication: **24.08.2020** Bull. № **24**

Mail address:
119234, Moskva, ul. Lomonosovskij prospekt, 27, str. 1, Moskovskij gosudarstvennyj universitet imeni M.V. Lomonosova, Fond "Natsionalnoe intellektualnoe razvitie"

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

(73) Proprietor(s):
Federalnoe gosudarstvennoe byudzhetnoe obrazovatelnoe uchrezhdenie vysshego obrazovaniya "Moskovskij gosudarstvennyj universitet imeni M.V. Lomonosova" (MGU) (RU)

RU 2730554 C1

(54) METHOD OF DETECTING AN ATTACK ON QUANTUM STATES IN A QUANTUM COMMUNICATION CHANNEL

(57) Abstract:

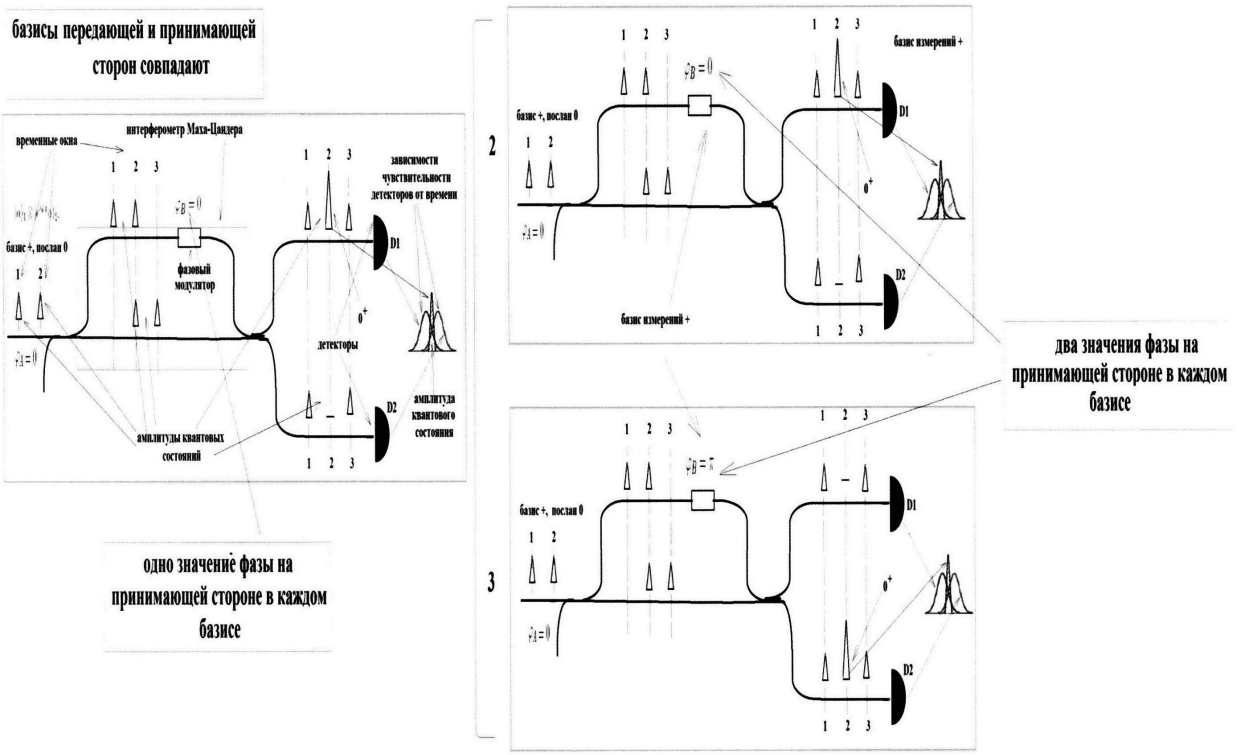
FIELD: quantum cryptography.

SUBSTANCE: invention relates to the field of quantum cryptography. Technical result is achieved due to the fact that at the stage of transmission of the series of packages the length of the series of parcels is set and for each sending in the series the preparation of the transmitting and receiving sides is performed, transmission of the sending by the transmitting side and reception of the sending by the receiving side, wherein preparation of transmitting side includes selecting randomly and equitably one of two transmission side bases, selecting randomly and equitably one of two phase values in the selected basis, synchronizing the total time between the transmitting and receiving sides and preparing the transmitting side of the quantum state which unambiguously corresponds to the selected phase value.

EFFECT: technical result consists in provision of detection in systems of quantum cryptography with phase and polarization encoding of false quantum states in quantum communication channel generated by intruder.

3 cl, 6 dwg

RU 2730554 C1



RU 2730554 C1

RU 2730554 C1

Область техники, к которой относится изобретение

Изобретение относится к области квантовой криптографии, а именно, к защите от атаки на квантовые состояния, использующей разную по времени зависимость чувствительности однофотонных детекторов, в системах квантовой криптографии с фазовым и поляризационным кодированием.

Уровень техники

Квантовая криптография решает центральную проблему симметричной криптографии, а именно, проблему распределения криптографических ключей, представляющих собой случайную идентичную последовательность нулей и единиц на передающей и принимающей сторонах, неизвестную третьей стороне. Распределение ключей происходит путем согласования - синхронизации двух независимых заранее сгенерированных случайных последовательностей на передающей и приемной сторонах посредством передачи серии квантовых состояний через открытый и доступный для вторжения квантовый канал связи (оптическое волокно или атмосферный канал), с передающей стороны на приемную сторону. Квантовые состояния выбираются на передающей стороне в соответствии со случайной последовательностью на передающей стороне, и последующих измерений на принимающей стороне, которые выбираются в соответствии со случайной последовательностью на принимающей стороне. Измерения выбираются таким образом, что в посылках, где базис измерений на принимающей стороне и базис приготовления квантовых состояний на передающей стороне совпадали, квантовые состояния, соответственно биты ключа, в отсутствии вторжений в канал связи идентифицируются однозначно и без ошибок. Номера посылок, где базисы передающей и принимающей стороны не совпадали, отбрасываются посредством сообщений через открытый аутентичный классический канал связи. Таким образом, происходит синхронизация случайных последовательностей.

Из уровня техники известны способы детектирования попыток подслушивания (обнаружения атаки) при вторжении в квантовый канал связи, основанные на законах квантовой механики, которые гарантируют, что вторжение в квантовый канал связи будет приводить к искажению передаваемых квантовых состояний и, соответственно, возникновению ошибок на приемной стороне. Факт вторжения в квантовый канал связи детектируется по возникновению ошибок на принимающей стороне. Для этого часть посылок - позиции и значения бит в этих позициях на передающей и принимающей сторонах, раскрываются через открытый аутентичный классический канал связи, затем сравниваются, и оценивается процент ошибок. В дальнейшем раскрытая часть последовательности отбрасывается. Законы квантовой механики позволяют при данном наблюдаемом проценте ошибок получить верхнюю границу утечки информации к подслушивателю. Если процент ошибок, соответственно, утечка информации к подслушивателю, меньше критической величины, то ошибки в нераскрытой части последовательности исправляются посредством обмена классической информацией через открытый аутентичный канал связи. В результате возникает общий идентичный на передающей и принимающей стороне очищенный ключ, о котором, подслушиватель имеет частичную информацию, при условии, что наблюдаемый процент ошибок меньше критической величины. Очищенный ключ сжимается посредством хеш-функций, посредством сообщений через открытый классический канал связи, до финального секретного ключа - битовой строки, меньшей длины, о которой подслушиватель не имеет уже никакой информации. Выбор хеш-функций осуществляется открыто через классический аутентичный канал связи.

Системы квантовой криптографии представляют собой открытые системы, вторжение

в канал связи может быть реализовано активным зондированием посредством лазерного излучения состояния передающей и принимающей аппаратуры или изменением параметров аппаратуры. Системы квантовой криптографии используют для регистрации квантовых состояний однофотонные детекторы, которые обычно работают в стробируемом режиме. На детекторы в момент прихода фотона накладывается короткий стробирующий импульс напряжения. В отсутствии стробирующего напряжения детектор не активен. Квантовая эффективность однофотонного детектора - вероятность регистрации фотона внутри стробирующего импульса, зависит от времени и определяется конкретным типом детектора. В системах квантовой криптографии с фазовым и поляризационным кодированием может использоваться два однофотонных детектора, которые имеют разные зависимости чувствительности как функции времени (Фиг. 1). Вероятность зарегистрировать квантовое состояние излучения длительностью меньше длительности строба зависит от длительности квантового состояния и его положения по времени. При штатной работе системы положение по времени и длительность квантовых состояний выбираются таким образом, чтобы они попадали в область чувствительности по времени обоих детекторов (Фиг. 1).

Наиболее близким к заявляемому изобретению является способ выявления атаки на квантовые состояния в квантовом канале связи, реализованного по протоколу BB84 (C.H. Bennett and G. Brassard, in Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing (IEEE Press, New York, 1984), pp. 175-179.). Способ включает этапы формирования ключей, описанные выше, с использованием системы квантовой криптографии, также описанной выше этап оценки количества ошибок, на котором происходит выявление атаки по величине ошибки. Если ошибка в канале связи меньше приблизительно 11%, то информация, доступная подслушивателю, заведомо не превосходит взаимной информации между приемной и принимающей сторонами, и секретная передача данных возможна. Обнаружение и исправления ошибок осуществляют посредством перемешивания и разбиения синхронизированных последовательностей на блоки, которые проверяют на четность в несколько итераций, уменьшая каждый размер именно тех блоков, четность которых не совпала. Однако, данный способ характеризуется определенными недостатками, а именно, если длительность квантового состояния и его положение по времени внутри стробирующего импульса выбраны таким образом, что состояние не попадает в максимум кривой чувствительности детектора (состояние не накрывается кривой чувствительности детектора), то регистрации состояния не происходит. Подслушиватель может подменять истинные квантовые состояния ложными состояниями (fake states) с меньшей длительностью и положением по времени, тем самым навязывая отсчет детектора или отсутствие отчета для заранее выбранной посылки на одном из двух детекторов. Такие атаки на техническую реализацию, использующие разную по времени зависимость чувствительности однофотонных детекторов, известны из уровня техники (Effects of detector efficiency mismatch on security of quantum cryptosystems, Vadim Makarov, Andrey Anisimov, and Johannes Skaar, Physical Review, A74, 022313 (2006)). При такой атаке подслушиватель знает весь ключ, не производит ошибок на принимающей стороне и не детектируется, система уязвима относительно такой атаки и не обеспечивает секретность ключей.

Технической проблемой, решаемой настоящим изобретением, является невозможность выявления атаки, использующей разную по времени зависимость чувствительности однофотонных детекторов, в системах квантовой криптографии с фазовым и поляризационным кодированием, характеризующейся ложными квантовыми

состояниями, сгенерированными подслушивателем, для которых длительность и положение по времени выбраны таким образом, что квантовые состояния находятся вне максимума кривой чувствительности регистрирующего его детектора.

Раскрытие сущности изобретения

Техническим результатом изобретения является выявление в системах квантовой криптографии с фазовым и поляризационным кодированием ложных квантовых состояний в квантовом канале связи, сгенерированных подслушивателем, в виде несовпадений, обнаруживаемых при обмене информацией между передающей и принимающей сторонами по открытому каналу связи.

Технический результат достигается при реализации способа выявления атаки на квантовые состояния в квантовом канале связи между передающей стороной и принимающей стороной, включающего этап передачи серии посылок, этап обмена информацией по открытому каналу связи, этап выявления атаки, при этом

на этапе передачи серии посылок задают длину серии посылок и для каждой посылки в серии выполняют подготовку передающей и принимающей сторон, передачу посылки передающей стороной и прием посылки принимающей стороной, при этом

подготовка передающей стороны включает выбор случайно и равновероятно одного из двух базисов передающей стороны, выбор случайно и равновероятно одного из двух значений фазы в выбранном базисе, синхронизацию общего времени между передающей и принимающей сторонами и приготовление передающей стороной квантового состояния, однозначно соответствующего выбранному значению фазы;

подготовка принимающей стороны включает выбор случайно и равновероятно одного из двух значений фазы в качестве базиса измерений; и для каждого выбранного значения фазы случайно и равновероятно меняют базис измерений на ортогональный либо оставляют базис неизменным;

передача посылки передающей стороной включает передачу приготовленного на передающей стороне квантового состояния в квантовый канал связи;

прием посылки принимающей стороной осуществляют на вход преобразователя квантовых состояний, снабженного двумя выходами с последующей регистрацией сигнала одним из детекторов, установленных на каждом из выходов преобразователя квантовых состояний в зависимости от принятого квантового состояния и значения фазы, предварительно выбранного случайно и равновероятно на принимающей стороне;

на этапе обмена информацией по открытому каналу связи передающая сторона передает принимающей стороне или принимающая сторона передает передающей стороне информацию о выбранном базисе для каждой переданной или принятой посылки, принимающая сторона формирует обновленную серию посылок путем удаления из принятой серии посылок, для которых базисы, выбранные на передающей и принимающей сторонах, не совпадают;

на этапе выявления атаки определяют число не совпадающих посылок в переданной и принятой сериях, при этом каждое несовпадение трактуют как атаку на квантовые состояния в квантовом канале связи,

В качестве преобразователя квантовых состояний может быть использован интерферометр Маха-Цандера, в качестве детекторов на принимающей стороне -лавинные однофотонные фотодетекторы.

Таким образом, технический результат достигается при использовании способа выявления атаки на квантовые состояния в квантовом канале связи в системах квантовой криптографии с фазовым и поляризационным кодированием, при которой подслушиватель знает весь криптографический ключ и не обнаруживается, где согласно

заявляемому изобретению, принимающая сторона в каждом базисе измерений случайно выбирает не одно значение фазы, как имело место в известных системах, а два значения фазы: фазу 0 или пи в одном базисе, и фазу пи/2 или 3пи/2 в другом базисе. За счет такого случайного выбора фаз при атаке подслушивателя, использующей разную по времени зависимость чувствительности однофотонных детекторов, неизбежно возникают ошибки на принимающей стороне, по которым происходит обнаружение подслушивателя.

Краткое описание чертежей

Изобретение поясняется чертежами, где на фиг. 1. представлена схема реализации передачи состояния, соответствующего значению 0 при совпадении базисов передающей и принимающей сторон; на фиг. 2 - схема реализации передачи состояния, соответствующего значению 1 при совпадении базисов передающей и принимающей сторон; на фиг. 3 - схема, иллюстрирующая передачу фаз из разных базисов; на фиг. 4 - схема процесса передачи состояния при совпадении базиса подслушивателя с базисами передающей и принимающей сторон; на фиг. 5 - схема процесса передачи состояния при не совпадении базиса подслушивателя с базисами передающей и принимающей сторон; на фиг. 6 - схема процесса детектирования попыток атаки подслушивателя.

Подробное описание осуществления изобретения

В заявляемом изобретении представлен способ обнаружения и защиты от атаки, использующей разную по времени зависимость чувствительности однофотонных детекторов, в системах квантовой криптографии с фазовым кодированием и поляризационным.

Ниже представлено описание работы системы квантового распределения ключей в отсутствии атаки, а затем самой атаки, использующей разные временные зависимости чувствительности однофотонных детекторов, и способ детектирования такой атаки.

Атака на системы квантового распределения ключей с фазовым кодированием на примере протокола BB84 (C.H. Bennett and G. Brassard, in Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing (IEEE Press, New York, 1984), pp. 175-179.), который является базовым протоколом, проводится следующим образом (для систем с поляризационным кодированием и других протоколов атака проводится аналогично).

В протоколе BB84 используют два базиса + и x, которые на передающей стороне выбираются случайно и равновероятно в соответствии со случайной последовательностью О и 1. Внутри каждого базиса случайно и равновероятно выбираются также в соответствии со случайной последовательностью одно из двух значений фазы, значение фазы однозначно сопоставляется с квантовым состоянием, приготавливаемым на передающей стороне. В системах квантовой криптографии с фазовым кодированием каждое квантовое состояние представляет собой пару квазиоднофотонных когерентных состояний вида (фиг. 1, 2), локализованных во временных окнах 1 и 2

$$|\alpha\rangle_1 \otimes |e^{i\varphi_A}\alpha\rangle_2,$$

где α -- амплитуда квазиоднофотонного когерентного состояния, индексы 1 и 2 обозначают временные окна (фиг. 1), выбор базиса и состояний внутри каждого базиса фиксируется выбором относительной фазы между квазиоднофотонными состояниями внутри пары (фиг. 1, 2), относительная фаза когерентных состояний, локализованных во временных окнах 1 и 2 в базисах + и x, имеет вид

$$\begin{cases} 0^{+} \rightarrow \varphi_A = 0 \\ 1^{+} \rightarrow \varphi_A = \pi \end{cases}, \quad \begin{cases} 0^{\times} \rightarrow \varphi_A = \frac{\pi}{2} \\ 1^{\times} \rightarrow \varphi_A = \frac{3\pi}{2} \end{cases}.$$

Зависимости чувствительности однофотонных детекторов по времени различаются (фиг. 1, 2).

При штатном режиме работы длительность квантовых состояний и положение по времени выбираются таким образом, чтобы состояния попадали в общую область по времени зависимости чувствительности обоих однофотонных детекторов D1 и D2 (фиг. 1, 2).

На принимающей стороне выбор базиса измерения - базиса либо +, либо x производится случайно и равновероятно в соответствии со случайной последовательностью на принимающей стороне. В базисе + выбирается значений фазы $\varphi_B = 0$, в базисе x, $\varphi_B = \frac{\pi}{2}$. Выбор фазы производится наложением напряжения на фазовый модулятор в плече интерферометра Мах-Цандера (МЦ) (фиг. 1, 2).

Перед детектированием состояний на передающей стороне в системах квантовой криптографии с фазовым кодированием, состояния, поступающие из квантового канала связи, подвергаются преобразованию на интерферометре МЦ (фиг. 1, 2).

Вероятность отсчета на детекторах в центральном временном окне 2 (фиг. 1 - левая половина) определяется разностью фаз передающей и принимающей стороны. Интенсивность на детекторе D1 пропорциональна

$$\mathrm{D1} \rightarrow \quad \cos^2 \frac{(\varphi_A - \varphi_B)}{2},$$

а на детекторе D2 пропорциональна

$$\mathrm{D2} \rightarrow \quad \sin^2 \frac{(\varphi_A - \varphi_B)}{2}.$$

Если базисы передающей и приемной сторон совпадают, то при разности фаз состояний, выбранных передающей стороной и принимающей стороной ϕ_A-ϕ_B=0 конструктивная интерфереция имеет место на входе детектора D1 (фиг. 1, где левая половина, отвечает ситуации, когда посылался 0 в базисе +, фиг. 2 отвечает ситуации, когда посылалась 1 в базисе +), что будет приводить к отсчету в детекторе D1 в центральном временном окне 2. Иначе говоря, при совпадении базисов, например, базис +, передающая сторона выбирает фазу 0, и принимающая сторона, фазу 0, то после преобразований входных состояний на интерферометре МЦ, идеальная конструктивная интерференция будет иметь место на детекторе D1. Из-за деструктивной интерференции на детекторе D2, срабатывания детектора не будет (фиг. 1 левая половина). Отсчет детектора D1 интерпретируется как логический 0 (фиг. 1 левая половина).

Если передающая сторона посылала 1 в базисе + (фиг. 2 левая половина), что отвечает выбору фазы пи, то на детекторе D2 будет конструктивная интерференция, которая приведет к срабатыванию детектора D2. Из-за деструктивной интерференции на детекторе D1, срабатывания детектора D1 не будет (фиг. 2 левая половина). Отсчет детектора D2 интерпретируется как логическая 1.

Аналогично, если передающая часть посылала состояние 1 в базисе +, т.е. передающая

сторона выбрала фазу $\phi_A=\pi$ принимающая фазу $\phi_B=0$.В этом случае конструктивная интерференция будет иметь место на детекторе D2 (фиг. 2 левая половина), что приведет к отсчету детектора D2. На детекторе D1 (фиг. 2 левая половина) будет деструктивная интерференция - отсутствие срабатывания детектора D1 (фиг. 2 левая половина).

При несовпадающих базисах передающей и принимающей сторон, полной конструктивной или деструктивной интерференции на детекторах D1 и D2 не происходит (фиг. 3).

Интенсивность сигнала независимо от посланного состояния (фиг. 3), соответственно, выбора фаз в несовпадающих базисах, будет пропорциональна на обоих детекторах D1 и D2:

$$\sin^2\frac{(\varphi_A-\varphi_B)}{2}=\cos^2\frac{(\varphi_A-\varphi_B)}{2}=\frac{1}{2} \quad (1),$$

если фазы ϕ_A и ϕ_B выбираются из разных базисов, причем независимо от самого выбора фаз. Отсчет будет иметь место на обоих детекторах D1 и D2 (фиг. 3) с одинаковой вероятностью, независимо от того, какую фазу состояний выбрала передающая и принимающая сторона.

При атаке подслушиватель разрывает квантовый канал связи и использует для измерений в каждой посылке аппаратуру, аналогичную аппаратуре на принимающей стороне. Подслушиватель выбирает базис наугад в каждой посылке, производит измерение в выбранном базисе и интерпретирует результат как 0 или 1 в своем выбранном базисе.

Далее в соответствии с результатом измерений перепосылает состояние, аналогичное состоянию с передающей стороны, но в другом базисе по отношению к которому подслушиватель проводил свои измерения.

Принципиальный момент стратегии подслушивателя состоит в следующем, длительность и положение по времени подменного состояния (fake state) всегда выбирается таким образом, чтобы оно не попадало в область чувствительности по времени того однофотонного детектора, который должен был бы регистрировать перепосланное квантовое состояние в данном базисе, т.е. в базисе, в котором подменное состояние перепосылается (фиг. 4).

Поскольку передающая и принимающая стороны оставляют только те посылки, в которых базисы совпадали, то при атаке подслушивателя возможны две ситуации.

Базис, выбранный подслушивателем, по отношению к базису передающей/принимающей стороны, был угадан правильно (отметим, что факт правильного или ошибочного выбора им базиса, подслушивателю при его измерениях неизвестен), то подслушиватель при регистрации получает правильное состояние. Далее подслушиватель перепосылает противоположное состояния тому, которое он зарегистрировал (если зарегистрирован 0, перепосылает 1, и наоборот) и в другом базисе (измерения были в базисе +, то перепосылает в базисе x, и наоборот) с меньшей длительностью и сдвинутые относительно кривой чувствительности соответствующего детектора. Если перепосылается состояние 1, то сдвиг по времени относительно кривой чувствительности детектора D1 (фиг. 4), который должен бы регистрировать логический 0. В результате перепосланные состояния не дают ошибочных отсчетов. Возникает только правильный отсчет в детекторе D1, где он и должен был бы быть от истинных состояний (фиг. 4).

Базис, выбранный подслушивателем по отношению к базису передающей/принимающей стороны, подслушивателем был угадан неправильно (фиг. 5). В этом случае отсчет у подслушивателя равновероятно может быть в одном из двух детекторов.

Это следует из формулы (1). Пусть для определенности базис передающей и принимающей стороны есть +, а базис измерений подслушивателя есть x. Противоположная ситуация рассматривается полностью аналогично. Подслушиватель перепосылает состояния в противоположном базисе, по отношению к которому он проводил свои измерения. Поскольку базис измерений подслушивателя не совпадал с базисом передающей и принимающей стороны, то подслушиватель будет перепосылать состояния уже в правильном базисе в зависимости от результата своих измерений. При этом также возможны две ситуации.

2.1) Отсчет у подслшивателя произошел в детекторе D1 (фиг. 5). Данный отсчет подслушивателем интерпретируется как 0 в базисе x. Тогда подслушиватель перепосылает состояние 1 в базисе +, но меньшей длительности и сдвинутое по времени таким образом, чтобы оно не попадала в область чувствительности детектора D2 (фиг. 5). Поскольку в этом случае перепосылается неправильное состояние (1 в базисе +, истинное состояние передающей стороны 0 в базисе +), то такое состояние дает конструктивную интерференцию только на детекторе D2 (фиг. 5), на детекторе D1 имеет место отсутствие состояния за счет деструктивной интерференции (фиг. 2). Если бы неправильное состояние 1 в базисе + не было сдвинуто по времени, то возник бы ошибочный отсчет. Из-за сдвига неправильного состояния по времени (фиг. 5), отсчет на обоих детекторах отсутствует. Отсутствие отсчета не есть ошибка, отсутствие отсчетов списывается на потери в линии.

2.2) Отсчет у подслушивателя произошел на детекторе D2. Данный отсчет подслушиватель интерпретирует как 1 в базисе x. Подслушиватель перепосылает состояние 0 в противоположном базисе +, сдвинутое по времени так, чтобы оно не попадало по времени в область чувствительности по времени того однофотонного детектора (в данном случае детектора D1 (фиг. 5)), который должен был бы регистрировать перепосланное квантовое состояние в данном базисе, в базисе в котором подменное состояние перепосылается (фиг. 5). В итоге отсчетов на обоих детекторах не будет (фиг. 5). Отсутствие отсчетов не есть ошибка, отсутствие отсчетов списывается на потери в канале связи.

В результате атаки подслушиватель знает весь передаваемый ключ, не производит ошибок на принимающей стороне - ошибочные отсчеты отсутствуют и не детектируется. Система не обеспечивает секретность ключей.

Аналогичная ситуация имеет место и в системах с поляризационным кодированием.

Сущность изобретения поясняется фиг. 6.

Способ измерений на приемной стороне отличается тем, что в каждом базисе на приемной стороне значения фазы случайно выбирается из двух значений. В базисе + фазы

выбираются из значений 0 и π. В базисе x из двух значений $\pi/2$ и $\pi/2$

На фиг. 6 на левой половине показан известный способ измерений на принимающей стороне, на правой половине показан предлагаемый способ.

В базисе + выбор одного значения фазы приводит к тому, что состояние 0+, поступающее на приемную сторону, приводит к конструктивной интерференции на детекторе D1 и отсчету на нем. Отсчет на детекторе D2 из-за деструктивной интерференции на нем отсутствует (фиг. 6).

Если в базисе + выбираются два значения фазы, то отсчет в детекторе D1 или в детекторе D2 от полученного состояния 0+ будет иметь место в зависимости от выбора фазы на принимающей стороне. При выборе фазы 0 отсчет в детекторе D1, при выборе фазы пи - отсчет в детекторе D2 (фиг. 6).

Аналогично, если на детектор поступает 1+, то при одном выборе фазы равной О, отсчет будет иметь место на детекторе D2. При двух значениях фазы отсчет будет иметь место на обоих детекторах в зависимости от выбора фазы. При выборе фазы π отсчет от состояния 1+ будет на детекторе D1 (фиг. 1), при выборе фазы 0, отсчет будет иметь место на детекторе D2 (фиг. 6).

Таким образом, при двух значениях фаз на принимающей стороне внутри базиса состояния, отвечающие 0+ и 1+, дают отсчеты в обоих детекторах, в зависимости от выбора фазы. Аналогичная ситуация имеет место в базисе x.

Случайный выбор двух значений фаз внутри каждого базиса приводит к тому, что подслушиватель неизбежно будет производить ошибки на принимающей стороне и будет детектироваться.

Пусть передающая сторона посылала 0 в базисе + (фиг. 6). Если базис измерений подслушивателя не совпадает с базисом передающей и принимающей стороны -подслушиватель выбрал базис x, то подслушиватель будет равновероятно получать правильный и ошибочный результат.

Правильный отсчет (фиг. 6), отсчет у подслушивателя в детекторе D1 - интерпретируется как логический 0 - правильный результат (фиг. 6).

Результат - отсчет на детекторе D1 - интерпретируется как Ox. В этом случае подслушиватель перепосылает состояние в противоположном базисе 1+, сдвинутое по времени так, чтобы не попадать в кривую по времени чувствительности детектора D2 - блокировать отсчет в детекторе D2 (фиг. 6).

В этом случае перепосланное состояние не произведет ошибочного отсчета в детекторе D2, при условии, что принимающая сторона выбрала фазу 0 в базисе+. Однако, если принимающая сторона выбрала фазу π, то состояние 1+ даст конструктивную интерференцию на детекторе D1 (рис. 6) и ошибочный отсчет на нем, поскольку при истинном состоянии 0+ и выборе фазы π отсчета от истинного состояния 0+ на детекторе на детекторе D1 не должно быть. Должен быть отсчет только на детктоpe D2 (рис. 6).

Ошибочный отсчет (фиг. 6), Отсчет у подслушивателя в детекторе D2 - интерпретируется как логичская 1 - ошибочный результат (фиг. 6). Результат - отсчет на детекторе D2 - интерпретируется как 1x. В этом случае подслушиватель перепосылает состояние в противоположном базисе 0+, сдвинутое по времени так, чтобы не попадать в кривую по времени чувствительности детектора Dl -- блокировать отсчет в детекторе D1 (фиг. 6).

В этом случае перепосланное состояние не произведет ошибочного отсчета в детекторе D1, при условии, что принимающая сторона выбрала фазу 0 в базисе +. Если принимающая сторона выбрала фазу π то состояние 0+ даст конструктивную интерференцию на детекторе D2 (фиг. 6) как и должно быть, поскольку при истинном состоянии 0+ и выборе фазы π; отсчет от истинного состояния 0+ должен быть на детекторе D2 (рис. 6).

Аналогичная ситуация имеет место, если передающей и принимающей стороной выбран базис x.

Таким образом, подслушиватель неизбежно своим вторжением в линию связи при атаке, использующей разную по времени зависимость чувствительности однофотонных детекторов, в системах квантовой криптографии с фазовым и поляризационным кодированием, при которой подслушиватель знает весь криптографический ключ и не обнаруживается, будет обнаружен при использовании заявляемого способа, в соответствии с которым принимающая сторона в каждом базисе измерений выбирает

не одно значение фазы, как имело место в известных системах, а в каждом базисе случайно выбирает два значения фазы: фазу 0 или π в одном базисе, и случайно фазу π/2 или -π/2 в другом базисе, за счет такого случайного выбора фаз при атаке подслушивателя, использующей разную по времени зависимость чувствительности однофотонных детекторов, неизбежно будет производить ошибки в тех посылках, где базис измерений подслушивателя не совпадает с базисом передающей и принимающей сторон.

Аналогичная ситуация имеет место в системах с поляризационным кодированием. В этих системах значениям фазы отвечают углы поляризации фотона по отношению к выбранной системе координат.

Пример осуществления изобретения.

В целях демонстрации эффективности заявляемого способа для случая фазового кодирования была реализована экспериментальная система связи с квантовым распределением ключа по схеме, описанной в статье [Yi Zhao, Chi-Hang Fred Fung, Bing Qi, Christine Chen, and Hoi-Kwong Lo. Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems// PHYSICAL REVIEW A 78, 042333 (2008)]. Для демонстрации эффективности заявляемого способа в случае поляризационного кодирования была реализована экспериментальная система связи по схеме, описанной в статье [Sebastien Sauge, Lars Lydersen, Andrey Anisimov, Johannes Skaar, and Vadim Makarov. Controlling an actively-quenched single photon detector with bright light// Optics Express Vol.19, Issue 23, pp. 23590-23600 (2011)]. При этом реализация заявляемого способа обеспечивалась путем подачи дополнительных управляющих сигналов с генератора случайных чисел на фазовый модулятор на стороне Боба.

Атака подслушивателя на канал связи осуществлялась по схеме, описанной в статьях [Yi Zhao, Chi-Hang Fred Fung, Bing Qi, Christine Chen, and Hoi-Kwong Lo. Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems// PHYSICAL REVIEW A 78, 042333 (2008); Vadim Makarov and Johannes Skaar. Faked states attack using detector efficiency mismatch on SARG04, phase-time, DPSK, and Ekert protocols// arXiv:quant-ph/0702262v3 23 Nov 2007].

В серии проведенных экспериментов, проведенных как для фазового, так и для поляризационного кодирования, при передаче квантовых состояний со стороны Алисы на сторону Боба были реализованы попытки подслушивателя подменить перехваченные в канале связи квантовые состояния состояниями, сгенерированными подслушивателем. При этом каждая попытка была зарегистрирована в виде существенного повышения уровня ошибок, регистрируемых на принимающей стороне. Таким образом, эффективность заявляемого способа подтверждена экспериментально.

(57) Формула изобретения

1. Способ выявления атаки на квантовые состояния в квантовом канале связи между передающей стороной и принимающей стороной, включающий этап передачи серии посылок, этап обмена информацией по открытому каналу связи, этап выявления атаки, при этом

на этапе передачи серии посылок задают длину серии посылок и для каждой посылки в серии выполняют подготовку передающей и принимающей сторон, передачу посылки передающей стороной и прием посылки принимающей стороной, при этом

подготовка передающей стороны включает выбор случайно и равновероятно одного из двух базисов передающей стороны, выбор случайно и равновероятно одного из двух значений фазы в выбранном базисе, синхронизацию общего времени между передающей

и принимающей сторонами и приготовление передающей стороной квантового состояния, однозначно соответствующего выбранному значению фазы;

подготовка принимающей стороны включает выбор случайно и равновероятно одного из двух значений фазы в качестве базиса измерений; и для каждого выбранного значения фазы случайно и равновероятно меняют базис измерений на ортогональный либо оставляют базис неизменным;

передача посылки передающей стороной включает передачу приготовленного на передающей стороне квантового состояния в квантовый канал связи;

прием посылки принимающей стороной включает пересылку принятой посылки на вход преобразователя квантовых состояний, снабженного двумя выходами и регистрацию сигнала одним из детекторов, установленных на каждом из выходов преобразователя квантовых состояний в зависимости от принятого квантового состояния и значения фазы, предварительно выбранного случайно и равновероятно на принимающей стороне;

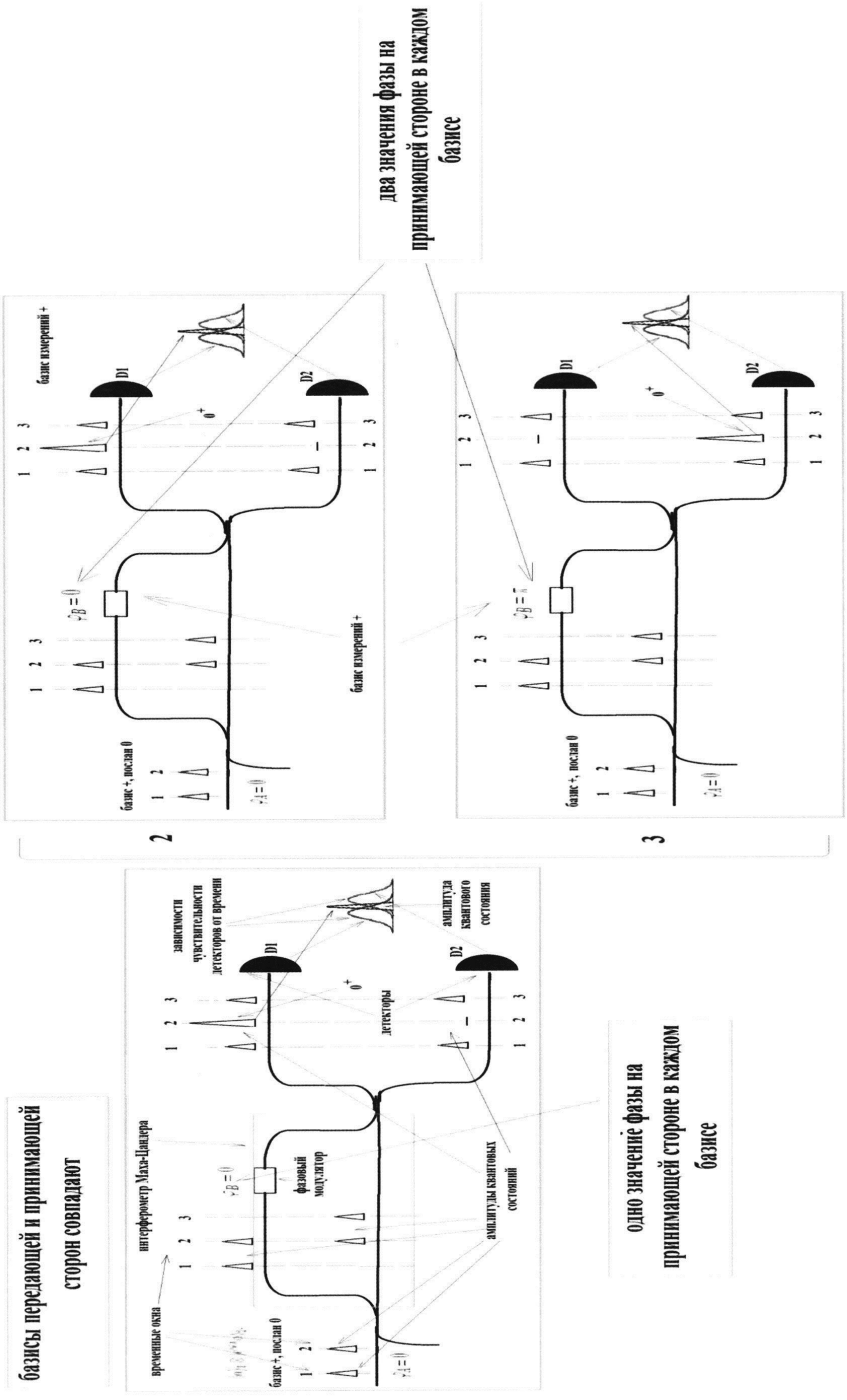
на этапе обмена по открытому каналу связи передающая сторона передает принимающей стороне или принимающая сторона передает передающей стороне информацию о выбранном базисе для каждой переданной или принятой посылки, принимающая сторона формирует обновленную серию посылок путем удаления из принятой серии посылок, для которых базисы, выбранные на передающей и принимающей сторонах, не совпадают;

на этапе выявления атаки определяют число не совпадающих посылок в переданной и принятой сериях, при этом каждое несовпадение трактуется как атака на квантовые состояния в квантовом канале связи,

2. Способ по п. 1, в котором в качестве преобразователя квантовых состояний выбирают интерферометр Маха-Цандера.

3. Способ по п. 1, в котором в качестве детекторов на принимающей стороне выбирают лавинные однофотонные фотодетекторы.

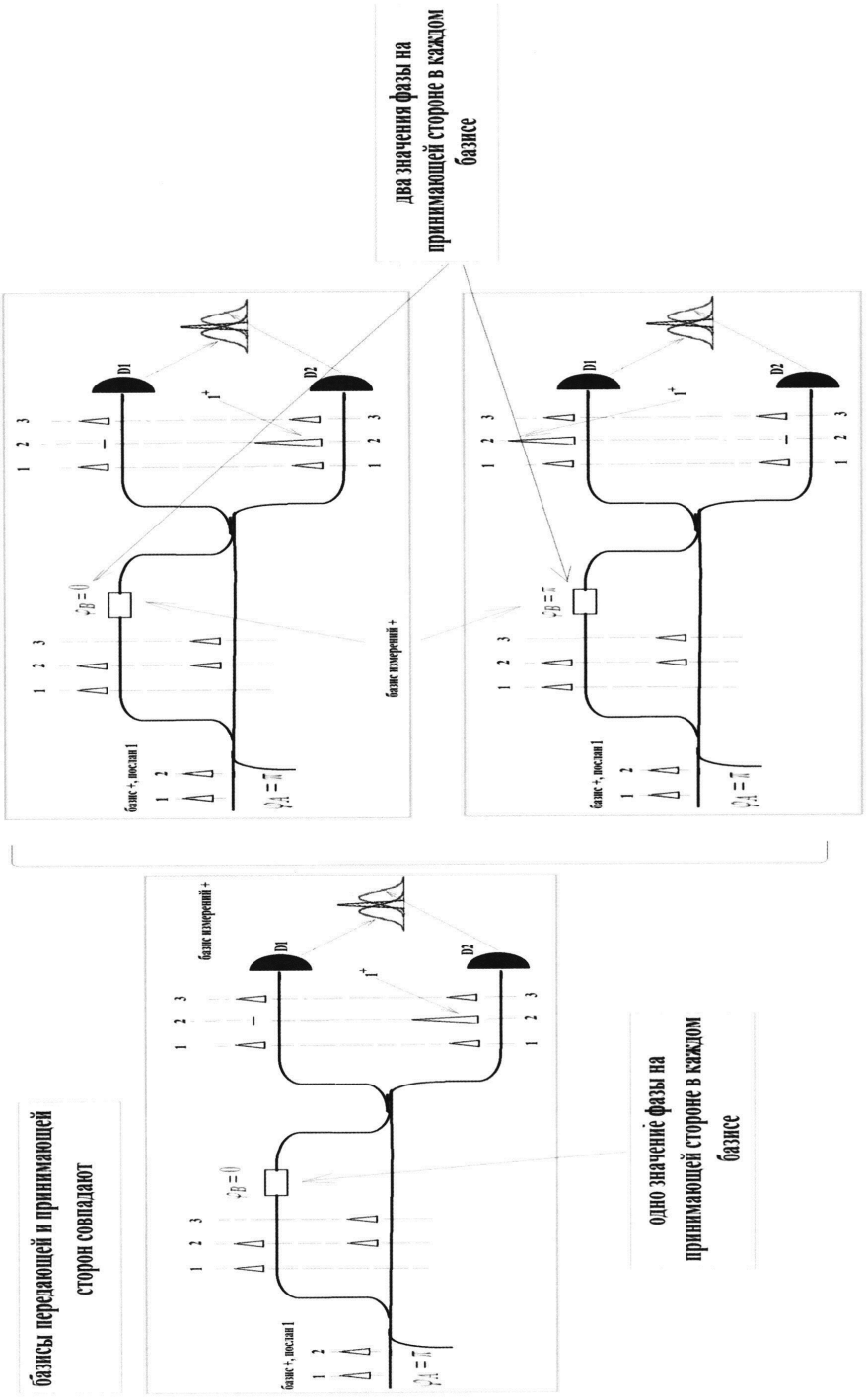
1


два значения фазы на принимающей стороне в каждом базисе
базис измерений+
базис +, послан 0
фазовый модулятор
интерферометр Маха-Цандера
временные окна
зависимости чувствительности детекторов от времени
детекторы
амплитуда квантового состояния
амплитуды квантовых состояний
базисы передающей и принимающей сторон совпадают
одно значение фазы на принимающей стороне в каждом базисе
D1
D2
2
3

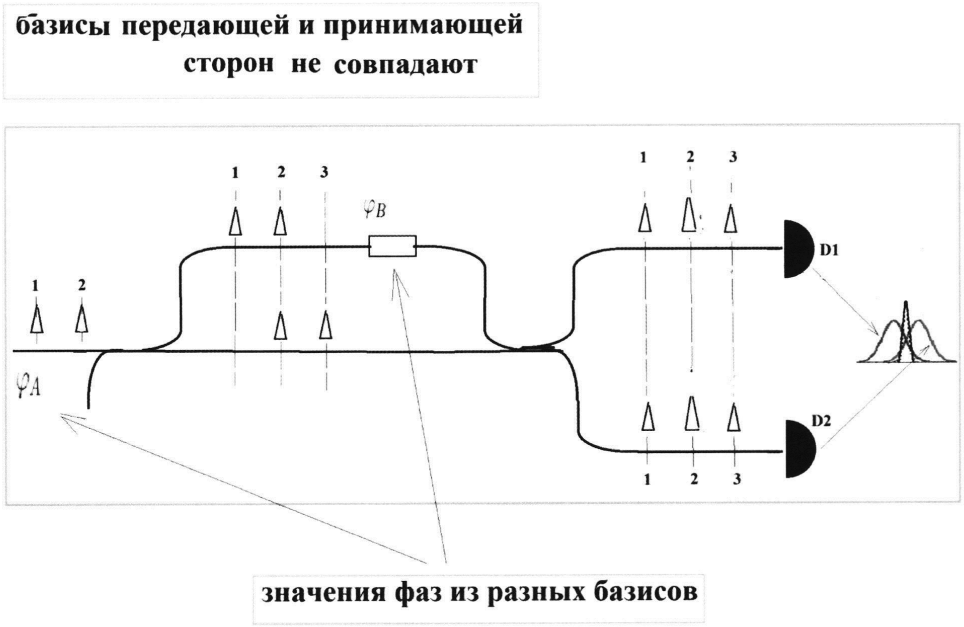
Фиг. 1

1

2

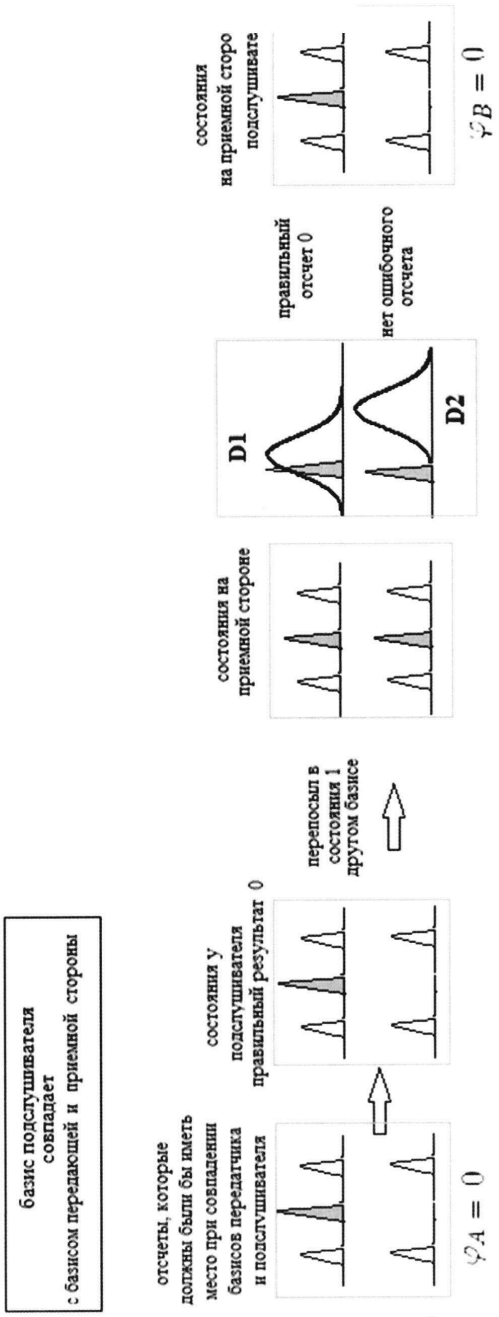

два значения фазы на принимающей стороне в каждом базисе
базисы передающей и принимающей сторон совпадают
одно значение фазы на принимающей стороне в каждом базисе
базис измерений +
базис +, посылал 1
D1
D2
1 2 3

Фиг.2

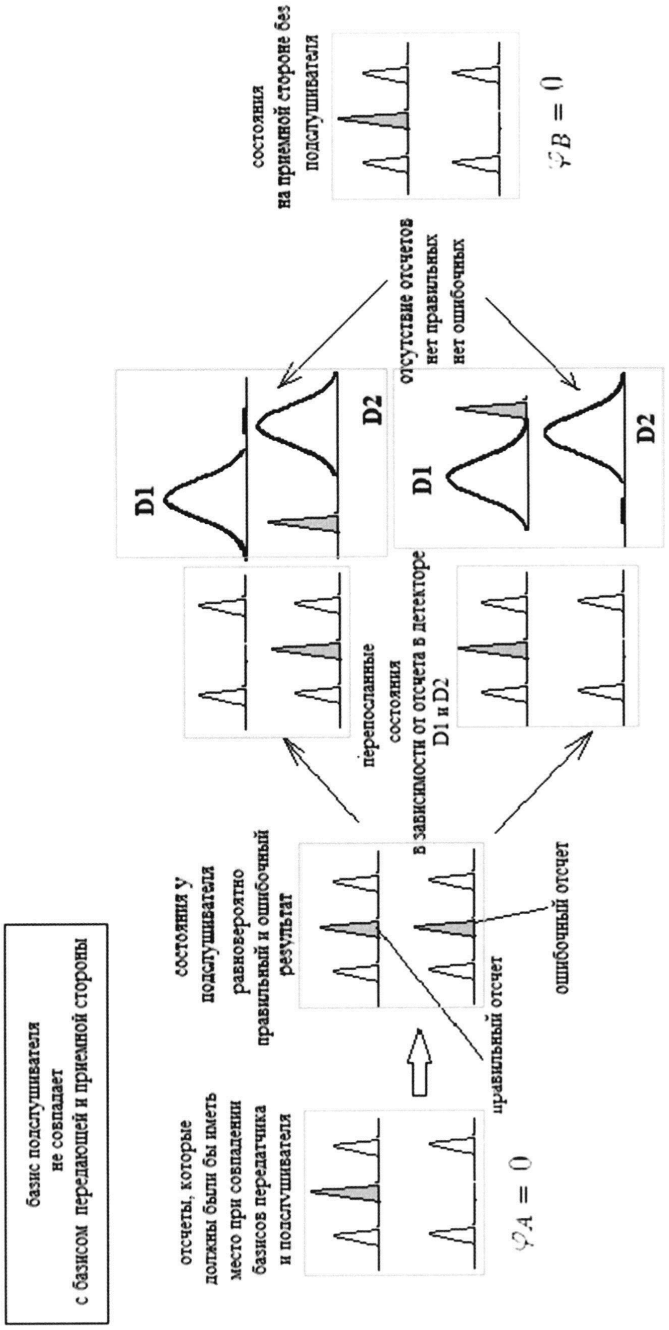

базисы передающей и принимающей сторон не совпадают
1
2
3
φB
1
2
φA
1
2
3
D1
D2
1
2
3
значения фаз из разных базисов

Фиг.3

4

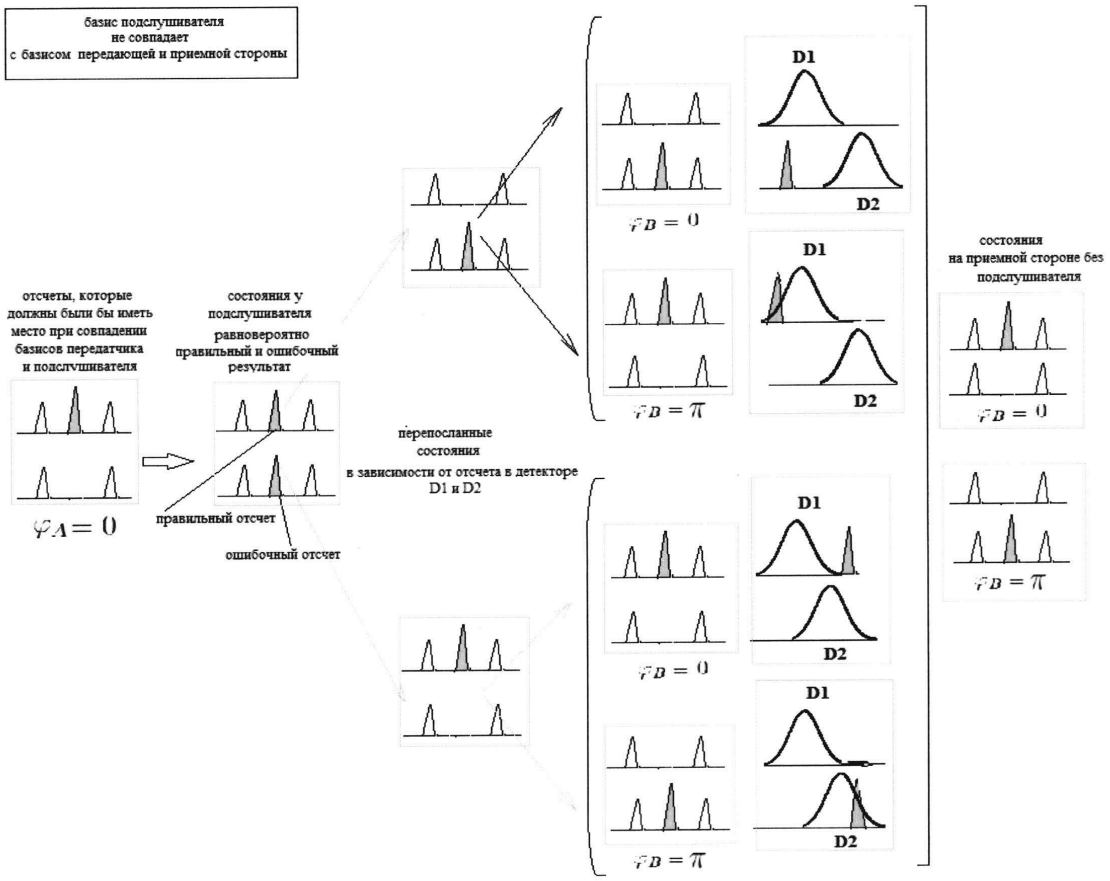

базис подслушивателя
совпадает
с базисом передающей и приемной стороны
отсчеты, которые
должны были бы иметь
место при совпадении
базисов передатчика
и подслушивателя
состояния у
подслушивателя
правильный результат 0
переносыл в
состояния 1
другом базисе
состояния на
приемной стороне
D1
D2
правильный
отсчет 0
нет ошибочного
отсчета
состояния
на приемной стороне
подслушивате
$\varphi_A = 0$
$\varphi_B = 0$

Фиг.4


базис подслушивателя
не совпадает
с базисом перелающей и приемной стороны
отсчеты, которые
должны были бы иметь
место при совпадении
базисов передатчика
и подслушивателя
состояния у
подслушивателя
равновероятно
правильный и ошибочный
результат
правильный отсчет
ошибочный отсчет
$\varphi A = 0$
перепосланные
состояния
в зависимости от отсчета в детекторе
D1 и D2
D1
D2
D1
D2
отсутствие отсчетов
нет правильных
нет ошибочных
состояния
на приемной стороне без
подслушивателя
$\varphi B = 0$

Фиг.5

6


базис подслушивателя
не совпадает
с базисом передающей и приемной стороны
отсчеты, которые
должны были бы иметь
место при совпадении
базисов передатчика
и подслушивателя
$\varphi_A = 0$
состояния у
подслушивателя
равновероятно
правильный и ошибочный
результат
правильный отсчет
ошибочный отсчет
перепосланные
состояния
в зависимости от отсчета в детекторе
D1 и D2
$\varphi_B = 0$
$\varphi_B = \pi$
D1
D2
состояния
на приемной стороне без
подслушивателя

Фиг.6