РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 706 175**(13) **C1**

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

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК
H04L 9/08 (2019.05); G06F 21/72 (2019.05)

(21)(22) Заявка: **2018146854, 27.12.2018**

(24) Дата начала отсчета срока действия патента:
27.12.2018

Дата регистрации:
14.11.2019

Приоритет(ы):
(22) Дата подачи заявки: **27.12.2018**

(45) Опубликовано: **14.11.2019** Бюл. № **32**

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):
Втюрина Анна Георгиевна (RU),
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 2566335 C1, 20.10.2015. RU 2621605 C2, 06.06.2017. RU 2671620 C1, 02.11.2018. RU 2665249 C1, 28.08.2018. US 2018/0191496 A1, 05.07.2018.**

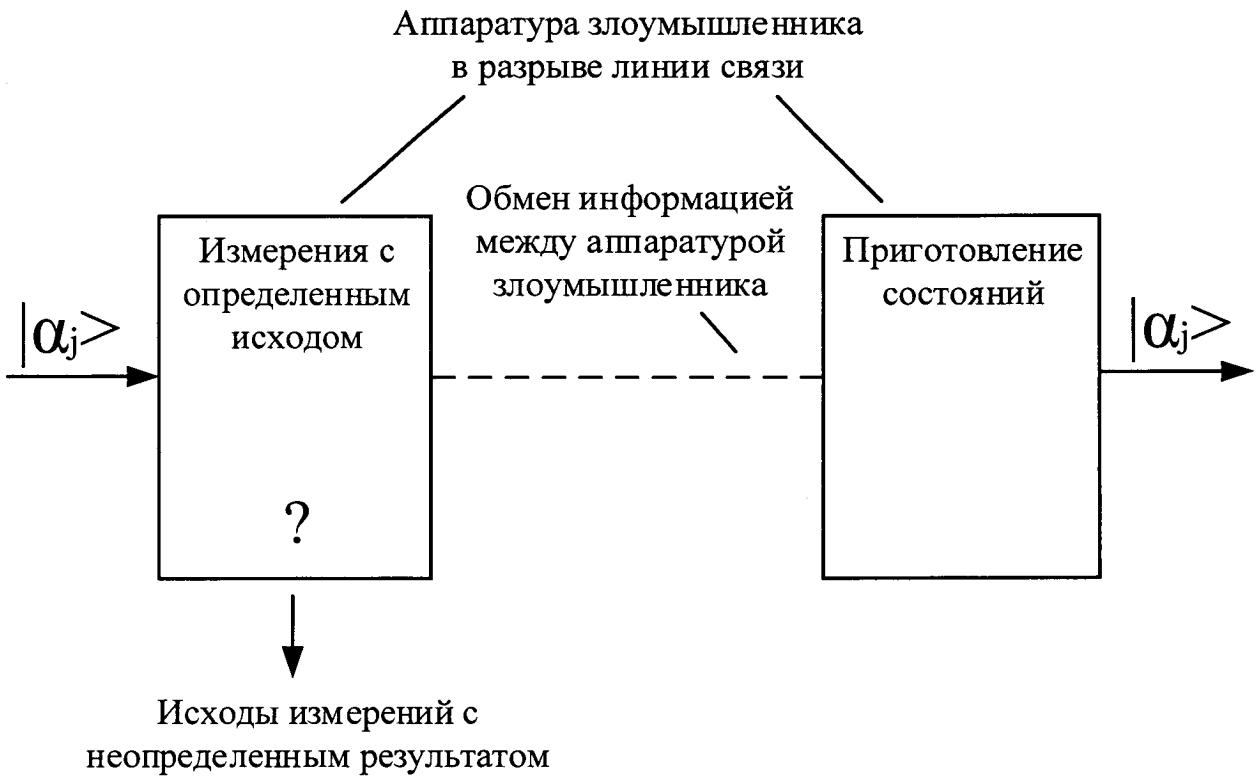
(54) Способ квантового распределения ключей в однопроходной системе квантового распределения ключей

(57) Реферат:

Изобретение относится к области квантовой криптографии. Технический результат заключается в обеспечении возможности получения секретного ключа заданной длины при установленной длине линии связи и неизменной системе КРК. Технический результат достигается за счет способа квантового распределения ключей, обеспечивающего увеличение длины линии связи с секретным распределением ключей по сравнению с известными протоколами за счет выбора равномерно распределенных по углу относительных фаз информационных квазиоднофотонных когерентных состояний, в которые кодируются биты ключа, и их числа, которое выбирается в зависимости от длины линии связи, на которую требуется обеспечить секретность передачи ключей. Переход на новую длину линии связи осуществляется увеличением числа базисов и, соответственно, числа информационных состояний. 4 ил.

RU 2706175 C1

RU 2706175 C1



Фиг. 1

RU 2706175 C1

RU 2706175 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 706 175**(13) **C1**

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

(12) ABSTRACT OF INVENTION

(52) CPC
H04L 9/08 (2019.05); G06F 21/72 (2019.05)

(21)(22) Application: **2018146854, 27.12.2018**

(24) Effective date for property rights:
27.12.2018

Registration date:
14.11.2019

Priority:
(22) Date of filing: **27.12.2018**

(45) Date of publication: **14.11.2019** Bull. № **32**

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

(72) Inventor(s):
Vtyurina Anna Georgievna (RU),
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 2706175 C1

(54) METHOD FOR KEY QUANTUM DISTRIBUTION IN SINGLE-PASS QUANTUM KEY DISTRIBUTION SYSTEM

(57) Abstract:

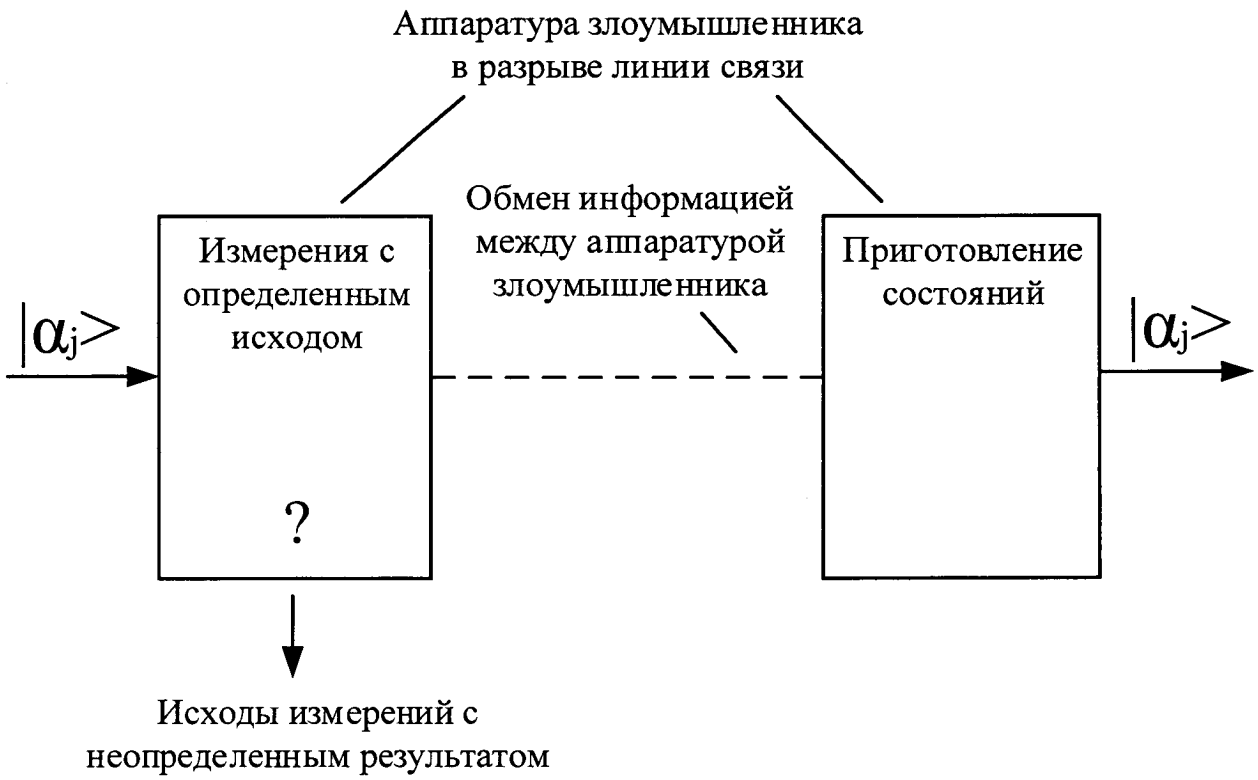
FIELD: cryptography.

SUBSTANCE: invention relates to the field of quantum cryptography. Technical result is achieved by a method of quantum key distribution, which increases the length of the communication line with secret distribution of keys compared to existing protocols by selecting uniformly distributed relative to the angle of relative phases of information quasi-one-photon coherent states, in which the key bits are encoded, and their number, which is selected depending on the communication line length, on which it is required to provide key transmission security. Switching to a new communication line length is carried out by increasing the number of bases and, correspondingly, the number of information states.

EFFECT: technical result consists in provision of possibility to obtain private key of preset length at established length of communication line and unchanged system of QKD.

1 cl, 4 dwg

RU 2706175 C1



Фиг. 1

RU 2706175 C1

RU 2706175 C1

Область техники, к которой относится изобретение

Предлагаемое изобретение относится к области квантовой криптографии - системам квантового распределения ключей (КРК), а более конкретно способам кодирования и передачи криптографических ключей с использованием сильно ослабленного когерентного излучения лазера - квазиоднофотонных квантовых состояний.

Уровень техники

Системы квантовой криптографии позволяют обнаруживать попытки несанкционированного вторжения в канал связи и гарантировать секретность передаваемых криптографических ключей, если длина линии связи не превышает некоторой критической величины.

В настоящее время не существует строго однофотонного источника излучения. В качестве квазиоднофотонных состояний используются ослабленные когерентные состояния лазерного излучения, которые являются квазиоднофотонными состояниями и имеют пуассоновскую статистику по числу фотонов. Квазиоднофотонный источника, потери в оптоволоконной линии связи и темновые шумы фотодетекторов являются факторами, ограничивающими дальность передачи ключей.

Основной причиной, ограничивающей дальность передачи ключей с гарантией их секретности, в известных способах кодирования в квантовой криптографии является так называемая атака с измерениями с определенным исходом.

Данная атака имеет место в канале с потерями и не строго однофотонном источнике информационных квантовых состояний и основана на следующем фундаментальном факте относительно измеримости квантовых состояний: квазиоднофотонные когерентные квантовые состояния являются линейно независимыми.

Линейная независимость квантовых состояний является необходимым и достаточным условием для существования измерений с определенным исходом. Для линейно независимых состояний измерения с определенным исходом позволяют различать такие состояния с определенностью, хотя и с некоторой вероятностью исхода. Причем такая атака может быть реализована при существующем уровне технологий, поскольку не требует у злоумышленника наличия долгосрочной квантовой памяти.

Атака злоумышленника состоит из следующих шагов. Поскольку волоконная линия связи в квантовой криптографии не контролируется, то злоумышленник разрывает линию связи в двух местах (фиг. 1): вблизи передающей части и принимающей, вставляет свою аппаратуру для проведения измерений квантовых состояний $|\alpha_j\rangle$ вблизи передающей части, производит измерения с определенным исходом. Вблизи принимающей части злоумышленник использует аппаратуру, аналогичную аппаратуре передающей части, для передачи своих квантовых состояний, аналогичных измеренным.

Если получен определенный исход, то есть определено передаваемое квантовое состояние и, соответственно, бит будущего ключа, то злоумышленник сообщает своему партнеру вблизи принимающей части, какое состояние послать на принимающую часть. В таких сериях, где злоумышленником был получен определенный исход, злоумышленник знает передаваемый бит ключа, не производит ошибок на принимающей части, поскольку передает правильные состояния, и не обнаруживается.

Если в какой-то посылке получен неопределенный исход измерений, то есть истинное передаваемое состояние злоумышленнику неизвестно (исход измерений «?» на фиг. 1), то партнер злоумышленника ничего не передает на принимающую часть, никаких отсчетов на принимающей части при этом не происходит.

Если вероятность потерь в исходной линии связи P_{Loss} больше, чем вероятность неопределенного исхода $P_?$, то потеря состояния, то есть отсутствие факта регистрации

состояния на принимающей части, списывается легитимными пользователями на потери в линии связи. Злоумышленник сохраняет общее число зарегистрированных состояний на принимающей части, поскольку посылает состояния непосредственно на принимающую часть через разрыв линии связи, то есть без потерь.

Начиная с некоторой длины линии связи и, соответственно, потерь в ней, злоумышленник знает весь передаваемый ключ, не производит ошибок на принимающей части, не меняет общего числа зарегистрированных посылок на принимающей части и не обнаруживается. Следовательно, система квантовой криптографии не обеспечивает секретность передаваемых ключей.

Таким образом, длина линии связи, до которой гарантируется секретность ключей, ограничена и определяется соотношением вероятности неопределенного исхода и вероятности потерь в линии связи. Поскольку потери в линии связи являются известными, определяются свойствами оптического волокна и их нельзя существенно уменьшить на существующем технологическом уровне, то увеличить дальность передачи ключей можно только за счет увеличения вероятности неопределенного исхода $P_?$ (фиг. 1) и, соответственно, уменьшения вероятности определенного исхода при измерениях злоумышленника. Значения этих вероятностей определяются используемым протоколом КРК, то есть структурой информационных квантовых состояний.

Известны различные способы увеличения дальности передачи ключей путем модификации протокола КРК, например, протоколы: BB84, SARG04, decoy state, COW (CohereNt ONe Way протокол) и др. (патент США №7359513, приоритет от 12.11.2003 г.; патент США №8995650, приоритет от 04.06.2010 г.; международная заявка WO 2006024939, опубл. 09.03.2006 г.).

Данные протоколы имеют различную дальность гарантированной секретной передачи ключей: протокол BB84 - дальность 25-60 км, протокол SARG04 - 60-80 км, протокол COW - дальность 80-115 км, то есть протоколы перекрывают различный диапазон длин линии связи.

Однако, разнородность протоколов приводит к тому, что при изменении длины линии связи необходимо переходить на другой протокол, причем для каждого протокола необходимо использовать свою оптоволоконную схему и блок управления, проводить отдельный анализ криптографической стойкости. Для ряда протоколов ввиду их непрозрачности и сложности полный анализ до сих пор не сделан, то есть критическая длина линии связи, до которой гарантируется распределение секретных ключей, по сути, точно неизвестна, что не позволяет надежно гарантировать секретность распределения ключей.

Это связано с тем, что неизвестно точное значение вероятности определенного исхода, которое и определяет критическую длину линии связи, до которой гарантируется секретное распределение ключей. Примером протокола с наибольшей дальностью передачи ключей является протокол COW. Для данного протокола точное значение длины линии связи, до которой гарантируется секретное распределение ключей, неизвестно. Это связано с тем, что состояния в протоколе являются распределенными - отдельные передаваемые серии квантовых состояний не являются независимыми, возмущение одного состояния влияет на другие состояния, по этой причине вычислить точную длину линии связи практически невозможно.

Таким образом, одной их основных задач выбора протокола КРК является выбор такого набора базисов и состояний, чтобы вероятность неопределенного исхода (вероятность успеха) была бы значительно больше вероятности общих потерь при выбранной длине линии связи: $P_{Loss} << P_?$.

Существует насущная практическая необходимость иметь набор однотипных протоколов или универсальный протокол, которые были бы прозрачны для анализа стойкости, обеспечивали бы максимальную дальность передачи ключей, могли бы быть реализованы на той же базовой оптоволоконной схеме и общей управляющей электронике, причем выбор протокола мог бы осуществляться автоматически в зависимости от длины оптоволоконного канала связи.

Кроме того, практическая необходимость требует увеличения длины линии связи, на которой протоколом гарантируется секретная передача ключей, по сравнению с той, которую могут на данный момент гарантировать известные протоколы.

Раскрытие изобретения

Техническим результатом является:

1) обеспечение возможности получения секретного ключа заданной длины при установленной длине линии связи и неизменной системе КРК,

2) обеспечение защиты от атаки с измерениями с определенным исходом.

Для этого предлагается способ квантового распределения ключей в однопроходной системе квантового распределения ключей, причем система включает

• передающую часть, содержащую

○ генератор случайных чисел,

○ лазер,

○ интерферометр,

○ фазовый модулятор,

○ блок управления;

• принимающую часть, содержащую о генератор случайных чисел,

○ интерферометр,

○ фазовый модулятор,

○ фотоприемный блок, имеющий однофотонный лавинный детектор для регистрации квантовых информационных состояний,

○ блок обработки,

○ блок управления;

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

• цифровую линию связи, соединяющую передающую и принимающую части;

способ заключается в том, что

• выбирают количество информационных состояний N, использующихся в протоколе квантового распределения ключей, и количество базисов K=N/2;

• вычисляют вероятность определенных исходов измерений информационных состояний:

$$P_D = N \min_r \left(\frac{1}{N} \sum_{j=0}^{N-1} \left(\exp\left(\mu \exp\left(\frac{i 2\pi j}{N} - 1 \right) \right) \exp\left(- \frac{i 2\pi j r}{N} \right) \right) \right),$$

где μ - среднее число фотонов при передаче информационных состояний;

$0 \le r \le N-1$;

• вычисляют длину секретного ключа l_S в битах в пересчете на серию переданных информационных состояний:

$l_S = 1 - \exp(-\mu\eta) - P_D$,

где η - квантовая эффективность однофотонного лавинного детектора;

• формируют в передающей части серию квазиоднофотонных когерентных состояний,

причем для каждого квазиоднофотонного когерентного состояния выбирают случайно и равновероятно состояние $|\alpha_j\rangle$, характеризующееся значением 0 или 1 внутри базисов, осуществляя равномерно распределенный по углу сдвиг по фазе;

• передают полученные квазиоднофотонные когерентные состояния из передающей части в принимающую часть по оптической линии связи;

• принимают квазиоднофотонные когерентные состояния в принимающей части;

• выбирают для регистрации состояний случайно, равновероятно и независимо от передающей части базисы измерений из числа K;

• получают результат измерений состояний как 0 или 1;

• сравнивают базисы измерений с базисами из передающей части;

• формируют первичный ключ, оставляя только те позиции квазиоднофотонных когерентных состояний, где базисы на передающей части и принимающей части совпали;

• обрабатывают первичный ключ, получая секретный ключ;

• сравнивают расчетную длину секретного ключа с полученной длиной секретного ключа;

• если длина секретного ключа меньше расчетной длины ключа, то увеличивают число информационных состояний N.

Технический результат достигается применением способа КРК, основанного на специальных квазиоднофотонных информационных состояниях с равномерным распределением по углу фаз (однородным распределением), в которые кодируются биты ключа, позволяющего точно вычислить длину линии и потери в ней, до которых гарантируется секретность ключей, и увеличить длину линии связи с секретным распределением ключей по сравнению с известными протоколами за счет равномерно распределенного по углу выбора относительных фаз квантовых состояний и их числа, которое выбирается в зависимости от длины линии связи, на которую требуется обеспечить секретность передачи ключей, тем самым обеспечивая защиту от атаки с измерениями с определенным исходом, заключающейся в возможности различения линейно независимых состояний с некоторой вероятностью и ограничивающей дальность передачи ключей с гарантией их секретности, при этом не требуются изменения оптической схемы системы и использование новой управляющей электроники. Переход на новую длину линии связи осуществляется на программном уровне увеличением числа базисов и, соответственно, числа информационных состояний.

Суть способа основана на специальном выборе информационных квазиоднофотонных когерентных состояний.

Информационными состояниями являются когерентные состояния $|\alpha_j\rangle = U^j|\alpha\rangle$ с равномерно распределенным по углу сдвигом по фазе

$$\alpha_j = e^{\frac{2\pi j}{N}i}\alpha, \quad (1)$$

где α - комплексное число, квадрат модуля которого определяет среднее число фотонов μ в когерентном состоянии,

N - число информационных состояний, которое выбирается в зависимости от длины линии, на которую требуется передавать ключи,

j=0, 1, … N-1

В предлагаемом способе используется K=N/2 базисов (пример для N=4 и N=8 приведен на фиг. 2). В каждом базисе имеется два состояния, состояния внутри базисов на фиг. 2 обозначены дугами.

Все информационные состояния получаются равномерно распределенным по углу сдвигом по фазе согласно (1).

Передающая часть случайным образом сначала выбирает базис, затем случайно и равновероятно выбирает состояние, отвечающее 0 или 1 внутри базиса, и посылает на принимающую часть.

В принимающей части случайно и независимо от передающей части выбирается базис измерений. Проводятся измерения в выбранном базисе, и их результат интерпретируется как 0 или 1. После передачи серии состояний, передающая и принимающая части через цифровую линию связи согласовывают (сравнивают) базисы серии переданных состояний - посылки, причем состояния в отдельных посылках являются независимыми. Если базисы для состояний передающей и принимающей частей для каждой посылки не совпадают, то такие позиции базисов отбрасываются. Если нет возмущений исходных информационных состояний, то в посылках, где базисы передающей и принимающей частей совпадали, возникает одинаковый результат - последовательность 0 и 1. На принимающей стороне возможны ошибки, и данную последовательность 0 и 1 обычно называют "сырой" или "неочищенный" ключ.

Атака с измерениями с определенным исходом возможна в реальном канале связи с потерями и базируется на фундаментальном свойстве квантовых состояний - линейной независимости, которая является необходимым и достаточным условием для таких измерений квантовых состояний. Иными словами, для линейно независимых состояний существуют измерения, которые позволяют различать такие состояния с определенностью, хотя и с некоторой вероятностью подобного исхода.

Злоумышленник в доле 5 переданных информационных квантовых состояний проводит атаку с измерениями с определенным исходом. В $\delta\cdot(1-P_?)$ доле переданных информационных квантовых состояний злоумышленник получает определенный результат измерения, а в доле $\delta\cdot P_?$ переданных информационных квантовых состояний - неопределенный результат. Далее злоумышленник отбрасывает эти информационные квантовые состояния с неопределенным исходом. В переданных информационных квантовых состояниях, где получен определенный исход, злоумышленник передает более интенсивные когерентные состояния $|\alpha_j\cdot e^{i\frac{\pi j}{2}}\rangle$ (где i - мнимая единица), которые гарантированно регистрируются на принимающей части. В остальных 1-δ информационных квантовых состояниях злоумышленник производит измерения, пытаясь различить информационные квантовые состояния с минимальной вероятностью ошибки.

Любое измерение в квантовой механике строится следующим образом. Каждому исходу измерений приписывается положительный эрмитов оператор - положительная операторно-значная мера (POVM) $M_j^+M_j$. Индекс j нумерует исходы измерений. Сумма операторов по всем исходам должна равняться единичным операторам, это гарантирует то, что сумма вероятностей по всем исходам при данном измерении, независимо от измеряемого квантового состояния, будет равна единице. Набор таких операторов является математическим описанием измерения и называется разложением единицы (единичного оператора). Вероятность каждого исхода измерений зависит от измерения - положительной операторно-значной меры и измеряемого квантового состояния.

Разложение единицы имеет вид:

$$I_B = \sum_j^N M_j^+ M_j + M_?^+ M_?,$$

где $M_j^+M_j$ и $M_?^+M_?$ - положительные операторно-значные меры (POVM), отвечающие за определенный и неопределенный исход соответственно.

Причем

$$Tr\left\{|\alpha_j\rangle_{BB}\langle\alpha_j|M_i M_i^+\right\} = P_{D_j}\delta_{i,j}$$

и

$$Tr\left\{|\alpha_j\rangle_{BB}\langle\alpha_j|M_? M_?^+\right\} = P_{?_j}.$$

Таким образом, если получен определенный исход, то точно известно, что входным было состояние $|\alpha_j\rangle$ и никакое другое. Неопределенный исход «?» может быть получен от любого состояния.

Вероятность успешного различения информационных квантовых состояний зависит от структуры этих состояний и степени их неортогональности. Типичная вероятность неопределенного исхода измерений составляет 10^{-2} (ScaraNi V., et al., Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations // Physical Review Letters, 92. 2004), что и определяет масштаб критических потерь P_{Loss} в линии связи, до которых гарантируется секретность ключа.

Если вероятность пропускания канала, то есть вероятность прохождения информационных квантовых состояний через линию связи меньше (соответственно, потери в канале больше), чем вероятность успешного различения информационных квантовых состояний (соответственно, вероятность неудачи при различении этих состояний), то протокол распределения ключей становится несекретным.

Атака с измерениями с определенным исходом устроена следующим образом: злоумышленник разрывает канал связи вблизи передающей и принимающей сторон, перехватывает информационные квантовые состояния от передающей части и измеряет их. Если успешно удалось различить информационные квантовые состояния (соответственно, биты будущего секретного ключа), то со второго разрыва линии связи вблизи принимающей части злоумышленник посылает на принимающую часть свои информационные квантовые состояния, которые совпадают с информационными квантовыми состояниями передающей части.

Если попытка различения информационных квантовых состояний неудачна, то злоумышленник ничего не посылает на принимающую часть.

Из-за потерь в линии связи блокирование части информационных квантовых состояний невозможно обнаружить - блокирование не уменьшает числа регистрируемых посылок из-за потерь в линии связи.

В итоге при атаке с измерениями с определенным исходом злоумышленник не производит ошибок на принимающей части, не меняет числа регистрируемых информационных квантовых состояний, знает все биты будущего секретного ключа и не обнаруживается.

Критическая длина линии связи, до которой можно гарантировать секретность ключа, определяется из равенства двух величин:

1) вероятности полной потери сигнала в канале связи,

2) вероятности неопределенного исхода измерения квантового состояния.

При определенной длине линии доля неопределенных исходов равна величине потерь в линии. Начиная с этой длины, злоумышленник знает весь передаваемый ключ и не производит ошибок на приемной части.

Атака с измерениями с определенным исходом описывается оператором, преобразующим квантовые состояния:

$$\mathcal{T}(|i_b\rangle_{AA}\langle i_b| \otimes |\alpha_{ib}\rangle_{BB}\langle\alpha_{ib}|) = \sum_j^N |i_b\rangle_{AA}\langle i_b|Tr\{M_j(|\alpha_{ib}\rangle_{BB}\langle\alpha_{ib}|)M_j^+\} \otimes$$

$$|\alpha_{ib}^*\rangle_{BB}\langle\alpha_{ib}^*| \otimes |i_b\rangle_{EE}\langle i_b| + |i_b\rangle_{AA}\langle i_b|Tr\{M_?(|\alpha_{ib}\rangle_{BB}\langle\alpha_{ib}|)M_?^+\} \otimes |vac\rangle_{BB}\langle vac| \otimes$$

$$\otimes |discard\rangle_{EE}\langle discard|$$

Для квантовых когерентных состояний с равномерно распределенным по углу сдвигом по фазе оптимальные измерения, минимизирующие вероятность неопределенного исхода, могут быть построены явно.

Найдем POVM для геометрически равномерно распределенных по углу квантовых состояний, которые минимизируют ошибку различения состояний у злоумышленника.

Спектральное разложение оператора U имеет вид:

$$U = \sum_{j=0}^{N-1} e^{i\frac{2\pi j}{N}} |\lambda_j\rangle\langle\lambda_j|,$$

где $|\lambda_j\rangle$ - собственные векторы оператора.

Набор векторов состояний в обратной решетке (точечной трехмерной решетке в абстрактном обратном пространстве, где расстояния имеют размерность обратной длины) также является набором геометрически равномерно распределенных по углу квантовых состояний, поэтому имеем:

$$|\alpha_j\rangle = \sum_{j=0}^{N-1} c_k e^{i\frac{2\pi jk}{N}} |\lambda_k\rangle,$$

$$|\alpha_j^{\perp}\rangle = \frac{1}{\sqrt{Z}} \sum_{j=0}^{N-1} \frac{1}{c_r^*} e^{i\frac{2\pi jr}{N}} |\lambda_r\rangle,$$

$$Z = \sum_{j=0}^{N-1} \frac{1}{|c_r|^2}.$$

При этом POVM, отвечающие за определенные исходы, выражаются следующим образом:

$$M_D = \sum_j^N M_j^+ M_j = \frac{1}{N^2} \sum_{j,r,r'} P_j C_{r'}^{*-1} C_{r'}^{-1} e^{i\frac{2\pi j(r-r')}{N}} |\lambda_{r'}\rangle\langle\lambda_r|$$

Для нижней границы вероятности определенных исходов как функции от среднего числа фотонов и числа базисов получаем:

$$P_D(N,\mu) \leq N \min_r (|c_r|^2) = N \min_r \left(\frac{1}{N} \sum_{j=0}^{N-1} e^{\mu\left(e^{i\frac{2\pi j}{N}}-1\right)} e^{-i\frac{2\pi jr}{N}} \right). \qquad (2)$$

Соответственно, структура квантовых когерентных состояний с равномерно распределенным по углу сдвигом по фазе определяет вероятность неопределенного исхода, для которой имеется точное решение:

$$P_? = 1 - \min_r \left| \frac{1}{N} \sum_{j=0}^{N_b-1} e^{\mu\left(e^{i\frac{2\pi j}{N_b}}-1\right)} e^{-i\frac{2\pi jr}{N_b}} \right|,$$

где $0 \leq r \leq N_b - 1$

Структура квантовых когерентных состояний с равномерно распределенным по углу сдвигом по фазе позволяет получить точное значение вероятности неопределенного исхода для измерений с определенным исходом. При рабочих параметрах однопроходной системы квантовой криптографии данная вероятность составляет не

более 10^{-6}.

Возможно из (2) получить длину секретного ключа (в пересчете на каждую зарегистрированную посылку - долю секретных бит) в зависимости от среднего числа фотонов μ и длины линии связи L:

$$l_s(N,\mu,L) = 1 - e^{-\eta\mu(L)} - P_D(N,\mu), \qquad (3)$$

где η - квантовая эффективность однофотонного лавинного детектора, установленного на принимающей части для регистрации квантовых информационных состояний,

$$\mu(L) = \mu 10^{-\frac{\delta L}{10}},$$

L - длина линии связи в километрах,

δ≈0,2 дБ/км - коэффициент удельных потерь в одномодовом оптическом волокне, использующемся в качестве линии связи,

N - число информационных состояний, которое предлагается выбирать в зависимости от длины линии (фиг. 3, 4).

Измерения при заданном числе состояний N, которое считается известным злоумышленнику, имеет N+1 исходов (фиг. 1), которые происходят случайно с определенной вероятностью. Если произошел один из N исходов, то злоумышленник точно знает передаваемое состояние, и посылает правильное состояние из второго разрыва линии на принимающую часть. При этом (N+1)-й исход является для злоумышленника неопределенным. В этом случае злоумышленник ничего не посылает на принимающую часть.

Критическая длина линии L, до которой гарантируется секретное распределение ключей, при заданных параметрах однопроходной системы квантовой криптографии определяется из условия равенства нулю длины секретного ключа в формуле (3):

$$l_s(N,\mu,L) = 0 \qquad (4)$$

Величина L определяется как корень трансцендентного уравнения (4).

Расчеты показывают, например, что, если длина линии до 60 км (фиг. 3), то выбирается число состояний N-4, число базисов в этом случае равно 2. Поскольку остаются только те посылки, где базисы совпадали (примерно половина исходной последовательности), то в этом случае скорость генерации секретных ключей будет в два раза выше, чем при числе информационных состояний N=8 и числе базисов, равном 4, поскольку при таком числе базисов остается только четверть исходной последовательности. Таким образом, при длине линии до 60 км можно обеспечить секретность ключей при числе состояний N=4 и обеспечить повышенную скорость передачи.

При длинах линии более 60 км (фиг. 4) для обеспечения секретности ключей можно перейти на протокол с увеличенным числом информационных состояний без изменения оптической части системы КРК.

Краткое описание чертежей

На фиг. 1 показана схема атаки злоумышленника с использованием измерений с определенным исходом передающей части.

На фиг. 2 показано распределение фаз когерентных состояний при различном числе N принимающей части.

На фиг. 3 показана зависимость относительной длины секретного ключа от длины линии связи L для N=4 информационных состояний при различных средних числах

фотонов μ: кривая 1: μ=0,25, кривая 2: μ=0,15, кривая 3: μ=0,1.

На фиг. 4 показана зависимость относительной длины секретного ключа от длины оптической линии связи L для N=S информационных состояний при различных средних числах фотонов μ: кривая 1: μ=1, кривая 2: μ=0,5, кривая 3: μ=0,25.

Осуществление изобретения

Предлагаемый способ может быть реализован, например, с использованием известной однопроходной системы КРК (патент РФ №2665249).

В составе системы два разнесенных независимых интерферометра Маха-Цандера с разной длиной плеч, один из которых находится на передающей части, а второй на принимающей части, а также фазовые модуляторы на передающей части и принимающей части.

В передающей части 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. Выбор фаз информационных состояний осуществляется наложением соответствующих напряжений на фазовые модуляторы на передающей части и принимающей части. 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 снова поступают на интерферометр Маха-Цандера, на котором пары пространственно разнесенных квазиоднофотонных когерентных состояний с различной фазой сводятся в один фотонный импульс. После чего оптические импульсы регистрируются однофотонным лавинным детектором. Получаемая интерференционная картина обладает видностью, которая будет максимальной и равной 1 в случае, когда количество единиц и нулей в принятом ключе будет одинаковым (так же, как и в передаваемом ключе). Отклонение видности от максимального значения однозначно связано с регистрируемой разностью количества нулей и единиц в ключе, а следовательно, с уровнем потерь в оптической линии связи.

Полученная последовательность нулей и единиц обрабатывается в блоке обработки, и система КРК получает секретный криптографический ключ, готовый к использованию.

Далее происходит оценка вероятности потерь в линии связи P_{Loss} и вероятности измерений с неопределенным исходом $P_?$ и, соответственно, доли секретного ключа, доступного злоумышленнику. Если вероятность потерь в линии связи больше, чем вероятность неопределенного исхода $P_{Loss}>P_?$, то секретность полученного криптографического ключа не гарантируется протоколом КРК с используемым числом базисов и информационных состояний N. Для увеличения вероятности неопределенного исхода $P_?$ и, соответственно, уменьшения вероятности определенного исхода при измерениях злоумышленника с помощью управляющих сигналов в блоке управления происходит увеличение числа информационных состояний N, при этом не требуется изменение оптической схемы системы КРК или перепрограммирование управляющей электроники.

Применение предлагаемого способа распределения ключей позволяет поддерживать

требуемый уровень секретности криптографического ключа при заданной длине линии связи.

(57) Формула изобретения

Способ квантового распределения ключей в однопроходной системе квантового распределения ключей, причем система включает:

передающую часть, содержащую

генератор случайных чисел,

лазер,

интерферометр,

фазовый модулятор,

блок управления;

принимающую часть, содержащую

генератор случайных чисел,

интерферометр, фазовый модулятор,

фотоприемный блок, имеющий однофотонный лавинный детектор для регистрации квантовых информационных состояний,

блок обработки,

блок управления;

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

способ заключается в том, что

выбирают количество информационных состояний N, использующихся в протоколе квантового распределения ключей, и количество базисов:

K=N/2;

вычисляют вероятность определенных исходов измерений информационных состояний:

$$P_D = N \min_r \left(\frac{1}{N} \sum_{j=0}^{N-1} (\exp(\mu \exp(\frac{i2\pi j}{N} - 1)) \exp(-\frac{i2\pi jr}{N}) \right),$$

где μ - среднее число фотонов при передаче информационных состояний;

0≤r≤N-1;

вычисляют длину секретного ключа ls в битах в пересчете на серию переданных информационных состояний:

$l_S = 1 - \exp(-\mu\eta) - P_D$,

где η - квантовая эффективность однофотонного лавинного детектора; формируют в передающей части серию квазиоднофотонных когерентных состояний, причем для каждого квазиоднофотонного когерентного состояния выбирают случайно и равновероятно состояние $|\alpha_j\rangle$, характеризующееся значением 0 или 1 внутри базисов, осуществляя равномерно распределенный по углу сдвиг по фазе;

передают полученные квазиоднофотонные когерентные состояния из передающей части в принимающую часть по оптической линии связи; принимают квазиоднофотонные когерентные состояния в принимающей части;

выбирают для регистрации состояний случайно, равновероятно и независимо от передающей части базисы измерений из числа K;

получают результат измерений состояний как 0 или 1; сравнивают базисы измерений

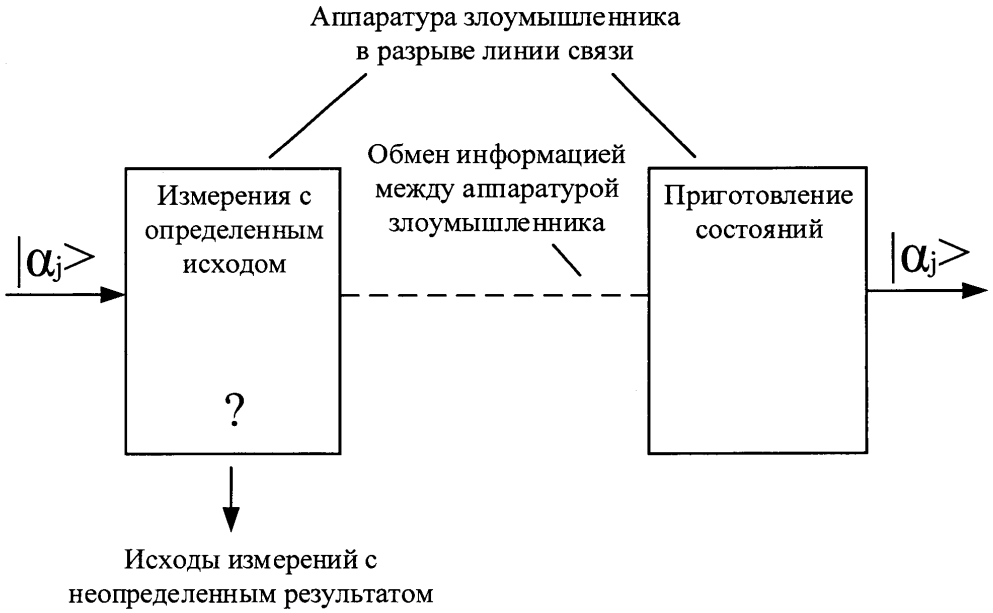
с базисами из передающей части; формируют первичный ключ, оставляя только те позиции квазиоднофотонных когерентных состояний, где базисы на передающей части и принимающей части совпали;

обрабатывают первичный ключ, получая секретный ключ;

сравнивают расчетную длину секретного ключа с полученной длиной секретного ключа;

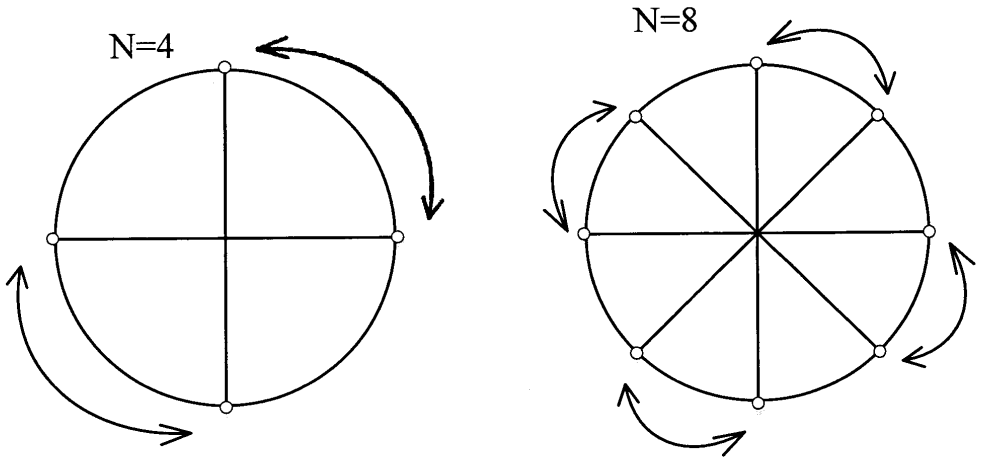
если длина секретного ключа меньше расчетной длины ключа, то увеличивают число информационных состояний N.

1


Аппаратура злоумышленника
в разрыве линии связи
Обмен информацией
между аппаратурой
злоумышленника
Измерения с
определенным
исходом
?
Приготовление
состояний
|αj>
|αj>
Исходы измерений с
неопределенным результатом

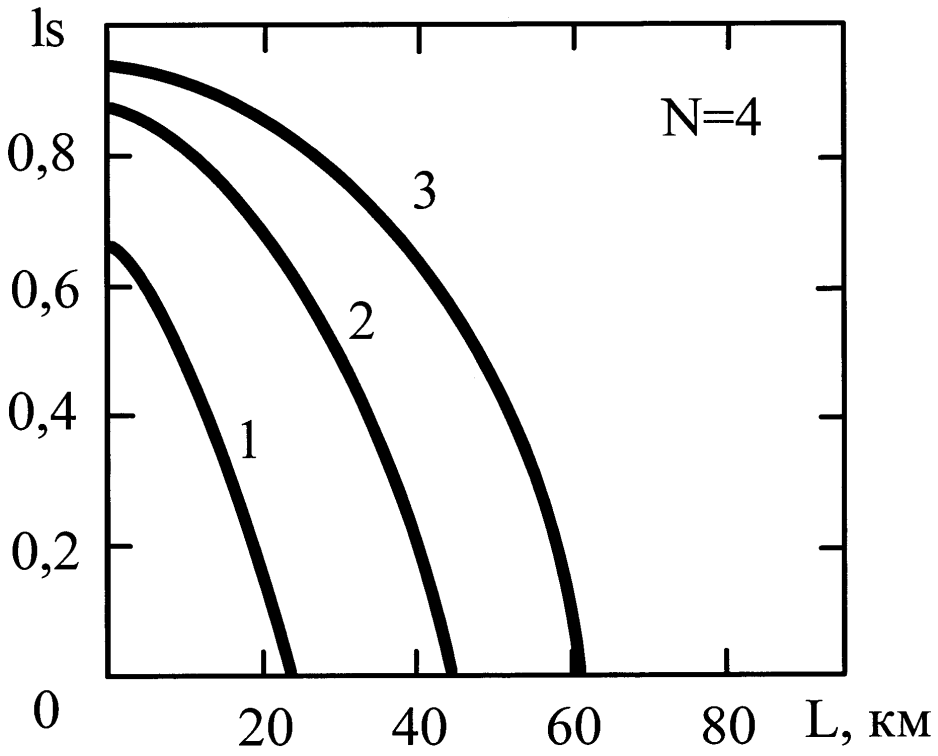
Фиг. 1

2



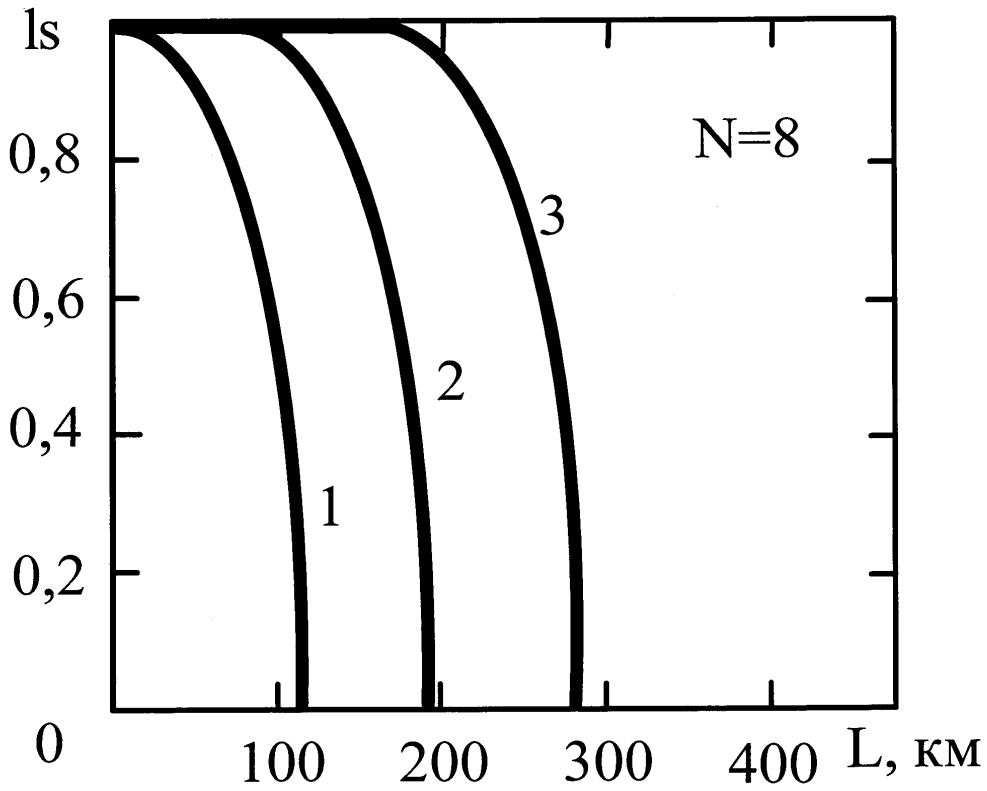
Фиг. 2

3



Фиг. 3

4



Фиг. 4