РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2 736 870**(13) **C1**

(51) МПК
H04L 9/08 (2006.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК
H04L 9/08 (2020.08); H04L 9/0852 (2020.08); G06F 21/72 (2020.08)

(21)(22) Заявка: **2019144324, 27.12.2019**

(24) Дата начала отсчета срока действия патента:
27.12.2019

Дата регистрации:
23.11.2020

Приоритет(ы):
(22) Дата подачи заявки: **27.12.2019**

(45) Опубликовано: **23.11.2020** Бюл. № **33**

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),
Жиляев Андрей Евгеньевич (RU)

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

(56) Список документов, цитированных в отчете о поиске: **KZ 27358 A4, 16.09.2013. RU 2708511 C1, 09.12.2019. RU 2621605 C2, 06.06.2017. US 20180191496 A1, 05.07.2018. RU 2454810 C1, 27.06.2012.**

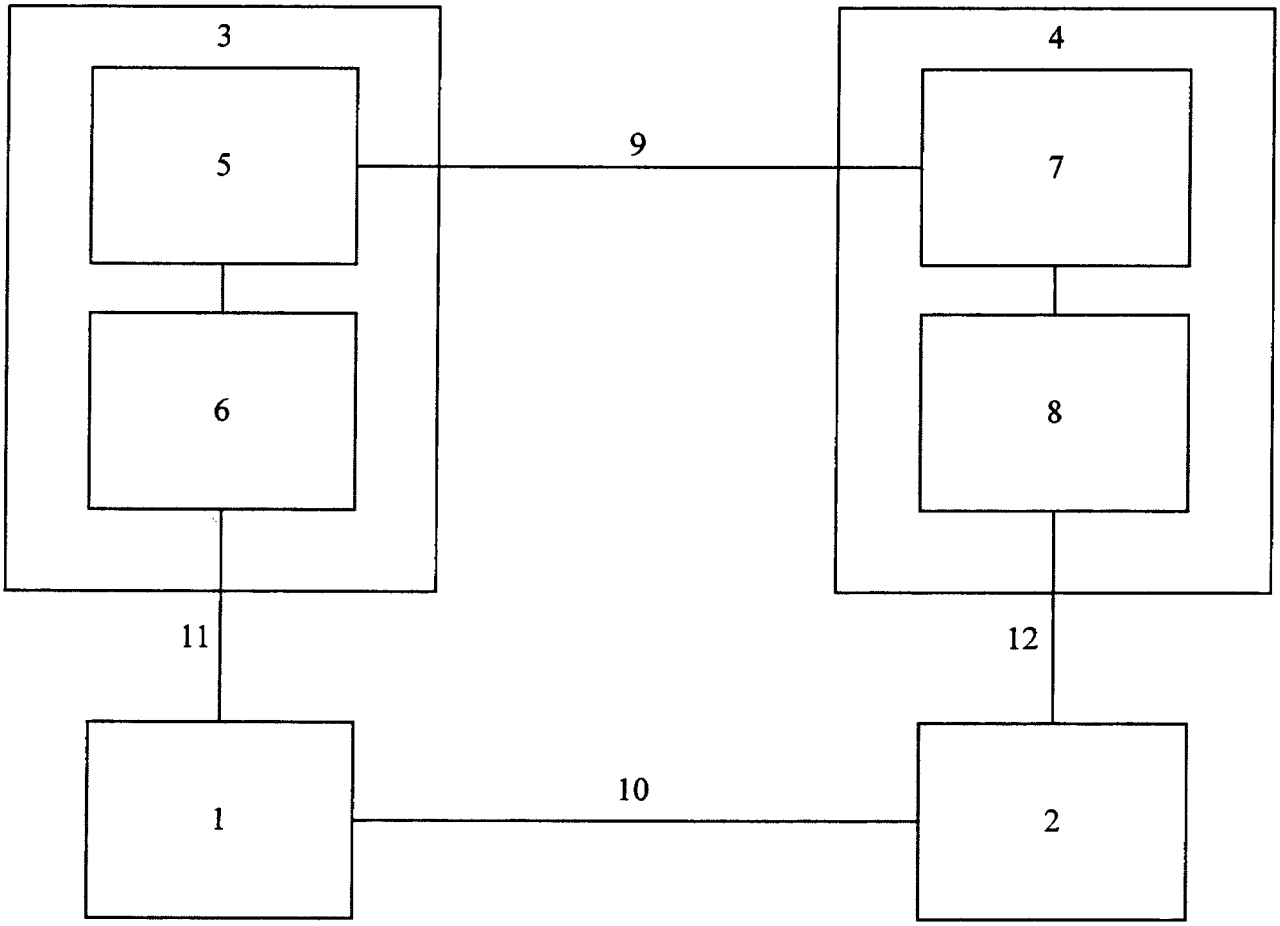
(54) Комплекс для защищенной передачи данных в цифровой сети передачи данных с использованием однопроходной системы квантового распределения ключей и способ согласования ключей при работе комплекса

(57) Реферат:

Изобретение относится к защите информации. Технический результат заключается в повышении защищенности передаваемых пользовательских данных, в повышении надежности комплекса, в повышении стойкости квантовых ключей, вырабатываемых системой квантового распределения ключей (КРК), за счет аутентификации служебных данных системы КРК на ключах аутентификации, сформированных из квантовых ключей, и аутентификации служебных данных системы КРК целиком, до разбиения на блоки, используемые при передаче по цифровой линии связи, и последующего шифрования служебных данных системы КРК. В комплексе используется транспортная линия связи, соединяющая два шифратора и два узла системы КРК. Канал передачи системы КРК состоит из аутентифицированного с использованием квантовых ключей канала передачи служебной информации и квантовых ключей из приемного узла системы КРК в сопряженный шифратор и обратно, аутентифицированного с использованием квантовых ключей канала передачи пользовательских данных между шифраторами, аутентифицированного с использованием квантовых ключей канала передачи служебной информации и квантовых ключей из передающего узла системы КРК в сопряженный шифратор и обратно. 2 н.п. ф-лы, 1 ил.

RU 2736870 C1

RU 2736870 C1



RU 2736870 C1

RU 2736870 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 736 870**(13) **C1**

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

(12) ABSTRACT OF INVENTION

(52) CPC
H04L 9/08 *(2020.08);* ***H04L 9/0852*** *(2020.08);* ***G06F 21/72*** *(2020.08)*

(21)(22) Application: **2019144324, 27.12.2019**

(24) Effective date for property rights:
27.12.2019

Registration date:
23.11.2020

Priority:
(22) Date of filing: **27.12.2019**

(45) Date of publication: **23.11.2020** Bull. № **33**

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),
Zhilyaev Andrej Evgenevich (RU)

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

RU 2736870 C1

(54) COMPLEX FOR SECURE DATA TRANSMISSION IN DIGITAL DATA NETWORK USING SINGLE-PASS QUANTUM KEY DISTRIBUTION SYSTEM AND METHOD OF KEYS ADJUSTMENT DURING OPERATION OF SYSTEM

(57) Abstract:

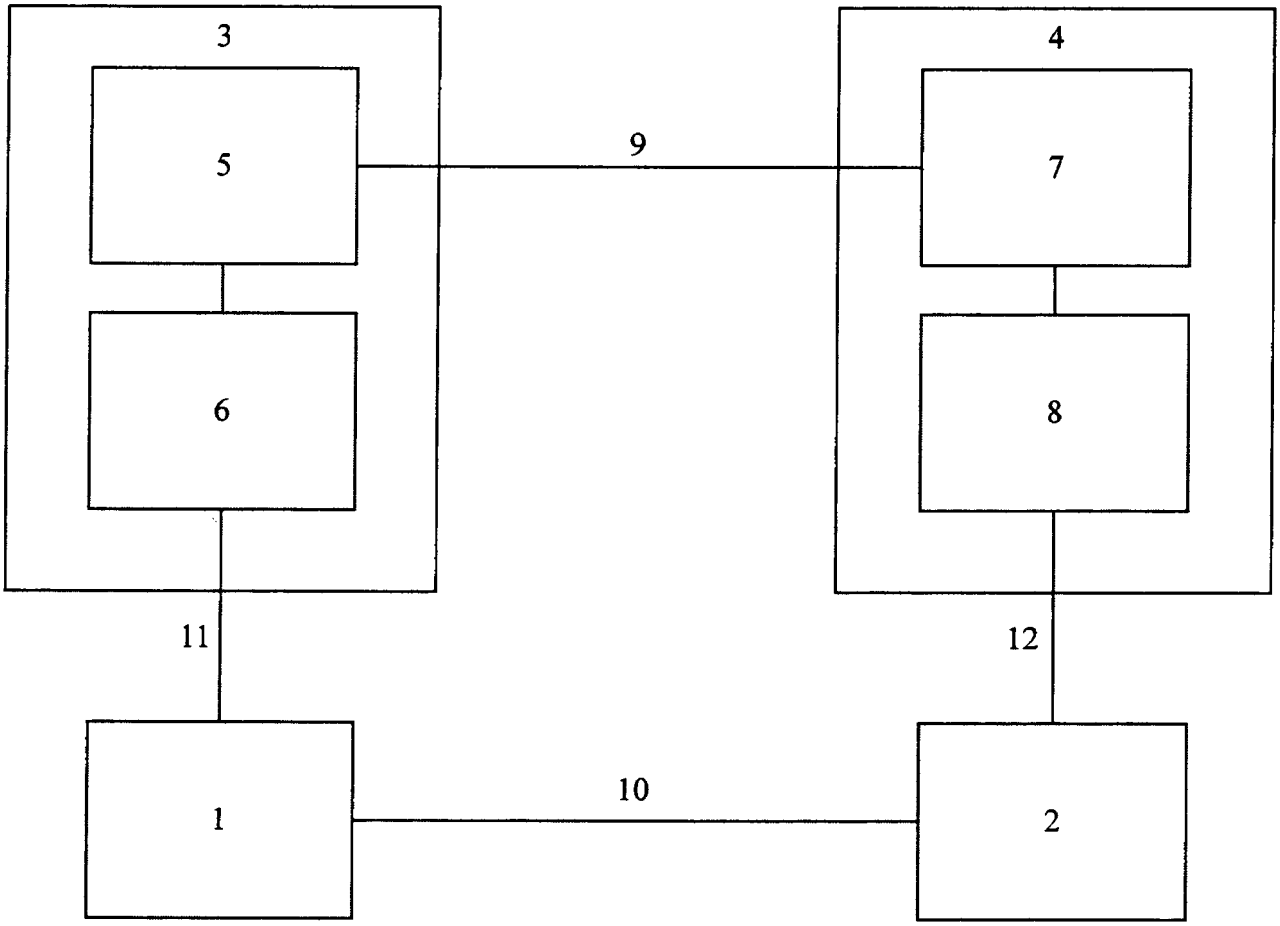
FIELD: physics.

SUBSTANCE: invention relates to information protection. Complex employs a transport communication line connecting two encoders and two QKD system units. Channel for transmitting an QKD system consists of a service information service channel authenticated using quantum keys and quantum keys from the receiving system of the QKD system to the conjugate encoder and back, authenticated using the quantum keys of the user data transmission channel between the encoders, authenticated using quantum keys of channel of service information transmission and quantum keys from transmitting node of QKD system to conjugate encoder and back.

EFFECT: high security of transmitted user data, high reliability of the complex, high durability of quantum keys generated by the quantum key distribution system (QKD), due to authentication of QKD system service data on authentication keys formed from quantum keys, and authentication of service data of the QKD system as a whole, before breaking down into blocks used when transmitting over a digital communication line, and subsequent encryption of service data of the QKD system.

2 cl, 1 dwg

RU 2736870 C1



RU 2736870 C1

RU 2736870 C1

Область техники, к которой относится изобретение

Предполагаемое изобретение относится к области криптографической защиты информации и передачи данных, а более конкретно, системам криптографической защиты информации, использующим для повышения защищенности передаваемой информации ключи, получаемые из квантовых ключей от сопряженной системы квантового распределения ключей.

Уровень техники

Для защиты передаваемой информации в цифровых сетях передачи данных перспективным является использование систем квантового распределения ключей (КРК). Использование квантово-криптографической аппаратуры защиты информации может обеспечить доставку абонентам симметричного ключа для зашифрования и расшифрования передаваемых пользовательских данных, а также оперативную замену ключа в соответствии с требованиями безопасности.

Известен способ и устройство для передачи информации с использованием технологии КРК (заявка США №20180054304, приоритет от 19.08.2016 г.), в котором коммуникационное устройство состоит из модуля загрузки, модуля контроля потока и модуля криптографической обработки, а способ предусматривает передачу и использование ключей в устройстве. Модуль загрузки предоставляет криптографические ключи, полученные с помощью технологии КРК. В случае, если при получении данных коммуникационным устройством отсутствует криптографический ключ, модуль контроля потока выполняет одно из трех действий: отбрасывает (удаляет данные), сохраняет данные в буфер или добавляет к данным метку, что криптографический ключ не был предоставлен, с последующей передачей данных в модуль криптографической обработки. При получении данных от модуля контроля потока модуль криптографической обработки производит криптографическую обработку (зашифрование) данных с использование криптографического ключа.

С помощью данного устройства реализуется система передачи информации, состоящая из устройств генерации, производящих криптографические ключи с помощью технологии КРК, и коммуникационных устройств, описанных выше.

Данное устройство и способ имеют следующие недостатки.

Если в течении продолжительного промежутка времени отсутствует криптографический ключ, то защищенная передача данных прерывается. При этом отбрасывание данных может быть недопустимым в силу характера передаваемых данных, а размер буфера для данных, ожидающих ключа - ограниченным, то есть выполнение первого действия модулем контроля потока может быть запрещено, а выполнение второго невозможно из-за заполненного буфера данных.

Ключи, передаваемые в два коммуникационных устройства системы, в общем случае могут быть различны из-за непредвиденных ошибок. Однако проверка на идентичность загружаемых ключей не производится, как и контроль использования одного и того же ключа для зашифрования и расшифрования данных, что может привести к невозможности расшифрования в одном коммуникационном устройстве данных, зашифрованных на другом ключе в другом коммуникационном устройстве. Таким образом, становится невозможно выполнение устройством своего функционального предназначения по передаче информации.

Известен способ аутентификации и устройство для его осуществления для системы квантовой криптографии (заявка США №20190238326, приоритет от 29.01.2018 г.); способ заключается в сравнении последовательностей, переданных по квантовому каналу передачи в позициях совпадающих базисов.

Этот способ имеет следующий недостаток: аутентифицируются непосредственно устройства квантовой криптографии, но не данные, передаваемые в процессе выработки квантового ключа, а именно: служебные сообщения по согласованию базисов измерений, исправлению ошибок и этапа усиления секретности. Таким образом, не гарантируется целостность и аутентичность этих служебных данных, и нарушитель может осуществить атаку «человек посередине», встроившись в квантовый и классический канал системы КРК и навязывая служебный трафик.

Также известен способ и устройство для шифрования с использованием технологии КРК (заявка США №20050063547, приоритет от 03.05.2004 г.), в котором устройство состоит

• из первого и второго получающего/передающего узла, соединенных соответственно с первым и вторым зашифровывающим/расшифровывающим процессором;

• первой и второй станции КРК, соединенных соответственно с первым и вторым зашифровывающим/расшифровывающим процессором и адаптированных для обмена квантовыми ключами и передачи их в первый и второй зашифровывающий/расшифровывающий процессоры;

• первым и вторым узлами классического распределения ключей, соединенных соответственно с первым и вторым зашифровывающим/расшифровывающим процессором и адаптированных к обмену классическими ключами и передачи классических ключей в первый и второй зашифровывающий/расшифровывающий процессор.

Зашифровывающий/расшифровывающий процессоры адаптированы для получения сигналов от одной получающей/передающей станции; зашифрования сигналов с использованием сессионного ключа, полученного в зашифровывающем/расшифровывающем процессоре путем сложения операцией XOR квантового и классического ключа; передачи зашифрованного сигнала на другую получающую/передающую станцию.

В устройстве реализуется способ передачи зашифрованных сигналов между первой и второй приемной/передающей станциями, включающий:

• передачу первого открытого сигнала с первой приемной/передающей станции на первый зашифровывающий/зашифровывающий процессор классической системы шифрования, содержащей также второй зашифровывающий/расшифровывающий процессор,

• обмен квантовыми ключами между первым и вторым узлом КРК системы КРК и предоставление квантовых ключей первому и второму зашифровывающему/расшифровывающему процессору,

• обмен классическими ключами между первой и второй классическими станциями и предоставление классических ключей первому и второму зашифровывающему/расшифровывающему процессору,

• формирование сессионного ключа путем сложения операцией XOR полученных классического и квантового ключа,

• формирование зашифрованного сигнала из первого открытого сигнала на первом зашифровывающем/расшифровывающем процессоре с использованием сессионного ключа, сформированного на первом процессоре,

• формирование расшифрованного сигнала из зашифрованного сигнала, полученного от первого зашифровывающего/расшифровывающего процессора на втором зашифровывающем/расшифровывающем процессоре с использованием сессионного ключа, сформированного на втором процессоре,

• передачу второго открытого сигнала на вторую приемную/передающую станцию.

Известное устройство и способ выбраны в качестве прототипов.

Однако известное техническое решение имеет ряд недостатков.

Контроль идентичности используемых ключей (квантовых и классических) в зашифровывающем/расшифровывающем процессорах производится передачей идентификаторов ключей в открытом виде по линии связи между процессорами, что может вызвать навязывание использования различных сессионных ключей для зашифрования и расшифрования сигнала в процессоре.

Применение в изобретении внешнего источника классических ключей в целях частого распределения ключей требует использования технологий, основанных на ассиметричной криптографии, что приводит к увеличению рисков компрометации распределяемых ключей.

Недостатком изобретения является также наличие отдельных каналов взаимодействия для системы КРК и системы обмена классическими ключами, что повышает затраты на создание и развертывание устройства.

Раскрытие сущности изобретения

Техническим результатом является:

1) повышение защищенности передаваемых пользовательских данных;

2) повышение надежности комплекса, в том числе в случае искажений (случайных или преднамеренных), вносимых локальной линией связи; в случае непредвиденных или преднамеренных кратковременных сбоев системы КРК, выражающихся во временном прекращении генерации квантовых ключей; в случае низкой скорости генерации квантовых ключей и/или генерации квантовых ключей малой длины; а также в случае навязывания ложных идентификаторов ключей;

3) снижение затрат на создание, развертывание и эксплуатацию комплекса за счет уменьшения числа классических линий связи;

4) повышение стойкости квантовых ключей, вырабатываемых системой КРК, за счет аутентификации служебных данных системы КРК на ключах аутентификации, сформированных из квантовых ключей, и аутентификации служебных данных системы КРК целиком, до разбиения на блоки, используемые при передаче по цифровой линии связи, и последующего шифрования служебных данных системы КРК.

Для этого предлагается комплекс для защищенной передачи данных в цифровой сети передачи данных с использованием однопроходной системы квантового распределения ключей, имеющий в составе

• передающий узел системы квантового распределения ключей (КРК), включающий

o передающий модуль выработки квантовых ключей, o модуль согласования ключей передающего узла;

o приемный узел системы КРК, включающий

• приемный модуль выработки квантовых ключей, o модуль согласования ключей приемного узла;

• 1-й шифратор, связанный с модулем согласования ключей передающего узла;

• 2-й шифратор, связанный с модулем согласования ключей приемного узла;

причем

• передающий модуль выработки квантовых ключей связан с приемным модулем выработки квантовых ключей квантовой линией связи, выполненной в виде оптоволоконной линии;

• 1-й шифратор связан со 2-м шифратором транспортной линией связи, выполненной в виде цифровой сети передачи данных;

• 1-й шифратор связан с модулем согласования ключей передающего узла посредством 1-й локальной линии связи (1-я ЛС);

• 2-й шифратор связан с модулем согласования ключей приемного узла посредством 2-й локальной линии связи (2-я ЛС);

• 1-й шифратор связан с внешней цифровой сетью передачи данных;

• 2-й шифратор связан с внешней цифровой сетью передачи данных; при этом

• передающий модуль выработки квантовых ключей выполнен с возможностью

○ генерировать случайные числа,

○ формировать квантовые информационные состояния,

○ отправлять квантовые информационные состояния по квантовой линии связи в приемный модуль выработки квантовых ключей,

○ вырабатывать квантовые ключи совместно с приемным модулем выработки квантовых ключей путем обработки информации, полученной из квантовых информационных состояний;

• модуль согласования ключей передающего узла выполнен с возможностью

○ формировать ключи аутентификации и ключи шифрования на основе квантовых ключей,

○ согласовывать ключи аутентификации и ключи шифрования с ключами аутентификации и ключами шифрования, сформированными модулем согласования ключей приемного узла,

○ принимать данные из 1-го шифратора по 1-й ЛС,

○ передавать данные в 1-й шифратор по 1-й ЛС;

• приемный модуль выработки квантовых ключей выполнен с возможностью

○ генерировать случайные числа,

○ принимать квантовые информационные состояния по квантовой линии связи из передающего модуля выработки квантовых ключей,

○ обрабатывать квантовые информационные состояния,

○ вырабатывать квантовые ключи совместно с передающим модулем выработки квантовых ключей путем обработки информации, полученной из квантовых информационных состояний;

• модуль согласования ключей приемного узла выполнен с возможностью

○ формировать ключи аутентификации и ключи шифрования на основе квантовых ключей,

○ согласовывать ключи аутентификации и ключи шифрования с ключами аутентификации и ключами шифрования, сформированными модулем согласования ключей передающего узла,

○ принимать данные из 2-го шифратора по 2-й ЛС,

○ передавать данные во 2-й шифратор по 2-й ЛС;

• 1-й шифратор выполнен с возможностью

○ принимать ключи шифрования и служебные данные из модуля согласования ключей передающего узла по 1-й ЛС,

○ передавать служебные данные в модуль согласования ключей передающего узла по 1-й ЛС,

○ принимать данные из внешней цифровой сети передачи данных,

○ зашифровывать данные, поступившие в него по внешней цифровой сети передачи данных или по 1-й ЛС, с использованием ключей шифрования,

- передавать данные, зашифрованные с использованием ключей шифрования, по транспортной линии связи,
- расшифровывать данные, поступившие из транспортной линии связи, с использованием ключей шифрования,
- передавать данные во внешнюю цифровую сеть передачи данных;

• 2-й шифратор выполнен с возможностью

- принимать ключи шифрования и служебные данные из модуля согласования ключей приемного узла по 2-й ЛС,
- передавать служебные данные в модуль согласования ключей приемного узла по 2-й ЛС,
- принимать данные из внешней цифровой сети передачи данных,
- зашифровывать данные, поступившие в него по внешней цифровой сети передачи данных или по 2-й ЛС, с использованием ключей шифрования,
- передавать данные, зашифрованные с использованием ключей шифрования, по транспортной линии связи,
- расшифровывать данные, поступившие из транспортной линии связи, с использованием ключей шифрования,
- передавать данные во внешнюю цифровую сеть передачи данных.

Предлагается также способ согласования ключей при работе комплекса, заключающийся в том, что

• выбирают квантовый протокол;

• выбирают размер блока равным b, где b кратно степени целого числа 2;

• выбирают размер ключа шифрования равным n блоков;

• выбирают размер ключа аутентификации равным m блоков;

• выбирают минимальный объем накопленного квантового ключа равным Key=m+n блоков;

• устанавливают значение счетчика ключей аутентификации в модуле согласования ключей передающего узла M1=1;

• устанавливают значение счетчика ключей аутентификации в модуле согласования ключей приемного узла M2=2;

• устанавливают значение счетчика ключей шифрования в модуле согласования ключей передающего узла N1=1;

• устанавливают значение счетчика ключей шифрования в модуле согласования ключей приемного узла N2=2;

• формируют текущий ключ аутентификации размером m блоков, выполняя следующие действия:

- добавляют к ключу аутентификации идентификатор в виде блока данных, содержащий значение счетчика M1 и значение признака ключа аутентификации;
- увеличивают значение счетчика M1 на 1;

• формируют текущий ключ шифрования размером n блоков, выполняя следующие действия:

- добавляют к ключу шифрования идентификатор в виде блока данных, содержащий значение счетчика N1 и значение признака ключа шифрования;
- увеличивают значение счетчика N1 на 1;

• загружают текущий ключ аутентификации в модули согласования ключей приемного и передающего узла;

• загружают текущий ключ шифрования в 1-й и 2-й шифраторы;

• (А) накапливают квантовые ключи в модулях согласования ключей передающего и приемного узлов системы КРК, выполняя следующие действия:

○ (Б) вырабатывают квантовый ключ в передающем и приемном модулях выработки квантовых ключей согласно выбранному квантовому протоколу, причем в ходе выполнения квантового протокола в части передачи служебных данных от передающего к приемному модулю выработки квантового ключа выполняют следующие действия:

■ формируют служебное сообщение из служебных данных в передающем модуле выработки квантовых ключей;

■ передают служебные данные из передающего модуля выработки квантовых ключей в модуль согласования ключей передающего узла;

■ осуществляют аутентификацию служебного сообщения с помощью текущего ключа аутентификации в модуле согласования ключей передающего узла;

■ передают аутентифицированное служебное сообщение по 1-й ЛС в 1-й шифратор;

■ зашифровывают аутентифицированное служебное сообщение с помощью текущего ключа шифрования в 1-м шифраторе;

■ передают зашифрованное аутентифицированное служебное сообщение во 2-й шифратор через транспортную линию связи;

■ расшифровывают зашифрованное аутентифицированное служебное сообщение во 2-м шифраторе с помощью текущего ключа шифрования;

■ передают аутентифицированное служебное сообщение из 2-го шифратора в модуль согласования ключей приемного узла по 2-й ЛС;

■ проверяют аутентичность полученного служебного сообщения с помощью текущего ключа аутентификации в модуле согласования ключей приемного узла, причем если проверка аутентичности успешна, то

➢ передают служебное сообщение из модуля согласования ключей приемного узла в приемный модуль выработки квантовых ключей;

иначе

➢ сигнализируют о неуспешной аутентификации;

➢ переходят к этапу Б;

○ в ходе выполнения квантового протокола в части передачи служебных данных от приемного к передающему модулю выработки квантового ключа выполняют следующие действия:

■ формируют служебное сообщение из служебных данных в приемном модуле выработки квантовых ключей;

■ передают служебные данные из приемного модуля выработки квантовых ключей в модуль согласования ключей приемного узла;

■ осуществляют аутентификацию служебного сообщения с помощью текущего ключа аутентификации в модуле согласования ключей приемного узла;

■ передают аутентифицированное служебное сообщение по 2-й ЛС во 2-й шифратор;

■ зашифровывают аутентифицированное служебное сообщение с помощью текущего ключа шифрования во 2-м шифраторе;

■ передают зашифрованное аутентифицированное служебное сообщение в 1-й шифратор через транспортную линию связи;

■ расшифровывают зашифрованное аутентифицированное служебное сообщение в 1-м шифраторе с помощью текущего ключа шифрования;

■ передают аутентифицированное служебное сообщение из 1-го шифратора в модуль

согласования ключей передающего узла по 1-й ЛС;

■ проверяют аутентичность полученного служебного сообщения с помощью текущего ключа аутентификации в модуле согласования ключей передающего узла, причем если проверка аутентичности успешна, то

➢ передают служебное сообщение из модуля согласования ключей передающего узла в передающий модуль выработки квантовых ключей;

иначе

➢ сигнализируют о неуспешной аутентификации;

➢ переходят к этапу Б;

○ после выработки квантового ключа в приемном и передающем модулях выработки квантовых ключей передают полученный квантовый ключ из приемного модуля выработки квантовых ключей в модуль согласования ключей приемного узла и из передающего модуля выработки квантовых ключей в модуль согласования ключей передающего узла;

○ сохраняют полученный квантовый ключ в модулях согласования ключей приемного и передающего узла;

○ проверяют суммарный размер сохраненных квантовых ключей в модулях согласования квантовых ключей приемного и передающего узлов, причем если суммарный размер сохраненных квантовых ключей меньше Key блоков, то переходят к этапу Б;

• формируют новый ключ аутентификации и новый ключ шифрования из Key блоков сохраненного квантового ключа в модулях согласования квантовых ключей приемного и передающего узлов, выполняя следующие действия:

○ формируют новый ключ аутентификации в модуле согласования квантовых ключей передающего узла путем конкатенации первых m блоков накопленного квантового ключа;

○ добавляют к ключу аутентификации идентификатор в виде блока данных, содержащий значение счетчика ключей аутентификации M1 и значение признака ключа аутентификации;

○ увеличивают значение M1 счетчика ключей аутентификации на единицу;

○ формируют новый ключ шифрования в модуле согласования квантовых ключей передающего узла путем конкатенации последующих n блоков накопленного квантового ключа;

○ добавляют к ключу шифрования идентификатор в виде блока данных, содержащий значение счетчика ключей шифрования N1 и значение признака ключа шифрования;

○ увеличивают значение N1 счетчика ключей шифрования на единицу;

○ формируют новый ключ аутентификации в модуле согласования квантовых ключей приемного узла путем конкатенации первых m блоков накопленного квантового ключа;

○ добавляют к ключу аутентификации идентификатор в виде блока данных, содержащий значение счетчика ключей аутентификации M2 и значение признака ключа аутентификации;

○ увеличивают значение M2 счетчика ключей аутентификации на единицу;

○ формируют новый ключ шифрования в модуле согласования квантовых ключей приемного узла путем конкатенации последующих n блоков накопленного квантового ключа;

○ добавляют к ключу шифрования идентификатор в виде блока данных, содержащий

значение счетчика ключей шифрования N2 и значение признака ключа шифрования;

- увеличивают значение N2 счетчика ключей шифрования на единицу;

• сравнивают идентификаторы полученного нового ключа аутентификации и полученного нового ключа шифрования из модуля согласования ключей приемного узла с идентификаторами нового ключа аутентификации и нового ключа шифрования в модуле согласования ключей передающего узла, причем

- если идентификаторы ключей аутентификации совпали, то
  - передают сообщение об успешной проверке идентификаторов ключей аутентификации из модуля согласования ключей передающего узла в модуль согласования ключей приемного узла как служебное зашифрованное аутентифицированное сообщение, зашифрованное на текущем ключе шифрования и аутентифицированное на текущем ключе аутентификации,
  - получают в модуле согласования ключей передающего узла служебное сообщение об успешной проверке идентификаторов ключей аутентификации,
  - заменяют текущий ключ аутентификации новым ключом аутентификации в модулях согласования ключей приемного и передающего узла;

иначе

- переходят к этапу А;
- если идентификаторы ключей шифрования совпали, то
  - передают сообщение об успешной проверке идентификаторов ключей шифрования из модуля согласования ключей передающего узла в модуль согласования ключей приемного узла как служебное зашифрованное аутентифицированное сообщение, зашифрованное на текущем ключе шифрования и аутентифицированное на текущем ключе аутентификации,
  - получают в модуле согласования ключей передающего узла служебное сообщение об успешной проверке идентификаторов ключей шифрования,

иначе

- переходят к этапу А;

• передают сформированные новые ключи шифрования из модуля согласования ключей передающего узла в 1-й шифратор по 1-й ЛС и из модуля согласования ключей приемного узла в 2-й шифратор по 2-й ЛС;

• сравнивают идентификатор полученного нового ключа шифрования во 2-м шифраторе с идентификаторами нового ключа шифрования, выполняя следующие действия:

- передают идентификатор нового ключа шифрования из 1-го шифратора во 2-й шифратор как служебное зашифрованное сообщение, зашифрованное на текущем ключе шифрования;
- получают во 2-м шифратор служебное сообщение с идентификатором нового ключа шифрования;
- проводят во 2-м шифраторе сравнение идентификаторов новых ключей шифрования;
- если идентификаторы ключей шифрования не совпали, то
  - сигнализируют о неуспешном приеме ключей шифрования шифраторами;
  - переходят к этапу А;

иначе

- сохраняют полученные ключи шифрования в шифраторах для дальнейшего

использования.

Назначение комплекса - организация шифрованного канала связи между двумя узлами доверенной сети связи (например, в локальных сетях государственных учреждений и ведомств, корпораций).

Комплекс получает данные, которые необходимо защищенным образом доставить по назначению (например, пользовательские данные), в 1-й шифратор. Полученные 1-м шифратором данные зашифровываются с помощью текущих ключей, созданных с использованием согласованных ключей, полученных с использованием квантовых ключей из системы КРК. Стойкость текущих ключей шифрования обусловлена стойкостью квантовых ключей, из которых получены текущие ключи шифрования, что приводит к повышению защищенности пользовательских данных, передаваемых с защитой на таких ключах.

Затем 1-й шифратор передает зашифрованные данные по транспортной линии связи во 2-й шифратор, который расшифровывает информацию с помощью текущих ключей шифрования, созданных с использованием согласованных ключей, полученных с использованием квантовых ключей из системы КРК, и передает по назначению.

Для обеспечения защищенной передачи информации шифраторам необходимы идентичные ключи шифрования. Применение предлагаемого способа согласования ключей гарантирует использование идентичных ключей как для зашифрования данных, так и для их расшифрования, чем достигается преимущество в защищенности передаваемых пользовательских данных по сравнению с выбранным прототипом, в котором возможно навязывание использования различных сессионных ключей для зашифрования и расшифрования.

В предлагаемом способе квантовые ключи используются не только для создания ключей шифрования, но и для создания ключей аутентификации. Идентичность ключей шифрования и идентичность ключей аутентификации в сопряженных шифраторах по разные стороны транспортной линии связи необходима для корректного выполнения соответствующих операций, а именно, шифрования и расшифрования, а также аутентификации данных и проверки аутентичности данных.

Квантовые ключи, с использованием которых формируются ключи шифрования и ключи аутентификации, идентичны в двух составных частях системы КРК (передающем и приемном узле) в силу особенностей функционирования квантового протокола. При дальнейшем формировании новых ключей из квантовых ключей необходимо убедиться, что в двух шифраторах, соединенных транспортной линией связи (или в двух модулях согласования ключей системы КРК), будут применяться идентичные ключи шифрования (или ключи аутентификации).

Для этого в предлагаемом способе применяется согласование ключей по их идентификаторам путем сравнения идентификаторов ключей. Если идентификаторы не совпадают, то соответствующие им ключи отбрасываются (удаляются), чтобы не нарушать работоспособность комплекса из-за расхождения ключей, которые должны быть идентичными. За счет дополнительного сравнения идентификаторов ключей шифрования в шифраторах (помимо их сравнения в модулях согласования ключей перед передачей ключей шифрования в шифраторы) достигается повышение надежности комплекса в случае искажений (случайных или преднамеренных), вносимых локальной линией связи, связывающей узел системы КРК с шифратором.

Использование части квантового ключа для аутентификации служебных данных системы КРК, в том числе данных квантового протокола по постобработке последовательностей, которые передаются в квантовом канале, повышает стойкость

вырабатываемых квантовых ключей. Как известно, стойкость квантовых ключей зависит от стойкости способа передачи квантовых состояний по квантовому каналу, способа кодирования и детектирования квантовых состояний, от алгоритмов постобработки последовательностей, полученных из квантовых состояний, и от способа защиты данных, которыми обмениваются составные части системы КРК при постобработке последовательностей, полученных из квантового канала. Выбранный квантовый протокол определяет стойкость способа кодирования и детектирования квантовых состояний, а также алгоритма постобработки последовательностей, но не определяет способ защиты служебных данных в процессе постобработки последовательностей. В отсутствии защиты этих служебных данных возможны атаки типа "человек посередине" на системы, КРК. Защита служебных данных достигается их аутентификацией и/или шифрованием.

Аутентификацию передаваемых данных можно обеспечить либо с помощью предварительно распределенных симметричных ключей (предраспределенных ключей), либо с помощью квантовых ключей. В начальный момент функционирования комплекса квантовые ключи для аутентификации еще недоступны, поскольку сама выработка квантовых ключей требует аутентифицированного канала между приемным и передающем узлами системы КРК. Таким образом, первичная аутентификация всех сторон взаимодействия в комплексе основывается на предраспределенных ключах. Для обеспечения аутентификации в дальнейшем используются квантовые ключи согласно предлагаемому способу.

В предлагаемом способе согласования ключей производится аутентификация каждого передаваемого сообщения целиком, что гарантирует его целостность на принимающей стороне. Обычно при аутентификации сообщений, передаваемых по классическим линиям связи, сообщение перед передачей разбивается на части (например, кадры для линии связи, выполненной в виде Ethernet, или IP-пакеты для линии связи, выполненной в виде WAN, LAN) с последующим добавлением ими-товставки к каждой части. Такой способ гарантирует целостность каждой части в отдельности, но не гарантирует целостность полного сообщения, собранного из отдельных частей, так как, например, может быть нарушен порядок частей сообщения. В предлагаемом способе за счет аутентификации целиком каждого сообщения гарантирована его целостность, что повышает стойкость квантовых ключей.

При высоких скоростях шифрования требуется часто заменять текущий ключ шифрования на новый в связи с израсходованием допустимой нагрузки на ключ шифрования. Для этих целей применяется однопроходная система КРК из состава комплекса. С помощью данной системы КРК вырабатываются квантовые ключи, которые затем накапливаются в модулях согласования ключей системы КРК.

Накопление квантовых ключей до требуемого объема с последующим формированием ключей шифрования для передачи в шифраторы позволяет применять комплекс даже при низкой скорости генерации квантовых ключей и/или генерации квантовых ключей длины, меньше требуемой шифратором. Помещение ключей шифрования, переданных в шифратор, в хранилище ключей вместо незамедлительного использования, позволяет полностью использовать допустимую нагрузку на текущий ключ шифрования и осуществлять запланированную смену текущего ключа шифрования.

После накопления достаточного количества квантовых ключей из них формируются ключи шифрования для шифраторов и ключи аутентификации для аутентификации служебных данных системы КРК, передающихся между приемным и передающим

узлами системы КРК в процессе выполнения квантового протокола. Под достаточным количеством накопленных квантовых ключей понимается число квантовых ключей, суммарная длина которых не меньше суммарной длины хотя бы одного ключа шифрования и одного ключа аутентификации. Необходимые длины ключей шифрования и ключей аутентификации определяются применяемыми способом шифрования и способом аутентификации.

За счет накопления квантовых ключей перед дальнейшим формированием ключей шифрования и ключей аутентификации достигается повышение надежности комплекса в случае непредвиденных кратковременных сбоев однопроходной системы КРК, выражающихся во временном прекращении генерации квантовых ключей или вызванных, например, атаками нарушителя на квантовый канал связи. В таком случае уже выработанные квантовые ключи сохраняются, и после восстановления работоспособности системы КРК продолжается накопление квантовых ключей к уже имеющимся накопленным ранее квантовым ключам. Также работоспособность комплекса сохраняется в случае выработки системой КРК квантовых ключей, длина которых недостаточна для формирования новых ключей шифрования и ключей аутентификации. В этом случае происходит накопление квантовых ключей для формирования требуемых ключей шифрования и ключей аутентификации уже из совокупности накопленных квантовых ключей.

Шифрование как служебных данных, так и идентификаторов, используемых при согласовании и вводе в эксплуатацию ключей, повышает защищенность пользовательских данных и надежность комплекса от навязывания ложных идентификаторов ключей. За счет этого гарантируется выполнение устройством своей основной функции по защищенной передаче пользовательских данных с последующим гарантированным расшифрованием.

Также предлагаемый комплекс имеет преимущество по защищенности данных по сравнению с известным прототипом, поскольку не использует дополнительное распределение классических ключей (кроме первично предраспределенных ключей для инициализации комплекса, которые необходимы для любой типовой системы КРК), получая таким образом стойкие к атакам квантовым компьютером ключи шифрования, используемые в шифраторах. Используемая в прототипе система обмена классическими ключами требует построения собственной линии связи, отличной от линии связи между зашифровывающими/расшифровывающими процессорами в прототипе.

В предлагаемом комплексе используется только одна классическая линия связи (транспортная линия связи), соединяющая как два шифратора, так и два узла системы КРК.

Канал передачи служебных сообщений системы КРК состоит из перечисленных ниже каналов передачи информации:

- аутентифицированный с использованием квантовых ключей канал передачи служебной информации и квантовых ключей из приемного узла системы КРК в сопряженный шифратор и обратно,
- аутентифицированный с использованием квантовых ключей канал передачи пользовательских данных между шифраторами,
- аутентифицированный с использованием квантовых ключей канал передачи служебной информации и квантовых ключей из передающего узла системы КРК в сопряженный шифратор и обратно.

Таким образом, по сравнению с прототипом, в предлагаемом техническом решении не требуется отдельный канал для обмена служебными данными узлов системы КРК

при выработке квантовых ключей, вместо этого используется единый канал для передачи служебных сообщений системы КРК и передачи зашифрованных пользовательских данных, что позволяет снизить затраты на создание, развертывание и эксплуатацию комплекса.

Транспортная линия связи может быть доступной для атак возможного нарушителя. При использовании предлагаемого устройства и способа критически важная информация, содержащая сведения о данных в транспортной линии связи, включая служебные данные классического канала системы КРК о квантовом ключе, передается в зашифрованном виде на текущем ключе шифрования. Данное решение повышает защищенность передаваемых пользовательских данных и надежность комплекса.

Краткое описание чертежей

На чертеже показана схема комплекса для защищенной передачи данных с использованием системы КРК.

На чертеже обозначены:

1 - 1-й шифратор,
2 - 2-й шифратор,
3 - передающий узел системы КРК,
4 - приемный узел системы КРК,
5 - модуль выработки квантовых ключей передающего узла системы КРК,
6 - модуль согласования ключей передающего узла системы КРК,
7 - модуль выработки квантовых ключей приемного узла системы КРК,
8 - модуль согласования ключей приемного узла системы КРК,
9 - квантовая линия связи,
10 - транспортная линия связи,
11 - 1-я локальная линия связи,
12 - 2-я локальная линия связи.

Осуществление изобретения

Предлагаемые комплекс и способ могут быть реализованы, например, с использованием известной однопроходной системы КРК (патент РФ №2706175) и двух промышленных шифраторов, например, программно-аппаратных комплексов ViPNet L2 10G (статья по адресу https://infotecs.ru/about/press-centr/news/infoteks-i-eci-telecom-proveli-ispytaniya-na-sovmestimost-svoikh-produktov.html).

Модули согласования ключей 6,8 (на фигуре графического изображения) целесообразно выполнить в виде программных модулей в составе передающего узла 3 и приемного узла 4 однопроходной системы КРК. Возможность принимать ключи шифрования и служебные данные по локальным линиям связи 11, 12 реализуется в шифраторах 1, 2 также программно. Соответствующие программы и модули могут быть сформированы специалистом по программированию (программистом) на основе знания выполняемых функций.

В качестве квантовой линии связи 9 выбирается одномодовое оптоволокно типа SMF-28 допустимой длины. В качестве двух локальных линий связи 11, 12 выбирается два Ethernet патчкорда, которыми соединяются 1-й шифратор 1 с модулем согласования ключей передающего узла 6 системы КРК и 2-й шифратор 2 с модулем согласования ключей приемного узла 8 системы КРК соответственно. В качестве транспортной линии связи 10 может быть выбрано стандартное телекоммуникационное оптоволокно или линия Ethernet.

Для осуществления способа выполняют следующие действия:

Выбирают квантовый протокол, например, протокол на геометрически однородных

когерентных состояниях (Молотков С.Н. О геометрически однородных когерентных квантовых состояниях в квантовой криптографии, Письма в ЖЭТФ, том 95, вып. 6, с. 361-366, 2012).

Выбирают размер блока равным 8 бит.

Выбирают размер ключа шифрования равным 32 блокам, то есть 256 бит, что соответствует, например, размеру ключа шифрования блочного шифра ГОСТ 34.12-2018 "Кузнечик".

Выбирают размер ключа аутентификации равным 32 блокам.

Выбирают минимальный объем накопленного квантового ключа равным Key=32+32=64 блока.

Устанавливают программное значение счетчиков ключей аутентификации и ключей шифрования соответственно M1=1, M2=2, N1=1, N2=2.

Формируют текущий ключ аутентификации длиной 32 блока, например, с помощью квантового генератора случайных чисел (Балыгин К.А. др. Квантовый генератор случайных чисел, основанный на пуассоновской статистике фотоотсчетов, со скоростью около 100 Мбит/с, ЖЭТФ, том 153, вып. 6, с. 879-894, 2018). Присваивают идентификатор ключа аутентификации равным ID=(1, auth).

Формируют текущий ключ шифрования длиной 32 блока, например, с помощью генератора случайных чисел. Присваивают идентификатор ключа шифрования равным ID=(1, cipher).

Увеличивают значение счетчиков M1 и N1 на 1. Новые значения счетчиков M1=2 и N1=2 соответственно.

Загружают сформированный ключ аутентификации в модули согласования ключей приемного и передающего узлов системы КРК, а ключ шифрования - в шифраторы.

Запускают накопление квантовых ключей в модулях согласования. Для этого запускают выполнение выбранного квантового протокола для получения квантового ключа. Служебные данные, генерируемые модулями выработки квантовых ключей 5, 7 системы КРК в процессе выполнения квантового протокола, аутентифицируются с помощью текущего ключа аутентификации, например, путем вычисления имитовставки от аутентифицируемых данных по ГОСТ Р 34.13-2015 и конкатенации ее к служебным данным, в модуле согласования ключей узла системы КРК.

Затем аутентифицированные служебные данные передаются по локальной линии связи в сопряженный шифратор. В шифраторе эти данные зашифровываются с помощью текущего ключа шифрования с помощью алгоритмом шифрования, реализуемого выбранным шифратором. Зашифрованные данные передаются по транспортной линии связи во 2-й шифратор. Во 2-м шифраторе полученные данные расшифровываются и передаются по локальной линии связи в сопряженный модуль согласования ключей второго узла системы КРК. В модуле согласования ключей проверяется аутентичность полученных служебных данных, например, путем вычисления имитовставки по ГОСТ Р 34.13-2015 от служебных данных с помощью текущего ключа аутентификации и сравнения вычисленной имитовставки с полученной по служебной линии связи. В случае совпадения имитовставок служебные данные признаются аутентичными, в противном случае подается сигнал о неуспешной аутентификации служебных данных и прекращение выработки квантового ключа.

Сигнал о неуспешной аутентификации может быть выработан в каком-либо удобном виде, например, в виде звукового сигнала, текстового сообщения и т.п., и выдан администратору или дежурному специалисту из состава персонала, обслуживающего комплекс. Дальнейшие действия при получении сигнала должны определяться принятым

регламентом реагирования на аварийные или нештатные ситуации при эксплуатации комплекса.

После завершения выполнения квантового протокола в модули согласования ключей передаются выработанные квантовые ключи некоторой длины. В силу особенностей квантовых протоколов длина полученного квантового ключа не фиксирована. Поэтому после получения каждого квантового ключа в модуле согласования ключей производят проверку, достаточна ли суммарная длина накопленных квантовых ключей, включая длину только что полученного ключа. Допустим, длина первого полученного квантового ключа оказалась 120 бит. Выбранная минимальная длина накопленных квантовых ключей 64 блока, что составляет 512 бит. Следовательно, полученного квантового ключа недостаточно, его сохраняют в памяти модулей согласования ключей для дальнейшего накопления. Запускают выработку следующего квантового ключа.

Пусть второй квантовый ключ получен длиной 270 бит. Проверяют суммарную длину накопленных квантовых ключей. В данном случае суммарная длина накопленных квантовых ключей, включая полученный, составляет 120+270=390 бит, что снова меньше выбранной минимальной длины. Второй полученный квантовый ключ также сохраняют в памяти модулей согласования ключей и запускают выработку третьего квантового ключа.

Пусть третий квантовый ключ получен длиной 150 бит. Суммарная длина накопленных квантовых ключей после получения третьего квантового ключа 120+270+150=540 бит, что больше выбранного порога в 512 бит. Поэтому сохраняют третий квантовый ключ в памяти модулей согласования ключей и переходят к следующему шагу способа.

Из сохраненных квантовых ключей формируют новый ключ шифрования и новый ключ аутентификации одновременно в обоих модулях согласования ключей узлов системы КРК. Для этого выполняют конкатенацию трех квантовых ключей в одну строку бит. Из первых 32 блоков бит из полученной строки формируют новый ключ аутентификации. К ключу аутентификации добавляют его идентификатор, полученный из значения счетчика и признака использования ключа, то есть ID=(2, auth). Счетчики ключей аутентификации увеличиваются на 1, то есть M1=3, M2=3. Из следующих 32 бит формируют новый ключ шифрования, к которому аналогично добавляют идентификатор ID=(2, cipher), а значения счетчиков ключей шифрования увеличивают N1=3, N2=3.

После формирования новых ключей шифрования и ключей аутентификации проверяют, что полученные ключи согласованы. Для этого производят сравнение их идентификаторов. В частности, идентификаторы ключа шифрования и ключа аутентификации передают как служебные данные из модуля согласования ключей приемного узла системы КРК в передающий узел системы КРК, где производят сравнение идентификаторов. При этом в процессе передачи идентификаторов по транспортной линии связи между шифраторами, идентификаторы аутентифицированы на текущем ключе аутентификации и зашифрованы на текущем ключе шифрования, что защищает от навязывания ложных идентификаторов нарушителем.

При совпадении идентификаторов назначают новый ключ аутентификации текущим, на котором будет производиться аутентификация последующих служебных данных. Новые ключи шифрования вместе с их идентификаторами передают по служебной линии связи в соответствующие шифраторы.

После поступления новых ключей шифрования в шифраторы проверяется согласованность этих ключей аналогичным образом, путем сравнения идентификаторов.

При совпадении идентификаторов новых ключей шифрования, данные ключи вместе с их идентификаторами сохраняют в хранилищах ключей шифраторов для дальнейшего использования.

После этого запускают новую выработку квантовых ключей.

Использование ключей может осуществляться для защиты данных пользователей, при этом пользователи могут подключаться к любому шифратору.

(57) Формула изобретения

1. Комплекс для защищенной передачи данных в цифровой сети передачи данных с использованием однопроходной системы квантового распределения ключей, имеющий в составе

передающий узел системы квантового распределения ключей (КРК), включающий

передающий модуль выработки квантовых ключей,

модуль согласования ключей передающего узла;

приемный узел системы КРК, включающий

приемный модуль выработки квантовых ключей,

модуль согласования ключей приемного узла;

1-й шифратор, связанный с модулем согласования ключей передающего узла;

2-й шифратор, связанный с модулем согласования ключей приемного узла;

причем передающий модуль выработки квантовых ключей связан с приемным модулем выработки квантовых ключей квантовой линией связи, выполненной в виде оптоволоконной линии;

1-й шифратор связан со 2-м шифратором транспортной линией связи, выполненной в виде цифровой сети передачи данных;

1-й шифратор связан с модулем согласования ключей передающего узла посредством 1-й локальной линии связи (1-я ЛС);

2-й шифратор связан с модулем согласования ключей приемного узла посредством 2-й локальной линии связи (2-я ЛС);

1-й шифратор связан с внешней цифровой сетью передачи данных;

2-й шифратор связан с внешней цифровой сетью передачи данных;

при этом передающий модуль выработки квантовых ключей выполнен с возможностью

генерировать случайные числа,

формировать квантовые информационные состояния,

отправлять квантовые информационные состояния по квантовой линии связи в приемный модуль выработки квантовых ключей,

вырабатывать квантовые ключи совместно с приемным модулем выработки квантовых ключей путем обработки информации, полученной из квантовых информационных состояний;

модуль согласования ключей передающего узла выполнен с возможностью

формировать ключи аутентификации и ключи шифрования на основе квантовых ключей,

согласовывать ключи аутентификации и ключи шифрования с ключами аутентификации и ключами шифрования, сформированными модулем согласования ключей приемного узла,

принимать данные из 1-го шифратора по 1-й ЛС,

передавать данные в 1-й шифратор по 1-й ЛС;

приемный модуль выработки квантовых ключей выполнен с возможностью

генерировать случайные числа,

принимать квантовые информационные состояния по квантовой линии связи из передающего модуля выработки квантовых ключей,

обрабатывать квантовые информационные состояния,

вырабатывать квантовые ключи совместно с передающим модулем выработки квантовых ключей путем обработки информации, полученной из квантовых информационных состояний;

модуль согласования ключей приемного узла выполнен с возможностью формировать ключи аутентификации и ключи шифрования на основе квантовых ключей,

согласовывать ключи аутентификации и ключи шифрования с ключами аутентификации и ключами шифрования, сформированными модулем согласования ключей передающего узла,

принимать данные из 2-го шифратора по 2-й ЛС,

передавать данные во 2-й шифратор по 2-й ЛС;

1-й шифратор выполнен с возможностью

принимать ключи шифрования и служебные данные из модуля согласования ключей передающего узла по 1-й ЛС,

передавать служебные данные в модуль согласования ключей передающего узла по 1-й ЛС,

принимать данные из внешней цифровой сети передачи данных,

зашифровывать данные, поступившие в него по внешней цифровой сети передачи данных или по 1-й ЛС, с использованием ключей шифрования,

передавать данные, зашифрованные с использованием ключей шифрования, по транспортной линии связи,

расшифровывать данные, поступившие из транспортной линии связи, с использованием ключей шифрования,

передавать данные во внешнюю цифровую сеть передачи данных;

2-й шифратор выполнен с возможностью

принимать ключи шифрования и служебные данные из модуля согласования ключей приемного узла по 2-й ЛС,

передавать служебные данные в модуль согласования ключей приемного узла по 2-й ЛС,

принимать данные из внешней цифровой сети передачи данных,

зашифровывать данные, поступившие в него по внешней цифровой сети передачи данных или по 2-й ЛС, с использованием ключей шифрования,

передавать данные, зашифрованные с использованием ключей шифрования, по транспортной линии связи,

расшифровывать данные, поступившие из транспортной линии связи, с использованием ключей шифрования,

передавать данные во внешнюю цифровую сеть передачи данных.

2. Способ согласования ключей при работе комплекса, заключающийся в том, что

выбирают квантовый протокол;

выбирают размер блока равным b, где b кратно степени целого числа 2;

выбирают размер ключа шифрования равным n блоков;

выбирают размер ключа аутентификации равным m блоков;

выбирают минимальный объем накопленного квантового ключа равным Key=m+n блоков;

устанавливают значение счетчика ключей аутентификации в модуле согласования

ключей передающего узла M1=1;

устанавливают значение счетчика ключей аутентификации в модуле согласования ключей приемного узла M2=2;

устанавливают значение счетчика ключей шифрования в модуле согласования ключей передающего узла N1=1;

устанавливают значение счетчика ключей шифрования в модуле согласования ключей приемного узла N2=2;

формируют текущий ключ аутентификации размером m блоков, выполняя следующие действия:

добавляют к ключу аутентификации идентификатор в виде блока данных, содержащий значение счетчика M1 и значение признака ключа аутентификации;

увеличивают значение счетчика M1 на 1;

формируют текущий ключ шифрования размером n блоков, выполняя следующие действия:

добавляют к ключу шифрования идентификатор в виде блока данных, содержащий значение счетчика N1 и значение признака ключа шифрования;

увеличивают значение счетчика N1 на 1;

загружают текущий ключ аутентификации в модули согласования ключей приемного и передающего узла;

загружают текущий ключ шифрования в 1-й и 2-й шифраторы;

(А) накапливают квантовые ключи в модулях согласования ключей передающего и приемного узлов системы КРК, выполняя следующие действия:

(Б) вырабатывают квантовый ключ в передающем и приемном модулях выработки квантовых ключей согласно выбранному квантовому протоколу, причем в ходе выполнения квантового протокола в части передачи служебных данных от передающего к приемному модулю выработки квантового ключа выполняют следующие действия:

формируют служебное сообщение из служебных данных в передающем модуле выработки квантовых ключей;

передают служебные данные из передающего модуля выработки квантовых ключей в модуль согласования ключей передающего узла;

осуществляют аутентификацию служебного сообщения с помощью текущего ключа аутентификации в модуле согласования ключей передающего узла;

передают аутентифицированное служебное сообщение по 1-й ЛС в 1-й шифратор;

зашифровывают аутентифицированное служебное сообщение с помощью текущего ключа шифрования в 1-м шифраторе;

передают зашифрованное аутентифицированное служебное сообщение во 2-й шифратор через транспортную линию связи;

расшифровывают зашифрованное аутентифицированное служебное сообщение во 2-м шифраторе с помощью текущего ключа шифрования;

передают аутентифицированное служебное сообщение из 2-го шифратора в модуль согласования ключей приемного узла по 2-й ЛС;

проверяют аутентичность полученного служебного сообщения с помощью текущего ключа аутентификации в модуле согласования ключей приемного узла, причем если проверка аутентичности успешна, то

передают служебное сообщение из модуля согласования ключей приемного узла в приемный модуль выработки квантовых ключей;

иначе сигнализируют о неуспешной аутентификации;

переходят к этапу Б;

в ходе выполнения квантового протокола в части передачи служебных данных от приемного к передающему модулю выработки квантового ключа выполняют следующие действия:

формируют служебное сообщение из служебных данных в приемном модуле выработки квантовых ключей;

передают служебные данные из приемного модуля выработки квантовых ключей в модуль согласования ключей приемного узла;

осуществляют аутентификацию служебного сообщения с помощью текущего ключа аутентификации в модуле согласования ключей приемного узла;

передают аутентифицированное служебное сообщение по 2-й ЛС во 2-й шифратор;

зашифровывают аутентифицированное служебное сообщение с помощью текущего ключа шифрования во 2-м шифраторе;

передают зашифрованное аутентифицированное служебное сообщение в 1-й шифратор через транспортную линию связи;

расшифровывают зашифрованное аутентифицированное служебное сообщение в 1-м шифраторе с помощью текущего ключа шифрования;

передают аутентифицированное служебное сообщение из 1-го шифратора в модуль согласования ключей передающего узла по 1-й ЛС;

проверяют аутентичность полученного служебного сообщения с помощью текущего ключа аутентификации в модуле согласования ключей передающего узла, причем если проверка аутентичности успешна, то

передают служебное сообщение из модуля согласования ключей передающего узла в передающий модуль выработки квантовых ключей;

иначе сигнализируют о неуспешной аутентификации;

переходят к этапу Б;

после выработки квантового ключа в приемном и передающем модулях выработки квантовых ключей передают полученный квантовый ключ из приемного модуля выработки квантовых ключей в модуль согласования ключей приемного узла и из передающего модуля выработки квантовых ключей в модуль согласования ключей передающего узла;

сохраняют полученный квантовый ключ в модулях согласования ключей приемного и передающего узла;

проверяют суммарный размер сохраненных квантовых ключей в модулях согласования квантовых ключей приемного и передающего узлов, причем если суммарный размер сохраненных квантовых ключей меньше Key блоков, то переходят к этапу Б;

формируют новый ключ аутентификации и новый ключ шифрования из Key блоков сохраненного квантового ключа в модулях согласования квантовых ключей приемного и передающего узлов, выполняя следующие действия:

формируют новый ключ аутентификации в модуле согласования квантовых ключей передающего узла путем конкатенации первых m блоков накопленного квантового ключа;

добавляют к ключу аутентификации идентификатор в виде блока данных, содержащий значение счетчика ключей аутентификации M1 и значение признака ключа аутентификации;

увеличивают значение M1 счетчика ключей аутентификации на единицу;

формируют новый ключ шифрования в модуле согласования квантовых ключей передающего узла путем конкатенации последующих n блоков накопленного квантового

ключа;

добавляют к ключу шифрования идентификатор в виде блока данных, содержащий значение счетчика ключей шифрования N1 и значение признака ключа шифрования;

увеличивают значение N1 счетчика ключей шифрования на единицу; формируют новый ключ аутентификации в модуле согласования квантовых ключей приемного узла путем конкатенации первых m блоков накопленного квантового ключа;

добавляют к ключу аутентификации идентификатор в виде блока данных, содержащий значение счетчика ключей аутентификации M2 и значение признака ключа аутентификации;

увеличивают значение M2 счетчика ключей аутентификации на единицу;

формируют новый ключ шифрования в модуле согласования квантовых ключей приемного узла путем конкатенации последующих n блоков накопленного квантового ключа;

добавляют к ключу шифрования идентификатор в виде блока данных, содержащий значение счетчика ключей шифрования N2 и значение признака ключа шифрования;

увеличивают значение N2 счетчика ключей шифрования на единицу; сравнивают идентификаторы полученного нового ключа аутентификации и полученного нового ключа шифрования из модуля согласования ключей приемного узла с идентификаторами нового ключа аутентификации и нового ключа шифрования в модуле согласования ключей передающего узла, причем

если идентификаторы ключей аутентификации совпали, то

передают сообщение об успешной проверке идентификаторов ключей аутентификации из модуля согласования ключей передающего узла в модуль согласования ключей приемного узла как служебное зашифрованное аутентифицированное сообщение, зашифрованное на текущем ключе шифрования и аутентифицированное на текущем ключе аутентификации,

получают в модуле согласования ключей передающего узла служебное сообщение об успешной проверке идентификаторов ключей аутентификации, заменяют текущий ключ аутентификации новым ключом аутентификации в модулях согласования ключей приемного и передающего узла;

иначе переходят к этапу A;

если идентификаторы ключей шифрования совпали, то

передают сообщение об успешной проверке идентификаторов ключей шифрования из модуля согласования ключей передающего узла в модуль согласования ключей приемного узла как служебное зашифрованное аутентифицированное сообщение, зашифрованное на текущем ключе шифрования и аутентифицированное на текущем ключе аутентификации,

получают в модуле согласования ключей передающего узла служебное сообщение об успешной проверке идентификаторов ключей шифрования,

иначе переходят к этапу A;

передают сформированные новые ключи шифрования из модуля согласования ключей передающего узла в 1-й шифратор по 1-й ЛС и из модуля согласования ключей приемного узла в 2-й шифратор по 2-й ЛС;

сравнивают идентификатор полученного нового ключа шифрования во 2-м шифраторе с идентификаторами нового ключа шифрования, выполняя следующие действия:

передают идентификатор нового ключа шифрования из 1-го шифратора во 2-й шифратор как служебное зашифрованное сообщение, зашифрованное на текущем

ключе шифрования;

получают во 2-м шифраторе служебное сообщение с идентификатором нового ключа шифрования;

проводят во 2-м шифраторе сравнение идентификаторов новых ключей шифрования;

если идентификаторы ключей шифрования не совпали, тогда сигнализируют о неуспешном приеме ключей шифрования шифраторами;

переходят к этапу А;

иначе сохраняют полученные ключи шифрования в шифраторах для дальнейшего использования.

1