РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 697 696**(13) **C1**

(51) МПК
H04L 9/08 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК
H04L 9/0858 (2019.05)

(21)(22) Заявка: **2019101393, 18.01.2019**

(24) Дата начала отсчета срока действия патента:
18.01.2019

Дата регистрации:
16.08.2019

Приоритет(ы):
(22) Дата подачи заявки: **18.01.2019**

(45) Опубликовано: **16.08.2019** Бюл. № **23**

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):
Поздняков Александр Михайлович (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 2488965 C1, 27.07.2013. RU 2621605 C2, 06.06.2017. EP 717895 B1, 25.11.1998.**

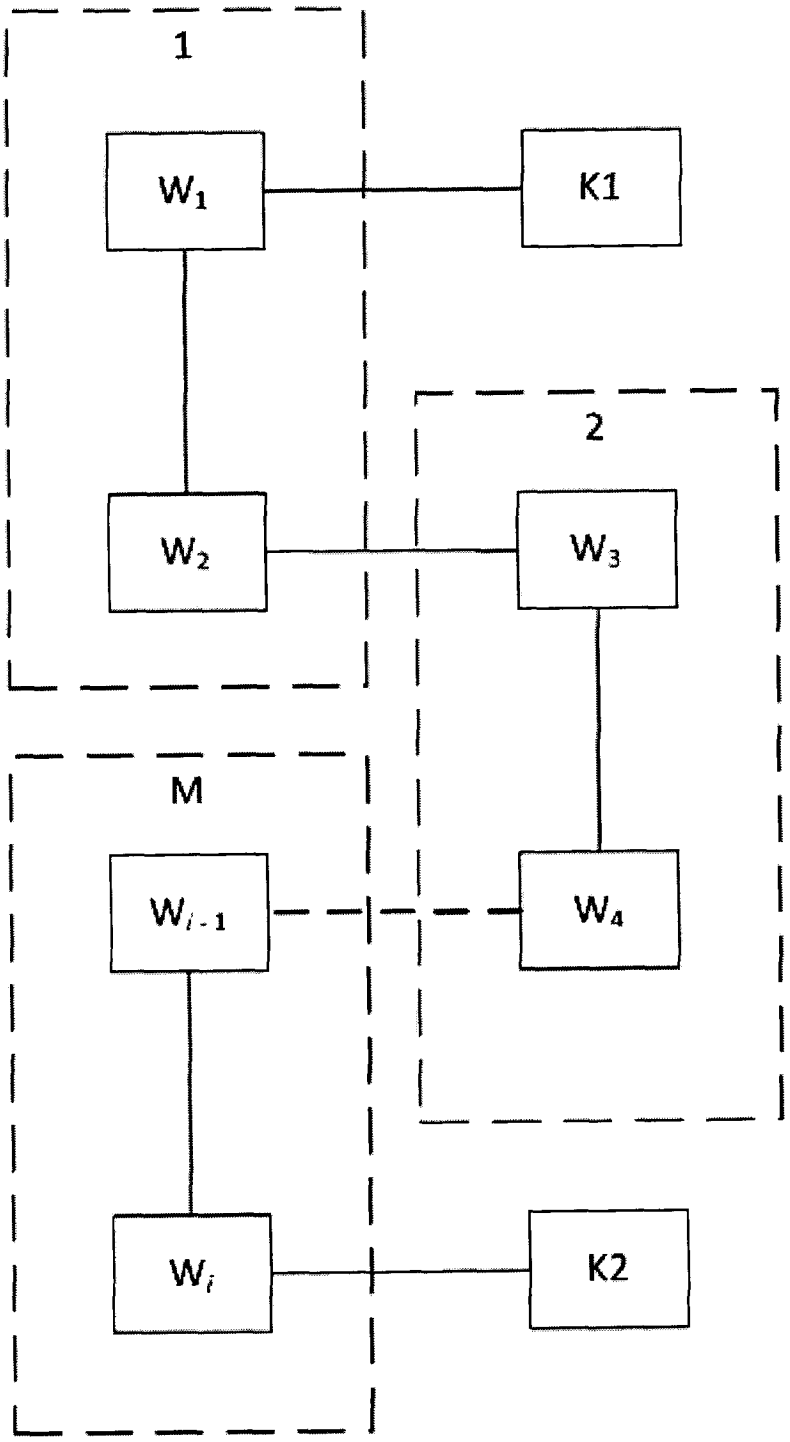
(54) Способ передачи сообщения через вычислительную сеть с применением аппаратуры квантового распределения ключей

(57) Реферат:

Изобретение относится к области защищенных информационных сетей с квантовым распределением криптографических ключей. Техническим результатом является повышение защищенности передаваемого сообщения. Способ заключается в том, что (А) зашифровывают сообщение в блоке обработки выходного узла k-го звена обработки, при этом: получают квантовый ключ длинной X_k бит; зашифровывают сообщение на квантовом ключе k-го звена обработки с применением выбранного алгоритма шифрования; передают зашифрованное сообщение в блок обработки входного узла k-го звена обработки; добавляют к полученному зашифрованному сообщению ключ X_k, полученный во входном узле k-го звена обработки; формируют значение Y_k в зависимости от длины ключа X_k; добавляют к полученному сообщению Y_k; формируют значение Z_k в зависимости от выбранного алгоритма шифрования; добавляют к полученному сообщению Z_k, получая входное сообщение для следующего входного узла; если k<M, то передают входное сообщение в блок обработки выходного узла k+1 звена через цифровую сеть передачи данных; вычисляют k=k+1; получают зашифрованное сообщение в блоке обработки входного узла k-го звена обработки через цифровую сеть передачи данных; обрабатывают зашифрованное сообщение в блоке обработке входного узла k-го звена обработки. 1 ил.

RU 2697696 C1

RU 2697696 C1



RU 2697696 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 697 696**(13) **C1**

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

(12) ABSTRACT OF INVENTION

(52) CPC
H04L 9/0858 (2019.05)

(21)(22) Application: **2019101393, 18.01.2019**

(24) Effective date for property rights:
18.01.2019

Registration date:
16.08.2019

Priority:
(22) Date of filing: **18.01.2019**

(45) Date of publication: **16.08.2019** Bull. № **23**

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

(72) Inventor(s):
Pozdnyakov Aleksandr Mikhajlovich (RU)

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

RU 2697696 C1

(54) METHOD OF TRANSMITTING A MESSAGE OVER A COMPUTER NETWORK USING HARDWARE FOR QUANTUM KEY DISTRIBUTION

(57) Abstract:

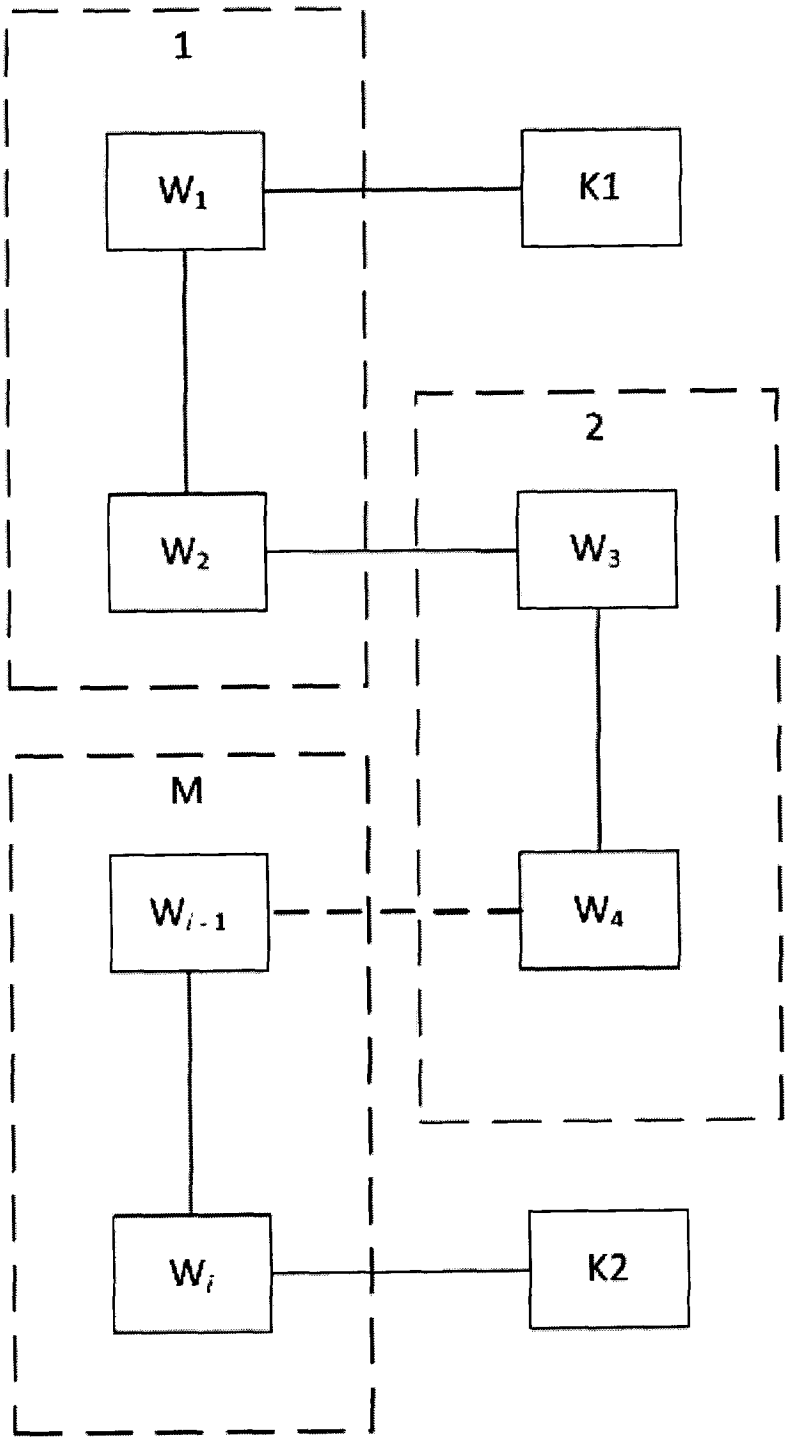
FIELD: cryptography.

SUBSTANCE: invention relates to secure information networks with quantum distribution of cryptographic keys. Method comprises (A) encoding a message in a processing unit of an output node of the k-th processing link, wherein: obtaining a quantum key with a long X_k bits; encoding a message on a quantum key of the k-th processing link using the selected encryption algorithm; sending the encrypted message to the processing unit of the input node of the k-th processing link; adding to received encrypted message key X_k, obtained in input unit of k-th processing link; generating value Y_k depending on key length X_k; adding to received message Y_k; Z_k value is formed depending on selected encryption algorithm; adding to received message Z_k, obtaining an input message for the next input node; if k<M, the input message is transmitted to the link output node k+1 processing unit through the digital data network; calculating k=k+1; obtaining an encrypted message in the processing unit of the input node of the k-th processing link through the digital data network; processing the encrypted message in the processing unit of the input node of the k-th processing link.

EFFECT: technical result is higher security of a transmitted message.

1 cl, 1 dwg

RU 2697696 C1



RU 2697696 C1

Область техники, к которой относится изобретение

Предполагаемое изобретение относится к сетевой волоконно-оптической квантовой криптографии - к защищенным информационным сетям с квантовым распределением криптографических ключей, к технике, предназначенной для защищенной передачи конфиденциальной информации, через вычислительную сеть, которая взаимодействует с аппаратурой, реализующей протокол квантового распределения криптографических ключей.

Уровень техники

Для защиты данных, передаваемых в современных цифровых сетях передачи данных, обычно используют различные методы шифрования, основанные на секретности ключа шифрования. Распределение ключей обычно выполняют либо при помощи алгоритмов, которые основаны на протоколе Диффи-Хеллмана, либо при помощи передачи по доверенному каналу (курьерская рассылка). Таким образом распределяют ключи шифрования, которые используется в системе зашифрования и расшифрования передаваемой информации.

Известен способ квантового распределения ключей посредством синхронизации ключей между клиентами, расположенными в разных локальных сетях с использованием нескольких систем с квантовым распределением ключей (патент РФ №2621605, приоритет от 02.10.2015 г.), включающий:

• осуществление процесса квантового распределения общего секретного ключа между первым клиентом и первым сервером, которые соединены между собой волоконно-оптическим каналом связи и расположены в первой локальной сети, при этом формируется общий ключ K1;

• осуществление процесса квантового распределения общего секретного ключа между вторым клиентом и вторым сервером, которые соединены между собой волоконно-оптическим каналом связи и расположены во второй локальной сети, при этом формируется общий ключ K3;

• осуществление процесса квантового распределения общего секретного ключа между первым сервером и вспомогательным клиентом второго сервера, которые соединены между собой волоконно-оптическим каналом связи, при этом формируется ключ K2;

• просмотр первым сервером позиций ключей K1 и K2 и отправку первому клиенту

• номера позиций в ключе K1, значения которых не совпали со значениями в ключе K2;

• получение первым клиентом номеров несовпавших позиций и формирование ключа K21 путем инвертирования в ключе K1 вышеуказанных несовпавших позиций;

• просмотр вторым сервером позиций ключей K3 и K2 и отправка второму клиенту

• номера позиций в ключе K3, значения которых не совпали со значениями в ключе K2;

• получение вторым клиентом номеров несовпавших позиций и формирование ключа K22 путем инвертирования в ключе K3 вышеуказанных несовпавших позиций.

Известный способ может обеспечить защиту передаваемых данных. Однако при этом не обеспечивается возможность применения аппаратуры КРК, реализующей разные протоколы выработки квантового ключа и для реализации известного способа необходимо многократно обрабатывать одну и ту же последовательность бит (позиции ключа), которая определяет квантовый ключ на всех доверенных промежуточных узлах сети, что делает возможным проведение атак, которые основаны включении злоумышленника посередине.

Также известен способ передачи данных с использованием системы квантового распределения ключей (Tajima A. et al. Quantum key distribution network for multiple applications, Quantum Science and Technology, 2017, v. 2, №3, статья по адресу: http://iopscience.iop.org/article/10.1088/2058-9565/aa7154/meta).

Для передачи данных между компьютерами пользователей, например, компьютером 1 и компьютером 2, используется интегрированная система, включающая цифровую сеть передачи данных и систему квантового распределения ключей (КРК).

Система КРК включает несколько иерархически связанных уровней:

- уровень поддержки ключей (верхний уровень),
- уровень управления ключами,
- квантовый уровень (нижний уровень).

В состав квантового уровня входит несколько звеньев, каждое из которых содержит

- M последовательно соединенных звеньев обработки, причем
  - каждое звено состоит из входного и выходного узлов аппаратуры КРК, выполненной с возможностью формирования квантовых ключей в результате выполнения установленного протокола КРК,
  - входной и выходной узлы обработки каждого звена связаны цифровой линией передачи,
  - на каждом входном узле установлен блок обработки, выполненный с возможностью
    - принимать данные,
    - обрабатывать данные,
    - передавать данные;
  - на каждом выходном узле установлен блок обработки, выполненный с возможностью
    - принимать данные,
    - обрабатывать данные,
    - передавать данные;

Блок обработки выходного узла каждого звена соединен через цифровую сеть передачи данных с сервером уровня управления ключами, причем через этот сервер обеспечивается также взаимодействие с блоками обработки уровня поддержки ключей.

При необходимости установки соединения и передачи данных от компьютера 1 в компьютер 2, компьютер 1 запрашивает через цифровую сеть передачи данных ключ у системы КРК. При этом учитывается, что компьютера 1 относится к участку сети, находящемуся в зоне действия определенного (начального) узла сети КРК, а компьютер 2 - к зоне действия другого (конечного) узла сети КРК.

Сервер уровня управления ключами инициирует формирование ключа в цепочке звеньев обработки сети КРК от начального до конечного узла сети КРК.

Ключ, сгенерированный в первом звене квантового уровня, с помощью операции XOR (исключающее ИЛИ) обрабатывается совместно с ключом следующего звена, полученный результат зашифровывается шифром типа "одноразовый блокнот" на ключе следующего звена и посылается через цифровую сеть передачи данных на узел следующего звена. После этого результат на узле следующего звена расшифровывается на ключе следующего звена.

Далее результат снова с помощью операции XOR обрабатывается совместно с ключом очередного звена, при этом ключ следующего звена из результата удаляется, и эти операции повторяются, пока результат не будет получен на конечном узле сети КРК.

Таким образом, на конечном узле сети КРК после пересылки и обработки оказывается ключ, сгенерированный в первом звене.

Этот ключ посылается в компьютер 2, после чего в компьютере 1 на этом ключе данные, подлежащие пересылке, зашифровываются на этом ключе и посылаются в зашифрованном виде через цифровую сеть передачи данных в компьютер 2. Затем в компьютере 2 данные расшифровываются на этом же ключе и используются по назначению.

Известный способ принят за прототип.

Однако известный способ имеет недостатки.

Перед очередной пересылкой на каждом узле сети КРК необходимо расшифровывать и зашифровывать один и тот же квантовый ключ, в результате чего ключ появляется в открытом виде на каждом узле, что делает возможным проведение атак, которые основаны на сборе статистики по побочным каналам. Кроме того, при случайном или преднамеренном получении доступа к любому узлу со стороны злоумышленника секретность ключа утрачивается, что снижает защищенность.

Помимо этого, не обеспечивается возможность использования разных алгоритмов шифрования на каждом промежуточном звене.

Раскрытие изобретения

Техническим результатом является:

1) повышение защищенности передаваемого сообщения,

2) отсутствие необходимо расшифровывать передаваемое сообщение на каждом промежуточном узле в процессе передачи,

3) возможность использования разных алгоритмов шифрования на каждом промежуточном звене, в том числе с динамическим переключением между алгоритмами,

4) устранение возможности проведения атаки по побочным электромагнитным излучениям и наводкам (ПЭМИН) электронной аппаратуры шифрования промежуточного узла передачи.

Для этого предлагается способ передачи сообщения через вычислительную сеть, причем сеть содержит

- М последовательно соединенных звеньев обработки, причем
  - каждое звено состоит из входного и выходного узлов аппаратуры квантового распределения ключей, выполненной с возможностью формирования квантовых ключей в результате выполнения установленного протокола квантового распределения ключей;
  - входной и выходной узлы аппаратуры квантового распределения ключей соседних звеньев связаны оптоволоконной линией;
  - на каждом входном узле установлен блок обработки, связанный с цифровой сетью передачи данных и выполненный с возможностью
    - принимать данные,
    - обрабатывать данные,
    - передавать данные;
  - на каждом выходном узле установлен блок обработки, связанный с цифровой сетью передачи данных и выполненный с возможностью
    - принимать данные,
    - обрабатывать данные,
    - передавать данные;
- 1-й компьютер, связанный с блоком обработки выходного узла 1-го звена обработки через цифровую линию передачи данных и выполненный с возможностью

передавать сообщение во входной узел;

- 2-й компьютер, связанный с блоком обработки входного узла M-го звена через цифровую линию передачи данных и выполненный с возможностью принимать сообщение от входного узла;

способ, заключающийся в том, что

- формируют сообщение размером N бит в 1-м компьютере;
- передают сообщение из 1-го компьютера в блок обработки выходного узла 1-го звена обработки через цифровую линию передачи данных;
- получают сообщение из 1-го компьютера в блоке обработки выходного узла 1-го звена обработки;
- вычисляют k=1;
- вычисляют длину записи Y в битах для записи в двоичном виде значений длины ключа шифрования для каждого звена обработки;
- вычисляют длину записи Z в битах для записи в двоичном виде значений уловного кода алгоритма шифрования для каждого звена обработки;
- (A) зашифровывают сообщение в блоке обработки выходного узла k-го звена обработки, выполняя следующие действия:
  - получают квантовый ключ длинной бит, который выработан в результате выполнения протокола квантового распределения ключей на k-м звене обработки;
  - зашифровывают сообщение на квантовом ключе k-го звена обработки с применением выбранного алгоритма шифрования;
- передают зашифрованное сообщение в блок обработки входного узла k-го звена обработки;
- добавляют к полученному зашифрованному сообщению ключ X_k, полученный во входном узле k-го звена обработки;
- формируют значение Y_k в зависимости от длины ключа X_k;
- добавляют к полученному сообщению Y_k;
- формируют значение в зависимости от выбранного алгоритма шифрования;
- добавляют к полученному сообщению Z_k, получая входное сообщение для следующего входного узла;
- если k<M, то
  - передают входное сообщение в блок обработки выходного узла k+1 звена через цифровую сеть передачи данных;
  - вычисляют k=k+1;
  - переходят к этапу A;
- получают зашифрованное сообщение в блоке обработки входного узла k-го звена обработки через цифровую сеть передачи данных;
- обрабатывают зашифрованное сообщение в блоке обработке входного узла k-го звена обработки, выполняя следующие действия:
  - расшифровывают зашифрованное сообщение с использованием квантового ключа M-го узла, в результате получают входное сообщение, которое было передано в блок обработки выходного узла k-го звена обработки;
  - (B) отделяют от входного сообщения длину записи Y_k;
  - определяют длину ключа из значения Y_k;
  - отделяют ключ k-го звена обработки от входного сообщения;

- отделяют от сообщения Z_k;
- определяют алгоритм шифрования из кода, записанного в значении Z_k;
- расшифровывают оставшуюся часть входного сообщения с использованием отделенного k-го ключа;
- если k>1, то
- вычисляют k=k-1;
- переходят к этапу (B);
- получают исходное сообщение;
- передают сообщение из блока обработки входного узла M-го звена обработки во 2-й компьютер через цифровую линию передачи данных.

Повышение защищенности передаваемого сообщения достигается тем, что сеть передачи информации строится из последовательно подключенных узлов аппаратуры КРК, таким образом, что в месте соединения блока обработки входного узла КРК одного звена с блоком обработки выходного узла КРК следующего звена организуется доверенная линия передачи для передачи сообщения, зашифрованного на ключе предыдущего звена КРК. Причем передача осуществляется без расшифровки передаваемого сообщения, а ключ, на котором зашифровано сообщение, передается доверенным образом во входной узел КРК следующего звена напрямую от входного узла КРК предыдущего звена.

Таким образом, сообщение передается в защищенном виде. Кроме того, перед передачей в следующее звено ни сообщение, ни ключ не подвергаются обработке, которая позволила бы осуществить атаку, основанную на сборе информации по побочным каналам (по ПЭМИН), так как в предлагаемом способе обеспечивается то, что последовательность бит, которая представляет собой передаваемое сообщение, на каждом звене передачи отличается от последовательности бит на других звеньях за счет последовательного зашифровывания передаваемого сообщения на ключе передающего звена, причем значения бит в последовательностях независимы от значений бит в других последовательностях и между собой. В то же время ключ звена передается доверенным образом, без сохранения и только один раз в рамках доверенного узла.

Повышение защищенности передаваемого сообщения также достигается путем использования определенного алгоритма шифрования для каждого этапа передачи. В общем случае, для передачи сообщения на каждом этапе могут быть определены разные алгоритмы шифрования, тогда необходимо формировать значение в зависимости от длины используемого ключа шифрования на k-м этапе X_k. Для этого необходимо определить длину записи значений $Y_к$, которая может быть вычислена по следующей формуле:

$$Y = | \log_2 [N*2^M] |,$$

где N - длина сообщения,

M - количество узлов в цепи передачи.

Длина ключа k-го звена передачи записывается в соответствующее значение Yk.

Также для повышения защищенности передаваемого сообщения может быть организовано динамическое переключение алгоритмов шифрования для каждого узла передачи, тогда необходимо формировать значение в зависимости от используемого алгоритма шифрования на k-ом этапе. Условный код используемого алгоритма на k-ом звене передачи записывается в значение Z_k. Причем количество используемых алгоритмов шифрования конечно и может быть определено исходя из конкретных

требований к реализации сети передачи. Для этого необходимо определить длину записи значений Z_k, которая может быть вычислена по следующей формуле

$$Z = | \log_2 L |,$$

где L - количество алгоритмов шифрования, используемых в сети.

В общем случае, получение исходного сообщения происходит на конечном узле цепочки посредством последовательного расшифровывания полученного сообщения, при котором последовательно используются ключи, на которых было зашифровано сообщение. Поскольку сообщение представляет собой последовательность бит, то ключ - это определенное количество бит этого сообщения, которые определяются с использованием значения Y_k: от сообщения отделяется та длина последовательности бит, которая записана в значении Y_k и применяется для расшифрования. Для определения алгоритма шифрования определяется условный код алгоритма из значения Z_k.

В частном случае, на каждом этапе передачи может использоваться алгоритм, при котором длина ключа выбирается равной длине передаваемого сообщения (шифр типа одноразовый блокнот). Тогда формирование значений Z_k и Y_k не требуется, но на каждом этапе передачи длина передаваемого сообщения будет удваиваться. При этом в процессе расшифрования ключом для каждого этапа будет являться последняя половина полученного сообщения.

Повышение защищенности передаваемого сообщения получается также за счет выбора алгоритма шифрования, причем независимо от количества звеньев в сети и длины передаваемого сообщения. Количество звеньев в сети будет влиять только на время получения исходного сообщения конечным пользователем, т.к. количество информации, которое требуется зашифровать, с каждым следующем шагом увеличивается на длину ключа и длину записи значений Z_k и Y_k. Самое быстрое увеличение зашифровываемой информации на каждом этапе будет при использовании алгоритма, в котором длина ключа выбирается равной длине сообщения. Для такого случая необходимо будет обеспечить выработку ключа с удвоенной длиной на каждом последующем этапе. При фиксированной длине ключа прирост длины передаваемого сообщения на каждом этапе будет одинаковым, что не внесет значительной задержки в передачу исходного сообщения.

Дополнительно повысить защищенность передаваемого сообщения можно, если само сообщение перед передачей через сеть будет уже зашифровано.

Отсутствие необходимости расшифровывать передаваемое сообщение на каждом промежуточном узле достигается за счет того, что для каждого следующего звена передачи зашифрованное сообщение, полученное от предыдущего узла, является передаваемым сообщением. В предлагаемом способе нет ограничения, при котором необходимо было бы фиксировать длину предаваемого сообщения для всех звеньев в цепи передачи. Таким образом, сообщение не расшифровывается для того, чтобы заново быть зашифрованным. С другой стороны, на каждом звене передачи передаваемое сообщение зашифровывается на ключе, выработанном на этом звене.

Возможность использования разных алгоритмов шифрования на каждом промежуточном звене достигается за счет того, что каждое звено КРК вырабатывает симметричные ключи независимо от других звеньев, а сообщение на промежуточном узле не подвергается расшифрованию. При этом вместе с длиной ключа в параметре Z нужно фиксировать условный код алгоритма шифрования для обеспечения

возможности получения исходного сообщения на последнем узле. Таким образом, для каждого промежуточного узла можно выбрать алгоритм шифрования в зависимости от требований, предъявляемых к конкретному звену передачи, в то же время расшифрование проводится только в одном узле последнего звена, поэтому безопасность процесса расшифрования требуется обеспечивать только в одном узле. Использование нескольких разных алгоритмов шифрования также повышает защищенность передаваемого сообщения, особенно, если алгоритмы динамически меняются, т.е. каждый набор алгоритмов действует в течении определенного периода времени.

Соответственно, параметр Z, например, целочисленный, может характеризовать тип алгоритма шифрования, в виде 1 - алгоритм шифрования по ГОСТ Р 34.12-2015, 2 - одноразовый блокнот, 3 - AES и т.д.

Период времени действия набора алгоритмов шифрования может устанавливаться автоматически, например, по таймеру, или вручную администратором цифровой сети передачи данных.

Устранение возможности проведения атаки по побочным электромагнитным излучениям и наводкам (ПЭМИН) электронной аппаратуры шифрования промежуточного узла передачи достигается за счет того, что информация в одном и том же виде предается только один раз. Поскольку информация переставляет собой сообщение в виде последовательности бит, то каждая последующая передача изменяет вид передаваемого сообщения посредством зашифрования этого сообщения на ключе конкретного звена КРК, через которое передается это сообщение. Таким образом, независимость квантовых ключей, выработанных на каждом звене КРК, обеспечивает независимость последовательностей бит, которые и составляют передаваемое сообщение. А когда передача осуществляется один раз, то злоумышленник может получить только случайную информацию по каналу ПЭМИН, то есть информацию, которая не будет коррелировать с любой другой информацией в системе (Side-Channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing. Авторы YongBin Zhou, DengGuo Feng. 2005, статья по адресу:

https://ru.bmstu.wiki/Атаки_по_побочным_каналам:
_десять_лет_после_публикации_и_воздействие_на_криптографический_модуль_тестирования_безопасности#D09AD0BED0BDD182D180D0BCD0B5D180D18B)

Краткое описание чертежей

На фигуре графического изображения показана схема сети передачи ключевой информации с использованием аппаратуры КРК.

Использованы следующие обозначения:

• 1, 2, M - звенья обработки интегрированной аппаратурой квантового распределения ключей,

• K1, K2 - 1-й и 2-й компьютеры,

• W_1, W_2, W_3, W_4 - 1-й, 2-й, 3-й и 4-й узлы обработки звеньев аппаратуры КРК, причем узлы с нечетными индексами являются выходными узлами обработки, а узлы с четными индексами являются входными узлами обработки,

• W_i - входной узел последнего звена аппаратуры КРК,

• W_{i-1} - выходной узел последнего звена обработки.

Осуществление изобретения

Для осуществления предлагаемого способа передачи сообщения через вычислительную сеть с применением аппаратуры КРК необходимо сначала сформировать сеть из последовательно соединенных звеньев аппаратуры КРК.

В качестве такой аппаратуры можно, например, использовать известную

однопроходную систему КРК (патент РФ №2665249).

Каждое звено должно иметь входной и выходной узлы обработки, связанные оптоволоконной линией. На каждом узле необходимо установить блок обработки с возможностью принимать данные, обрабатывать данные и передавать данные. С выходным узлом 1-го звена КРК должен быть связан 1-й компьютер с возможностью передавать сообщение в блок обработки входного узла, а с блоком обработки входного узла последнего звена КРК - 2-й компьютер с возможностью принимать сообщение от блока обработки входного узла.

Рассмотрим реализацию предложенного способа на примере использования M=2 звеньев, соответственно, в сети будет 4 узла (см. схему на фигуре графического изображения).

Установим также, что динамическое переключение алгоритмов шифрования не применяется (используется только алгоритмов шифрования по ГОСТ Р 34.12-2015), поэтому значение параметра Z не используется.

Система КРК запускается, и в каждом звене вырабатываются квантовые ключи.

В 1-м компьютере формируется передаваемое сообщение, например, длиной N=256 бит, и передается через цифровую линию передачи данных в блок обработки выходного узла 1-го звена обработки.

Сообщение из 1-го компьютера получают в блоке обработки выходного узла 1-го звена обработки.

Вычисляют длину записи Y в битах для записи в него значения длины ключа в цепи передачи по формуле:

$$Y = |\log_2[N*2^M]|$$

В рассматриваемом примере длина значения Y=10 бит.

Далее зашифровывают сообщение в блоке обработки выходного узла первого звена обработки, выполняя следующие действия:

• получают квантовый ключ длинной X1 бит, который выработан в результате выполнения протокола КРК в 1-м звене обработки, для определенности примем, что длина ключа X1=256 бит,

• зашифровывают сообщение на квантовом ключе 1-го звена обработки, с применением установленного алгоритма зашифрования (по ГОСТ Р 34.12-2015).

После этого

• передают зашифрованное сообщение в блок обработки входного узла 1-го звена обработки,

• получают зашифрованное сообщение в блоке обработке входного узла 1-го звена обработки,

• добавляют к полученному зашифрованному сообщению ключ X1,

• вычисляют длину X1 в двоичном виде, соответственно, для X1=256 бит получим значение "01 0000 0000", которое записывают в Y1,

• добавляют к полученному сообщению Y1, получая входное сообщение для входного узла 2-го звена обработки,

• передают входное сообщение в блок обработки выходного узла 2-го звена.

После получения входного сообщения в блоке обработки выходного узла 2-го звена обработки, зашифровывают входное сообщение, выполняя следующие действия:

• получают квантовый ключ длиной X2 бит, который выработан в результате выполнения протокола КРК во 2-ом звене обработки, длина ключа также равна X2= 256 бит,

• зашифровывают сообщение на квантовом ключе 2-ого звена обработки, с применением установленного алгоритма зашифрования (по ГОСТ Р 34.12-2015),

• добавляют к полученному зашифрованному сообщению ключ X2,

• вычисляют длину X2 в двоичном виде, соответственно, для X2=256 бит получим значение "01 0000 0000", которое записывают в Y2,

• добавляют к полученному сообщению Y2, получая входное сообщение для входного узла 2-го звена обработки,

• передают входное сообщение в блок обработки входного узла 2-го звена.

Затем

• передают зашифрованное сообщение в блок обработки входного узла 2-го звена обработки,

• получают зашифрованное сообщение в блоке обработки входного узла 2-го звена обработки,

Затем расшифровывают сообщение в блоке обработки входного узле 2-го звена обработки, выполняя следующие действия:

• отделяют от входного сообщения Y2 с длиной записи значения Y2=10 бит,

• определяют из значения Y2 длину ключа X1=256 бит,

• отделяют ключ X2 2-го звена обработки длиной 256 бит от входного сообщения,

• расшифровывают зашифрованное сообщение с использованием квантового ключа X2, в результате получают входное сообщение, которое было передано в блок обработки входного узла 2-го звена обработки,

• отделяют от расшифрованного сообщения Y1 с длиной записи значения Y1=10 бит,

• определяют из значения Y1 длину ключа X1=256 бит,

• отделяют ключ X1 2-го звена обработки длиной 256 бит от входного сообщения,

• расшифровывают оставшуюся часть входного сообщения с использованием отделенного ключа X1, получая исходное сообщение.

После этого передают исходное сообщение из блока обработки входного узла 2-го звена обработки во 2-й компьютер.

(57) Формула изобретения

Способ передачи сообщения через вычислительную сеть с применением аппаратуры квантового распределения ключей, причем сеть содержит

M последовательно соединенных звеньев обработки, причем

каждое звено состоит из входного и выходного узлов аппаратуры квантового распределения ключей, выполненной с возможностью формирования квантовых ключей в результате выполнения установленного протокола квантового распределения ключей;

входной и выходной узлы аппаратуры квантового распределения ключей соседних звеньев связаны оптоволоконной линией;

на каждом входном узле установлен блок обработки, связанный с цифровой сетью передачи данных и выполненный с возможностью

принимать данные,

обрабатывать данные,

передавать данные;

на каждом выходном узле установлен блок обработки, связанный с цифровой сетью передачи данных и выполненный с возможностью

принимать данные,

обрабатывать данные,

передавать данные;

1-й компьютер, связанный с блоком обработки выходного узла 1-го звена обработки через цифровую линию передачи данных и выполненный с возможностью передавать сообщение во входной узел;

2-й компьютер, связанный с блоком обработки входного узла M-го звена через цифровую линию передачи данных и выполненный с возможностью принимать сообщение от входного узла;

способ, заключающийся в том, что

формируют сообщение размером N бит в 1-м компьютере;

передают сообщение из 1-го компьютера в блок обработки выходного узла 1-го звена обработки через цифровую линию передачи данных;

получают сообщение из 1-го компьютера в блоке обработки выходного узла 1-го звена обработки;

вычисляют k=1;

вычисляют длину записи Y в битах для записи в двоичном виде значений длины ключа шифрования для каждого звена обработки;

вычисляют длину записи Z в битах для записи в двоичном виде значений условного кода алгоритма шифрования для каждого звена обработки;

(A) зашифровывают сообщение в блоке обработки выходного узла k-го звена обработки, выполняя следующие действия:

получают квантовый ключ длинной X_k бит, который выработан в результате выполнения протокола квантового распределения ключей на k-м звене обработки;

зашифровывают сообщение на квантовом ключе k-го звена обработки с применением выбранного алгоритма шифрования;

передают зашифрованное сообщение в блок обработки входного узла k-го звена обработки;

добавляют к полученному зашифрованному сообщению ключ X_k, полученный во входном узле k-го звена обработки;

формируют значение Y_k в зависимости от длины ключа X_k;

добавляют к полученному сообщению Y_k;

формируют значение Z_k в зависимости от выбранного алгоритма шифрования;

добавляют к полученному сообщению Z_k, получая входное сообщение для следующего входного узла;

если k<M, то

передают входное сообщение в блок обработки выходного узла k+1 звена через цифровую сеть передачи данных;

вычисляют k=k+1;

переходят к этапу A;

получают зашифрованное сообщение в блоке обработки входного узла k-го звена обработки через цифровую сеть передачи данных;

обрабатывают зашифрованное сообщение в блоке обработке входного узла k-го звена обработки, выполняя следующие действия:

расшифровывают зашифрованное сообщение с использованием квантового ключа M-го узла, в результате получают входное сообщение, которое было передано в блок обработки выходного узла k-го звена обработки;

(B) отделяют от входного сообщения длину записи Y_k;

определяют длину ключа из значения Y_k;

отделяют ключ k-го звена обработки от входного сообщения;
отделяют от сообщения Z_k;
определяют алгоритм шифрования из кода, записанного в значении Z_k;
расшифровывают оставшуюся часть входного сообщения с использованием отделенного k-го ключа;
если k>1, то
вычисляют k=k-1;
переходят к этапу (B);
получают исходное сообщение,
передают сообщение из блока обработки входного узла M-го звена обработки во 2-й компьютер через цифровую линию передачи данных.

1