РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2 469 485** (13) **C1**

(51) МПК
H04L 9/14 (2006.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: **2011119636/08, 05.10.2009**

(24) Дата начала отсчета срока действия патента:
05.10.2009

Приоритет(ы):
(30) Конвенционный приоритет:
17.10.2008 US 12/253,411

(45) Опубликовано: **10.12.2012** Бюл. № **34**

(56) Список документов, цитированных в отчете о поиске: **US 6909708 B1, 21.06.2005. US 20020091975 A1, 11.07.2002. US 20070112676 A1, 17.05.2007. EP 1693731 A1, 23.08.2006. RU 2196392 C2, 10.01.2003. RU 2158446 C2, 27.10.2000.**

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **17.05.2011**

(86) Заявка PCT:
US 2009/059503 (05.10.2009)

(87) Публикация заявки PCT:
WO 2010/045044 (22.04.2010)

Адрес для переписки:
129090, Москва, ул. Б. Спасская, 25, стр.3, ООО "Юридическая фирма Городисский и Партнеры"

(72) Автор(ы):
ЧАУДХАРИ Дипендра М. (US),
БЕЛМОНТ Джон П. (US),
ВИАТРОВСКИ Дэвид Г. (US)

(73) Патентообладатель(и):
МОТОРОЛА СОЛЮШНЗ, ИНК. (US)

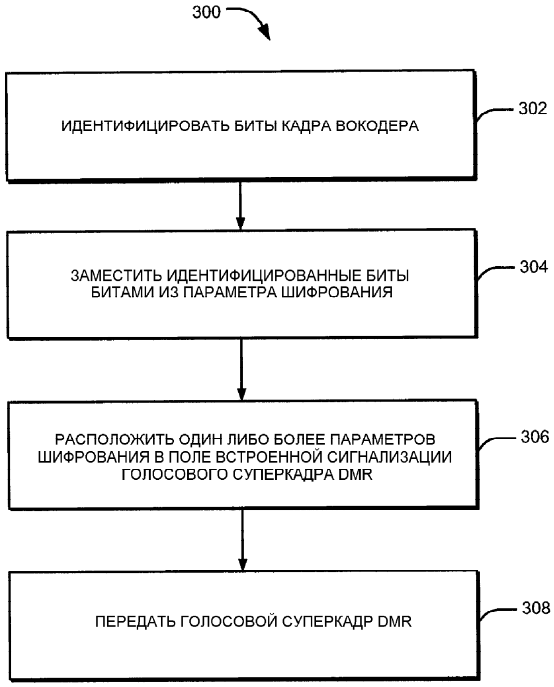
RU 2469485 C1

RU 2469485 C1

(54) СПОСОБ И УСТРОЙСТВО ДЛЯ ПЕРЕДАЧИ ПАРАМЕТРОВ ШИФРОВАНИЯ

(57) Реферат:

Изобретение относится к передаче параметров шифрования в голосовом суперкадре ETSI DMR. Техническим результатом является расширение функциональных возможностей за счет передачи параметров шифрования, которые могут быть реализованы в системе DMR. Передающее устройство шифрует голосовые суперкадры DMR, используя параметры шифрования, и передает параметры шифрования в по меньшей мере одном из голосовых суперкадров с помощью: идентификации выбранного числа битов из множества кадров вокодера голосового суперкадра; замещения каждого из идентифицированных битов соответствующим битом первого параметра шифрования; расположения по меньшей мере одного параметра шифрования в поле встроенной сигнализации голосового суперкадра; и передачи голосового суперкадра с параметрами шифрования в приемное устройство. Приемное устройство извлекает параметры шифрования, которые могут быть идентификатором ключа, идентификатором алгоритма и вектором инициализации для использования в дешифрованных сообщениях от передающего устройства. 3 н. и 12 з.п. ф-лы, 8 ил.



Фиг.3

RU 2469485 C1

RU 2469485 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 469 485** (13) **C1**

(51) Int. Cl.
H04L 9/14 (2006.01)

(12) ABSTRACT OF INVENTION

(21)(22) Application: **2011119636/08, 05.10.2009**

(24) Effective date for property rights:
05.10.2009

Priority:
(30) Convention priority:
17.10.2008 US 12/253,411

(45) Date of publication: **10.12.2012 Bull. 34**

(85) Commencement of national phase: **17.05.2011**

(86) PCT application:
US 2009/059503 (05.10.2009)

(87) PCT publication:
WO 2010/045044 (22.04.2010)

Mail address:
129090, Moskva, ul. B. Spasskaja, 25, str.3, OOO "Juridicheskaja firma Gorodisskij i Partnery"

(72) Inventor(s):
ChAUDKhARI Dipendra M. (US),
BELMONT Dzhon P. (US),
VIATROVSKI Dehvid G. (US)

(73) Proprietor(s):
MOTOROLA SOLJuShNZ, INK. (US)

RU 2469485 C1

(54) METHOD AND DEVICE FOR TRANSMISSION OF CODING PARAMETERS

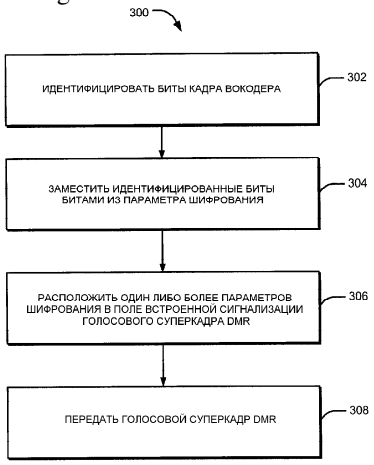
(57) Abstract:

FIELD: information technologies.

SUBSTANCE: transmitting device codes voice superframes DMR using coding parameters, and sends coding parameters in at least one of voice superframes with the help of the following: identification of a selected number of bits from multiple frames of a vocoder of a voice superframe; replacement of each of identified bits with an appropriate bit of the first coding parameter; placement of at least one coding parameter in the field of inbuilt alarm of the voice superframe; and transmission of a voice superframe with coding parameters into a receiving device. The receiving device extracts coding parameters, which may be an identifier of a key, an identifier of a logic and an initialisation vector for use in decoded messages from the transmitting device.

EFFECT: expansion of functional possibilities due to transfer of coding parameters, which may be implemented in a DMR system.

15 cl, 8 dwg



Фиг.3

RU 2469485 C1

ОБЛАСТЬ ТЕХНИКИ

Область техники относится в целом к системам беспроводной связи и, в частности, к передаче параметров шифрования в голосовом суперкадре ETSI DMR.

ПРЕДШЕСТВУЮЩИЙ УРОВЕНЬ ТЕХНИКИ

В течение последних нескольких десятилетий цифровые сети двусторонней радиосвязи стали широко распространенными. Устройства двусторонней радиосвязи типично позволяют пользователям принимать, а также передавать речь либо данные. Для предоставления функциональной совместимости между различными системами и разработчиками цифровой двусторонней радиосвязи Европейский институт стандартизации в области электросвязи (ETSI) представил стандарт DMR-радиоинтерфейса (цифровая мобильная радиосвязь), который определяет различные протоколы, используемые устройствами двусторонней радиосвязи на уровне передачи данных (т.е. уровень 2) из хорошо известной семиуровневой модели взаимодействия открытых систем сетевых компьютеров, и которая описана в ETSI TS (техническая спецификация) 102 361-1 v1.4.5 (2007-12). Ссылка в данном документе на стандарт ETSI DMR включает в себя текущую версию технической спецификации и все последующие и будущие версии.

Стандарт ETSI DMR определяет TDMA-структуру (множественный доступ с временным разделением) с двумя интервалами, которую могут использовать передающие и приемные устройства для отправки голосовых сигналов и/или сигналов данных. Голосовые сигналы и сигналы данных передаются в интервалах TDMA согласно общему формату пакетов, заданному в стандарте. Кроме того, пакеты, содержащие голосовые сигналы, передаются в суперкадрах, которые имеют длину 360 мс и которые имеют шесть пакетов, обозначенных буквами с «A» по «F».

Более того, голосовые и информационные сообщения могут передаваться явно как открытая информация либо могут шифроваться и создаваться конфиденциальными так, что данные не могут быть считаны либо речь нельзя услышать на любом устройстве, отличающемся от того, которое имеет соответствующие параметры, необходимые для дешифровки сообщений. Соответственно, шифрование и дешифрование (либо конфиденциальность) являются способами защиты связи и сохранения ее конфиденциальной во время передачи сообщений между двумя устройствами. Тем не менее, в контексте этого изобретения конфиденциальность не предоставляет какого-либо механизма для аутентификации устройства либо пользователей либо для защиты целостности сообщений, например, чтобы гарантировать, что сообщения декодируются соответствующим образом либо что все сообщения действительно были приняты в приемном устройстве.

Процесс шифрования в целом содержит передающее устройство, объединяющее определенные криптографические параметры с открытой информацией для формирования защищенной информации, которая отсылается в приемное устройство. Для процессов шифрования, которые используют криптографический алгоритм, например, ARC4, криптографические параметры типично включают в себя ключ, криптографический алгоритм и вектор инициализации (IV) для алгоритма. Соответственно, для того чтобы правильно дешифровать защищенную информацию, приемное устройство должно знать и использовать тот же самый ключ, криптографический алгоритм и IV, которые использовались передающим устройством.

Для того чтобы сделать криптографические параметры известными для приемного устройства, передающее устройство может отсылать в приемное устройство сами криптографические параметры и/или идентификаторы (ID) шифрования, которые

идентифицируют один либо более криптографических параметров. Криптографические параметры и идентификаторы шифрования вместе упоминаются в данном документе как параметры шифрования. Таким образом, когда ссылаются на набор параметров шифрования, набор может включать в себя лишь один либо более криптографических параметров, лишь один либо более идентификаторов шифрования либо сочетание как криптографических параметров, так и идентификаторов шифрования. В настоящее время не существует заданного в стандарте DMR способа для переноса параметров шифрования.

Таким образом, существует необходимость в способе и устройстве для передачи параметров шифрования, которые могут быть реализованы в системе DMR.

КРАТКОЕ ОПИСАНИЕ ЧЕРТЕЖЕЙ

Прилагаемые чертежи, где аналогичные номера ссылок относятся к идентичным либо функционально аналогичным элементам по всем отдельным представлениям, которые включены ниже вместе с подробным описанием и создают часть спецификации и служат для дополнительной иллюстрации различных вариантов осуществления понятий, которые включают в себя заявленное изобретение, и для того чтобы пояснить различные принципы и преимущества этих вариантов осуществления.

Фиг.1 показывает блок-схему системы связи согласно иллюстративному варианту осуществления.

Фиг.2 иллюстрирует варианты осуществления, реализованные в структуре голосового суперкадра DMR, голосовом пакете в суперкадре и кадрах вокодера в голосовом пакете.

Фиг.3 показывает блок-схему способа для передачи параметров шифрования в голосовом суперкадре DMR согласно иллюстративному варианту осуществления.

Фиг.4 показывает блок-схему способа расположения IV в голосовом суперкадре DMR согласно иллюстративному варианту осуществления.

Фиг.5 показывает выбор битов из кадров вокодера в голосовом суперкадре DMR и замещение их модифицированными битами IV согласно иллюстративному варианту осуществления.

Фиг.6 показывает блок-схему способа для расположения идентификаторов шифрования в голосовом суперкадре DMR согласно иллюстративному варианту осуществления.

Фиг.7 показывает расположение идентификаторов шифрования в поле встроенной сигнализации голосового пакета DMR согласно иллюстративному варианту осуществления.

Фиг.8 показывает блок-схему способа для приема параметров шифрования в голосовом суперкадре DMR согласно иллюстративному варианту осуществления.

Опытные специалисты поймут, что элементы на фигурах проиллюстрированы для простоты и ясности и не обязательно должны быть начерчены в масштабе. Например, размеры некоторых элементов на чертежах могут быть увеличены относительно других элементов, чтобы способствовать пониманию различных вариантов осуществления. Кроме того, описание и чертежи не обязательно требуют проиллюстрированного порядка расположения. Представлены компоненты устройства и составляющие способа, которым отведены, где это необходимо, обычные символы на чертежах, показывающие только те конкретные подробности, которые имеют отношение к пониманию различных вариантов осуществления, так чтобы не затруднять понимание изобретения подробностями, которые будут полностью очевидны обычным специалистам в данной области техники, имеющие

преимущество описания в данном документе. Таким образом, будет принято во внимание, что для простоты и ясности иллюстрации общие и хорошо понятные элементы, которые полезны либо необходимы в коммерчески выполнимом варианте осуществления, могут быть не отображены для того, чтобы помочь в менее затруднительном представлении этих различных вариантов осуществления.

ПОДРОБНОЕ ОПИСАНИЕ

В сущности, в соответствии с различными вариантами осуществления передающее устройство шифрует голосовые суперкадры DMR, используя криптографические параметры, которые в одном варианте осуществления включают в себя ключ, алгоритм шифрования и IV и отсылает голосовые кадры DMR в приемное устройство. Для того чтобы помочь приемному устройству в дешифровании голосовых суперкадров DMR, передающее устройство: идентифицирует выбранное число битов из множества кадров вокодера голосового суперкадра DMR; замещает каждый из идентифицированных битов соответствующим битом параметра шифрования (например, IV либо модифицированным IV); располагает, по меньшей мере, один параметр шифрования (например, ID ключа и ID алгоритма) в поле встроенной сигнализации голосового суперкадра DMR; и передает голосовой суперкадр DMR с параметрами шифрования в приемное устройство. Приемное устройство: извлекает идентификаторы шифрования; извлекает выбранное число битов из множества кадров вокодера голосового суперкадра DMR; компонует извлеченные биты для получения IV; и использует извлеченный IV и идентификаторы шифрования для дешифрования голосовых суперкадров DMR.

В одном варианте осуществления ID ключа и ID алгоритма отсылаются в поле встроенной сигнализации голосового кадра DMR пакета F и, следовательно, не мешают передаче какой-либо другой информации. В дополнительном варианте осуществления биты из кадров вокодера, которые замещаются IV (либо битами модифицированного IV), являются наименьшими значащими битами для способствования минимальному искажению голосового сигнала. Более того, в другом варианте осуществления IV, ID ключа и ID алгоритма отсылаются в каждом голосовом суперкадре DMR для способствования минимальной задержке последнего ввода абонентского блока для голосового вызова. Специалисты в данной области техники поймут, что вышеуказанные преимущества и другие преимущества, описанные в данном документе, являются всего лишь иллюстративными и не подразумевают полное изложение всех преимуществ различных вариантов осуществления.

Ссылаясь теперь на чертежи, фиг.1 показывает блок-схему системы 100 связи согласно иллюстративному варианту осуществления. Система 100 связи отображена в очень обобщенной форме. Например, система 100 проиллюстрирована как содержащая единственное инфраструктурное устройство 106 и три устройства 102, 104, 108 беспроводной связи для облегчения иллюстрации. Тем не менее, идеи в данном документе могут быть реализованы в системе, имеющей дополнительные инфраструктурные устройства и устройства беспроводной связи.

Каждое инфраструктурное устройство и устройство беспроводной связи, по меньшей мере, оснащено приемопередатчиком 110 (т.е. передатчик и приемник), памятью 112 и устройством 114 обработки и дополнительно оснащено любыми дополнительными компонентами, что необходимо для коммерческого варианта осуществления. Приемопередатчик 110, память 112 и устройство 114 обработки имеют любую подходящую физическую реализацию и топологически соединяются в

зависимости от конкретной реализации устройства. Эти компоненты дополнительно функционально соединяются и могут адаптироваться, располагаться, конфигурироваться и проектироваться для осуществления способов согласно идеям в данном документе, например, как иллюстративно описано по ссылке на оставшиеся фигуры с фиг.2 по фиг.8.

Как указано в данном документе, устройство беспроводной связи включает в себя, но не ограничено устройствами, в общем упоминаемыми как терминалы доступа, подвижные радиостанции, мобильные станции, абонентские блоки, абонентское оборудование, мобильные устройства либо любое другое устройство, допускающее работу в беспроводной среде. Примеры устройств беспроводной связи включают в себя, но не ограничены, устройствами двусторонней связи, мобильными телефонами, сотовыми телефонами, персональными цифровыми помощниками (PDA), портативными компьютерами и пейджерами с поддержкой двусторонней связи. Как используется в материалах данной заявки, инфраструктурное устройство является устройством, которое является частью фиксированной сетевой инфраструктуры и может принимать информацию (либо управляющую, либо мультимедийную, например, данные, речь (звук), видео и т.д.) в сигнале от устройства беспроводной связи и передавать информацию в сигналах в одно либо более устройств беспроводной связи через линию связи. Инфраструктурное устройство включает в себя, но не ограничено оборудованием, обычно упоминаемым как повторители, базовые радиостанции, базовые станции, базовые приемопередающие станции, точки доступа, маршрутизаторы либо любой другой тип инфраструктурного оборудования, взаимодействующий с устройством беспроводной связи в беспроводной среде.

В этом иллюстративном варианте осуществления система 100 является системой DMR, и инфраструктурное устройство 106 и устройства 102, 104 и 108 беспроводной связи осуществляют связь, используя радиоинтерфейс, как определено в стандарте DMR (как таковое, устройство 106 в дальнейшем в данном документе упоминается как базовая станция (либо BS), и устройства 102, 104 и 108 в дальнейшем в данном документе упоминаются как мобильные станции либо (MS)). В соответствии со стандартом DMR MS могут осуществлять связь в «прямом режиме» либо «режиме разговор вокруг», в котором MS осуществляют связь непосредственно друг с другом без управления BS. MS 102 и 104 проиллюстрированы на фиг.1 как осуществляющие связь в прямом режиме. MS может также осуществлять связь в «режиме повторителя», в котором MS осуществляет связь через BS. MS 102 и 108 проиллюстрированы на фиг.1 как осуществляющие связь в режиме повторителя, используя BS 106. Передачи от BS в MS в режиме повторителя называются исходящими передачами, и передачи от MS в BS в режиме повторителя называются входящими передачами.

Как упоминалось ранее, устройства в системе 100 осуществляют связь, используя линии связи (также упоминаемые в данном документе как каналы). Каналы содержат физические каналы и логические каналы. Физические каналы являются физическими ресурсами связи, по которым отсылается информация между элементами внутри системы 100. Физические каналы могут содержать проводные либо беспроводные линии связи. Если физические каналы содержат беспроводные линии связи, соответствующие физические ресурсы являются назначением радиоспектра, который разбивается на РЧ-несущие с каждой РЧ-несущей, разбитой во времени на кадры и временные интервалы. Интервалы для двух физических TDMA-каналов отмечены как канал «1» и канал «2». Пакет DMR является промежутком РЧ-несущей, которая модулируется потоком данных (различного формата), и представляет собой

физический канал единственного временного интервала. Пакет является наименьшим автономным блоком TDMA-передачи, заданным в стандарте DMR.

Физический канал требуется для поддержки логического канала, который является логической магистралью связи между двумя либо более сторонами. Логические каналы разделены на две категории: каналы трафика, передающие речь либо информацию в виде данных; и каналы управления, передающие сигнализацию, которые определенно связаны с созданием и управлением соединениями и с управлением в системе 100. Сигнализация от цели до источника упоминается в данном документе как сигнализация обратного канала (RC). Подробности иллюстративных вариантов осуществления в дальнейшем описаны с помощью ссылки на фигуры с фиг.2 по фиг.8.

Фиг.2 иллюстрирует варианты осуществления, реализованные в структуре голосового суперкадра DMR, голосовом пакете в голосовом суперкадре DMR и кадрах вокодера в голосовом пакете. Временная диаграмма для голосового суперкадра DMR проиллюстрирована на 200. Голосовой суперкадр DMR отсылается передающей MS в приемную MS и может отсылаться либо в прямом режиме, либо в режиме повторителя. Голосовой суперкадр DMR отсылается по одному из двух каналов и содержит шесть пакетов 204, отмеченных с «A» по «F», т.е. 204-A, 204-B, 204-C, 204-D, 204-E и 204-F. Другой канал, содержащий блоки 206, может быть неиспользуемым либо может использоваться другими устройствами в системе 100.

Один из пакетов 204 голосового суперкадра DMR проиллюстрирован по ссылке на 210. Структура исходного пакета включает в себя два голосовых 108 битовых поля 212 и 214 полезной нагрузки и 48-битовое поле 208 в центре пакета, упоминаемого в данном документе как поле «встроенной сигнализации». Поле 208 встроенной сигнализации передает либо синхронизацию либо встроенную сигнализацию в зависимости от конкретного пакета в голосовом суперкадре DMR. Передача заданного пакета занимает 27,5 мс, и за ним может следовать защитный интервал в 2,5 мс либо канал общего оповещения (CACH). Таким образом, один пакет равен 30 мс; один кадр из двух смежных временных интервалов, упоминаемых как 1 и 2, равен 60 мс; и один голосовой суперкадр DMR равен 360 мс (из-за временного согласования для другого канала).

В одном варианте осуществления пакет A, который обозначает начало голосового суперкадра DMR, содержит синхронизацию (например, в виде известных синхронизирующих комбинаций) в поле 208. Пакеты с B по F могут содержать встроенную сигнализацию, например, управление линией связи (включая, но не ограничиваясь, исходные адреса и адреса назначения, тип сообщения, длину), RC-сигнализацию и т.д. в поле 208, и в некоторых сценариях реализации поле 208 в, по меньшей мере, одном из пакетов с B по F может быть пустым (нулевым) либо иметь несколько неиспользуемых битов.

Как хорошо известно в обработке голосовых сообщений, вокодер используется передающим устройством для кодирования оцифрованной речи для целей использования прямого исправления ошибок (FEC), сжатия, шифрования, перемежения и т.д. В варианте осуществления передающее устройство содержит вокодер в 3600 бит/с, который порождает 72-битовые кадры (включая FEC) каждые 20 мс. Таким образом, голосовой пакет 204 передает три 72-битовых кадра 222, 224 и 226 вокодера (включая FEC), включая 48-битовое поле встроенной сигнализации, как проиллюстрировано на 220. Фиг.3-8 иллюстрируют варианты осуществления, в которых передающее устройство отсылает параметры шифрования (в этом случае IV,

ID ключа и ID алгоритма) в поле встроенной сигнализации и в кадрах вокодера, которые содержат зашифрованные голосовые биты. Тем не менее, до описания вариантов осуществления переноса параметров шифрования ниже указано краткое описание того, как получены параметры шифрования и, в целом, как используются в иллюстративном процессе шифрования и дешифрования.

В варианте осуществления передающее устройство использует криптографические параметры ключа, криптографический алгоритм и IV для инициализации криптографического алгоритма. Алгоритм ключа и криптографический алгоритм могут быть выбраны из нескольких ключей и алгоритмов, сохраненных в и обычно используемых как передающими устройствами, так и приемными устройствами. В иллюстративном примере выбранный ключ равен длине в 40 битов и однозначно идентифицируется ID ключа, и алгоритм (например, ARC4 как хорошо известный в данной области техники) является тем, который требует IV и идентифицируется с помощью уникального ID алгоритма. Более того, различные ключи и алгоритмы могут использоваться для шифрования голосовых сообщений в отличие от информационных сообщений.

IV является блоком битов, который используется как источник для алгоритма создания потока уникальных ключей независимого от других потоков ключей, созданных тем же самым ключом. В этом иллюстративном примере передающее устройство формирует IV длиной в 32 бита, который инициализируется случайным числом, которое отличается для каждой инициализации и для каждой MS. Инициализация может быть выполнена либо при включении питания либо в начале голосового либо информационного вызова. Более того, для предоставления надежной криптографической защиты формируется другой поток ключей для каждого блока данных пакетов (PDU) DMR и для каждого голосового суперкадра DMR. Например, IV может обновляться с помощью применения линейного регистра сдвига с обратными связями (LFSR) к предыдущему IV. Тем не менее, в других вариантах осуществления тот же самый IV может использоваться для формирования потока ключей для множества голосовых суперкадров DMR (либо PDU) либо один раз для каждого вызова, но эти способы предоставляют меньшую криптографическую защиту. Следует также отметить, что побитовая длина ключа и IV и конкретный алгоритм, предоставленные в данном документе, указаны лишь в качестве примеров и не предназначены ограничивать объем идей данного документа. Соответственно, любой подходящий ключ, алгоритм, IV либо другой релевантный параметр шифрования могут использоваться в зависимости от конкретной реализованной методики шифрования.

Возвращаясь к описанию иллюстративного процесса шифрования, для того чтобы защитить открытую информацию, передающее устройство выбирает ключ и конкатенирует ключ с IV, чтобы использовать в инициализации криптографического алгоритма, который используется для формирования потока ключей байт за байтом на выходе алгоритма. Поток ключей объединяется с открытой информацией, используя логический оператор исключающего ИЛИ (т.е. исключающее ИЛИ) для формирования защищенной информации, которая передается в приемное устройство. Для дешифрования защищенной информации приемное устройство должно сформировать тот же самый поток ключей, который был сформирован в передающем устройстве, и исключающее ИЛИ потока ключей с защищенной информацией для получения открытой информации, которую можно прочесть либо услышать пользователю приемного устройства. Тем не менее, для того чтобы сформировать тот

же самый поток ключей, приемное устройство должно использовать тот же самый ключ, криптографический алгоритм и IV, которые использовались в передающем устройстве. Оставшиеся фиг.3-8 предоставлены для иллюстративного варианта осуществления для передающего устройства, чтобы переносить параметры шифрования в приемное устройство в голосовом суперкадре DMR, и для приемного устройства для извлечения этих параметров шифрования для использования в процессе дешифрования.

Обратимся теперь к фиг.3, на которой показана блок-схема способа 300 для передачи параметров шифрования в голосовом суперкадре DMR согласно иллюстративному варианту осуществления. В целом, параметры шифрования переносятся в голосовом суперкадре DMR в поле встроенной сигнализации и с помощью замещения битов кадра вокодера на биты одного либо более параметров шифрования.

Более конкретно, на этапе 302 передающее устройство идентифицирует выбранное число битов из множества кадров вокодера. Любые биты могут быть идентифицированы и замещены. Тем не менее, идентификация и замещение только наименьших значащих битов является выгодным в том, что это имеет наименьшее воздействие либо, другими словами, вызывает минимальное искажение звука, слышимого в приемном устройстве. Как используется в материалах настоящей заявки, фраза «наименьшие значащие биты» - это те биты вокодера, которые имеют наименее заметное воздействие на качество звучания безотносительно к расположению битов. Таким образом, как используется в этом смысле, наименьшие значащие биты относятся не только лишь к битам, имеющим нумерацию самого младшего бита согласно тому, как пронумерованы биты вокодера.

Передающее устройство замещает (304), по меньшей мере, некоторые из идентифицированных битов соответствующими битами, по меньшей мере, одного параметра шифрования. В вариантах осуществления, описанных ниже со ссылкой на фиг.4 и 5, идентифицированные биты замещаются соответствующими битами IV, и, более конкретно, каждый из идентифицированных битов замещается соответствующими битами модифицированного IV, которые объединяются с битами контроля ошибок (т.е. биты четности обнаружения ошибок и/или биты четности прямого обнаружения ошибок). Тем не менее, в другом варианте осуществления идентифицированные биты могут замещаться соответствующими битами усеченного либо укороченного IV. В еще одном варианте осуществления идентифицированные биты кадра вокодера могут замещаться битами других параметров шифрования, например, ключа, ID ключа, ID алгоритма и т.д. в дополнение либо альтернативно к IV либо к модифицированному IV.

Передающее устройство на 306 также размещает один либо более параметров шифрования в поле встроенной сигнализации в голосовом суперкадре DMR. Любые параметры шифрования (либо их часть) могут размещаться в одном либо более полях встроенной сигнализации любых голосовых пакетов. Тем не менее, так чтобы не мешать передаче другой информации и сигнализации в голосовом суперкадре DMR, параметры шифрования меньшего размера, например, идентификаторы шифрования (например, ID ключа и ID алгоритма) размещаются в поле встроенной сигнализации в пакете, который имеет биты, которые не используются иным образом другой информацией либо сигнализацией, например, в пакете F. Иллюстративный вариант осуществления расположения параметров шифрования в поле встроенной сигнализации описан со ссылкой на фиг.6 и 7. Передающее устройство затем

передает (308) голосовой суперкадр DMR с параметрами шифрования в одно либо более приемных устройств.

Обратимся теперь к фиг.4, на нем показана блок-схема способа расположения модифицированного IV в голосовом суперкадре DMR согласно иллюстративному варианту осуществления. Фиг.4 описана совместно с фиг.5, чтобы показать определенный пример каждого из выбранных битов кадра вокодера, которые замещаются соответствующими битами модифицированного IV. При формировании IV (502) передающее устройство вычисляет (402) биты четности обнаружения ошибок по IV, которые соединены (404) с IV для формирования соединенного IV. Любые методики обнаружения ошибок могут использоваться для формирования битов четности обнаружения ошибок, включая, но не ограничиваясь хэш-функциями, простой четностью, контрольной суммой и т.д. Тем не менее, в варианте осуществления, который проиллюстрирован со ссылкой на фиг.5, передающее устройство вычисляет проверку CRC (циклическая проверка по избыточности) по IV для формирования битов 504 четности обнаружения ошибок, которые добавлены к IV 502. В одном иллюстративном примере CRC вычисляется, используя полиномиальную арифметику, использующую порождающий полином CRC, например, x4+x+1 для формирования 4-битовой CRC, но может использоваться любой другой подходящий способ для вычисления CRC.

На 406 передающее устройство добавляет биты четности исправления ошибок к конкатенированному IV для формирования модифицированного IV, используя любую подходящую методику исправления ошибок, включая, но не ограничиваясь использованием, например, методику ARQ (автоматический запрос повторной передачи), код Хемминга, код Голея, код Рида-Соломона. В варианте осуществления, проиллюстрированном со ссылкой на фиг.5, передающее устройство разбивает 36-битовый конкатенированный IV на три сегмента и использует расширенный (24, 12, 8) код Голея для конкатенированного IV, для добавления 36 битов четности FEC (прямое исправление ошибок) и, таким образом, формирования 72 бита модифицированного IV 506. Может быть сформировано больше либо меньше, чем 72 бита, если используется другая методика исправления ошибок. Передающее устройство разделяет модифицированный IV на три равных сегмента 508, 510 и 512 из 24 битов, которые необходимо перенести в кадрах вокодера голосового суперкадра DMR. Как показано на фиг.5, сегмент 508 содержит биты от 0 до 23; сегмент 510 содержит биты с 24 по 47; сегмент 512 содержит биты с 48 по 71. Разделение модифицированного IV на равные сегменты из 24 битов не требуется для реализации идей в данном документе. Модифицированный IV не нужно разделять полностью, либо он может разделяться на другое число сегментов, которые имеют равное либо неравное число битов.

Передающее устройство идентифицирует (408) выбранное число битов из кадров вокодера и замещает эти биты 72 битами модифицированного IV. В иллюстративном варианте осуществления передающее устройство идентифицирует четыре наименьших значащих бита из каждого из трех кадров (VF1, VF2, VF3) вокодера в каждом из шести пакетов (с 204-A по 204-F) суперкадра DMR, показанного на фиг.2, и перемежает (410) модифицированные биты IV в позициях идентифицированных битов кадра вокодера. В случае если модифицированный IV длиннее либо короче, чем 72 бита, из кадров вокодера может быть идентифицировано больше либо меньше битов для переноса IV. Используя определенные вокодеры 3600 бит/с, может быть выбрано до шести битов из кадров вокодера с минимальным искажением для переданного голосового сигнала.

Биты из каждого модифицированного сегмента 508, 510, 512 IV могут последовательно размещаться в позициях идентифицированных битов вокодера. Тем не менее, в этом иллюстративном примере модифицированный IV перемежается в позициях бита кадра вокодера для того, чтобы расположить биты IV несмежным образом для защиты IV в отношении ошибок пакетов во время передачи. Биты модифицированного IV могут перемежаться побитно, но в этом примере небольшие блоки битов (например, четыре битовых блока в этом случае) перемежаются в позициях блоков равного размера идентифицированных битов кадра вокодера. Например, блок 514 сегмента 508 располагается в кадре (VF3) вокодера пакета 204-F. Блок 516 сегмента 510 располагается в кадре (VF2) вокодера пакета 204-F; и блок 518 сегмента 512 располагается в вокодере (VF1) пакета 204-F. Аналогично следующий четырехбитовый блок из каждого сегмента 508, 510, 512 располагается в кадрах VF3, VF2 и VF1 вокодера пакета 204-E и так далее.

Как упомянуто выше, фиг.6 и 7 предоставляют иллюстративный пример расположения параметров шифрования (в этом случае ID 702 ключа и ID 704 алгоритма) в голосовом суперкадре DMR. В одном варианте осуществления длина ID ключа равна 8 битам и длина ID алгоритма равна 3 битам, хотя длина идентификаторов шифрования может изменяться. Более конкретно, согласно способу 600 передающее устройство формирует (602) биты четности исправления ошибок по одному либо более из идентификаторов шифрования и соединяет (604) биты четности исправления ошибок с идентификаторами шифрования. Как проиллюстрировано на фиг.7, 21 бит 706 четности FEC формируется по ID 702 ключа и ID 704 алгоритма и затем добавляется к ID ключа и алгоритма. Биты четности исправления ошибок могут формироваться, используя любые подходящие методики исправления ошибок, включая любую из вышеупомянутых, чтобы таким образом формировать то же самое число, больше либо меньше битов четности исправления ошибок, либо биты четности исправления ошибок могут быть вычислены только по ID ключа либо ID алгоритма. Более того, в другом варианте осуществления передающее устройство может вычислять биты четности обнаружения ошибок (например, используя CRC, контрольную сумму, простую четность и т.д.) по одному либо более из идентификаторов шифрования до формирования битов четности исправления ошибок либо вместо формирования битов четности исправления ошибок.

В этом иллюстративном варианте осуществления передающее устройство располагает (606) ID 702 ключа, ID 704 алгоритма и конкатенированные биты 706 четности FEC в поле 208-F встроенной сигнализации голосового суперкадра DMR пакета F 204-F, показанного на фиг.2. Как упомянуто выше, расположение параметров шифрования в пакете F является выгодным, так как теперь поле встроенной сигнализации является нулевым. Тем не менее, параметры шифрования могут располагаться в поле встроенной сигнализации любого одного либо более пакетов в голосовом суперкадре DMR. Более того, передающее устройство может располагать параметры шифрования в единственном поле встроенной сигнализации во всем голосовом вызове (содержащий множество голосовых суперкадров DMR) либо периодически располагать параметры шифрования в нескольких полях встроенной сигнализации во время вызова. Тем не менее, для того чтобы наилучшим образом облегчить последний ввод с помощью приемного устройства для голосового вызова после того, как первоначальные заголовки, имеющие параметры шифрования, были переданы, для передающего устройства дополнительно является выгодным располагать параметры шифрования в каждом голосовом суперкадре DMR вызова.

Фиг.8 показывает блок-схему способа 800 для приема параметров шифрования в голосовом суперкадре DMR согласно иллюстративному варианту осуществления. При приеме (802) голосовых передач от передающего устройства приемное устройство обнаруживает, что передачи зашифрованы. Например, в одном варианте осуществления приемное устройство обнаруживает, что секретный бит установлен в заголовке управления линией голосовой связи (LC), который указывает, что приемному устройству необходимо извлечь параметры шифрования для того, чтобы дешифровать голосовые передачи. В дополнение либо альтернативно бит может быть установлен во встроенной сигнализации LC во время голосовой передачи и/или в ограничителе LC в конце голосовой передачи для обозначения приемному устройству извлечь параметры шифрования из голосовых суперкадров DMR. Другие способы обозначения приемного устройства для извлечения параметров шифрования могут быть также реализованы без отклонения от объема идей данного документа.

Соответственно, приемное устройство (804) извлекает, по меньшей мере, один параметр шифрования из поля встроенной сигнализации голосового суперкадра 200 DMR. В этом случае приемное устройство извлекает ID 702 ключа и ID 704 алгоритма из поля встроенной сигнализации пакета F и использует биты 706 FEC для этих идентификаторов шифрования для исправления любых ошибок, если таковые имеются. Приемное устройство также извлекает и обратно перемежает (806) биты из кадров вокодера из голосового суперкадра DMR для получения IV.

Более конкретно, приемное устройство устраняет четыре наименьших значащих бита (четырехбитовые блоки) из каждого из восемнадцати кадров вокодера в голосовых суперкадрах DMR и обратно перемежает четырехбитовые блоки для получения 72-битового модифицированного IV, который включает в себя биты четности FEC. В другом варианте реализации подмножество четырехбитовых блоков может быть устранено из кадров вокодера для получения IV. FEC используется по защищенному от ошибок IV для получения 32-битового IV и четырехбитовой CRC. При проверке 4-битовой CRC приемное устройство выбирает соответствующий ключ, как определено ID ключа, и соответствующий алгоритм, как определено ID алгоритма.

В этом случае алгоритмом является ARC4, который использует ключ, соединенный с IV, чтобы сформировать тот же самый поток ключей, который был сформирован в передающем устройстве. Для того чтобы получить открытую полезную голосовую нагрузку голосового суперкадра DMR, приемное устройство осуществляет операцию исключающего ИЛИ зашифрованной части полезной нагрузки с помощью потока ключей. Способ 800 может осуществляться для каждого голосового суперкадра DMR, либо, если параметры шифрования получены в конкретном голосовом суперкадре DMR, они могут использоваться для дешифрования этого суперкадра DMR.

Для каждого последующего голосового суперкадра DMR приемное устройство может просто обновить IV, используя LFSR предыдущего IV для дешифрования последующего голосового суперкадра DMR.

В вышеупомянутой спецификации описаны определенные варианты осуществления. Тем не менее, обычный специалист в данной области техники примет во внимание, что различные модификации и изменения могут быть выполнены без отступления от объема изобретения, как задано в формуле далее. Следовательно, описание и фигуры должны быть рассмотрены в иллюстративном, а не ограничительном смысле, и все подобные модификации предназначены для того, чтобы быть включенными в объем настоящих идей. Выгоды, преимущества, решения проблем и любой элемент(ы), который может приводить к тому, что появилась или стала более явной любая

выгода, преимущество и решение, не должны истолковываться как критические, обязательные или существенные функции или элементы любого пункта либо всей формулы. Изобретение задано только прилагаемой формулой, включающей в себя любые поправки, сделанные во время нахождения на рассмотрении этой заявки и всех эквивалентов этой формулы, как опубликовано.

Более того, в этом документе родственные термины, например, «первый» и «второй», «верхний» и «нижний» и тому подобное, могут использоваться только для отличия одного объекта либо действия от другого объекта либо действия без необходимого требования либо подразумевания любой фактической подобной связи либо порядка между подобными объектами либо действиями. Термины «заключает в себе», «заключающий в себе», «имеет», «имеющий», «включает», «включающий», «содержит», «содержащий» или любая другая их разновидность предназначены, чтобы охватить неисключительное включение, так чтобы процесс, способ, изделие или устройство, которое заключает в себе, имеет, включает в себя, содержит список элементов, который не включает в себя только эти элементы, но может включать в себя другие элементы, не перечисленные в явном виде или внутренне присущие такому процессу, способу, изделию или устройству. Элемент, за которым продолжается «заключает в себе», «имеет», «включает», содержит», не препятствует без каких-либо ограничений существованию дополнительных идентичных элементов в процессе, способе, изделии либо устройстве, которое заключает в себе, имеет, включает в себя, содержит элемент. Термины в единственном числе заданы как один либо более, пока в данном документе явно не утверждается иное. Термины «главным образом», «по существу», «приблизительно», «около» либо какой-либо иной их вариант определены как близкие, как понимает специалист в данной области техники, и в одном неограничивающем варианте осуществления термин задан находящимся в пределах 10%, в другом варианте осуществления в пределах 5%, в еще одном варианте осуществления в пределах 1% и в еще одном варианте осуществления в пределах 0,5%. Термин «присоединенный», в качестве используемого в материалах настоящей заявки, определен как связанный, хотя не обязательно непосредственно и не обязательно механически. Устройство либо структура, которые «конфигурируются» определенным способом, конфигурируются, по меньшей мере, этим способом, но может также конфигурироваться способами, которые не перечислены.

Будет принято во внимание, что некоторые варианты осуществления могут содержать один либо более типичных либо специализированных процессоров (либо «устройств обработки»), например, микропроцессоры, цифровые сигнальные процессоры, заказные процессоры и программируемые пользователем вентильные матрицы (FPGA) и уникальные сохраненные программные команды (включая как программное обеспечение, так и встроенное программное обеспечение), которые управляют одним либо более процессорами для реализации в сочетании с определенными непроцессорными схемами некоторых, большинства либо всех функций способа и устройства для передачи параметров шифрования, описанных в данном документе. Непроцессорные схемы могут включать в себя, но не ограничены радиоприемником, радиопередатчиком, возбудителями сигналов, схемой синхронизации, схемами источника мощности и устройствами пользовательского ввода. Как таковые эти функции могут интерпретироваться как этапы способа для осуществления передачи параметров шифрования, описанных в данном документе. Альтернативно некоторые или все функции могут быть реализованы конечным автоматом, который не имеет сохраненных программных команд, или в одной или

более специализированных интегральных схемах (ASIC), в которых каждая функция или некоторые комбинации определенных функций реализованы как заказные логические схемы. Естественно, может использоваться комбинация двух подходов. Как конечный автомат, так и ASIC рассматриваются в данном документе как «устройство обработки» для целей вышеизложенного рассмотрения и языка формулы изобретения.

Более того, вариант осуществления может быть реализован как машиночитаемый элемент запоминающего устройства либо носителя, имеющего сохраненный в нем машиночитаемый код для программирования компьютера (например, содержащий устройство обработки) для осуществления способа, как описано и заявлено в данном документе. Примеры подобных машиночитаемых элементов запоминающего устройства включают в себя, но не ограничены жестким диском, компакт-диском (CD-ROM), оптическим запоминающим устройством, магнитным запоминающим устройством, постоянным запоминающим устройством (ROM), программируемым ПЗУ (PROM), стираемым программируемым ПЗУ (EPROM), электрически стираемым программируемым ПЗУ (EEPROM) и флэш-памятью. Дополнительно предполагается, что специалист в данной области техники, несмотря на возможные значительные усилия и многочисленные варианты проектов, причиной которых является, например, доступное время, существующая технология и экономические соображения, направляемые идеями и принципами, раскрытыми в данном документе, легко будет способен сформировать подобные программные команды и программы и интегральные схемы с минимальным экспериментированием.

Реферат предоставлен, чтобы позволить читателю быстро определить суть технического изобретения. Он представляется на рассмотрение с пониманием того, что он не будет использоваться для интерпретирования или ограничения объема или смысла формулы изобретения. Кроме того, в вышеизложенном подробном описании можно увидеть, что различные признаки сгруппированы вместе в различных вариантах осуществления с целью рационализации изобретения. Этот способ раскрытия не интерпретируется, как отражающий намерение, что заявленные варианты осуществления требуют больше признаков, чем явно перечислено в каждом пункте формулы. Скорее, как отражает последующая формула изобретения, предмет изобретения заключается в менее чем во всех признаках единственно раскрытого варианта осуществления. Таким образом, последующая формула изобретения включена в подробное описание с каждым пунктом формулы, имеющим самостоятельную силу, как отдельно заявленным предметом изобретения.

Формула изобретения

1. Способ для передачи параметров шифрования в голосовом суперкадре DMR ETSI (цифровая мобильная радиосвязь) (Европейский институт стандартизации в области электросвязи), способ содержит этапы, на которых:

идентифицируют выбранное число битов из множества кадров вокодера голосового суперкадра DMR;

замещают по меньшей мере некоторые из идентифицированных битов соответствующим битом первого параметра шифрования;

располагают по меньшей мере второй параметр шифрования в поле встроенной сигнализации голосового суперкадра DMR; и

передают голосовой суперкадр DMR, который включает в себя параметры шифрования.

2. Способ по п.1, в котором первый параметр шифрования содержит вектор инициализации (IV).

3. Способ по п.2, в котором замещение по меньшей мере некоторых из идентифицированных битов соответствующим битом IV содержит этапы, на которых:

формируют модифицированный IV с помощью объединения IV с по меньшей мере одним из битов четности обнаружения ошибок либо битов четности прямого исправления ошибок; и

замещают каждый из идентифицированных битов соответствующим битом модифицированного IV.

4. Способ по п.3, в котором формирование модифицированного IV содержит этапы, на которых:

вычисляют код проверки циклическим избыточным кодом (CRC) для IV;

конкатенируют CRC с IV для формирования конкатенированного IV;

добавляют биты четности прямого исправления ошибок (FEC) к конкатенированному IV для формирования модифицированного IV.

5. Способ по п.2, в котором замещение каждого из идентифицированных битов содержит этап, на котором перемежают биты IV в позициях идентифицированных битов.

6. Способ по п.1, в котором расположение по меньшей мере второго параметра шифрования в поле встроенной сигнализации содержит размещение по меньшей мере одного идентификатора шифрования в поле встроенной сигнализации пакета F голосового суперкадра DMR.

7. Способ по п.1, в котором по меньшей мере второй параметр шифрования содержит по меньшей мере одно из: идентификатора ключа шифрования, идентификатора алгоритма шифрования, идентификатора ключа шифрования, объединенного с битами контроля ошибок, идентификатора алгоритма шифрования, объединенного с битами контроля ошибок, либо идентификатора ключа шифрования и идентификатора алгоритма шифрования, объединенных с битами контроля ошибок.

8. Способ для приема параметров шифрования в голосовом суперкадре DMR ETSI (цифровая мобильная радиосвязь) (Европейский институт стандартизации в области электросвязи), способ содержит этапы, на которых:

принимают голосовой суперкадр DMR;

извлекают первый параметр шифрования из поля встроенной сигнализации принятого голосового суперкадра DMR;

извлекают выбранное число битов из множества кадров вокодера голосового суперкадра DMR; и

компонуют извлеченные биты для получения второго параметра шифрования.

9. Способ по п.8, в котором первый параметр шифрования извлекается из поля встроенной сигнализации пакета F голосового суперкадра DMR.

10. Способ по п.8, в котором по меньшей мере первый параметр шифрования содержит по меньшей мере одно из: идентификатора ключа шифрования, идентификатора алгоритма шифрования, идентификатора ключа шифрования, объединенного с битами контроля ошибок, идентификатора алгоритма шифрования, объединенного с битами контроля ошибок, либо идентификатора ключа шифрования и идентификатора алгоритма шифрования, объединенных с битами контроля ошибок.

11. Способ по п.10, дополнительно содержащий этап, на котором дешифруют принятый суперкадр DMR, используя ключ, выбранный на основе ID ключа, и алгоритм шифрования, выбранный на основе ID алгоритма.

12. Способ по п.1 или 8, в котором выбранное число битов из множества кадров вокодера содержит выбранное число наименьших значащих битов.

13. Способ по п.12, в котором выбранное число наименьших значащих бита содержит четыре наименьших значащих бита, извлеченных из каждого из множества кадров вокодера голосового суперкадра DMR.

14. Способ по п.8, в котором второй параметр шифрования содержит IV и в котором способ дополнительно содержит этап, на котором дешифруют принятый суперкадр DMR, используя IV.

15. Устройство для передачи параметров шифрования в голосовом суперкадре DMR ETSI (цифровая мобильная радиосвязь) (Европейский институт стандартизации в области электросвязи), устройство, содержащее:

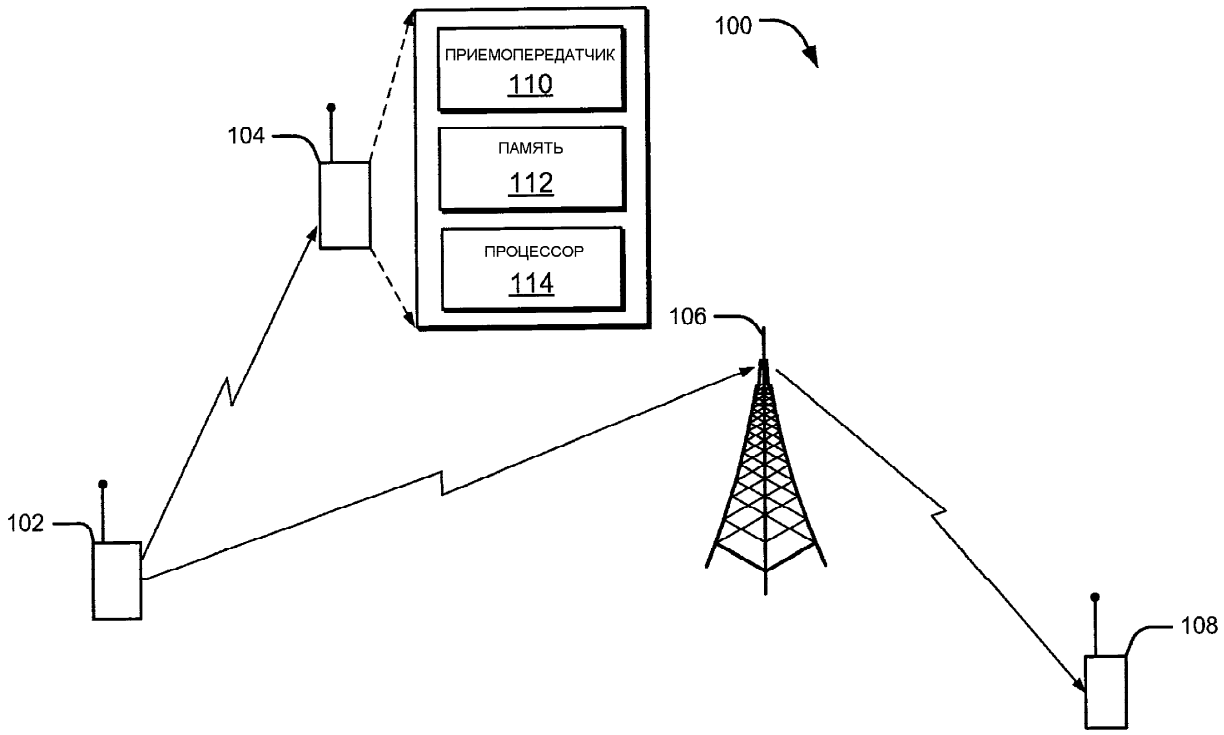
устройство обработки для:

идентификации выбранного числа битов из множества кадров вокодера голосового суперкадра DMR;

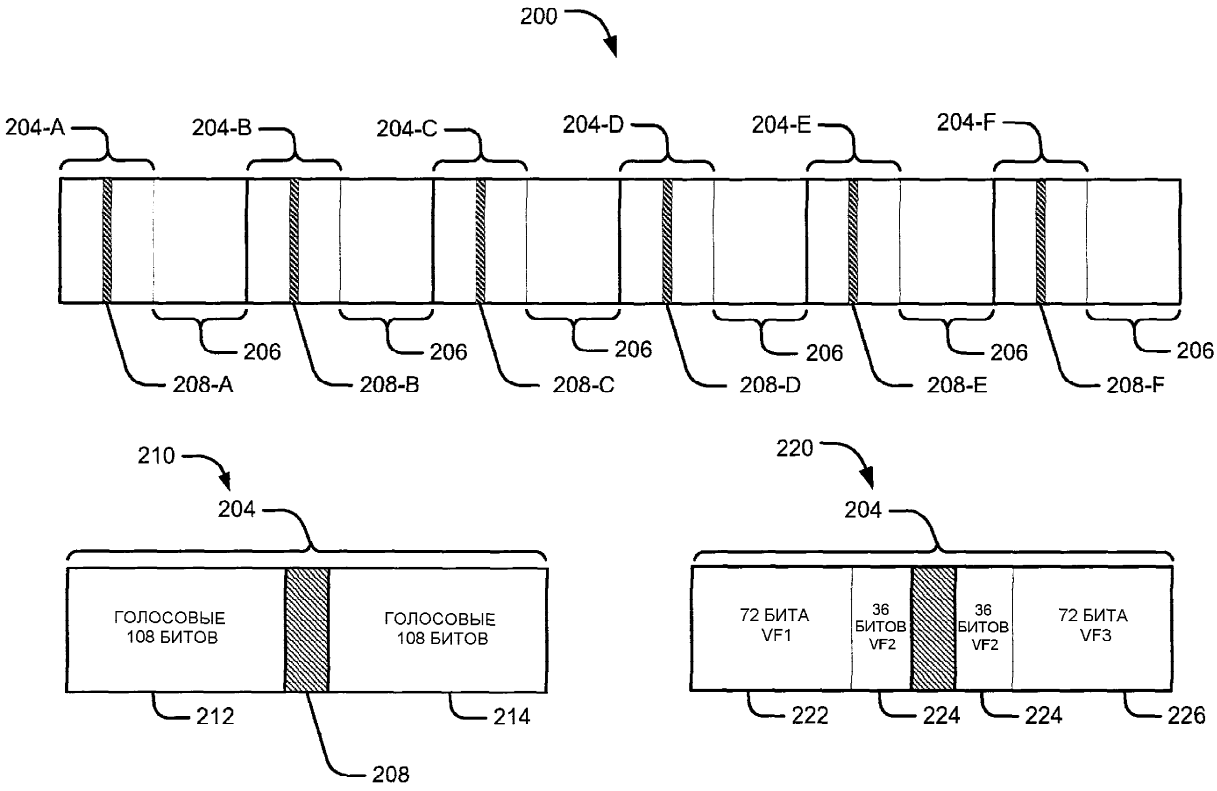
замещения по меньшей мере некоторых из идентифицированных битов соответствующим битом вектора инициализации (IV); и

размещения по меньшей мере одного идентификатора шифрования в поле встроенной сигнализации голосового суперкадра DMR; и

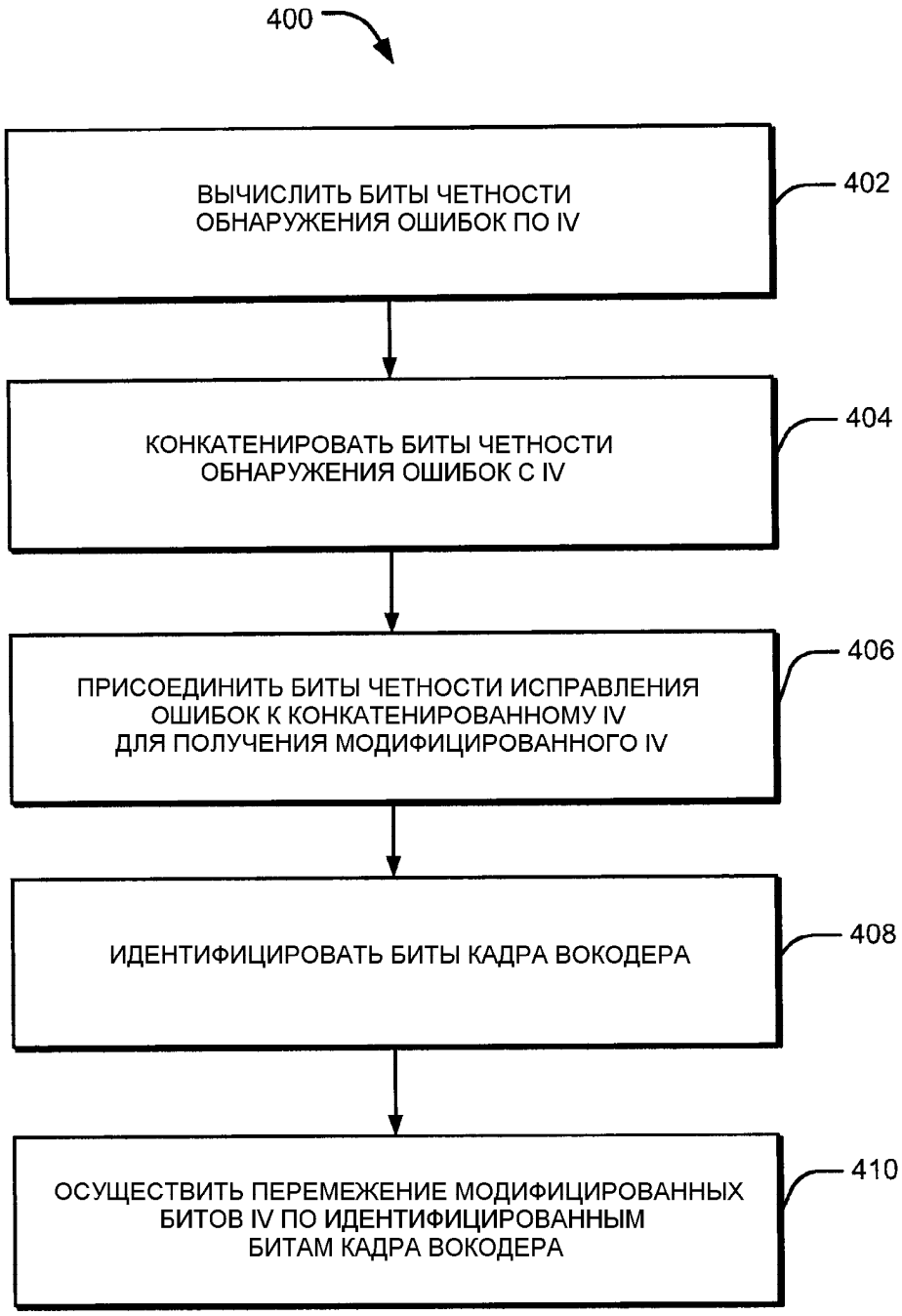
приемопередатчик, присоединенный к устройству обработки, для передачи голосового суперкадра DMR, который включает в себя IV и идентификаторы шифрования.


100
ПРИЕМОПЕРЕДАТЧИК
110
ПАМЯТЬ
112
ПРОЦЕССОР
114
104
106
102
108

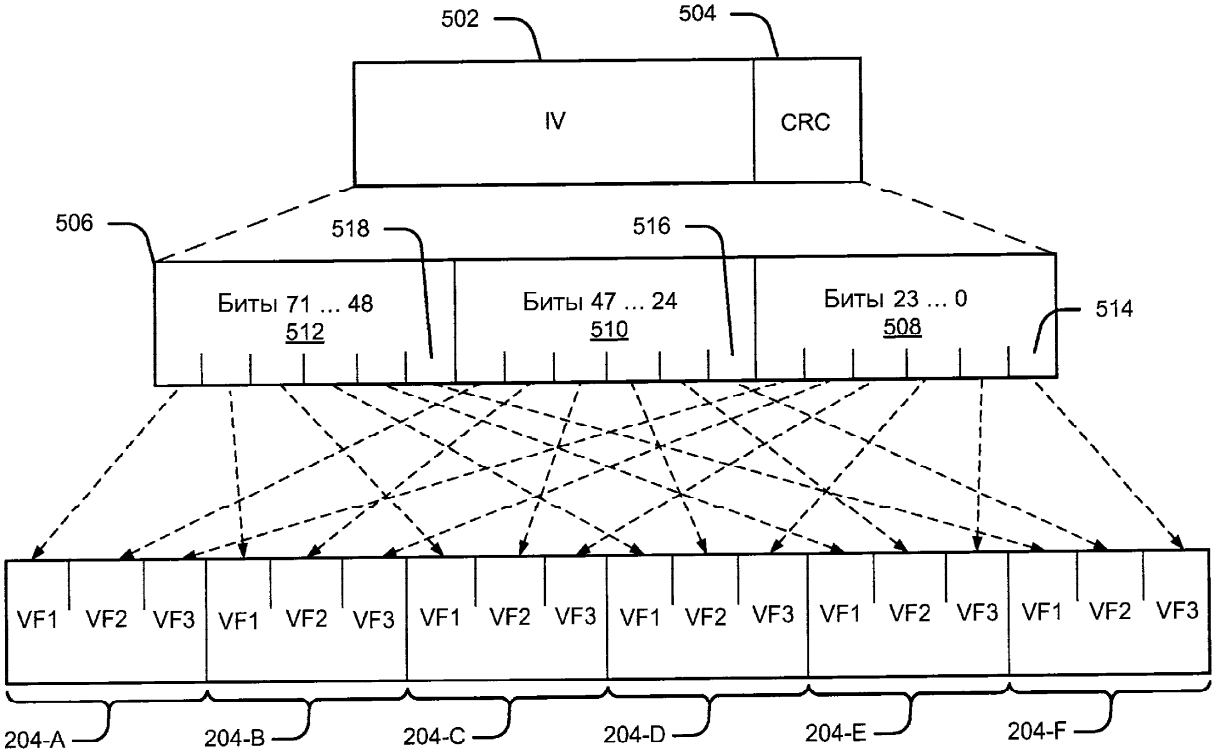
Фиг.1


200
204-A
204-B
204-C
204-D
204-E
204-F
206
208-A
208-B
208-C
208-D
208-E
208-F
210
204
ГОЛОСОВЫЕ
108 БИТОВ
ГОЛОСОВЫЕ
108 БИТОВ
212
214
208
220
204
72 БИТА
VF1
36
БИТОВ
VF2
36
БИТОВ
VF2
72 БИТА
VF3
222
224
224
226

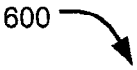
Фиг.2

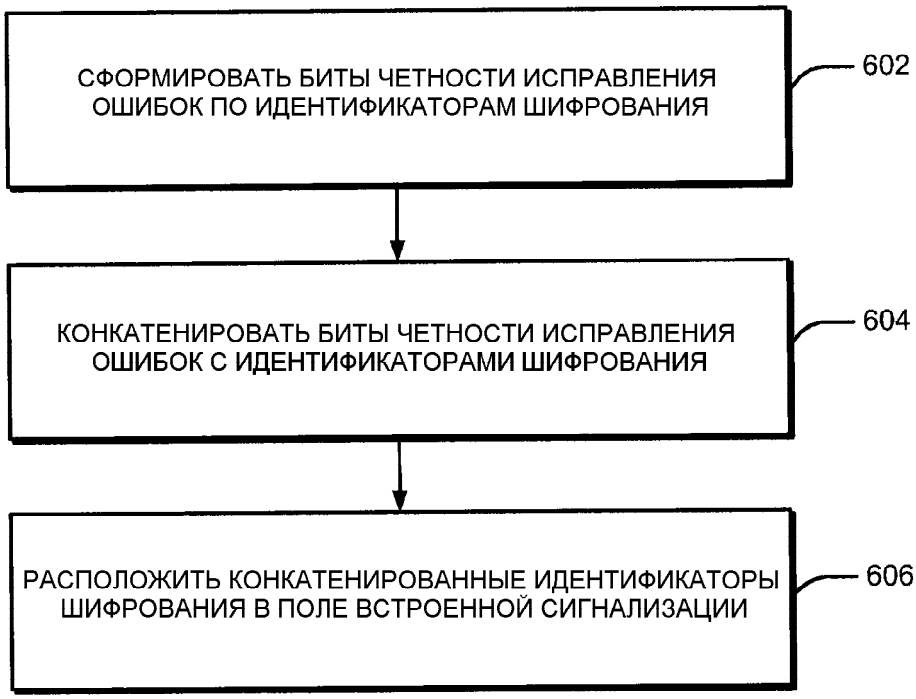

400
ВЫЧИСЛИТЬ БИТЫ ЧЕТНОСТИ ОБНАРУЖЕНИЯ ОШИБОК ПО IV
402
КОНКАТЕНИРОВАТЬ БИТЫ ЧЕТНОСТИ ОБНАРУЖЕНИЯ ОШИБОК С IV
404
ПРИСОЕДИНИТЬ БИТЫ ЧЕТНОСТИ ИСПРАВЛЕНИЯ ОШИБОК К КОНКАТЕНИРОВАННОМУ IV ДЛЯ ПОЛУЧЕНИЯ МОДИФИЦИРОВАННОГО IV
406
ИДЕНТИФИЦИРОВАТЬ БИТЫ КАДРА ВОКОДЕРА
408
ОСУЩЕСТВИТЬ ПЕРЕМЕЖЕНИЕ МОДИФИЦИРОВАННЫХ БИТОВ IV ПО ИДЕНТИФИЦИРОВАННЫМ БИТАМ КАДРА ВОКОДЕРА
410

Фиг.4

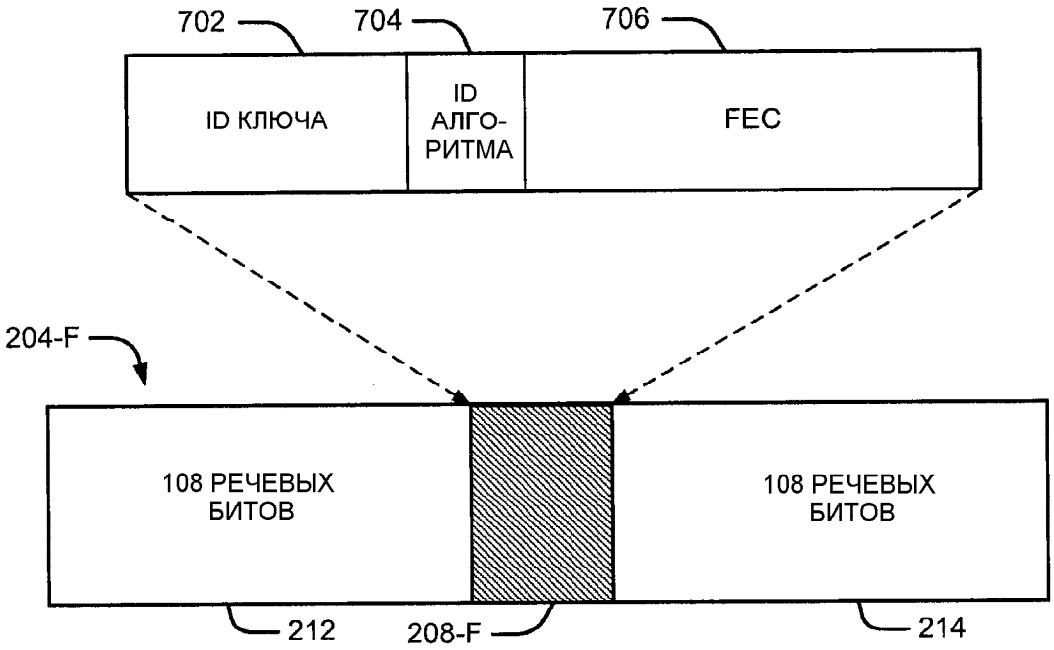

502
504
IV
CRC
506
518
516
Биты 71 ... 48
512
Биты 47 ... 24
510
Биты 23 ... 0
508
514
VF1 VF2 VF3 VF1 VF2 VF3 VF1 VF2 VF3 VF1 VF2 VF3 VF1 VF2 VF3 VF1 VF2 VF3
204-A
204-B
204-C
204-D
204-E
204-F

Фиг.5

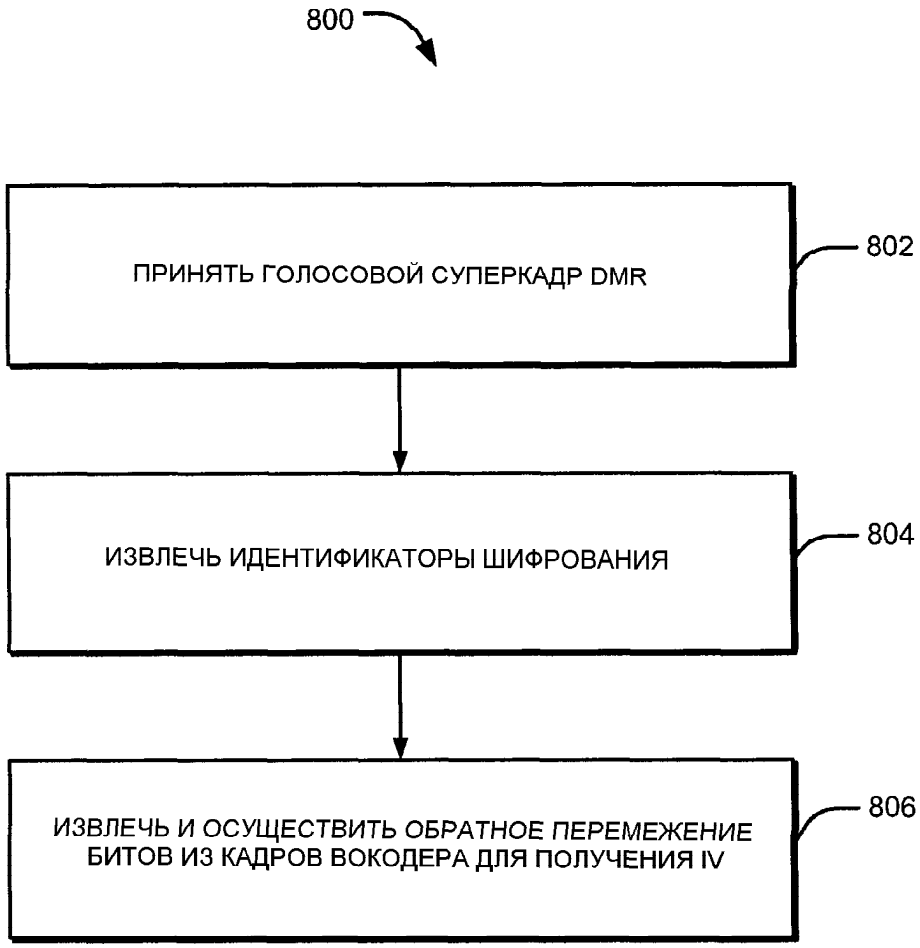

600


СФОРМИРОВАТЬ БИТЫ ЧЕТНОСТИ ИСПРАВЛЕНИЯ ОШИБОК ПО ИДЕНТИФИКАТОРАМ ШИФРОВАНИЯ
602
КОНКАТЕНИРОВАТЬ БИТЫ ЧЕТНОСТИ ИСПРАВЛЕНИЯ ОШИБОК С ИДЕНТИФИКАТОРАМИ ШИФРОВАНИЯ
604
РАСПОЛОЖИТЬ КОНКАТЕНИРОВАННЫЕ ИДЕНТИФИКАТОРЫ ШИФРОВАНИЯ В ПОЛЕ ВСТРОЕННОЙ СИГНАЛИЗАЦИИ
606

Фиг.6


702
704
706
ID КЛЮЧА
ID АЛГО-РИТМА
FEC
204-F
108 РЕЧЕВЫХ БИТОВ
108 РЕЧЕВЫХ БИТОВ
212
208-F
214

Фиг.7


800
ПРИНЯТЬ ГОЛОСОВОЙ СУПЕРКАДР DMR
802
ИЗВЛЕЧЬ ИДЕНТИФИКАТОРЫ ШИФРОВАНИЯ
804
ИЗВЛЕЧЬ И ОСУЩЕСТВИТЬ ОБРАТНОЕ ПЕРЕМЕЖЕНИЕ БИТОВ ИЗ КАДРОВ ВОКОДЕРА ДЛЯ ПОЛУЧЕНИЯ IV
806

Фиг.8