РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 329 613** (13) **C2**

(51) МПК
H04N 7/173 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21), (22) Заявка: **2005100833/09, 21.07.2003**

(24) Дата начала отсчета срока действия патента:
21.07.2003

(30) Конвенционный приоритет:
24.07.2002 CH 2002 1298/02

(43) Дата публикации заявки: **10.07.2005**

(45) Опубликовано: **20.07.2008 Бюл. № 20**

(56) Список документов, цитированных в отчете о поиске: **WO 01/50755 A1, 12.07.2001. RU 2115952 C1, 20.07.1998. RU 2106758 C1, 10.03.1998. RU 2169437 C1, 20.06.2001. WO 00/56068 A1, 21.09.2000.**

(85) Дата перевода заявки PCT на национальную фазу:
24.02.2005

(86) Заявка PCT:
IB 03/003344 (21.07.2003)

(87) Публикация PCT:
WO 2004/010698 (29.01.2004)

Адрес для переписки:
191186, Санкт-Петербург, а/я 230, "АРС-ПАТЕНТ", пат.пов. М.В.Хмаре, рег. № 771

(72) Автор(ы):
НИКОЛЯ Кристоф (CH)

(73) Патентообладатель(и):
НАГРАКАРД С.А. (CH)

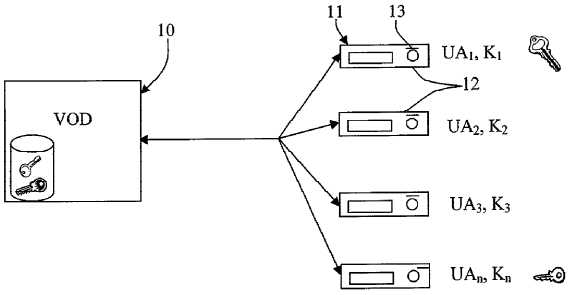
RU 2329613 C2

RU 2329613 C2

(54) СПОСОБ БЕЗОПАСНОЙ ПЕРЕДАЧИ ДАННЫХ ПО СХЕМЕ "ТОЧКА-ТОЧКА" И ЭЛЕКТРОННЫЙ МОДУЛЬ, РЕАЛИЗУЮЩИЙ ЭТОТ СПОСОБ

(57) Реферат:

Изобретение относится к области передачи данных по схеме «точка-точка» и включает в себя способ защиты данных, при использовании которого данные, дешифруемые одним из пользователей, становятся непригодными для других пользователей. Технический результат заключается в повышении уровня защиты при передаче зашифрованных данных. Способ заключается в том, что осуществляют посылку пользовательским устройством (D_1, D_2,..., D_n) в центр (10) управления запроса с заказом на передачу определенного содержания (CT), посылают в центр (10) управления уникальный идентификатор (UA_1, UA_2,..., UA_n), причем этот идентификатор однозначно определяет пользовательское устройство, пославшее запрос, определяют по базе (14) данных, связанной с центром управления, ключ (K_n), соответствующий указанному пользовательскому устройству, пославшему запрос, определяют контрольное слово или слова, связанное (связанные) с содержанием (CT) предназначенным для передачи, дополнительно шифруют указанное предназначенное для передачи содержание (CT) индивидуальным для каждого пользовательского устройства способом, передают указанное зашифрованное содержание в пользовательское устройство, пославшее запрос, передают зашифрованные контрольные слова в пользовательское устройство, пославшее запрос. 4 з.п. ф-лы, 10 ил.



Фиг. 1

RU 2329613 C2

RU 2329613 C2

RUSSIAN FEDERATION

(19) **RU** (11) **2 329 613** (13) **C2**

(51) Int. Cl.
H04N 7/173 (2006.01)

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY,
PATENTS AND TRADEMARKS

(12) ABSTRACT OF INVENTION

(21), (22) Application: **2005100833/09, 21.07.2003**

(24) Effective date for property rights: **21.07.2003**

(30) Priority:
24.07.2002 CH 2002 1298/02

(43) Application published: **10.07.2005**

(45) Date of publication: **20.07.2008 Bull. 20**

(85) Commencement of national phase: **24.02.2005**

(86) PCT application:
IB 03/003344 (21.07.2003)

(87) PCT publication:
WO 2004/010698 (29.01.2004)

Mail address:
191186, Sankt-Peterburg, a/ja 230, "ARS-PATENT", pat.pov. M.V.Khmare, reg. № 771

(72) Inventor(s):
NIKOLJa Kristof (CH)

(73) Proprietor(s):
NAGRAKARD S.A. (CH)

(54) METHOD OF SAFE DATA TRANSFER ON PEER-TO-PEER PRINCIPLE AND ELECTRONIC MODULE TO IMPLEMENT THIS METHOD

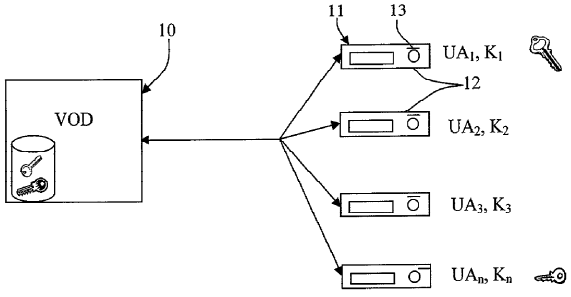
(57) Abstract:

FIELD: information technology.

SUBSTANCE: invention belongs to the field of data transfer on the basis of peer-to-peer principle and includes the data protection method where the data decrypted by one of the users becomes useless for others. The essence of the method is that the request for a certain content (CT) is sent by the user device (D_1, D_2,..., D_n) to the request control centre (10), the unique identifier (UA_1, UA_2,..., UA_n) , which unequivocally determines the user device that has sent the request, is also sent to the request control centre, the key (K_n) relating to the specific user device that has sent the request is obtained from the database (14) connected with the request control centre, the sending content (CT)-related check word(s) are defined; the content to be sent (CT) is additionally encrypted by unique methods for each individual user. The encrypted content is then sent to the user request-sending device that has sent the request, and the encrypted check words are also sent to the user request-sending device.

EFFECT: enhancement of the encrypted data transfer protection level.

5 cl, 10 dwg



Фиг. 1

RU 2329613 C2

RU 2329613 C2

Настоящее изобретение относится к области способов безопасной передачи данных по схеме "точка-точка" между центром управления и одним из множества пользовательских устройств, связанных с указанным центром управления.

Кроме того, настоящее изобретение относится к электронному модулю, позволяющему реализовать этот способ.

Уровень техники

В общем случае передачи данных по схеме "точка-точка", и, в частности, в случае передачи видео по запросу (videos on demand, VOD), файлы данных, содержащие, например, изображения и звук, хранятся в базе данных, называемой "центром управления" или "VOD-сервером". Все эти данные или файлы могут быть заказаны любым пользователем, связанным с данным центром управления. Кроме того, данные являются файлами, которые могут передаваться вещательным способом; в частности это данные, которые могут передаваться по каналам, доступ к которым осуществляется по подписке. Далее по тексту данные, предназначенные для передачи, называются содержанием.

Между центром управления и пользовательскими устройствами могут размещаться промежуточные центры. Эти промежуточные центры выполняют часть операций, связанных с передачей данных и проверкой полномочий, и используются в некоторых существующих системах в качестве ретрансляторов. Далее по тексту термины "центр управления" или "VOD-сервер" включают в себя, помимо прочего, и эти промежуточные центры. Такие центры, в частности, описаны в документе WO 00/11871.

Содержание файлов данных может храниться, как известно специалистам в данной области техники, в явном виде или, что более соответствует современному уровню техники, предварительно зашифрованном виде. Эти файлы содержат, во-первых, видеоданные, т.е., в общем случае изображение и звук, и, во-вторых, служебную информацию. Эта служебная информация представляет собой данные, которые позволяют контролировать использование видеоданных, и, в частности, включают в себя заголовок. Эта информация может быть незашифрованной или частично зашифрованной.

Когда пользователь желает получить содержание какого-либо файла, например просмотреть видеофайл, в центр управления передается соответствующий запрос, после чего центр управления передает пользователю приемного устройства/декодера, во-первых, сам видеофайл в виде потока зашифрованных данных, и, во-вторых, поток контрольных сообщений, позволяющих выполнять дешифрование потока данных. Указанный второй поток называется потоком ECM (Entitlement Control Message, контрольное сообщение полномочий) и содержит регулярно обновляемые "контрольные слова" (control words, cw), используемые для дешифрования передаваемого центром управления зашифрованного содержания. Контрольные слова в потоке ECM, как правило, шифруются с помощью ключа, специфичного для системы передачи информации между центром управления и модулем защиты, соединенным с приемным устройством/декодером. Фактически связанные с защитой операции выполняются в модуле защиты, который, как правило, представляет собой карту с микропроцессором, которая считается защищенной. Этот модуль может быть как сменным, так и интегрированным в приемное устройство.

В процессе дешифрования контрольного сообщения (ECM), в модуле защиты выполняется проверка наличия полномочий на доступ к данному содержанию. Эти полномочия могут предоставляться сообщениями авторизации (EMM = Entitlement Management Message, сообщение управления полномочиями), посредством которых осуществляется загрузка этих полномочий в модуль защиты. Возможны и другие способы, например передача конкретных ключей дешифрования.

Оборудование передачи цифровых данных с условным доступом схематично разделяется на три модуля. Первый модуль выполняет кодирование цифровых данных с помощью контрольных слов (cw) и передачу этих данных.

Второй модуль выполняет создание контрольных сообщений (ECM), содержащих контрольные слова (cw), а также условия доступа, и их передачу по запросам пользователей.

Третий модуль выполняет создание и передачу сообщений авторизации (EMM), которые предназначены для формирования полномочий на прием в модулях защиты, соединенных с приемными устройствами.

Первые два модуля, как правило, независимы от приемных устройств, в то время как третий модуль имеет дело со всем множеством пользователей и передает информацию одному пользователю, некоторой совокупности пользователей или всем пользователям.

Как упомянуто выше, в настоящее время в большинстве конкретных реализаций контрольные слова изменяются регулярно через определенные интервалы времени и являются одинаковыми для всех пользователей. Пользователь таким образом может получать контрольные слова "традиционным" способом, путем подписки на соответствующую услугу или оплаты полномочий, связанных с передачей заказанной информации. Эти контрольные слова впоследствии могут быть переданы другим пользователям, не имеющим необходимых полномочий. В случае распространения фальсифицированных модулей защиты, в которых не выполняется проверка полномочий или ответ на эту проверку всегда дает положительный результат, такой модуль защиты, следовательно, возвращает контрольные слова в декодер в незашифрованном виде. В этом случае возможно, что другие люди воспользуются полученными таким образом контрольными словами, не имея на то соответствующих полномочий, так как эти контрольные слова идентичны для всех пользователей. Это особенно важно, учитывая то, что передача по схеме "точка-точка" редко представляет собой фактическую передачу между двумя точками, а именно центром управления и каждым приемным устройством/декодером, связанным с этим центром управления. Очень часто имеет место передача по схеме "точка-точка" от центра управления к "узлу связи", обслуживающему, например, здание или квартал жилого массива. Начиная с этой точки разветвления связи все приемные устройства/декодеры связаны между собой по "внутренней" сети. Поэтому возможно, что в определенных условиях все участники этой внутренней сети получат возможность использования полномочий одного из участников.

Электронные модули, используемые в настоящее время в приемных устройствах/декодерах, в основном включают в себя вычислительный блок, запоминающее устройство, дешифратор и декомпрессор звука и изображения. Эти модули способны выполнять дешифрование только однократно зашифрованных данных. Выходной сигнал такого модуля представляет собой аналоговый сигнал, который может использоваться для отображения информации из файла данных. В дополнение к этому модулю приемное устройство/декодер содержит приемный блок, предназначенный для выбора и приема сигнала по кабельному, спутниковому или наземному каналу, а также улучшения его качества.

Такой модуль функционирует согласно стандарту, связанному с нормами стандартного цифрового телевидения (Digital Video Broadcasting, DVB) или нормами других операторов (например, DirectTV), и имеет фиксированный набор операций, которые он может выполнять. Этот модуль не способен выполнять некоторые операции, которые могут оказаться необходимыми для используемых способов передачи данных.

Раскрытие изобретения

Задача, на решение которой направлено настоящее изобретение, состоит в устранении недостатков способов, относящихся к предшествующему уровню техники, путем реализации способов передачи зашифрованных данных, при использовании которых данные, дешифруемые одним из пользователей, непригодны для использования другим пользователем.

В соответствии с изобретением решение поставленной задачи достигается путем применения способа безопасной передачи данных по схеме "точка-точка" между центром управления и одним из множества пользовательских устройств, связанных с указанным центром управления, причем указанные данные включают в себя содержание, зашифрованное с помощью по меньшей мере одного контрольного слова, а каждое пользовательское устройство включает в себя по меньшей мере один декодер/приемное

устройство, снабженный по меньшей мере одним ключом шифрования, индивидуальным для каждого пользовательского устройства, отличающегося тем, что он включает в себя следующие шаги:

пользовательское устройство посылает в центр управления запрос с заказом на передачу определенного содержания;

в центр управления посылается уникальный идентификатор, причем этот идентификатор однозначно определяет пользовательское устройство, пославшее запрос;

по базе данных, связанной с центром управления, определяется ключ, соответствующий указанному пользовательскому устройству, пославшему запрос;

определяется контрольное слово или слова, связанное (связанные) с содержанием, предназначенным для передачи;

указанные контрольные слова шифруются с помощью указанного ключа, соответствующего указанному пользовательскому устройству, пославшему запрос, с целью получения зашифрованных контрольных слов;

зашифрованные контрольные слова передаются в пользовательское устройство, пославшее запрос;

указанное зашифрованное содержание передается в пользовательское устройство, пославшее запрос.

Указанная задача также решается путем применения способа безопасной передачи данных по схеме "точка-точка" между центром управления и одним из множества пользовательских устройств, связанных с указанным центром управления, причем указанные данные включают в себя содержание, зашифрованное с помощью по меньшей мере одного контрольного слова, а каждое пользовательское устройство содержит по меньшей мере один декодер/приемное устройство, снабженное по меньшей мере одним ключом шифрования, индивидуальным для каждого пользовательского устройства, отличающегося тем, что он включает в себя следующие шаги:

пользовательское устройство посылает в центр управления запрос с заказом на передачу определенного содержания;

в центр управления посылается уникальный идентификатор, причем этот идентификатор однозначно определяет пользовательское устройство, пославшее запрос;

по базе данных, связанной с центром управления, определяется ключ, соответствующий указанному пользовательскому устройству, пославшему запрос;

определяется контрольное слово или слова, связанное (связанные) с содержанием, предназначенным для передачи;

данные, предназначенные для передачи, шифруются индивидуальным способом для каждого пользовательского устройства;

указанное зашифрованное содержание передается в указанное пользовательское устройство, пославшее запрос;

зашифрованные контрольные слова передаются в пользовательское устройство, пославшее запрос.

Кроме того, в настоящем изобретении описывается способ устранения недостатков электронных модулей, относящихся к предшествующему уровню техники, путем изготовления модуля, имеющего возможность дешифрования потоков данных, индивидуальных для пользовательского устройства.

Эта задача решается путем применения электронного модуля, включающего в себя вычислительный блок, запоминающее устройство, дешифратор, декомпрессор звука и изображения и блок дешифрования, использующий ключ, индивидуальный для каждого пользовательского устройства.

Перечень чертежей

Другие свойства и достоинства настоящего изобретения станут ясны из нижеследующего описания, содержащего ссылки на прилагаемые чертежи, которые иллюстрируют различные варианты осуществления изобретения, не вносящие каких-либо ограничений. На чертежах:

на фиг.1 представлен общий вид устройства, реализующего способ в соответствии с изобретением;

на фиг.2 показан первый вариант осуществления способа в соответствии с изобретением;

на фиг.3 показан второй вариант осуществления способа в соответствии с изобретением;

на фиг.4 показан вариант осуществления способа, показанного на фиг.3;

на фиг.5 представлена комбинация вариантов осуществления способа в соответствии с фиг.2 и фиг.3;

на фиг.6 представлена комбинация вариантов осуществления способа в соответствии с фиг.2 и фиг.4;

на фиг.7 показан конкретный вариант осуществления способа в соответствии с настоящим изобретением;

на фиг.8 представлен электронный модуль в соответствии с настоящим изобретением;

на фиг.9 приведена подробная иллюстрация первого варианта осуществления части способа в соответствии с настоящим изобретением;

на фиг.10 приведена подробная иллюстрация первого варианта осуществления части способа в соответствии с изобретением аналогично фиг.9.

Осуществление изобретения

Описание изобретения предполагает, что между сервером цифровых файлов, используемым для предоставления видео по запросу, и устройством, помещенным в доме пользователя и называемым пользовательским устройством, установлена связь по схеме "точка-точка". Цифровой файл может представлять собой видеофайл, который содержит, как правило, изображение и звук, и может содержать другую информацию, в частности служебную информацию, предоставляющую доступ к использованию данных.

На фиг.1 представлен видеосервер или центр управления передачей видео по запросу, в котором находятся файлы, соответствующие различным программам, например фильмам или спортивным событиям, причем эти файлы могут быть заказаны пользователями. На фиг.1 также показано несколько пользовательских устройств 11, каждое из которых представляет собой приемное устройство/декодер 12, возможно, связанный с модулем 13 защиты, при этом каждое из устройств располагается в доме пользователя. Как схематично показано на фиг.1, каждое пользовательское устройство имеет уникальный идентификационный номер (UA_1, UA_2,...,UA_n) и ключ (K_1, K_2,...,K_n), также уникальный и индивидуальный для каждого устройства. Этот ключ может быть так называемым симметричным ключом или одним из ключей асимметричной криптографической пары. Далее по тексту термин "ключ" используется для описания обоих случаев без каких-либо различий, за исключением явного указания того, о каком виде ключа идет речь. Модуль13 защиты может представлять собой, например, карту с микропроцессором, помещаемую в приемное устройство/декодер, или быть интегрированным в указанное устройство/декодер. С другой стороны, модуль защиты может и отсутствовать в устройстве. Если предполагается использование модуля защиты, он предпочтительно должен содержать ключ, который позволяет осуществлять взаимное согласование модуля защиты и приемного устройства/декодера 12. Ключ (K_1, K_2,...,K_n), размещаемый в пользовательском устройстве, может вводиться в зависимости от ситуации в приемное устройство или в модуль защиты. Кроме того, ключ может быть размещен в обоих этих компонентах. Если местонахождение ключа не указано, это означает, что оно очевидно для специалиста в данной области техники или местонахождение ключа не имеет значения.

Аналогичным образом уникальный идентификационный номер может быть связан с приемным устройством, с модулем защиты или с обоими этими элементами. При этом накладывается условие уникальности, которое требует обеспечения однозначной идентификации пользовательского устройства среди устройств, связанных с центром управления.

На фиг.2 показан вариант осуществления способа в соответствии с изобретением, в котором видеосервер 10 передает цифровой файл в одно из пользовательских устройств 12, изображенных на фиг.1.

Способ в соответствии с описанием со ссылками на фиг.1 и 2 реализуется следующим образом.

Пользователь, обладающий устройством n, имеющим уникальный идентификационный номер UA_n, и желающий просмотреть содержание цифрового файла, посылает запрос в центр 10 управления или на VOD-сервер. Этот запрос содержит, в частности, уникальный идентификационный номер UAn, который позволяет VOD-серверу опознать устройство, пославшее запрос.

VOD-сервер содержит базу 14 данных, данные в которой представляют собой идентификационные номера (UA_1, UA_2...UA_n), причем эти номера являются уникальными для каждого устройства, подключенного к серверу, а также ключи (K_1, K_2...K_n), связанные с этими устройствами. Ключ может представлять собой симметричный ключ, и, следовательно, быть идентичным в устройстве и в базе данных VOD-сервера. Он может также быть так называемым асимметричным открытым ключом, состоящим в паре асимметричных ключей. Второй ключ пары, а именно ключ, называемый секретным, хранится в пользовательском устройстве. Этот ключ может постоянно храниться, например, в электронном модуле или микропроцессоре декодера/приемного устройства. Симметричный ключ или пара асимметричных ключей является уникальным (уникальной) и индивидуальным (индивидуальной) для каждого приемного устройства.

Вариант с использованием персонализированных контрольных слов

Как правило, содержание (content, CT) цифрового файла подвергается шифрованию с помощью контрольных слов (cw), причем это шифрование выполняется перед сохранением содержания в VOD-сервере или в реальном времени во время его передачи. Зашифрованный файл передается в приемное устройство, в котором он может сохраняться в запоминающем устройстве 15 большой емкости или дешифроваться для просмотра пользователем.

Для дешифрования содержания необходимо наличие контрольных слов (cw). Вначале эти слова шифруются с помощью ключа K_n, содержащегося в базе данных и индивидуального для каждого пользовательского устройства. Этот ключ является либо симметричным ключом либо открытым ключом из пары асимметричных ключей. В результате создаются зашифрованные контрольные слова $cw'=K_n$ (cw), которые являются индивидуальными для каждого пользовательского устройства. Эти зашифрованные контрольные слова передаются обычным образом, например после их шифрования с помощью ключа шифрования, известного как "системный ключ" (system key, SK), который идентичен для всех пользовательских устройств, связанных с центром управления. Посредством указанного кодирования с помощью системного ключа создается файл контрольных сообщений, который передается в виде потока ECM в пользовательское устройство n, запросившее видеофайл. Поскольку контрольные слова шифруются с помощью ключа шифрования K_n, который является уникальным и индивидуальным для каждого пользовательского устройства, они также являются уникальными и индивидуальными для каждого устройства.

Пользовательское устройство n, для которого предназначен этот поток, содержит либо симметричный ключ либо секретный асимметричный ключ, соответствующий открытому ключу, использованному для шифрования контрольных слов. Это позволяет устройству выполнять дешифрование контрольных слов (cw') путем обработки этих контрольных слов (cw') с помощью ключа K_n и получать их в незашифрованном виде.

Таким образом, зашифрованный видеопоток, сохраненный в приемном устройстве, может быть дешифрован с помощью контрольных слов, которые имеются в незашифрованном виде. Следует отметить, что сохранение видеопотока может быть выполнено и ранее, и между временем сохранения и временем просмотра программы может пройти любой период времени. С другой стороны, можно использовать информацию

в видеофайле и контрольные слова без сохранения видеопотока путем дешифрования его в реальном времени.

Поскольку контрольные слова (cw) шифруются с помощью индивидуального для данного приемного устройства ключа K_n, факт получения информации, содержащейся в потоке ECM, не позволяет получить доступ к полезной информации целой группе пользователей. Поэтому фальсифицированная карта, в которой все доступные полномочия обозначаются как полученные, не дает возможности просматривать данные, поступающие от другого пользователя. Индивидуальный ключ может находиться в модуле защиты или в приемном устройстве.

В этом варианте осуществления данные могут храниться в центре 10 управления в незашифрованном или зашифрованном виде, при этом на практике часто предпочитается второй способ. Это не влечет за собой никаких изменений в описанном способе. Единственное условие заключается в наличии достаточной вычислительной мощности, если шифрование данных выполняется в реальном времени.

Вариант с использованием содержания, персонализируемого с помощью контрольных слов

Второй вариант осуществления, представленный на фиг.3, особенно подходит для применения в случае, если приемные устройства 13 имеют запоминающие устройства с емкостью, достаточной для сохранения, по меньшей мере, одного целого видеофайла. В этом варианте осуществления контрольные слова (cw) вначале шифруются с помощью ключа K_n пользовательского устройства n. Этот ключ, который должен быть симметричным ключом, хранится в базе 14 данных VOD-сервера. В результате создаются зашифрованные контрольные слова $cw'=K_n$ (cw). Затем содержание видеофайла шифруется с помощью зашифрованных контрольных слов cw'. Это содержание может быть сохранено в центре 10 управления, что, однако, не является предпочтительным решением. Чаще всего оно передается напрямую в приемное устройство n, где оно должно сохраняться в запоминающем устройстве 15 большой емкости или отображаться в реальном времени.

Если ключ K_n, с помощью которого выполняется шифрование контрольных слов (cw), индивидуален для каждого пользовательского устройства, зашифрованное содержание также будет индивидуальным для каждого приемного устройства. Таким образом, предпочтительно сохранять зашифрованное содержание не в VOD-сервере, который в этом случае сможет использовать его для обслуживания только одного приемного устройства, а в запоминающем устройстве приемного устройства.

Одновременно выполняется традиционное шифрование контрольных слов (cw), например, с помощью системного ключа (SK), после чего создается файл ECM, который передается в соответствующее приемное устройство в виде потока.

Если приемное устройство должно выполнить дешифрование сохраненного в нем содержания, прежде всего оно должно выполнить традиционное дешифрование контрольных слов (cw), которые были переданы посредством потока ECM. Для этого устройство применяет операцию, обратную операции шифрования, с помощью системного ключа (SK).

Дешифрование указанного содержания выполняется следующим образом: контрольные слова (cw) дешифруются так, как описано выше. Затем они шифруются с помощью симметричного ключа K_n, который был использован VOD-сервером для шифрования контрольных слов. В результате создаются зашифрованные контрольные слова $cw'=K_n$ (cw). Далее выполняется обработка зашифрованного содержания с помощью зашифрованных контрольных слов cw', результатом которой является получение содержания (CT) в незашифрованном виде.

В этом варианте осуществления важно то, что ключ K_n является симметричным. Фактически шифрование видеофайла (CT) выполняется с помощью уже зашифрованных контрольных слов. Необходимо, чтобы зашифрованные контрольные слова в центре управления и зашифрованные контрольные слова в пользовательском устройстве полностью совпадали, иначе дешифрование файла данных будет невозможным.

Как и в предыдущем варианте осуществления, данные, передаваемые от VOD-сервера 10 в пользовательские устройства 12, индивидуальны для каждого устройства. Следовательно, абоненты, не приобретавшие полномочия, связанные с передаваемым содержанием, не могут использовать данные, которые абонент получает "стандартным" путем, на других устройствах. Это позволяет осуществлять эффективное взаимное согласование VOD-сервера и каждого пользовательского устройства с тем, чтобы содержание, предназначенное для данного пользовательского устройства, могло использоваться исключительно этим устройством и никаким другим.

Вариант с использованием содержания, персонализируемого с помощью индивидуального ключа

В варианте осуществления, показанном на фиг.4, содержание (CT) хранится в центре 10 управления в предварительно зашифрованном виде. В этом случае содержание (CT) в незашифрованном виде заранее шифруется с помощью набора контрольных слов (cw). Это зашифрованное содержание обозначено на рисунке как cw(CT). Оно хранится в виде результата этой операции шифрования. В тот момент, когда содержание необходимо передать, предварительно зашифрованное содержание вначале шифруется с помощью индивидуального ключа K_n пользовательского устройства 12, запросившего передачу файла. Содержание обозначено на чертежах как имеющее форму K_n (cw (CT)). Затем оно передается в этой форме в указанное пользовательское устройство. В этом случае реализуется преимущество, состоящее в том, что отсутствует необходимость хранения содержания в центре управления в незашифрованном виде, что на практике не приветствуется владельцами носителей.

Одновременно выполняется традиционное шифрование контрольных слов (cw) и их передача в приемное устройство в потоке ECM.

Для дешифрования содержания, принимаемого пользовательским устройством, в показанном на фиг.4 варианте осуществления необходимо, прежде всего, выполнять традиционное дешифрование контрольных слов, поступающих в потоке ECM. Далее должно выполняться дешифрование содержания K_n (cw (CT)), принимаемого от центра 10 управления, с помощью ключа K_n. Результатом выполнения этих операций является содержание в том виде, в котором оно хранится в центре управления, т.е. предварительно зашифрованное содержание cw (CT). На этом шаге можно применить к этим данным дешифрованные контрольные слова (cw), извлекаемые из потока ECM. Результатом этой операции является получение содержания (CT) в незашифрованном виде.

Вариант с использованием персонализированных контрольных слов аналогично варианту, показанному на фиг.2 и персонализированного содержания аналогично варианту, показанному на фиг.3

На фиг.5 показан вариант осуществления, в котором контрольные слова (cw) персонализируются способом, аналогичным способу, описанному со ссылками на фиг.2, а содержание персонализируется способом аналогичным способу, описанному со ссылками на фиг.3. Вначале выполняется шифрование контрольных слов с помощью первого ключа K'_n, индивидуального для пользовательского устройства. Этот ключ может быть симметричным или асимметричным. Результатом этой операции являются зашифрованные контрольные слова $cw^*=K'_n$ (cw). Затем они шифруются традиционным способом с помощью системного ключа (SK) для передачи в потоке ECM в соответствующее пользовательское устройство. Применение симметричного ключа или второго ключа криптографической пары в случае использования асимметричного ключа K'_n, позволяет выполнять дешифрование контрольных слов cw^* и получать эти слова в незашифрованном виде.

Параллельно с описанным выше процессом выполняется шифрование контрольных слов с помощью ключа K_n (обязательно симметричного), который является индивидуальным для пользовательского устройства и извлекается из базы 14 данных,

связанной с центром управления. Результатом этой операции являются зашифрованные контрольные слова $cw'=K_n(cw)$. Они далее используются для шифрования содержания, предназначенного для передачи, аналогично варианту осуществления, показанному на фиг.3. Затем это содержание передается в соответствующее пользовательское устройство 11. Дешифрование содержания выполняется способом, описанным со ссылками на фиг.3. Более конкретно контрольные слова cw^* дешифруются с помощью ключа K'_n. Затем они вновь шифруются с помощью ключа K_n, что позволяет получить зашифрованные контрольные слова cw'. Они используются для обработки зашифрованного содержания cw'(CT), принимаемого от центра управления, с целью получения содержания CT в незашифрованном виде.

Следует отметить, что в этом варианте осуществления используется принцип хранения предварительно зашифрованной информации, аналогичный принципу, описанному со ссылками на фиг.4. Таким образом, во всех случаях возможно сохранение предварительно зашифрованного содержания в центре управления с применением персонализации потока ECM, потока данных или обоих потоков.

Вариант с использованием персонализированных контрольных слов аналогично варианту, показанному на фиг.2, и персонализированного содержания аналогично варианту, показанному на фиг.4

На фиг.6 показан вариант осуществления способа, который также предусматривает персонализацию контрольных слов cw и потока данных CT. Контрольные слова персонализируются способом, показанным на фиг.5. Они шифруются с помощью первого ключа K'_n, индивидуального для соответствующего пользовательского устройства, и затем вновь шифруются традиционным способом с помощью системного ключа SK для передачи в потоке ECM в соответствующее пользовательское устройство.

Содержание персонализируется способом, аналогичным способу в варианте осуществления, показанном на фиг.4. Содержание (CT) в незашифрованном виде вначале шифруется с помощью контрольных слов cw. Перед передачей предварительно зашифрованное содержание шифруется с помощью индивидуального ключа K_n пользовательского устройства, запросившего передачу содержания. Затем содержание передается в соответствующее пользовательское устройство.

Для дешифрования содержания, принимаемого пользовательским устройством, вначале необходимо выполнить дешифрование контрольных слов, полученных в составе потока ECM, с помощью системного ключа SK и индивидуального ключа K'_n.

Затем необходимо выполнить дешифрование содержания, принимаемого от центра управления, с помощью ключа K_n. Результатом выполнения этих операций является содержание в том виде, в котором оно хранится в центре управления, т.е. предварительно зашифрованное содержание cw (CT). На этом шаге можно применить к этим данным дешифрованные контрольные слова (cw), извлекаемые из потока ECM. Результатом этой операции является получение содержания (CT) в незашифрованном виде.

Оба описанных выше варианта осуществления обеспечивают повышенную защиту по сравнению с предыдущими вариантами осуществления и вариантами осуществления, относящимися к предшествующему уровню техники, поскольку оба потока, передаваемые между центром 10 управления и соответствующим пользовательским устройством 11, являются индивидуальными для данного устройства. Это означает, что даже в том случае, если не имеющее необходимых полномочий лицо получит возможность дешифрования одного из потоков, его невозможно будет использовать без дешифрования другого потока.

В этих вариантах осуществления ключи K'_n и K_n могут быть различными. Если эти два ключа являются симметричными, возможно также использовать один и тот же ключ для обеих операций шифрования. Кроме того, можно предусмотреть размещение одного из ключей в приемном устройстве/декодере, в то время как другой ключ будет находиться в соединенном с ним модуле защиты. Это представляет особый интерес вследствие того, что

при этом гарантируется взаимное согласование используемых декодера и модуля защиты и необходимость их взаимодействия.

Вариант с использованием вещания на устройства множества пользователей

В приведенном выше описании приводятся различные способы реализации процесса передачи данных по схеме "точка-точка". Возможно, возникнет желание применить пользовательское устройство, реализующее этот способ, для вещательной передачи, при которой содержание CT и контрольные слова cw шифруются единым образом для всех пользователей. На фиг.7 показан вариант осуществления, в котором содержание CT и контрольные слова cw шифруются единым образом для всех пользователей. Это означает, что данные и контрольные слова являются общими для всех приемных устройств, что позволяет применять этот вариант осуществления для организации вещания.

Данные CT шифруются традиционным образом с помощью контрольных слов cw. Контрольные слова cw, со своей стороны, шифруются с помощью системного ключа SK. Содержание и поток ECM передаются в приемное устройство. При приеме содержания приемным устройством это содержание шифруется с помощью ключа K^*_n, в качестве которого предпочтительно использовать симметричный ключ, хотя возможно и использование асимметричного ключа. Этот ключ K^*_n является индивидуальным для данного пользовательского устройства. Поток может сохраняться в запоминающем устройстве 15 большой емкости. При дешифровании содержания приемным устройством, в котором оно сохранено, это содержание вначале дешифруется с помощью ключа K^*_n, а затем оно дешифруется вторично с помощью контрольных слов cw для получения содержания в незашифрованном виде. Ключ K^*_n предпочтительно должен находиться в электронном модуле, например микропроцессоре приемного устройства. Напомним, что в то время как изменение контрольных слов происходит, как правило, регулярно, ключ K^*_n имеет, очевидно, более длинный срок службы и может быть, например, помещен в пользовательское устройство в фиксированном и неизменном виде. Этот вариант осуществления имеет определенные преимущества по сравнению с обычной безопасной передачей данных. Поскольку в пользовательском устройстве перед сохранением содержания выполняется его шифрование с помощью ключа K^*_n, индивидуального для данного устройства, при получении третьим лицом доступа к этому содержанию это лицо не сможет использовать указанное содержание на другом пользовательском устройстве, отличном от того, для которого предназначено это содержание. Кроме того, даже в случае дешифрования содержания при его поступлении в приемное устройство использование этого содержания в другом приемном устройстве было бы бесполезным. Фактически каждое приемное устройство ожидает поступления содержания, зашифрованного с помощью ключа K^*_n, который является его индивидуальным ключом. Если в приемное устройство, ожидающее поступления зашифрованного содержания, будет поступать незашифрованное содержание, это приемное устройство будет выполнять дешифрование данных, поступающих в незашифрованном виде, и результат этой операции будет таким образом непригодным для использования.

Другое преимущество этого варианта осуществления состоит в том, что копирование файла, например видеофайла, с приемного устройства/декодера возможно, но полученная копия не может быть использована на другом приемном устройстве/декодере. Фактически копия будет представлять собой содержание, зашифрованное с помощью контрольных слов cw и индивидуального ключа K^*_n. Поскольку этот индивидуальный ключ уникален для каждого приемного устройства/декодера, дешифрование копии будет невозможным. Таким образом реализуется эффективная защита от несанкционированного копирования.

В варианте осуществления, показанном на фиг.4 и 7, дешифрование содержания должно выполняться дважды. В случае, приведенном на фиг.4, первая операция дешифрования является обратной операции шифрования, выполняемой с помощью контрольных слов cw', индивидуальных для одного из пользовательских устройств, а

вторая операция дешифрования является обратной операции шифрования, выполняемой с помощью контрольных слов cw, общих для всех пользовательских устройств. Существующие в настоящее время электронные микропроцессоры не позволяют реализовать этот вид дешифрования.

На фиг.8 схематично изображен электронный модуль, предназначенный для выполнения такого дешифрования. Как показано на фиг.8, модуль (CD) в соответствии с изобретением в основном включает в себя вычислительный блок (CPU), запоминающее устройство (ROM, RAM), дешифратор (DESCR), декомпрессор (MPEG) звука и изображения и блок (ETD) дешифрования. Блок (ETD) дешифрования выполняет дешифрование содержания, которое в варианте осуществления, показанном на фиг.7, дополнительно шифруется с помощью индивидуального ключа K^*_n при поступлении в приемное устройство/декодер.

Если пользовательское устройство используется в вещательном режиме, это двойное шифрование, естественно, не выполняется, поскольку данные являются общими для всех приемных устройств/декодеров. Поэтому в этом случае активируется блок (PE) шифрования, который выполняет шифрование содержания с помощью того же самого индивидуального ключа K^*_n. Только после этой операции содержание может быть сохранено в запоминающем устройстве 15 высокой емкости, которое может быть установлено в этом пользовательском устройстве.

Этот блок (PE) шифрования предпочтительно должен состоять из одной схемы, из которой достаточно трудно извлечь индивидуальный ключ K^*_n. Также осуществляется согласование этой схемы и электронного модуля (CD), так как в этих двух компонентах находится один и тот же ключ.

Если требуется установить пользовательское устройство, поддерживающее как режим передачи "точка-точка", так и вещательный режим, блок (PE) шифрования можно отключить. Фактически, если содержание шифруется с помощью индивидуального ключа K^*_n на передающей стороне, этот блок должен предусматривать возможность отключения. Это не создает каких-либо проблем с точки зрения безопасности, поскольку блок (ETD) дешифрования в электронном модуле (CD) не может быть отключен. Следовательно, если при использовании вещательного режима блок (PE) шифрования будет отключен, то содержание, поступающее в электронный модуль (CD), невозможно будет правильно дешифровать, так как блок (ETD) дешифрования будет выполнять дешифрование содержания с помощью индивидуального ключа K^*_n, который не применялся для шифрования этого содержания.

Блок (ETD) дешифрования, как и блок (PE) шифрования, могут выполнять относительно быстрые и простые операции. Например, может быть использована функция XOR (исключающее ИЛИ), которая не вносит практически никакой задержки при передаче содержания. Для серии данных обычно используется серия шагов шифрования, которые инициируются в определенной последовательности.

Следует отметить, что блок (PE) шифрования может также быть интегрирован в электронный модуль, в результате чего этот модуль реализует создание выходных данных блока шифрования для сохранения содержания в запоминающем устройстве 15 большой емкости и создание входных данных блока дешифрования для дешифрования содержания, получаемого из этого запоминающего устройства.

Согласование

Как правило, если пользовательское устройство содержит приемное устройство/декодер и модуль защиты, каждый из этих двух компонентов содержит ключ, известный как ключ K_p согласования, который является индивидуальным для каждого пользовательского устройства и может быть симметричным или асимметричным. Поток ECM поступает в модуль защиты, где он дешифруется и из него извлекаются контрольные слова с помощью системного ключа SK. При передаче контрольных слов из модуля защиты в приемное устройство/декодер выполняется шифрование этих контрольных слов либо с помощью

ключа K_p согласования, либо с помощью ключа сеанса в зависимости от этого ключа согласования. Этот процесс подробно описан в документе WO 99/57901. Контрольные слова дешифруются в декодере с помощью ключа, соответствующего ключу, используемому для шифрования. Это позволяет гарантировать, что конкретный модуль защиты будет взаимодействовать только с одним приемным устройством/декодером, т.е. эти компоненты будут таким образом согласованы друг с другом.

Настоящее изобретение, кроме того, позволяет обеспечить согласование различными способами как между модулем защиты и приемным устройством/декодером, так и между центром управления и приемным устройством/декодером.

Взаимное согласование модуля защиты и приемного устройства/декодера

На фиг.9 показан вариант осуществления, в котором приемное устройство/декодер согласуется с модулем защиты. В описываемом случае пользовательское устройство имеет два ключа, а именно ключ K_n, индивидуальный для каждого пользовательского устройства, и ключ K_p согласования. С целью реализации совместимости между режимом передачи "точка-точка" и вещательным режимом индивидуальный ключ K_n сохраняется и в модуле защиты.

Вещательный режим

Если пользовательское устройство используется в вещательном режиме, поток ECM, содержащий контрольные слова cw, поступает в модуль защиты. Этот модуль выполняет извлечение контрольных слов cw с помощью системного ключа SK. Затем контрольные слова вновь шифруются с помощью индивидуального ключа K_n для получения зашифрованных контрольных слов cw'. После этого полученные контрольные слова cw' повторно шифруются в модуле защиты с помощью ключа K_p согласования для получения зашифрованных контрольных слов $cw''=K_p(cw')$. В этой форме они передаются в приемное устройство/декодер. В последнем зашифрованные контрольные слова cw'' вначале дешифруются с помощью ключа K_p согласования. Затем они дешифруются вторично с помощью индивидуального ключа K_n для получения этих контрольных слов в незашифрованном виде. После этого они могут использоваться для дешифрования содержания CT.

В варианте осуществления, показанном на фиг.9, индивидуальный ключ хранится в дешифраторе. Этот ключ может быть фиксированным и однократно записанным, например, в устройстве типа PROM, ROM. Ключ согласования может быть программным ключом, сохраняемым в декодере вне дешифратора. С другой стороны, оба ключа могут совместно размещаться в дешифраторе или вне его.

Режим передачи по схеме "точка-точка"

Если пользовательское устройство используется в режиме передачи по схеме "точка-точка", поток ECM, содержащий контрольные слова cw', персонализируется в центре управления. Из этого следует, что нет необходимости выполнять кодирование с помощью индивидуального ключа K_n. Поток ECM таким образом дешифруется с помощью системного ключа с целью извлечения контрольных слов. Затем они немедленно шифруются повторно с помощью ключа K_p согласования, после чего передаются в приемное устройство/декодер. В нем они вначале дешифруются с помощью ключа K_p согласования, а затем с помощью индивидуального ключа K_n. Это позволяет получить контрольные слова cw в незашифрованном виде.

Взаимное согласование центра управления и приемного устройства/декодера

В варианте осуществления, показанном на фиг.10, представлен пример, в котором реализуется согласование центра управления и приемного устройства/декодера. Контрольные слова шифруются с помощью индивидуального ключа K_n, как показано на фиг.2. Поток ECM, содержащий эти индивидуальные зашифрованные контрольные слова cw', передается либо в модуль защиты, который передает их в приемное устройство/декодер без изменений, либо напрямую в приемное устройство/декодер без прохождения через модуль защиты. В приемном устройстве/декодере выполняется их дешифрование с помощью индивидуального ключа K_n для получения их в

незашифрованном виде. Этот вариант осуществления позволяет устанавливать взаимное согласование центра управления и приемного устройства/декодера, вследствие чего пригодный для использования результат будет выдаваться только тем приемным устройством/декодером, которое (который) обладает индивидуальным ключом, хранящимся в центре управления.

Как указано выше, ключи могут быть неизменными и могут быть совместно расположены в микропроцессоре приемного устройства. Они могут также располагаться в модуле защиты каждого пользовательского устройства. Эти ключи могут также передаваться из центра управления и, следовательно, изменяться. Один из способов выполнения этой операции состоит, например, в передаче нового ключа в составе хорошо защищенного потока контрольных сообщений, называемого "главным потоком ECM". Это позволяет повысить уровень защиты, поскольку по прошествии некоторого времени использования ключа этот ключ может быть изменен.

Формула изобретения

1. Способ безопасной передачи данных по схеме "точка-точка" между центром (10) управления и одним из множества пользовательских устройств, связанных с указанным центром (10) управления, причем указанные данные включают в себя содержание (CT), зашифрованное посредством, по меньшей мере, одного контрольного слова (cw), а каждое пользовательское устройство содержит, по меньшей мере, один декодер/приемное устройство (12), снабженный (снабженное), по меньшей мере, одним ключом (K_1, K_2,..., K_n) шифрования, индивидуальным для каждого пользовательского устройства, включающий в себя следующие шаги:

осуществляют посылку пользовательским устройством (D_1, D_2,..., D_n) в центр (10) управления запроса с заказом на передачу определенного содержания (CT),

посылают в центр (10) управления уникальный идентификатор (UA_1, UA_2,..., UA_n), причем этот идентификатор однозначно определяет пользовательское устройство, пославшее запрос,

определяют по базе (14) данных, связанной с центром управления, ключ (K_n), соответствующий указанному пользовательскому устройству, пославшему запрос,

определяют контрольное слово или слова, связанное (связанные) с содержанием (CT), предназначенным для передачи,

отличающийся тем, что дополнительно включает в себя следующие шаги:

шифруют указанное предназначенное для передачи содержание (CT), индивидуальным для каждого пользовательского устройства способом,

передают указанное зашифрованное содержание в пользовательское устройство, пославшее запрос,

передают зашифрованные контрольные слова в пользовательское устройство, пославшее запрос.

2. Способ по п.1, отличающийся тем, что содержание (CT), предназначенное для передачи, шифруют посредством указанного ключа (K_n), индивидуального для приемного устройства.

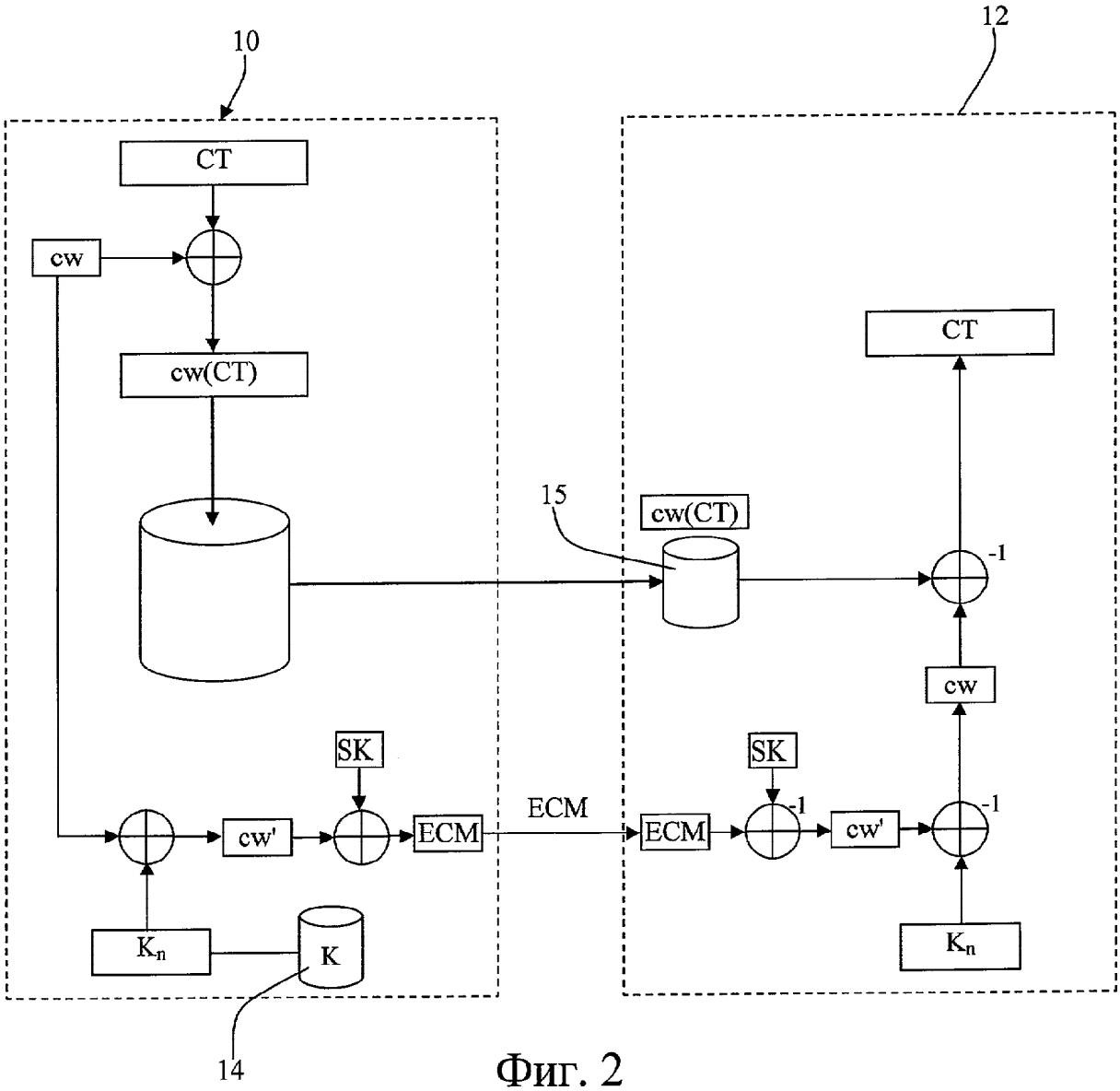
3. Способ по п.1, отличающийся тем, что контрольные слова (cw) шифруют посредством указанного ключа (K_n), соответствующего пользовательскому устройству, пославшему запрос, с целью получения зашифрованных контрольных слов (cw'), и указанное содержание (CT), предназначенное для передачи, шифруют посредством этих зашифрованных контрольных слов (cw').

4. Способ по п.1, отличающийся тем, что ключ, посредством которого шифруют содержание (CT) и который соответствует пользовательскому устройству, отличается от ключа, посредством которого шифруют контрольные слова (cw) и который соответствует пользовательскому устройству.

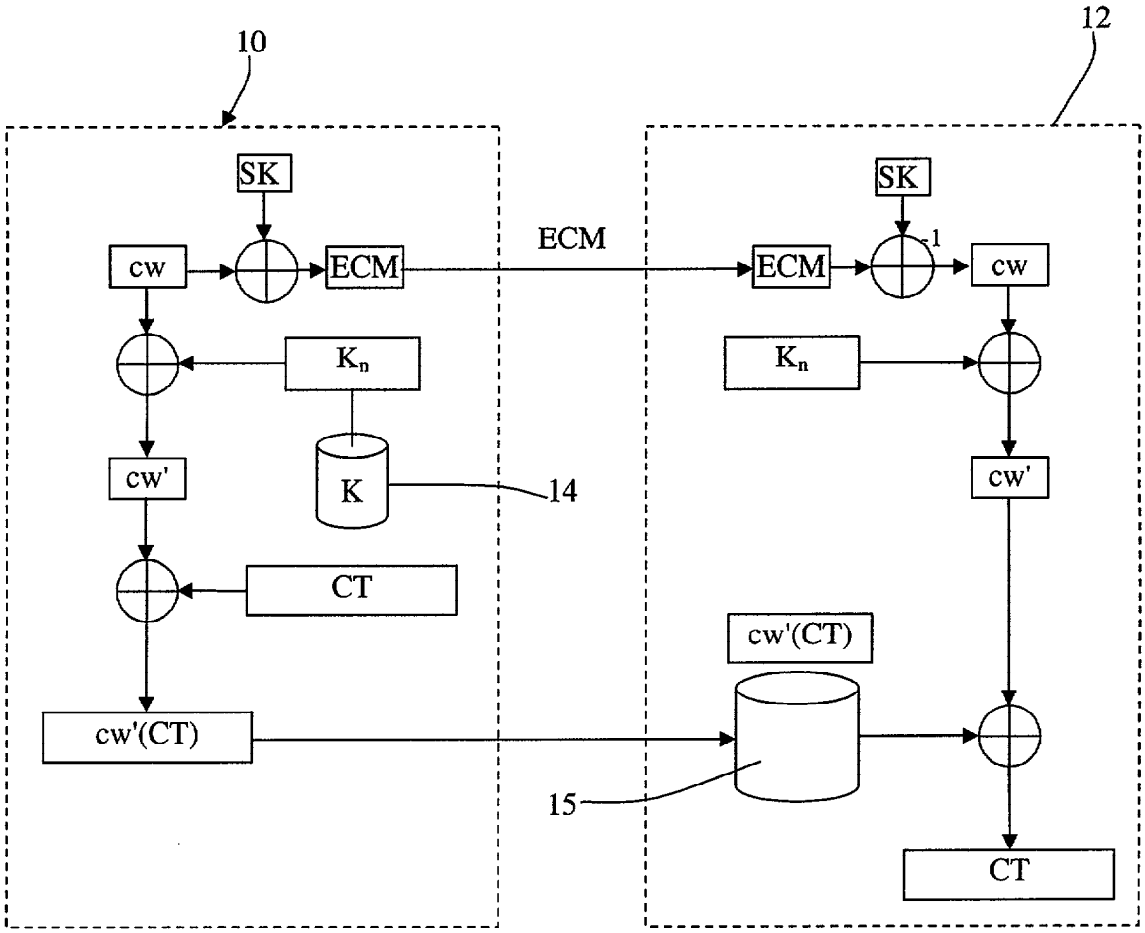
5. Способ по п.1, отличающийся тем, что соответствующий пользовательскому устройству ключ, посредством которого шифруют содержание (CT), идентичен ключу,

посредством которого шифруют контрольные слова (cw) и который соответствует пользовательскому устройству,

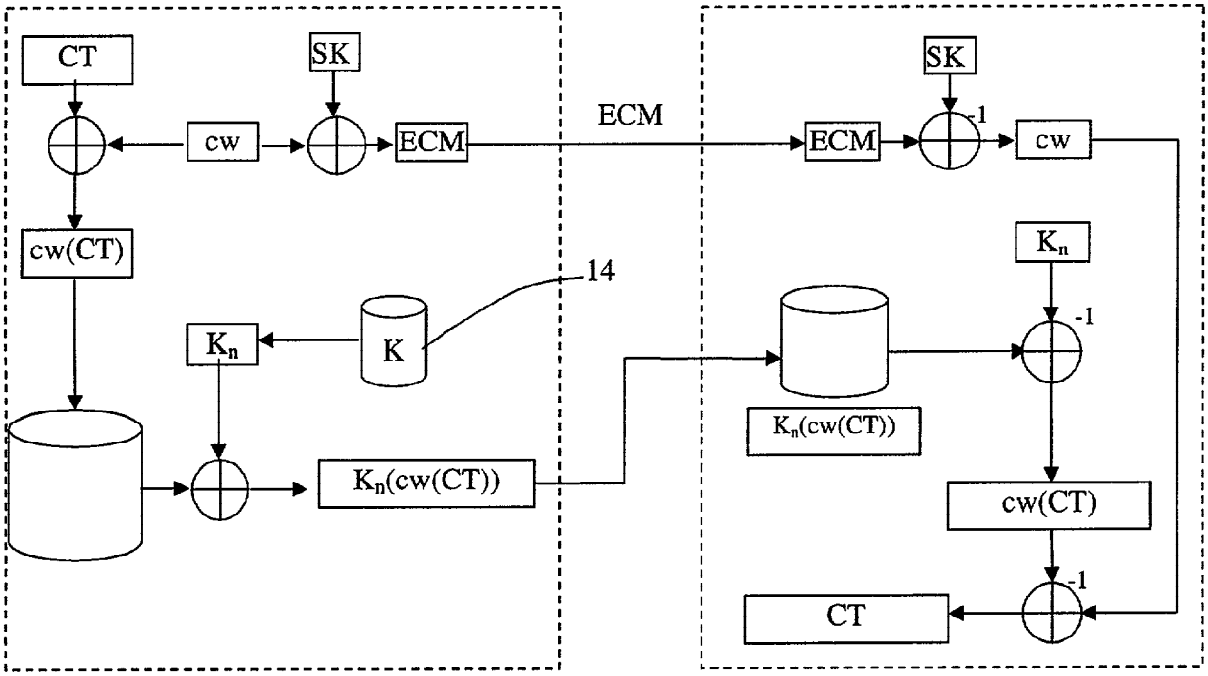
6. Модуль защиты, предназначенный для приема содержания (CT), зашифрованного посредством по меньшей мере одного контрольного слова (cw) и по меньшей мере одним ключом, индивидуальным для каждого пользовательского устройства, включающий в себя запоминающее устройство (ROM, RAM) с возможностью сохранения ключа, индивидуального для каждого пользователя, дешифратор (DESCR), декомпрессор (MPEG) звука и изображения, представляющих содержание (CT), причем дешифратор (DESCR) выполнен с возможностью приема контрольных слов (cw), отличающийся тем, что дополнительно включает в себя блок (ETD) дешифрования, обрабатывающий принятое содержание (CT) и использующий ключ, индивидуальный для каждого пользовательского устройства.



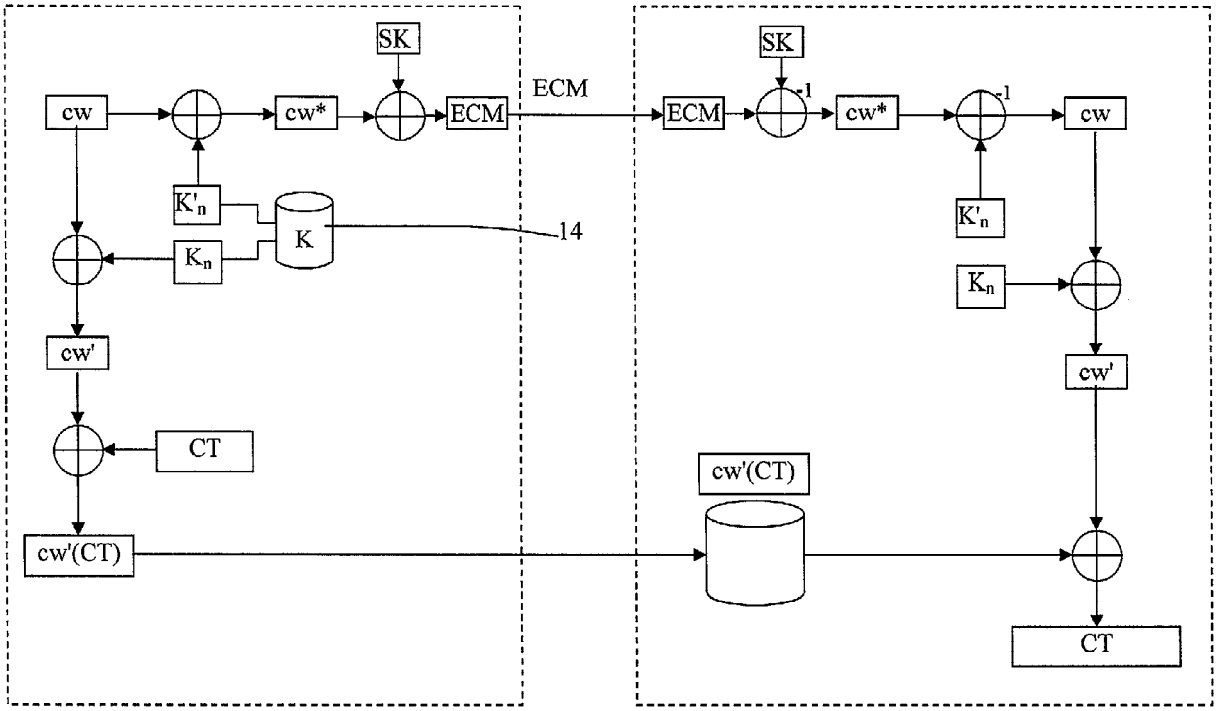
Фиг. 2


10
12
SK
cw
ECM
ECM
SK
-1
ECM
cw
K_n
K_n
cw'
K
14
cw'
CT
cw'(CT)
cw'(CT)
15
CT

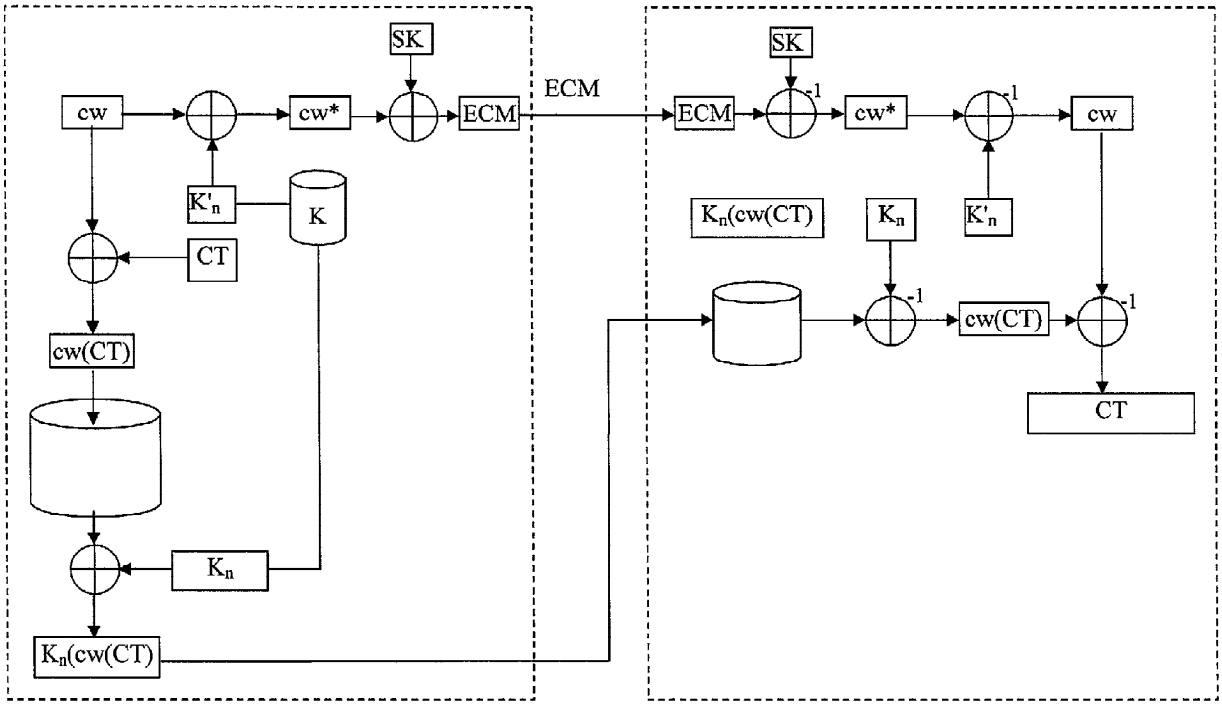
Фиг. 3


CT
SK
cw
ECM
ECM
SK
-1
ECM
cw
cw(CT)
K_n
14
K_n
K
-1
K_n(cw(CT))
K_n(cw(CT))
cw(CT)
-1
CT

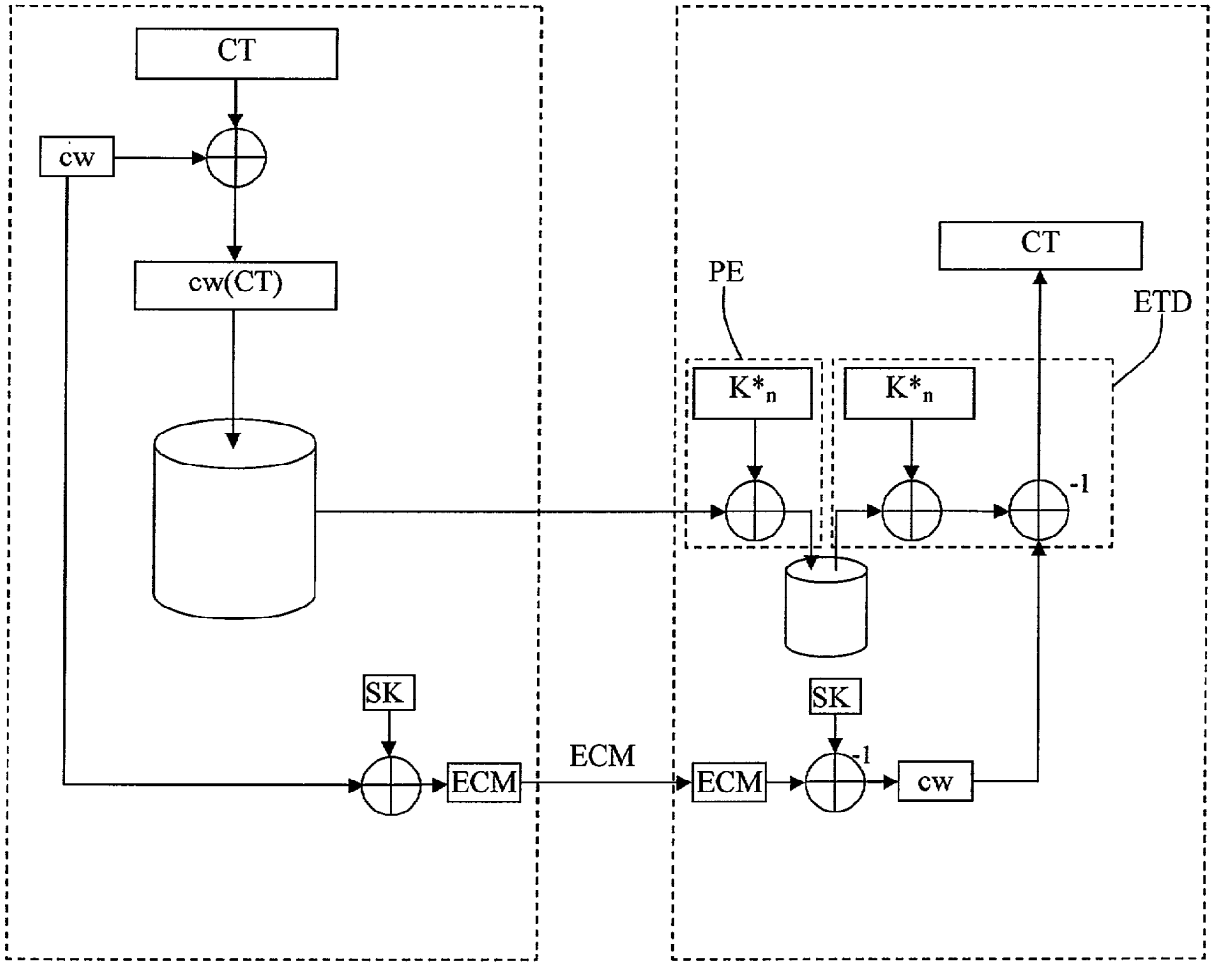
Фиг. 4


SK
cw
cw*
ECM
ECM
K'n
K
14
Kn
cw'
CT
cw'(CT)
SK
-1
cw*
-1
cw
K'n
Kn
cw'
cw'(CT)
CT

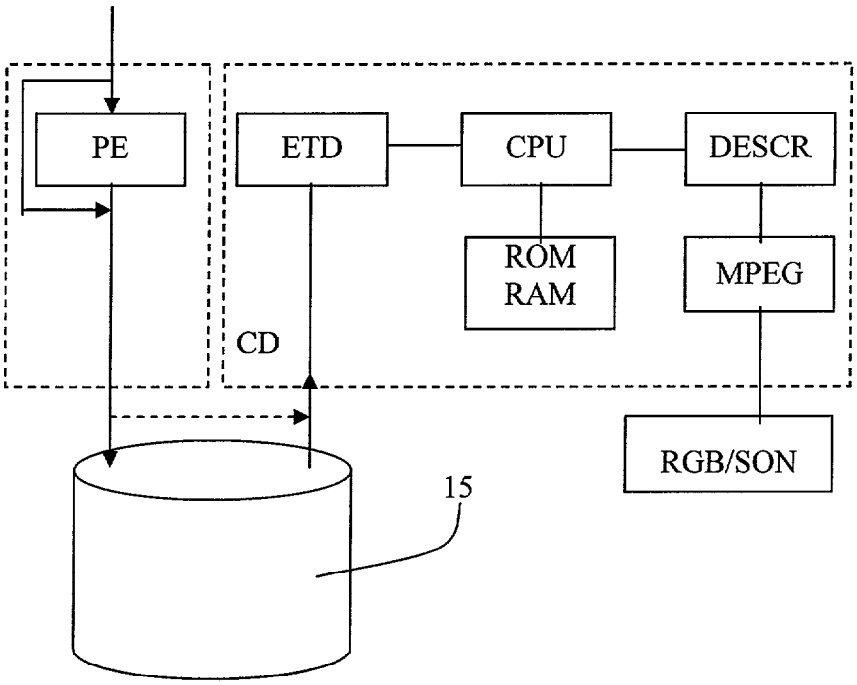
Фиг. 5


SK
cw
cw*
ECM
ECM
K'n
K
CT
cw(CT)
Kn
Kn(cw(CT))
SK
-1
cw*
-1
cw
Kn(cw(CT))
Kn
K'n
-1
cw(CT)
-1
CT

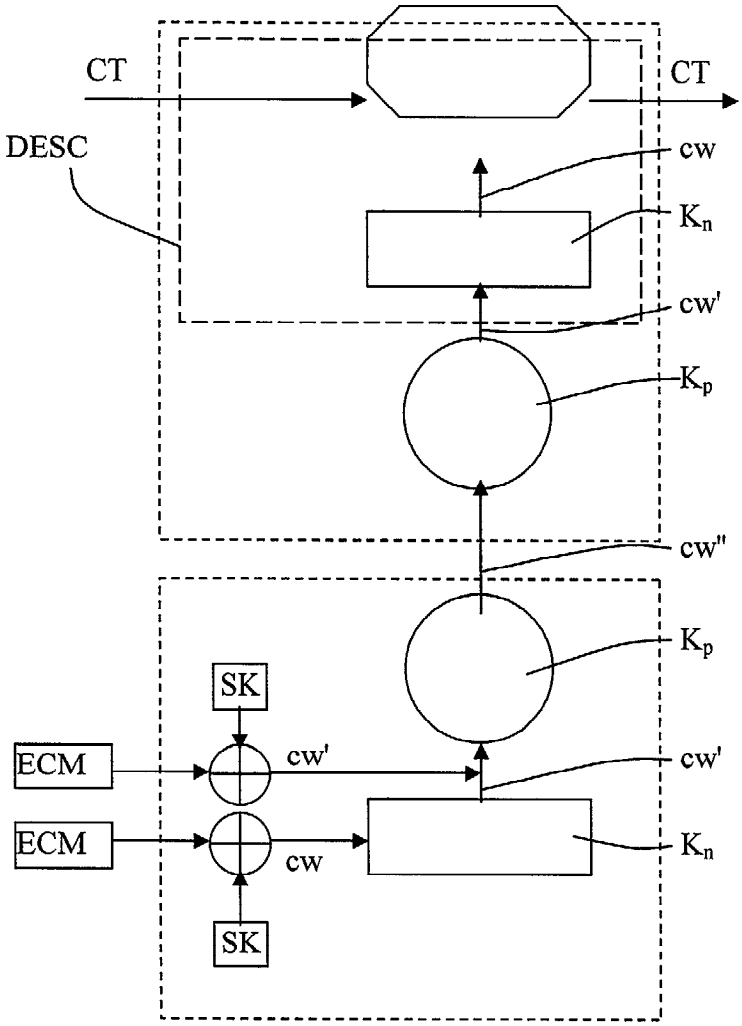
Фиг. 6


CT
cw
cw(CT)
PE
CT
ETD
K*n
K*n
-1
SK
SK
ECM
ECM
ECM
-1
cw

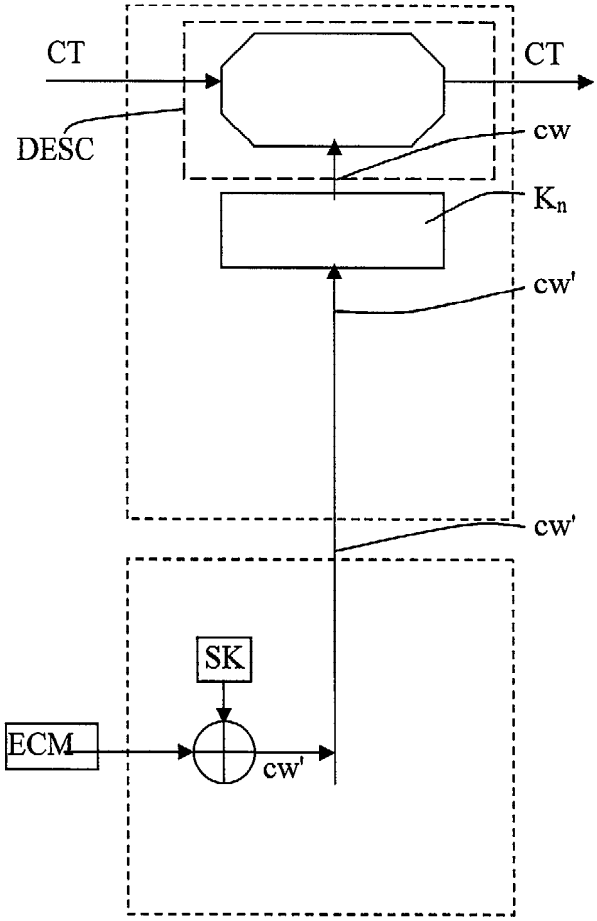
Фиг. 7


PE
ETD
CPU
DESCR
ROM
RAM
MPEG
CD
RGB/SON
15

Фиг. 8



Фиг. 9



Фиг. 10