



(19) **RU** ⁽¹¹⁾ **2 195 086** ⁽¹³⁾ **C2**
(51) МПК⁷ **H 04 N 7/167**

РОССИЙСКОЕ АГЕНТСТВО
ПО ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) **ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ РОССИЙСКОЙ ФЕДЕРАЦИИ**

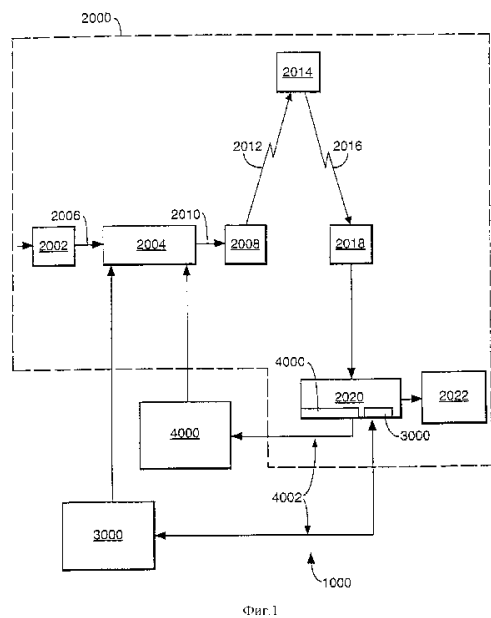
(21), (22) Заявка: 99121836/09, 25.04.1997
(24) Дата начала действия патента: 25.04.1997
(30) Приоритет: 21.03.1997 EP 97400650.4
(46) Дата публикации: 20.12.2002
(56) Ссылки: EP 0752786 A1, 08.01.1997. RU 2024213 C1, 30.11.1994. EP 0687113 A1, 13.12.1995. EP 0752786 A1, 08.01.1997. US 5365272 A, 15.11.1994. US 5579317 A, 26.11.1996.
(85) Дата перевода заявки РСТ на национальную фазу: 21.10.1999
(86) Заявка РСТ: EP 97/02111 (25.04.1997)
(87) Публикация РСТ: WO 98/43431 (01.10.1998)
(98) Адрес для переписки: 193036, Санкт-Петербург, а/я 24, "НЕВИНПАТ", А.В.Поликарпову

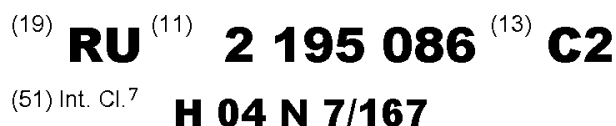
(71) Заявитель: КАНАЛЬ+ СОСЬЕТЭ АНОНИМ (FR)
(72) Изобретатель: САРФАТИ Жан-Клод (FR), МЕРИК Жером (FR)
(73) Патентообладатель: КАНАЛЬ+ СОСЬЕТЭ АНОНИМ (FR)
(74) Патентный поверенный: Поликарпов Александр Викторович

(54) СПОСОБ ЗАГРУЗКИ ДАННЫХ В ПРИЕМНИК/ДЕКОДЕР MPEG И СИСТЕМА ТРАНСЛЯЦИИ MPEG ДЛЯ ЕГО РЕАЛИЗАЦИИ

(57)
В системе цифрового телевидения, в которой телевизор принимает ТВ-сигнал через приемник/декодер, например, в виде приставки, в приемник/декодер может загружено и выполнено приложение. Код приложения представлен в виде модулей, и загрузке модулей предшествует поиск модуля каталога в пределах заданного локального адреса. Модули подписываются, и модуль каталога подписывается и зашифровывается так, чтобы для всех модулей, составляющих приложение, используется одна операция шифрования. В ПЗУ приемника/декодера хранится множество общедоступных шифровальных ключей, так что приложения

могут создаваться различными источниками, причем этим источникам нет необходимости знать шифровальные ключи друг друга. Предоставляется средство для временного хранения шифровального ключа в оперативной памяти приемника/декодера, так что изготовитель приемника/декодера может проверять его функции. Подпись каталога может быть спрятана в любой позиции блока фиктивных данных в модуле каталога. Подлежащее загрузке приложение может быть проверено с использованием битового массива проверки допустимости, хранящегося в памяти приемника/декодера. 13 с. и 90 з.п.ф-лы, 10 ил.



(12) **ABSTRACT OF INVENTION**

(71) Applicant:
KANAL'+ SOS'ETeh ANONIM (FR)

(72) Inventor: **SARFATI Zhan-Klod (FR),
MERIK Zherom (FR)**

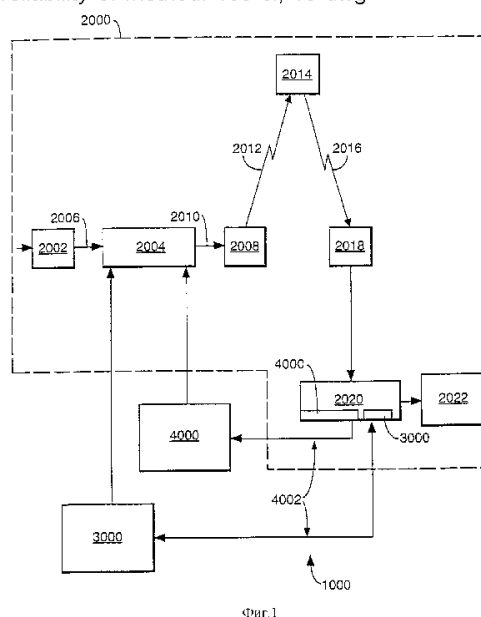
(73) Proprietor:
KANAL'+ SOS'ETeh ANONIM (FR)

(74) Representative:
Polikarpov Aleksandr Viktorovich

(57) Abstract:

FIELD: digital television. **SUBSTANCE:** invention refers to digital television system in which TV set receives TV signal through receiver/decoder, for instance, in the form of attachment, and application can be loaded into receiver/decoder and realized. Application code comes in the form of modules and search for catalogue module within limits of specified local address precedes module loading. Modules are signed and catalogue module is so signed and encoded that single coding operation is used for all modules. Permanent storage of receiver/decoder stores collection of accessible coding keys so that applications can be formed by various sources. There is no necessity for these sources to know one another. Aid for temporary storage of coding key in on-line storage of receiver/decoder is allotted so that manufacturer of receiver/decoder can test its functions. Catalogue signature can be hidden in any position of fictitious data unit in catalogue module. Application subject to loading can be tested with use of bit array

of test of accessibility kept in storage of receiver/decoder. EFFECT: improved reliability of method. 103 cl. 10 dwg



Предлагаемое изобретение относится к способу загрузки данных в приемник/декодер MPEG; такому приемнику/декодеру; и системе трансляции MPEG.

Появление систем передачи цифровых данных, предназначенных в первую очередь для сигналов телевизионного вещания, в особенности, но не исключительно, систем спутникового телевидения, открыло возможность использования таких систем для других целей. Одной из них является предоставление пользователю интерактивного режима работы.

Одним из способов его обеспечения является выполнение приложения в приемнике/декодере, с помощью которого принимается телевизионный сигнал. Код этого приложения можно было бы постоянно хранить в приемнике/декодере. Однако это было бы ограничивающим фактором. Предпочтительно приемник/декодер должен быть в состоянии загружать код для требуемого приложения. Таким образом может быть обеспечена большая гибкость, и приложение может быть при необходимости обновлено без какого-либо участия пользователя.

В системе MPEG код приложения может загружаться в MPEG таблицах. Однако существует ограничение на размер фрагмента кода, который может быть загружен с помощью одной MPEG таблицы. К тому же, если перед тем, как приложение может быть выполнено, его необходимо загрузить полностью, это может привести к задержке, которая будет неприемлемой для пользователя. Следовательно, возникает желание иметь возможность загружать приложение в виде набора модулей. Это, однако, в свою очередь, создает проблему обеспечения возможности идентификации и выделения из потока битов MPEG модулей, необходимых для данного приложения. Первый аспект данного изобретения направлен на решение этой проблемы.

В соответствии с первым аспектом данного изобретения предлагается способ загрузки в приемник/декодер MPEG хотя бы части приложения, содержащий следующие операции:

разделение приложения на множество модулей;

форматирование каждого модуля в виде соответствующей MPEG таблицы, причем все таблицы имеют одинаковый идентификатор таблицы (TID) и соответствующие разные расширения идентификатора таблицы (TID-расширения), отличные от одного заранее определенного TID-расширения;

генерирование MPEG таблицы каталога для модулей, имеющей тот же упомянутый TID и упомянутое заранее определенное TID-расширение, при этом каталог содержит имена каждого из модулей и соответствующие TID-расширения;

циклическая трансляция MPEG таблицы каталога и MPEG таблиц модулей в потоке битов MPEG; и в приемнике/декодере MPEG:

прием потока битов MPEG;

загрузка той MPEG таблицы, которая имеет упомянутое заранее определенное TID-расширение, с тем чтобы загрузить MPEG таблицу каталога;

определение из содержимого MPEG

таблицы каталога TID-расширений MPEG таблиц модулей; и

загрузка хотя бы одной из MPEG таблиц модулей, имеющих тот же самый TID, что и загруженная MPEG таблица каталога, и TID-расширение, определенное из загруженной MPEG таблицы каталога.

Таким образом, приложение создается из нескольких модулей, которые могут быть загружены, и, соответственно, выполняется, если это необходимо. Таблица каталога может быть легко идентифицирована, поскольку она имеет особое TID-расширение, и как только она загружена, она позволяет приемнику/декодеру идентифицировать таблицы модулей по соответствующим TID-расширениям.

Предпочтительно способ содержит дополнительно следующие операции: включение в транслируемую MPEG таблицу каталога идентификации ее версии; и

в приемнике/декодере:

определение того, является ли версия транслируемой в данный момент MPEG таблицы каталога более новой, чем версия загруженной на данный момент MPEG таблицы каталога и, если это так, повторение операций загрузки MPEG таблицы каталога, определения TID-расширений и загрузки хотя бы одной из MPEG таблиц модулей.

Таким образом, если приложение следует изменить, это может быть определено автоматически, и будут загружены обновленный каталог и любые обновленные модули.

Хотя бы одна из MPEG таблиц модулей может быть отформатирована в виде множества секций, которые транслируются отдельно в потоке битов MPEG, при этом каждая из MPEG секций содержит в ее заранее определенной части идентификацию положения этой MPEG секции в упомянутой MPEG таблице и количества секций в упомянутой MPEG таблице.

В соответствии со вторым аспектом данного изобретения предлагается приемник/декодер MPEG для осуществления части способа по любому из предшествующих пунктов, содержащий:

приемник для приема потока битов MPEG; средство хранения;

и средство обработки, которое программируется таким образом, чтобы инициировать загрузку в средство хранения той из принятых MPEG таблиц, которая имеет заранее определенное TID-расширение, определять из содержимого MPEG таблицы каталога TID-расширения MPEG таблиц модулей и инициировать загрузку в средство хранения хотя бы одной из MPEG таблиц модулей, имеющей тот же TID, что и загруженная MPEG таблица каталога, и TID-расширение, определенное из загруженной MPEG таблицы каталога.

Предпочтительно средство обработки запрограммировано определять, является ли версия принимаемой в данный момент MPEG таблицы каталога более новой, чем версии загруженной MPEG таблицы каталога, и, если это так, повторять загрузку MPEG таблицы каталога, определение TID-расширений и загрузку хотя бы одной из MPEG таблиц модулей.

В случае, когда приемник/декодер выполнен с возможностью приема хотя бы

одной из таблиц модулей, отформатированной в виде множества отдельно транслируемых секций, предпочтительно средство обработки запрограммировано инициировать циклическую загрузку MPEG секций в средство хранения до тех пор, пока средство обработки не определит по идентификации положения секций и указанию количества секций загруженных секций, что все секции уже загружены.

Предпочтительно приемник/декодер содержит параллельный порт и/или последовательный порт, выполненные с возможностью приема приложения, отформатированного в виде хотя бы одной MPEG таблицы, и в этом случае предпочтительно используется короткий формат MPEG-2, в то время как длинный формат MPEG-2 предпочтительно используется для удаленного приема, например, через спутник или по кабелю.

Это особенно удобно в случае, когда изготовитель желает протестировать конкретные функции приемника/декодера, поскольку приложение может быть загружено без необходимости транслировать его через систему спутникового телевидения.

В соответствии с третьим аспектом данного изобретения предлагается система трансляции MPEG, содержащая:

средство для разделения приложения, подлежащего загрузке в приемник/декодер MPEG, на множество модулей;

средство для форматирования каждого из модулей в виде соответствующей MPEG таблицы, причем все таблицы имеют одинаковый TID и соответствующие различные TID-расширения, отличные от заранее определенного TID-расширения;

средство для генерирования MPEG таблицы каталога для модулей, имеющей тот же упомянутый TID и упомянутое заранее определенное TID-расширение, при этом каталог содержит для каждого модуля имя этого модуля и соответствующее TID-расширение;

средство для генерирования MPEG таблицы каталога для модулей, имеющих одинаковые TID и упомянутые заранее определенные TID-расширения, при этом каталог содержит имена каждого из модулей и соответствующие TID-расширения; и

средство для циклической трансляции MPEG таблицы каталога и MPEG таблиц модулей в потоке битов MPEG.

Предпочтительно система дополнительно содержит средство для генерирования идентификатора версии для MPEG таблицы каталога, и в этой системе средство генерирования MPEG таблицы каталога выполнено с возможностью добавления в MPEG таблицу каталога сгенерированного идентификатора ее версии.

Средства форматирования модулей могут быть выполнены с возможностью форматирования хотя бы одной из MPEG таблиц модулей в виде множества MPEG секций, каждая из которых содержит в ее заранее определенной части идентификацию положения этой MPEG секции в упомянутой MPEG таблице и указание количества секций в упомянутой MPEG таблице.

Желательно, чтобы приемник/декодер был защищен от загрузки несанкционированных

приложений, которые могут содержать, например, вирус. В соответствии с этим может быть рассмотрена концепция шифровки и использования подписей для хотя бы части кода приложения.

5 В соответствии с четвертым аспектом данного изобретения предлагается способ загрузки данных в приемник/декодер MPEG, содержащий следующие операции:

10 генерирование подписи для данных, подлежащих загрузке;

шифрование подписи с использованием секретного ключа;

форматирование подлежащих загрузке данных, зашифрованной подписи и идентификатора секретного ключа в виде MPEG таблицы;

15 трансляция MPEG таблицы; и в приемнике/декодере:

прием MPEG таблицы;

20 выбор одного из множества общедоступных ключей в соответствии с идентификатором ключа в принятой MPEG таблице;

дешифровка зашифрованной подписи в принятой MPEG таблице с использованием выбранного общедоступного ключа для получения дешифрованной подписи;

25 генерирование подписи для данных в принятой MPEG таблице;

и сравнение дешифрованной подписи и подписи, сгенерированной приемником/декодером для принятых данных.

30 Таким образом, приемник/декодер может использоваться для загрузки имеющих зашифрованные подписи приложений более чем от одного источника, при этом источникам нет необходимости знать секретные ключи друг друга.

35 Способ может дополнительно содержать операции загрузки в приемник/декодер приложения, имеющего подпись, зашифрованную с использованием секретного ключа, имеющего заранее определенный идентификатор, выполнения приложения в приемнике/декодере с целью инициирования приема приемником/декодером

40 дополнительного ключа, сохранения дополнительного ключа в область оперативной памяти приемника/декодера. В этом случае при выполнении приложения

45 дополнительный ключ может предоставляться приемнику/декодеру на месте, например, через параллельный порт, последовательный порт или устройство считывания смарт-карты приемника/декодера.

50 Если приемник/декодер имеет подключенный модем, то приемник/декодер предпочтительно выполнен так, чтобы воспрепятствовать получению такого дополнительного ключа через модем.

55 Эти особенности позволяют производителю, который может пожелать протестировать приемник/декодер, загрузить ключ в приемник/декодер.

60 Способ может дополнительно содержать операции, в приемнике/декодере, поиска в защищенной области памяти приемника/декодера флага допустимости для выбранного общедоступного ключа и запрета или прекращения загрузки данных, если найденный флаг не установлен.

Соответственно, хотя множество общедоступных ключей может постоянно находиться в памяти приемника/декодера,

любые из них могут быть выборочно отключены, что может быть необходимо в случае, например, когда секретность секретного ключа, соответствующего конкретному общедоступному ключу, нарушена, или когда два оператора, использующие одинаковые ключи, решают, что они желают иметь отдельные ключи.

В случае, когда приемник/декодер выполнен с возможностью загрузки приложения, имеющего подпись, зашифрованную с использованием секретного ключа, имеющего заранее определенный идентификатор ключа, как указано выше, в защищенной области памяти приемника/декодера секретный ключ, имеющий заранее заданный идентификатор ключа, имеет флаг проверки допустимости, который может быть изменен упомянутым приложением, а также возможность приема упомянутого дополнительного ключа определяется в зависимости от состояния этого флага проверки допустимости.

Эти дополнительные особенности флага проверки допустимости для общедоступных ключей могут быть предоставлены независимо от четвертого аспекта изобретения. Соответственно, в пятом аспекте данного изобретения предлагается способ загрузки данных в приемник/декодер MPEG, содержащий следующие операции:

генерирование подписи для подлежащих загрузке данных;

шифрование подписи с использованием секретного ключа;

форматирование подлежащих загрузке данных, зашифрованной подписи и идентификатора секретного ключа в виде MPEG таблицы;

трансляция MPEG таблицы; и в приемнике/декодере:

прием MPEG таблицы;

поиск в защищенной области памяти приемника/декодера флага проверки допустимости для выбранного общедоступного ключа, соответствующего идентификатору секретного ключа, указанного в принятой MPEG таблице; и, если найденный флаг установлен:

дешифровка зашифрованной подписи в принятой MPEG таблице с использованием общедоступного ключа, соответствующего идентификатору секретного ключа, указанному в принятой MPEG таблице, для получения дешифрованной подписи;

генерирование подписи для данных в принятой MPEG таблице; и сравнение дешифрованной подписи и подписи, сгенерированной в приемнике/декодере для принятых данных.

Способы четвертого и пятого аспектов настоящего изобретения предпочтительно включают дополнительно следующие операции: генерирование кода допустимости для подлежащих загрузке данных, который зашифровывается вместе с подписью при выполнении операции шифрования и дешифруется вместе с подписью при выполнении операции дешифровки;

поиск сохраненного кода проверки допустимости в защищенной области памяти приемника/декодера; и сравнение найденного кода проверки допустимости и дешифрованного кода проверки допустимости.

Таким образом, приемник/декодер может быть настроен на прием только определенных приложений или типов приложений.

Эти дополнительные особенности могут быть предоставлены независимо от четвертого и пятого аспектов изобретения. В соответствии с этим в шестом аспекте данного изобретения предлагается способ загрузки данных в приемник/декодер MPEG, содержащий следующие операции:

генерирование кода проверки допустимости для подлежащих загрузке данных;

генерирование подписи для подлежащих загрузке данных или их части;

шифрование кода проверки допустимости и подписи с использованием секретного ключа;

форматирование подлежащих загрузке данных и зашифрованных кода проверки допустимости и подписи в виде хотя бы одной MPEG таблицы;

трансляция данной или каждой из MPEG таблиц; и в приемнике/декодере:

прием данной или всех MPEG таблиц;

дешифровка зашифрованных кода проверки допустимости и подписи в принятой(ых) MPEG таблице(ах) с использованием общедоступного ключа, соответствующего указанному секретному ключу;

поиск сохраненного кода проверки допустимости в защищенной области памяти приемника/декодера;

сравнение найденного ключа проверки допустимости и дешифрованного ключа проверки допустимости;

генерирование подписи для данных в принятых(ой) MPEG таблице(ах) или упомянутой их части;

и сравнение расшифрованной подписи и подписи, сгенерированной в приемнике/декодере, для принятых данных.

Предпочтительно способ дополнительно содержит операцию запрета или прекращения загрузки данных в случае, если по результатам сравнения кодов проверки допустимости найденный код проверки допустимости и дешифрованный код проверки допустимости не совпадают друг с другом.

В четвертом-шестом аспектах данного изобретения может быть предусмотрено, что подпись подлежащих загрузке данных зашифровывается в блоке данных, содержащем и другие данные, с некоторым выбранным смещением между началом блока данных и началом подписи, и зашифрованный блок данных дешифруется при выполнении операции дешифровки в приемнике/декодере, и дополнительно включающий операции, в приемнике/декодере, поиска хотя бы одного смещения, хранящегося в защищенной области памяти приемника/декодера, а также извлечения подписи из дешифрованного блока данных с использованием упомянутого одного найденного смещения от начала дешифрованного блока данных.

Таким образом, подпись может быть замаскирована среди фиктивных данных, что затрудняет обнаружение местоположения подписи. Как альтернатива, или дополнительно, эта особенность обеспечивает доступ к данным только одной или несколькими определенными группам

приемников/декодеров.

Эти особенности могут быть предоставлены независимо от аспектов изобретения с четвертого по шестой. В соответствии с изложенным выше в седьмом аспекте данного изобретения предлагается способ загрузки данных в приемник/декодер MPEG, содержащий следующие операции:

генерирование подписи для подлежащих загрузке данных;

включение подписи и других данных в блок данных с выбранным смещением между началом блока данных и началом подписи;

шифрование блока данных с использованием секретного ключа;

форматирование подлежащих загрузке данных и зашифрованного блока данных в виде MPEG таблицы;

трансляция MPEG таблицы; и в приемнике/декодере:

и прием MPEG таблицы;

дешифровка зашифрованного блока данных в принятой MPEG таблице с использованием общедоступного ключа, соответствующего упомянутому секретному ключу;

поиск хотя бы одного смещения, хранящегося в защищенной области памяти приемника/декодера;

извлечение подписи из дешифрованного блока данных с использованием упомянутого найденного смещения от начала дешифрованного блока данных;

генерирование подписи для данных в принятой MPEG таблице; и

сравнение подписи, извлеченной из дешифрованного блока данных, и подписи, сгенерированной в приемнике/декодере для принятых данных.

В случае, когда упомянутая защищенная область памяти содержит хотя бы два таких сохраненных смещения и, если по результатам операции сравнения извлеченная подпись и сгенерированная подпись не совпадают, способ предпочтительно включает дополнительную операцию повторения операций поиска, извлечения и сравнения с использованием других сохраненных смещений.

Хотя бы некоторые из остальных данных в блоке данных могут быть фиктивными или произвольными данными, но, если это так, предпочтительно ни один из фрагментов фиктивных данных не совпадает с подписью.

В аспектах изобретения от четвертого до седьмого данные могут загружать в виде множества модулей данных, и способ может содержать следующие операции:

генерирование подписи модуля для каждого модуля данных, подлежащего загрузке;

форматирование модулей данных в виде соответствующих MPEG таблиц модулей;

генерирование каталога, включающего идентификатор каждой MPEG таблицы модуля и соответствующую подпись, причем указанный каталог является объектом операции генерирования подписи по любому из пп.11-24; и в приемнике/декодере:

генерирование соответствующей подписи модуля для каждого из модулей в принятых MPEG таблицах модулей; и

сравнение каждой подписи модуля в принятой MPEG таблице каталога с соответствующей подписью модуля,

сгенерированной в приемнике/декодере.

Следовательно, хотя данные, подлежащие загрузке, состоят из множества модулей для зашифровки модулей требуется только один процесс зашифровки; и только один процесс дешифровки требуется для обеспечения проверки подписей.

Эти особенности могут быть предоставлены независимо от аспектов изобретения с четвертого по седьмой. В соответствии с изложенным выше в восьмом аспекте данного изобретения предлагается способ загрузки множества модулей данных в приемник/декодер MPEG, содержащий следующие операции:

генерирование подписи модуля для каждого модуля подлежащих загрузке данных; форматирование модулей данных в виде соответствующих MPEG таблиц модулей;

генерирование каталога, содержащего идентификатор каждой MPEG таблицы модуля и соответствующую подпись;

генерирование подписи каталога для каталога;

шифрование подписи каталога с использованием секретного ключа;

форматирование каталога и зашифрованной подписи каталога в виде MPEG таблицы каталога;

трансляция MPEG таблиц каталога и модулей; и в приемнике/декодере:

прием MPEG таблиц каталога и модулей; дешифровка зашифрованной подписи каталога в принятой MPEG таблице каталога с использованием общедоступного ключа, соответствующего указанному секретному ключу;

генерирование подписи каталога для каталога в принятой MPEG таблице каталога; сравнение дешифрованной подписи каталога и подписи каталога, сгенерированной в приемнике/декодере;

генерирование соответствующей подписи модуля для каждого из модулей в принятых MPEG таблицах модулей; и

сравнение подписи каждого модуля в принятой MPEG таблице каталога с соответствующей подписью модуля, сгенерированной в приемнике/декодере.

Предпочтительно способ дополнительно включает операцию запрета или прекращения загрузки модуля данных, если подпись модуля в принятой MPEG таблице каталога и соответствующая подпись модуля, сгенерированная в приемнике/декодере для данного модуля, не совпадают друг с другом.

Описанный выше способ предпочтительно содержит также операцию запрета или прекращения загрузки данных, если по результатам сравнения указанная или каждая из дешифрованных подписей и сгенерированная подпись не совпадают друг с другом.

В соответствии с девятым аспектом данного изобретения предлагается приемник/декодер MPEG для осуществления части способа по четвертому аспекту изобретения, содержащий:

средство для приема MPEG таблиц;

средство для хранения множества общедоступных ключей и идентификатора для каждого общедоступного ключа; и

средство обработки, которое программируется таким образом, чтобы выбрать один из сохраненных общедоступных

ключей в соответствии с идентификатором ключа в принятой MPEG таблице; дешифровать зашифрованную подпись в принятой MPEG таблице с использованием выбранного общедоступного ключа для получения дешифрованной подписи; генерировать подпись для данных в принятой MPEG таблице; и сравнивать дешифрованную подпись и подпись, сгенерированную в приемнике/декодере для принятых данных.

Предпочтительно в качестве средства хранения ключей используется ПЗУ, и идентификатор для каждого из общедоступных ключей может быть определен через физическое расположение данного общедоступного ключа в средстве хранения ключа.

Приемник/декодер может дополнительно содержать область энергозависимой памяти, и в котором средство обработки выполнено с возможностью загрузки приложения, имеющего подпись, зашифрованную с использованием секретного ключа, имеющего заранее определенный идентификатор, выполнения приложения в приемнике/декодере с целью инициирования приема приемником/декодером дополнительного ключа, и сохранения дополнительного ключа в области энергозависимой памяти приемника/декодера.

Приемник/декодер может дополнительно содержать средство для приема такого дополнительного ключа, который предоставляется в приемник/декодер на месте, например параллельный порт, последовательный порт или устройство считывания смарт-карты приемника/декодера. Предпочтительно энергозависимая память обеспечивается посредством оперативной памяти. Опять-таки, если приемник/декодер имеет соединение с модемом, предпочтительно приемник/декодер выполнен так, чтобы он мог воспрепятствовать поступлению такого дополнительного ключа через модем.

Приемник/декодер может дополнительно содержать защищенную область памяти для хранения флага проверки допустимости для каждого из хотя бы некоторых общедоступных ключей, в котором средство обработки запрограммировано на поиск в защищенной области памяти флага проверки допустимости для выбранного общедоступного ключа, а также на запрет или завершение загрузки данных в случае, если найденный флаг не установлен.

Приемник/декодер может также дополнительно содержать защищенную область памяти для хранения флага проверки допустимости для секретного ключа, имеющего заранее заданный идентификатор ключа, и в котором средство обработки выполнено с возможностью при выполнении упомянутого приложения изменять этот флаг проверки допустимости и разрешать сохранение дополнительного ключа в зависимости от состояния этого флага.

Эта последняя особенность может быть предоставлена независимо от девятого аспекта данного изобретения. Соответственно, в десятом аспекте данного изобретения предлагается приемник/декодер MPEG для осуществления части способа по

п.17, содержащий:

средство для приема MPEG таблиц;
средство для хранения общедоступного ключа и идентификатора для указанного общедоступного ключа; и

5 защищенную область памяти для хранения флага проверки допустимости для общедоступного ключа; и
средство обработки, которое запрограммировано на поиск в защищенной области памяти приемника/декодера флага проверки допустимости для общедоступного ключа, соответствующего секретному ключу, указанному в принятой MPEG таблице, и, если найденный флаг установлен, дешифровку зашифрованной подписи в принятой MPEG таблице с использованием общедоступного ключа, соответствующего секретному ключу, указанному в принятой MPEG таблице, с целью получения дешифрованной подписи, генерирование подписи для данных в принятой MPEG таблице, и сравнение дешифрованной подписи и подписи, сгенерированной в приемнике/декодере для принятых данных.

Предпочтительно память для хранения флага(ов) проверки допустимости является перезаписываемой энергонезависимой памятью.

В случае, когда сохраняется множество таких общедоступных ключей, предпочтительно память для хранения флага(ов) проверки допустимости организована в виде битового массива.

30 Приемник/декодер в девятом или десятом аспекте данного изобретения может дополнительно содержать защищенную область памяти для хранения кода проверки допустимости, и в котором средство обработки запрограммировано на дешифровку кода проверки допустимости в такой принятой MPEG таблице, поиск сохраненного кода проверки допустимости и сравнение найденного кода проверки допустимости и дешифрованного кода проверки допустимости.

Эта последняя особенность может быть предоставлена независимо от девятого и десятого аспекта данного изобретения. Соответственно, в одиннадцатом аспекте данного изобретения предлагается

45 приемник/декодер MPEG, содержащий:
средство для приема MPEG таблиц;
средство для хранения общедоступного ключа и идентификатора для указанного общедоступного ключа;

50 защищенную область памяти для хранения кода проверки допустимости; и
средство обработки, запрограммированное на дешифровку зашифрованного кода проверки допустимости и подписи в принятых MPEG таблицах с использованием сохраненного

55 общедоступного ключа, соответствующего секретному ключу; поиск сохраненного кода проверки допустимости в защищенной области памяти; сравнение найденного кода проверки допустимости и дешифрованного кода проверки допустимости; генерирование подписи для данных в принятой MPEG таблице или упомянутой ее части; и сравнение дешифрованной подписи и подписи, сгенерированной в приемнике/декодере для принятых данных.

Предпочтительно средство обработки

запрограммировано на запрет или завершение загрузки данных в случае, если найденный код проверки допустимости и дешифрованный код проверки допустимости не совпадают друг с другом.

Предпочтительно память для хранения кодов проверки допустимости обеспечивается перезаписываемой энергонезависимой памятью и организована в виде битового массива.

Приемник/декодер из аспектов данного изобретения с девятого по одиннадцатый может дополнительно содержать защищенную область памяти для хранения хотя бы одного смещения, и в котором средство обработки может быть запрограммировано на дешифровку зашифрованного блока данных в принятой MPEG таблице, поиск упомянутого одного сохраненного смещения в защищенной области памяти и извлечение подписи из дешифрованного блока данных с использованием найденного смещения от начала дешифрованного блока данных.

Эта последняя особенность может быть предоставлена независимо от аспектов данного изобретения с девятого по одиннадцатый. Соответственно, в двенадцатом аспекте данного изобретения предлагается приемник/декодер MPEG, содержащий: средство для приема MPEG таблиц;

средство для хранения общедоступного ключа и идентификатора для указанного общедоступного ключа;

защищенную область памяти для хранения хотя бы одного смещения; и

средство обработки, запрограммированное на дешифровку зашифрованного блока данных в принятой MPEG таблице, используя сохраненный общедоступный ключ, соответствующий секретному ключу; поиск упомянутого сохраненного смещения в защищенной области памяти; извлечение подписи из дешифрованного блока данных с использованием упомянутого смещения от начала дешифрованного блока данных; генерирование подписи для данных в принятой MPEG таблице; и сравнение подписи, извлеченной из дешифрованного блока данных, и подписи, сгенерированной в приемнике/декодере для принятых данных.

Предпочтительно память для хранения смещения обеспечивается перезаписываемой энергонезависимой памятью.

В приемнике/декодере из аспектов данного изобретения с девятого по двенадцатый средство обработки может быть запрограммировано на генерирование соответствующей подписи модуля для каждого из модулей в принятых MPEG таблицах модулей и сравнение каждой подписи модуля в принятой MPEG таблице каталога с соответствующей подписью модуля, сгенерированной приемником/декодере.

Эта последняя особенность может быть предоставлена независимо от аспектов данного изобретения с девятого по двенадцатый. Соответственно, в тринадцатом аспекте данного изобретения предлагается приемник/декодер MPEG, содержащий:

средство для приема MPEG таблиц каталога и модулей;

средство для хранения общедоступного ключа и идентификатора для этого общедоступного ключа; и средство обработки, запрограммированное на дешифровку зашифрованной подписи каталога в принятой MPEG таблице каталога с использованием сохраненного общедоступного ключа, соответствующего секретному ключу; генерирование подписи каталога для каталога в принятой MPEG таблице каталога; сравнение дешифрованной подписи каталога и подписи каталога, сгенерированной приемником/декодере; генерирование соответствующей подписи модуля для каждого из модулей в принятых MPEG таблицах модулей; и сравнение каждой подписи модуля в принятой MPEG таблице каталога и соответствующей подписи модуля, сгенерированной приемником/декодере.

Предпочтительно средство обработки запрограммировано на запрет или аварийное завершение загрузки модуля данных, если подпись модуля в принятой MPEG таблице каталога и соответствующая подпись модуля, сгенерированная в приемнике/декодере, не совпадают друг с другом.

Предпочтительно в приемнике/декодере из аспектов данного изобретения с девятого по тринадцатый средство обработки запрограммировано на запрет или завершение загрузки данных в случае, если одна или каждая из дешифрованных подписей и сгенерированная подпись не совпадают друг с другом.

Теперь предпочтительные особенности данного изобретения будут описаны исключительно на примере с использованием прилагаемых чертежей, на которых:

на фиг.1 представлена общая архитектура системы цифрового телевидения;

на фиг.2 показана архитектура интерактивной системы в системе цифрового телевидения с фиг.1;

на фиг. 3 приведена функциональная схема интерфейса приемника/декодера, являющегося частью системы, представленной на фиг.1 и 2;

на фиг. 4 приведено схематическое изображение устройства дистанционного управления, используемого в системе цифрового телевидения;

фиг. 5 иллюстрирует расположение файлов в загружаемом в приемник/декодер модуле;

фиг.6 иллюстрирует взаимосвязь между компонентами потока битов MPEG;

на фиг.7 показано, как приложение может быть разбито на модули/таблицы, которые, в свою очередь, могут состоять из секций;

фиг.8 иллюстрирует содержимое модуля каталога;

фиг.9 иллюстрирует более подробно часть содержимого модуля каталога;

фиг. 10 иллюстрирует различные области памяти в приемнике/декодере системы телевидения.

Общая структура системы вещания и приема цифрового телевидения 1000 согласно данному изобретению приведена на фиг.1. Изобретение включает самую обычную систему цифрового телевидения 2000, которая использует известную систему сжатия MPEG-2 для передачи сжатых цифровых сигналов. Более подробно, устройство сжатия MPEG-2 2002 в центре

вещания принимает поток цифровых сигналов (обычно поток видеосигналов). Устройство сжатия 2002 подключается к мультиплексору и скремблеру 2004 с помощью канала 2006. Мультиплексор 2004 принимает множество входных сигналов, собирает один или несколько несущих потоков и передает сжатые цифровые сигналы в передатчик 2008 центра вещания через канал 2010, тип которого, естественно, может быть различным, включая каналы телекоммуникаций. Передатчик 2008 передает электромагнитные сигналы через канал "земля-спутник" 2012 на спутниковый ретранслятор 2014, где выполняется их обработка электронными средствами и вещание через виртуальный канал "спутник-земля" 2016 на наземный приемник 2018, обычно имеющий форму тарелки, принадлежащий конечному пользователю или арендуемый им. Сигналы, принимаемые приемником 2018, передаются в совмещенный приемник/декодер 2020, принадлежащий конечному пользователю или арендуемый им, и подключенный к телевизору 2022 конечного пользователя. Приемник/декодер 2020 декодирует сжатый MPEG-2 сигнал в телевизионный сигнал для телевизора 2022.

Система условного доступа 3000 подключается к мультиплексору 2004 и приемнику/декодеру 2020 и располагается частично в центре вещания и частично в декодере. Она позволяет конечному пользователю осуществлять доступ к вещательным передачам цифрового телевидения от одного или нескольких операторов вещания. В приемник/декодер 2020 может устанавливаться смарт-карта, которая может декодировать сообщения, относящиеся к коммерческим предложениям (одна или несколько телевизионных программ, продаваемых оператором вещания). С использованием декодера и смарт-карты пользователь может покупать передачи в режиме подписки или оплаты за просмотр (PPV).

Интерактивная система 4000, также подключенная к мультиплексору 2004 и приемнику/декодеру 2020 и также располагающаяся частично в центре вещания и частично в декодере, позволяет конечному пользователю взаимодействовать с различными приложениями через модемный обратный канал 4002.

На фиг. 2 приведена общая структура телевизионной интерактивной системы 4000 системы цифрового телевидения 1000 в соответствии с настоящим изобретением.

Например, интерактивная система 4000 позволяет конечному пользователю покупать товары по экранным каталогам, просматривать локальные новости и карты погоды по запросу и играть в игры, используя свой телевизор.

Интерактивная система 4000 содержит, вообще говоря, четыре основных элемента:

- средство разработки 4004 в центре вещания или в другом месте, позволяющее оператору вещания создавать, разрабатывать, отлаживать и тестировать приложения;

- сервер приложений и данных 4006 в центре вещания, соединенный со средством разработки 4004, для предоставления

оператору вещания возможности подготавливать, удостоверять подлинность и форматировать приложения и данные для отправления в мультиплексор и скремблер 2004 для вставки его в несущий поток MPEG-2 (обычно в его приватную секцию), подлежащий вещанию для конечного пользователя;

- виртуальную машину, содержащую подсистему реального времени (RTE - Real Time Engine) 4008, которая представляет собой исполняемый код, инсталлированный в приемнике/декодере 2020, принадлежащем конечному пользователю или арендуемом им, для обеспечения конечному пользователю возможности принимать, удостоверить подлинность, разворачивать и загружать приложения в рабочую память декодера 2020 для выполнения. Подсистема 4008 также выполняет резидентные приложения общего назначения. Подсистема 4008 не зависит от аппаратного обеспечения и операционной системы; и

- обратный модемный канал 4002 между приемником/декодером 2020 и сервером приложений и данных 4006 для подачи сигналов, указывающих серверу 4006 вставлять данные и приложения в несущий поток MPEG-2 по требованию конечного пользователя.

Телевизионная интерактивная система работает с использованием т.н. "приложений", которые управляют функционированием приемника/декодера и различными устройствами, входящими в его состав. Приложения представлены в подсистеме 4008 как т.н. "файлы ресурсов". "Модуль" - это набор файлов ресурсов и данных. "Том памяти" приемника/декодера - это пространство для хранения модулей. Модули могут загружаться в приемник/декодер 2020 из несущего потока MPEG-2.

Для загрузки данных используются физические интерфейсы приемника/декодера 2020. Как показано на фиг.3, декодер 2020 содержит, например, шесть устройств загрузки: тюнер потока MPEG 4028, последовательный интерфейс 4030, параллельный интерфейс 4032, модем 4034 и два устройства считывания карт 4036.

Применительно к данному описанию, приложение - это фрагмент компьютерного кода для управления высокоуровневыми функциями приемника/декодера 2020. Например, когда конечный пользователь позиционирует фокус устройства дистанционного управления 2026 (подробно показанный на фиг.4) на объекте кнопки, видимом на экране телевизора 2022, и нажимает клавишу подтверждения, выполняется последовательность инструкций, соответствующая этой кнопке.

Интерактивное приложение обеспечивает меню и исполняет команды по соответствующему запросу конечного пользователя и предоставляет данные в соответствии с назначением данного приложения. Приложения могут быть либо резидентными приложениями, т.е. хранящимися в ПЗУ (либо в FLASH памяти, либо другой энергонезависимой памяти) приемника/декодера 2020, либо передающимися путем вещания и загружаемыми в ОЗУ (или FLASH) декодера 2020.

Примерами приложений являются:

- Приложение инициализации. Приемник/декодер 2020 снабжен резидентным приложением инициализации, которое является адаптируемым набором модулей (более подробно этот термин поясняется ниже) и позволяет приемнику/декодеру 2020 быть непосредственно готовым к работе в среде MPEG-2. Это приложение предоставляет базовые функции, которые могут быть при необходимости модифицированы оператором вещания. Оно предоставляет также интерфейс между резидентными приложениями и загружаемыми приложениями.

- Приложение запуска. Приложение запуска позволяет выполняться в приемнике/декодере 2020 любому приложению, либо загружаемому, либо резидентному. Это приложение работает как программа начальной загрузки, выполняемая при поступлении услуги для того, чтобы запустить приложение. Приложение запуска загружается в оперативную память и, следовательно, может быть легко обновлено. Оно может быть сконфигурировано таким образом, что интерактивные приложения, доступные по разным каналам, могут быть выбраны и выполнены либо сразу же после загрузки, либо после предварительной загрузки. В случае предварительной загрузки приложение загружается в память 2024 и активируется приложением запуска по необходимости.

- Руководство по программам. Руководство по программам - это интерактивное приложение, которое предоставляет полную информацию по программам. Например, оно может содержать информацию, скажем, о программе телевизионных передач на неделю, предоставляемых каждым каналом из пакета ("букета") каналов цифрового телевидения. Нажатием на клавишу устройства дистанционного управления 2026 конечный пользователь получает доступ к добавочному экрану, который с перекрытием накладывается на передачу, которая демонстрируется в данный момент на экране телевизора 2022. Этот добавочный экран представляет собой средство просмотра, предоставляющее информацию о текущих и последующих передачах каждого канала букета цифрового ТВ. С помощью нажатия на другую клавишу устройства дистанционного управления 2026 конечный пользователь получает доступ к приложению, которое выдает на экран информацию о программе передач на неделю. Конечный пользователь может также производить поиск и сортировку программ по простым и индивидуальным критериям. Конечный пользователь может также получать доступ непосредственно к выбранному каналу.

- Приложение PPV (PPV - Pay Per View, оплата производится за каждую просмотренную передачу). Приложение PPV - это интерактивная услуга, имеющаяся на каждом PPV канале букета цифрового ТВ с системой условного доступа 3000. Конечный пользователь может получать доступ к указанному приложению с использованием ТВ меню или браузера каналов. Кроме того, это приложение запускается автоматически, как

только на PPV канале обнаруживается PPV передача. Затем конечный пользователь может купить текущую программу либо с помощью его дочерней смарт-карты 3020, или с помощью сервера связи 3022 (с использованием модема, телефона и DTMF кодов (кодов тонового набора), MINITEL, или другим подобным образом). Это приложение может быть резидентным в ПЗУ приемника/декодера 2020 или загружаться в оперативную память приемника/декодера 2020.

- Приложение загрузки в ПК. Конечный пользователь может по запросу загружать компьютерное программное обеспечение с использованием приложения загрузки в ПК.

- Приложение просмотра журнала. Приложение просмотра журнала обеспечивает периодическое вещание видеоизображений с обеспечением пользователю возможности навигации с помощью кнопок на экране.

- Приложение телевикторины. Приложение телевикторины предпочтительно синхронизируется с вещаемой программой телевикторины. Например, на экран телевизора 2022 выдаются несколько возможных ответов, и пользователь может выбрать ответ с помощью устройства дистанционного управления 2026. Приложение телевикторины может информировать пользователя, правилен его ответ или нет, и может подсчитывать набранные пользователем очки.

- Приложение дистанционных покупок. В одном из примеров приложения дистанционных покупок предложения товаров к продаже транслируются на приемник/декодер 2020 и затем выдаются на экран телевизора 2022. С помощью устройства дистанционного управления пользователь может выбрать для покупки какой-либо конкретный товар. Заказ на этот товар передается через обратный модемный канал 4002 в сервер приложений и данных 4006 или в отдельную систему продаж, номер телефона которой был загружен в приемник/декодер, возможно - с поручением дебетовать счет кредитной карты, которая установлена в одном из устройств считывания карты 4036 приемника/декодера 2020.

- Приложение дистанционных банковских услуг. В одном из примеров приложения дистанционных банковских услуг пользователь устанавливает банковскую карту в одно из устройств считывания карты 4036 приемника/декодера 2020. Приемник/декодер 2020 звонит банку пользователя с использованием номера телефона, записанного в банковской карте пользователя или хранящегося в приемнике/декодере, и затем приложение предоставляет набор средств, которые могут быть выбраны с помощью устройства дистанционного управления 2026, например, для загрузки по телефонной линии отчета о состоянии счета, перевода средств с одного счета на другой, запрашивания чековой книжки и т.д.

- Приложение Интернет-браузера. В одном примере приложения Интернет-браузера инструкции от пользователя, такие как запрос просмотра веб-страницы, имеющей конкретный URL, вводятся с использованием устройства дистанционного управления 2026,

и они пересылаются по обратному модемному каналу 4002 в сервер приложений и данных 4006. Соответствующая веб-страница затем включается в транслируемые из центра вещания данные, принимаемые приемником/декодером 2020 через канал "земля-спутник" 2012, ретранслятор 2014 и канал "спутник-земля" 2016, и затем выдается на экран телевизора 2022.

Приложения сохраняются в ячейках памяти приемника/декодера 2020 и представляются в виде файлов ресурсов. Под файлами ресурсов понимаются файлы библиотек описаний графических объектов, файлы библиотек блоков переменных, файлы последовательностей команд, файлы приложений и файлы данных.

Файлы библиотек описаний графических объектов описывают экраны, человеко-машинный интерфейс приложения. Файлы библиотек блоков переменных описывают структуры данных, которыми оперирует приложение. Файлы последовательностей команд описывают функциональные действия, выполняемые приложением. Файлы приложений предоставляют точки входа для приложений.

Приложения, составляемые таким способом, могут использовать файлы данных, такие как файлы библиотек пиктограмм, файлы изображений, файлы шрифтов, файлы таблиц цветов и файлы текстов ASCII. Интерактивное приложение может также получать оперативные данные, задействуя входы и/или выходы.

Подсистема 4008 загружает в свою память только те файлы ресурсов, которые необходимы ей в данное время. Эти файлы ресурсов считываются из файлов библиотек описаний графических объектов, файлов последовательностей команд и файлов приложений; файлы библиотек блоков переменных записываются в память после вызова процедуры загрузки модулей и остаются там до тех пор, пока не будет произведен специальный вызов процедуры выгрузки модулей.

Со ссылкой на фиг.5 модуль 4010, как например модуль дистанционных покупок, представляет собой набор файлов ресурсов и данных, содержащий следующее:

один файл приложения 4012; неопределенное количество файлов библиотек описаний графических объектов 4014;

неопределенное количество файлов библиотек блоков переменных 4016;

неопределенное количество файлов последовательностей команд 4018; и если необходимо, файлы данных 4020, такие как файлы библиотек пиктограмм, файлы изображений, файлы шрифтов, файлы таблиц цветов и файлы текстов ASCII.

Идея использования модулей 4010 вместе с идеей загрузки небольших фрагментов кода обеспечивают легкость наращивания приложений. Они могут загружаться в постоянную флэш-память декодера 2020 как резидентное программное обеспечение или вещаться с целью загрузки в оперативную память декодера 2020 только в случае возникновения потребности в них у пользователя.

Для загрузки модуля 4010 из несущего сигнала сначала загружается каталог,

доступный из несущего сигнала. Этот каталог представляет собой просто список имен модулей 4010, которые могут быть загружены из несущего сигнала. Как только каталог загружен, приложение может загрузить один или несколько модулей 4010. В случае MPEG потока каталог передается в одной MPEG таблице. Далее один модуль 4010 передается в одной MPEG таблице. В случае модулей, транслируемых в тюнер MPEG 4028, используется длинный MPEG-2 формат с длинным заголовком и CRC-кодом. Также обстоит ситуация и с пятью

другими интерфейсами (последовательный порт 4030, параллельный порт 4032, модем 4034 и два устройства считывания карты 4036), за исключением случая, когда используется "короткий" MPEG формат с коротким заголовком, и CRC не используется.

Как показано, в частности, на фиг.6, и как является известным, поток битов MPEG-2 включает таблицу доступа к программам (PAT) 10, имеющую идентификатор пакета (PID), равный 0. PAT содержит ссылки на PID таблиц распределения программ (PMT - Programme Map File) 12 ряда программ. Каждая PMT содержит ссылки на PID в потоках аудио MPEG таблиц 14 и видео MPEG таблиц 16 для данной программы. Пакет, имеющий идентификатор PID, равный 0, то есть таблица доступа к программам 10, предоставляет точку входа для обращения ко всей MPEG информации.

Для того чтобы загружать приложения и данные для них, определяются два новых типа потоков, и соответствующая PMT содержит также ссылки на идентификаторы PID в потоках MPEG таблиц приложений 18 (или их секций) и MPEG таблиц данных 20 (или их секций).

Как показано на фиг.7, для загрузки приложения 22 указанное приложение разделяется на модули 24, каждый из которых образуется MPEG-таблицей, причем некоторые из модулей состоят из одной секции 18, и некоторые могут состоять из множества секций 18. Типовая секция 18 имеет заголовок 26, который содержит однобайтовый идентификатор таблицы ("TID") 28, номер секции 30 для данной секции в таблице, общее число секций 32 в данной таблице и двухбайтовое расширение TID 34. Каждая секция содержит также данные 36 и CRC 38. Для конкретного модуля/таблицы 24 все секции 18, образующие эту таблицу 24, имеют одинаковый TID 28 и одинаковое расширение TID 34. Для конкретного приложения 22 все таблицы 24, составляющие это приложение 22, имеют одинаковый TID 28, но разные соответствующие расширения TID.

Для каждого приложения 22 существует одна такая MPEG таблица 24, изображенная более подробно на фиг.8, которая используется в качестве каталога. Таблица каталога 40 содержит заголовок 26, данные каталога 42, идентификатор ключа 44, зашифрованную подпись 46 и CRC 38. Из сказанного выше следует, что таблица каталога 40 имеет в заголовке 26 тот же идентификатор TID 28, что и остальные модули/таблицы 24, образующие приложение. Однако таблица каталога имеет заранее определенное расширение TID 34, равное 0, а

все остальные модули 24 имеют ненулевые расширения TID. Заголовок также включает для таблицы каталога 40 номер версии 48. Данные каталога 42 для каждого из остальных модулей/таблиц 24, образующих приложение 22, включают имя 50 данного модуля, расширение TID 34 для данного модуля и подпись 52 данного модуля. Данные каталога 42 могут также включать для каждого из остальных модулей/таблиц 24 размер данного модуля и номер версии модуля.

Возвращаясь к фиг.6, во время работы, RAT 10, PMT 12 и компоненты потока таблиц приложений и данных 18, 20 периодически транслируются, и, по мере необходимости, обновляются. Каждое приложение, которое транслируется, имеет соответствующий заранее определенный TID 28. Чтобы загрузить приложение, в приемник/декодер 2020 загружается MPEG таблица, имеющая соответствующий TID и расширение TID, равное 0. Это, таким образом, и есть таблица каталога 40 для требуемого приложения. Затем данные каталога обрабатываются приемником/декодером с целью определения расширений TID 34 таблиц модулей, составляющих требуемое приложение, и затем может быть загружена любая необходимая таблица модуля, имеющая тот же TID, что и таблица каталога, и расширение TID, определяемое из данных каталога.

Приемник/декодер 2020 выполнен с возможностью осуществлять проверку таблицы каталога на наличие в ней любых обновлений. Это может быть выполнено путем периодической повторной загрузки таблицы каталога, например, каждые 30 секунд, каждую минуту или пять минут, и сравнения номера версии новой загруженной таблицы каталога с номером версии ранее загруженной таблицы каталога. Если номер новой загруженной версии более поздний, то модули, относящиеся к предыдущей таблице каталога, или любые такие модули, для которых имеются более поздние номера версий, деинсталлируются, и производится загрузка и установка модулей более поздних версий. В альтернативном варианте входной поток битов фильтруется с использованием маски, в которой значения TID задано равным TID приложения, расширения TID - 0, и номера версии - на единицу большим, чем номер версии загруженного в данный момент каталога. В соответствии с этим приращение номера версии может быть обнаружено, и как только оно обнаружено, загружается каталог и приложение обновляется, как описано выше. Подробное описание такой фильтрации содержится в одновременно рассматриваемой заявке (номер дела поверенного PDC/ASB/19716). Если приложение должно быть удалено, транслируется пустой каталог со следующим номером версии, но без указания в каталоге каких-либо модулей. В ответ на прием такого пустого каталога приемник/декодер 2020 запрограммирован деинсталлировать приложение.

Ниже подробно описано использование подписи и шифрования для таблиц приложения.

Как описано выше, запись о каждом модуле в таблице каталога 40 содержит подпись модуля. Подпись модуля генерируется с использованием известного

алгоритма генерирования подписи MD5 на основе данных в соответствующей таблице модуля.

Кроме того, таблица каталога 40 содержит зашифрованную подпись 46, которая сгенерирована способом, который будет описан ниже со ссылкой на фиг.9. Формируется блок данных 54 размером 64 байта. Первый байт 56 равен нулю. Следующие три байта 58 могут быть пустыми или содержать произвольные данные. Следующие восемь байтов 60 образуют битовый массив проверки допустимости приложения, который будет описан ниже. Последние четыре байта 62 являются резервными. Оставшиеся 48 байтов содержат 16-байтовую подпись 64, которая начинается со смещения, принимающего значения от 0 до 31 байта после первого байта, следующего после битового массива проверки допустимости 60. Фиктивные данные 66 вставляются между битовым массивом проверки допустимости приложения 60 и подписью 64 и/или между подписью 64 и резервными байтами 62. Подпись 64 получается с использованием известного алгоритма генерирования подписи MD5 на основе данных каталога 42 в таблице каталога 40. Затем блок 54 зашифровывается с использованием известного алгоритма шифрования и некоторого секретного ключа с целью получения зашифрованной подписи и битового массива проверки допустимости приложения 46. Этот блок данных 46 включается в таблицу каталога 40, и в качестве идентификатора ключа 44 в таблицу каталога 40 включается 1-байтовый идентификатор секретного ключа, который использовался для шифрования блока.

В итоге генерирование приложения и его трансляция включают следующие операции:

- генерирование приложения в виде множества модулей;
- запоминание для приложения заранее заданного TID 28;
- назначение имен и ненулевых расширений TID 34 для модулей;
- форматирование каждого модуля в виде MPEG таблицы 24 или секций 18 MPEG таблицы;
- генерирование подписи MD5 52 для каждого модуля;
- генерирование данных каталога 42;
- генерирование подписи MD5 64 для каталога;
- выбор битового массива проверки допустимости приложения 60;
- выбор смещения;
- генерирование блока 54;
- шифрование блока 54 с использованием шифрования с выбранным секретным ключом;
- генерирование MPEG таблицы каталога 40 с назначенным TID 28, нулевым расширением TID, данными каталога 42, идентификатором ключа 44 и зашифрованной подписью 46;
- трансляция таблицы каталога 40 и таблиц модулей 24 или секций 18.

Ниже описывается функционирование приемника/декодера 2020 при обработке подписей и дешифровке во время загрузки приложения. Как показано на фиг.10, приемник/декодер 2020 содержит электрически стираемое ППЗУ 68, ПЗУ 70 и оперативную память 72. Электрически

стираемое ПЗУ содержит защищенную область 74, которая используется виртуальной машиной, запись в которую может производить только виртуальная машина (но не обычное приложение). Защищенная область 74 содержит битовый массив проверки допустимости ключа 76 размером 16 или 256 битов, битовый массив проверки допустимости приложения 78 из 64 битов и битовый массив смещения 80 из 32 битов. ПЗУ 70 содержит, в одной реализации, шестнадцать общедоступных ключей 82, и в этом случае используется 16-битовый массив проверки допустимости ключа, либо, в другой реализации, 256 общедоступных ключей, и в этом случае используется 256-битовый массив проверки допустимости ключа. Общедоступные ключи идентифицируются по их физическому расположению в ПЗУ 70, или, как альтернатива, они могут быть включены в справочную таблицу, в которой идентификатору конкретного ключа будет соответствовать соответствующий общедоступный ключ. Оперативная память 72 может использоваться для хранения временного ключа 84.

Как упоминалось выше, когда необходимо загрузить приложение, в первую очередь загружается таблица каталога, содержащая заранее заданный TID для этого приложения и нулевое расширение TID. Затем из таблицы каталога извлекается идентификатор ключа 44 и производится проверка битового массива проверки допустимости ключа 76 в защищенной области памяти 74, установлен ли бит, соответствующий извлеченному идентификатору ключа 44. Если нет, то загрузка приложения прекращается. Однако, если соответствующий бит установлен, из ПЗУ 70 выбирается общедоступный ключ 82, соответствующий извлеченному идентификатору ключа 44. Затем для дешифровки зашифрованного блока 46 в таблице каталога 40 для получения блока 54 используется выбранный общедоступный ключ и известный процесс дешифровки. Затем из дешифрованного блока 54 извлекается битовый массив проверки допустимости приложения 60 и над его содержимым и содержимым битового массива проверки допустимости приложения 78, хранящегося в защищенной памяти 74, выполняется операция AND. Если результат выполнения операции AND нулевой, то загрузка приложения прекращается. Однако, если результат выполнения операции AND ненулевой, производится поиск установленного бита смещения, содержащегося в битовом массиве смещения 80 в защищенной памяти 74, или, если установлен более чем один бит смещения, производится поиск каждого бита смещения по очереди, и из дешифрованного блока 54 извлекаются 16 байтов данных, начиная с найденного смещения от первого байта после битового массива проверки допустимости приложения 60. Для одного или каждого найденного смещения эти 16 байтов рассматриваются как подпись, транслируемая с таблицей каталога 40. Подпись данных каталога 42 таблицы каталога 40 вычисляется с использованием известного процесса MD5, и эта вычисленная подпись сравнивается с подписью, извлеченной из блока 54. Если две подписи для одного или каждого найденного

смещения не совпадают, то загрузка приложения прекращается. Однако, если одна из подписей подходит, то загрузка модулей, указанных в данных каталога 42, может производиться. Как упомянуто выше, чтобы загрузить конкретный модуль, из данных каталога 42 получают расширение TID для данного модуля и загружается MPEG таблица 24 или секция 18 с тем же TID, что и у таблицы каталога, и с полученным расширением TID. Как только загрузится MPEG таблица модуля, приемник/декодер 2020 вычисляет подпись загруженной таблицы с использованием известного процесса MD5 и затем сравнивает эту вычисленную подпись с подписью, содержащейся в соответствующем элементе данных каталога. Если подписи совпадают, то модуль принимается, если не совпадают - модуль отвергается.

Таким способом могут быть загружены все модули приложения, и приложение может быть выполнено приемником/декодером.

После описания особенностей операции загрузки, обычно используемых в режиме загрузки, опишем теперь некоторые особенности настроек приемника/декодера 2020 и изменения его настроек.

Приемник/декодер программируется так, что защищенная область памяти может быть изменена, но только приложением, которое загружается с использованием одного специального идентификатора ключа, например ключа 15, и специального смещения, например, нуль байтов от первого байта после битового массива проверки допустимости приложения 60. Необходимость в изменении защищенной памяти 74 может возникнуть, например, если два оператора, которые использовали один и тот же общедоступный ключ, принимают решение использовать различные общедоступные ключи, или, если содержимое секретного ключа было открыто, то в этом случае соответствующий общедоступный ключ может быть отмечен как недействительный в битовом массиве проверки допустимости ключа 76.

Приемник/декодер 2020 может быть устроен так, чтобы один из указанных ключей, например ключ 15, был всегда доступен, и в этом случае для такого ключа не требуется бита в битовом массиве проверки допустимости ключа 76. Соответственно, этот бит может быть использован для другой цели. В частности, может быть предусмотрено, что приложение, подлинность которого удостоверяется ключом 15, устанавливает этот конкретный бит в 1, и в этом случае приемник/декодер программируется так, чтобы разрешить загрузку в оперативную память 72 временного ключа 84, но только через последовательный интерфейс 4030, параллельный интерфейс 4032 или одно из двух устройств считывания карты 4036. Эта возможность может использоваться, например, изготовителем приемника/декодера 2020, которому может быть предоставлено для использования приложение с целью разрешить загрузку временного ключа в приемник/декодер 2020, с тем, чтобы он мог быть протестирован.

Описанная выше методика шифрования и подписания обеспечивают ряд важных возможностей. В частности:

приложение может быть загружено только тогда, когда приемник/декодер 2020 имеет сохраненный в памяти общедоступный ключ, соответствующий идентификатору ключа 44 в загруженной таблице каталога;

для всех ключей, за исключением одного, приложение может быть загружено с использованием некоторого ключа только в том случае, если битовый массив проверки допустимости ключа 76 в памяти приемника/декодера 2020 установлен так, чтобы разрешить использование данного ключа;

приложение может быть загружено только тогда, когда установленный бит в битовом массиве смещения 80, хранящемся в памяти приемника/декодера 2020, соответствует смещению, используемому при генерировании таблицы каталога;

приложение может быть загружено только тогда, когда битовый массив проверки допустимости приложения 78 в памяти приемника/декодера 2020 установлен таким образом, что разрешается загрузка приложения;

приложение может быть загружено только если таблица каталога не была повреждена после того, как была первоначально сгенерирована ее подпись;

каждый модуль приложения может быть загружен только если соответствующая таблица модуля не была повреждена после того, как была первоначально сгенерирована ее подпись;

только одна операция шифрования необходима для подготовки приложения к загрузке, даже если приложение состоит из нескольких MPEG таблиц, и в приемнике/декодере для загрузки всего приложения необходима только одна операция дешифровки;

можно использовать несколько ключей, так что различные провайдеры услуг могут иметь разные секретные ключи;

может использоваться временный ключ, например, изготовителем, для целей тестирования.

Очевидно, что настоящее изобретение было описано выше исключительно в виде примера, и возможны различные модификации в пределах данного изобретения.

Каждая особенность, изложенная в описании, а также (где это уместно) пункты формулы и фигуры могут быть предоставлены независимо или в соответствующем сочетании.

В вышеупомянутых предпочтительных вариантах реализации некоторые средства предлагаемого изобретения реализованы с использованием программного обеспечения. Однако опытному специалисту, конечно, понятно, что любые эти средства могут быть реализованы аппаратно. Далее, понятно, что функции, выполняемые аппаратными средствами, программное обеспечение компьютера и тому подобное выполняются на или с использованием электрических и им подобных сигналов.

Перекрестные ссылки выполнены на наши совместно рассматриваемые заявки с той же самой датой подачи и озаглавленные как "Генерирование сигналов и вещание" (номер дела поверенного PC/ASD/19707), "Смарт-карта для использования в приемнике

зашифрованных вещательных сигналов и приемник" (номер дела поверенного PC/ASD/19708), "Система вещания и приема и система условного доступа для нее" (номер дела поверенного PC/ASD/19710), "Загрузка компьютерного файла из передатчика через приемник/декодер в компьютер" (номер дела поверенного PC/ASD/19711), "Трансляция и прием телевизионных программ и других данных" (номер дела поверенного PC/ASD/19712), "Загрузка данных" (номер дела поверенного PC/ASD/19713), "Организация памяти компьютера" (номер дела поверенного PC/ASD/19714), "Разработка системы управления телевидением и радио" (номер дела поверенного PC/ASD/19715), "Извлечение разделов данных из потока транслируемых данных" (номер дела дела поверенного PC/ASD/19716), "Система управления доступом" (номер дела поверенного PC/ASD/19717), "Система обработки данных" (номер дела поверенного PC/ASD/19718), "Система вещания и приема, а также приемник/декодер и удаленный контроллер для нее" (номер дела поверенного PC/ASD/19720). Раскрытие содержимого этих документов включено сюда посредством ссылок. Список заявок включает и предлагаемое изобретение.

Формула изобретения:

1. Способ загрузки по меньшей мере части приложения в приемник/декодер MPEG, включающий разделение приложения на множество модулей, отличающийся тем, что он содержит следующие операции: форматирование каждого модуля в виде соответствующей MPEG таблицы, причем упомянутые таблицы имеют одинаковый идентификатор таблицы (TID) и соответствующие разные расширения идентификатора таблицы (TID-расширения), отличные от одного заранее определенного TID-расширения, генерирование MPEG таблицы каталога для упомянутых модулей, имеющей тот же упомянутый TID и упомянутое заранее определенное TID-расширение, при этом каталог содержит для каждого модуля имя данного модуля и соответствующее TID-расширение, циклическая трансляция упомянутых MPEG таблицы каталога и MPEG таблиц модулей в потоке битов MPEG, и в приемнике/декодере MPEG: прием упомянутого потока битов MPEG, загрузка той MPEG таблицы, которая имеет упомянутое заранее определенное TID-расширение, с тем чтобы загрузить MPEG таблицу каталога, определение из содержимого упомянутой MPEG таблицы каталога TID-расширений MPEG таблиц модулей, и загрузка по меньшей мере одной из MPEG таблиц модулей, имеющих тот же самый TID, что и загруженная MPEG таблица каталога, и TID-расширение, определенное из загруженной MPEG таблицы каталога.

2. Способ по п. 1, дополнительно включающий следующие операции: включение в транслируемую MPEG таблицу каталога идентификатора ее версии, и в приемнике/декодере: определение того, является ли версия транслируемой в данный момент MPEG таблицы каталога более новой, чем версия загруженной на данный момент MPEG таблицы каталога, и, если это так, повторение операций загрузки MPEG таблицы

каталога, определения TID-расширений и загрузки по меньшей мере одной из MPEG таблиц модулей.

3. Способ по п. 1 или 2, в котором по меньшей мере одна из упомянутых MPEG таблиц модулей отформатирована в виде множества MPEG секций, которые в потоке битов MPEG транслируются отдельно, при этом каждая из упомянутых MPEG секций содержит в ее заранее определенной части идентификатор положения данной MPEG секции в упомянутой MPEG таблице и указание количества секций в упомянутой MPEG таблице.

4. Приемник/декодер MPEG для загрузки из потока битов MPEG по меньшей мере части приложения, включающего в себя множество модулей, каждый из которых отформатирован в виде соответствующей MPEG таблицы, причем упомянутые таблицы имеют одинаковый идентификатор таблицы (TID) и соответствующие разные расширения идентификатора таблицы (TID-расширения), отличные от одного заранее определенного TID-расширения, причем упомянутый поток битов MPEG включает в себя MPEG таблицу каталога для упомянутых модулей, имеющую тот же TID и упомянутое заранее определенное TID-расширение и содержащую, для каждого модуля, имя данного модуля и соответствующее TID-расширение, содержащий приемник для приема упомянутого потока битов MPEG и средство хранения, отличающийся тем, что он также содержит средство обработки, которое программируется таким образом, чтобы инициировать загрузку в упомянутое средство хранения той из принимаемых MPEG таблиц, которая имеет упомянутое заранее определенное TID-расширение, определять из содержимого этой MPEG таблицы каталога TID-расширения MPEG таблиц модулей и инициировать загрузку в упомянутое средство хранения по меньшей мере одной из MPEG таблиц модулей, имеющих тот же TID, что и загруженная MPEG таблица каталога, и TID-расширение, определенное из загруженной MPEG таблицы каталога.

5. Приемник/декодер по п. 4 для использования в способе по п. 2, в котором средство обработки программируется таким образом, чтобы определять, является ли версия принимаемой в данный момент MPEG таблицы каталога более новой, чем версия загруженной на данный момент MPEG таблицы каталога и, если это так, повторять загрузку MPEG таблицы каталога, определение TID-расширений и загрузку по меньшей мере одной из MPEG таблиц модулей.

6. Приемник/декодер по п. 4 или 5 для использования в способе по п. 3, в котором средство обработки программируется таким образом, чтобы инициировать циклическую загрузку MPEG секций в средство хранения до тех пор, пока средство обработки не определит по идентификаторам положения секций и указанию количества секций, содержащимся в загруженных секциях, что все секции уже загружены.

7. Приемник/декодер по любому из пп. 4-6, дополнительно содержащий параллельный порт и/или последовательный порт, выполненные с возможностью приема приложения, отформатированного в виде по

меньшей мере одной MPEG таблицы.

8. Система трансляции MPEG, содержащая средство для разделения приложения, подлежащего загрузке в приемник/декодер MPEG, на множество модулей, отличающаяся тем, что она содержит средство для форматирования упомянутые каждого из модулей в виде соответствующей MPEG таблицы, причем упомянутые таблицы имеют одинаковый TID и соответствующие различные TID-расширения, отличные от заранее определенного TID-расширения, средство для генерирования MPEG таблицы каталога для упомянутых модулей, имеющей тот же упомянутый TID и упомянутое заранее определенное TID-расширение, при этом упомянутый каталог для каждого модуля содержит имя этого модуля и соответствующее TID-расширение и средство для циклической трансляции упомянутых MPEG таблицы каталога и MPEG таблиц модулей в потоке битов MPEG.

9. Система по п. 8, дополнительно содержащая средство для генерирования идентификатора версии для MPEG таблицы каталога, и в которой средство генерирования MPEG таблицы каталога выполнено с возможностью добавления в MPEG таблицу каталога сгенерированного идентификатора ее версии.

10. Система по п. 8 или 9, в которой упомянутое средство форматирования модулей выполнено с возможностью форматирования по меньшей мере одной из MPEG таблиц модулей в виде множества MPEG секций, каждая из которых в своей заранее определенной части содержит идентификатор положения этой MPEG секции в упомянутой MPEG таблице и указание количества секций в упомянутой MPEG таблице.

11. Способ загрузки данных в приемник/декодер MPEG, включающий генерирование подписи для упомянутых данных, подлежащих загрузке, отличающийся тем, что он включает такие операции: шифрование упомянутой подписи с использованием секретного ключа, форматирование упомянутых подлежащих загрузке данных, упомянутой зашифрованной подписи и идентификатора секретного ключа, использованного для шифрования упомянутой подписи, в виде MPEG таблицы, трансляция упомянутой MPEG таблицы, и в приемнике/декодере: сохранение множества общедоступных ключей, прием упомянутой MPEG таблицы, выбор одного из упомянутого множества общедоступных ключей, в соответствии с упомянутым идентификатором секретного ключа, содержащимся в упомянутой принятой MPEG таблице, дешифровка зашифрованной подписи, содержащейся в упомянутой принятой MPEG таблице, с использованием выбранного общедоступного ключа, для получения дешифрованной подписи, генерирование подписи для упомянутых данных, содержащихся в упомянутой принятой MPEG таблице, и сравнение дешифрованной подписи и подписи, сгенерированной приемником/декодером для упомянутых принятых данных.

12. Способ по п. 11, дополнительно включающий операции загрузки в

приемник/декодер приложения, имеющего подпись, зашифрованную с использованием секретного ключа, имеющего некоторый заранее определенный идентификатор, выполнения упомянутого приложения в приемнике/декодере, для обеспечения приема приемником/декодером некоторого временного ключа, сохранения упомянутого временного ключа в области энергозависимой памяти приемника/декодера.

13. Способ по п. 12, в котором при выполнении упомянутого приложения упомянутый временный ключ предоставляется приемнику/декодеру на месте.

14. Способ по п. 13, в котором упомянутый временный ключ предоставляется приемнику/декодеру через параллельный порт, последовательный порт или устройство считывания смарт-карты приемника/декодера.

15. Способ по любому из пп. 11-14, дополнительно включающий в приемнике/декодере операции нахождения в защищенной области памяти приемника/декодера флага проверки допустимости для выбранного общедоступного ключа и запрета или прекращения загрузки упомянутых данных в случае, если найденный флаг не установлен.

16. Способ по любому из пп. 12-14, дополнительно включающий операции в приемнике/декодере нахождения в защищенной области памяти приемника/декодера флага проверки допустимости для выбранного общедоступного ключа и запрета или прекращения загрузки упомянутых данных, если найденный флаг не установлен, причем упомянутый секретный ключ, имеющий идентификатор, имеет в защищенной области памяти приемника/декодера флаг проверки допустимости, который может быть изменен упомянутым приложением, а возможность приема упомянутого временного ключа определяется в зависимости от состояния этого флага проверки допустимости.

17. Способ по любому из пп. 11-16, дополнительно включающий следующие операции: генерирование кода допустимости для упомянутых подлежащих загрузке данных, который зашифровывается вместе с подписью при выполнении упомянутой операции шифрования и дешифруется вместе с подписью при выполнении упомянутой операции дешифровки, нахождение сохраненного кода проверки допустимости в защищенной области памяти приемника/декодера, сравнение найденного кода проверки допустимости и дешифрованного кода проверки допустимости.

18. Способ по п. 17, дополнительно содержащий операцию запрета или прекращения загрузки упомянутых данных в случае, если по результатам упомянутого сравнения кодов проверки допустимости упомянутые найденный код проверки допустимости и дешифрованный код проверки допустимости не совпадают друг с другом.

19. Способ по любому из пп. 11-18, в котором упомянутая подпись упомянутых подлежащих загрузке данных зашифровывается в блоке данных, с

некоторым выбранным смещением между началом этого блока данных и началом упомянутой подписи, и зашифрованный блок данных дешифруется при выполнении упомянутой операции дешифровки в приемнике/декодере, и дополнительно включающий операции в приемнике/декодере нахождения по меньшей мере одного значения смещения, хранящегося в защищенной области памяти приемника/декодера, а также извлечения подписи из упомянутого дешифрованного блока данных с использованием упомянутого одного найденного значения смещения от начала дешифрованного блока данных.

20. Способ по п. 19, в котором упомянутая защищенная область памяти содержит по меньшей мере два таких сохраненных значения смещения, и который, если по результатам упомянутой операции сравнения упомянутые извлеченная подпись и сгенерированная подпись не совпадают, включает дополнительную операцию повторения операций нахождения, извлечения и сравнения с использованием другого из упомянутых сохраненных значений смещения.

21. Способ по п. 19 или 20, в котором упомянутый блок данных включает в себя, помимо упомянутой подписи, фиктивные или произвольные данные.

22. Способ по любому из пп. 11-21, в котором упомянутые данные загружаются в виде множества модулей данных, включающий следующие операции: генерирование подписи для каждого модуля данных, подлежащего загрузке, форматирование упомянутых модулей данных в виде соответствующих MPEG таблиц модулей, генерирование каталога, содержащего идентификатор каждой MPEG таблицы модуля и соответствующую подпись, причем упомянутый каталог является объектом операции генерирования подписи по любому из пп. 11-21, и в приемнике/декодере: генерирование соответствующей подписи для каждого из упомянутых модулей, содержащихся в принятых MPEG таблицах модулей, и сравнение каждой из подписей для модулей, содержащихся в принятой MPEG таблице каталога, с соответствующей подписью для модуля, сгенерированной в приемнике/декодере.

23. Способ по п. 22, дополнительно включающий операцию запрета или прекращения загрузки такого модуля упомянутых данных, если подпись для упомянутого модуля, содержащаяся в принятой MPEG таблице каталога, и соответствующая подпись, сгенерированная для данного модуля в приемнике/декодере, не совпадают друг с другом.

24. Способ по любому из пп. 11-23, дополнительно включающий операцию запрета или прекращения загрузки упомянутых данных в случае, если по результатам упомянутой(ых) операции(й) сравнения упомянутая дешифрованная подпись (или каждая из них) и упомянутая сгенерированная подпись не совпадают друг с другом.

25. Способ загрузки данных в приемник/декодер MPEG, включающий генерирование подписи для упомянутых

подлежащих загрузке данных, отличающийся тем, что он включает следующие операции: шифрование упомянутой подписи с использованием секретного ключа, форматирование упомянутых подлежащих загрузке данных, зашифрованной подписи и идентификатора упомянутого секретного ключа, использованного для шифрования упомянутой подписи, в виде MPEG таблицы, трансляция упомянутой MPEG таблицы, и в приемнике/декодере: сохранение в защищенной области памяти множества флагов проверки допустимости, каждый из которых предназначен для соответствующего общедоступного ключа, прием упомянутой MPEG таблицы, нахождение в упомянутой защищенной области памяти приемника/декодера флага проверки допустимости для общедоступного ключа, соответствующего секретному ключу, обозначенному идентификатором секретного ключа, содержащимся в принятой MPEG таблице, и если упомянутый флаг установлен: дешифровка зашифрованной подписи, содержащейся в принятой MPEG таблице, с использованием упомянутого общедоступного ключа, соответствующего секретному ключу, обозначенному идентификатором секретного ключа, содержащимся в принятой MPEG таблице, для получения дешифрованной подписи, генерирование подписи для упомянутых данных, содержащихся в принятой MPEG таблице, и сравнение дешифрованной подписи и подписи, сгенерированной в приемнике/декодере для упомянутых принятых данных.

26. Способ по п. 25, дополнительно включающий следующие операции: генерирование кода допустимости для упомянутых подлежащих загрузке данных, который зашифровывается вместе с подписью при выполнении упомянутой операции шифрования и дешифруется вместе с подписью при выполнении упомянутой операции дешифровки, нахождение сохраненного кода проверки допустимости в защищенной области памяти приемника/декодера, сравнение найденного кода проверки допустимости и дешифрованного кода проверки допустимости.

27. Способ по п. 26, дополнительно содержащий операцию запрета или прекращения загрузки упомянутых данных в случае, если по результатам упомянутого сравнения кодов проверки допустимости упомянутые найденный код проверки допустимости и дешифрованный код проверки допустимости не совпадают друг с другом.

28. Способ по любому из пп. 25-27, в котором упомянутая подпись упомянутых подлежащих загрузке данных зашифровывается в блоке данных, с некоторым выбранным смещением между началом этого блока данных и началом упомянутой подписи, и зашифрованный блок данных дешифруется при выполнении упомянутой операции дешифровки в приемнике/декодере, и дополнительно включающий операции, в приемнике/декодере, нахождения по меньшей мере одного значения смещения, хранящегося в защищенной области памяти приемника/декодера, а также извлечения

подписи из упомянутого дешифрованного блока данных с использованием упомянутого одного найденного значения смещения от начала дешифрованного блока данных.

29. Способ по п. 28, в котором упомянутая защищенная область памяти содержит по меньшей мере два таких сохраненных значения смещения, и который, если по результатам упомянутой операции сравнения упомянутые извлеченная подпись и сгенерированная подпись не совпадают, включает дополнительную операцию повторения операций нахождения, извлечения и сравнения с использованием другого из упомянутых сохраненных значений смещения.

30. Способ по пп. 28 и 29, в котором упомянутый блок данных включает в себя, помимо упомянутой подписи, фиктивные или произвольные данные.

31. Способ по любому из пп. 25-30, в котором упомянутые данные загружаются в виде множества модулей данных, включающий следующие операции: генерирование подписи для каждого модуля данных, подлежащего загрузке, форматирование упомянутых модулей данных в виде соответствующих MPEG таблиц модулей, генерирование каталога, содержащего идентификатор каждой MPEG таблицы модуля и соответствующую подпись, причем упомянутый каталог является объектом операции генерирования подписи по любому из пп. 25-30, и в приемнике/декодере: генерирование соответствующей подписи для каждого из упомянутых модулей, содержащихся в принятых MPEG таблицах модулей, и сравнение каждой из подписей для модулей, содержащихся в принятой MPEG таблице каталога, с соответствующей подписью для модуля, сгенерированной в приемнике/декодере.

32. Способ по п. 31, дополнительно включающий операцию запрета или прекращения загрузки такого модуля упомянутых данных, если подпись для упомянутого модуля, содержащаяся в принятой MPEG таблице каталога, и соответствующая подпись, сгенерированная для данного модуля в приемнике/декодере, не совпадают друг с другом.

33. Способ по любому из пп. 25-32, дополнительно включающий операцию запрета или прекращения загрузки упомянутых данных в случае, если по результатам упомянутой(ых) операции(й) сравнения упомянутая дешифрованная подпись (или каждая из них) и упомянутая сгенерированная подпись не совпадают друг с другом.

34. Способ загрузки данных в приемник/декодер MPEG, отличающийся тем, что он включает следующие операции: генерирование кода проверки допустимости для упомянутых подлежащих загрузке данных, генерирование подписи для упомянутых подлежащих загрузке данных или их части, шифрование упомянутых кода проверки допустимости и подписи с использованием секретного ключа, форматирование упомянутых подлежащих загрузке данных и зашифрованных кода проверки допустимости и подписи в виде по меньшей мере одной MPEG таблицы,

трансляция каждой MPEG таблицы, и в приемнике/декодере: сохранение кода проверки допустимости в защищенной области памяти, прием каждой MPEG таблицы, дешифровка зашифрованных кода проверки допустимости и подписи, содержащихся в принятых MPEG таблицах, с использованием общедоступного ключа, соответствующего упомянутому секретному ключу, нахождение упомянутого сохраненного кода проверки допустимости в упомянутой защищенной области памяти приемника/декодера, сравнение найденного кода проверки допустимости и упомянутого дешифрованного кода проверки допустимости, генерирование подписи для упомянутых данных, содержащихся в принятых MPEG таблицах, или упомянутой их части; и сравнение дешифрованной подписи и подписи, сгенерированной в приемнике/декодере для упомянутых принятых данных.

35. Способ по п. 34, дополнительно содержащий операцию запрета или прекращения загрузки упомянутых данных в случае, если по результатам упомянутого сравнения кодов проверки допустимости упомянутые найденный код проверки допустимости и дешифрованный код проверки допустимости не совпадают друг с другом.

36. Способ по п. 34 или 35, в котором упомянутая подпись упомянутых подлежащих загрузке данных зашифровывается в блоке данных, с некоторым выбранным смещением между началом этого блока данных и началом упомянутой подписи, и зашифрованный блок данных дешифруется при выполнении упомянутой операции дешифровки в приемнике/декодере, и дополнительно включающий операции в приемнике/декодере нахождения по меньшей мере одного значения смещения, хранящегося в защищенной области памяти приемника/декодера, а также извлечения подписи из упомянутого дешифрованного блока данных с использованием упомянутого одного найденного значения смещения от начала дешифрованного блока данных.

37. Способ по п. 36, в котором упомянутая защищенная область памяти содержит по меньшей мере два таких сохраненных значения смещения, и который, если по результатам упомянутой операции сравнения упомянутые извлеченная подпись и сгенерированная подпись не совпадают, включает дополнительную операцию повторения операций нахождения, извлечения и сравнения с использованием другого из упомянутых сохраненных значений смещения.

38. Способ по п. 36 или 37, в котором упомянутый блок данных включает в себя, помимо упомянутой подписи, фиктивные или произвольные данные.

39. Способ по любому из пп. 34-38, в котором упомянутые данные загружаются в виде множества модулей данных, включающий следующие операции: генерирование подписи для каждого модуля данных, подлежащего загрузке, форматирование упомянутых модулей данных в виде соответствующих MPEG таблиц модулей, генерирование каталога, содержащего идентификатор каждой MPEG

таблицы модуля и соответствующую подпись, причем упомянутый каталог является объектом операции генерирования подписи по любому из пп. 34-38, и в приемнике/декодере: генерирование соответствующей подписи для каждого из упомянутых модулей, содержащихся в принятых MPEG таблицах модулей, и сравнение каждой из подписей для модулей, содержащихся в принятой MPEG таблице каталога, с соответствующей подписью для модуля, сгенерированной в приемнике/декодере.

40. Способ по п. 39, дополнительно включающий операцию запрета или прекращения загрузки такого модуля упомянутых данных, если подпись для упомянутого модуля, содержащаяся в принятой MPEG таблице каталога, и соответствующая подпись, сгенерированная для данного модуля в приемнике/декодере, не совпадают друг с другом.

41. Способ по любому из пп. 34-40, дополнительно включающий операцию запрета или прекращения загрузки упомянутых данных в случае, если по результатам упомянутой(ых) операции(й) сравнения упомянутая дешифрованная подпись (или каждая из них) и упомянутая сгенерированная подпись не совпадают друг с другом.

42. Способ загрузки данных в приемник/декодер MPEG, включающий генерирование подписи для упомянутых подлежащих загрузке данных, отличающийся тем, что он включает следующие операции: включение упомянутой подписи в блок данных, с некоторым выбранным смещением между началом этого блока данных и началом упомянутой подписи, шифрование упомянутого блока данных с использованием секретного ключа, форматирование упомянутых подлежащих загрузке данных и упомянутого зашифрованного блока данных в виде MPEG таблицы, трансляция упомянутой MPEG таблицы, и в приемнике/декодере: сохранение в защищенной области памяти приемника/декодера по меньшей мере одного значения смещения, прием упомянутой MPEG таблицы, дешифровка упомянутого зашифрованного блока данных, содержащегося в принятой MPEG таблице, с использованием общедоступного ключа, соответствующего упомянутому секретному ключу, нахождение по меньшей мере одного значения смещения в упомянутой защищенной области памяти приемника/декодера, извлечение упомянутой подписи из упомянутого дешифрованного блока данных с использованием упомянутого найденного значения смещения от начала упомянутого дешифрованного блока данных, генерирование подписи для упомянутых данных, содержащихся в принятой MPEG таблице, и сравнение подписи, извлеченной из упомянутого дешифрованного блока данных, и подписи, сгенерированной в приемнике/декодере для упомянутых принятых данных.

43. Способ по п. 42, в котором упомянутая защищенная область памяти содержит по меньшей мере два таких сохраненных значения смещения, и который, если по результатам упомянутой операции сравнения упомянутые извлеченная подпись и

сгенерированная подпись не совпадают, включает дополнительную операцию повторения операций нахождения, извлечения и сравнения с использованием другого из упомянутых сохраненных значений смещения.

44. Способ по п. 42 или 43, в котором упомянутый блок данных включает в себя, помимо упомянутой подписи, фиктивные или произвольные данные.

45. Способ по любому из пп. 42-44, в котором упомянутые данные загружаются в виде множества модулей данных, включающий следующие операции: генерирование подписи для каждого модуля данных, подлежащего загрузке, форматирование упомянутых модулей данных в виде соответствующих MPEG таблиц модулей, генерирование каталога, содержащего идентификатор каждой MPEG таблицы модуля и соответствующую подпись, причем упомянутый каталог является объектом операции генерирования подписи по любому из пп. 42-44, и в приемнике/декодере: генерирование соответствующей подписи для каждого из упомянутых модулей, содержащихся в принятых MPEG таблицах модулей, и сравнение каждой из подписей для модулей, содержащихся в принятой MPEG таблице каталога, с соответствующей подписью для модуля, сгенерированной в приемнике/декодере.

46. Способ по п. 45, дополнительно включающий операцию запрета или прекращения загрузки такого модуля упомянутых данных, если подпись для упомянутого модуля, содержащаяся в принятой MPEG таблице каталога, и соответствующая подпись, сгенерированная для данного модуля в приемнике/декодере, не совпадают друг с другом.

47. Способ по любому из пп. 42-46, дополнительно включающий операцию запрета или прекращения загрузки упомянутых данных в случае, если по результатам упомянутой(ых) операции(й) сравнения упомянутая дешифрованная подпись (или каждая из них) и упомянутая сгенерированная подпись не совпадают друг с другом.

48. Способ загрузки множества модулей данных в приемник/декодер MPEG, включающий следующие операции: генерирование подписи для каждого модуля данных, подлежащего загрузке, форматирование упомянутых модулей данных в виде соответствующих MPEG таблиц модулей, генерирование каталога, содержащего идентификатор каждой MPEG таблицы модуля и соответствующую подпись, и генерирование подписи для каталога, отличающийся тем, что он также включает следующие операции: шифрование упомянутой подписи для каталога с использованием секретного ключа, форматирование каталога и зашифрованной подписи для каталога в виде MPEG таблицы каталога, трансляция упомянутых MPEG таблиц каталога и модулей, и в приемнике/декодере: прием упомянутых MPEG таблиц каталога и модулей, дешифровка зашифрованной подписи для каталога, содержащейся в принятой MPEG таблице каталога, с использованием

общедоступного ключа, соответствующего упомянутому секретному ключу, генерирование подписи для упомянутого каталога, содержащегося в принятой MPEG таблице каталога, сравнение упомянутой дешифрованной подписи для каталога и подписи для каталога, сгенерированной в приемнике/декодере, генерирование соответствующей подписи для каждого из упомянутых модулей, содержащихся в принятых MPEG таблицах модулей, и сравнение каждой из подписей для модулей, содержащихся в принятой MPEG таблице каталога, с соответствующей подписью для модуля, сгенерированной в приемнике/декодере.

49. Способ по п. 48, дополнительно включающий операцию запрета или прекращения загрузки такого модуля упомянутых данных, если подпись для упомянутого модуля, содержащаяся в принятой MPEG таблице каталога, и соответствующая подпись, сгенерированная для данного модуля в приемнике/декодере, не совпадают друг с другом.

50. Способ по п. 48 или 49, дополнительно включающий операцию запрета или прекращения загрузки упомянутых данных в случае, если по результатам упомянутой(ых) операции(й) сравнения упомянутая дешифрованная подпись (или каждая из них) и упомянутая сгенерированная подпись не совпадают друг с другом.

51. Приемник/декодер MPEG для загрузки данных, представленных в форме MPEG таблицы, включающей в себя упомянутые подлежащие загрузке данные, зашифрованную подпись для этих данных и идентификатор секретного ключа, использованного для шифрования упомянутой подписи, содержащий средство для приема таких MPEG таблиц, и средство для хранения множества общедоступных ключей и по одному идентификатору для каждого из этих общедоступных ключей, отличающийся тем, что он также содержит средство обработки, которое программируется таким образом, чтобы выбирать один из упомянутых сохраненных общедоступных ключей, в соответствии с упомянутым идентификатором секретного ключа, содержащимся в принятой MPEG таблице, дешифровать упомянутую зашифрованную подпись, содержащуюся в принятой MPEG таблице, с использованием выбранного общедоступного ключа, для получения дешифрованной подписи, генерировать подпись для упомянутых данных, содержащихся в принятой MPEG таблице, и сравнивать дешифрованную подпись и подпись, сгенерированную в приемнике/декодере для упомянутых принятых данных.

52. Приемник/декодер по п. 51, в котором в качестве упомянутого средства для хранения ключей используется ПЗУ.

53. Приемник/декодер по п. 51 или 52, в котором упомянутый идентификатор для каждого из упомянутых общедоступных ключей представлен местом хранения данного общедоступного ключа в упомянутом средстве для хранения ключей.

54. Приемник/декодер по пп. 51-53, для использования в способе по п. 14, дополнительно содержащий некоторую

область энергозависимой памяти, и в котором упомянутое средство обработки выполнено с возможностью загрузки приложения, имеющего подпись, зашифрованную с использованием секретного ключа, имеющего некоторый заранее определенный идентификатор, выполнения упомянутого приложения для обеспечения приема приемником/декодером некоторого временного ключа, и сохранения упомянутого временного ключа в упомянутой области энергозависимой памяти приемника/декодера.

55. Приемник/декодер по п. 54, дополнительно содержащий средство для приема такого временного ключа, который предоставляется приемнику/декодеру на месте.

56. Приемник/декодер по п. 55, в котором упомянутый временный ключ предоставляется через параллельный порт, последовательный порт или устройство считывания смарт-карты приемника/декодера.

57. Приемник/декодер по любому из пп. 54-56, в котором упомянутая энергозависимая память обеспечивается посредством оперативной памяти.

58. Приемник/декодер по любому из пп. 51-57 для использования в способе по п. 15, дополнительно содержащий защищенную область памяти для хранения флага проверки допустимости для каждого из по меньшей мере некоторых из упомянутых общедоступных ключей, и в котором упомянутое средство обработки программируется таким образом, чтобы находить в упомянутой защищенной области памяти флаг проверки допустимости для такого выбранного общедоступного ключа, а также запрещать или прекращать загрузку упомянутых данных в случае, если найденный флаг не установлен.

59. Приемник/декодер по любому из пп. 54-57 для использования в способе по п. 15, дополнительно содержащий защищенную область памяти для хранения флага проверки допустимости для каждого из по меньшей мере некоторых из упомянутых общедоступных ключей, и в котором упомянутое средство обработки программируется таким образом, чтобы находить в упомянутой защищенной области памяти флаг проверки допустимости для такого выбранного общедоступного ключа, а также запрещать или прекращать загрузку упомянутых данных в случае, если найденный флаг не установлен, и также дополнительно содержащий защищенную область памяти для хранения флага проверки допустимости для упомянутого секретного ключа, имеющего упомянутый заранее определенный идентификатор ключа, и в котором упомянутое средство обработки выполнено с возможностью изменения, при выполнении упомянутого приложения, этого флага проверки допустимости и разрешения сохранения упомянутого временного ключа в зависимости от состояния этого флага.

60. Приемник/декодер по п. 58 или 59, в котором упомянутая память для хранения флага(ов) проверки допустимости для ключа(ей) является перезаписываемой энергонезависимой памятью.

61. Приемник/декодер по любому из пп. 58-60, в котором упомянутая память для

хранения флага(ов) проверки допустимости для ключа(ей) в случае, когда сохраняется множество таких общедоступных ключей, организована в виде битового массива.

62. Приемник/декодер по любому из пп. 57-61 для использования в способе по п. 34 дополнительно содержащий защищенную область памяти для хранения кода проверки допустимости, и в котором средство обработки программируется таким образом, чтобы дешифровать код проверки допустимости, содержащийся в такой принятой MPEG таблице, находить упомянутый сохраненный код проверки допустимости и сравнивать найденный код проверки допустимости и дешифрованный код проверки допустимости.

63. Приемник/декодер по п. 62, в котором средство обработки программируется таким образом, чтобы запрещать или прекращать загрузку упомянутых данных в случае, если упомянутые найденный код проверки допустимости и дешифрованный код проверки допустимости не совпадают друг с другом.

64. Приемник/декодер по п. 62 или 63, в котором упомянутая память для хранения упомянутого кода проверки допустимости обеспечивается посредством перезаписываемой энергонезависимой памяти.

65. Приемник/декодер по любому из пп. 62-64, в котором упомянутая память для хранения упомянутого кода проверки допустимости организована в виде битового массива.

66. Приемник/декодер по любому из пп. 51-65 для использования в способе по любому из пп. 19, 28, 36, дополнительно содержащий защищенную область памяти для хранения по меньшей мере одного значения смещения, и в котором упомянутое средство обработки программируется таким образом, чтобы дешифровать упомянутый зашифрованный блок данных, содержащийся в принятой MPEG таблице, находить упомянутое одно сохраненное значение смещения в упомянутой защищенной области памяти и извлекать подпись из упомянутого дешифрованного блока данных с использованием упомянутого найденного значения смещения от начала упомянутого дешифрованного блока данных.

67. Приемник/декодер по п. 66, в котором в упомянутой защищенной области памяти хранятся по меньшей мере два таких значения смещения, и упомянутое средство обработки выполнено с возможностью осуществления, в случае, если упомянутые извлеченная подпись и сгенерированная подпись не совпадают, повторных нахождения, извлечения и сравнения с использованием другого из упомянутых сохраненных значений смещения.

68. Приемник/декодер по любому из п. 66 или 67, в котором упомянутая память для хранения значения смещения обеспечивается посредством перезаписываемой энергонезависимой памяти.

69. Приемник/декодер по любому из пп. 51-68, для использования в способе по любому из пп. 22, 31, 39, 45, в котором упомянутое средство обработки программируется таким образом, чтобы генерировать соответствующую подпись для

каждого из упомянутых модулей, содержащихся в упомянутых принятых MPEG таблицах модулей и сравнивать каждую подпись для модуля, содержащуюся в упомянутой принятой MPEG таблице каталога, с соответствующей подписью для модуля, сгенерированной приемником/декодером.

70. Приемник/декодер по п. 69, в котором средство обработки программируется таким образом, чтобы запрещать или прекращать загрузку такого модуля упомянутых данных в случае, если подпись для данного модуля, содержащаяся в принятой MPEG таблице каталога, и соответствующая подпись, сгенерированная для этого модуля в приемнике/декодере, не совпадают друг с другом.

71. Приемник/декодер по любому из пп. 51-70, в котором упомянутое средство обработки программируется таким образом, чтобы запрещать или прекращать загрузку упомянутых данных в случае, если упомянутая дешифрованная подпись (или каждая из них) и упомянутая сгенерированная подпись не совпадают друг с другом.

72. Приемник/декодер MPEG для загрузки данных, представленных в форме MPEG таблицы, включающей в себя упомянутые подлежащие загрузке данные, зашифрованную подпись для этих данных и идентификатор секретного ключа, использованного для шифрования упомянутой подписи, содержащий средство для приема таких MPEG таблиц, и средство для хранения общедоступного ключа и идентификатора этого общедоступного ключа, отличающийся тем, что он также содержит защищенную область памяти, для хранения флага проверки допустимости для упомянутого общедоступного ключа, и средство обработки, которое программируется таким образом, чтобы находить в упомянутой защищенной области памяти приемника/декодера флаг проверки допустимости для общедоступного ключа, соответствующего упомянутому секретному ключу, идентификатор которого содержится в принятой MPEG таблице, и, если найденный флаг установлен, дешифровать упомянутую зашифрованную подпись, содержащуюся в принятой MPEG таблице, с использованием упомянутого общедоступного ключа, соответствующего секретному ключу, идентификатор которого содержится в принятой MPEG таблице, для получения дешифрованной подписи, генерировать подпись для упомянутых данных, содержащихся в принятой MPEG таблице, и сравнивать дешифрованную подпись и подпись, сгенерированную в приемнике/декодере для упомянутых принятых данных.

73. Приемник/декодер по п. 72, в котором упомянутая память для хранения флага(ов) проверки допустимости для ключа(ей) является перезаписываемой энергонезависимой памятью.

74. Приемник/декодер по п. 72 или 73, в котором упомянутая память для хранения флага(ов) проверки допустимости для ключа(ей) в случае, когда сохраняется множество таких общедоступных ключей, организована в виде битового массива.

75. Приемник/декодер по любому из пп.

72-74 для использования в способе по п. 34 дополнительно содержащий защищенную область памяти для хранения кода проверки допустимости, и в котором средство обработки программируется таким образом, чтобы дешифровать код проверки допустимости, содержащийся в такой принятой MPEG таблице, находить упомянутый сохраненный код проверки допустимости и сравнивать найденный код проверки допустимости и дешифрованный код проверки допустимости.

76. Приемник/декодер по п. 75, в котором средство обработки программируется таким образом, чтобы запрещать или прекращать загрузку упомянутых данных в случае, если упомянутые найденный код проверки допустимости и дешифрованный код проверки допустимости не совпадают друг с другом.

77. Приемник/декодер по п. 75 или 76, в котором упомянутая память для хранения упомянутого кода проверки допустимости обеспечивается посредством перезаписываемой энергонезависимой памяти.

78. Приемник/декодер по любому из пп. 75-77, в котором упомянутая память для хранения упомянутого кода проверки допустимости организована в виде битового массива.

79. Приемник/декодер по любому из пп. 72-78 для использования в способе по любому из пп. 19, 28, 36 дополнительно содержащий защищенную область памяти для хранения по меньшей мере одного значения смещения, и в котором упомянутое средство обработки программируется таким образом, чтобы дешифровать упомянутый зашифрованный блок данных, содержащийся в принятой MPEG таблице, находить упомянутое одно сохраненное значение смещения в упомянутой защищенной области памяти и извлекать подпись из упомянутого дешифрованного блока данных с использованием упомянутого найденного значения смещения от начала упомянутого дешифрованного блока данных.

80. Приемник/декодер по п. 79, в котором в упомянутой защищенной области памяти хранятся по меньшей мере два таких значения смещения, и упомянутое средство обработки выполнено с возможностью осуществления, в случае, если упомянутые извлеченная подпись и сгенерированная подпись не совпадают, повторных нахождения, извлечения и сравнения с использованием другого из упомянутых сохраненных значений смещения.

81. Приемник/декодер по п. 79 или 80, в котором упомянутая память для хранения значения смещения обеспечивается посредством перезаписываемой энергонезависимой памяти.

82. Приемник/декодер по любому из пп. 72-81 для использования в способе по любому из пп. 22, 31, 39, 45, в котором упомянутое средство обработки программируется таким образом, чтобы генерировать соответствующую подпись для каждого из упомянутых модулей, содержащихся в упомянутых принятых MPEG таблицах модулей и сравнивать каждую подпись для модуля, содержащуюся в упомянутой принятой MPEG таблице

каталога, с соответствующей подписью для модуля, сгенерированной приемником/декодером.

83. Приемник/декодер по п. 82, в котором средство обработки программируется таким образом, чтобы запрещать или прекращать загрузку такого модуля упомянутых данных в случае, если подпись для данного модуля, содержащаяся в принятой MPEG таблице каталога, и соответствующая подпись, сгенерированная для этого модуля в приемнике/декодере, не совпадают друг с другом.

84. Приемник/декодер по любому из пп. 72-83, в котором упомянутое средство обработки программируется таким образом, чтобы запрещать или прекращать загрузку упомянутых данных в случае, если упомянутая дешифрованная подпись (или каждая из них) и упомянутая сгенерированная подпись не совпадают друг с другом.

85. Приемник/декодер MPEG для загрузки данных, представленных в форме MPEG таблицы, включающей в себя упомянутые подлежащие загрузке данные, зашифрованный код проверки допустимости, для проверки допустимости упомянутых данных, зашифрованную подпись для упомянутых данных или некоторой их части и идентификатор секретного ключа, использованного для шифрования упомянутых подписи и кода проверки допустимости, содержащий средство для приема таких MPEG таблиц, средство для хранения общедоступного ключа и идентификатора этого общедоступного ключа, отличающийся тем, что он также содержит защищенную область памяти, для хранения кода проверки допустимости для проверки допустимости данных; и средство обработки, которое программируется таким образом, чтобы дешифровать упомянутые зашифрованные код проверки допустимости и подпись, содержащиеся в такой принятой MPEG таблице, с использованием упомянутого сохраненного общедоступного ключа, соответствующего упомянутому секретному ключу, находить в защищенной области памяти упомянутый сохраненный код проверки допустимости, сравнивать найденный код проверки допустимости и дешифрованный код проверки допустимости, генерировать подпись для упомянутых данных, содержащихся в принятой MPEG таблице, или упомянутой их части, и сравнивать дешифрованную подпись и подпись, сгенерированную в приемнике/декодере для упомянутых принятых данных.

86. Приемник/декодер по п. 85, в котором средство обработки программируется таким образом, чтобы запрещать или прекращать загрузку упомянутых данных в случае, если упомянутые найденный код проверки допустимости и дешифрованный код проверки допустимости не совпадают друг с другом.

87. Приемник/декодер по п. 85 или 86, в котором упомянутая память для хранения упомянутого кода проверки допустимости обеспечивается посредством перезаписываемой энергонезависимой памяти.

88. Приемник/декодер по любому из пп. 85-87, в котором упомянутая память для

хранения упомянутого кода проверки допустимости организована в виде битового массива.

89. Приемник/декодер по любому из пп. 85-88 для использования в способе по любому из пп. 19, 28, 36, дополнительно содержащий защищенную область памяти для хранения по меньшей мере одного значения смещения, и в котором упомянутое средство обработки программируется таким образом, чтобы дешифровать упомянутый зашифрованный блок данных, содержащийся в принятой MPEG таблице, находить упомянутое одно сохраненное значение смещения в упомянутой защищенной области памяти и извлекать подпись из упомянутого дешифрованного блока данных с использованием упомянутого найденного значения смещения от начала упомянутого дешифрованного блока данных.

90. Приемник/декодер по п. 89, в котором в упомянутой защищенной области памяти хранятся по меньшей мере два таких значения смещения, и упомянутое средство обработки выполнено с возможностью осуществления, в случае, если упомянутые извлеченная подпись и сгенерированная подпись не совпадают, повторных нахождения, извлечения и сравнения с использованием другого из упомянутых сохраненных значений смещения.

91. Приемник/декодер по п. 89 или 90, в котором упомянутая память для хранения значения смещения обеспечивается посредством перезаписываемой энергонезависимой памяти.

92. Приемник/декодер по любому из пп. 85-91 для использования в способе по любому из пп. 22, 31, 39, 45, в котором упомянутое средство обработки программируется таким образом, чтобы генерировать соответствующую подпись для каждого из упомянутых модулей, содержащихся в упомянутых принятых MPEG таблицах модулей и сравнивать каждую подпись для модуля, содержащуюся в упомянутой принятой MPEG таблице каталога, с соответствующей подписью для модуля, сгенерированной приемником/декодером.

93. Приемник/декодер по п. 92, в котором средство обработки программируется таким образом, чтобы запрещать или прекращать загрузку такого модуля упомянутых данных в случае, если подпись для данного модуля, содержащаяся в принятой MPEG таблице каталога, и соответствующая подпись, сгенерированная для этого модуля в приемнике/декодере, не совпадают друг с другом.

94. Приемник/декодер по любому из пп. 85-93, в котором упомянутое средство обработки программируется таким образом, чтобы запрещать или прекращать загрузку упомянутых данных в случае, если упомянутая дешифрованная подпись (или каждая из них) и упомянутая сгенерированная подпись не совпадают друг с другом.

95. Приемник/декодер MPEG для загрузки данных, представленных в форме MPEG таблицы, включающей в себя упомянутые подлежащие загрузке данные и зашифрованный блок данных, включающий в себя подпись для упомянутых данных, с некоторым выбранным смещением между

началом упомянутого блока данных и началом упомянутой подписи, содержащий средство для приема MPEG таблиц; и средство для хранения общедоступного ключа и идентификатора упомянутого общедоступного ключа, отличающийся тем, что он дополнительно содержит защищенную область памяти для хранения по меньшей мере одного значения смещения, средство обработки, которое программируется таким образом, чтобы дешифровать упомянутый зашифрованный блок данных, содержащийся в принятой MPEG таблице, используя упомянутый сохраненный общедоступный ключ, соответствующий упомянутому секретному ключу, находить в защищенной области памяти упомянутое сохраненное значение смещения, извлекать упомянутую подпись из дешифрованного блока данных, с использованием найденного значения смещения от начала упомянутого дешифрованного блока данных, генерировать подпись для упомянутых данных, содержащихся в принятой MPEG таблице, и сравнивать подпись, извлеченную из упомянутого дешифрованного блока данных, и подпись, сгенерированную в приемнике/декодере для упомянутых принятых данных.

96. Приемник/декодер по п. 95, в котором в упомянутой защищенной области памяти хранятся по меньшей мере два таких значения смещения, и упомянутое средство обработки выполнено с возможностью осуществления, в случае, если упомянутые извлеченная подпись и сгенерированная подпись не совпадают, повторных нахождения, извлечения и сравнения с использованием другого из упомянутых сохраненных значений смещения.

97. Приемник/декодер по п. 95 или 96, в котором упомянутая память для хранения значения смещения обеспечивается посредством перезаписываемой энергонезависимой памяти.

98. Приемник/декодер по любому из пп. 95-97 для использования в способе по любому из пп. 22, 31, 39, 45, в котором упомянутое средство обработки программируется таким образом, чтобы генерировать соответствующую подпись для каждого из упомянутых модулей, содержащихся в упомянутых принятых MPEG таблицах модулей и сравнивать каждую подпись для модуля, содержащуюся в упомянутой принятой MPEG таблице каталога, с соответствующей подписью для модуля, сгенерированной приемником/декодером.

99. Приемник/декодер по п. 98, в котором средство обработки программируется таким образом, чтобы запрещать или прекращать загрузку такого модуля упомянутых данных в случае, если подпись для данного модуля, содержащаяся в принятой MPEG таблице

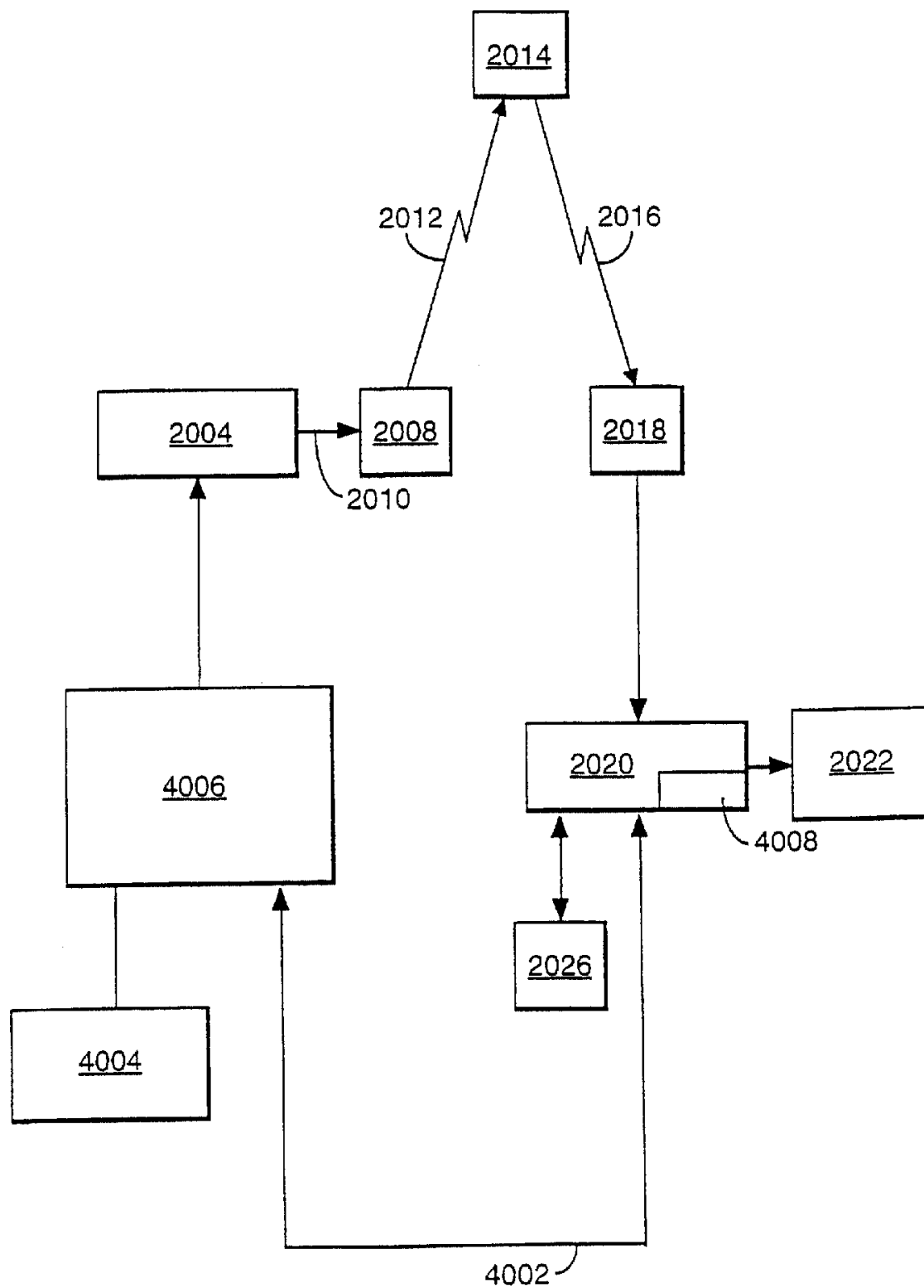
каталога, и соответствующая подпись, сгенерированная для этого модуля в приемнике/декодере, не совпадают друг с другом.

100. Приемник/декодер по любому из пп. 95-99, в котором упомянутое средство обработки программируется таким образом, чтобы запрещать или прекращать загрузку упомянутых данных в случае, если упомянутая дешифрованная подпись (или каждая из них) и упомянутая сгенерированная подпись не совпадают друг с другом.

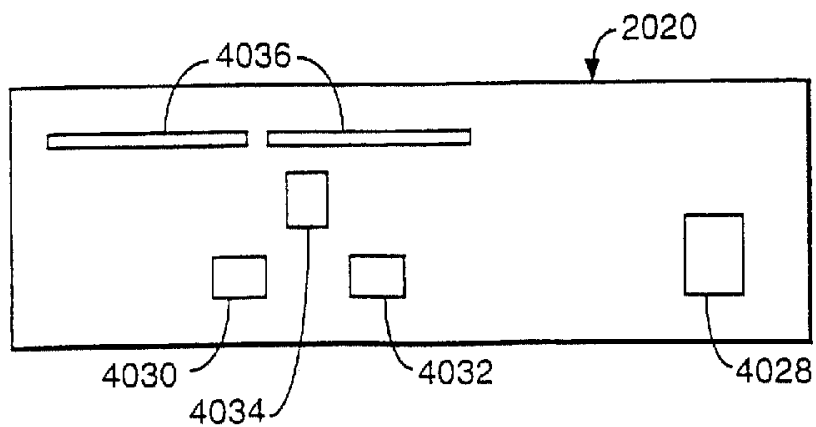
101. Приемник/декодер MPEG для загрузки MPEG таблиц, включающих в себя MPEG таблицы модулей и MPEG таблиц каталога для упомянутых MPEG таблиц модулей, включающую в себя идентификатор и подпись для каждой MPEG таблицы модуля, а также подпись для самого каталога, зашифрованную с использованием секретного ключа, содержащий средство для приема таких MPEG таблиц каталога и модулей, средство для хранения общедоступного ключа и идентификатора этого общедоступного ключа, отличающийся тем, что он также содержит средство обработки, которое программируется таким образом, чтобы дешифровать упомянутую зашифрованную подпись для каталога, содержащуюся в принятой MPEG таблице каталога, с использованием упомянутого сохраненного общедоступного ключа, соответствующего упомянутому секретному ключу, генерировать подпись для упомянутого каталога, содержащегося в принятой MPEG таблице каталога, сравнивать дешифрованную подпись для каталога и подпись для каталога, сгенерированную приемником/декодером, генерировать соответствующие подписи для каждого из упомянутых модулей, содержащихся в принятых MPEG таблицах модулей, и сравнивать каждую из упомянутых подписей, содержащихся в принятой MPEG таблице каталога, с соответствующей подписью для модуля, сгенерированной приемником/декодером.

102. Приемник/декодер по п. 101, в котором средство обработки программируется таким образом, чтобы запрещать или прекращать загрузку такого модуля упомянутых данных в случае, если подпись для данного модуля, содержащаяся в принятой MPEG таблице каталога, и соответствующая подпись, сгенерированная для этого модуля в приемнике/декодере, не совпадают друг с другом.

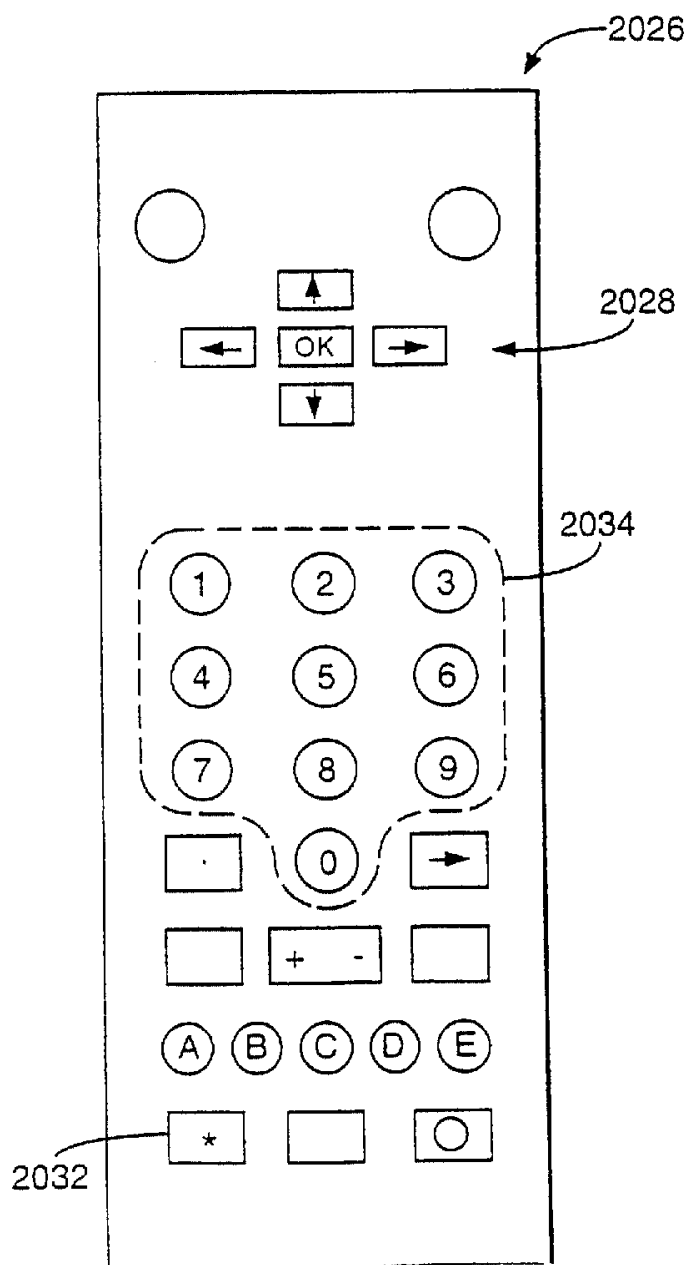
103. Приемник/декодер по п. 101 или 102, в котором упомянутое средство обработки программируется таким образом, чтобы запрещать или прекращать загрузку упомянутых данных в случае, если упомянутая дешифрованная подпись (или каждая из них) и упомянутая сгенерированная подпись не совпадают друг с другом.



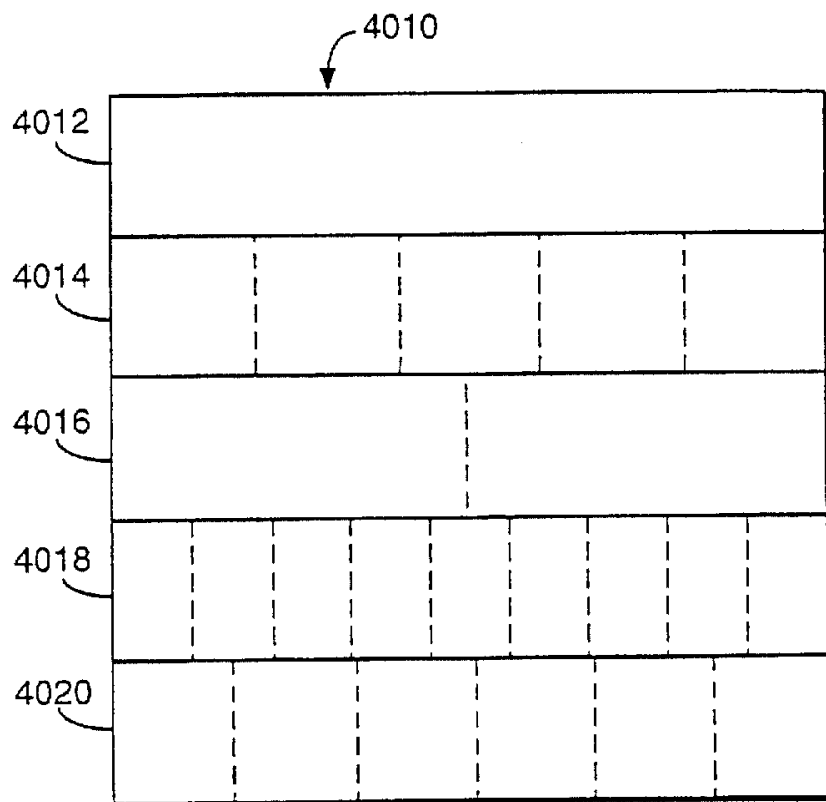
Фиг.2



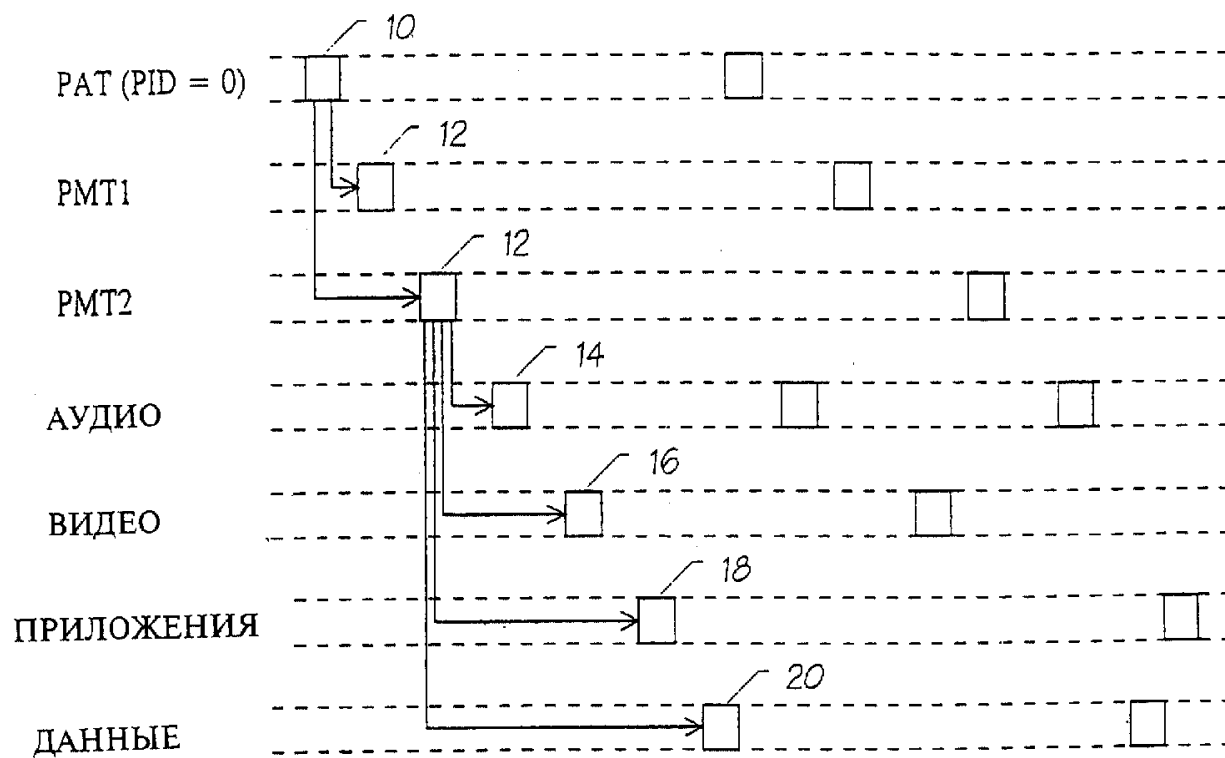
Фиг.3



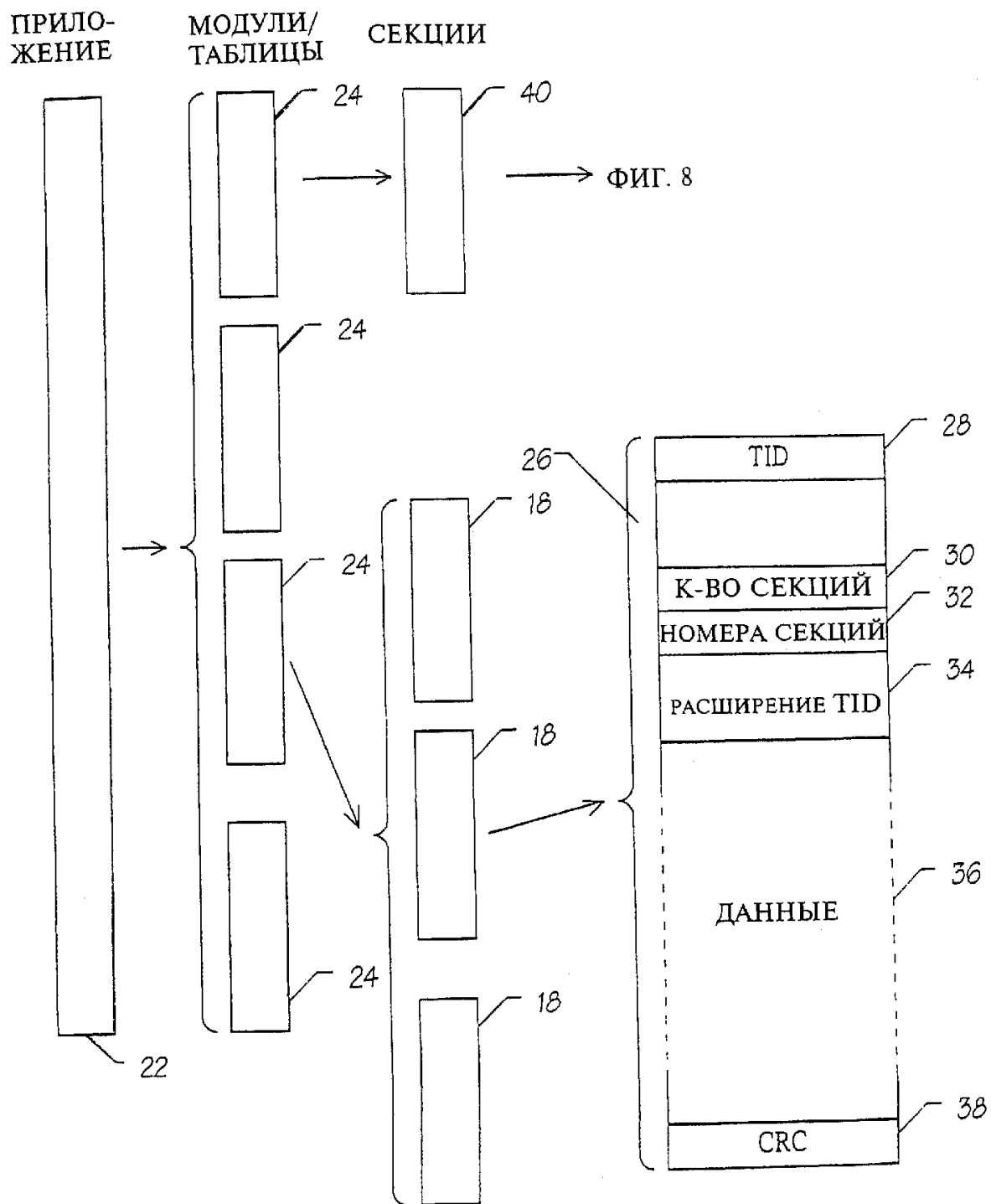
Фиг.4



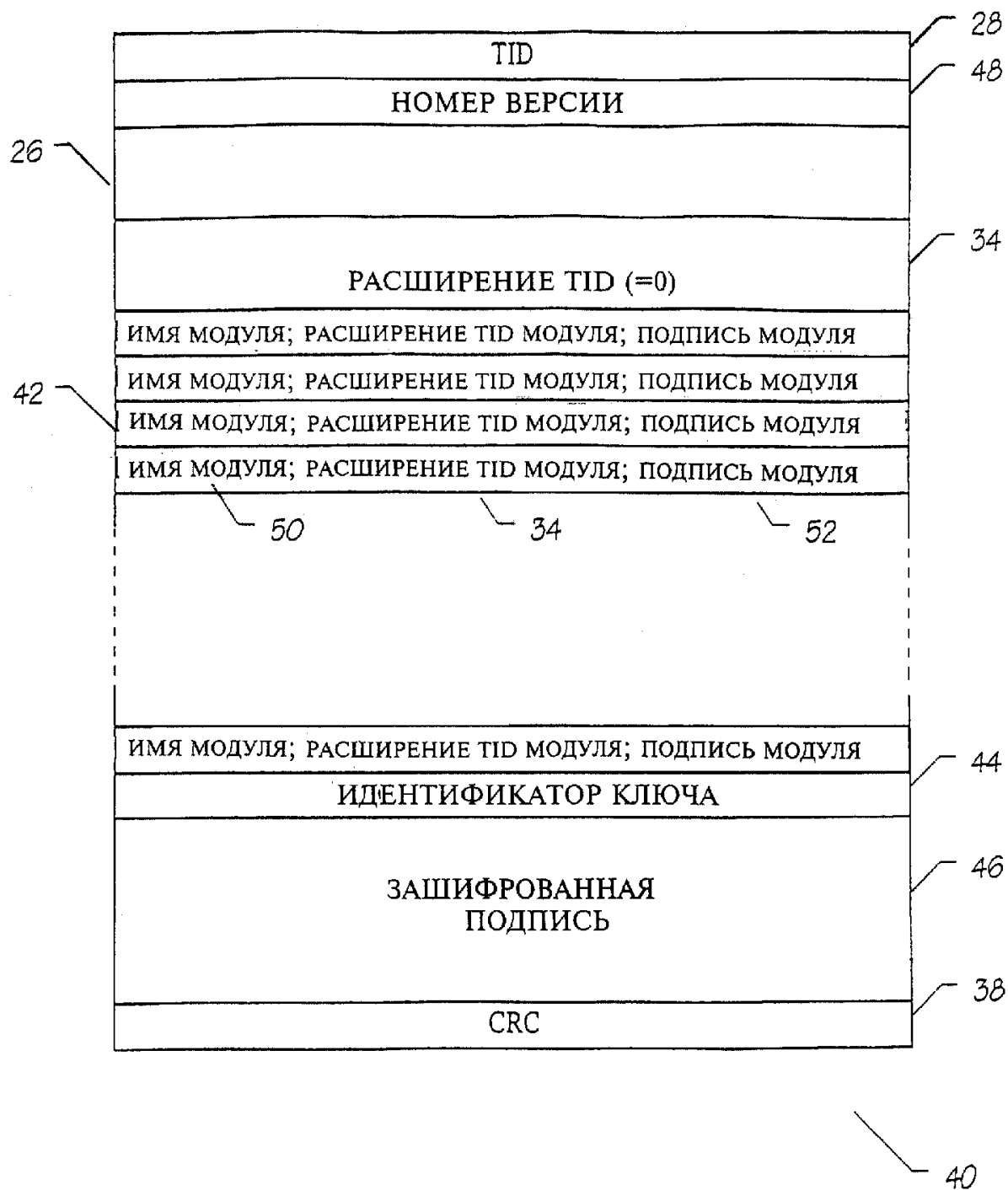
Фиг.5



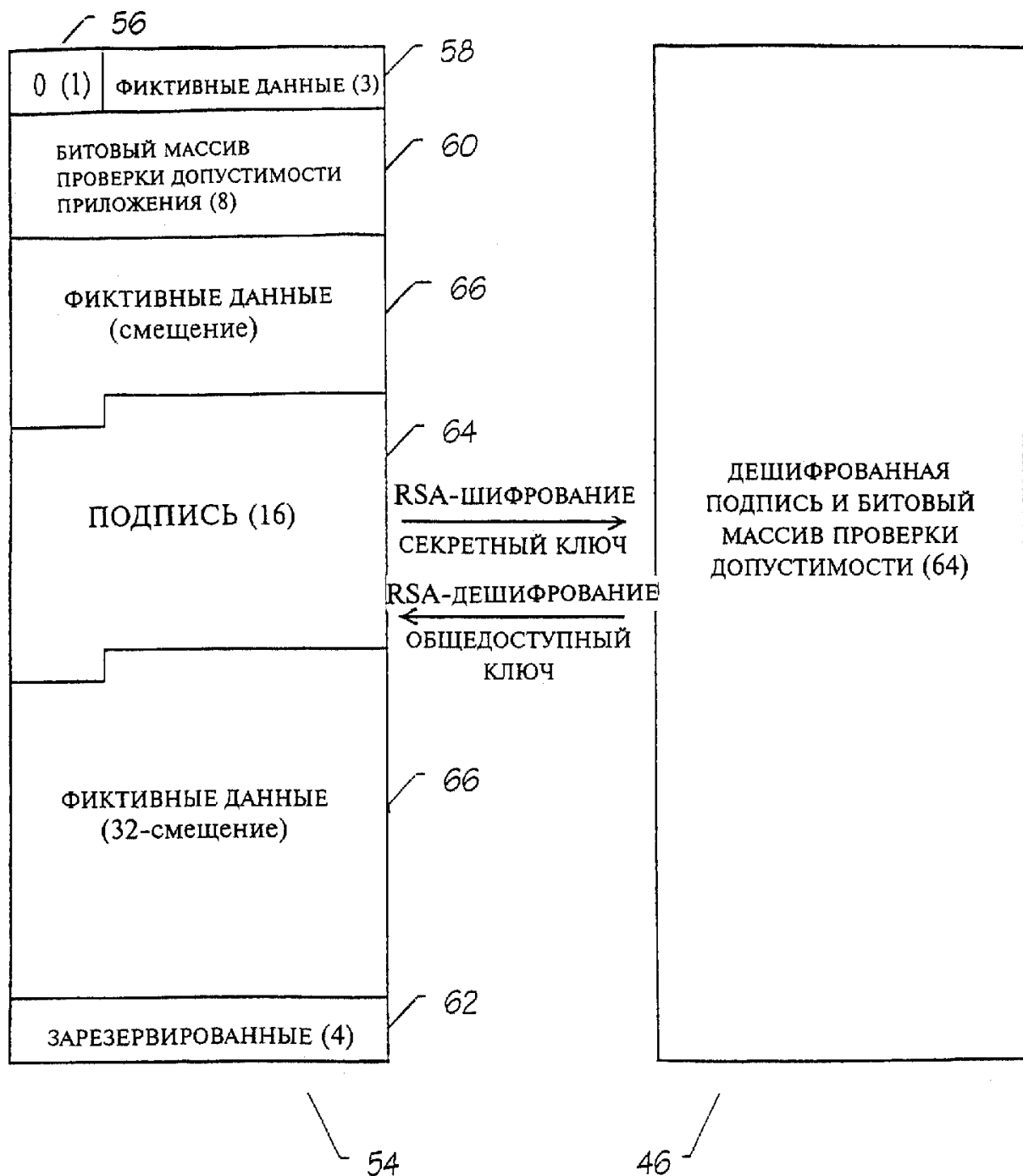
Фиг.6



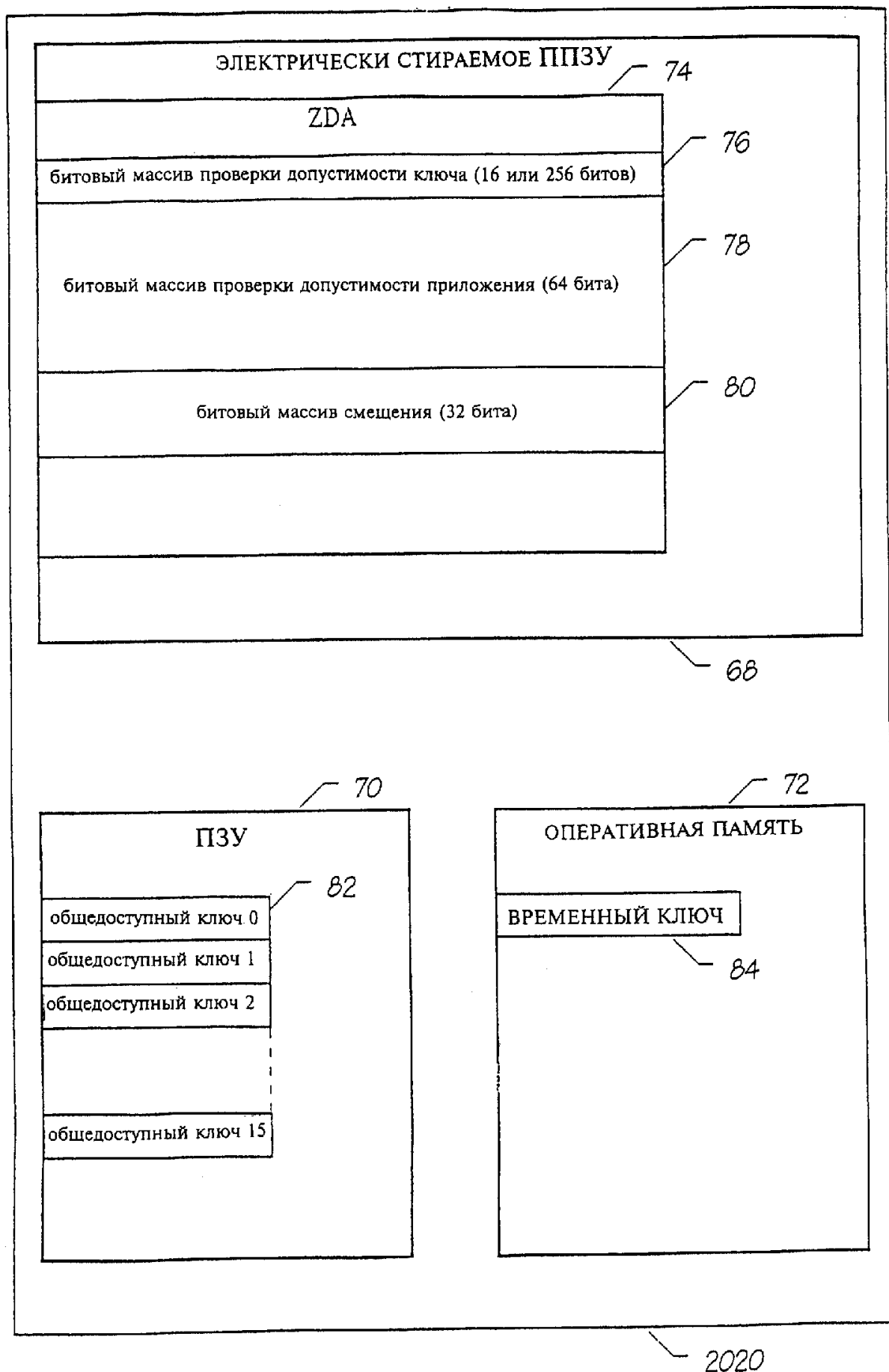
Фиг.7



Фиг.8



Фиг.9



Фиг.10