РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 290 767** (13) **C2**

(51) МПК
H04N 7/167 (2006.01)
G06F 1/00 (2006.01)
H04L 9/00 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21), (22) Заявка: **2003130084/09, 28.01.2002**

(24) Дата начала отсчета срока действия патента:
28.01.2002

(30) Конвенционный приоритет:
12.03.2001 (пп.1-10) EP 01200898.3

(43) Дата публикации заявки: **10.04.2005**

(45) Опубликовано: **27.12.2006 Бюл. № 36**

(56) Список документов, цитированных в отчете о поиске: **EP 0878796 A1, 18.11.1998. WO 0052558 A1, 08.09.2000. EP 1045388 A1, 18.10.2000. US 5787175 A1, 28.07.1998. WO 0117163 A1, 08.03.2001. US 5438508 A1, 01.09.1995. JP 2000-113048 A1, 21.04.2000. RU 2147790 C1, 20.04.2000. RU 2144269 C1, 10.01.2000.**

(85) Дата перевода заявки PCT на национальную фазу:
13.10.2003

(86) Заявка PCT:
IB 02/00245 (28.01.2002)

(87) Публикация PCT:
WO 02/073378 (19.09.2002)

Адрес для переписки:
129010, Москва, ул. Б. Спасская, 25, стр.3, ООО "Юридическая фирма Городисский и Партнеры", пат.пов. Ю.Д.Кузнецову, рег.№ 595

(72) Автор(ы):
БЕЛ Хендрик Й. (NL),
ЛОКОФФ Герардус С. П. (NL),
БРЕГОМ Михел Р. (NL),
ЭНГЕЛЕН Дирк В. Р. (NL),
ВАН ДЕР ПУЛ Петер (NL)

(73) Патентообладатель(и):
КОНИНКЛЕЙКЕ ФИЛИПС ЭЛЕКТРОНИКС Н.В. (NL)

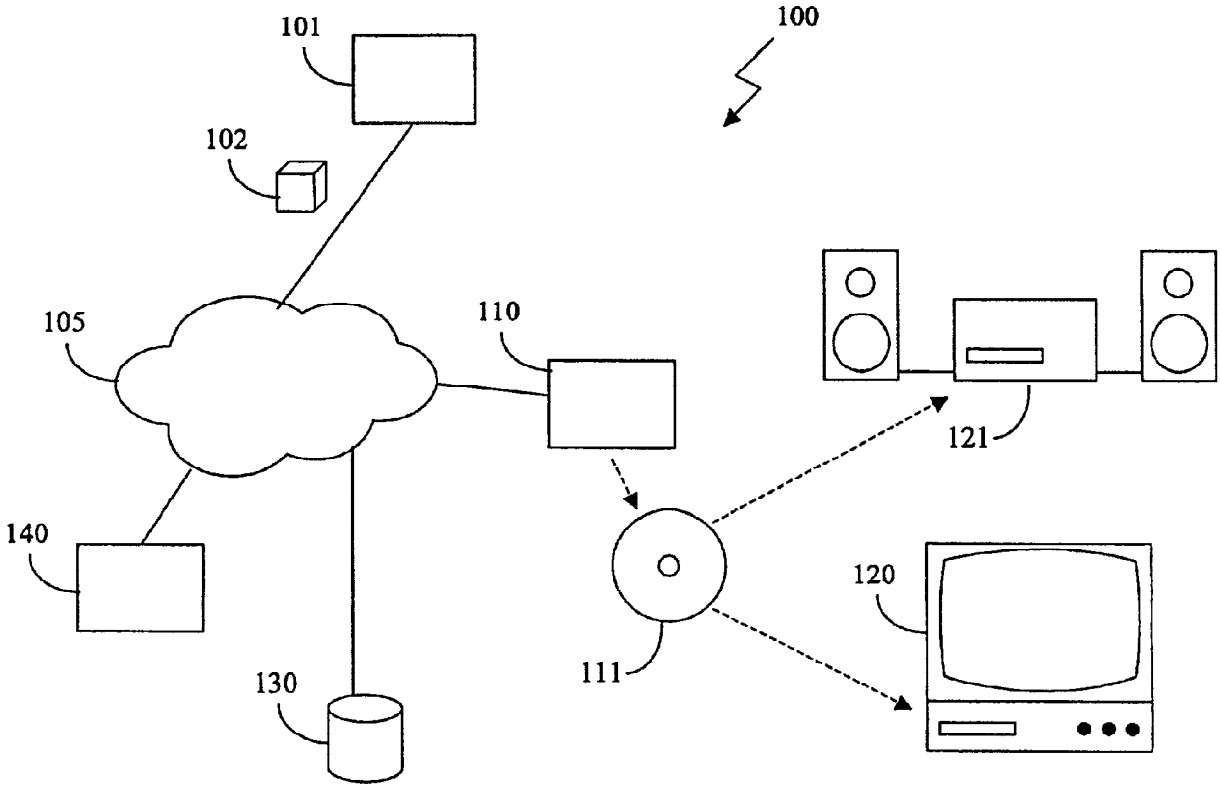
RU 2290767 C2

(54) ПРИЕМНОЕ УСТРОЙСТВО ДЛЯ ЗАЩИЩЕННОГО СОХРАНЕНИЯ ЕДИНИЦЫ КОНТЕНТА И УСТРОЙСТВО ВОСПРОИЗВЕДЕНИЯ

(57) Реферат:

Изобретение относится к системам загрузки и воспроизведения защищенной единицы контента. Техническим результатом является разработка системы загрузки и воспроизведения защищенной единицы контента, позволяющей осуществлять постоянный контроль использования единицы контента, достигаемый тем, что в приемном устройстве (110) для защищенного сохранения единицы (102) контента на носителе (111) информации единица (102) контента сохраняется в защищенном формате и имеет ассоциированный файл лицензии, файл (141) лицензии зашифрован с использованием открытого ключа, ассоциированного с группой устройств воспроизведения (120, 121), и таким образом каждое устройство (121) воспроизведения в группе может дешифровать файл (141) лицензии и проиграть единицу (102) контента, а устройства, не принадлежащие группе, не могут, причем устройство (121) воспроизведения может предоставить открытый ключ, специфичный для данного устройства, в Систему Управления Распределением Контента (СУРК), затем СУРК возвращает секретный ключ для группы, зашифрованный с открытым ключом устройства (121) воспроизведения, после чего устройство (121) воспроизведения защищенным способом

получает секретный ключ группы и может дешифровать файл (141) лицензии. 3 с. и 7 з.п. ф-лы 4 ил.



ФИГ.1

RU 2290767 C2

RU 2290767 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY,
PATENTS AND TRADEMARKS

(19) **RU** (11) **2 290 767** (13) **C2**

(51) Int. Cl.
H04N 7/167 (2006.01)
G06F 1/00 (2006.01)
H04L 9/00 (2006.01)

(12) ABSTRACT OF INVENTION

(21), (22) Application: **2003130084/09, 28.01.2002**

(24) Effective date for property rights: **28.01.2002**

(30) Priority:
12.03.2001 (cl.1-10) EP 01200898.3

(43) Application published: **10.04.2005**

(45) Date of publication: **27.12.2006 Bull. 36**

(85) Commencement of national phase: **13.10.2003**

(86) PCT application:
IB 02/00245 (28.01.2002)

(87) PCT publication:
WO 02/073378 (19.09.2002)

Mail address:
**129010, Moskva, ul. B. Spasskaja, 25, str.3,
OOO "Juridicheskaja firma Gorodisskij i
Partnery", pat.pov. Ju.D.Kuznetsovu, reg.№ 595**

(72) Inventor(s):
**BEL Khendrik J. (NL),
LOKOFF Gerardus S. P. (NL),
BREGOM Mikhel R. (NL),
EhNGELEN Dirk V. R. (NL),
VAN DER PUL Peter (NL)**

(73) Proprietor(s):
KONINKLEJKE FILIPS EhLEKTRONIKS N.V. (NL)

(54) RECEIVING DEVICE FOR PROTECTIVE PRESERVATION OF A UNIT OF CONTENT AND REPRODUCTION DEVICE

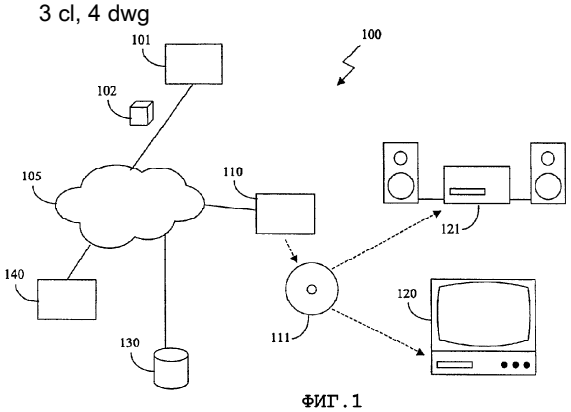
(57) Abstract:

FIELD: engineering of systems for loading and reproducing protective unit of content.

SUBSTANCE: in accordance to invention, in receiving device 110 for protected preservation of unit 102 of content on carrier 111 of information unit 102 of content is stored in protected format and has associated license file, file 141 of license being encrypted with usage of open key, associated with a group of reproduction devices 120,121, and, thus, each reproduction device 121 in group can decrypt file 141 of license and reproduce unit 102 of content, and devices not belonging to group can not do that, while device 121 for reproduction may provide the open key, specific for given device, to system for controlling content distribution, and then system for controlling content distribution returns secret key for group, encrypted with open key of device 121 for reproduction, after that device 121 of reproduction by protected method receives secret key of group and may decrypt file 141 of license.

EFFECT: creation of system for loading and reproducing protected unit of content, making it possible to constantly control usage of unit of content.

3 cl, 4 dwg



ФИГ.1

RU 2290767 C2

RU 2290767 C2

Данное изобретение относится к приемному устройству для защищенного сохранения единицы контента, содержащему средство загрузки для загрузки единицы контента, средство записи для записи загруженной единицы контента на носитель информации и средство лицензирования для получения файла лицензии от сервера лицензии, файл лицензии, по меньшей мере, содержащий разрешение записи загруженной единицы контента на носитель информации.

Дополнительно данное изобретение относится к устройству воспроизведения для воспроизведения единицы контента, сохраненной на носителе информации, содержащему средство воспроизведения единицы контента в соответствии с правами в файле лицензии для единицы контента, сохраненном на носителе информации.

В Интернете широко известны службы разделения ресурсов, такие как Napster (http://www.napster.com) или Gnutella (http://www.gnutella.co.uk). Они используются миллионами пользователей для обмена единицами контента, такими как музыка, как правило, в формате MP3. Каждый пользователь может предложить свою собственную музыкальную коллекцию любому другому, что позволяет каждому иметь большой выбор музыки, доступной для загрузки. Однако музыка, предлагаемая этими службами совместного использования файлов, обычно является популярной музыкой и прелагается без разрешения обладателей авторских прав. Для того чтобы гарантировать обладателям авторских прав полагающиеся им лицензионные отчисления, некоторые службы совместного использования файлов начали взимать подписную плату с их пользователей. Часть выручки от подписной платы может затем использоваться для выплаты по авторским правам.

Для того чтобы предотвратить распространение пользователями загруженных ими единиц контента без авторизации, эти единицы сделаны доступными в защищенным виде. Например, они могут распространяться в зашифрованном формате, в соответствии с чем программное обеспечение в устройстве воспроизведения разрешает воспроизведение, но не запись в незашифрованном виде. Один из способов для защиты единиц контента является технологией "Digifile" Intertrust, известной, например, из патента США 5892900. Согласно этому патенту, музыка сохраняется в защищенной цифровой форме, Digifile. Приемное устройство должно получить файл лицензии от сервера лицензий. Файл лицензии предоставляет ряд разрешений, например разрешение воспроизведения музыки, или разрешение сохранения единицы контента на носителе информации. Естественно, пользователь должен заплатить определенную сумму денег за каждое разрешение. Файл лицензии также содержит ключ дешифрования или другую информацию, требуемую для доступа к музыке внутри Digifile. Когда устройство воспроизведения получает лицензию, оно может дешифровать музыку и проиграть ее пользователю. Пользователь может передать Digifile другим, но они не смогут дешифровать музыку, не купив их собственный файл лицензии. Другие способы защиты единиц контента работают примерно таким же образом.

Разрешения могут быть переданы вместе с Digifile на другое устройство таким образом, что другое устройство сможет воспроизвести контент. Однако обычно для передачи Digifile и разрешений требуется, чтобы другое устройство было подключено к приемному устройству. В качестве альтернативы файл лицензии может быть привязан к пользователю, но при этом имеется тот недостаток, что необходимо аутентифицировать пользователя на каждом устройстве, на котором он желает воспроизвести контент.

Известные подходы имеют своим недостатком то, что они не оправдывают ожидания пользователя в отношении покупки и лицензирования музыки. Если пользователь купил компакт диск (CD) в магазине, он платит один раз и затем может проигрывать CD на любом принадлежащем ему устройстве или даже на устройствах, предоставленных ему другими. Он не рассчитывает, что должен платить каждый раз, когда воспроизводит музыку, или производить обременительные действия для передачи музыки и связанных с ней разрешений к другим устройствам. К тому же схема оплаты за каждое использование требует, чтобы устройство воспроизведения было подключено к сети для того, чтобы было

возможно произвести платеж и получить файл лицензии. Такой подход трудно применить в портативных устройствах.

Согласно преамбуле, задачей настоящего изобретения является создание устройства воспроизведения, которое запускает постоянный контроль использования единицы контента на носителе информации и также соответствует представлению пользователя о его применении.

Данная задача изобретения реализуется согласно настоящему изобретению в приемном устройстве, характеризуемом средством фиксации лицензии для шифрования файла лицензии с ключом шифрования, ассоциированным с группой устройств воспроизведения, и для предоставления шифрованного файла лицензии средству записи для записи шифрованного файла лицензии на носитель информации. Носитель информации, на котором при помощи такого приемного устройства записана единица контента (содержимого), может копироваться без ограничений, но эти единицы контента могут быть проиграны только на устройствах воспроизведения группы, с которой ассоциирован ключ шифрования, и в соответствии с файлом лицензии.

От пользователя требуется только один раз определить группу устройств воспроизведения, на которых он желает проигрывать единицу контента. Он может делать это, например, путем добавления к группе каждого устройства воспроизведения непосредственно после его покупки. Затем он может свободно пользоваться носителем информации, записанным на приемном устройстве. Как станет ясно далее, также возможно расширить группу, когда пользователь покупает новое устройство воспроизведения, так как они могут быть добавлены в любое время, и единица контента (содержимого) записывается таким образом, что любое устройство в группе имеет к ней доступ.

Само по себе известно, как зашифровать информацию таким образом, что только конкретное устройство может считать ее, например, при помощи шифрования данных с открытым ключом этого конкретного устройства, предпочтительно с использованием ключа сессии (сеанса). Это означает, что файл лицензии может быть альтернативно зашифрован много раз с использованием многих открытых ключей, по разу на каждое устройство воспроизведения в группе. Недостаток заключается в том, что количество данных на носителе информации несколько возрастает, но более важно, что затем невозможно добавить в группу новое устройство и обеспечить ему доступ к единице контента. В этом случае файл лицензии зашифрован таким образом, что его могут дешифровать только устройства воспроизведения, которые уже присутствовали в группе во время шифрования, поэтому для приемного устройства отсутствует возможность получить файл лицензии, чтобы зашифровать его с открытым ключом вновь добавляемого устройства. При использовании группового ключа приемному устройству не требуется дополнительных действий и не требуется модификация носителя информации. Вновь добавляемое устройство воспроизведения просто получает ключ дешифрования для группы и после этого оно способно дешифровать файл лицензии.

В варианте осуществления изобретения средства фиксации лицензии приспособлены для шифрования файла лицензии с Ключом Шифрования фиксатора Лицензии (КШФЛ), шифрования КШФЛ с ключом шифрования, ассоциированным с группой устройств воспроизведения, и дополнительно предоставляют зашифрованный КШФЛ средству записи для записи зашифрованного КШФЛ на носитель информации. Устройство воспроизведения, способное дешифровать закодированный КШФЛ, может затем также дешифровать файл лицензии. Файл лицензии затем может быть использован для воспроизведения единицы контента в соответствии с разрешениями, содержащимися в нем. Это обеспечивает дополнительную гибкость.

В другом варианте осуществления изобретения ключ шифрования является открытым ключом из пары открытый/секретный ключ. Соответствующий секретный ключ доступен в устройствах воспроизведения группы, так что они могут легко дешифровать зашифрованный файл лицензии. Дополнительное преимущество заключается в том, что теперь ключ дешифрования не требует защиты, так что устройство воспроизведения не

должно принимать какие-либо меры по защите этого ключа. Если ключ шифрования является секретным (симметричным) ключом, злонамеренный пользователь может похитить ключ из приемного устройства и затем дешифровать файл лицензии, и воспроизвести единицу контента (содержимого) на любом устройстве.

В другом варианте осуществления изобретения единица контента содержит, по меньшей мере, либо аудио- либо видеоданные. Популярность служб совместно используемого музыкального контента (содержимого), таких как Napster, ясно показывает, что существует большой спрос на распределение музыкального и аудиоконтента другого вида. То же самое ожидается и для видео, поскольку пропускная способность сети стала достаточно высокой, чтобы обеспечить широкое распространение видеоданных. Предоставляя, согласно настоящему изобретению приемные устройства, которые могут реализовывать защищенное распространение на носителе информации, становится возможным распространение среди групп людей.

В другом варианте осуществления изобретения средства фиксации лицензии дополнительно приспособлены для получения результата выбора идентификатора группы и для получения ключа шифрования, ассоциированного с результатом выбора, от сервера ключей. Если пользователь определил множество групп, является предпочтительным, чтобы он мог выбрать одну из них для использования при записи единицы контента на носитель информации. При обеспечении открытого ключа для группы на сервере ключей становится возможным для одного пользователя защищенная запись неких единиц контента, которые другой пользователь сможет воспроизвести. Так, например, пользователь может загрузить и сохранить набор песен на носителе информации, используя открытый ключ группы, зарегистрированной на друга. Он может затем отдать носитель информации другу, например, в качестве подарка, который сможет затем проигрывать его на каждом устройстве своей группы. Это позволит пользователю включить только те единицы контента, которые, как ему известно, понравятся его другу, создавая таким образом индивидуальный подарок.

Другой задачей изобретения является предоставление устройства воспроизведения, согласно преамбуле, которое запускает постоянный контроль использования единицы контента на носителе информации и также отвечает ожиданиям пользователя о его применении.

Данная задача изобретения реализуется согласно изобретению в устройстве воспроизведения, характеризуемом тем, что файл лицензии сохранен на носителе информации и что данное устройство воспроизведения дополнительно содержит защищенные средства хранения для хранения одного или более ключей дешифрования, ассоциированные с соответствующей группой устройств воспроизведения, средств декодирования для проверки, подходит ли сохраненный ключ дешифрования для дешифрования зашифрованного файла лицензии, и если да, дешифрующее файл лицензии, используя сохраненный ключ дешифрования и предоставляя дешифрованный файл лицензии средству воспроизведения. Так как файл лицензии сохранен зашифрованным, только устройство воспроизведения, которое может дешифровать его, может получить доступ к единице контента и использовать ее. Если устройство воспроизведения принадлежит верной группе, которая выбрана пользователем при записи единицы контента на носитель информации, верный ключ дешифрования будет предоставлен на защищенных средствах хранения.

В варианте осуществления изобретения зашифрованный файл лицензии хранится с Ключом Шифрования фиксатора Лицензии (КШФЛ), указанный КШФЛ хранится на носителе информации в зашифрованном виде с ключом дешифрования КШФЛ, один или более ключей дешифрования являются ключами дешифрования КШФЛ, и средство декодирования приспособлено для проверки, является ли сохраненный ключ дешифрования КШФЛ подходящим для дешифрования зашифрованного КШФЛ, и если да, получения КШФЛ из зашифрованного КШФЛ, используя сохраненный ключ дешифрования КШФЛ, и дешифрования файла лицензии, используя КШФЛ. Использование КШФЛ как

ключа сессии обеспечивает дополнительную гибкость.

В другом варианте осуществления изобретения ключ дешифрования является секретным ключом пары открытый/секретный ключ. Применение открытого ключа шифрования делает распространение ключей шифрования гораздо более простым, так как нет необходимости в их защищенном хранении. Ключ шифрования теперь может быть открыто передан приемному устройству, которое шифрует с его помощью файл лицензии. Только устройство воспроизведения, имеющее соответствующий ключ дешифрования, сможет затем дешифровать файл лицензии и получить доступ к файлу лицензии.

В другом варианте осуществления изобретения устройство воспроизведения дополнительно содержит средство регистрации для регистрации открытого ключа пары открытый/секретный ключ, ассоциированной с устройством воспроизведения в системе управления распределением контента (СУРК), секретный ключ указанной пары открытый/секретный ключ сохраняется на средстве защищенного хранения, и для приема ключа дешифрования, зашифрованного с указанным открытым ключом, дешифрование указанного зашифрованного ключа дешифрования, и сохранения ключа дешифрования на средстве защищенного хранения. При использовании распространения секретного ключа для группы устройствам воспроизведения в таком виде, достигается то, что отсутствуют моменты, когда секретный ключ открыт для злонамеренного пользователя, и никакое устройство воспроизведения не может получить доступ к секретному ключу без регистрации.

Дополнительно изобретение относится к компьютерному программному продукту, позволяющему программируемому устройству при выполнении указанного компьютерного программного продукта функционировать в качестве приемного устройства согласно настоящему изобретению.

Дополнительно изобретение имеет отношение к компьютерному программному продукту, позволяющему программируемому устройству при выполнении указанного компьютерного программного продукта функционировать в качестве устройства воспроизведения согласно настоящему изобретению.

Эти и другие аспекты настоящего изобретения будут очевидны и более понятны со ссылками на варианты осуществления изобретения, показанных на чертежах, на которых:

фиг.1 схематически показывает первый вариант осуществления системы согласно настоящему изобретению;

фиг.2 более детально схематически показывает приемное устройство согласно настоящему изобретению;

фиг.3 более детально схематически показывает устройство воспроизведения согласно настоящему изобретению; и

фиг.4 схематически показывает второй вариант осуществления системы.

На всех чертежах одинаковые ссылочные позиции обозначают аналогичные или соответствующие признаки. Некоторые из признаков, обозначенных на чертежах, обычно реализуются в виде программного обеспечения и таким образом представляют программные сущности, такие как программные модули или объекты.

Фиг.1 схематически изображает систему 100, содержащую передающее устройство 101 и приемное устройство 110, соединенные через сеть 105, такую как Интернет. К сети также подключен сервер 130 ключей и сервер 140 лицензий, чье функционирование станет понятным ниже. Система 100 позволяет приемному устройству 110 загрузить единицы контента, такие как единица 102 контента (содержимого), из передающего устройства 101. В предпочтительном варианте осуществления изобретения передающее устройство 101 и приемное устройство 110 соединены способом точка-точка, что позволяет им совместно использовать файлы друг с другом. В этом варианте осуществления изобретения может быть обеспечен сервер директорий (не показан) для того, чтобы позволить приемному устройству 110 найти, какие файлы доступны на передающем устройстве 101, без необходимости прямого контакта с передающим устройством 101. Это особенно полезно, если передающее устройство 101 является одним из множества

передающих устройств, соединенных друг с другом и с приемным устройством 110 способом точка-точка. В таком случае приемное устройство 110 может дополнительно быть приспособлено для функционирования в качестве передающего устройства для других устройств в данной системе способом точка-точка. В другом варианте осуществления изобретения передающее устройство 101 является файл-сервером, с которого приемное устройство 110 может загрузить единицы контента (содержимого).

Термин «единица контента» (содержимого) относится к материалам любого вида, которые люди могут желать загрузить. В частности, он относится к таким единицам как телевизионные программы, фильмы, музыка, статьи или книги. Единица 102 контента делается доступной на передающем устройстве 101 в защищенном виде. В предпочтительном варианте осуществления изобретения единица 102 контента сделана доступной в формате «Digifile» Intertrust, известном, например, из патента США 5892900. Также могут быть использованы другие способы защиты единиц контента, такие как формат CD-2. Единица 102 контента в защищенном формате необязательно может сопровождаться «дразнилкой», представляющей единицу контента в незащищенном формате. Это позволяет пользователю просмотреть дразнилку для того, чтобы определить, нравится ли ему единица контента, не покупая ее.

Приемное устройство 110 способно загрузить единицу 102 контента, если оно сделано доступным в таком защищенном формате, как это станет ясно ниже. Приемное устройство 110 может быть, например, телевизионной приставкой, персональным компьютером, шлюзом к домашней сети или устройством бытовой электроники (БЭ). С соответствующими разрешениями оно может затем воспроизвести единицу 102 контента, возможно, с помощью отдельного устройства воспроизведения (не показано). Например, приемное устройство 110 может быть телевизионной приставкой, которая загружает единицу 102 контента и передает ее на персональную развлекательную систему, которая может проиграть ее для пользователя.

Пользователь может купить файл лицензии для использования с единицей 102 контента от сервера 140 лицензий. Этот файл лицензии предоставляет набор разрешений, например разрешение воспроизведения музыки или разрешение сохранить единицу контента на носителе информации. Конечно, пользователь должен заплатить определенную сумму денег за каждое разрешение. Эти деньги могут быть предоставлены при сообщении информации о кредитной карте пользователя или при помощи идентификации пользователя и зачисления некоторой суммы денег на счет пользователя, или любым другим способом проведения платежей через сеть. Файл лицензии также содержит ключ дешифрования или другую информацию, требующуюся для доступа к единице 102 контента.

Когда пользователь покупает разрешение на запись единицы 102 контента, приемное устройство 110 может записать единицу 102 контента на носитель 111 информации, предпочтительно записываемый компакт диск, хотя, конечно, подойдут и другие носители информации, такие как записываемые универсальные диски (DVD), жесткие диски или карты твердотельной памяти. Единица 102 контента записывается на носитель 111 информации защищенным способом, например, в том же защищенном формате, в котором производилась загрузка. Однако большие преимущества дает применение другого способа защищенного распространения контента, например, в случае, если устройства, предполагаемые для чтения единицы 102 контента из носителя 111 информации, не могут обработать защищенный формат, в котором загружена единица 102 контента.

Затем пользователь может предоставить носитель 111 информации, предпочтительно являющийся съемным носителем информации, в подходящее устройство воспроизведения, такое как устройство 120 воспроизведения видео или устройство 121 воспроизведения аудио. Они затем могут прочесть единицу 102 контента с носителя 111 информации и проиграть ее для пользователя. Для того чтобы сделать это, им требуется разрешение на воспроизведение, предоставляемое в файле лицензии для единицы 102 контента. Каким образом они могут получить это разрешение, объяснено ниже со ссылками

на фиг.3.На фиг.2 более детально схематически показано приемное устройство 110. Единица 102 контента загружается модулем 201 загрузки, как объяснялось выше. Модуль 201 загрузки может быть, например, хорошо известным клиентом совместно используемого файла Napster. Модуль 202 транскодирования обрабатывает загруженную единицу 102 контента, преобразуя ее в формат, подходящий для сохранения на носителе 111 информации. Это может включать в себя дешифрование единицы 102 контента и ее шифрование с применением другого способа шифрования. Однако если оригинальный защищенный формат является приемлемым, необходимость в модуле 202 транскодирования отсутствует. Затем модуль 203 записи записывает единицу 102 контента на носитель 111 информации.

Модуль 204 лицензирования получает файл 141 лицензии от сервера 140 лицензий. Этот файл 141 лицензии должен содержать, по меньшей мере, разрешение на запись единицы 102 контента на носитель 111 информации. Если разрешение на запись не подразумевает разрешение на воспроизведение сохраненной единицы 102 контента, то файл 141 лицензии также должен содержать разрешение на воспроизведение. Модуль 204 лицензирования является интерфейсом между сервером 140 лицензий и пользователем и может быть реализован как уже известный модуль лицензирования, например модуль лицензирования, предоставляемый в варианте Intertrust. Этот модуль лицензирования предоставляет пользователю интерфейс, с помощью которого пользователь может подобрать лицензионные условия для единицы 102 контента, такие как разрешение однократного воспроизведения за небольшую сумму денег, однократное бесплатное воспроизведение в обмен на заполнение опросного листа или воспроизведение в течение месяца за большую сумму денег.

Модуль 204 лицензирования предоставляет файл 141 лицензии, если он имеет соответствующее разрешение, модулю 205 фиксации лицензии, который производит зашифрованную версию файла 141 лицензии, на которую ниже ссылаются как на Фиксатор Лицензии. Файл 141 лицензии предпочтительно шифруется с использованием ключа сессии (сеанса), на который ниже ссылаются как на Ключ Шифрования фиксатора Лицензии (КШФЛ). КШФЛ может быть сгенерирован с применением известных способов генерации ключей сессии, например путем хеширования выходного сигнала генератора псевдослучайных чисел для получения последовательности требуемой длины, например 128-битную хэш-функцию такую, как MD5, когда для шифрования файла 141 лицензии применяется 128-битный алгоритм шифрования.

Модуль 205 фиксации лицензии предоставляет Фиксатор Лицензии модулю 203 записи, который записывает его на носитель 111 информации вместе с единицей 102 контента. Для некоторых носителей информации, например записываемых компакт дисков, требуется, чтобы все данные были записаны за один раз. При использовании таких носителей информации, возможно, модуль 203 записи может иметь буфер для данных, предназначенных для записи, до тех пор, пока не будут получены все данные. Конечно, для, например, сменных жестких дисков в этом нет необходимости.

Затем КШФЛ также записывается на носитель 111 информации, но в зашифрованном виде. Устройство воспроизведения, которое может прочесть КШФЛ с носителя 111 информации и дешифровать его, может дешифровать файл 141 лицензии из фиксатора Лицензии и затем иметь возможность воспроизвести единицу 102 контента. При предоставлении единицы 102 контента и файла 141 лицензии таким способом данное изобретение позволяет пользователю воспроизводить сохраненную единицу 102 контента на устройстве воспроизведения, которому не требуется быть подключенным к сети 105.

В качестве альтернативы применению ключа сессии файл 141 лицензии также может быть зашифрован непосредственно с ключом шифрования, соответствующий ему ключ дешифрования доступен на устройстве воспроизведения, которое позже будет иметь доступ к носителю 111 информации. Шифрование может быть симметричным и несимметричным.

Желательно, чтобы воспроизведение единицы 102 контента было ограничено

определенным ограниченным числом устройств воспроизведения, поскольку это позволяет владельцу авторских прав контролировать использование единицы 102 контента. Однако управление устройствами, которые могут проигрывать контент, должно быть независимым от хранения единицы 102 контента на самом носителе 111 информации для того, чтобы сделать систему 100 соответствующую ожиданиям пользователя. Обычно покупатель контента не только проигрывает его сам, но также и его семья проигрывает его на различных устройствах, принадлежащих семье. Друзья и соседи также могут желать прослушать единицу 102 контента. Вообще говоря право проигрывать единицу 102 контента должно быть предоставлено определенной группе людей или группе устройств, которыми владеет указанная группа людей. Для того чтобы определить группу устройств, каждой группе присваивается Идентификатор Группы. Единица 102 контента связана с Идентификатором Группы, так что любое устройство в группе может воспроизвести единицу 102 контента с носителя 111 информации. С этой целью файл лицензии зашифрован таким образом, что любое устройство в группе может дешифровать его, но устройство вне группы не может.

В предпочтительном варианте осуществления изобретения КШФЛ шифруется с открытым ключом из пары открытый/секретный ключ, ассоциированной с группой, посредством чего все устройства в группе имеют доступ к соответствующему секретному ключу. В качестве альтернативы может применяться схема шифрования секретного ключа. Модуль 205 фиксации лицензии предлагает пользователю выбрать Идентификатор Группы, например, из списка, отображаемого на дисплее, подсоединенного к приемному устройству 110, и получает открытый ключ для группы, например, извлекая его с сервера 130 ключей. Затем оно шифрует КШФЛ с открытым ключом группы и предоставляет зашифрованный КШФЛ модулю 203 записи для записи на носитель 111 информации. После этого носитель 111 информации может быть предоставлен устройству воспроизведения, такому как устройство 120 воспроизведения видео или устройство 121 воспроизведения аудио.

Приемное устройство 110 может быть реализовано в виде компьютерного программного продукта 200, который организован так, что процессор выполняет шаги, описанные выше. Компьютерный программный продукт 200 позволяет программируемому устройству при исполнении указанного компьютерного продукта функционировать в качестве приемного устройства 110. Поскольку приемное устройство 110 не требует доступа к секретным ключам, то при использовании схемы шифрования с открытым ключом становится возможным полная реализация приемного устройства в виде компьютерного программного продукта 200, который может быть загружен и запущен на персональном компьютере, например, как дополнительный модуль к программе файлового обмена, такой как Napster. Это обеспечивает расширение клиента Napster, с которым пользователи смогут загружать и распространять музыкальные файлы, но без удаления контроля, желаемого владельцами авторских прав.

Фиг.3 более детально схематически показывает устройство 121 воспроизведения. Другие устройства воспроизведения, такие как устройство 120 воспроизведения видео, могут быть реализованы таким же образом. Пользователь может предоставить носитель 111 информации устройству 121 воспроизведения, например, вставляя его в приемное устройство 301. Модуль 302 декодирования считывает зашифрованный файл 141 лицензии с носителя 111 информации и дешифрует его, используя секретный ключ, хранящийся в модуле 309 защищенного хранения. В предпочтительном варианте осуществления изобретения модуль 302 декодирования считывает зашифрованный КШФЛ с носителя 111 информации и использует сохраненный секретный ключ для дешифрования зашифрованного КШФЛ. Модуль 302 декодирования затем использует полученный таким образом КШФЛ для дешифрования Фиксатора Лицензии и получает файл 141 лицензии.Может случиться, что этап дешифрования требует секретного ключа, который не хранится в модуле 309 защищенного хранения. В этом случае модуль 302 декодирования будет не в состоянии дешифровать файл 141 лицензии. Также устройство 121

воспроизведения может быть включено более чем в одну группу. В таком случае оно будет иметь множество ключей дешифрования, хранящихся в модуле защищенного хранения, один ключ на каждую группу. Таким образом, модуль 302 декодирования сначала должен проверить, хранится ли верный ключ в модуле 309 защищенного хранения, и в зависимости от результатов проверки либо дешифровать файл 141 лицензии либо уведомить пользователя, что получение файла 141 лицензии невозможно из-за отсутствия ключа дешифрования.

Такая проверка может быть проведена несколькими способами, например путем сравнения идентификатора ключа для хранящегося секретного ключа с идентификатором ключа, сохраненного вместе с зашифрованным файлом 141 лицензии. В качестве альтернативы файл 141 лицензии может содержать известный фрагмент информации, такой как номер версии или фиксированная текстовая строка. В этом случае модуль 302 декодирования может попытаться дешифровать файл 141 лицензии и затем сравнить результат с известным фрагментом информации. Если в выходном сигнале ожидаемый фрагмент информации отсутствует, то использованный ключ дешифрования является неверным. В качестве альтернативы секретные ключи могут содержать идентификаторы групп, к которым они принадлежат, и носитель 111 информации может содержать идентификаторы групп, для которых был зашифрован файл 141 лицензии. Модуль 302 декодирования затем может извлечь последний идентификатор и провести поиск секретного ключа, содержащего подходящий идентификатор в модуле 309 защищенного хранения. Модуль декодирования также может просто попытаться дешифровать файл 141 лицензии с каждым ключом дешифрования до тех пор, пока один из них не подойдет для получения корректного файла лицензии.

Этап дешифрования может быть реализован многими способами, частично зависящими от того, как хранится секретный ключ в модуле 309 защищенного хранения. Модуль 309 может быть реализован в виде аппаратного модуля со встроенным программным обеспечением дешифрования, так что модуль 302 декодирования может предоставить зашифрованный файл 141 лицензии модулю 309, который дешифрует его, используя подходящий ключ дешифрования, и возвращает файл 141 лицензии в простой форме модулю 302 декодирования. Это обеспечивает больший уровень защищенности, так как реальный секретный ключ хранится в аппаратном модуле, устойчивом к внешним воздействиям, и не может быть считан злонамеренным пользователем. В качестве альтернативы модуль 309 защищенного хранения может быть просто постоянным запоминающим устройством (ПЗУ), из которого модуль 302 декодирования может считывать секретный ключ дешифрования и самостоятельно дешифровать файл 141 лицензии. Модуль 309 может быть предоставлен на смарт-карте.

Модуль 302 декодирования предоставляет файл 141 лицензии модулю 305 воспроизведения. Модуль 305 воспроизведения считывает сохраненную единицу 102 контента с носителя 111 информации и проверяет, есть ли разрешение воспроизведения в файле 141 лицензии. Если да, он проигрывает единицу 102 контента, например, генерируя аудиосигналы на громкоговорителе 306.

Секретный ключ, установленный в устройстве 121 воспроизведения, в модуле 309 защищенного хранения может быть просто секретным ключом группы, соответствующим открытому ключу, используемому приемником 111, как это описано в связи с фиг.2. Это требует распределения секретного ключа группы среди всех устройств, добавленных в группу, что не является очень практичным и конечно не безопасно, если только не используются высокоустойчивые к внешним воздействиям аппаратные средства, такие как смарт-карты. Однако, для этого требуется, чтобы пользователь приобрел некоторое количество смарт-карт, по одной на каждое устройство в группе, что является обременительным.

Следовательно, является предпочтительным, чтобы каждое устройство в группе имело свою пару открытый/секретный ключ, ассоциированную с ним, посредством чего секретный ключ безопасно устанавливается в устройстве воспроизведения. Это может быть сделано,

например, на заводе, где изготавливается устройство воспроизведения. Для большей безопасности пара открытый/секретный ключ для устройства может быть сгенерирована при помощи независимого устройства, такого как Служба Сертификации (СС), и предоставлена на завод для установки производителем.

Устройство 121 воспроизведения имеет модуль 306 регистрации, который может предоставить открытый ключ для регистрации в Системе 310 Управления Распределением Контента (СУРК) вместе с уникальным идентификатором для устройства воспроизведения. Такой уникальный идентификатор может, например, содержать номер производителя, номер типа и серийный номер. Регистрация может быть произведена по запросу пользователя или когда устройство 121 воспроизведения включается в первый раз, или в другой подходящий момент. В качестве альтернативы открытый ключ может быть зарегистрирован СИ при установке производителем пары открытый/секретный ключ.

Как станет ясно ниже со ссылками с фиг.4, СУРК 310 затем шифрует секретный ключ группы один раз для каждого устройства в группе, используя зарегистрированный открытый ключ этого устройства. Зашифрованные секретные ключи затем посылаются в ответ модулям регистрации устройств воспроизведения, которые могут дешифровать их, используя свои собственные секретные ключи. Затем они сохраняют секретный ключ в своих модулях защищенного хранения. С этого момента они могут дешифровать любой файл 141 лицензии, зашифрованный с открытым ключом группы, используя соответствующий секретный ключ группы. При распространении секретного ключа группы подобным образом отсутствуют моменты, когда секретный ключ открыт для злонамеренного пользователя, и отсутствуют устройства воспроизведения, которые могут получить доступ к секретному ключу без предварительной регистрации. Это делает возможным, например, взимать с пользователя большую плату, если он желает получить разрешение на распространение единицы 102 контента для большей группы устройств. Дополнительно количество устройств в группе может быть ограничено в соответствии с желанием владельца авторских прав.

Устройство 120 воспроизведения может быть реализовано в виде компьютерного программного продукта 300, который организован так, что процессор выполняет шаги, описанные выше. Компьютерный программный продукт 300 позволяет программируемому устройству при исполнении указанного компьютерного продукта функционировать как устройство 120 воспроизведения. Должны быть предприняты меры, гарантирующие, что секретный ключ не скопирован на другое устройство, так как это позволило бы другому устройству имитировать устройство 120 воспроизведения, что нарушает возможность взимать плату за каждое устройство, на котором должна проигрываться сохраненная единица 102 контента.

Фиг.4 схематически показывает другой вариант осуществления изобретения 100, который иллюстрирует процесс регистрации групп и устройств. СУРК 310 поддерживает список 402 зарегистрированных групп G1, G2, G3 и устройств D1,..., D9 в каждой группе. Пользователь может запросить в СУРК создание новой группы на СУРК 310. Затем СУРК генерирует пару открытый/секретный ключ для данной группы. Открытый ключ группы может затем быть предоставлен серверу 130 ключей для загрузки приемным устройством 110. При предоставлении открытого ключа для группы на сервер 130 ключей становится возможным для одного пользователя сохранить в защищенном виде единицы контента, которые другой пользователь сможет воспроизвести. Так, например, пользователь может загрузить и сохранить набор песен на носителе 111 информации, используя открытый ключ группы, зарегистрированный на друга. Он может затем отдать носитель 111 информации другу, например, как подарок, и он затем сможет проиграть его на каждом устройстве в его группе. Включая только те единицы контента, которые, как он знает, понравятся его другу, и сохраняя их, используя группу его друга, пользователь создает персональный подарок.

После того как пользователь зарегистрировал группу, он может добавить в нее устройство воспроизведения. Если устройство, которое он хочет добавить, еще не

зарегистрировано, пользователь должен сначала зарегистрировать его, чтобы оно было добавлено в список 403 устройств, например, активировав модуль 306 регистрации устройства. При добавлении устройства в группу СУРК 310 шифрует секретный ключ открытым ключом этого устройства. Например, если пользователь добавил устройство D6 в группу G1, СУРК 310 шифрует секретный ключ G1 открытым ключом РК6. Этот зашифрованный секретный ключ необходим модулю 302 декодирования устройства D6. После того как устройство, которое он желает добавить, было зарегистрировано СУРК 310, он может просто выбрать его из списка 403 устройств предоставленного СУРК 310 и содержащего идентификаторы устройств UID1,..., UID9 и ассоциированных открытых ключей РК1,..., РК9 и добавить его в группу.

Пользователь также может удалять устройства из списка группы, например, для того, чтобы освободить место для новых устройств, если количество устройств в группе ограничено СУРК 310. Это делает возможным пользователю удалить устройство из списка для группы, но все еще проигрывает на этом устройстве контент, предназначенный для данной группы. Это возможно в силу того, что устройство все еще имеет секретный ключ группы, с которым можно дешифровать КШФЛ, так что файл 141 лицензии может быть дешифрован и единица 102 контента может быть проиграна. Это может быть предотвращено, например, периодической заменой пары открытый/секретный ключ группы и предоставление нового секретного ключа только устройствам, находящимся в списке группы на этот момент. К тому же назначение регистрационных платежей за каждое устройство, добавленное в группу или удаленное из нее, уменьшит побуждение пользователя к частой манипуляции списком его группы.

Для того чтобы гарантировать аутентичность открытых ключей, предоставляемых сервером 130 ключей, они могут быть сертифицированы Службой Сертификации (СС) перед тем, как станут доступными на сервере 130 ключей. Приемное устройство 110 может быть обеспечено сертификатом СС, так что оно может подтвердить аутентичность сертификатов и тем самым подтвердить аутентичность открытых ключей групп. Сертификат или открытый ключ для СС может быть загружен в приемное устройство 110 производителем, или быть загруженным с сервера 130 ключей при необходимости. Однако загрузка сертификата для СС в приемное устройство 130 производителем является более защищенным, так как это предоставляет для злонамеренных пользователей меньше возможностей подменить этот сертификат.

Дополнительным преимуществом записи единицы 102 контента на носителе 111 информации таким способом является то, что устройство воспроизведения, которое не принадлежит подходящей группе, все же может получить доступ к единице 102 контента, если оно получит новый файл лицензии. Единица 102 информации является, в конце концов, сохраненной в защищенном формате, доступ к которому может быть получен с подходящим файлом лицензии. Так, пользователь, создавший носитель 111 информации с его любимыми музыкальными треками, может одолжить носитель 111 информации другу, чьи устройства не входят в группу пользователя. Затем друг может купить лицензию на однократное воспроизведение и получить доступ к трекам на носителе 111 информации, для того чтобы узнать, что нравится пользователю. Если они ему также понравятся, он может попросить пользователя, чтобы он добавил его в свою группу, или самому загрузить треки. Пользователь также может создать новую группу, которая включает в себя его устройства и устройства его друга, и затем создать новый носитель информации, содержащий треки, которые нравятся им обоим.

Формула изобретения

1. Устройство (121) воспроизведения для воспроизведения единицы (102) контента, сохраненной на носителе (111) информации, содержащее средство (305) воспроизведения для воспроизведения единицы (102) контента в соответствии с разрешением в файле (141) лицензии для единицы (102) контента, и использования ключа дешифрования, содержащегося в файле лицензии, для дешифрования единицы контента, причем файл

(141) лицензии сохранен на носителе (111) информации в зашифрованном виде, средство (309) защищенного хранения для хранения одного или более ключей дешифрования в устройстве воспроизведения, при этом каждый ключ дешифрования ассоциирован с соответствующей группой устройств воспроизведения, средство (306) регистрации для регистрации открытого ключа пары открытый/секретный ключ, ассоциированного с устройством (121) воспроизведения, на удаленном сервере, называемом Системой Управления Распределением Контента (СУРК) (310), причем секретный ключ упомянутой пары открытый/секретный ключ сохранен в средстве (309) защищенного хранения, и для приема в ответ ключа дешифрования, ассоциированного с группой устройств воспроизведения, зашифрованного упомянутым открытым ключом, дешифрования упомянутого шифрованного ключа дешифрования и сохранения упомянутого ключа дешифрования в средстве (309) защищенного хранения, средство (302) декодирования для проверки, подходит ли сохраненный ключ дешифрования для дешифрования зашифрованного файла (141) лицензии, и, если да - дешифрования файла (141) лицензии, используя сохраненный ключ дешифрования, и предоставления дешифрованного файла (141) лицензии средству (305) воспроизведения.

2. Устройство (121) воспроизведения по п.1, в котором файл (141) лицензии хранится зашифрованным ключом сеанса, называемым Ключом Шифрования Фиксатора Лицензии (КШФЛ), причем упомянутый КШФЛ сохраняется на носителе (111) информации зашифрованным ключом шифрования КШФЛ, причем один или более ключей дешифрования являются ключами дешифрования КШФЛ, и средство (302) декодирования выполнено с возможностью проверки, подходит ли сохраненный ключ дешифрования КШФЛ для дешифрования зашифрованного КШФЛ, и, если да - получения КШФЛ из зашифрованного КШФЛ, используя сохраненный ключ дешифрования КШФЛ, и дешифрования файла (141) лицензии, используя КШФЛ.

3. Устройство (121) воспроизведения по п.1, в котором единица (102) контента содержит, по меньшей мере, одно из видеоданных или аудиоданных.

4. Устройство (121) воспроизведения по п.1, в котором сохраненный ключ дешифрования является секретным ключом из пары открытый/секретный ключ.

5. Устройство (121) воспроизведения по п.1, в котором носителем (111) информации является карта твердотельной памяти.

6. Устройство (121) воспроизведения по п.1, в котором устройством (309) защищенного хранения является сменный носитель информации.

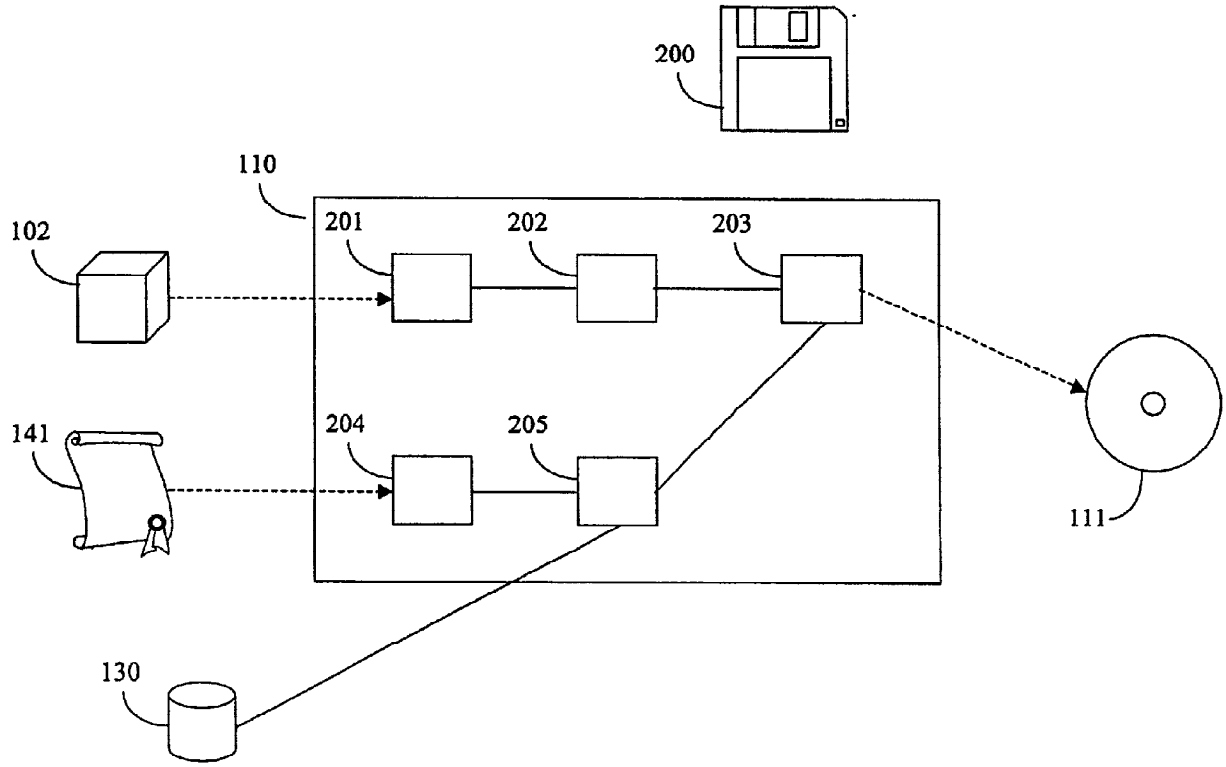
7. Компьютерный программный продукт (300) для обеспечения возможности программируемому устройству при выполнении упомянутого компьютерного продукта функционировать в качестве устройства (121) воспроизведения, содержащий средство (305) воспроизведения для воспроизведения единицы (102) контента в соответствии с разрешением в файле (141) лицензии для единицы (102) контента, и использования ключа дешифрования, содержащегося в файле лицензии, для дешифрования упомянутой единицы контента, причем файл (141) лицензии сохранен на носителе (111) информации в зашифрованном виде, средство (306) регистрации для регистрации открытого ключа пары открытый/секретный ключ, ассоциированного с устройством (121) воспроизведения, на удаленном сервере, называемом Системой Управления Распределением Контента (СУРК) (310), причем секретный ключ упомянутой пары открытый/секретный ключ сохранен в средстве (309) защищенного хранения, и для приема в ответ ключа дешифрования, ассоциированного с группой устройств воспроизведения, зашифрованного упомянутым открытым ключом, дешифрования упомянутого зашифрованного ключа дешифрования и сохранения упомянутого ключа дешифрования в средстве (309) защищенного хранения, средство (302) декодирования для проверки, подходит ли сохраненный ключ дешифрования для дешифрования зашифрованного файла (141) лицензии, и, если да - дешифрования файла (141) лицензии, используя сохраненный ключ дешифрования, и предоставления дешифрованного файла (141) лицензии средству (305) воспроизведения.

8. Система (100), содержащая устройство (121) воспроизведения по п.1 и сервер

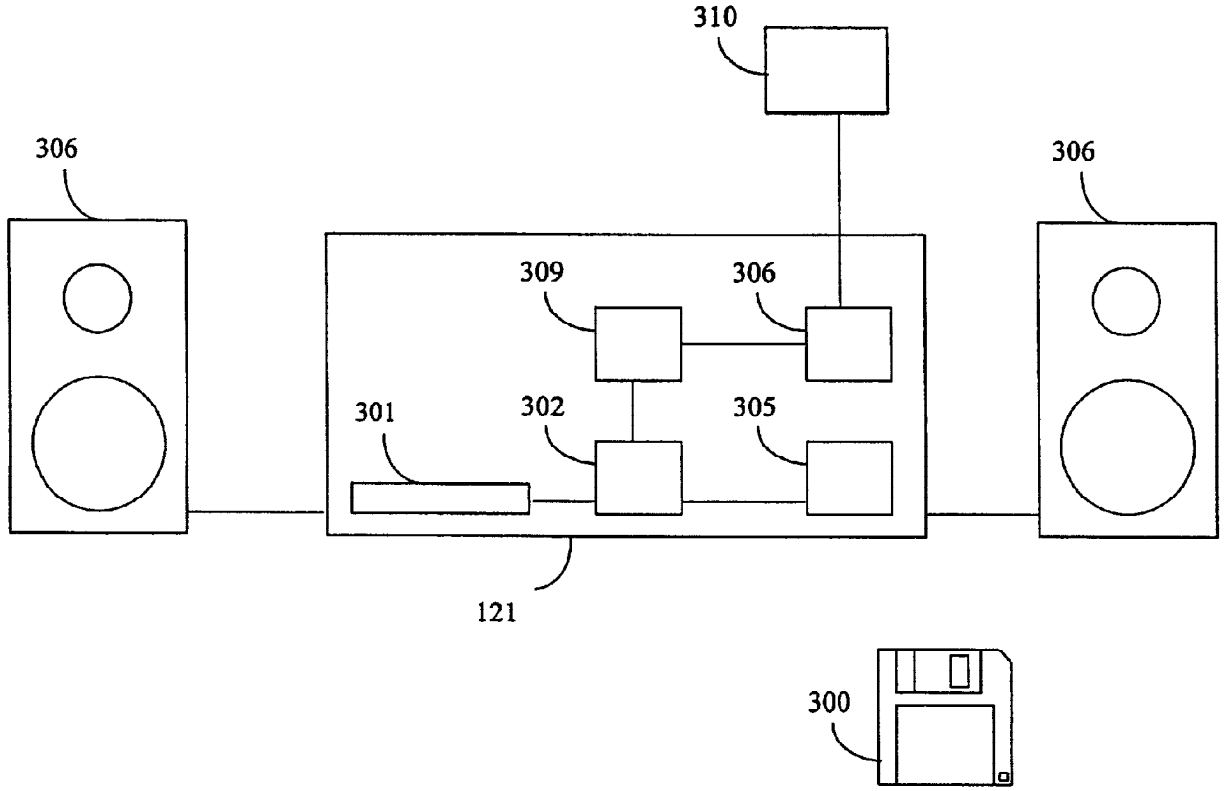
(310), причем устройство (121) воспроизведения дополнительно содержит средство (306) регистрации для регистрации открытого ключа пары открытый/секретный ключ, ассоциированного с устройством (121) воспроизведения, на сервере (310), при этом сервер (310) выполнен с возможностью шифрования ключа дешифрования, связанного с группой, членом которой является устройство (121) воспроизведения, упомянутым зарегистрированным открытым ключом и передачи шифрованного ключа дешифрования на устройство (121) воспроизведения, при этом устройство (121) воспроизведения выполнено с возможностью принимать шифрованный ключ дешифрования, дешифровывать упомянутый шифрованный ключ дешифрования для сохранения упомянутого ключа дешифрования в средстве (309) защищенного хранения.

9. Система (100) по п.8, в которой сервер выполнен с возможностью ограничивать количество устройств воспроизведения в группе.

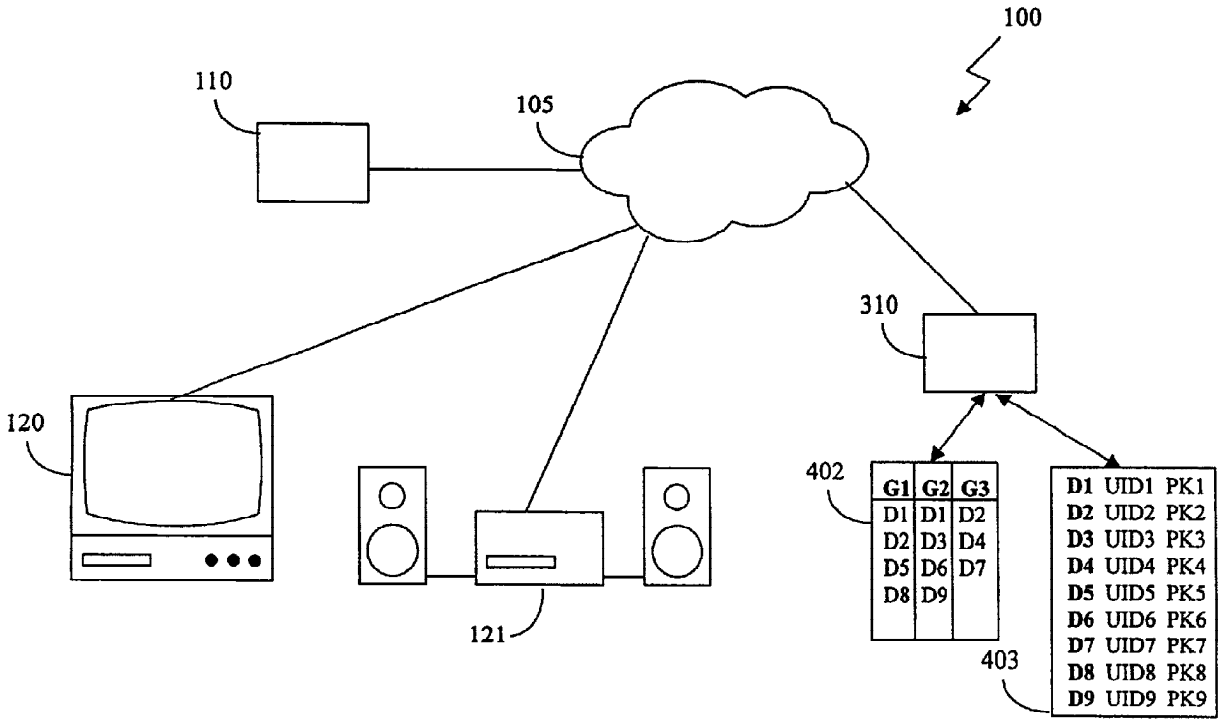
10. Система (100) по п.8, в которой сервер выполнен с возможностью периодически заменять ключи шифрования и дешифрования для группы и подавать только замененный ключ дешифрования на устройства, которые являются членами упомянутой группы.


200
110
102
201
202
203
141
204
205
111
130

ФИГ.2


310
306
306
309
306
301
302
305
121
300

ФИГ.3


100
110
105
310
120
121
402
403
G1 G2 G3
D1 D1 D2
D2 D3 D4
D5 D6 D7
D8 D9
D1 UID1 PK1
D2 UID2 PK2
D3 UID3 PK3
D4 UID4 PK4
D5 UID5 PK5
D6 UID6 PK6
D7 UID7 PK7
D8 UID8 PK8
D9 UID9 PK9

ФИГ. 4