РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 369 024** (13) **C2**

(51) МПК
H04L 9/08 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21), (22) Заявка: **2005125741/09, 13.01.2004**

(24) Дата начала отсчета срока действия патента:
13.01.2004

(30) Конвенционный приоритет:
15.01.2003 JP 2003-7349
04.04.2003 JP 2003-101455

(43) Дата публикации заявки: **10.01.2006**

(45) Опубликовано: **27.09.2009** Бюл. № **27**

(56) Список документов, цитированных в отчете о поиске: **RU 2154856 C1, 2000.08.20. RU 2067313 C1, 1996.09.27. EP 1176754 A3, 2002.01.30. WO 01/52234 A1, 2001.07.19. US 6301660 B1, 2001.10.09.**

(85) Дата перевода заявки PCT на национальную фазу: **15.08.2005**

(86) Заявка PCT:
JP 2004/000155 (13.01.2004)

(87) Публикация PCT:
WO 2004/064313 (29.07.2004)

Адрес для переписки:
129090, Москва, ул. Б.Спасская, 25, стр.3, ООО "Юридическая фирма Городисский и Партнеры", пат.пов. Ю.Д.Кузнецову, рег.№ 595

(72) Автор(ы):
НАКАНО Тосихиса (JP),
ОХМОРИ Мотодзи (JP),
МАЦУЗАКИ Нацуме (JP),
ТАТЕБАЯСИ Макото (JP),
ЯМАМОТО Наоки (JP),
ИСИХАРА Хидеси (JP)

(73) Патентообладатель(и):
ПАНАСОНИК КОРПОРЭЙШН (JP)

(54) СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИОННОГО СОДЕРЖАНИЯ, УСТРОЙСТВО ГЕНЕРАЦИИ ДАННЫХ КЛЮЧЕЙ И УСТРОЙСТВО ВОСПРОИЗВЕДЕНИЯ

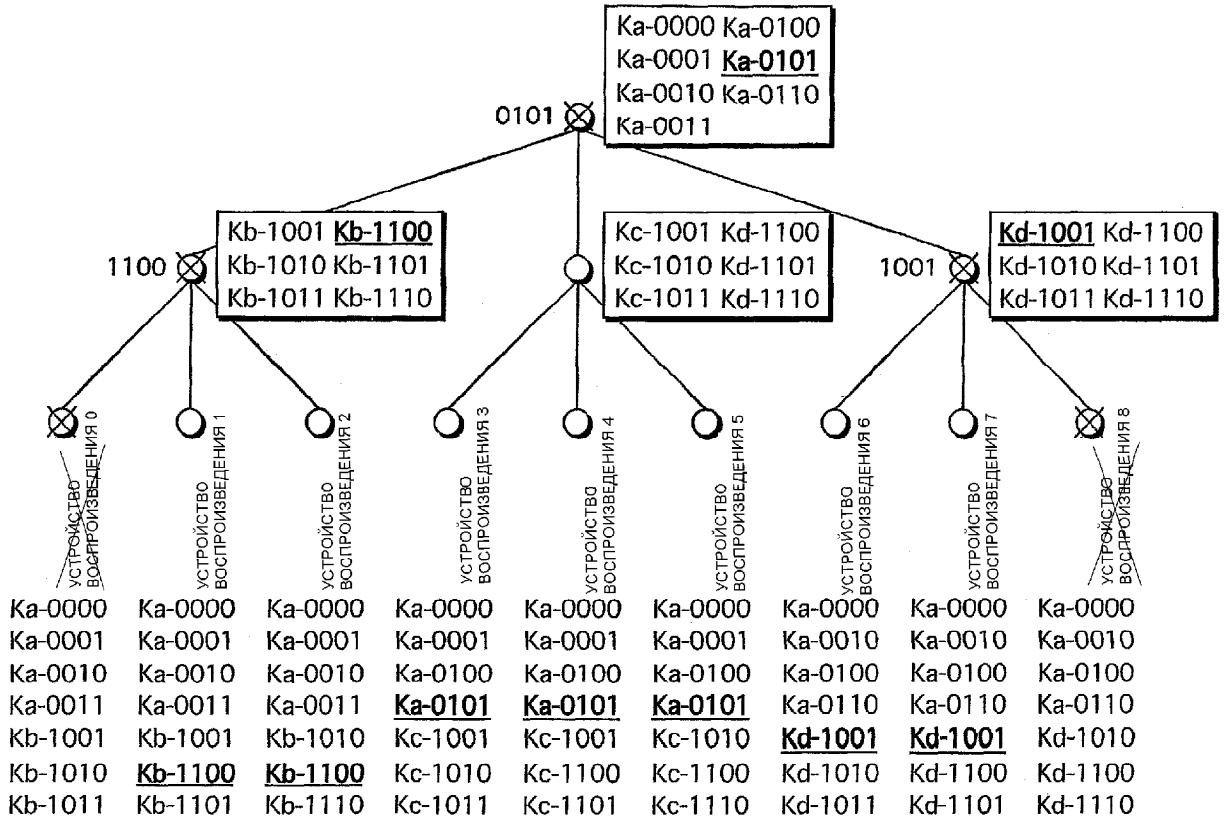
(57) Реферат:

Изобретение относится к системе для записи цифровых данных информационного содержания и воспроизведения информационного содержания. Система защиты содержания содержит устройство генерации данных ключей и пользовательский терминал. Устройство генерации данных ключей преобразует первые данные ключа, предназначенные для использования содержания, на основе предварительно заданного правила преобразования, при этом генерируя вторые данные ключа, зашифровывает вторые данные ключа с использованием ключа устройства, хранимого действительным оконечным устройством, и выводит зашифрованные данные ключа. Пользовательский терминал получает зашифрованные данные ключа, дешифрует зашифрованные данные ключа с

RU 2369024 C2

RU 2369024 C2

использованием ключа устройства, хранимого в пользовательском терминале, при этом генерируя вторые данные ключа, преобразует вторые данные ключа на основе правила обратного преобразования, соответствующего правилу преобразования, при этом генерируя первые данные ключа, и использует содержание с применением первых данных ключа. Технический результат - обеспечение защиты содержания путем предотвращения незаконного получения ключа. 5 н. и 25 з.п. ф-лы, 16 ил.



ФИГ. 3

RU 2369024 C2

RU 2369024 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY,
PATENTS AND TRADEMARKS

(19) **RU** (11) **2 369 024** (13) **C2**

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

(12) ABSTRACT OF INVENTION

(21), (22) Application: **2005125741/09, 13.01.2004**

(24) Effective date for property rights:
13.01.2004

(30) Priority:
15.01.2003 JP 2003-7349
04.04.2003 JP 2003-101455

(43) Application published: **10.01.2006**

(45) Date of publication: **27.09.2009 Bull. 27**

(85) Commencement of national phase: **15.08.2005**

(86) PCT application:
JP 2004/000155 (13.01.2004)

(87) PCT publication:
WO 2004/064313 (29.07.2004)

Mail address:
129090, Moskva, ul. B.Spasskaja, 25, str.3, OOO "Juridicheskaja firma Gorodisskij i Partnery", pat.pov. Ju.D.Kuznetsovu, reg.№ 595

(72) Inventor(s):
NAKANO Tosikhisa (JP),
OKhMORI Motodzi (JP),
MATsUZAKI Natsume (JP),
TATEBAJaSI Makoto (JP),
JaMAMOTO Naoki (JP),
ISIKhARA Khidesi (JP)

(73) Proprietor(s):
PANASONIK KORPOREhJShN (JP)

RU 2369024 C2

RU 2369024 C2

(54) SYSTEM FOR PROTECTING INFORMATION CONTENT, DEVICE FOR GENERATING KEY DATA AND DISPLAY DEVICE

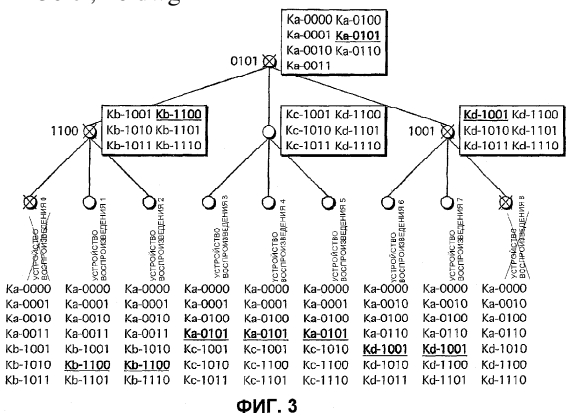
(57) Abstract:

FIELD: information technology.

SUBSTANCE: invention relates to a system for recording digital data and displaying information content. The system for protecting content has a device for generating key data and a user terminal. The device for generating key data transforms the first key data, meant for using content, based on a preset transformation rule. While generating second key data, the device encrypts second key data using a device key, stored by a real terminal device, and outputs encrypted key data. The user terminal receives encrypted key data, decrypts the data using a device key, stored in the user terminal. While generating second key data, the terminal transforms second key data based on an inverse transformation rule, which corresponds to the transformation rule, while generating first key data, and uses content, using first key data.

EFFECT: protection of content by preventing unauthorised key reception.

30 cl, 16 dwg



ФИГ. 3

Область техники

Настоящее изобретение относится к системе для записи цифровых данных информационного содержания, которое представляет собой произведение, подобное кинофильму, на носитель записи большой емкости, такой как оптический диск, и воспроизведения информационного содержания.

Предшествующий уровень техники

Для защиты от копирования информационного содержания (контента), которое представляет собой произведение, подобное кинофильму или музыкальному материалу, устройствам воспроизведения назначается множество ключей устройств, и содержание записывается в зашифрованном состоянии на носитель для записи вместе с данными ключей, которые используются для дешифрования содержимого, которое может быть воссоздано только устройством воспроизведения, которому разрешено воспроизводить содержание. Одним из способов управления ключами для генерации данного типа данных ключей является использование древовидной структуры.

Документ 1 раскрывает способ, относящийся к системе управления ключами, которая использует древовидную структуру, в которой объем информации ключей относительно мал и имеется возможность отзыва (аннулирования) индивидуальных ключей. Кроме того, документ 2 раскрывает способ, который основывается на способе, раскрытом в документе 1, и который относится к способу управления ключами для защиты цифрового содержания, препятствующему увеличению количества ключей устройств, сохраняемых заранее в устройствах воспроизведения, при сокращении объема информации ключей, записанной на носителе записи.

Ниже приведено краткое описание способа управления ключами, раскрытого в документе 1.

Организация управления ключами управляет ключами устройств таким образом, что «листья» древовидной структуры поставлены в соответствие по принципу «один к одному» устройствам воспроизведения. Каждое устройство воспроизведения хранит ключи устройства, соответствующие узлам, расположенным на маршруте от корня к листу, соответствующему устройству воспроизведения. Организация управления ключами зашифровывает содержание и ключ МК носителя, используемый для дешифрования содержимого, с использованием ключа К устройства, который представляет собой ключ устройства из всех распределяемых ключей устройств, которые совместно используются максимально возможным числом устройств воспроизведения. Затем организация управления ключами записывает зашифрованный ключ E(K, МК) носителя на носитель записи. Заметим, что E(X, Y) обозначает зашифрованный текст, получаемый шифрованием данных Y данными X ключа.

Если устройство воспроизведения проанализировано внутренним образом и все ключи устройства, сохраненные устройством воспроизведения, выявлены, то организация управления ключами отзывает (аннулирует) выявленные ключи и выбирает из оставшихся ключей устройств те, которые совместно используются максимальным числом устройств воспроизведения, и использует выбранные ключи устройства для шифрования ключа МК носителя.

Как показано на фиг. 11, в случае, если устройство 0 воспроизведения отозвано, ключи Kf, Kb и K1 устройств используются для шифрования ключа МК носителя, при этом генерируя зашифрованные тексты E(Kf, МК), E(Kb, МК) и E(K1, МК), которые записаны на носитель записи.

Соответственно, отозванное устройство 0 воспроизведения не способно получить

ключ МК носителя, поскольку оно не имеет никакого из ключей Kf, Kb и K1 устройств, и только устройства воспроизведения, имеющие любой из ключей Kf, Kb и K1 устройств, способны получить ключ МК носителя.

Таким образом, если уникальность ключей устройства потеряна, например, если соответствующие значения ключа Kf устройства и ключа K1 устройства идентичны, то значения зашифрованных текстов E(Kf, МК) и E(K1, МК), записанных на носитель записи, будут одними и теми же. Это означает, что общеизвестным станет то, что ключи Kf и K1 устройств имеют идентичные значения.

Если устройство 7 воспроизведения позже отзывается, как показано на фиг. 12, то организация управления ключами зашифровывает ключ M носителя с использованием ключей Kb, Kc, K1 и K6 устройств и на носитель записи записывается четыре зашифрованных текста E(Kb, МК), E(Kc, МК), E(K1, МК) и E(K6, МК).

Поскольку ключ Kf устройства, хранимый устройством 7 воспроизведения, уже был раскрыт и ввиду того факта, что стало общеизвестным, что ключи Kf и K1 устройства идентичны, имеется опасность того, что противоправная сторона будет использовать выявленный ключ Kf для дешифрования зашифрованного текста E(K1, МК) и тем самым сможет незаконно получить ключ МК носителя. Если для того чтобы предотвратить такие незаконные действия, зашифрованный текст E(K1, МК) не записывать на носитель записи, то возникает проблема, состоящая в том, что действительное устройство воспроизведения 1 не сможет получить ключ МК носителя и необоснованным образом будет отозвано.

Один из примеров способа, позволяющего предотвратить незаконное получение ключа носителя и при этом исключить возможность незаконного отзыва устройства воспроизведения, состоит в том, чтобы гарантировать уникальность каждого ключа устройства. Более конкретно, поскольку ключи устройств обычно генерируются с использованием генератора случайных чисел, который генерирует последовательность случайных чисел, один способ состоит в проверке, каждый раз, когда генерируется ключ, совпадает или нет ключ устройства с каким-либо из ранее генерированных ключей устройств. Последовательность случайных чисел разрушается, если существует совпадающий ключ, и используется, если не существует совпадающего ключа устройства.

Однако в крупномасштабных системах, в которых число устройств воспроизведения исчисляется в миллиардах, проверка того, совпадает или нет ключ устройства с каким-либо из ранее генерированных ключей устройств, требует чрезвычайно больших затрат времени. Даже если использовать способ управления ключами, раскрытый в документе 2, возникает та же самая проблема времени, требуемого на проведение проверки ключей устройств.

Документ 1

Nakano, Ohmori and Tatebayashi "Digital Content Hogo-you Kagi Kanri Houshiki (Key Management System for Digital Content Protection)", The 2001 Symposium on Cryptography and Information Security, SCIS2001, 5A-5, Jan. 2001.

Документ 2

Nakano, Ohmori and Tatebayashi "Digital Content Hogo-you Kanri Houshiki - Ki-kouzou Pattern Bunkatsu Houshiki (Key Management System for Digital Content Protection - Tree Pattern Division Method)", The 2002 Symposium on Cryptography and Information Security, 15 SCIS2002, 10C-1, Jan. 2002.

Раскрытие изобретения

Ввиду указанных проблем цель настоящего изобретения заключается в обеспечении

системы защиты содержания, которая препятствует незаконному обнаружению ключа носителя и необоснованному отзыву устройства воспроизведения, которое не должно отзываться, без проверки уникальности ключей устройств.

Для достижения указанной цели настоящее изобретение предусматривает систему защиты содержания, которая может использоваться только действительным оконечным устройством, содержащую устройство генерации данных ключей, которое содержит блок преобразования, предназначенный для преобразования на основе предварительно определенного правила преобразования первых данных ключа для использования при использовании содержания, при этом генерируя вторые данные ключа, блок шифрования, предназначенный для шифрования вторых данных ключа с использованием ключа устройства, хранимого действительным оконечным устройством, при этом генерируя зашифрованные данные ключа, блок вывода, предназначенный для вывода зашифрованных данных ключа, и оконечное устройство, которое содерит блок получения, предназначенный для получения зашифрованных данных ключа, блок дешифрования, предназначенный для дешифрования зашифрованных данных ключа с использованием ключа устройства, хранимого в оконечном устройстве, при этом генерируя вторые данные ключа, блок преобразования, предназначенный для преобразования на основе предварительно определенного правила преобразования вторых данных ключа, при этом получая первые данные ключа, и блок использования содержания, предназначенный для использования содержания на основе первых данных ключа.

В соответствии с описанной структурой, даже если ключи устройств имеют идентичные значения, зашифрованные данные ключа не обязательно будут иметь идентичные значения. Кроме того, невозможно определить, имеют или нет ключи устройств идентичные значения, с использованием зашифрованных данных ключа. Поэтому незаконное обнаружение первых данных ключа может быть предотвращено. Соответственно, предотвращается отзыв устройств воспроизведения, которые не должны отзываться.

Краткое описание чертежей

Фиг. 1 - блок-схема, показывающая структуру устройства 100 генерации данных ключей и носителя 300 записи;

Фиг. 2 - древовидная структура, отражающая корреляцию между ключами устройств, в устройстве 100 генерации данных ключей;

Фиг. 3 - иллюстрация корреляции между ключами устройств в случае, когда существуют ключи устройств, которые должны быть отозваны;

Фиг. 4 - содержание обработки преобразования ключа носителя и шифрования;

Фиг. 5 - структура областей записи DVD 300;

Фиг. 6 - блок-схема, показывающая структуру DVD 300 и устройства 200 воспроизведения;

Фиг. 7 - содержание обработки дешифрования зашифрованного ключа носителя и обратного преобразования;

Фиг. 8 - блок-схема алгоритма, показывающая обработку генерации данных ключа в устройстве 100 генерации данных ключей;

Фиг. 9 - блок-схема алгоритма, показывающая операции устройства 200 воспроизведения;

Фиг. 10 - блок-схема, показывающая операции указания позиций записи и генерации информации преобразования в устройстве 200 воспроизведения;

Фиг. 11 - пример способа управления ключами, который использует древовидную

структуру;

Фиг. 12 - пример способа управления ключами, который использует древовидную структуру.

Наилучший режим выполнения изобретения

Ниже описаны варианты осуществления настоящего изобретения со ссылками на чертежи.

Первый вариант осуществления

1. Структура системы защиты от копирования

Система защиты от копирования, как показано на фиг. 1 и 6, содержит устройство 100 генерации данных ключей, множество устройств 200a, 200b, и т.д. воспроизведения и DVD 300. На фиг. 6 обычная структура устройств 200a, 200b, и т.д. воспроизведения показана как устройство 200 воспроизведения.

Устройство 100 генерации данных ключей, которое находится в ведении организации, управляющей ключами, записывает содержание и данные ключей для воспроизведения содержания на DVD 300. Данные ключей выбираются таким образом, что только действительные устройства воспроизведения имеют возможность воспроизводить содержание, и распределяются согласно древовидной структуре.

Устройствам 200a, 200b, и т.д. воспроизведения, которые находятся в ведении соответствующих пользователей, заранее присвоено множество ключей устройств устройством 100 генерации данных ключей. Кроме того, каждое из устройств 200a, 200b, и т.д. воспроизведения выбирает соответствующий ключ устройства из распределенных ключей устройства и использует выбранный ключ устройства для дешифрования и воспроизведения зашифрованного содержания, записанного на DVD 300.

Ниже описана структура каждого из вышеуказанных средств.

1.1 Устройство 100 генерации данных ключей

Устройство 100 генерации данных ключей, как показано на фиг. 1, содержит блок 101 хранения ключей устройств, блок 102 выбора ключей устройств, блок 103 преобразования, блок 104 генерации информации преобразования, блок 105 шифрования ключа носителя, блок 106 шифрования ключа содержания, блок 107 шифрования содержания, блок 108 ввода, блок 109 управления и блок 110 вывода.

Более конкретно, устройство 100 генерации данных ключей представляет собой компьютерную систему, состоящую из микропроцессора, ПЗУ, ОЗУ, блока жесткого диска, блока отображения, клавиатуры, мыши и т.п. Компьютерная программа сохранена в ОЗУ или в блоке жесткого диска, и устройство 100 генерации данных ключей реализует свои функции посредством микропроцессора, работающего в соответствии с компьютерной программой.

(1) Блок 108 ввода и блок 110 вывода

Блок 108 ввода получает введенные данные ключа МК носителя, ключа СК содержания и содержание от внешнего источника и выдает ключ МК носителя на блок 103 преобразования и в блок 106 шифрования ключа содержания, ключ СК содержания в блок 106 шифрования ключа содержания и в блок 107 шифрования содержания и содержание - в блок 107 шифрования содержания.

Заметим, что ключ носителя может представлять собой информацию, уникальную для DVD 300, или ожет представлять собой данные ключа, генерированные из информации, уникальной для DVD 300.

Блок 110 вывода записывает информацию преобразования, зашифрованные данные ключа и зашифрованное содержание на DVD 300 под управлением блока 109

управления.

(2) Блок 109 управления

Блок 109 управления управляет блоком 102 выбора ключей устройств таким образом, чтобы обеспечить выбор им, по меньшей мере, одного ключа устройства из распределяемых ключей устройств, обычно хранимых большинством устройств воспроизведения.

Кроме того, блок 109 управления управляет блоком 104 генерации информации преобразования, обеспечивая генерацию им информации преобразования для каждого из выбранных ключей устройств.

Кроме того, блок 109 управления управляет блоком 103 преобразования таким образом, чтобы обеспечить преобразование им ключа МК носителя соответственно с использованием каждого сегмента информации, генерируемой блоком 104 генерации информации преобразования.

Кроме того, блок 109 управления управляет блоком 105 шифрования ключа носителя таким образом, чтобы обеспечить шифрование им преобразованных ключей МК носителей с использованием каждого из соответствующих выбранных ключей устройств.

Блок 109 управления также управляет блоком 106 шифрования ключа содержания, обеспечивая шифрование им принятого ключа содержания с использованием ключа носителя, и управляет блоком 107 шифрования содержания, обеспечивая шифрование им содержания.

Блок 109 управления имеет соответствующие зашифрованные данные ключа, информацию преобразования и зашифрованное содержание, записанное на DVD 300 посредством блока 110 вывода.

(3) Блок 101 хранения ключей устройств

Блок 101 хранения ключей устройств хранит все ключи устройств, выданные устройствам воспроизведения, принадлежащим системе защиты от копирования. Ключи устройства, сохраненные блоком 101 хранения ключей устройств, генерируются и присваиваются устройствам воспроизведения с использованием способа распределения ключей на основе древовидной структуры, показанной на фиг. 2.

Заметим, что хотя древовидная структура описана в рассматриваемом варианте осуществления как троичное дерево с тремя уровнями, древовидная структура не ограничена троичным деревом, а может иметь и большее количество уровней. Способ распределения на основе древовидной структуры описан детально в документе 2.

Ниже кратко описана древовидная структура.

Древовидная структура состоит из узлов и путей. Каждое «соединение» в дереве называется узлом, и узлы соединяются путми. Каждый уровень, на котором узлы позиционированы в древовидной структуре, называется уровнем. Узел, который находится выше конкретного узла и соединен с этим узлом одним путем, называется родительским узлом, а узлы, которые находятся ниже родительского узла и соединены с родительским узлом путями, называются дочерними узлами.

Кроме того, узел самого высокого уровня называется корнем, а узлы самого нижнего уровня называются листьями. Устройства воспроизведения соотнесены с соответствующими листьями как «один к одному». На фиг. 2 устройства воспроизведения показаны с номерами от 0 до 8, соответственно присвоенными им.

Кроме того, каждому узлу присвоен идентификатор ИД узла. ИД узлов представляют собой конкатенацию номеров путей от корня к конкретному узлу.

Номера 00, 01 и 10 путей присвоены путям в указанном порядке слева направо. Например, ИД узла для листа, к которому отнесено устройство 6 воспроизведения, соответствует «1000».

Ниже кратко описан порядок присвоения ключей устройств в системе защиты от копирования.

<Корень>

Множество ключей устройств присваивается корню. На фиг. 2 эти ключи устройств выражены как идентификационная информация Ка-0000, Ка-0001, Ка-0010, Ка-0011, Ка-0100, Ка-0101 и Ка-0110. В идентификационной информации «Ка» указывает на то, что ключ устройства присвоен корню. Четыре бита после «Ка» обозначают NRP (схему аннулирования узла), и старший бит NRP-данных идентифицирует то, является ли узел родительским узлом по отношению к листу. Старший бит равен «1», когда узел является родительским узлом, и «0» в случае любого другого узла.

Три младших бита в NRP-данных выражают информацию аннулирования. Информация аннулирования указывает для каждого дочернего узла корня, существует ли ключ или ключи устройства, которые должны быть аннулированы, среди ключей устройства, присвоенных дочернему узлу. В данном случае «1» выражает дочерний узел, имеющий ключ или ключи устройства, которые должны быть аннулированы, а «0» указывает, что дочерний узел не имеет ключа или ключей устройства, которые должны быть аннулированы. Информация аннулирования состоит из информации для каждого дочернего узла, конкатенированной в порядке слева направо в древовидной структуре.

Здесь «аннулирование» означает признание недействительным устройства воспроизведения и ключей устройства по причине, состоящей, например, в том, что устройство воспроизведения было подвергнуто анализу и ключи устройства были вскрыты. Узлы, соответствующие ключам устройства, аннулирванным таким образом, аннулируются. Такой узел называется аннулированным узлом.

Ка-0000 представляет собой ключ, хранимый всеми устройствами воспроизведения, принадлежащими древовидной структуре, и это именно тот ключ, который используется в исходном состоянии, когда ни одно из устройств воспроизведения в древовидной структуре не аннулировано.

Другие ключи устройств используются для шифрования ключа носителя, если аннулированный ключ устройства существует в дочерних узлах.

Например, если аннулированное устройство воспроизведения существует ниже самого левого дочернего узла корня и ни одного аннулированного устройства воспроизведения нет ниже других дочерних узлов, то используется ключ устройства с информацией аннулирования «100», идентифицированный посредством Ка-0100. Таким образом, ключ устройства присваивается каждой соответствующей информации аннулирования и согласно позиции аннулированного устройства воспроизведения в древовидной структуре осуществляется выбор ключей устройства, идентифицированных посредством тех сегментов информации аннулирования, которые должны затем использоваться.

Кроме того, не назначаются ключи устройства, имеющие информацию аннулирования «111». Это объясняется тем, что ключи устройства, присвоенные узлам самого нижнего уровня, используются, когда все дочерние узлы имеют аннулированное устройство воспроизведения.

<Узлы>

Шесть ключей устройства Kb-1001, Kb-1010, Kb-1011, Kb-1100, Kb-1101 и Kb-1110

присвоены самому левому узлу на уровне 1. Здесь «Kb» указывает ключ устройства, присвоенный самому левому узлу на уровне 1. Тем же самым путем, что и для ключей устройства, относящихся к корню, каждый ключ устройства идентифицируется информацией аннулирования о дочерних узлах. Кроме того, не назначаются ключи устройства с информацией аннулирования «000». Это объясняется тем, что если не существуют аннулированные устройства воспроизведения для узлов ниже конкретного узла, то используется ключ устройства, присвоенный корню, который является узлом выше конкретного узла. Кроме того, не назначаются ключи устройства с информацией аннулирования «111». Это объясняется тем, что если аннулированы все устройства воспроизведения, соответствующие листьям дерева, которые являются дочерними узлами, то ключи устройства, присвоенные узлу, не используются.

Каждому из других узлов присваиваются шесть ключей устройства, идентифицированных информацией аннулирования, как описано выше.

<Листья>

Каждому листу соответствует устройство воспроизведения, назначенное ему. В данном случае устройства воспроизведения идентифицированы номерами от 0 до 8.

Самому левому листу уровня 2 присвоены ключи устройства Ka-0000, Ka-0001, Ka-0010, Ka-0011, Kb-1001, Kb-1010 и Kb-1011.

Листу назначены все ключи устройства, которые присвоены узлам на путях от корня до листа, исключая ключ устройства, соответствующий схеме аннулирования, для случая, когда устройство 0 воспроизведения отозвано. Иными словами, ключи устройства Ka-0100, Ka-0101, Ka-0110, Ka-0011, Kb-1101, Kb-1101 и Kb-1110 не присвоены устройству 0 воспроизведения, поскольку они являются ключами устройства среди присвоенных корню и самому левому узлу уровня 1, которые используются, когда устройство 0 воспроизведения отозвано.

Другим листьям ключи устройств назначаются аналогичным способом.

(4) Блок 102 выбора ключей устройств

Блок 102 выбора ключей устройств выбирает ключи устройств так, чтобы отозванные устройства воспроизведения были неспособны использовать содержание, и выводит выбранные ключи устройств в блок 105 шифрования ключей носителей.

В исходном состоянии блок 102 выбора ключей устройств выбирает ключ Ka-0000 и выводит этот выбранный ключ устройства на блок 105 шифрования ключей носителей.

Способ выбора ключей устройств, когда существует одно или более отозванных устройств воспроизведения, описан со ссылкой на фиг. 3.

Если устройства 0 и 8 воспроизведения отозваны, то все узлы на путях от корня до каждого их листьев, соответствующие устройствам 0 и 8 воспроизведения, аннулируются. Каждый аннулированный узел указан крестом (x) на фиг. 3. Если одно или более устройств воспроизведения отзывается, то ключ устройства, который использовался ранее, больше не может быть использован. Иными словами, ключ Ka-0000, который использовался в исходном состоянии, не может использоваться.

Затем блок 102 выбора ключей устройств выбирает для каждого аннулированного узла ключ устройства, который соответствует схеме аннулирования узла. В случае корня блок 102 выбора ключей устройств выбирает ключ Ka-0101 устройства, информация аннулирования которого соответствует «101», поскольку левый и правый дочерние узлы аннулированы.

В случае самого левого узла уровня 1, блок 102 выбора ключей устройств выбирает ключ Kb-1100 устройства, информация аннулирования которого соответствует «100»,

поскольку самый левый дочерний узел аннулирован. Средний узел на уровне 1 не имеет аннулированных дочерних узлов, и поэтому используется ключ устройства, присвоенный вышележащему уровню, в этом случае Ka-0101, присвоенный корню. Для самого правого узла уровня 1, блок 102 выбора ключей устройств выбирает ключ Kd-1001 устройства, информация аннулирования которого соответствует «001», поскольку самый правый его дочерний узел аннулирован.

(5) Блок 104 генерации информации преобразования

Блок 104 генерации информации преобразования генерирует информацию преобразования для каждого из ключей устройств, выбранного блоком 102 выбора ключей устройств.

Информация схемы аннулирования узла (NRP) генерируется путем конкатенации соответствующих NRP-данных от корня до узла, которому назначен выбранный ключ устройства.

Как показано на фиг. 3, если устройства 0 и 8 воспроизведения отозваны, то блок 104 генерации информации преобразования генерирует информацию преобразования для ключей Ka-0101, Kb-1100 и Kd-1001, выбранных блоком 102 выбора ключей устройств.

В первую очередь блок 104 генерации информации преобразования генерирует информацию преобразования для ключа Ka-0101 устройства, совместно используемого устройствами воспроизведения с 3 по 5. В данном случае, поскольку только NRP-данные для узлов от корня до узла, которому назначен ключ Ka-0101 устройства, соответствуют «101», блок 104 генерации информации преобразования выдает «101» на блок 103 преобразования в качестве информации преобразования.

Затем блок 104 генерации информации преобразования генерирует информацию преобразования для ключа Kb-1100 устройства, совместно используемого устройствами воспроизведения 1 и 2. Поскольку NRP-данные для узлов от корня до узла, которому назначен ключ Kb-1100 устройства, соответствуют «101» и «100», блок 104 генерации информации преобразования конкатенирует эти NRP-данные для генерации информации преобразования «101100» и выдает генерированную информацию преобразования на блок 103 преобразования.

Затем блок 104 генерации информации преобразования генерирует информацию преобразования для ключа Kd-1001 устройства, совместно используемого устройствами воспроизведения 6 и 7. Поскольку NRP-данные для узлов от корня до узла, которому назначен ключ Kd-1001 устройства, соответствуют «101» и «001», блок 104 генерации информации преобразования конкатенирует эти NRP-данные для генерации информации преобразования «101001» и выдает генерированную информацию преобразования на блок 103 преобразования.

Кроме того, блок 104 генерации информации преобразования имеет NRP-данные, используемые для генерации информации преобразования, записываемой в область 301 записи информации преобразования DVD 300 посредством блока 110 вывода. В данном случае NRP-данные записываются в порядке высоты уровней, которым они присвоены.

Отметим, что если информация заголовка, присоединенная к зашифрованному ключу носителя или зашифрованному ключу содержания, используется в качестве информации преобразования, то нет необходимости записывать информацию преобразования. Кроме того, нет необходимости записывать информацию преобразования, если устройство воспроизведения имеет структуру, позволяющую ему генерировать информацию преобразования.

(6) Блок 103 преобразования

Блок 103 преобразования получает ключ носителя от внешнего источника посредством блока 108 ввода и получает информацию преобразования от блока 104 генерации информации преобразования. Блок 103 преобразования применяет соответствующие операции «исключающее ИЛИ» к ключу носителя с использованием каждого сегмента информации преобразования, тем самым осуществляя преобразование ключа носителя.

Более конкретно, как показано на фиг. 4A, блок 103 преобразования сначала преобразует ключ МК носителя с использованием информации «0101» преобразования, которая соответствует ключу Ka-0101 устройства, тем самым генерируя преобразованный ключ МК' носителя. Затем, как показано на фиг. 4B, блок 103 преобразования преобразует ключ МК носителя с использованием информации «01011100» преобразования, которая соответствует ключу Kb-1100 устройства, тем самым генерируя преобразованный ключ МК" носителя. Кроме того, блок 103 преобразования преобразует ключ МК носителя с использованием информации «01011001» преобразования, которая соответствует ключу Kd-1001 устройства, тем самым генерируя преобразованный ключ МК'" носителя, как показано на фиг. 4C.

Блок 103 преобразования выдает генерированные преобразованные ключи МК', МК" и МК'" носителей на блок 105 шифрования ключей носителей.

(7) Блок 105 шифрования ключей носителей

Блок 105 шифрования ключей носителей получает ключи устройства от блока 102 выбора ключей устройств и получает преобразованные ключи носителей от блока 103 преобразования. Блок 105 шифрования ключей носителей шифрует каждый преобразованный ключ носителя соответствующим принятым ключом устройства.

Более конкретно, как показано на фиг. 4A, блок 105 шифрования ключей носителей сначала применяет алгоритм шифрования E1 к преобразованному ключу МК' носителя с использованием ключа Ka-0101 устройства, тем самым генерируя зашифрованный ключ E(Ka-0101, МК') носителя. В данном случае алгоритм шифрования E1, в качестве примера, соответствует алгоритму AES (усовершенствованный стандарт шифрования). Поскольку алгоритм AES является широко известным, его описание опускается. Заметим, что E(X,Y) обозначает зашифрованный текст, полученный путем шифрования данных Y данными X ключа.

Таким же способом, как показано на фиг. 4B, блок 105 шифрования ключей носителей применяет алгоритм шифрования E1 к преобразованному ключу МК" носителя с использованием ключа Kb-1100 устройства, тем самым генерируя зашифрованный ключ E(Kb-1100, МК") носителя. Затем, как показано на фиг. 4C, блок 105 шифрования ключей носителей шифрует преобразованный ключ МК'" носителя с использованием ключа Kd-1001 устройства, тем самым генерируя зашифрованный ключ E(Kd-1001, МК'") носителя.

Кроме того, блок 105 шифрования ключей носителей записывает генерированные зашифрованные ключи E(Ka-0101, МК'), E(Kb-1100, МК") и E(Kd-1001, МК'") носителей посредством блока 110 вывода в область 302 записи данных ключей носителей DVD 300.

(8) Блок 106 шифрования ключа содержания

Блок 106 шифрования ключа содержания получает ключ СК содержания и ключ МК носителя посредством блока 108 ввода. Блок 106 шифрования ключа содержания применяет алгоритм E1 шифрования к ключу СК содержания с использованием

принятого ключа МК носителя для шифрования ключа СК содержания, генерируя при этом зашифрованный ключ E(МК, СК) содержания. Блок 106 шифрования ключа содержания затем записывает генерированный зашифрованный ключ E(МК, СК) содержания посредством блока 110 вывода в область 303 записи данных ключа содержания.

(9) Блок 107 шифрования содержания

Блок 107 шифрования содержания получает содержание и ключ СК содержания от внешнего источника посредством блока 108 ввода. Блок 107 шифрования содержания применяет алгоритм E1 шифрования к содержанию с использованием принятого ключа СК содержания для шифрования содержания, генерируя при этом зашифрованное содержание E(СК, содержание). Блок 107 шифрования содержания затем записывает полученное зашифрованное содержание E(СК, содержание) посредством блока 110 вывода в область 304 записи содержания DVD 300.

1.2 DVD 300

DVD 300, как показано на фиг. 5, содержит область 301 записи информации преобразования, область 302 записи данных ключей носителя, область 303 записи данных ключа содержания и область 304 записи содержания.

Область 301 записи информации преобразования представляет собой область, в которой записаны NRP-данные, используемые для генерации информации преобразования. NRP-данные записаны в порядке высоты уровней, которым они присвоены.

Область 302 записи данных ключей носителя представляет собой область для записи зашифрованных ключей носителя. Зашифрованные ключи носителя записываются в порядке от зашифрованного ключа носителя, который зашифрован с использованием ключа устройства, присвоенного самому высокому уровню в древовидной структуре.

Область 303 записи данных ключа содержания представляет собой область для записи зашифрованного ключа содержания.

Область 304 записи содержания представляет собой область для записи зашифрованного содержания.

1.3 Устройство 200 воспроизведения

Устройство 200 воспроизведения представляет собой структуру, общую для устройств 200a, 200b воспроизведения и т.д., и соответствует любому из устройств воспроизведения с 0 по 8 в древовидной структуре.

Устройство 200 воспроизведения, как показано на фиг. 6, состоит из блока 201 выбора ключей устройства, блока 202 хранения ключей устройства, блока 203 дешифрования ключа носителя, блока 204 преобразования, блока 205 дешифрования ключа содержания, блока 206 дешифрования содержания, блока 207 привода, блока 208 воспроизведения, блока 209 управления и блока 210 ввода. Монитор 220 и динамик 221 соединены с блоком 208 воспроизведения.

Подобно блоку 100 генерации данных ключей, устройство 200 воспроизведения представляет собой компьютерную систему, состоящую из микропроцессора, ПЗУ, ОЗУ, блока жесткого диска, блока отображения и т.п. Устройство 200 воспроизведения реализует свои функции посредством микропроцессора, работающего в соответствии с компьютерной программой, сохраненной в ОЗУ или на жестком диске.

(1) Блок 207 привода и блок 210 ввода

Блок 210 ввода получает вводимые данные от внешнего источника и выдает

полученную информацию ввода на блок 209 управления.

Блок 207 привода осуществляет считывание с DVD 300 под управлением блока 209 управления.

Сначала, под управлением блока 209 управления, блок 207 привода считывает информацию преобразования из области 301 записи информации преобразования и выводит считанную информацию преобразования на блок 201 выбора ключей устройств.

Затем блок 207 привода считывает зашифрованные ключи носителя из области 302 записи данных ключей носителя и выводит считанные зашифрованные ключи носителя на блок 203 дешифрования ключей носителя.

Затем блок 207 привода считывает зашифрованный ключ E(МК, содержание) содержания из области 303 записи ключей содержания и выводит считанный зашифрованный ключ E(МК, содержание) содержания на блок 205 дешифрования ключей содержания.

Блок 207 привода также считывает зашифрованное содержание E(СК, содержание) из области 304 записи содержания и выводит считанное зашифрованное содержание E(СК, содержание) на блок 206 дешифрования содержания.

(2) Блок 208 вопроизведения

Под управлением блока 209 управления, блок 208 воспроизведения генерирует видеосигнал и аудиосигнал из содержания, полученного от блока 206 дешифрования содержания, и выводит сформированные видеосигнал и аудиосигнал на монитор 220 и динамик 221 соответственно.

(3) Блок 209 управления

При получении информации команды, предписывающей воспроизведение записи содержания на DVD 300, блок 209 управления управляет блоком 207 привода для воспроизведения различных типов информации с DVD 300.

Сначала блок 209 управления управляет блоком 201 выбора ключей устройства для выбора ключа устройства, определения позиции записи зашифрованного ключа носителя и генерации информации преобразования.

Затем блок 209 управления управляет блоком 203 дешифрования ключа носителя для дешифрования зашифрованного ключа носителя, чтобы сформировать преобразованный ключ носителя, и блоком 204 преобразования для обратного преобразования преобразованного ключа носителя, чтобы сформировать ключ носителя.

Кроме того, блок 209 управления управляет блоком 205 дешифрования ключа содержания для дешифрования считанного зашифрованного ключа содержания с использованием ключа носителя, чтобы сформировать ключ содержания. Блок 209 управления также управляет блоком 206 дешифрования для дешифрования считанного зашифрованного содержания с использованием сформированного ключа содержания, чтобы генерировать содержание, и управляет блоком 208 воспроизведения для воспроизведения содержания.

(4) Блок 202 хранения ключей устройств

Блок 202 хранения ключей устройств хранит множество ключей устройства, присвоенных устройству 200 воспроизведения администратором. Присвоенные ключи устройства представлены на фиг. 2 посредством идентификаторов, показанных под каждым из устройств воспроизведения с 0 по 8. Например, устройство воспроизведения 6 имеет ключи устройства, указанные идентификационной информацией Ka-0000, Ka-0010, Ka-0100, Ka-0110, Kd-1001, Kd-1010 и Kd-1011.

Кроме того, блок 202 хранения ключей устройств хранит идентификационную информацию, указывающую позицию в древовидной структуре корня, которому соответствует устройство 200 воспроизведения.

(5) Блок 201 выбора ключей устройств

Блок 201 выбора ключей устройств выбирает ключ устройства и выводит выбранный ключ устройства на блок 203 дешифрования ключа носителя. Примером способа выбора ключей устройства может служить способ, в котором каждому ключу устройства заранее присвоен идентификатор, при этом устройство генерации данных ключей записывает идентификатор ключа устройства, подлежащего выбору, на DVD и устройство воспроизведения выбирает ключ устройства, указанный идентификатором, записанным на DVD. Этот способ выбора ключа устройства широко известен и поэтому детально не описывается.

Блок 201 выбора ключей устройства определяет позицию зашифрованного ключа носителя, который соответствует выбранному ключу устройства, генерирует информацию преобразования и выводит указание записи на блок 203 дешифрования ключа носителя и информацию преобразования на блок 204 преобразования. Обработка для указания позиции записи и генерации информации преобразования описана ниже.

(6) Блок 203 дешифрования ключа носителя

Блок 203 дешифрования ключа носителя получает ключ устройства и позицию записи зашифрованного ключа носителя из блока 201 выбора ключей устройств и считывает зашифрованный ключ носителя, записанный в области, указанной полученной позицией записи, с DVD с помощью блока 207 привода.

Блок 203 дешифрования ключа носителя применяет алгоритм D1 дешифрования к зашифрованному ключу носителя с использованием ключа устройства, чтобы сформировать преобразованный ключ носителя. Алгоритм D1 дешифрования выполняет обработку, обратную той, которую выполнял алгоритм E1 шифрования. Блок 203 дешифрования ключа носителя выводит сформированный преобразованный ключ носителя на блок 204 преобразования.

Для конкретного примера выбранного ключа Ka-1010 устройства, как показано на фиг. 7A, блок 203 дешифрования ключа носителя дешифрует зашифрованный ключ E(Ka-0101, MK') носителя с использованием выбранного ключа Ka-0101 устройства, генерируя при этом преобразованный ключ MK' носителя. В случае выбранного ключа Kb-1100 устройства, как показано на фиг. 7B, блок 203 дешифрования ключа носителя дешифрует зашифрованный ключ E(Kb-1100, MK") носителя, генерируя при этом преобразованный ключ MK" носителя. В случае выбранного ключа Kd-1001 устройства, как показано на фиг. 7C, блок 203 дешифрования ключа носителя дешифрует зашифрованный ключ E(Kd-1001, MK'") носителя, генерируя при этом преобразованный ключ MK'" носителя.

Блок 203 дешифрования ключа носителя выводит сформированные преобразованные ключи MK', MK" или MK'" носителя на блок 204 преобразования.

(7) Блок 204 преобразования

Блок 204 преобразования принимает преобразованный ключ носителя от блока 203 дешифрования ключа носителя и получает информацию преобразования от блока 201 выбора ключей устройств.

Блок 204 преобразования выполняет операцию «исключающее ИЛИ» на принятом преобразованном ключе носителя с использованием информации преобразования, сформированной блоком 201 выбора ключей устройств, чтобы сформировать ключ

носителя.

Для конкретного примера выбранного ключа Ka-1010 устройства, как показано на фиг. 7A, блок 204 преобразования преобразует преобразованный ключ МК' носителя с использованием информации «0101» преобразования, которая соответствует ключу Ka-0101 устройства, генерируя при этом ключ МК носителя. В случае выбранного ключа Kb-1100 устройства, как показано на фиг. 7B, блок 204 преобразования преобразует преобразованный ключ МК" носителя с использованием информации «01011100» преобразования, генерируя при этом ключ МК носителя. В случае выбранного ключа Kd-1001 устройства, как показано на фиг. 7C, блок 204 преобразования преобразует преобразованный ключ МК'" носителя с использованием информации «01011001» преобразования, генерируя при этом ключ МК носителя.

Блок 204 преобразования выводит сформированный ключ МК носителя на блок 205 дешифрования ключа содержания.

(8) Блок 205 дешифрования ключа содержания

Блок 205 дешифрования ключа содержания получает зашифрованный ключ содержания от блока 207 привода и ключ носителя от блока 204 преобразования. Блок 205 дешифрования ключа содержания применяет алгоритм D1 дешифрования к зашифрованному ключу содержания с использованием полученного ключа носителя, чтобы сформировать ключ содержания, и выводит сформированный ключ содержания на блок 206 дешифрования содержания.

(9) Блок 206 дешифрования содержания

Блок 206 дешифрования содержания получает зашифрованное содержание от блока 207 привода и ключ содержания от блока 205 дешифрования ключа содержания. Блок 206 дешифрования содержания применяет алгоритм D1 дешифрования к зашифрованному содержанию с использованием полученного ключа содержания, чтобы сформировать содержание, и выводит сформированное содержание на блок 208 воспроизведения.

2. Функционирование системы защиты от копирования

2.1 Функционирование устройства 100 генерации данных ключей

Ниже описаны операции, осуществляемые устройством 100 генерации данных ключей, со ссылкой на фиг. 8.

Блок 102 выбора ключей устройства выбирает один или более ключей устройства, совместно используемых наибольшим числом устройств воспроизведения, которые не были отозваны (этап 401), и выводит выбранные ключи устройства на блок 105 шифрования ключа носителя и блок 104 генерации информации преобразования.

Затем блок 104 генерации информации преобразования, блок 103 преобразования и блок 105 шифрования ключа носителя повторяют следующую обработку для каждого из выбранных ключей устройства. Отметим, что на фиг. 8 «A» обозначает число выбранных ключей устойства.

Блок 104 генерации информации преобразования генерирует информацию преобразования (этап 403) и выводит информацию преобразования на блок 103 преобразования. Блок 103 преобразования преобразует ключ носителя, полученный посредством блока 108 ввода, генерируя при этом преобразованный ключ носителя (этап 404) и выводит сформированный преобразованный ключ носителя в блок 105 шифрования ключа носителя. Блок 105 шифрования ключа носителя получает выбранный ключ устройства и преобразованный ключ носителя и шифрует преобразованный ключ носителя с использованием полученного ключа устройства, генерируя при этом зашифрованный ключ носителя (этап 405).

После того как обработка на этапах с 403 по 405 выполнена для всех выбранных ключей устройства, генерированная информация преобразования и зашифрованный ключ носителя записываются на DVD 300 с помощью блока 110 вывода (этап 406).

Затем блок 106 шифрования ключа содержания зашифровывает ключ содержания с использованием непреобразованного ключа носителя (ключа носителя до преобразования), генерируя при этом зашифрованный ключ содержания, и записывает генерированный зашифрованный ключ содержания на DVD 300 с помощью блока 110 вывода (этап 407).

Кроме того, блок 107 шифрования содержания зашифровывает содержание с использованием ключа содержания, генерируя при этом зашифрованное содержание, и записывает полученное зашифрованное содержание на DVD 300 с помощью блока 110 вывода (этап 408).

2.2 Функционирование устройства воспроизведения

Ниже, со ссылкой на фиг. 9, описаны операции, осуществляемые устройством 200 воспроизведения для воспроизведения содержимого, записанного на DVD 300.

Блок 201 выбора ключей устройства выбирает ключ устройства на основе информации преобразования, считанной блоком 207 привода, и выполняет определение позиции записи зашифрованного ключа носителя и генерацию информации преобразования (этап 411). Блок 201 выбора ключей устройства выводит выбранный ключ устройства и позицию записи на блок 203 дешифрования ключа носителя и выводит информацию преобразования на блок 204 преобразования.

Блок 203 дешифрования ключа носителя (этап 412) считывает зашифрованный ключ носителя соответственно позиции записи с DVD 300 с помощью блока 207 привода и дешифрует зашифрованный ключ носителя с использованием ключа устройства, полученного от блока 201 выбора ключей устройства (этап 413) и выводит полученный в результате ключ носителя на блок 205 дешифрования ключа содержания.

Блок 205 дешифрования ключа содержания дешифрует зашифрованный ключ содержания, считанный с DVD 300 с помощью блока 207 привода, с использованием ключа носителя, чтобы сформировать ключ содержания (этап 414), и выводит ключ содержания на блок 206 дешифрования содержания.

Блок 206 дешифрования дешифрует зашифрованное содержание, считанное с DVD 300 с помощью блока 207 привода, с использованием ключа содержания, полученного от блока 205 дешифрования ключа содержания, чтобы сформировать содержание (этап 415), и выводит содержание на блок 208 воспроизведения.

Блок 208 воспроизведения воспроизводит принятое содержание и выводит его на монитор 220 и динамик 221 (этап 416).

2.3 Определение зашифрованного ключа носителя и генерация информации преобразования

(1) Ниже, со ссылкой на фиг. 10, описаны определение зашифрованного ключа носителя и генерация информации преобразования на этапе 411.

Блок 201 выбора ключей устройства проверяет по порядку NRP-данные, записанные в области 301 записи информации преобразования. Блок 201 выбора ключей устройства имеет переменную Y, указывающую позицию проверяемых NRP-данных, переменную X, указывающую позицию записи зашифрованного ключа носителя, переменную A, указывающую позицию NRP-данных, относящихся к устройству 200 воспроизведения, переменную W, указывающую число NRP-данных на конкретном уровне, и значение D, указывающее число уровней в древовидной

структуре. NRP-данные, относящиеся к устройству 200 воспроизведения, представляют собой NRP-данные узлов на маршруте от листа, с которым сопоставлено пользовательское устройство, до корня в древовидной структуре.

Блок 201 выбора ключей устройства выполняет анализ согласно следующей процедуре, от уровня i=0 до уровня i=D-1.

Блок 201 выбора ключей устройства устанавливает следующие начальные значения: переменная A=0, переменная W=1, переменная i=0, переменная Y=0 и X=0 (этап 421).

Блок 201 выбора ключей устройства сравнивает переменную i и значение D, и если переменная i больше, чем значение D (этап 422), то завершает обработку, поскольку устройство 200 воспроизведения отозвано.

Если переменная i равна или меньше, чем значение D (этап 422), то блок 201 выбора ключей устройства определяет, равны ли «111» три младшие бита в Y-ых NRP-данных, записанных в области 301 записи информации преобразования (этап 423). Если три младших бита равны «111», то блок 201 выбора ключей устройств вычисляет Y=Y+1 (этап 426) и возвращается к обработке на этапе 423.

Если три младших бита не равны «111», то блок 201 выбора ключей устройств определяет, равно ли значение Y значению A (этап 424). Если эти значения различны, то блок 201 выбора ключей устройства вычисляет X=X+1 (этап 425), вычисляет Y=Y+1 (этап 426) и возвращается к обработке на этапе 423.

Если это значение переменной Y равно значению переменной A, то блок 201 выбора ключей устройства сохраняет значение Y-ых NRP-данных на уровне i (этап 427).

Затем блок 201 выбора ключей устройства проверяет, равно ли из четырех битов, составляющих Y-ые NRP-данные, значение B в битовой позиции, соответствующей значению старшего 2i-го бита и 2i-1-го бита, «0» или «1» (этап 428). Здесь соответствующая битовая позиция является самым левым битом Y-ых NRP-данных в случае, если значение старшего 2i-го бита и 2i-1-го бита равно «00», средним битом Y-ых NRP-данных в случае «01» и правым битом Y-ых NRP-данных в случае «10». Идентификационная информация составляется на основе правила, что, как показано на фиг. 2, в древовидной структуре левым путям присвоено «00», средним путям присвоено «01», и правым путям присвоено «10», и поэтому указывает маршрут от корня до листа, соответствующего устройству воспроизведения.

Если значение B есть «1» (этап 428), то блок 201 выбора ключей устройства отсчитывает число «единиц» в W NRP-данных на уровне i. Однако блок 201 выбора ключей устройств не считает число «единиц» в NRP-данных, у которых старший бит равен «1». Блок 201 выбора ключей устройств присваивает отсчитанное значение переменной W. Переменная W, полученная таким образом, указывает число NRP-данных на следующем уровне i+1 (этап 429).

Затем блок 201 выбора ключей устройства отсчитывает число «единиц» в NRP-данных от первых NRP-данных до NRP-данных в соответствующей битовой позиции. Однако блок 201 выбора ключей устройства не считает число «единиц» в NRP-данных, у которых старший бит равен «1». Блок 201 выбора ключей устройств присваивает отсчитанное значение переменной A. В данном случае блок 201 выбора ключей устройств не отсчитывает значение соответствующей битовой позиции. Переменная A, полученная таким образом, указывает позицию NRP-данных, относящихся к устройству 200 воспроизведения (этап 430).

Затем блок 201 выбора ключей устройства вычисляет X=X+1 (этап 431), Y=0

(этап 432) и i=i+1 (этап 433) и возвращается к обработке на этапе 422.

Если на этапе 428 B=0, то блок 201 выбора ключей устройств выводит значение переменной X в блок 203 дешифрования ключа носителя в качестве позиции записи зашифрованного ключа носителя, выводит генерированную информацию преобразования на блок 204 преобразования (этап 434) и завершает обработку.

(2)Ниже описана обработка для выбора зашифрованного ключа носителя и генерации информации преобразования с использованием устройства 6 воспроизведения, показанного на фиг. 2, в качестве примера.

Устройство воспроизведения 6 заанее сохраняет ключи Ka-0000, Ka-0010, Ka-0100, Ka-0110, Kd-1001, Kd-1010 и Kd-1011 в качестве ключей устройства и «1000» в качестве идентификационной информации.

a) Блок 201 выбора ключей устройств определяет, равны ли «111» три младшие бита в 0-ых NRP-данных «0101», записанных в области 301 записи информации преобразования (этап 423).

b) Поскольку три младшие бита не равны «111», то блок 201 выбора ключей устройств сравнивает значения переменной Y и переменной A (этап 424), и поскольку эти значения равны, то сохраняет значение «0101» 0-ых NRP-данных на уровне 0 (этап 427).

c) Поскольку значение верхних двух битов идентификационной информации есть «10», то блок 201 выбора ключей устройства проверяет самый правый из младших трех битов 0-ых NRP-данных (этап 428). Поскольку самый правый бит равен «1», то блок 201 выбора ключей устройств продолжает обработку, начиная с этапа 429 и далее.

d) Блок 201 выбора ключей устройств отсчитывает число «единиц» в младших трех битах NRP-данных «0101» на уровне 0 (этап 429). Поскольку отсчитанное значение равно «2», то известно, что два NRP существуют на следующем уровне 1.

e) Затем блок 201 выбора ключей устройства отсчитывает число «единиц» в трех младших битах из «0101» для NRP-данных вплоть до соответствующей битовой позиции. Блок 201 выбора ключей устройств не отсчитывает значение в соответствующей битовой позиции. Поскольку отсчитанное значение есть «1», то известно, что позиция A соответствующих NRP-данных на следующем уровне 1 есть позиция 1.

f) Блок 201 выбора ключей устройств вычисляет X=X+1, Y=0 и i=i+1 (этапы 431 - 433). В результате значение переменной X становится «1».

g) Блок 201 выбора ключей устройств определяет, равны ли «111» три младшие бита в 0-ых NRP-данных «1100» на уровне 1, записанных в области 301 записи информации преобразования (этап 423), и поскольку три младшие бита не равны «111», то сравнивает значения переменной Y и переменной A (этап 424).

h) Поскольку значения переменной Y и переменной A различаются, то блок 201 выбора ключей устройств вычисляет X=X+1 (этап 425). В результате значение X становится равным «2». Блок 201 выбора ключей устройств также вычисляет Y=Y+1 (этап 426). В результате значение Y становится равным «1».

i) Блок 201 выбора ключей устройств определяет, равны ли «111» три младшие бита первых NRP-данных «1001» на уровне 1, и поскольку три младшие бита не равны «111», то сравнивает значения переменной Y и переменной A (этап 424).

j) Поскольку значения переменной Y и переменной A равны, то блок 201 выбора ключей устройств конкатенирует NRP-данные «1001» в позиции 1 на уровне 1 с NRP-данными «0101», сохраненными в предыдущий момент времени, и сохраняет

полученное в результате конкатенированное значение (этап 427).

k) Поскольку значение третьего и четвертого верхних битов идентификационной информации равно «00», то блок 201 выбора ключей устройств проверяет самый левый бит из младших трех битов NRP-данных в позиции 1 (этап 428). Самый левый бит равен «0», поэтому анализ завершается.

l) Блок 201 выбора ключей устройств выводит значение «2» переменной X в блок 203 дешифрования ключа носителя в качестве позиции записи и выводит «01011001» на блок 204 преобразования в качестве информации преобразования (этап 434).

Результатом описанной обработки является определение зашифрованного ключа E(Kd-1001, MK) носителя из позиции 2 записи устройства 6 воспроизведения, и генерируется информация «01011001» преобразования.

3. Модификации

Хотя настоящее изобретение описано на основе предпочтительного варианта осуществления, оно не ограничено описанным вариантом. Описанные ниже модификации также включены в объем изобретения.

(1) Способ шифрования не ограничен алгоритмом AES, а также может использоваться другой способ шифрования.

(2) Хотя в предпочтительном варианте осуществления ключ носителя и ключ содержания вводятся из внешнего источника, они вместо этого могут храниться в устройстве генерации данных ключей. Альтернативно ключ носителя и ключ содержания могут генерироваться каждый раз при использовании устройства генерации данных ключей.

(3) В предпочтительном варианте осуществления использованы два уровня шифрования. Иными словами, содержание шифруется с использованием ключа содержания, и ключ содержания шифруется с использованием ключа носителя. Однако вместо этого можно использовать один уровень шифрования, при котором содержание зашифровывается с помощью ключа носителя, или обеспечить дополнительный ключ или ключи и увеличить число уровней шифрования. Если число уровней шифрования увеличивается, то достаточно для одного из ключей, который зашифрован, чтобы он был преобразован.

(4) Информация преобразования не ограничивается NRP-данными, как описано в предпочтительном варианте осуществления. Информация преобразования может представлять собой любую информацию, генерируемую для указания соотношения в древовидной структуре между позицией узла, которому присвоен ключ устройства, и другими узлами и для следования заданным правилам относительно числа путей, информации позиции узлов, NRP-данных и т.д. Примеры информации преобразования описаны ниже в пунктах (a) - (f).

(a) Блок 104 генерации информации преобразования находит идентификатор узла, которому присвоен выбранный ключ стройства, а также находит NRP-данные. Они конкатенируются для генерации информации преобразования. Ниже приведен конкретный пример.

Если отозваны устройства воспроизведения 0, 1 и 8, как показано на фиг. 3, то блок 102 выбора ключей устройств выбирает следующие ключи устройств: Ka-0101, Kb-1100 и Kd-1001.

Блок 104 генерации информации преобразования сначала генерирует информацию преобразования для ключа Ka-0101 устройства. Здесь узел, которому присвоен ключ Ka-0101 устройства, является корнем, и поскольку для него не существует

идентификатор узла, то информацией преобразования будет «0101», что представляет собой NRP-данные.

Затем блок 104 генерации информации преобразования генерирует информацию преобразования для ключа Kb-0101 устройства. Здесь идентификатором узла, которому присвоен ключ Kb-0101 устройства, является «00», и NRP-данными является «1100». Эти данные конкатенируются для генерации информации преобразования «001100».

Затем блок 104 генерации информации преобразования генерирует информацию преобразования для ключа Kd-0101 устройства. Здесь идентификатором узла, которому присвоен ключ Kd-0101 устройства, является «10», и NRP-данными является «1001». Эти данные конкатенируются для генерации информации преобразования «101001».

Кроме того, вместо конкатенации идентификатора узла с NRP-данными в качестве информации преобразования может использоваться только идентификатор узла. В таком случае, поскольку для ключа Ka-0101 устройства не существует информация преобразования, ключ Ka-0101 устройства может зашифровываться без преобразования или зашифровываться с использованием информации преобразования, заранее установленной для корня. В этом случае значение, используемое для такой информации преобразования, отличается от другой информации преобразования.

(b) Каждому узлу в древовидной структуре присвоен идентификационный номер в порядке сверху вниз и слева направо, начиная от корня, как показано на фиг. 2, и идентификационные номера используются как информация преобразования.

Иными словами, если отозваны устройства воспроизведения 0, 1 и 8, как показано на фиг. 3, то информацией преобразования ключа Ka-0101 будет «0», информацией преобразования ключа Kb-1100 будет «01», и информацией преобразования ключа Kd-1001 будет «11».

(c) Каждому уровню в древовидной структуре присвоен номер уровня, как показано на фиг. 2, и узлам на одном и том же уровне присвоены относительные номера уровня в порядке слева направо. Информация позиции узла генерируется на основе номера уровня и относительного номера уровня, начная от корня, и эта генерированная информация позиции используется как информация преобразования.

(d) NRP-данные всех узлов от корня до узла, которому присвоен выбранный ключ устройства, извлекаются в порядке от наивысшего уровня до самого нижнего уровня и слева направо на каждом уровне и конкатенируются для генерации информации преобразования. Если необходимо, эта информация преобразования может быть сжата и преобразована в последовательности произвольной длины, и эти последовательности используются в качестве информации преобразования.

(e) Считывание узлов осуществляется в порядке с самого верхнего уровня до самого нижнего уровня, начиная от корня, и количество «единиц» (или «нулей») подсчитывается вплоть до узла, которому соответствует ключ устройства. Подсчитанное значение используется в качестве информации преобразования.

В данном случае подсчитанное значение может быть преобразовано в двоичное число, и двоичные данные конкатенируются с NRP-данными для генерации информации преобразования. NRP-данные, используемые при этом, могут соответствовать таким данным от корня до узла, которому присвоен ключ устройства, или могут соответствовать всем NRP-данными, считанным на основе приведенных выше правил. Альтернативно двоичные данные могут

конкатенироваться только с одними NRP-данными, которые были считаны последними. Еще одной альтернативой является конкатенирование двоичных данных с идентификатором использованного ключа устройства.

(f) Все NRP-данные от корня до узла, которому присвоен ключ устройства, извлекаются и преобразуются в десятичные числа, и их сумма используется в качестве информации преобразования. Альтернативно NRP-данные в двоичной форме могут подвергаться операции «исключающее ИЛИ», и результат этой операции может использоваться в качестве информации преобразования.

(5) В предпочтительном варианте осуществления старший бит NRP-данных указывает, находится ли узел на уровне на один выше листа, однако этот бит может использоваться для передачи другой информации. Например, старший бит может использоваться для указания того, существуют ли какие-либо действительные устройства в узлах-потомках данного узла. Альтернативно, можно использовать только два или три из младших из четырех битов NRP-данных. Аналогичным образом не обязательно, чтобы номер пути состоял из двух битов. Как и в случае NRP-данных, номер пути может иметь другую информацию, связанную с ним. Кроме того, можно использовать все или некоторые из битов из номеров пути.

(6) В настоящем изобретении описанное извлечение не ограничено выполнением в порядке от самого верхнего уровня до самого низкого уровня и слева направо. Может быть использован любой способ, основанный на предварительно заданном правиле. Например, извлечение может выполняться в направлении налево в древовидной структуре или с предшествованием в глубину.

(7) В настоящем изобретении операция, которой подвергается информация преобразования и ключ носителя, не ограничивается операцией «исключающее ИЛИ», описанной в предпочтительном варианте осуществления изобретения. Например, может использоваться любая из четырех основных арифметических операций.

(8) В случае формата, который включает в себя биты четности в данных ключа носителя, информация преобразования может быть встроена в биты четности ключа носителя вместо применения к ключу носителя и информации преобразования некоторой операции.

Например, если используется алгоритм DES, то восемь битов из 64-битового ключа носителя представляют собой биты четности, и устройство 100 генерации данных ключей преобразует ключ носителя так, чтобы он содержал информацию преобразования, встроенную в эти восемь битов.

Не является обязательным, чтобы устройство 200 воспроизведения генерировало информацию преобразования. Вместо этого устройство 200 воспроизведения может считывать зашифрованный ключ носителя с DVD 300, удалять восемь битов четности из данных ключа носителя и использовать 56 битов действительных данных ключа в качестве ключа носителя.

Кроме того, ключ носителя может быть преобразован путем встраивания отличающегося случайного числа в качестве битов четности каждый раз, когда ключ носителя зашифровывается ключом устройства. В этом случае устройство 200 воспроизведения удаляет биты четности без проверки и использует 56 битов действительных данных ключа в качестве ключа носителя.

(9) Если биты четности включены, как описано выше в пункте (5), то информация преобразования или случайное число могут встраиваться в некоторые из битов четности, а остальная часть битов четности может использоваться для информации преобразования.

Например, если имеется восемь битов четности, случайное число может встраиваться в семь из этих битов, а оставшийся один бит может использоваться для информации преобразования. Примером того, каким образом бит может использоваться для информации преобразования, является использование этого бита в качестве флага, указывающего, например, существует или нет список идентификаторов ключей, которые должны быть аннулированы, на носителе записи, на котором записаны данные ключей. В этом случае бит, используемый для передачи этой информации, является фиксированным значением для конкретного носителя записи, но поскольку некоторое случайное число встроено в качестве остальных семи битов четности, то преобразованный ключ носителя является отличающимся для каждого ключа устройства.

(10) В предпочтительном варианте осуществления устройство 100 генерации данных ключей генерирует данные ключей, зашифровывает содержание и записывает данные ключей и зашифрованное содержание на носитель записи. Однако не является обязательным, чтобы все эти операции выполнялись для устройства 100 генерации данных ключей. Иными словами, возможно использование отдельных устройств, которые соответственно будут генерировать данные ключей, записывать данные ключей и записывать содержание.

Кроме того, устройство 100 генерации данных ключей может распределять ключи устройств для устройства записи в дополнение к ключам устройств для устройств воспроизведения.

В этом случае устройство записи хранит ключи устройств, присвоенные листьям древовидной структуры. Устройство 100 генерации данных ключей выполняет обработку, описанную в приведенном варианте осуществления, генерирует информацию преобразования и данные ключей носителя и записывает эти данные на DVD.

При шифровании ключа содержания для зашифровывания содержания устройство записи выполняет ту же обработку, что и устройство 200 воспроизведения, и выбирает и получает соответствующий ключ устройства из сохраненных ключей устройств. Устройство записи зашифровывает ключ содержания с использованием полученного ключа носителя и записывает зашифрованный ключ содержания и зашифрованное содержание на DVD.

Кроме того, устройство записи может использовать в качестве ключа содержания данные ключа, записанные устройством 100 генерации данных ключей.

(11) Данные ключей не ограничены записью на DVD. Может использоваться любой носитель записи, который является портативным и встраиваемым как в устройство 100 генерации данных ключей, так и в устройство 200 воспроизведения, например CD, MD (магнитный диск), MO (магнито-оптический диск), BD и т.д.

(12) Настоящее изобретение может представлять собой способы, описанные выше. Кроме того, способы могут быть реализованы компьютерной программой, исполняемой компьютером, и цифровым сигналом компьютерной программы.

Кроме того, настоящее изобретение может представлять собой машиночитаемый носитель, такой как гибкий диск, жесткий диск, CD-ROM (ПЗУ на компакт-диске), MO, DVD-ROM (ПЗУ на цифровом многоцелевом диске), DVD-RAM (ОЗУ на цифровом многоцелевом диске), BD или полупроводниковая память, которая сохраняет компьютерную программу или цифровой сигнал. Кроме того, настоящее изобретение может представлять собой компьютерную программу или цифровой сигнал, записанный на любом из вышеупомянутых устройств носителей записи.

Кроме того, настоящее изобретение может представлять собой компьютерную программу или цифровой сигнал, передаваемый по коммуникационному каналу, беспроводному или проводному коммуникационному каналу или по сети, например Интернет.

Кроме того, настоящее изобретение может представлять собой компьютерную систему, которая включает в себя микропроцессор и память, причем память хранит компьютерную программу, а микропроцессор функционирует в соответствии с этой компьютерной программой.

Кроме того, путем переноса программы или цифрового сигнала на устройство носителя записи, или путем переноса программы или цифрового сигнала через сеть или т.п. программа или цифровой сигнал могут исполняться другой независимой компьютерной системой.

(13) Настоящее изобретение может представлять собой любую комбинацию вышеописанного варианта осуществления и указанных модификаций.

4. Заключение

Как описано выше, настоящее изобретение представляет собой систему защиты содержания, которая может использоваться только действительным оконечным устройством, содержащую устройство генерации данных ключей, которое содержит блок преобразования, предназначенный для преобразования на основе предварительно заданного правила преобразования первых данных ключа для использования при использовании содержания, при этом генерируя вторые данные ключа, блок шифрования, предназначенный для шифрования вторых данных ключа с использованием ключа устройства, хранимого действительным оконечным устройством, при этом генерируя зашифрованные данные ключа, блок вывода, предназначенный для вывода зашифрованных данных ключа, и оконечное устройство, которое содержит блок получения, предназначенный для получения зашифрованных данных ключа, блок дешифрования, предназначенный для дешифрования зашифрованных данных ключа с использованием ключа устройства, хранимого в оконечном устройстве, при этом генерируя вторые данные ключа, блок преобразования, предназначенный для преобразования на основе предварительно определенного правила преобразования вторых данных ключа, при этом получая первые данные ключа, и блок использования содержания, предназначеный для использования содержания на основе первых данных ключа.

Кроме того, настоящее изобретение представляет собой устройство генерации данных ключей, которое генерирует данные ключей, чтобы содержание могло использоваться только действительным оконечным устройством, и которое содержит блок преобразования, предназначенный для преобразования на основе предварительно определенного правила преобразования первых данных ключа для использования при использовании содержания, при этом генерируя вторые данные ключа; блок шифрования, предназначенный для шифрования вторых данных ключа с использованием ключа устройства, хранимого действительным оконечным устройством, при этом генерируя зашифрованные данные ключа; и блок вывода, предназначенный для вывода зашифрованных данных ключа.

Кроме того, настоящее изобретение представляет собой оконечное устройство, которое использует содержание, которое содержит блок получения, предназначенный для получения зашифрованных данных ключа, которые были генерированы устройством генерации данных ключей, преобразующим первые данные ключа на основе предварительно заданного правила преобразования для генерации данных

ключа и шифрования вторых данных ключа с использованием ключа устройства, причем первые данные ключа предназначены для использования при использовании содержания; блок дешифрования, предназначенный для дешифрования зашифрованных данных ключа с использованием ключа устройства, хранимого в оконечном устройстве, при этом получая вторые данные ключа; блок преобразования, предназначенный для преобразования на основе предварительно заданного правила преобразования вторых данных ключа, при этом получая первые данные ключа; и блок использования содержания предназначенный для использования содержания на основе первых данных ключа.

В соответствии с описанной структурой, даже если ключи устройств имеют идентичные значения, зашифрованные данные ключа не обязательно будут иметь идентичные значения. Кроме того, невозможно определить, имеют или нет ключи устройств идентичные значения, с использованием зашифрованных данных ключа. Поэтому незаконное обнаружение первых данных ключа может быть предотвращено. Соответственно, предотвращается отзыв устройств воспроизведения, которые не должны отзываться.

При этом в устройстве генерации данных ключей блок преобразования может генерировать вторые данные ключа путем генерации информации преобразования для ключа устройства и выполнения обратимой операции над генерируемой информацией преобразования и првыми данными ключа, причем блок вывода может дополнительно выводить информацию преобразования.

Кроме того, оконечное устройство может дополнительно включать в себя блок хранения для хранения множества ключей устройств; и блок выбора, предназначенный для выбора одного из ключей устройств, причем блок получения получает зашифрованные данные, которые были генерированы устройством генерации данных ключей, получая вторые данные ключа путем выполнения обратимой операции над первыми данными ключа и информацией преобразования, генерированной для ключа устройства, и шифрования вторых данных ключа, причем блок дешифрования осуществляет дешифрование с использованием выбранного ключа устройства, и блок преобразования генерирует информацию первого ключа путем генерации информации преобразования для выбранного ключа устройства и применения предварительно заданной операции к выбранному ключу устройства с использованием информации преобразования.

В соответствии с описанной структурой устройство генерации данных ключей применяет обратимую операцию к первым данным ключа, используя информацию преобразования, генерированную для выбранного ключа устройства, при этом генерируя вторые данные ключа. Только оконечное устройство, которое хранит ключ устройства, имеет возможность обратного преобразования вторых данных ключа для генерации первых данных ключа.

При этом устройство генерации данных ключей может дополнительно содержать блок распределения ключей, предназначенный для соотнесения ключей устройств, которые хранятся в оконечных устройствах, с узлами древовидной структуры, которая определяет соотношения между ключами устройств, совместно используемыми оконечными устройствами; и блок выбора, предназначенный для выбора из ключей устройств, хранимых действительными оконечными устройствами, одного или более ключей устройств, которые соответствуют узлу в самой верхней позиции в древовидной структуре, причем блок преобразования генерирует информацию преобразования на основе информации о позиции каждого из одного или

более выбранных ключей устройств в древовидной структуре, и блок шифрования шифрует вторые данные ключа в соответствии с использованием каждого из одного или более выбранных ключей устройства.

Кроме того, в оконечном устройстве блок преобразования может генерировать информацию преобразования из информации заголовка, связанной с зашифрованными данными ключа.

Кроме того, в оконечном устройстве информация заголовка может использоваться для генерации информации преобрзования и может генерироваться устройством генерации данных ключей, которое распределяет ключи устройств с использованием древовидной структуры, выбирая из ключей устройств, хранимых действительными оконечными устройствами, одного или более ключей устройств, которые соответствуют узлу в самой верхней позиции в древовидной структуре, и генерируя информацию заголовка на основе информации о позиции каждого из одного или более выбранных ключей устройства в древовидной структуре, причем блок хранения может хранить информацию о позиции оконечного устройства, и блок преобразования может генерировать информацию преобразования с использованием информации заголовка и хранимой информации о позиции.

В соответствии с описываемой структурой, устройство генерации данных ключей преобразует первые данные ключа с использованием информации преобразования, генерированной на основе позиции выбранного ключа устройства в древовидной структуре. Поэтому даже если ключи устройства совместно используют одинаковые значения, ключ устройства в отличающемся положении в древовидной структуре не сможет использоваться для обратного преобразования вторых данных ключа корректным образом. Соответственно, может быть предотвращено незаконное получение первого ключа.

При этом устройство генерации данных ключей может дополнительно содержать блок распределения ключей, предназначенный для соотнесения ключей устройств, которые хранятся в оконечных устройствах, с узлами древовидной структуры, которая определяет соотношения между ключами устройств, совместно используемыми оконечными устройствами, и определяет, не был ли каждый из ключей устройств аннулирован; и блок выбора, предназначенный для выбора, из ключей устройств, хранимых действительными оконечными устройствами, одного или более ключей устройств, которые соответствуют узлу в самой верхней позиции в древовидной структуре, причем блок преобразования генерирует информацию преобразования для каждого из одного или более выбранных ключей устройств на основе информации об аннулировании, на основе узла, с которым соотнесен выбранный ключ устройства, и состояния аннулирования для других узлов.

Кроме того, в оконечном устройстве, информация заголовка может предназначаться для генерации информации преобразования и может генерироваться путем соотнесения ключей устройств, которые хранятся в оконечных устройствах, с узлами в древовидной структуре, которая определяет соотношения между ключами устройств, совместно используемыми оконечным устройствами, определения, аннулирован или нет каждый из ключей устройств, выбора из ключей устройств, хранимых действительными оконечными устройствами, по меньшей мере, одного ключа устройства, который соответствует узлу в самой верхней позиции в древовидной структуре, основывая информацию заголовка на информации аннулирования, определенной на основе узла, которому соответствует выбранный ключ устройства, и состоянии аннулирования других узлов, сохраняющий блок может

сохранять информацию о позиции оконечного устройства в древовидной структуре для распределения ключей устройств для оконечных устройств в устройстве генерации данных ключей, и блок преобразования может генерировать информацию преобразования с использованием информации заголовка и сохраненной информации о позиции.

В соответствии с описанной структурой, информация о преобразовании генерируется в соответствии с соотношением позиций в древовидной структуре для аннулированного ключа устройства, и поэтому ключ устройства, имеющий другую позицию в древовидной структуре, не может использоваться для обратного преобразования вторых данных ключа корректным образом. Соответственно, незаконное получение первых данных ключа может быть предотвращено.

В данном случае в устройстве генерации данных ключей блок преобразования может генерировать информацию преобразования для каждого из одного или более выбранных ключей устройства путем конкатенации сегментов идентификационной информации, каждый из которых идентифицирует путь на маршруте от корня до узла, которому соответствует выбранный ключ устройства в древовидной структуре.

Кроме того, в устройстве генерации данных ключей блок преобразования может генерировать в качестве информации преобразования для каждого из одного или более выбранных ключей устройств данные, которые отражают позицию узла, соответствующего выбранному ключу устройства, причем позиция выражается в терминах соотношения позиций между уровнями в древовидной структуре и между узлами на одном уровне.

Кроме того, блок преобразования может генерировать информацию преобразования путем конкатенации сегментов информации аннулирования, каждый из которых относится к узлу, размещенному на маршруте от корня до узла, которому соответствует выбранный ключ устройства.

Кроме того, в устройстве генерации данных ключей блок преобразования может генерировать информацию преобразования путем конкатенации из информации аннулирования, соответствующей узлам, упорядоченным в предварительно заданном порядке, от ервого сегмента информации аннулирования до сегмента информации аннулирования узла, который соответствует выбранному ключу устройства.

В соответствии с представленной структурой, поскольку существует множество комбинаций, соответствующих позиции ключа устройства в древовидной структуре, оконечное устройство, которое не имеет информации о позиции действительного ключа устройства в древовидной структуре, не способно генерировать информацию преобразования, и поэтому не способно обнаружить первые ключевые данные.

В данном случае в устройстве генерации данных ключей блок преобразования может генерировать вторые данные ключа путем генерации информации преобразования для ключа устройства и помещать информацию преобразования, по меньшей мере, в часть избыточной части первых данных ключа.

Кроме того, в устройстве генерации данных ключей блок преобразования генерирует вторые данные ключа путем генерации случайного числа для ключа устройства и встраивания генерированного случайного числа в, по меньшей мере, часть избыточной части первых данных ключа.

Кроме того, в оконечном устройстве, вторые данные ключа могут генерироваться устройством генерации данных ключа путем встраивания информации преобразования, генерированной для ключа устройства, по меньшей мере, в часть избыточной части первых данных ключа, и блок преобразования может генерировать

первые данные ключа путем удаления избыточной части вторых данных ключа.

В соответствии с представленной структурой, если избыточный бит включен в первые данные ключа, избыточный бит встраивается с информацией преобразования или со значением, отличающимся для каждого преобразования, тем самым затрудняя нахождение данных ключа, зашифрованных ключом устройства с идентичным значением. Поэтому только оконечное устройство, которое имеет возможность определить корректную позицию данных ключа, может получить первые данные ключа.

В данном случае в устройстве генерации данных ключей блок преобразования может использовать оставшуюся часть избыточной части, в которую не встроено случайное число, для передачи другой информации.

В соответствии с представленной структурой случайное число встраивается в некоторые из избыточных битов и оставшиеся избыточные биты используются для переноса информации. Поэтому другая информация может переноситься, в то время как незаконное получение первых данных ключа может быть предотвращено.

Промышленная применимость

Настоящее изобретение может использоваться в способе распределения ключей, который использует древовидную структуру и особенно пригоден для предотвращения незаконного получения данных ключей.

Формула изобретения

1. Система защиты содержания, в которой содержание может использоваться только действительным устройством воспроизведения, содержащая

устройство генерации данных ключей, которое содержит:

блок преобразования, предназначенный для преобразования, на основе предварительно заданного правила преобразования, ключа носителя с использованием информации преобразования от блока генерации информации преобразования, для формирования преобразованного ключа носителя;

блок шифрования ключа носителя, предназначенный для шифрования преобразованного ключа носителя от блока преобразования с использованием ключа устройства, хранимого действительным устройством воспроизведения, для формирования зашифрованных данных ключа носителя;

блок шифрования ключа содержания, предназначенный для шифрования ключа содержания с использованием ключа носителя для формирования зашифрованного ключа содержания;

блок шифрования содержания, предназначенный для шифрования содержания с использованием ключа содержания для формирования зашифрованного содержания; и

блок вывода, предназначенный для вывода информации преобразования с блока генерации информации преобразования,

зашифрованных данных ключа носителя с блока шифрования ключа носителя, зашифрованного ключа содержания с блока шифрования ключа содержания и зашифрованного содержания с

блока шифрования содержания под управлением блока управления, устройство воспроизведения, которое содержит:

блок получения, предназначенный для получения информации преобразования, зашифрованных данных ключа носителя, зашифрованного ключа содержания и зашифрованного содержания;

блок дешифрования зашифрованных данных ключа носителя, предназначенный

для дешифрования зашифрованных данных ключа носителя с использованием ключа устройства, хранимого в устройстве воспроизведения, для получения дешифрованных данных ключа носителя;

блок преобразования, предназначенный для преобразования, на основе предварительно заданного правила преобразования, дешифрованных данных ключа носителя, для получения ключа носителя;

блок дешифрования ключа содержания, предназначенный для дешифрования зашифрованного ключа содержания с использованием полученного ключа носителя для получения ключа содержания;

блок дешифрования содержания, предназначенный для дешифрования зашифрованного содержания с использованием ключа содержания для формирования содержания;

блок использования содержания, предназначенный для использования сформированного содержания.

2. Система защиты содержания по п.1, в которой устройство генерации данных ключей дополнительно содержит:

блок распределения ключей, предназначенный для определения ключей устройств, хранимых в устройствах воспроизведения, путем соотнесения ключей устройств с узлами в древовидной структуре; и

блок выбора, предназначенный для выбора, по меньшей мере, одного из определенных ключей устройств;

при этом блок преобразования преобразует ключ носителя, с использованием информации преобразования, которая является информацией, определенной в соответствии с позицией узла, которому выбранный ключ устройства соответствует в древовидной структуре, при этом формируя преобразованный ключ носителя; и

блок шифрования шифрует преобразованный ключ носителя с использованием выбранного ключа устройства для формирования зашифрованных данных ключа носителя.

3. Устройство генерации данных ключей, которое генерирует данные ключей таким образом, чтобы использовать содержание только действительным устройством воспроизведения, содержащее:

блок преобразования, предназначенный для преобразования, на основе предварительно заданного правила преобразования, ключа носителя с использованием информации преобразования от блока генерации информации преобразования, для формирования преобразованного ключа носителя;

блок шифрования ключа носителя, предназначенный для шифрования преобразованного ключа носителя от блока преобразования с использованием ключа устройства, хранимого действительным устройством воспроизведения, для формирования зашифрованных данных ключа носителя; и

блок вывода, предназначенный для вывода информации преобразования с блока генерации информации преобразования и зашифрованных данных ключа носителя с блока шифрования ключа носителя под управлением блока управления.

4. Устройство генерации данных ключей по п.3, дополнительно содержащее:

блок распределения ключей, предназначенный для определения ключей устройств, хранимых в устройствах воспроизведения, путем соотнесения ключей устройств с узлами в древовидной структуре; и

блок выбора, предназначенный для выбора, по меньшей мере, одного из определенных ключей устройств;

при этом блок преобразования преобразует ключ носителя, с использованием информации преобразования, которая является информацией, определенной в соответствии с позицией узла, которому выбранный ключ устройства соответствует в древовидной структуре, при этом формируя преобразованный ключ носителя; и

блок шифрования шифрует преобразованный ключ носителя с использованием выбранного ключа устройства, при этом формируя зашифрованные данные ключа носителя.

5. Устройство генерации данных ключей по п.4, в котором

блок преобразования формирует преобразованный ключ носителя путем генерации информации преобразования для ключа устройства и выполнения обратимой операции над сгенерированной информацией преобразования и ключом носителя, и

блок вывода дополнительно записывает информацию преобразования.

6. Устройство генерации данных ключей по п.3, в котором блок выбора выбирает из ключей устройств, хранимых действительными устройствами воспроизведения, один или более ключей устройств, которые соответствуют узлу в самой верхней позиции в древовидной структуре.

7. Устройство генерации данных ключей по п.6, в котором блок преобразования генерирует информацию преобразования для каждого из одного или более выбранных ключей устройства путем конкатенации сегментов идентификационной информации, каждый из которых идентифицирует путь на маршруте от корня до узла, которому соответствует выбранный ключ устройства в древовидной структуре.

8. Устройство генерации данных ключей по п.4, в котором блок преобразования генерирует, в качестве информации преобразования для каждого из одного или более выбранных ключей устройств, данные, которые отражают позицию узла, соответствующего выбранному ключу устройства, причем позиция выражается через соотношение позиций между уровнями в древовидной структуре и между узлами на одном уровне.

9. Устройство генерации данных ключей по п.4, в котором блок преобразования генерирует информацию преобразования путем конкатенации сегментов информации аннулирования, каждый из которых относится к узлу, позиционированному на маршруте от корня до узла, которому соответствует выбранный ключ устройства.

10. Устройство генерации данных ключей по п.4, в котором блок вывода записывает зашифрованные данные ключа на переносной носитель записи.

11. Устройство генерации данных ключей по п.4, в котором блок вывода выводит зашифрованные данные ключа с использованием среды передачи данных.

12. Устройство генерации данных ключей по п.4, в котором блок преобразования преобразует ключ носителя на основе правила преобразования, определенного во взаимосвязи с ключами устройств, хранимых действительными устройствами воспроизведения.

13. Устройство генерации данных ключей по п.3, дополнительно содержащее:

блок распределения ключей, предназначенный для определения ключей устройств, хранимых в устройствах воспроизведения, путем соотнесения ключей устройств с узлами древовидной структуры, и для определения, не был ли аннулирован каждый з ключей устройств; и

блок выбора, предназначенный для выбора, из ключей устройств, хранимых в действительных устройствах воспроизведения, одного или более ключей устройств, которые соответствуют узлу в самой верхней позиции в древовидной структуре;

причем блок преобразования генерирует информацию преобразования для каждого

из одного или более выбранных ключей устройств на основе информации об аннулировании, определенной на основе узла, с которым соотнесен выбранный ключ устройства, и состояния аннулирования для других узлов.

14. Устройство генерации данных ключей по п.13, в котором блок преобразования генерирует информацию преобразования путем конкатенации, из информации аннулирования, соответствующей узлам, упорядоченным в предварительно заданном порядке, от первого сегмента информации аннулирования до сегмента информации аннулирования узла, который соответствует выбранному ключу устройства.

15. Устройство генерации данных ключей по п.3, в котором блок преобразования формирует преобразованный ключ носителя путем генерации информации преобразования для ключа устройства, и помещает информацию преобразования, по меньшей мере, в часть избыточной части ключа носителя.

16. Устройство генерации данных ключей по п.15, в котором блок преобразования формирует преобразованный ключ носителя путем генерации случайного числа для ключа устройства и помещения генерированного случайного числа, по меньшей мере, в часть избыточной части ключа носителя.

17. Устройство генерации данных ключей по п.16, в котором блок преобразования использует оставшуюся часть избыточной части, в которую не помещено случайное число, для передачи другой информации.

18. Устройство воспроизведения, которое использует содержание, содержащее:

блок получения, предназначенный для получения зашифрованных данных ключа носителя, которые были генерированы устройством генерации данных ключей, преобразующим ключ носителя, на основе предварительно заданного правила преобразования, для формирования преобразованного ключа носителя и шифрования преобразованного ключа носителя с использованием ключа устройства, причем ключ носителя предназначен для использования при использовании содержания;

блок дешифрования, предназначенный для дешифрования зашифрованных данных ключа носителя с использованием ключа устройства, хранимого в устройстве воспроизведения, для получения дешифрованных данных ключа носителя;

блок преобразования, предназначенный для преобразования, на основе предварительно заданного правила преобразования, дешифрованных данных ключа носителя для получения ключа носителя; и

блок использования содержания, предназначенный для использования содержания, на основе ключа носителя.

19. Устройство воспроизведения по п.18, дополнительно содержащее:

блок хранения ключа устройства, предназначенный для хранения ключа устройства; и

блок хранения информации преобразования, предназначенный для хранения информации преобразования, которая является информацией, определенной в соответствии с позицией узла, которому соответствует выбранный ключ устройства в древовидной структуре;

при этом блок получения получает зашифрованные данные ключа носителя от устройства генерации данных ключей по п.4, которое распределяет ключи устройств с использованием древовидной структуры;

блок дешифрования дешифрует зашифрованные данные ключа носителя с использованием ключа устройства для получения дешифрованных данных ключа носителя; и

блок преобразования преобразует дешифрованные данные ключа носителя с

использованием информации преобразования, для получения ключа носителя.

20. Устройство воспроизведения по п.19, дополнительно содержащее:

блок хранения, предназначенный для хранения множества ключей устройств; и

блок выбора, предназначенный для выбора одного из ключей устройств;

причем блок получения получает зашифрованные данные ключа носителя, которые были генерированы устройством генерации данных ключей, получающим преобразованный ключ носителя путем выполнения обратимой операции над ключом носителя и информацией преобразования, сгенерированной для ключа устройства, и шифрующим преобразованный ключ носителя;

блок дешифрования осуществляет дешифрование с использованием выбранного ключа устройства; и

блок преобразования формирует ключ носителя путем генерации информации преобразования для выбранного ключа устройства и применения предварительно заданной операции к выбранному ключу устройства с использованием информации преобразования.

21. Устройство воспроизведения по п.20, в котором блок преобразования генерирует информацию преобразования из информации заголовка, присоединенной к зашифрованным данным ключа носителя.

22. Устройство воспроизведения по п.21, в котором

информация заголовка используется для генерации информации преобразования и генерирована устройством генерации данных ключей, которое распределяет ключи устройств с использованием древовидной структуры, выбирая из ключей устройств, хранимых действительными устройствами воспроизведения, один или более ключей устройств, которые соответствуют узлу в самой верхней позиции в древовидной структуре, и генерирует информацию заголовка на основе информации о позиции каждого из одного или более выбранных ключей устройств в древовидной структуре;

блок хранения хранит информацию о позиции для устройства воспроизведения; и

блок преобразования генерирует информацию преобразования с использованием информации заголовка и хранимой информации о позиции.

23. Устройство воспроизведения по п.21, в котором

информация заголовка предназначена для генерации информации преобразования и генерирована путем соотнесения ключей устройств, которые хранятся в устройствах воспроизведения, с узлами в древовидной структуре, которая определяет соотношения между ключами устройств, совместно используемыми устройствами воспроизведения, и определяет, аннулирован или нет каждый из ключей устройств, выбирая из ключей устройств, хранимых действительными устройствами воспроизведения, по меньшей мере, один ключ устройства, который соответствует узлу в самой верхней позиции в древовидной структуре, и основывая информацию заголовка на информации аннулирования, определенной на основе узла, которому соответствует выбранный ключ устройства, и состоянии аннулирования других узлов;

блок сохранения сохраняет информацию о позиции для устройства воспроизведения в древовидной структуре для распределения ключей устройств для устройств воспроизведения в устройстве генерации данных ключей; и

блок преобразования генерирует информацию преобразования с использованием информации заголовка и сохраненной информации о позиции.

24. Устройство воспроизведения по п.20, в котором блок использования содержания содержит:

субблок шифрования, предназначенный для шифрования содержания на основе

ключа носителя, при этом генерируя зашифрованное содержание; и

субблок вывода, предназначенный для вывода зашифрованного содержания.

25. Устройство воспроизведения по п.20, в котором блок использования содержания дополнительно содержит:

субблок получения содержания, предназначенный для получения зашифрованного содержания;

субблок дешифрования, предназначенный для дешифрования зашифрованного содержания на основе ключа носителя, при этом генерируя содержание; и

субблок воспроизведения, предназначенный для воспроизведения содержания.

26. Устройство воспроизведения по п.18, в котором

преобразованный ключ носителя формируется устройством генерирования данных ключей путем помещения информации преобразования, генерированной для ключа устройства, по меньшей мере, в часть избыточной части ключа носителя; и

блок преобразования генерирует ключ носителя путем удаления избыточной части преобразованного ключа носителя.

27. Способ генерации данных ключей в устройстве генерации данных ключей, которое генерирует данные ключей таким образом, что содержание может использоваться только действительным устройством воспроизведения, причем способ содержит:

этап преобразования в блоке преобразования, преобразующем, на основе предварительно заданного правила преобразования, ключ носителя для использования при использовании содержания, при этом формируя преобразованный ключ носителя;

этап шифрования в блоке шифрования, зашифровывающем преобразованный ключ носителя с использованием ключа устройства, хранимого действительным устройством воспроизведения, при этом формируя зашифрованные данные ключа носителя; и

этап вывода в блоке вывода, выводящем зашифрованные данные ключа носителя.

28. Способ по п.27, дополнительно содержащий:

этап распределения ключей для определения ключей устройств, хранимых в устройствах воспроизведения, путем соотнесения ключей устройств с узлами в древовидной структуре;

этап выбора для выбора, по меньшей мере, одного из определенных ключей устройства;

при этом этап преобразования преобразует ключ носителя, с использованием информации преобразования, которая является информацией, определенной в соответствии с позицией узла, которому выбранный ключ устройства соответствует в древовидной структуре, при этом формируя преобразованный ключа носителя; и

этап шифрования шифрует преобразованный ключ носителя с использованием выбранного ключа устройства, при этом формируя зашифрованные данные ключа носителя.

29. Машиночитаемый носитель записи, содержащий записанную на нем программу, используемую устройством генерации данных ключей, которое генерирует данные ключей таким образом, что содержание может использоваться только действительным устройством воспроизведения, причем программа содержит:

этап преобразования в блоке преобразования, преобразующем, на основе предварительно заданного правила преобразования, ключ носителя для использования при использовании содержания, при этом формируя преобразованный

ключ носителя;

этап шифрования в блоке шифрования, зашифровывающем преобразованный ключ носителя с использованием ключа устройства, хранимого действительным устройством воспроизведения, при этом формируя зашифрованные данные ключа носителя; и

этап вывода в блоке вывода, выводящем зашифрованные данные ключа носителя.

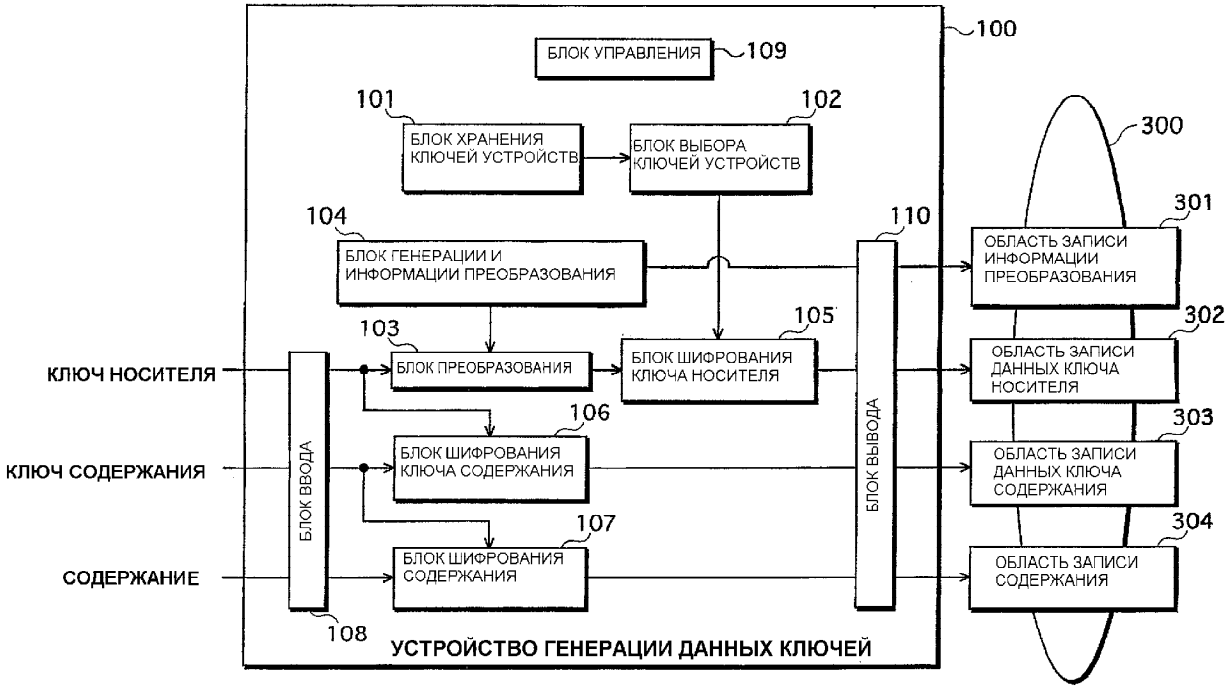
30. Машиночитаемый носитель по п.29, дополнительно содержащий:

этап распределения ключей для определения ключей устройств, хранимых в устройствах воспроизведения, путем соотнесения ключей устройств с узлами в древовидной структуре;

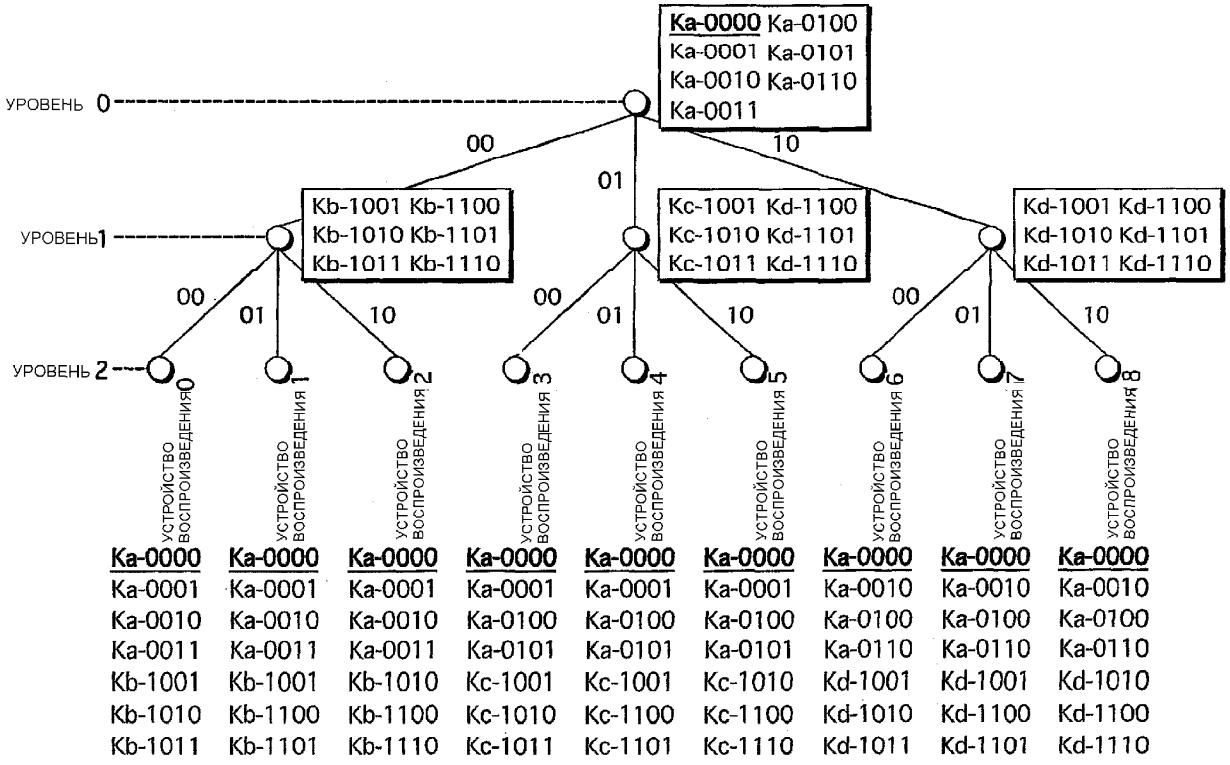
этап выбора для выбора, по меньшей мере, одного из определенных ключей устройств;

при этом этап преобразования преобразует ключ носитля, с использованием информации преобразования, которая является информацией, определенной в соответствии с позицией узла, которому выбранный ключ устройства соответствует в древовидной структуре, при этом формируя преобразованный ключ носителя; и

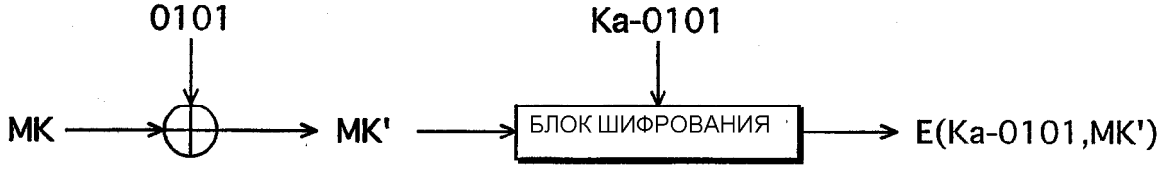
этап шифрования шифрует преобразованный ключ носителя с использованием выбранного ключа устройства, при этом генерируя зашифрованные данные ключа носителя.



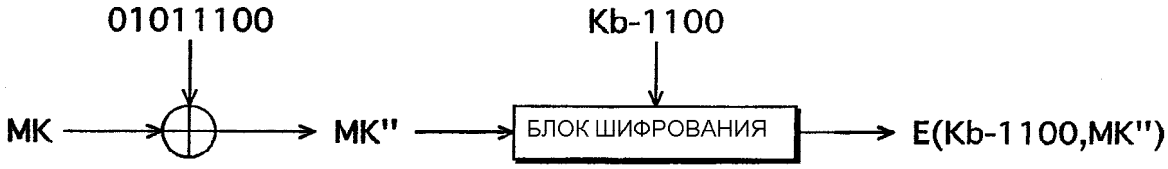
ФИГ. 1



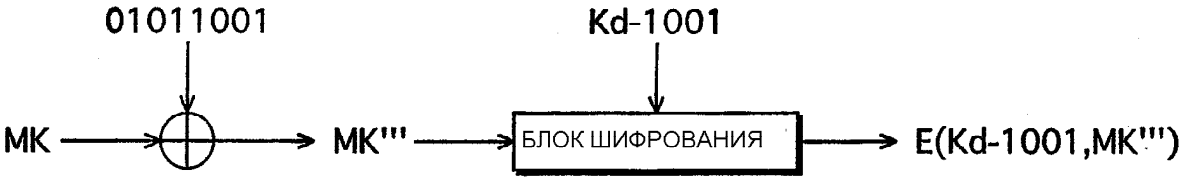
ФИГ. 2



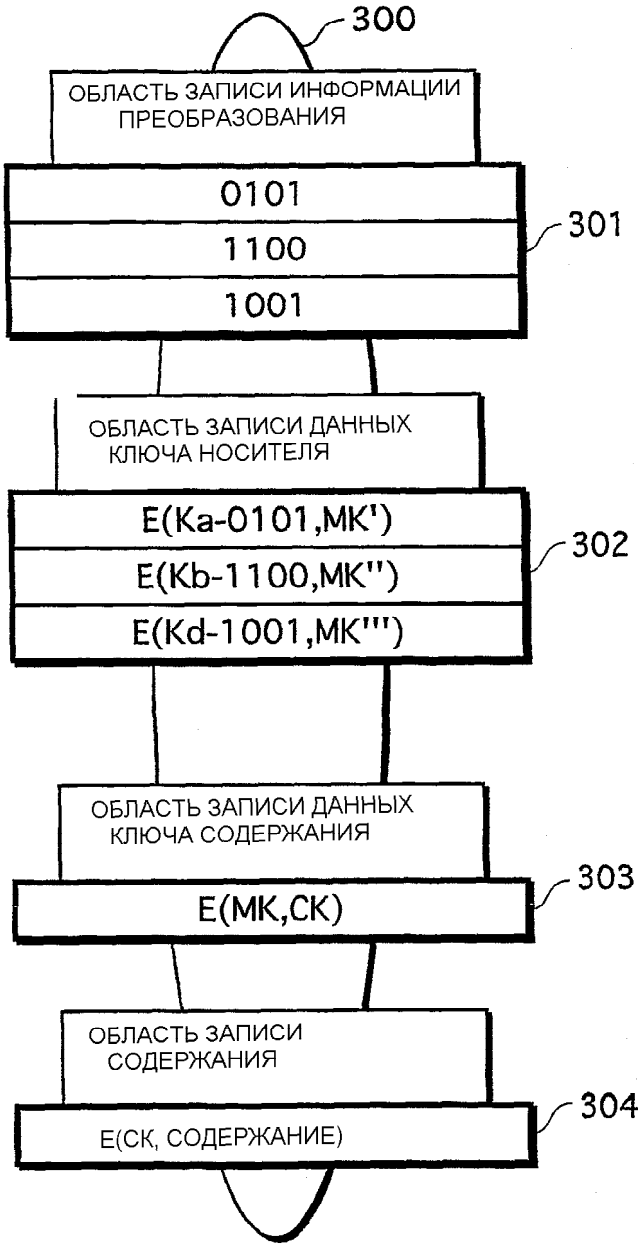
ФИГ. 4А



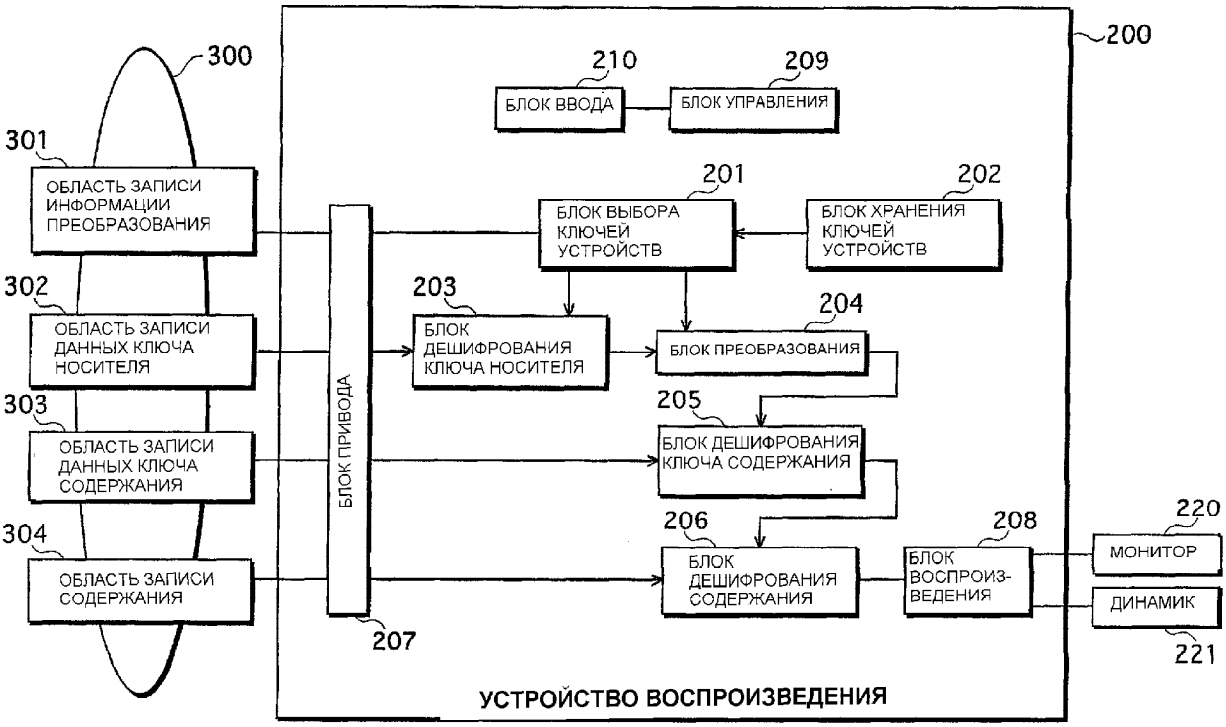
ФИГ. 4B



ФИГ. 4C

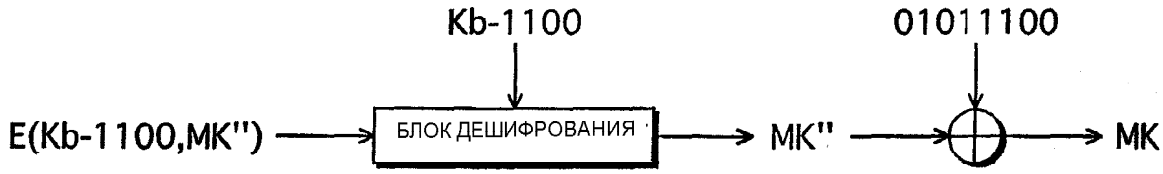


ФИГ. 5

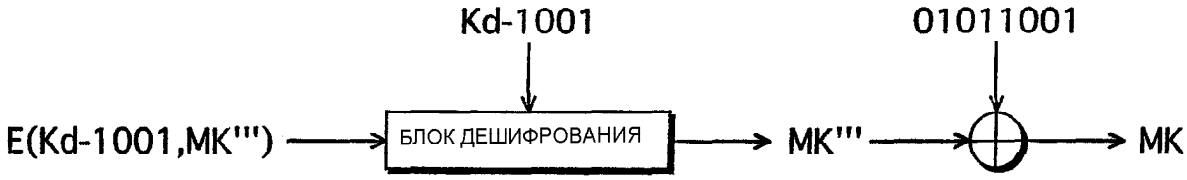


ФИГ. 6

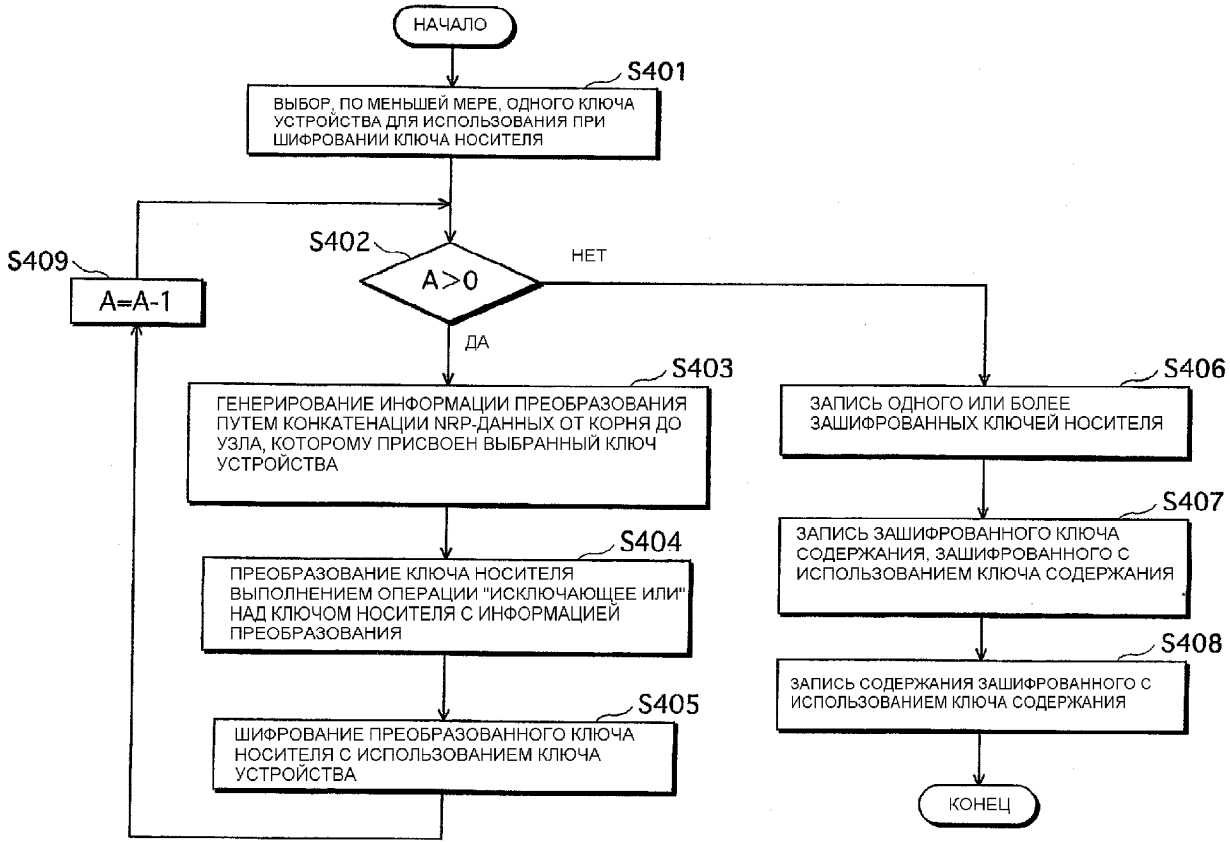
ФИГ. 7A



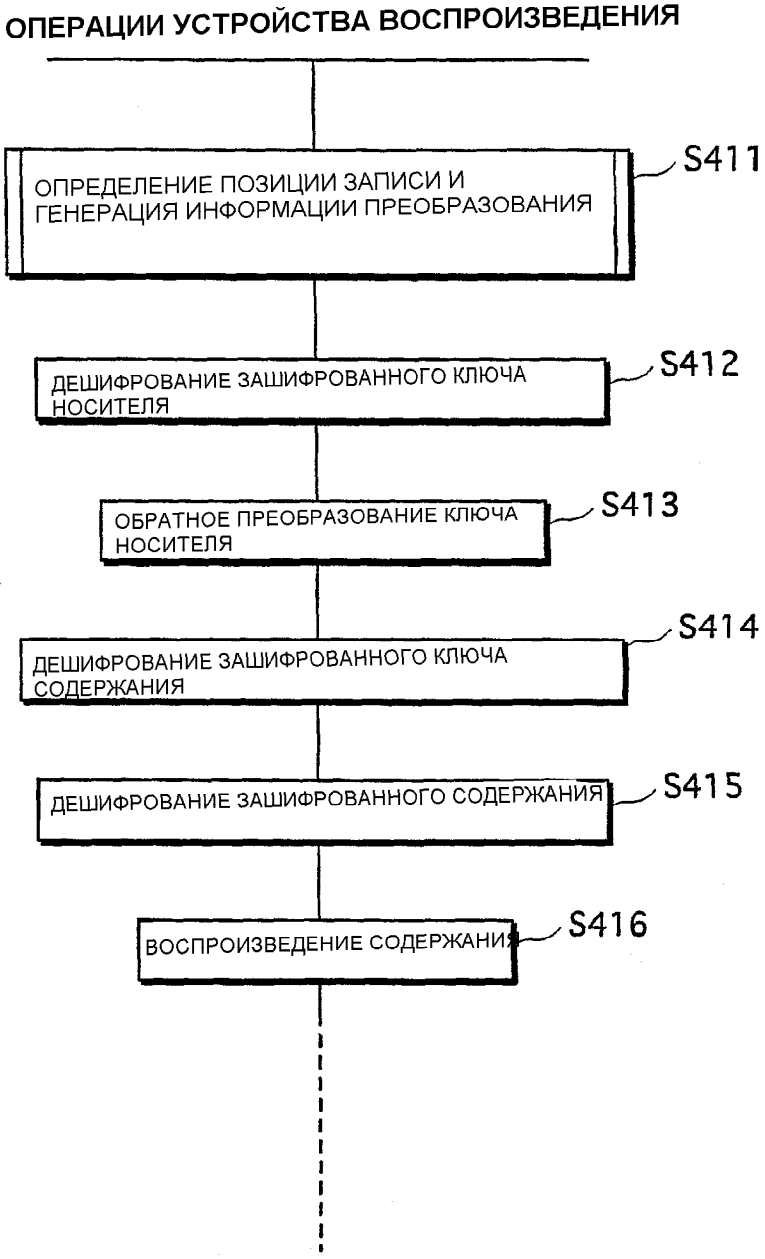
ФИГ. 7B



ФИГ. 7C

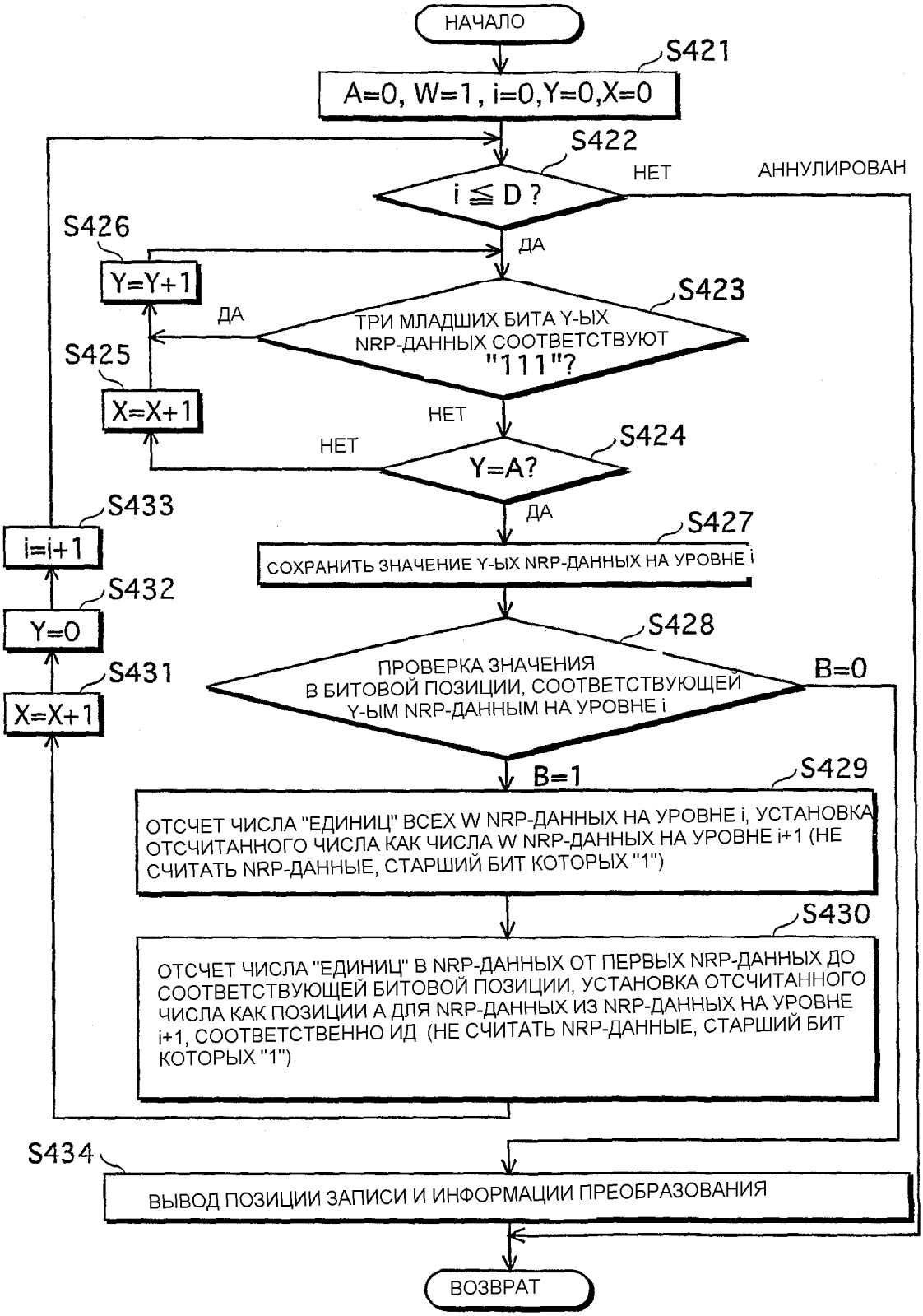

НАЧАЛО
S401
ВЫБОР, ПО МЕНЬШЕЙ МЕРЕ, ОДНОГО КЛЮЧА УСТРОЙСТВА ДЛЯ ИСПОЛЬЗОВАНИЯ ПРИ ШИФРОВАНИИ КЛЮЧА НОСИТЕЛЯ
S402
A>0
НЕТ
ДА
S409
A=A-1
S403
ГЕНЕРИРОВАНИЕ ИНФОРМАЦИИ ПРЕОБРАЗОВАНИЯ ПУТЕМ КОНКАТЕНАЦИИ NRP-ДАННЫХ ОТ КОРНЯ ДО УЗЛА, КОТОРОМУ ПРИСВОЕН ВЫБРАННЫЙ КЛЮЧ УСТРОЙСТВА
S404
ПРЕОБРАЗОВАНИЕ КЛЮЧА НОСИТЕЛЯ ВЫПОЛНЕНИЕМ ОПЕРАЦИИ "ИСКЛЮЧАЮЩЕЕ ИЛИ" НАД КЛЮЧОМ НОСИТЕЛЯ С ИНФОРМАЦИЕЙ ПРЕОБРАЗОВАНИЯ
S405
ШИФРОВАНИЕ ПРЕОБРАЗОВАННОГО КЛЮЧА НОСИТЕЛЯ С ИСПОЛЬЗОВАНИЕМ КЛЮЧА УСТРОЙСТВА
S406
ЗАПИСЬ ОДНОГО ИЛИ БОЛЕЕ ЗАШИФРОВАННЫХ КЛЮЧЕЙ НОСИТЕЛЯ
S407
ЗАПИСЬ ЗАШИФРОВАННОГО КЛЮЧА СОДЕРЖАНИЯ, ЗАШИФРОВАННОГО С ИСПОЛЬЗОВАНИЕМ КЛЮЧА СОДЕРЖАНИЯ
S408
ЗАПИСЬ СОДЕРЖАНИЯ ЗАШИФРОВАННОГО С ИСПОЛЬЗОВАНИЕМ КЛЮЧА СОДЕРЖАНИЯ
КОНЕЦ

ФИГ. 8

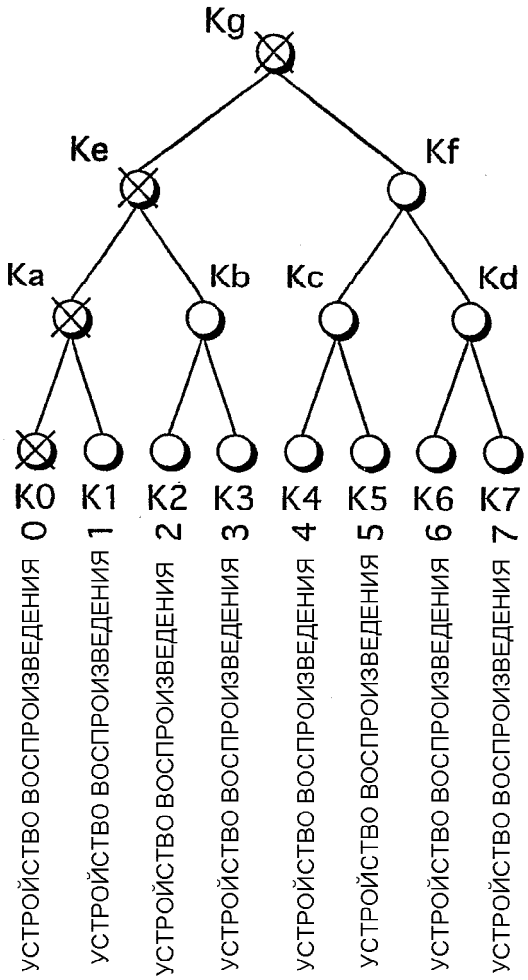

ОПЕРАЦИИ УСТРОЙСТВА ВОСПРОИЗВЕДЕНИЯ
ОПРЕДЕЛЕНИЕ ПОЗИЦИИ ЗАПИСИ И ГЕНЕРАЦИЯ ИНФОРМАЦИИ ПРЕОБРАЗОВАНИЯ
S411
ДЕШИФРОВАНИЕ ЗАШИФРОВАННОГО КЛЮЧА НОСИТЕЛЯ
S412
ОБРАТНОЕ ПРЕОБРАЗОВАНИЕ КЛЮЧА НОСИТЕЛЯ
S413
ДЕШИФРОВАНИЕ ЗАШИФРОВАННОГО КЛЮЧА СОДЕРЖАНИЯ
S414
ДЕШИФРОВАНИЕ ЗАШИФРОВАННОГО СОДЕРЖАНИЯ
S415
ВОСПРОИЗВЕДЕНИЕ СОДЕРЖАНИЯ
S416

ФИГ. 9

ОПРЕДЕЛЕНИЕ ПОЗИЦИИ ЗАПИСИ И ГЕНЕРАЦИЯ ИНФОРМАЦИИ ПРЕОБРАЗОВАНИЯ

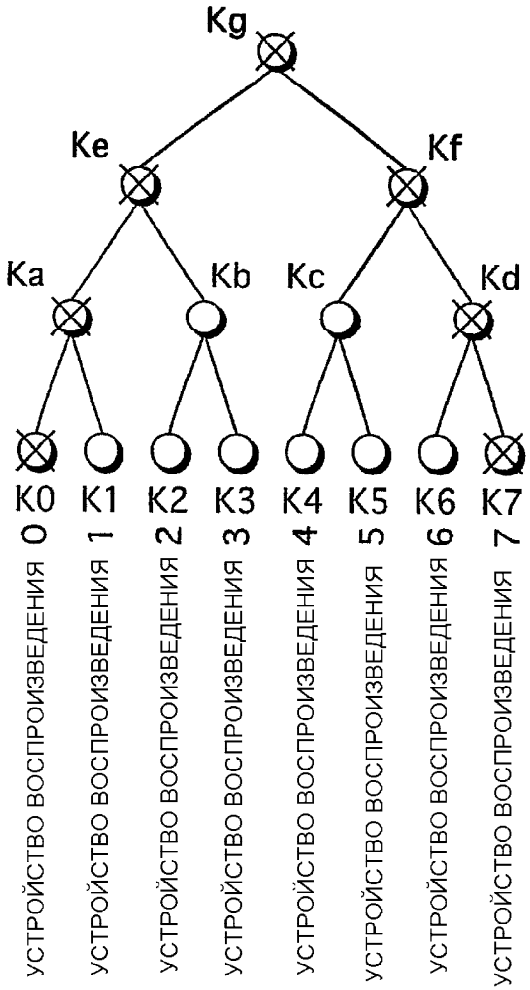


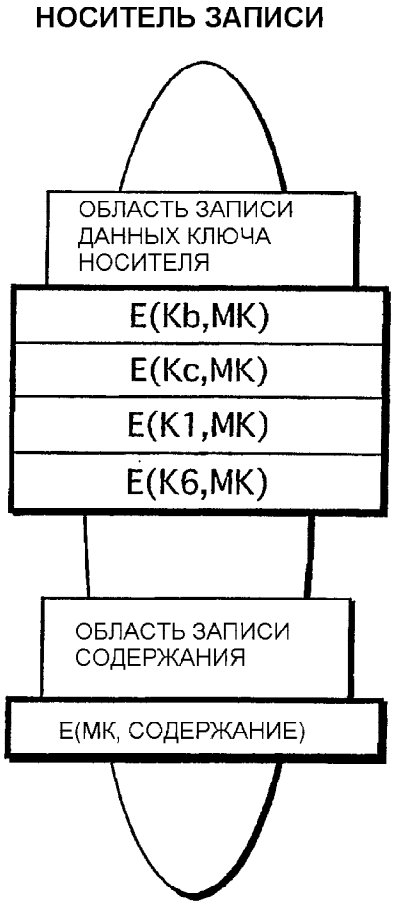
ФИГ. 10


Kg
Ke
Kf
Ka
Kb
Kc
Kd
K0
K1
K2
K3
K4
K5
K6
K7
УСТРОЙСТВО ВОСПРОИЗВЕДЕНИЯ 0
УСТРОЙСТВО ВОСПРОИЗВЕДЕНИЯ 1
УСТРОЙСТВО ВОСПРОИЗВЕДЕНИЯ 2
УСТРОЙСТВО ВОСПРОИЗВЕДЕНИЯ 3
УСТРОЙСТВО ВОСПРОИЗВЕДЕНИЯ 4
УСТРОЙСТВО ВОСПРОИЗВЕДЕНИЯ 5
УСТРОЙСТВО ВОСПРОИЗВЕДЕНИЯ 6
УСТРОЙСТВО ВОСПРОИЗВЕДЕНИЯ 7


НОСИТЕЛЬ ЗАПИСИ
ОБЛАСТЬ ЗАПИСИ ДАННЫХ КЛЮЧА НОСИТЕЛЯ
E(Kf,MK)
E(Kb,MK)
E(K1,MK)
ОБЛАСТЬ ЗАПИСИ СОДЕРЖАНИЯ
E(MK, СОДЕРЖАНИЕ)

ФИГ. 11


Kg
Ke
Kf
Ka
Kb
Kc
Kd
K0
K1
K2
K3
K4
K5
K6
K7
УСТРОЙСТВО ВОСПРОИЗВЕДЕНИЯ 0
УСТРОЙСТВО ВОСПРОИЗВЕДЕНИЯ 1
УСТРОЙСТВО ВОСПРОИЗВЕДЕНИЯ 2
УСТРОЙСТВО ВОСПРОИЗВЕДЕНИЯ 3
УСТРОЙСТВО ВОСПРОИЗВЕДЕНИЯ 4
УСТРОЙСТВО ВОСПРОИЗВЕДЕНИЯ 5
УСТРОЙСТВО ВОСПРОИЗВЕДЕНИЯ 6
УСТРОЙСТВО ВОСПРОИЗВЕДЕНИЯ 7


НОСИТЕЛЬ ЗАПИСИ
ОБЛАСТЬ ЗАПИСИ ДАННЫХ КЛЮЧА НОСИТЕЛЯ
E(Kb,MK)
E(Kc,MK)
E(K1,MK)
E(K6,MK)
ОБЛАСТЬ ЗАПИСИ СОДЕРЖАНИЯ
E(MK, СОДЕРЖАНИЕ)

ФИГ. 12