РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 261 315** (13) **C2**

(51) МПК[7] **E 05 B 49/00, G 07 C 9/00**

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21), (22) Заявка: **2002127121/12, 09.03.2001**

(24) Дата начала действия патента: **09.03.2001**

(30) Приоритет: **10.03.2000 (пп.1-12) SE 0000795-5**

(43) Дата публикации заявки: **20.03.2004**

(45) Опубликовано: **27.09.2005 Бюл. № 27**

(56) Список документов, цитированных в отчете о поиске: **US 6005487 A, 21.12.1999. US 4736419 A, 05.04.1988. WO 9825000 A1, 11.06.1998. US 4912310 A, 27.03.1990. WO 9015211 A1, 13.12.1990. EP 410024 A1, 30.01.1991. RU 94039940 A1, 10.09.1996.**

(85) Дата перевода заявки PCT на национальную фазу: **10.10.2002**

(86) Заявка PCT:
SE 01/00501 (09.03.2001)

(87) Публикация PCT:
WO 01/66888 (13.09.2001)

Адрес для переписки:
191186, Санкт-Петербург, а/я 230, "АРС-ПАТЕНТ", пат.пов. В.М.Рыбакову, рег. № 90

(72) Автор(ы):
ЛИДЕН Инге (SE),
НОРБЕРГ Рольф (SE),
МАГНУССОН Бьёрн (SE),
СИВОНЕН Ханну (FI),
БРЕННЕКЕ Гудрун (DE),
ШАНЕЛЬ Кристоф (DE),
КРЮН Юрген (DE),
КИКЕБУШ Бернд (DE),
ЛЕФЕБВР Арно (FR)

(73) Патентообладатель(ли):
АССА АБЛОЙ АБ (SE)

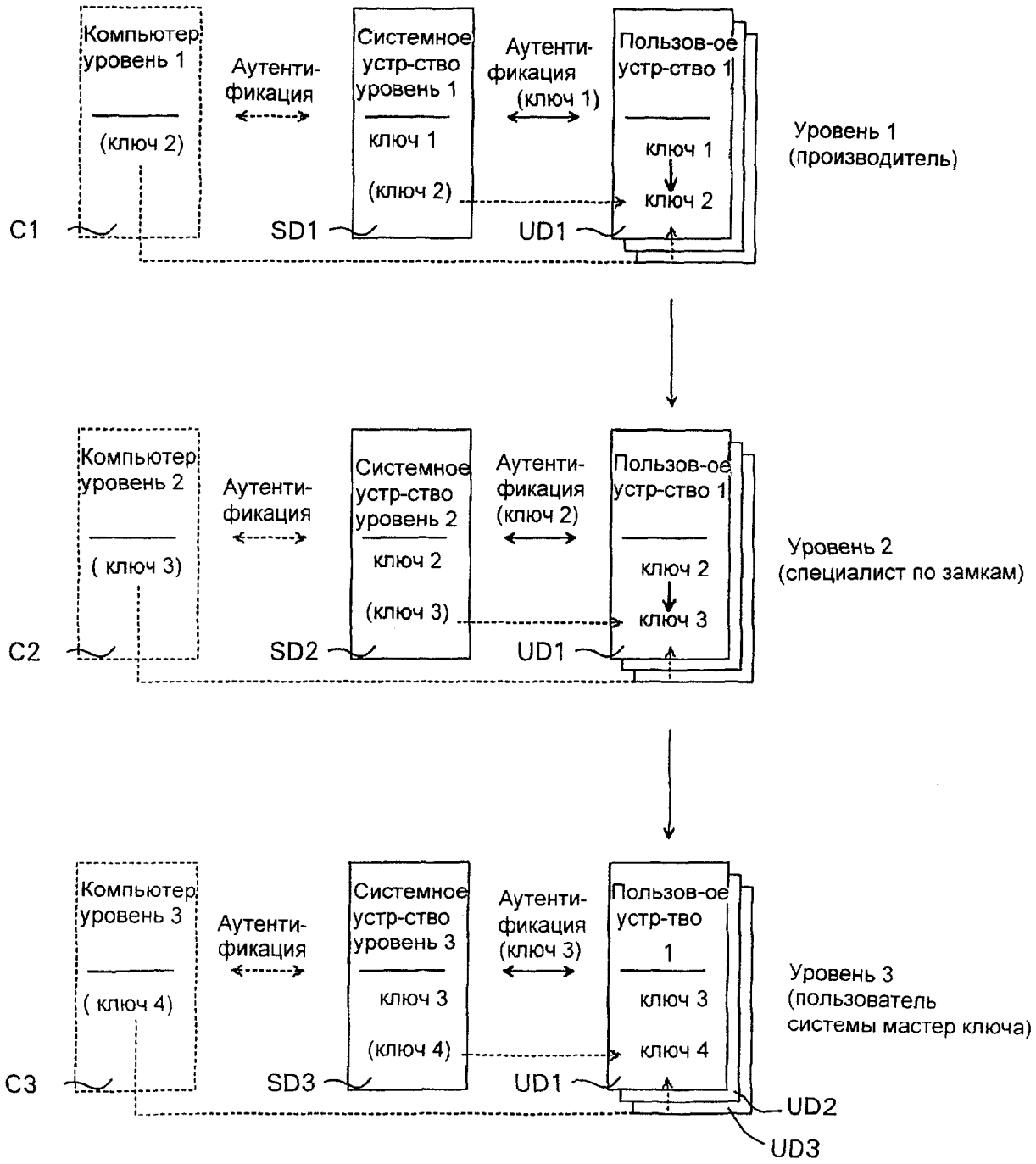
(54) ЗАПОРНОЕ УСТРОЙСТВО С КЛЮЧОМ

(57) Реферат:

Изобретение относится к области электромеханических запорных устройств и касается запорного устройства с ключом, содержащего несколько пользовательских устройств, включающих несколько пользовательских ключей с электронной схемой, которая содержит электронную память, способную хранить переменный электронный шифровальный ключ, и несколько замков с электронной схемой, способной хранить переменный электронный шифровальный ключ. Замок и пользовательский ключ способны совместно работать, только если в их память записаны идентичные шифровальные ключи. Имеется, по меньшей мере, одно системное устройство, имеющее электронную схему с электронной памятью, способной хранить постоянный электронный шифровальный ключ. Компьютерное программное обеспечение может изменять переменный электронный шифровальный ключ пользовательского устройства таким образом, что в случае успешной процедуры аутентификации, осуществляемой между замком или пользовательским ключом с записанным переменным электронным шифровальным ключом и системным устройством с записанным шифровальным ключом, идентичным упомянутому шифровальному ключу замка или пользовательского ключа, первый шифровальный ключ заменяется вторым шифровальным ключом. Данное устройство обеспечивает высокий уровень безопасности. 3 н. и 9 з.п. ф-лы, 8 ил.

RU 2261315 C2

RU 2261315 C2



ФИГ.1

RU 2261315 C2

RUSSIAN FEDERATION

(19) **RU** (11) **2 261 315** (13) **C2**

(51) Int. Cl.[7] **E 05 B 49/00, G 07 C 9/00**

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY,
PATENTS AND TRADEMARKS

(12) ABSTRACT OF INVENTION

(21), (22) Application: **2002127121/12, 09.03.2001**

(24) Effective date for property rights: **09.03.2001**

(30) Priority: **10.03.2000 (cl.1-12) SE 0000795-5**

(43) Application published: **20.03.2004**

(45) Date of publication: **27.09.2005 Bull. 27**

(85) Commencement of national phase: **10.10.2002**

(86) PCT application:
SE 01/00501 (09.03.2001)

(87) PCT publication:
WO 01/66888 (13.09.2001)

Mail address:
191186, Sankt-Peterburg, a/ja 230, "ARS-PATENT", pat.pov. V.M.Rybakovu, reg. № 90

(72) Inventor(s):
LIDEN Inge (SE),
NORBERG Rol'f (SE),
MAGNUSSON B'ern (SE),
SIVONEN Khannu (FI),
BRENNEKE Gudrun (DE),
ShANEL' Kristof (DE),
KRJuN Jurgen (DE),
KIKEBUSh Bernd (DE),
LEFEBVR Arno (FR)

(73) Proprietor(s):
ASSA ABLOJ AB (SE)

(54) KEY-OPERATED LOCKING DEVICE

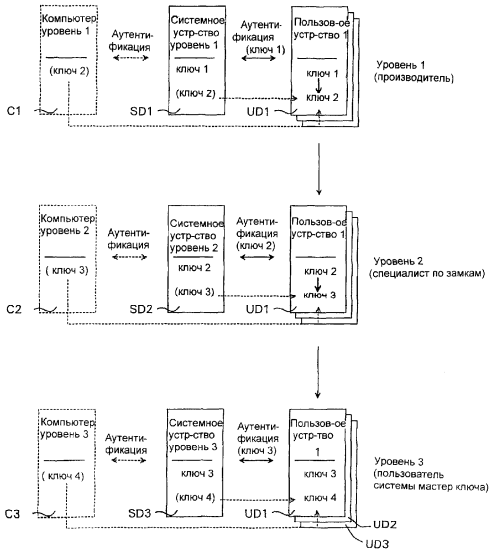
(57) Abstract:

FIELD: electromechanical locking devices, particularly electric permutation locks and circuits therefore.

SUBSTANCE: locking device comprises a number of user devices including several user keys with electronic circuit. The electronic circuit includes electronic memory which is adapted to store changeable electronic coded key and several locks with electronic circuits adapted to store changeable electronic coded key. Lock and user key may cooperate only when identical coded keys are saved in memory thereof. The device also has at least one system component having electronic circuit with electronic memory adapted to store constant electronic coded key. Software is used to change changeable coded key of used device so that when identity verification procedure between lock or user key with changeable coded key and system component with saved coded key identical to above coded key of the lock or user key is successfully completed the first coded key is substituted for the second one.

EFFECT: increased security level.

12 cl, 8 dwg



ФИГ.1

RU 2261315 C2

RU 2261315 C2

ОБЛАСТЬ ТЕХНИКИ, К КОТОРОЙ ОТНОСИТСЯ ИЗОБРЕТЕНИЕ

Настоящее изобретение в основном относится к запорному устройству с ключом, а более конкретно, к электромеханическому запорному устройству, пригодному для использования в запорной системе, в которой для повышения уровня безопасности между различными уровнями запорной системы на стадии производства применяется переменный электронный шифровальный ключ. Изобретение также относится к способу и системе, в которой используется переменный шифровальный ключ.

УРОВЕНЬ ТЕХНИКИ

Известны электромеханические запорные системы, в которых выдача ключей различным пользователям происходит обычным образом, подобным распределению ключей в механической запорной системе. Однако выполнение такого распределения весьма затруднительно, и оно является обременительной процедурой в плане выдачи новых ключей. Кроме того, постоянно существует опасность попадания системного ключа неуполномоченному лицу, что приводит к угрозе безопасности и т.д.

Другая проблема заключается в том, что электронные коды могут быть скопированы, например, путем "записи" кода при помощи считывающего устройства, в силу чего в системе возможно наличие копий ключей без уведомления об этом владельца системы.

Следующая проблема известных из уровня техники систем заключается в возможности использования заготовок ключей любым лицом, что также ставит вопрос об угрозе безопасности.

В патентном документе США №6005487 (Hyatt, Jr. и др.) раскрыта электронная система безопасности, включающая электронный запорный механизм и электронный ключ. С целью устранения необходимости дорогостоящего повторного изготовления ключей в случае их утраты, а также возможности внутреннего воровства и подделок, система согласно Hyatt, Jr. и др. предусматривает смену идентификационного кода ключа или замка. Однако вышеупомянутые проблемы уровня техники в данной системе не решены.

СУЩНОСТЬ ИЗОБРЕТЕНИЯ

Задачей настоящего изобретения является создание электромеханического запорного устройства ранее упомянутого типа, используемого в системе, в которой распределение и авторизация (выдача разрешений на осуществление определенных операций) ключей и замков между производителем, дистрибьютором и пользователем происходит на высоком уровне безопасности.

Другая задача настоящего изобретения состоит в обеспечении электромеханического запорного устройства с усовершенствованной процедурой распределения и авторизации ключей.

Следующая задача - это создание ключа, копирование которого было бы затруднительно без уведомления собственника системы.

Очередная задача заключается в разработке заготовки ключа, использование которой было бы ограничено некоторым числом дистрибьюторов.

Еще одна задача состоит в обеспечении простой и надежной процедуры добавления ключей и замков к запорной системе.

Следующая задача - это разработка способа и системы безопасного хранения и отображения информации о системе мастер ключа.

Другая задача заключается в разработке способа и системы обмена информацией между производителем, дистрибьютором и конечным пользователем запорного устройства.

В основе изобретения лежит представление о том, что вышеупомянутые проблемы уровня техники могут быть решены за счет обеспечения и замены электронных кодов в ключах и замках, причем эти коды используются для шифрования данных, передаваемых между ключами и замками, а также между различными сторонами, работающими в здании и занятыми в обслуживании запорной системы.

В соответствии с настоящим изобретением предлагается способ, определенный в пункте 1.

В соответствии с настоящим изобретением также предлагается запорное устройство с

ключом, определенное в пункте 9, а также запорное устройство с ключом, определенное в пункте 12.

Дальнейшие предпочтительные варианты осуществления изобретения определены в зависимых пунктах.

Способ, запорное устройство с ключом и система согласно изобретению позволяют решить, по меньшей мере, некоторые из перечисленных выше проблем предшествующего уровня техники.

ПЕРЕЧЕНЬ ФИГУР ЧЕРТЕЖЕЙ

Далее изобретение описывается при помощи примеров со ссылками на сопроводительные чертежи, где

на фиг.1 представлена схема, поясняющая основную идею настоящего изобретения;

на фиг.2 представлен общий вид иерархической запорной системы, содержащей запорные устройства согласно изобретению.

на фиг.3а и 3б представлены информационные элементы соответственно ключа и замка запорного устройства согласно изобретению;

на фиг.4 представлен пример информационного потока системы, показанной на фиг.2;

на фиг.5 дано общее представление кодовых элементов электронного ключа, имеющихся в запорном устройстве согласно изобретению;

на фиг.6 представлена схема, иллюстрирующая защищенный обмен данными между производителем, дистрибьютором и пользователем;

на фиг.7 представлен общий вид процедуры шифрования базы данных, используемой в рамках изобретения; и

на фиг.8 представлены примерные таблицы шифрования файлов базы данных.

СВЕДЕНИЯ, ПОДТВЕРЖДАЮЩИЕ ВОЗМОЖНОСТЬ ОСУЩЕСТВЛЕНИЯ ИЗОБРЕТЕНИЯ

Далее описываются предпочтительные варианты осуществления изобретения. Для ясности изложения понятие "ключ" уточняется добавлением прилагательного "физический", если ключ относится к физическим ключам, то есть механическим ключам, используемым для замков, или добавлением прилагательного "электронный" или "шифровальный", если он относится к электронным ключам, таким как шифровальные ключи.

Кроме того, приставка "e" используется для обозначения закодированной информации, а приставка "d" - для обозначения декодированной информации. За приставкой идет шифровальный ключ, использованный для операции кодирования или декодирования. Таким образом, например, выражение eKx(файл 1) означает файл 1, закодированный с помощью шифровального ключа "Kx".

В данном описании иногда приводится понятие "устройство". В контексте изобретения устройство понимается как запорное устройство с ключом.

Сначала поясняется основная идея настоящего изобретения со ссылкой на фиг.1, иллюстрирующей схему различных частей запорной системы согласно изобретению. Показаны три "уровня" запорной системы, обозначенные соответственно как "Производитель", "Мастер по замкам" и "Пользователь MKS (системы мастер-ключа)". На каждом уровне предусмотрено системное устройство и в качестве необязательного компонента компьютер, присутствующий на одном или более уровнях. На различных уровнях показаны пользовательские устройства, такие как ключи и/или замки. Однако "устройство 1 пользователя" является одним и тем же на всех уровнях, хотя и находится в различных "режимах".

Каждое системное и пользовательское устройство имеет скрытый шифровальный ключ, "ключ 1", "ключ 2" и т.д., хранимый в памяти этого устройства. Эти шифровальные ключи используются для процедуры аутентификации (опознавания) между системными и пользовательскими устройствами, а также между различными пользовательскими устройствами, то есть между ключами и замками, на уровне конечного пользователя. Шифровальные ключи, хранимые в памяти пользовательских устройств, являются переменными, то есть они могут быть изменены при помощи системного устройства,

используемого для этой цели, возможно, совместно с компьютером, на котором установлено программное обеспечение, как будет пояснено в дальнейшем.

Изначально пользовательское устройство UD1, находящееся на уровне 1, содержит шифровальный ключ "ключ 1", записанный, например, во время изготовления заготовки ключа. Когда пользовательское устройство 1 должно быть отправлено на уровень 2, между системным устройством SD1 и пользовательским устройством UD1 инициируется процедура аутентификации с использованием шифровального ключа "ключ 1". В случае успешного опознавания в ходе этой процедуры "ключ 1", хранимый в памяти пользовательского устройства, заменяется "ключом 2", и процедура завершается. Новый шифровальный ключ "ключ 2" может быть обеспечен либо самим системным устройством, либо, факультативно, компьютером C1. На этом уровне между данным пользовательским устройством и системным устройством в дальнейшем невозможно успешное осуществление процессов аутентификации, поскольку шифровальные ключи не соответствуют друг другу.

Теперь пользовательское устройство может быть без риска переправлено на уровень 2 мастера по замкам, так как мошенник, получивший незаконным путем это устройство, не в состоянии использовать его без получения скрытого шифровального ключа, содержащегося в памяти этого устройства, то есть "ключа 2".

Как и на уровне 1, на уровне 2 соответствующая процедура выполняется перед моментом доставки пользовательского устройства конечному пользователю, а именно, "ключ 2", хранимый в памяти пользовательского устройства, заменяется "ключом 3" при помощи системного устройства SD2, используемого для этой цели, возможно, вместе с компьютером C2.

Пользовательское устройство, получаемое на уровне 3 конечного пользователя, не может быть применено до его авторизации, осуществляемой системным устройством SD3 таким же образом, как и на уровне 2. Это означает, что шифровальный ключ "ключ 3" заменяется "ключом 4" после успешного опознавания с использованием "ключа 3". Все пользовательские устройства, то есть все ключи и замки системы мастер ключа должны пройти через такой процесс до начала их использования. Это также означает, что все "активированные" пользовательские устройства содержат в памяти шифровальный ключ "ключ 4" и тем самым способны успешно опознавать друг друга. В результате обеспечивается полная безопасность при распределении ключей или замков конечному пользователю системы мастер ключа.

В дальнейшем со ссылкой на фиг.2 подробно описывается запорная система, содержащая запорные устройства согласно изобретению. На фиг.2 показан обычный порядок распределения аппаратных средств и программного обеспечения по различным иерархическим уровням, а именно, уровню (системе) 100 пользователя или клиента, уровню (системе) 200 дистрибьютора или продавца и уровню (системе) 300 производителя или изготовителя.

Пользовательские ключи

В системе 100 пользователя имеются несколько пользовательских ключей 101, используемых с некоторым количеством замков 20. Вместе эти ключи и замки составляют систему мастер ключа (MKS). Каждый ключ содержит уникальный индивидуальный электронный код, управляющий его работой. Код разделен на различные сегменты, которые используются производителями, дистрибьюторами и пользователями. Для открытой (общедоступной) информации предусмотрен открытый сегмент, а для закрытой информации - закрытый сегмент. Сегменты далее разделены на различные элементы электронного кода или атрибуты. Ниже применительно к описанию защищенных режимов объясняется, что такое электронный код ключа.

Ключ программирования и авторизации

В системе 100 пользователя предусмотрен, по меньшей мере, один пользовательский ключ 102 программирования и авторизации (C-ключ). C-ключи, а также D-ключи и M-ключи (описаны в дальнейшем) в данной заявке именуются системными ключами (SYS-ключами).

Программируемый модуль пользователя

В системе пользователя предусмотрен программируемый модуль 106, соединяемый с компьютером (персональным компьютером) 104 через, например, последовательный интерфейс. Этот программируемый модуль содержит статическое считывающее устройство 107 и применяется для программирования системы пользователя. Статическое считывающее устройство представляет собой устройство для считывания данных с ключа, не имеющего блокирующего механизма, и содержащее электронные схемы и т.п. для считывания и программирования ключа.

Хотя программируемый модуль пользователя и представлен на фиг.2, он может отсутствовать в очень небольших запорных системах.

Программное обеспечение пользователя

Пользователь имеет доступ к персональному компьютеру 104, на котором установлено управляющее программное обеспечение пользователя (С-обеспечение), работающее только с открытой системной информацией. Таким образом, С-обеспечение ведет в так называемой таблице замка учет разрешенных ключей для каждого замка данной системы мастер ключа. Однако секретные идентификаторы (описаны ниже) всех ключей хранятся в зашифрованном виде и могут быть считаны лишь при помощи системного ключа.

Ключ авторизации дистрибьютора

Предусмотрен ключ 202 авторизации дистрибьютора (D-ключ), предназначенный для дистрибьютора запорной системы, которым может быть, например, мастер по замкам.

Программируемый модуль дистрибьютора

В системе дистрибьютора имеется также программируемый модуль 206, соединяемый с компьютером 204 (персональным компьютером) через, например, последовательный интерфейс. Этот программируемый модуль может быть идентичен или подобен модулю, описанному применительно к системе 100 пользователя.

Программное обеспечение дистрибьютора

Дистрибьютор обладает специальным компьютерным программным обеспечением (D-обеспечением), предназначенным для персонального компьютера 204. Это D-обеспечение содержит открытый раздел для отображения открытой системной информации, а также для внесения изменений и т.п. Кроме того, обеспечение содержит закрытый раздел, включающий используемые в системе коды разрешений и секретные пароли. D-обеспечение поддерживает передачу данных в зашифрованном виде на компьютер 304 производителя запорной системы, осуществляемую, например, через модемную схему 208, как будет пояснено в дальнейшем.

В качество одного из модулей программное обеспечение производителя использует регистр ключей или замков, описывающий систему пользователя. Таким образом, дистрибьютор может работать незаметно для пользователя, как если бы программное обеспечение дистрибьютора и пользователя являлось бы одной системой. Это необходимо для дистрибьютора, если он собирается вплотную заниматься обслуживанием системы пользователя.

Ключ авторизации производителя

Для производителя запорной системы предусмотрен ключ 302 авторизации производителя (М-ключ).

Программируемый модуль производителя

В системе производителя также имеется программируемый модуль 306, который подобен программируемому модулю 206 дистрибьютора и может быть соединен с компьютером 304 (персональным компьютером).

Программное обеспечение производителя

Производитель имеет доступ к персональному компьютеру 304, на котором установлено программное обеспечение (М-обеспечение) с полным разрешением на проведение операций добавления и удаления ключей и замков.

Информационные элементы

Все ключи и замки имеют уникальную электронную идентификацию или код, содержащий

несколько информационных элементов, управляющих функционированием ключей и замков. Информационные элементы ключа и замка далее описываются соответственно со ссылками на фиг.3a и 3b.

Электронный код разделен на различные сегменты, используемые производителями, дистрибьюторами и пользователями. Некоторые открытые элементы являются общими для нескольких устройств системы мастер ключа, в то время как для хранения закрытой информации предусмотрен закрытый сегмент, который всегда индивидуален для группы.

Каждый электронный код ключа содержит следующие части:

- открытый идентификатор ключа (PKID), включающий:
- идентификатор производителя (M);
- идентификатор системы мастер ключа (MKS);
- идентификатор ролевой функции (F);
- идентификатор группы (GR);
- уникальную идентификацию (UID);
- шифровальный ключ (K_{DES});
- секретный идентификатор ключа (SKID), включающий
- секретный идентификатор группы (SGR).

Соответственно, каждый электронный код замка содержит следующие части:

- открытый идентификатор замка (PLID), включающий
- идентификатор производителя (M);
- идентификатор системы мастер ключа (MKS);
- идентификатор ролевой функции (F);
- идентификатор группы (GR);
- уникальную идентификацию (UID);
- шифровальный ключ (K_{DES});
- секретный идентификатор замка (SLID), включающий
- секретный идентификатор группы (SGR).

Более подробно основные элементы описываются ниже.

M-производитель

Элемент M означает производителя системы мастер ключа. Таким образом, каждому производителю, использующему техническое решение согласно изобретению, присваивается уникальный M код, распознающий ключи и замки, которые поставлены этим производителем.

MKS - система мастер ключа

Элемент MKS идентифицирует различные системы 100 мастер ключа. К замку подойдет пользовательский ключ или C-кпюч, только если их коды MKS совпадают.

F-ролевая функция

Элемент F идентифицирует ролевое имя устройства, то есть является ли оно замком, пользовательским ключом, C-ключом, D-ключом, M-ключом и т.д.

GR-группа

Элемент GR является целым числом, идентифицирующим группу устройств. Элемент GR уникален для каждой системы мастер ключа, а его значение возрастает на единицу, начиная от числа 1.

UID - уникальная идентификация

Элемент UID идентифицирует различных пользователей в группе. Он уникален для каждой группы и возрастает на единицу, начиная от числа 1. Таким образом, комбинация идентификатора группы и элемента уникальной идентификации однозначным образом распознает устройство в системе мастер ключа.

K_{DES} - шифровальный ключ

K_{DES} - шифровальный ключ - содержит случайно генерируемый шифровальный ключ. В предпочтительном варианте осуществления изобретения используется шифровальный алгоритм DES (стандарт шифрования данных) отчасти в связи с его скоростью реализации, а предпочтительно тройной DES (трехкратное применение стандарта шифрования

данных). Существуют несколько режимов DES-шифрования, в изобретении предусмотрены два из них: ECB (режим электронной кодовой книги) и CBC (режим шифрования со сцеплением блоков).

Для всех устройств системы мастер ключа ключ K_{DES} идентичен.

K_{DES} никоим образом не может быть считан извне и используется только алгоритмами, выполняемыми внутри запорных устройств согласно изобретению. Это является очень важной особенностью, поскольку устраняет возможность копирования ключа просто путем считывания содержимого его памяти. Далее, K_{DES} присутствует только в ключах, находящихся в рабочем режиме. Ниже приведено описание защищенного режима.

K_{DES} используется в процедуре авторизации, реализуемой между различными устройствами. Таким образом, чтобы ключ был способен приводить в действие замок, оба этих устройства должны иметь одинаковый K_{DES}. Иначе процедура авторизации не будет успешной.

SGR - секретная группа

Элемент SGR является случайно генерируемым числом, которое одинаково для одной группы. Вышеупомянутые информационные элементы, так же как и другие электронные данные, используемые в запорной системе согласно изобретению, представляют собой информацию, которая, без сомнения, жизненно важна для функционирования системы. Таким образом, с целью обеспечения целостности данных для некоторых их видов применяется MAC (код идентификации сообщения). В запорном устройстве этот код применяется для каждого перечня разрешений, содержащемся в чипе, который использует K_{DES}. Он также применяется для некоторых элементов данных до момента переведения устройства в рабочий режим, как поясняется ниже, а также для некоторых других элементов информации. В C-, D- и M-обеспечении код MAC используется для некоторых незашифрованных файлов данных.

Запорное устройство согласно изобретению демонстрирует очень высокий уровень безопасности. Архитектура безопасности основана на том обстоятельстве, что системный ключ, то есть C-, D- или M-ключ, способен работать с многими видами программного обеспечения. Таким образом, изменение идентификационного шифровального ключа для каждой операции аутентификации (распознавания) является непростой задачей. На фиг.4 показан обычный информационный поток иерархической системы, представленной на фиг.2. Фиг.4 дает примерное представление о сложности системы и обмене информацией между различными уровнями, то есть производителем, дистрибьютором и пользователем.

В приведенном примере пользователь имеет намерение добавить пользовательский ключ к своей системе мастер ключа (стадия 401). Таким образом, при использовании программы компоновки (стадия 402) информация, относящаяся к запрашиваемым изменениям, передается производителю, например, через модемную схему 108-308, показанную на фиг.2. В системе 300 производителя, где используется M-обеспечение 304 (стадия 403), посредством M-ключа (стадия 405) предоставляется доступ к базе данных M-обеспечения 304 (стадия 404). Затем происходит обновление базы данных M-обеспечения и соответствующая информация передается D-обеспечению (стадия 406), например, через модемную схему 308-208.

В системе 200 дистрибьютора посредством D-ключа 202 (стадия 408) предоставляется доступ к базе данных D-обеспечения 204 (стадия 407) и производится обновление содержащейся в ней информации. Изготавливается устройство, принадлежащее к данной системе мастер ключа, которое находится в защищенном режиме. Это устройство программируется при помощи D-ключа 202 и программируемого модуля 206.

В системе 100 пользователя C-обеспечение 104 получает информацию от дистрибьютора (стадия 409), поступающую, например, через модемную схему. Предоставляется доступ к базе данных C-обеспечения (стадия 410) и происходит обновление содержащейся в ней информации. Новое устройство, поставленное дистрибьютором, программируется на стадии 411 при помощи программируемого модуля 106 и C-ключа 102 (стадия 412). После переведения на стадии 413 в рабочий режим

устройства, находящегося в защищенном режиме, М-обеспечение 304 получает уведомление об осуществлении этой операции, и происходит соответствующее обновление базы данных М-обеспечения.

Читатель может представить всю сложность таких операций и необходимость в простом, но в то же время безопасном способе передачи электронной информации, а также в простом и безопасном запорном устройстве с ключом.

Защищенный режим

Для решения проблемы безопасной передачи устройства пользователю или дистрибьютору в запорном устройстве согласно изобретению предусмотрен так называемый защищенный режим. По существу это означает, что участники на различных иерархических уровнях, то есть производитель, дистрибьютор и конечный пользователь, способны полностью управлять авторизацией принадлежащих системе устройств.

Это достигается за счет использования переменного шифровального ключа, записанного в электронном коде в памяти устройства. Назначение этого ключа описывается в дальнейшем со ссылкой на фиг.5а -5е, на которых показано содержание электронного кода, хранимого в электронной памяти устройства.

На первой стадии в системе производителя изготавливается так называемая заготовка устройства, то есть устройство без механической или электронной кодировки. Таким образом, память, содержащая электронный код, пуста, смотри фиг.5а.

На следующей стадии в системе производителя в память устройства записывается кодовый элемент, характерный для данного производителя, смотри фиг.5b. Этот второй элемент, обозначенный буквой "М", определяет конкретного производителя и является уникальным для каждого производителя. Таким образом, в результате простого считывания элемента М существует возможность установления, кто изготовил ключ.

Элемент, обозначенный как "K_{DES-M}", является шифровальным ключом DES, используемым производителем в качестве кода в процессе транспортировки или хранения устройства. Как уже обсуждалось, шифровальный ключ K_{DES-M}, необходимый для функционирующих устройств, присутствует лишь в устройствах, находящихся в рабочем режиме, то есть активированных ключах и замках, работающих в системе мастер ключа 100 пользователя. Ключ K_{DES-M} генерируется программным обеспечением производителя (М-обеспечением), и никто, кроме обладающего М-обеспечением производителя, не имеет возможности создать заготовку ключа, содержащую этот ключ K_{DES-M}, уникальный для данного конкретного производителя. Следовательно, ключи защищены в процессе их хранения на уровне производителя, так как они не представляют собой никакой ценности ни для кого, кроме истинного производителя.

Когда производитель готовится отправить устройство дистрибьютору, добавляется элемент электронного кода, характерный для данного дистрибьютора, смотри фиг.5с. Этот элемент, обозначенный буквой "D", определяет конкретного дистрибьютора и уникален для каждого дистрибьютора. Он записан в ячейке, обычно занимаемой кодом MKS.

Одновременно на уровне производителя осуществляется замена шифровального ключа K_{DES-M} на K_{DES-D}, то есть на шифровальный ключ, уникальный для данного дистрибьютора. Однако чтобы обеспечить возможность такой замены, необходима процедура аутентификации между ключом, находящимся в защищенном режиме в системе производителя, и М-ключом. Эта процедура успешна лишь в случае, если шифровальные ключи такого защищенного устройства и М-ключа, то есть шифровальный ключ K_{DES-M}, идентичны. Ключ K_{DES-D} хранится в М-обеспечении и извлекается из него после успешного завершения процедуры аутентификации. После записи шифровального ключа K_{DES-M} устройство переводится в защищенный режим в системе дистрибьютора.

Когда пользователь направляет заказ либо производителю, либо дистрибьютору, инициируется процедура перевода ключа в защищенный режим в системе пользователя, как описано со ссылкой на фиг.4. Необходимая для этого информация направляется дистрибьютору от программного обеспечения производителя электронным образом, но не в открытом тексте. Направляемая информация шифруется с помощью шифровального

ключа K_{DES-D} дистрибьютора. Например, шифровальный ключ K_{DES-C} пользователя, предназначенный для устройств, находящихся в защищенном режиме в системе пользователя, отсылается в следующем формате: $eK_{DES-D}(K_{DES-C})$.

Другие важные информационные элементы, такие как MKS, GR, DID, K_{DES}, а также K_{DES-C}, если защищенный режим в системе пользователя не используется, отсылаются в закодированном таким же образом виде. Эта информация затем загружается в память ключа дистрибьютора, находящегося в защищенном режиме.

Для декодирования зашифрованной информации на уровне дистрибьютора необходима процедура аутентификации, которая осуществляется между находящимся в защищенном режиме устройством и D-ключом, в памяти которого записан шифровальный ключ K_{DES-D}. Таким образом, дешифруются кодовые элементы, при этом устройство, находящееся в защищенном режиме в системе дистрибьютора, показанное на фиг.5c, трансформируется в устройство, находящееся в защищенном режиме в системе пользователя, которое показано на фиг.5d. Одновременно в память устройства записывается истинный кодовый элемент F ролевой функции, указывающий на назначение устройства, например, пользовательский ключ.

Однако устройство, отправляемое с уровня дистрибьютора, не может еще использоваться в конечной системе мастер ключа пользователя, то есть оно не переведено в рабочий режим. При помощи C-обеспечения и C-ключа пользователь акцептует это устройство, находящееся в защищенном режиме в системе пользователя, и заменяет шифровальный ключ K_{DES-C} ключом K_{DES}, смотри фиг.5e. Только после этого возможно использование устройства в системе мастер ключа.

Производитель обычно поставляет C-ключ напрямую пользователю. Под выражением "защищенный режим в системе пользователя" подразумевается, что никакое лицо, за исключением истинного, уполномоченного пользователя, не может использовать доставленный дистрибьютором ключ, поскольку ключи запорной системы должны быть акцептованы системой при помощи C-ключа.

Та особенность, что для изменения кода другого устройства используется физический, то есть системный ключ, имеет несколько преимуществ. Во-первых, физический ключ прост в обращении. Во-вторых, он обеспечивает безопасность системы. Никто не имеет возможности перевести устройство в рабочий режим, не имея истинного системного ключа, например C-ключа.

В альтернативном варианте осуществления изобретения опускается стадия дистрибьютора. Таким образом, за осуществление операций на стадиях, описанных применительно к фиг.5a, 5b, ответственен производитель, который доставляет пользователю как устройства, так и системный ключ. Это не влияет негативным образом на безопасность системы, если устройства и системные ключи поставляются раздельно.

Альтернативно, по просьбе пользователя доставляемый ему ключ может находиться в рабочем режиме, то есть с уже записанным в память ключом K_{DES}. В результате безопасность системы несколько снижается, однако, возможность исключения одной или нескольких стадий является показателем гибкости концепции защищенного режима.

Как обсуждалось выше, информационный элемент F электронного кода - элемент ролевой функции - определяет функцию устройства. На время хранения ключа на уровне производителя или дистрибьютора этому элементу присваивается значение "0", иными словами, элемент в этот период времени не определен. При переводе устройства в рабочий режим указанному элементу присваивается заранее заданное значение, которое зависит от ролевой функции устройства, то есть является ли оно замком, пользовательским ключом, C-, D- или M-ключом. Для цели изобретения конкретный способ такой идентификации не является важной информацией.

Безопасность обмена данных

В дальнейшем обсуждаются аспекты безопасности обмена данных между программным обеспечением на различных иерархических уровнях со ссылкой на фиг.6. Каждая пара "производитель-дистрибьютор", "производитель-пользователь" и "дистрибьютор-

пользователь" обладает своим собственным шифровальным ключом для обеспечения достаточной степени безопасности. Однако те же самые шифровальные ключи используются в обоих направлениях, например, как в направлении от дистрибьютора к пользователю, так и обратно. Все необходимые шифровальные ключи хранятся в данном программном обеспечении. Шифровальные ключи поставляются вместе с программным обеспечением, а в случае необходимости их обновления производитель направляет новые шифровальные ключи, закодированные с помощью текущих коммуникационных шифровальных ключей.

Пользовательские и системные ключи

Каждый пользователь представленной на фиг.2 системы должен иметь возможность идентификации посредством используемого программного обеспечения. Для этой цели каждый пользователь имеет свое уникальное имя и принадлежит к одной из трех категорий пользователей: привилегированный пользователь, пользователь, имеющий возможность считывания и записи или только считывания. Разным категориям свойственен различный объем привилегий и ограничения на доступ, что вкратце описывается в дальнейшем.

Привилегированный пользователь способен изменять по своему усмотрению права пользователя и системные ключи. Он также может менять пароли и ПИН коды всех пользовательских и системных ключей и вносить изменения в программное обеспечение относительно авторизации С-ключа. Кроме того, такой пользователь способен осуществлять все операции, разрешенные пользователю, который имеет возможность считывания и записи. Для получения доступа к программному обеспечению привилегированному пользователю необходим специальный системный ключ, так называемый мастер ключ системы, а также требуется введение ПИН кода. Для каждого программного обеспечения существует только один мастер ключ системы.

Пользователь, имеющий возможность считывания и записи, способен изменять разрешения, записанные в таблице замка системы мастер ключа. Он также может расшифровывать или кодировать файлы, подлежащие передаче другому программному обеспечению системы. Для получения доступа к программному обеспечению такому пользователю требуется разрешенный системный ключ и введение ПИН кода.

Для получения доступа к программному обеспечению пользователю, имеющему возможность только считывания, требуется ключ, принадлежащий системе мастер ключа, а также введение пароля. Такой пользователь может только считывать конфигурацию запорной системы, то есть просматривать таблицу разрешений замка, но не имеет права вносить какие-либо изменения, относящиеся к разрешениям и т.п.

Между пользовательскими, системными ключами и различным программным обеспечением также предусмотрен протокол аутентификации. Шифровальный ключ K_{SWIDJ}, идентифицирующий программное обеспечение, содержится в нем в зашифрованном файле. Шифровальный ключ K_{SWIDJ} уникален для каждого системного ключа, и полная процедура аутентификации включает следующие стадии. Сначала между программным обеспечением и системным ключом происходит обмен открытыми идентификаторами. Затем пользователь вводит свое имя и ПИН код. После этого программное обеспечение проверяет подлинность системного ключа подобно тому, как описано ниже под заголовком "безопасность базы данных", используя вышеупомянутый уникальный шифровальный ключ, идентифицирующий программное обеспечение.

Безопасность базы данных

В дальнейшем со ссылкой на фиг.7 и 8, которые представляют процедуру шифрования базы данных, используемой в показанной на фиг.2 системе, обсуждаются некоторые аспекты безопасности базы данных. В одной и той же системе мастер ключа различные информационные элементы хранятся в разных файлах. Это означает, что в случае повреждения какого-либо шифровального ключа будет нарушена лишь часть базы данных. Примеры различных информационных элементов представлены ниже:

файл 1 - таблица разрешений замка;

файл 2 - перечень ключей и замков с их открытыми идентификаторами (PID);

...

файл i

Каждый из этих файлов зашифрован с помощью отдельного шифровального ключа, обозначенного в приведенном примере как K_{DB-F1}, K_{DB-F2},... K_{DB-Fi}, смотри фиг.7.

Пользователь, входящий в программное обеспечение, вводит свое имя и ПИН код, за исключением пользователя, имеющего возможность только считывания информации, который вводит пароль вместо имени и кода. Пользователь также применяет системный ключ j, и после этого начинается процедура аутентификации. Если эта процедура завершается успешно, в дальнейших операциях дешифровки используется шифровальный ключ K_{SYS}, записанный в системном ключе j, который применяется для получения доступа к программному обеспечению. Как показано на фиг. 7, ключ K_{SYS} используется при получении комплекта закодированных шифровальных ключей K_{DB-F1}, K_{DB-F2},... K_{DB-Fi} и т.д., используемых для шифрования файлов 1, 2, 3... базы данных. Таким образом, сами ключи K_{DB-F1}, K_{DB-F2},... K_{DB-Fi} и т.д. хранятся в зашифрованном с помощью ключа K_{SYS} виде и декодируются посредством этого шифровального ключа, хранимого в разрешенном физическом системном ключе.

Чтобы прочитать содержание файла 1, используется, например, декодированный ключ K_{DB-F1}, расшифровывающий информацию, которая содержится в базе данных. Однако с целью дальнейшего увеличения степени безопасности записанный в файл шифровальный ключ изменяется при каждом доступе к файлу. Такое изменение осуществляется посредством модификатора R_{DB-i}, показанного на фиг.7 и 8. Действительный шифровальный ключ, используемый для декодирования определенного файла, именуется $K_{DB-Fi-mod}=K_{DB-Fi}\otimes R_{DB-i}$. Каждый раз при сохранении файла i вычисляется новый модификатор R_{DB-i}, файл i шифруется с помощью нового ключа $K_{DB-Fi-mod}$, а новый модификатор R_{DB-i} записывается в незашифрованном виде.

Важно, чтобы используемые шифровальные ключи не хранились в памяти в течение излишне длительного промежутка времени. Таким образом, как показано на фиг.7, заключенные в блок A элементы данных хранятся лишь в первичной памяти и не записаны на диске. Элементы данных и файлы с информацией, заключенные в блок B, записаны на диске. Такое решение обеспечивает безопасное хранение базы данных ключей, поскольку шифровальные ключи существуют только во включенном компьютере. Если, например, компьютер с базой данных похищен, угроза появления декодированных шифровальных ключей в компьютерной системе отсутствует.

Процедура идентификации

После введения ключа в замок начинается процедура идентификации. Эта процедура основана на использовании закодированных ключей и дополнительно описана в находящейся на рассмотрении нашей заявке SE-9901643-8, на которую сделана ссылка. Однако важным является то, что два устройства, взаимодействующие друг с другом, должны иметь один и тот же шифровальный ключ для успешного осуществления какой-либо операции, например процедуры аутентификации.

Выше были описаны предпочтительные варианты осуществления изобретения. Специалисту понятно, что запорное устройство согласно изобретению может быть изменено, не выходя за определенные формулой пределы изобретения. Таким образом, хотя шифрование DES описывалось применительно к предпочтительному варианту, можно использовать также и другие способы шифрования.

Формула изобретения

1. Способ авторизации ключа или запорного устройства, включающий следующие операции: создание первого пользовательского устройства (UD1) с электронной схемой, создание первого системного устройства (SD1) с электронной схемой, используемого на первом уровне запорной системы (уровень 1) и запись первого шифровального ключа (ключ 1) в память первого пользовательского устройства, а также в память первого системного устройства, отличающийся тем, что процедуру аутентификации между первым

пользовательским устройством и первым системным устройством осуществляют с использованием первого шифровального ключа, а в случае успешного осуществления этой процедуры аутентификации при помощи первого системного устройства выполняют программную операцию, заключающуюся в замене первого шифровального ключа, записанного в памяти первого пользовательского устройства, вторым шифровальным ключом (ключ 2), причем этот второй шифровальный ключ записывают в память системных устройств (SD2) и пользовательских устройств (UD2, UD3), используемых на втором уровне упомянутой запорной системы (уровень 2), обеспечивая тем самым возможность работы первого пользовательского устройства с упомянутыми системными и пользовательскими устройствами, используемыми на втором уровне запорной системы.

2. Способ по п.1, отличающийся тем, что во время операции замены первого шифровального ключа (ключ 1), записанного в памяти первого пользовательского устройства, второй шифровальный ключ (ключ 2) обеспечивается первым системным устройством (SD1).

3. Способ по п.1, отличающийся тем, что во время операции замены первого шифровального ключа (ключ 1), записанного в памяти первого пользовательского устройства, второй шифровальный ключ (ключ 2) обеспечивается компьютером (C1).

4. Способ по п.3, отличающийся тем, что он содержит дополнительную операцию доставки второго шифровального ключа (ключ 2) компьютеру (C1), осуществляемую через компьютерную сеть, которая включает локальные компьютерные сети и телефонные сети общего пользования.

5. Способ по любому из пп.1-4, отличающийся тем, что первое системное устройство является системным ключом системы мастер ключа.

6. Способ по любому из пп.1-5, отличающийся тем, что первое пользовательское устройство является пользовательским ключом (101) системы (100) мастер-ключа.

7. Способ по любому из пп.1-5, отличающийся тем, что первое пользовательское устройство является замком (20) системы (100) мастер-ключа.

8. Способ по любому из пп.1-7, отличающийся тем, что электронные шифровальные ключи (ключ 1, ключ 2) являются читаемыми только в пределах упомянутой электронной схемы.

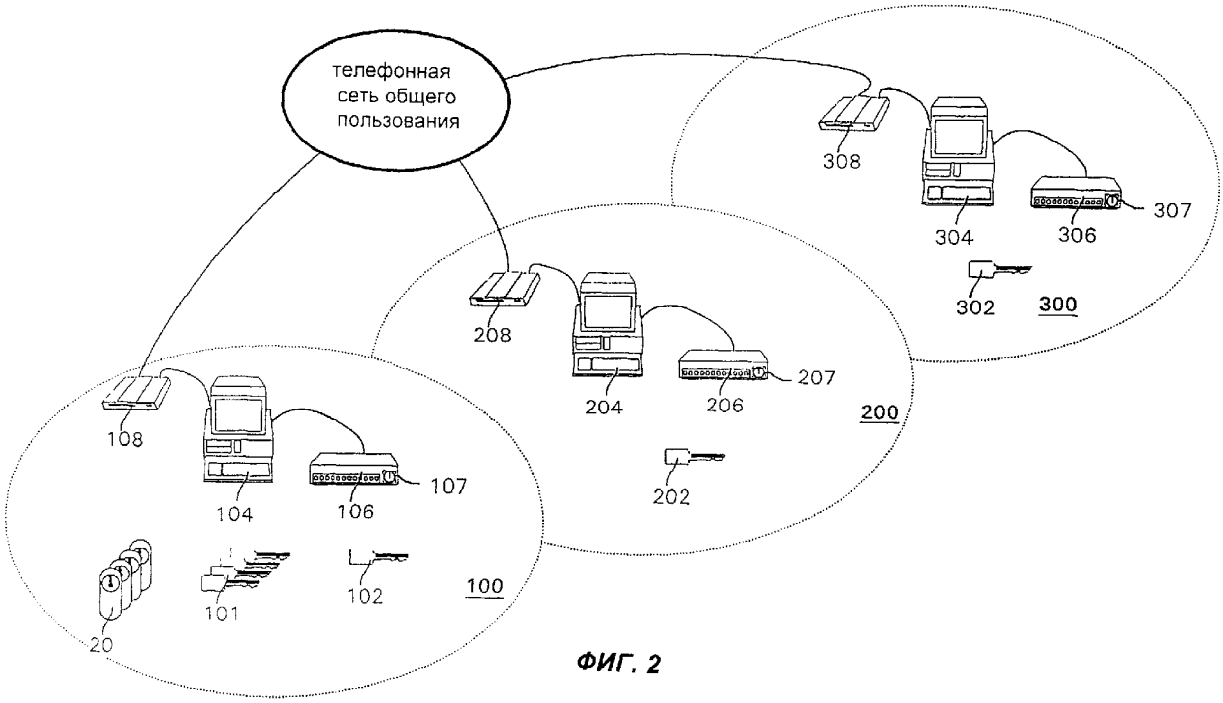
9. Электромеханическое запорное устройство с ключом, содержащее электронную схему с электронной памятью (101a), способной хранить электронный код, однозначно идентифицирующий устройство и включающий первый электронный шифровальный ключ (ключ 1), отличающееся тем, что упомянутый первый шифровальный ключ может быть заменен вторым шифровальным ключом (ключ 2) в результате подтвержденной программной операции, выполняемой при помощи первого системного устройства (SD1), которое содержит первый шифровальный ключ (ключ 1) и используется на первом уровне запорной системы (уровень 1), причем упомянутый второй шифровальный ключ хранится в памяти системных и пользовательских устройств, используемых на втором уровне запорной системы, обеспечивая тем самым возможность работы упомянутого первого пользовательского устройства с упомянутыми системными и пользовательскими устройствами, используемыми на втором уровне запорной системы.

10. Устройство по п.9, отличающееся тем, что первое системное устройство (SD1) является ключом с программируемой электронной схемой.

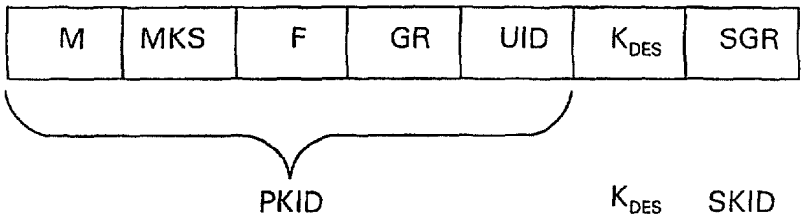
11. Устройство по любому из п.9 или 10, отличающееся тем, что электронные шифровальные ключи (ключ 1, ключ 2) являются читаемыми только в пределах упомянутой электронной схемы.

12. Запорное устройство с ключом, содержащее несколько пользовательских устройств (UD1-UD3), включающих несколько пользовательских ключей с электронной схемой, которая содержит электронную память, способную хранить переменный электронный шифровальный ключ, и несколько замков с электронной схемой, которая содержит электронную память, способную хранить переменный электронный шифровальный ключ, причем замок и пользовательский ключ способны совместно работать, только если в их

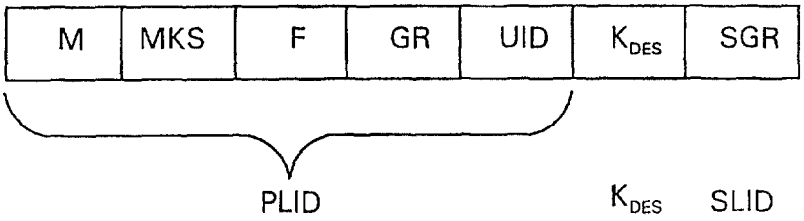
память записаны идентичные шифровальные ключи, отличающееся тем, что оно включает по меньшей мере одно системное устройство (SD1-SD3), имеющее электронную схему с электронной памятью, способной хранить постоянный электронный шифровальный ключ, а компьютерное программное обеспечение способно изменять упомянутый переменный электронный шифровальный ключ пользовательского устройства таким образом, что в случае успешной процедуры аутентификации, осуществляемой между замком или пользовательским ключом с записанным переменным электронным шифровальным ключом и системным устройством с записанным шифровальным ключом, идентичным упомянутому шифровальному ключу замка или пользовательского ключа, первый шифровальный ключ заменяется вторым шифровальным ключом.



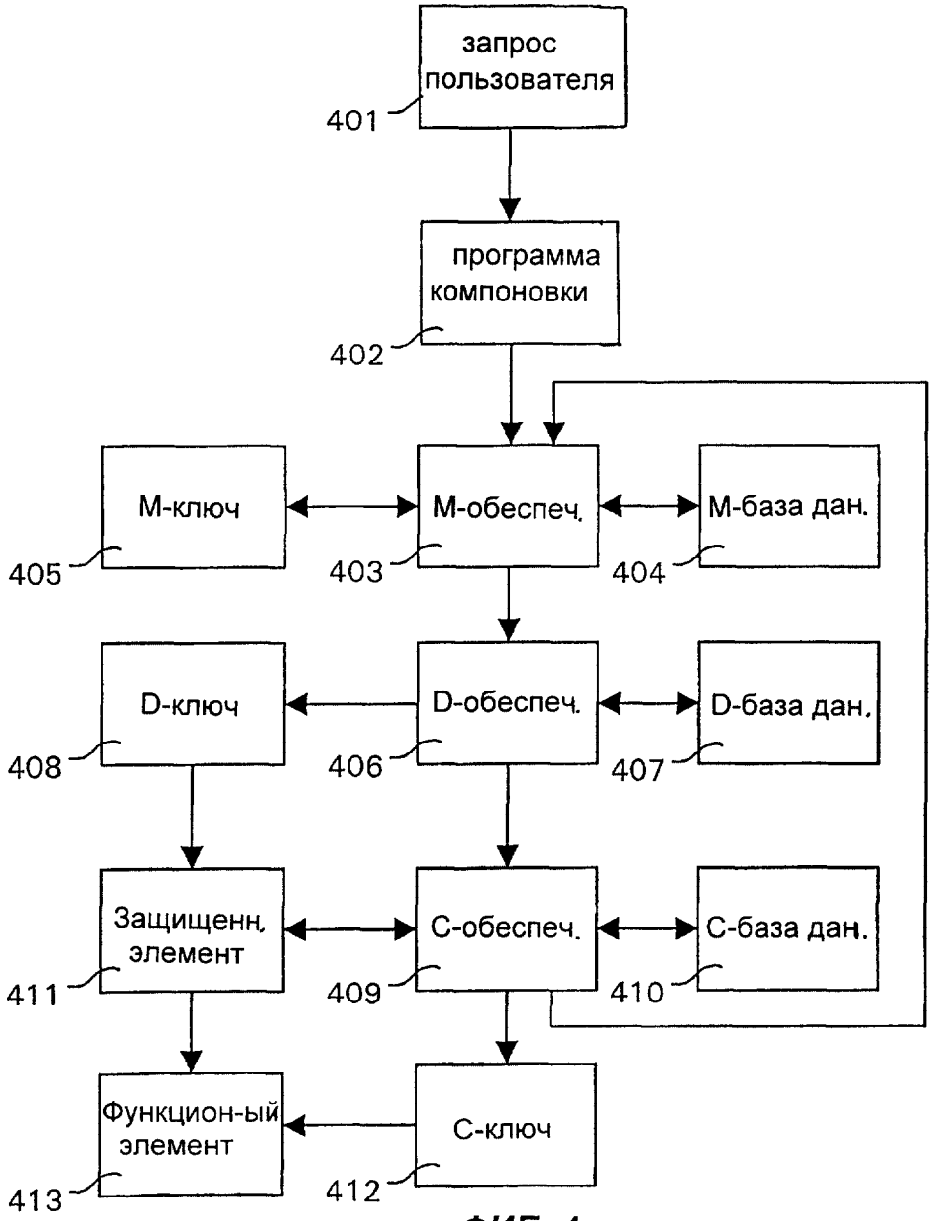
ФИГ. 2



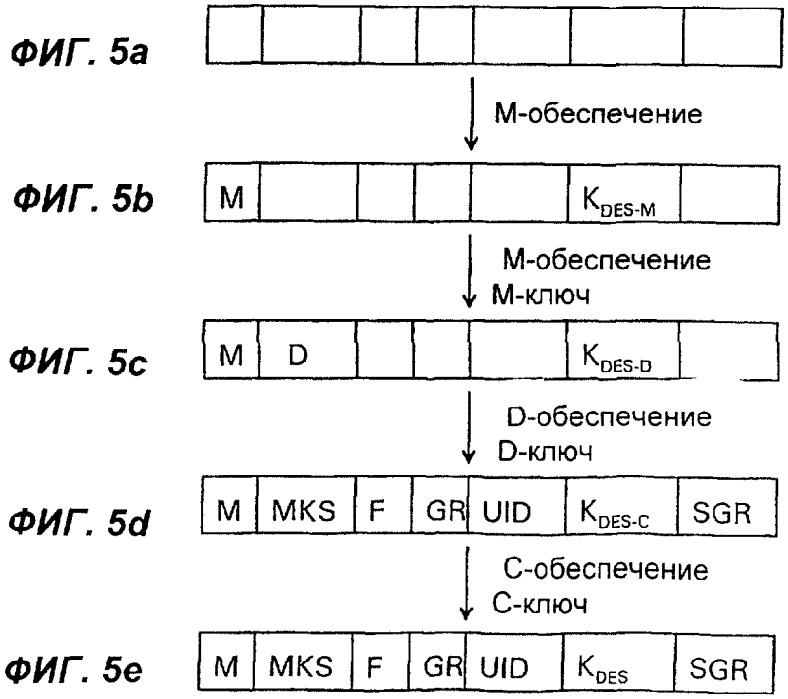
ФИГ.3a



ФИГ. 3b


запрос пользователя
401
программа компоновки
402
М-ключ
405
М-обеспеч.
403
М-база дан.
404
D-ключ
408
D-обеспеч.
406
D-база дан.
407
Защищенн. элемент
411
С-обеспеч.
409
С-база дан.
410
Функцион-ый элемент
413
С-ключ
412

ФИГ. 4



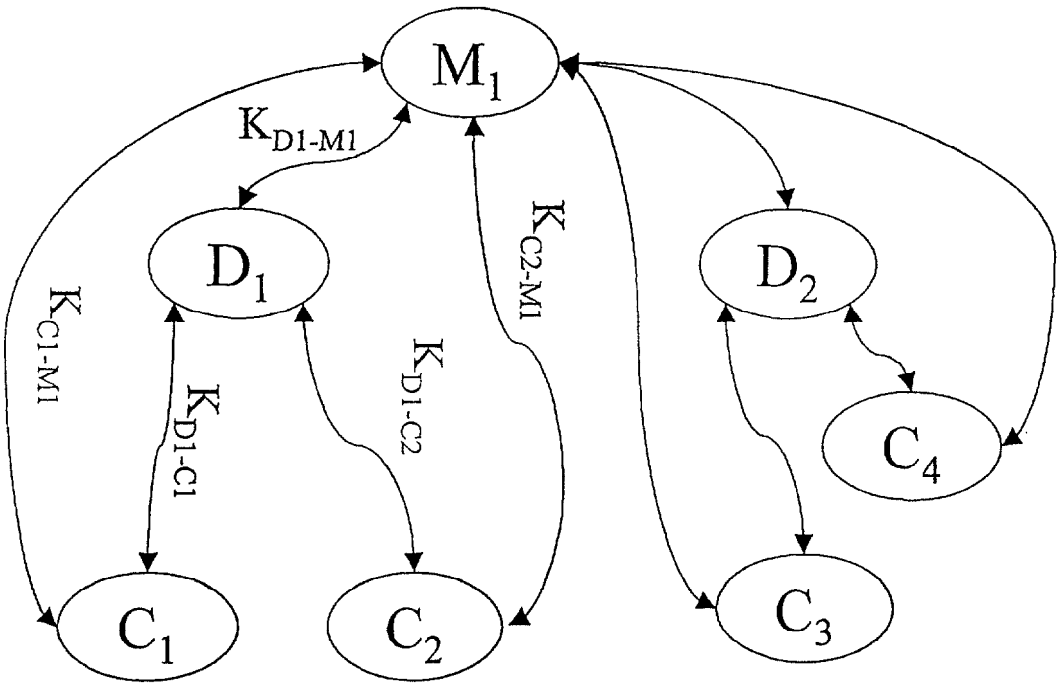
ФИГ. 5a

ФИГ. 5b

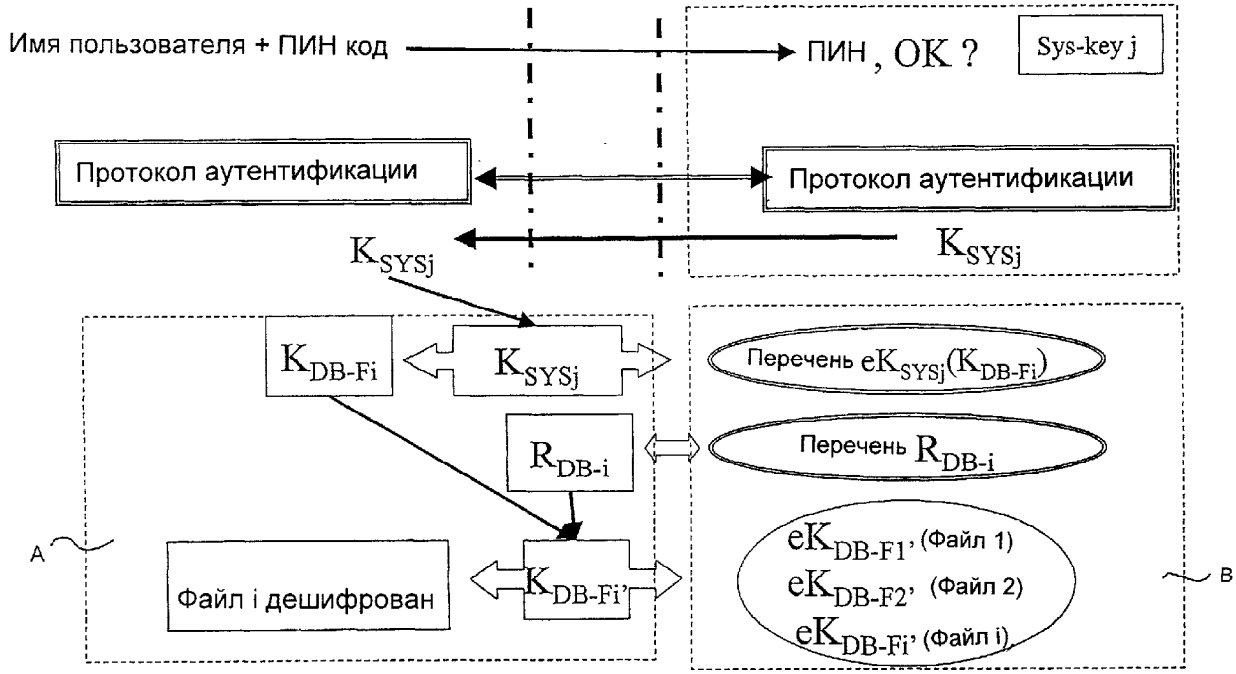
ФИГ. 5c

ФИГ. 5d

ФИГ. 5e



ФИГ. 6



ФИГ. 7

	DB- файл 1	DB- файл 2	...	DB- файл I
Sys-key1	$eeK_{SYS1}(K_{DB-F1})$	$eeK_{SYS1}(K_{DB-F2})$	...	$eeK_{SYS1}(K_{DB-Fi})$
Sys-key2	$eeK_{SYS2}(K_{DB-F1})$	$eeK_{SYS2}(K_{DB-F2})$	...	$eeK_{SYS2}(K_{DB-Fi})$
...	...	...	...	...
Sys-keyj	$eeK_{SYSj}(K_{DB-F1})$	$eeK_{SYSj}(K_{DB-F2})$	...	$eeK_{SYSj}(K_{DB-Fi})$

DB-файл 1	DB-файл 2	...	DB-файл i
R_{DB-F1}	R_{DB-F2}	...	R_{DB-Fi}

ФИГ. 8