(19) Евразийское патентное ведомство

(11) 036720 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2020.12.11

(21) Номер заявки
201991163

(22) Дата подачи заявки
2016.11.18

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

(54) СПОСОБ И СИСТЕМА ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО КОПИРОВАНИЯ (АНТИКЛОНИРОВАНИЯ)

(43) **2019.11.29**
(86) **PCT/IB2016/056960**
(87) **WO 2018/091946 2018.05.24**

(71)(73) Заявитель и патентовладелец:
ПЕРМАНЕНТ ПРАЙВЕСИ ЛТД. (VG)

(72) Изобретатель:
Юэнь Пак Кай (HK)

(74) Представитель:
Медведев В.Н. (RU)

(56) US-A1-2008063210
US-A1-2013054967
US-B1-6986044
LI JINGWEI ET AL.: "Rekeying for Encrypted Deduplication Storage", 2016 46TH ANNUAL IEEE/IFIP INTERNATIONAL CONFERENCE ON DEPENDABLE SYSTEMS AND NETWORKS (DSN), IEEE, 28 June 2016 (2016-06-28), pages 618-629, XP032973596, DOI: 10.1109/DSN.2016.62 [retrieved on 2016-09-29] the whole document

(57) Объект защищается от несанкционированного копирования за счет обеспечения генератора ключей для объекта, создания первого ключа, второго ключа и замка для ключей, сохранения первого ключа в объекте, сохранения второго ключа в базе данных, отдельной от объекта, считывания первого и второго ключей, открывания замка первым и вторым ключами, создания третьего и четвертого ключей и нового замка для объекта, объявления недействительными первого и второго ключей, замены первого ключа в объекте третьим ключом и замены второго ключа в базе данных четвертым ключом.

036720 B1

036720 B1

Область техники, к которой относится изобретение

Защита антиклонирования.

Описание уровня техники

Пропуска можно скопировать, даже если они зашифрованы. Такими пропусками могут быть паспорта и удостоверения личности, банкоматные карты или кредитные карты. Аппаратные устройства, например телевизионные приставки, и программное обеспечение, включающее в себя игры, программное обеспечение автоматизации, операционные системы или прикладные программы также могут быть скопированы, даже если они зашифрованы.

Также может быть трудно автоматически обнаруживать несанкционированную копию, например, пропуска и/или объявлять ее недействительной, или действия, в которых используется несанкционированная копия.

Сущность изобретения

В одном аспекте объект защищается от несанкционированного копирования за счет обеспечения замка для объекта, создания первого и второго ключей для замка или создания одного ключа и затем разделения ключа в первый и второй ключи, сохранения первого ключа в объекте, сохранения второго ключа в базе данных, отдельной от объекта, считывания первого и второго ключей, объединения или комбинирования первого и второго ключей друг с другом, открывания замка первым и вторым ключами, создания ключа и его разделения на третий и четвертый ключи, с использованием третьего и четвертого ключей для повторного шифрования информации счета для получения нового результата шифрования, причем новый результат шифрования совместно с третьим и четвертым ключами образует новый замок, причем новый замок эффективно объявляет недействительными первый и второй ключи, замены первого ключа в объекте третьим ключом и замены второго ключа в базе данных четвертым ключом.

В нескольких аспектах объектом является паспорт, банковская карта, электронный проездной билет, защищенный электронный документ, интеллектуальная телевизионная приставка, кабельная телевизионная приставка, автомобиль, деталь автомобиля, лицензия на программное обеспечение или цифровые информационные материалы.

В нескольких аспектах банковской картой является кредитная карта, банкоматная карта, дебетовая карта, депозитная карта или электронная платежная карта.

В нескольких аспектах электронным проездным билетом является карта Ойстер или карта Октопус.

В нескольких аспектах лицензией на программное обеспечение является лицензия на программу, лицензия на программное обеспечение автоматизации, лицензия на операционную систему или приложение для мобильного телефона.

В нескольких аспектах цифровыми информационными материалами являются игра, музыка, фильм, видеоклип, телепередача или телесериал в прямом эфире.

В дополнительном аспекте первый и второй ключи создаются путем шифрования информации счета и разделения зашифрованной информации счета на первый и второй ключи, при условии, что каждое шифрование отличается.

В дополнительном аспекте информация счета является информацией счета пользователя объекта.

В другом аспекте система защищает объект от несанкционированного копирования, система включает в себя память и процессор, подключенный к памяти, причем процессор выполнен с возможностью обеспечения первого и второго ключей или одного ключа, разделенного на первый и второй ключи, использования первого и второго ключей для шифрования информации счета для генерации нового замка, сохранения первого ключа в объекте, сохранения второго ключа в базе данных, отдельной от объекта, считывания первого и второго ключей, открывания замка первым и вторым ключами, создания третьего и четвертого ключей и генерирования нового замка, причем новый замок объявляет недействительными первый и второй ключи, замены первого ключа в объекте третьим ключом и замены второго ключа в базе данных четвертым ключом.

В еще одном аспекте устройство защищает объект от несанкционированного копирования, устройство включает в себя шифровальную машину, устройство чтения ключей объекта и устройство чтения ключей эмитента, подключенные к шифровальной машине и выполненные с возможностью считывания ключа объекта и ключа эмитента соответственно, блок удостоверения ключей, подключенный к шифровальной машине и выполненный с возможностью шифрования или дешифрования ключа объекта и ключа эмитента для удостоверения ключа объекта и ключа эмитента, генератор ключей, подключенный к шифровальной машине и выполненный с возможностью шифрования или дешифрования информации счета для генерации нового и другого кода шифрования и разделения кода шифрования на ключ объекта и ключ эмитента; и блок обновления ключей, подключенный к генератору ключей и выполненный с возможностью обновления ключа объекта и ключа эмитента путем замены ключа объекта и ключа эмитента новым ключом объекта и новым ключом эмитента, соответственно, и отказа от ключа объекта и ключа эмитента.

В еще одном аспекте объект защищается от несанкционированного копирования за счет обеспечения генератора ключей для объекта, создания первого и второго ключей и замка для первого и второго ключей, сохранения первого ключа в объекте, сохранения второго ключа и временного ключа в базе дан-

ных, отдельной от объекта, считывания первого и второго ключей, объединения первого и второго ключей, открывания замка посредством совпадения дешифрования объединенных первого и второго ключей с использованием сохраненного временного ключа, создания нового временного ключа, третьего и четвертого ключей и нового замка, объявления недействительными первого и второго ключей с помощью нового замка, замены первого ключа в объекте третьим ключом и замены обоих временного ключа и второго ключа в базе данных новым временным ключом и четвертым ключом.

В еще одном аспекте система защищает объект от несанкционированного копирования, система включает в себя память и процессор, подключенный к памяти, причем процессор выполнен с возможностью обеспечения генератора ключей для объекта, создания первого и второго ключей и замка для первого и второго ключей, сохранения первого ключа в объекте, сохранения второго ключа и временного ключа в базе данных, отдельной от объекта, считывания первого и второго ключей, объединения первого и второго ключей, открывания замка посредством совпадения дешифрования объединенных первого и второго ключей с использованием сохраненного временного ключа, создания нового временного ключа, третьего и четвертого ключей и нового замка, объявления недействительными первого и второго ключей с помощью нового замка, замены первого ключа в объекте третьим ключом и замены обоих временного ключа и второго ключа в базе данных новым временным ключом и четвертым ключом.

В еще одном аспекте устройство защищает объект от несанкционированного копирования, устройство включает в себя шифровальную машину, устройство чтения ключей объекта и устройство чтения ключей эмитента, подключенные к шифровальной машине и выполненные с возможностью считывания ключа объекта и ключа эмитента соответственно, блок удостоверения ключей, подключенный к шифровальной машине и выполненный с возможностью шифрования или дешифрования ключа объекта и ключа эмитента для удостоверения ключа объекта и ключа эмитента, генератор ключей, подключенный к шифровальной машине и выполненный с возможностью генерации временного ключа и шифрования или дешифрования ключа объекта и ключа эмитента для генерации кода шифрования и его разделения на ключ объекта и ключ эмитента, и блок обновления ключей, подключенный к генератору ключей и выполненный с возможностью обновления ключа объекта и ключа эмитента путем замены ключа объекта и ключа эмитента новым ключом объекта и новым ключом эмитента, соответственно, и отказа от ключа объекта и ключа эмитента.

Вышеописанные и другие признаки и преимущества настоящего изобретения, а также структура и принцип работы различных вариантов осуществления настоящего изобретения подробно описаны ниже со ссылкой на прилагаемые чертежи.

Краткое описание чертежей

Прилагаемые чертежи, которые включены сюда и образуют часть описания изобретения, иллюстрируют различные варианты осуществления настоящего изобретения и совместно с описанием дополнительно служат для объяснения принципов изобретения, позволяют специалисту в данной области техники делать и использовать изобретение. В чертежах сходные ссылочные позиции указывают идентичные или функционально аналогичные элементы. Более полное понимание изобретения и многих из его сопутствующих преимуществ достигается при обращении к нижеследующему подробному описанию, рассматриваемому со ссылкой на прилагаемые чертежи, в которых

фиг. 1 - схема системы для защиты объекта от несанкционированного копирования согласно варианту осуществления;

фиг. 2 - блок-схема операций способа защиты объекта от несанкционированного копирования согласно варианту осуществления;

фиг. 3 - схема системы для защиты объекта от несанкционированного копирования согласно варианту осуществления;

фиг. 4 - оборудование для использования согласно варианту осуществления.

Подробное описание предпочтительных вариантов осуществления

На фиг. 1 показана схема системы 100 для защиты объекта от несанкционированного копирования согласно варианту осуществления.

В основу изобретения легла система депозитарных ячеек, используемая в банках. При абонировании депозитарной ячейки в банке банк обеспечивает два ключа. Один ключ хранится у клиента, и другой ключ, именуемый "дежурным ключом", хранится в банке. "Замок" депозитарной ячейки можно открыть, только воспользовавшись двумя ключами вместе.

Вопрос: не будет ли безопаснее, если банк будет обеспечивать два новых ключа и менять замок после каждого посещения депозитарной ячейки?

Ответ: для депозитарной ячейки не будет ни практично, ни полезно, если банк будет обеспечивать два новых ключа и менять замок после каждого посещения клиентом.

Однако электронная версия этой идеи обеспечивает как безопасность, так и практичность (простоту использования).

Рассмотрим защищенные объекты 10, например "паспорта", "удостоверения личности" и "кредитные карты", например, показанные на фиг. 1. Для каждого защищенного объекта 10 эмитент 20 (банк, паспортный стол и т.д.) будет создавать два ключа 30, 40 (пароли). Один будет храниться внутри объекта

10 (например, на его магнитной полоске) и другой будет храниться в базе данных 50 эмитента.

Для каждого защищенного объекта 10, например паспорта, удостоверения личности и кредитной карты, "замок" 60 будет сконструирован с использованием шифрования данных, пригодного для защиты данного объекта 10. Замок 60 шифрования будет служить невидимым наружным слоем помимо любой существующей защиты объекта 10 (например, ПИН).

В случае кредитной карты, например, при ее вставке в устройство чтения карт будет считываться два ключа 30, 40 в замок "шифрования" эмитента. Когда два ключа 30, 40 являются правильными, они распознаются замком "шифрования", кредитная карта рассматривается как подлинная, и замок открывается. Держатель карты не видит этого, и это происходит так быстро, что не замедляет и не влияет на использование карты.

Все остальные сопутствующие действия, например считывание ПИН и финансовая транзакция, могут осуществляться как обычно.

Окончательный и наиболее важный этап: после завершении финансовой транзакции и до возврата кредитной карты устройство чтения карт (т.е. эмитент) создает два новых ключа и новый замок. Один ключ хранится в данном объекте, и другой ключ - в базе данных эмитента.

Предположим, несколько "паспортов", "удостоверений личности" и "кредитных карт" скопировано в преступных целях. Каждый из этих скопированных объектов будет иметь один и тот же ключ 30, 40 как конкретный подлинный объект, который был скопирован или клонирован.

Теперь при использовании подлинной карты или объекта замок и ключи внутри как подлинной карты, так и базы данных эмитента изменятся. В результате все незаконные копии объекта станут бесполезными, поскольку старый ключ внутри скопированного объекта не может совпадать с новым ключом в базе данных эмитента. Никакая копия или клон не сможет открыть новый замок шифрования.

В этой ситуации все несанкционированные копии объектов будут автоматически заблокированы. Пользователям, как и эмитенту, ничего не нужно делать для блокировки копий.

Обнаружение несанкционированных копий и/или обнаружение использования незаконных копий является проблемой безопасности для многих организаций, например банков. Предположим, несколько "паспортов", "удостоверений личности" и "кредитных карт" скопировано и используется до того, как был использован подлинный объект. В этом случае несанкционированный скопированный объект будет использоваться успешно.

Однако, когда подлинный объект используется после незаконной копии, подлинный объект не справится с замком шифрования, поскольку замок уже изменился. В этом случае известно, что подлинный объект был скопирован, и незаконно использовалась его копия. Теперь владелец подлинного объекта контактирует с эмитентом, и затем новые ключи и новый замок повторно устанавливаются в подлинный объект для блокировки всех незаконных копий объекта.

Изобретение особенно полезно для обнаружения незаконных копий паспорта и удостоверения личности и устранения такого рода подделок личности. Не имеет значения, сколько паспортов и удостоверений личности скопировано, можно использовать одну и только одну. Все остальные копии автоматически блокируются. Когда от эмитента используется или выявляется подлинная, все незаконные копии будут открываться и могут захватываться эмитентом.

Раньше было довольно трудно сообщать банку о наличии незаконной копии денежной карты или кредитной карты. Согласно настоящему изобретению, когда используется несанкционированная копия денежной карты (или кредитной карты), изменяется как ключ в скопированной карте, так и ключ в базе данных эмитента.

Однако ключ внутри подлинной карты, который является предыдущим ключом, не будет открывать замок шифрования системы. Это может использоваться как доказательство банку, что в обращении находится незаконная копия карты. Эмитент сможет проверять, что подлинная карта все еще имеет свой предыдущий ключ и поэтому не использовалась.

Телевизионные приставки и программное обеспечение, например игры, лицензии на программное обеспечение автоматизации, операционные системы и прикладные программы, все могут быть защищены вдоль аналогичных линий.

Для снижения кражи личности и обеспечения душевного спокойствия защищенные объекты, например денежные карты и кредитные карты, следует использовать по возможности регулярно. Во многих случаях просто проверка остатка даст необходимый эффект, поскольку это будет инициировать автоматическое создание новых ключей.

Кража личности будет значительно снижаться, если люди ежедневно проверяют свои защищенные объекты. Устройство чтения карт USB онлайн может быть разработано даже таким образом, чтобы люди могли проверять свои карты дома на своих ПК.

Раньше было трудно идентифицировать оригинал электронного (или электронно передаваемого) документа, например электронного контракта, законного документа и т.д.

Изобретение также можно использовать для идентификации исходного электронного документа, помещая ключ внутрь электронного документа, и рассматривать электронный документ в качестве защищенного объекта. Все одинаковые документы с различными ключами можно рассматривать как ко-

пию оригинала.

Процесс проверки исходного электронного документа может осуществляться программой.

Программа считывает ключ из документа и подключается к сайту эмитента в интернете, например, для второго ключа. При наличии двух ключей электронный документ можно проверять как исходный путем открывания замка.

В ряде случаев также можно размещать путем шифрования, что успешно считывать можно только исходный электронный документ.

Защита несколько копий защищенного объекта не является проблемой. Предположим, нужно защитить три банкоматных карты (например, card1, card2, card3) для одного и того же счета. Все, что нужно сделать, это сгенерировать три пары ключей, связанных с тремя банкоматными картами.

Например, первая пара ключей используется для защиты card1. Один ключ хранится внутри card1, и другой ключ хранится внутри базы данных счета со ссылкой на card1.

В ситуации этого изобретения широко используется, например, операционными системами, например Microsoft Windows, Apple Mac и интернетом. Большинство электронных и цифровых объектов, включающих в себя программное обеспечение, электронные документы и игры, могут быть защищены в глобальном масштабе. Можно до некоторой степени добиться глобальной дисциплины для несанкционированного копирования.

Основные сущности изобретения

Два ключа (или один ключ, разделенный на две части): один ключ хранится в защищенном объекте, и другой хранится в базе данных эмитента.

Замок шифрования: замок или шифрование может задаваться пользователем в зависимости от конкретного применения. Это может быть одностороннее шифрование (без дешифрования) или двустороннее шифрование (доступны как шифрование, так и дешифрование) или их комбинация.

Процесс проверки.

Процесс проверки можно рассматривать как открывание замка шифрования и может задаваться пользователем в зависимости от используемого шифрования. Например, замок рассматривается как открытый, когда одни и те же результаты шифрования достигаются с помощью двух ключей. В ряде случаев замок рассматривается как открытый, когда достигаются те же результаты дешифрования. Иногда может использоваться их комбинация.

Генератор ключей.

Генератор ключей это механизм (аппаратный или программный), который может генерировать два новых ключа и генерировать новый замок путем шифрования информации счета при каждом использовании или выборе ключей, связанных с шифрованием.

Существует несколько путей осуществления изобретения. В качестве еще одного очень простого примера осуществления рассмотрим ситуацию банковской карты.

Два ключа и замок могут генерироваться следующим образом.

Генератор ключей может генерировать временной ключ или пароль и продолжать изменять пароль каждый раз для шифрования следующей информации счета пользователя в базе данных банка с последующим сохранением временного ключа:

John Smith, 04929 1234 5678, XXBank и результатом шифрования может быть

01 69 f3 2b 10 88 40 ca 18 22 48 90 1d d4 1a c8 ca d9 df fa d3 68 8c 6f 1b bb fb 51 fc fc 1a e7 43 5e 1d d9 86 fd ca 5a d2 1c bf 6d c7 26 9c 56 78 8b bd af 35 63 bf 92

Эти результаты шифрования могут делиться на две части (т.е. как два ключа)

Key1=01 69 f3 2b 10 88 40 ca 18 22 48 90 1d d4 1a c8 ca d9 df fa d3 68 8c 6f 1b

Key2=bb fb 51 fc fc 1a e7 43 5e 1d d9 86 fd ca 5a d2 1c bf 6d c7 26 9c 56 78 8b bd af 35 63 bf 92

Затем Key1 будет сохраняться в банковскую карту, и оба, временной ключ и Key2, будут сохраняться в базе данных банка.

Способом подтверждения для этого простого примера будет простое дешифрование объединенных двух ключей сохраненным временным ключом для восстановления информации о пользователе и затем повторная активация генератора ключей для генерации новых ключей и нового временного ключа. В этом случае первый и второй ключи действуют как замок. Временным ключом может быть любой предмет, число или строка, связанный/ое/ая с временем, или просто любая произвольная строка, которая отличается каждый раз, когда генерируется.

На фиг. 2 показана блок-схема операций способа 200 для защиты объекта от несанкционированного копирования согласно варианту осуществления. Объектом может быть паспорт, банковская карта, электронный проездной билет, защищенный электронный документ, интеллектуальная телевизионная приставка, кабельная телевизионная приставка, автомобиль, деталь автомобиля, лицензия на программное обеспечение или цифровые информационные материалы. Банковской картой может быть кредитная карта, банкоматная карта, дебетовая карта, депозитная карта или электронная платежная карта. Электронным проездным билетом может быть карта Ойстер или карта Октопус. Лицензией на программное обеспечение может быть лицензия на программу, лицензия на программное обеспечение автоматизации, лицензия на операционную систему или приложение для мобильного телефона. Цифровыми информацион-

ными материалами может быть игра, музыка, фильм, видеоклип, телепередача или телесериал в прямом эфире.

В первой операции 202 обеспечивается генератор ключей для объекта. Во второй операции 204 для объекта создаются временной ключ и первый и второй ключи в качестве замка. Первый и второй ключи можно создавать путем шифрования информации счета с использованием временного ключа и разделения зашифрованной информации счета на первый и второй ключи. Информацией счета может быть информация счета пользователя объекта.

В третьей операции 206 первый ключ сохраняется в объекте. В четвертой операции 208 оба временной ключ и второй ключ сохраняются в базе данных, отдельной от объекта. В пятой операции 210 первый и второй ключи считываются. В шестой операции 212 первый и второй ключи объединяются. В седьмой операции 214 замок открывается посредством совпадения дешифрования объединенных первого и второго ключей с использованием сохраненного временного ключа. В восьмой операции 216 создаются новый временной ключ, третий и четвертый ключи, образующие новый замок. В девятой операции 218 первый и второй ключи объявляются недействительными новым замком. В десятой операции 220 первый ключ в объекте заменяется третьим ключом. В одиннадцатой операции 222 оба, временной ключ и второй ключ, в базе данных заменяются новым временным ключом и четвертым ключом.

На фиг. 3 показана схема системы 300 для защиты объекта от несанкционированного копирования согласно варианту осуществления. Система включает в себя память 302 и процессор 304, подключенный к памяти 302. Процессор 304 выполнен с возможностью обеспечивать генератор ключей для объекта, создавать первый и второй ключи и замок с использованием шифрования, сохранять первый ключ в объекте, сохранять второй ключ в базе данных, отдельной от объекта, считывать первый и второй ключи, открывать замок первым и вторым ключами, создавать третий и четвертый ключи и новый замок, объявлять недействительными первый и второй ключи с помощью нового замка, заменять первый ключ в объекте третьим ключом и заменять второй ключ в базе данных четвертым ключом.

На фиг. 4 показана схема устройства 400 для защиты объекта от несанкционированного копирования. Устройство 400 включает в себя шифровальную машину 402. Устройство 404 чтения ключей объекта и устройство 406 чтения ключей эмитента подключены к шифровальной машине 402 для считывания ключа объекта и ключа эмитента. Шифровальная машина 402 выполнена с возможностью считывания ключа объекта и ключа эмитента и их дешифрования. Блок 408 удостоверения ключей подключен к шифровальной машине 402 и выполнен с возможностью шифрования или дешифрования ключа объекта и ключа эмитента для удостоверения ключа объекта и ключа эмитента.

Генератор 410 ключей подключен к шифровальной машине 402 и выполнен с возможностью генерации временного ключа и шифрования информации счета пользователя для генерации кода шифрования и его разделения на ключ объекта и ключ эмитента. Блок 412 обновления ключей подключен к генератору 410 ключей и выполнен с возможностью обновления ключа объекта и ключа эмитента путем замены ключа объекта и ключа эмитента новым ключом объекта и новым ключом эмитента и новым временным ключом, соответственно, и отказа от ключа объекта и ключа эмитента.

Варианты осуществления могут быть реализованы в вычислительном оборудовании (вычислительном устройстве) и/или программном обеспечении, например (в неограничительном примере) любом компьютере, который может хранить, извлекать, обрабатывать и/или выводить данные и/или осуществлять связь с другими компьютерами. Полученные результаты могут отображаться на дисплее вычислительного оборудования. Программа/программное обеспечение, реализующая/ее варианты осуществления, может записываться на компьютерно-считываемых носителях, содержащих компьютерно-считываемые носители записи. Программа/программное обеспечение, реализующая/ее варианты осуществления, также может передаваться в средах связи. Примеры компьютерно-считываемых носителей записи включают в себя магнитное записывающее устройство, оптический диск, магнитооптический диск и/или полупроводниковую память (например, RAM, ROM и т.д.). Примеры магнитного записывающего устройства включают в себя жесткий диск (HDD), гибкий диск (FD) и магнитную ленту (MT). Примеры оптического диска включают в себя DVD (цифровой универсальный диск), DVD-RAM, CD-ROM (компакт-диск с возможностью только чтения) и CD-R (записывающий)/RW. Пример сред связи включает в себя сигнал несущей волны.

Дополнительно согласно аспекту вариантов осуществления можно предусмотреть любые комбинации описанных признаков, функций и/или операций.

Выше описаны принципы, варианты осуществления и режимы работы настоящего изобретения. Однако не следует считать, что изобретение ограничивается вышеописанными конкретными вариантами осуществления, поскольку их следует рассматривать как иллюстративные и не ограничительные. Очевидно, что специалисты в данной области техники могут предложить разновидности этих вариантов осуществления, не выходя за рамки объема настоящего изобретения.

Хотя выше описан предпочтительный вариант осуществления настоящего изобретения, следует понимать, что он представлен исключительно в порядке примера, но не ограничения. Таким образом, охват и объем настоящего изобретения не подлежат ограничению вышеописанным иллюстративным вариантом осуществления.

Очевидно, в свете вышеизложенных принципов возможны многочисленные модификации и вариации настоящего изобретения. Поэтому следует понимать, что изобретение можно осуществлять на практике иначе, чем конкретно описано здесь.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Способ (200) защиты объекта (10) от несанкционированного копирования, содержащий этапы, на которых

обеспечивают генератор (410) ключей для объекта (10);

создают первый и второй ключи (30, 40) и замок (60) для первого и второго ключей (30, 40);

сохраняют первый ключ (30) в объекте (10);

создают временной ключ для замка (60);

сохраняют второй ключ (40) и временной ключ в базе (50) данных, отдельной от объекта (10);

считывают первый и второй ключи (30, 40);

объединяют первый и второй ключи (30, 40);

открывают замок (60) посредством совпадения дешифрования объединенных первого и второго ключей (30, 40) с использованием сохраненного временного ключа;

создают новый временной ключ, третий и четвертый ключи и новый замок (60);

объявляют недействительными первый и второй ключи (30, 40) с помощью нового замка (60);

заменяют первый ключ (30) в объекте (10) третьим ключом и

заменяют оба, временной ключ и второй ключ (40), в базе (50) данных новым временным ключом и четвертым ключом,

при этом первый ключ (30) заменяют в объекте (10) третьим ключом, а временной ключ и второй ключ (40) заменяют в базе (50) данных новым временным ключом и четвертым ключом после каждого использования объекта (10).

2. Способ (200) по п.1, в котором объект (10) выбран из группы, состоящей из

паспорта,

банковской карты,

электронного проездного билета,

защищенного электронного документа,

интеллектуальной телевизионной приставки,

кабельной телевизионной приставки,

автомобиля,

детали автомобиля,

лицензии на программное обеспечение и

цифровых информационных материалов.

3. Способ (200) по п.2, в котором банковская карта выбрана из группы, состоящей из кредитной карты, банкоматной карты, дебетовой карты, депозитной карты и электронной платежной карты.

4. Способ (200) по п.2, в котором электронный проездной билет выбран из группы, состоящей из карты Ойстер и карты Октопус.

5. Способ (200) по п.2, в котором лицензия на программное обеспечение выбрана из группы, состоящей из лицензии на программу, лицензии на программное обеспечение автоматизации, лицензии на операционную систему и приложения для мобильного телефона.

6. Способ (200) по п.2, в котором цифровые информационные материалы выбраны из группы, состоящей из

игры,

музыки,

фильма,

видеоклипа,

телепередачи и

телесериала в прямом эфире.

7. Способ (200) по п.1, в котором первый и второй ключи (30, 40) создаются путем шифрования информации счета связанным с временем паролем или временным ключом и разделения зашифрованной информации счета на первый и второй ключи (30, 40).

8. Способ по п.7, в котором информация счета является информацией счета пользователя объекта (10).

9. Система (100, 300) для защиты объекта (10) от несанкционированного копирования, содержащая

память (302) и

процессор (304), подключенный к памяти (302) и выполненный с возможностью

обеспечивать генератор (410) ключей для объекта (10);

создавать первый и второй ключи (30, 40) и замок (60) для первого и второго ключей (30, 40);

сохранять первый ключ (30) в объекте (10);

создавать временной ключ для замка (60);

сохранять второй ключ (40) и временной ключ в базе (50) данных, отдельной от объекта (10);

считывать первый и второй ключи (30, 40);

объединять первый и второй ключи (30, 40);

открывать замок (60) посредством совпадения дешифрования объединенных первого и второго ключей (30, 40) с использованием сохраненного временного ключа;

создавать новый временной ключ, третий и четвертый ключи и новый замок (60);

объявлять недействительными первый и второй ключи (30, 40) с помощью нового замка (60);

заменять первый ключ (30) в объекте (10) третьим ключом и

заменять оба, временной ключ и второй ключ (40), в базе (50) данных новым временным ключом и четвертым ключом,

при этом первый ключ (30) заменяется в объекте (10) третьим ключом, а временной ключ и второй ключ (40) заменяются в базе (50) данных новым временным ключом и четвертым ключом после каждого использования объекта (10).

10. Система (100, 300) по п.9, в которой объект (10) выбран из группы, состоящей из

паспорта,

банковской карты,

электронного проездного билета,

защищенного электронного документа,

интеллектуальной телевизионной приставки,

кабельной телевизионной приставки,

автомобиля,

детали автомобиля,

лицензии на программное обеспечение и

цифровых информационных материалов.

11. Система (100, 300) по п.10, в которой банковская карта выбрана из группы, состоящей из кредитной карты, банкоматной карты, дебетовой карты, депозитной карты и электронной платежной карты.

12. Система (100, 300) по п.10, в которой электронный проездной билет выбран из группы, состоящей из карты Ойстер и карты Октопус.

13. Система (100, 300) по п.10, в которой лицензия на программное обеспечение выбрана из группы, состоящей из лицензии на программу, лицензии на программное обеспечение автоматизации, лицензии на операционную систему и приложения для мобильного телефона.

14. Система (100, 300) по п.10, в которой цифровые информационные материалы выбраны из группы, состоящей из игры, музыки, фильма, видеоклипа, телепередачи и телесериала в прямом эфире.

15. Система (100, 300) по п.9, в которой первый и второй ключи (30, 40) создаются путем шифрования информации счета с использованием сгенерированного временного ключа и разделения зашифрованной информации счета на первый и второй ключи (30, 40).

16. Система (100, 300) по п.15, в которой информация счета является информацией счета пользователя объекта (10).

17. Устройство (400) для защиты объекта (10) от несанкционированного копирования, содержащее

шифровальную машину (402);

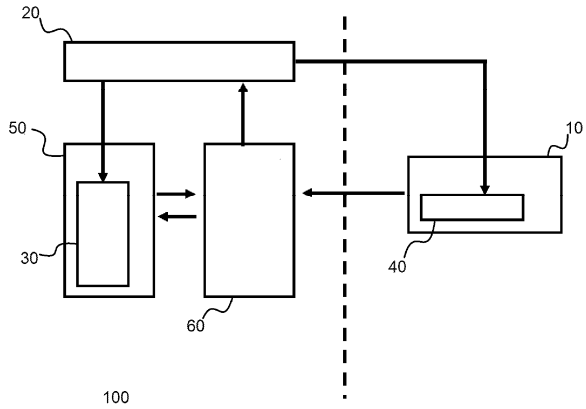
устройство (404) чтения ключей объекта и устройство (406) чтения ключей эмитента, подключенные к шифровальной машине (402) и выполненные с возможностью считывания ключа объекта и ключа эмитента соответственно;

блок (408) удостоверения ключей, подключенный к шифровальной машине (402) и выполненный с возможностью шифрования или дешифрования ключа объекта и ключа эмитента для удостоверения ключа объекта и ключа эмитента;

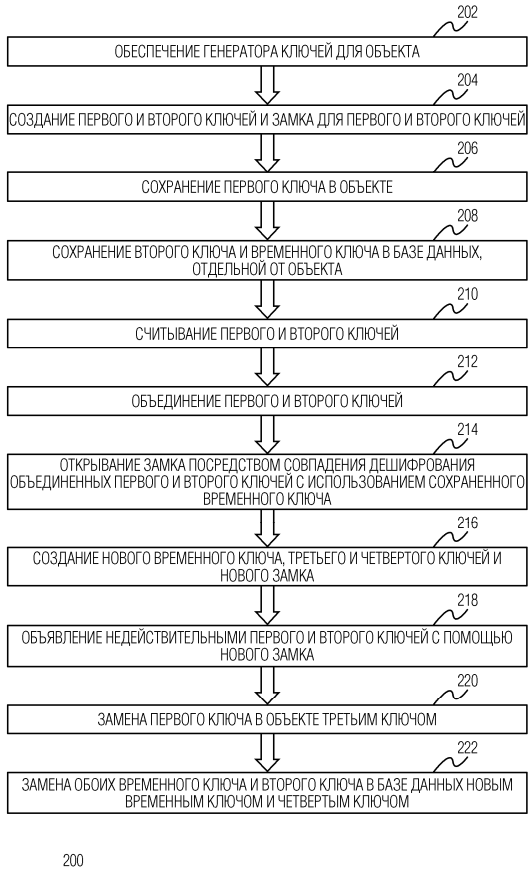
генератор (410) ключей, подключенный к шифровальной машине (402) и выполненный с возможностью генерации временного ключа и шифрования или дешифрования ключа объекта и ключа эмитента для генерации кода шифрования и его разделения на ключ объекта и ключ эмитента; и

блок обновления ключей, подключенный к генератору (410) ключей и выполненный с возможностью обновления ключа объекта и ключа эмитента путем замены ключа объекта и ключа эмитента новым ключом объекта и новым ключом эмитента, а также новым временным ключом, соответственно, и отказа от ключа объекта и ключа эмитента,

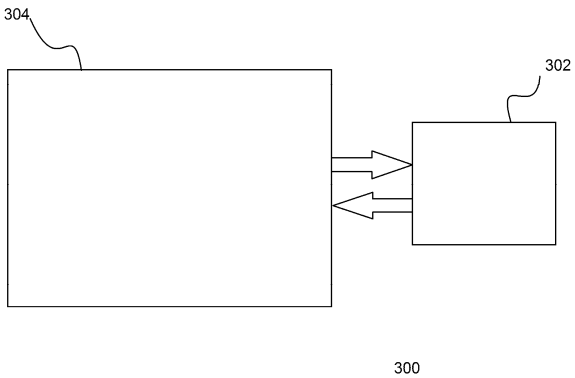
при этом ключ объекта заменяется новым ключом объекта, ключ эмитента заменяется новым ключом эмитента, а временной ключ заменяется новым временным ключом после каждого использования объекта (10).



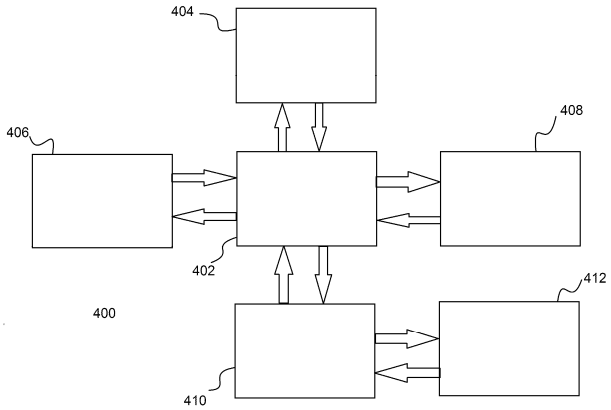
Фиг. 1



Фиг. 2



Фиг. 3



Фиг. 4

Евразийская патентная организация, ЕАПВ
Россия, 109012, Москва, Малый Черкасский пер., 2