

(19)



**Евразийское
патентное
ведомство**

(11) **034481**

(13) **B1**

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2020.02.12

(51) Int. Cl. **G09C 5/00** (2006.01)
H04L 9/00 (2006.01)

(21) Номер заявки
201591160

(22) Дата подачи заявки
2013.12.16

(54) СПОСОБ И УСТРОЙСТВО ДЛЯ МАРКИРОВАНИЯ ПРОМЫШЛЕННЫХ ИЗДЕЛИЙ

(31) 12197525.4

(32) 2012.12.17

(33) EP

(43) 2015.12.30

(86) PCT/EP2013/076725

(87) WO 2014/095737 2014.06.26

(71)(73) Заявитель и патентовладелец:
ИНЕКСТО СА (CH)

(72) Изобретатель:
Шане Патрик, Фраде Эрван (CH)

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

(56) WO-A1-0143086
WO-A1-9724699
US-B1-6212638

LEHTONEN MIKKO ET AL.: "Features, Identity, Tracing and Cryptography in Product Authentication", THE 13TH INTERNATIONAL CONFERENCE ON CONCURRENT ENTERPRISING: CONCURRENT INNOVATION: AN EMERGING PARADIGM FOR COLLABORATION & COMPETITIVENESS IN THE EXTENDED ENTERPRISE, CENTRE FOR CONCURRENT ENTERPRI, 4 June 2007 (2007-06-04), pages 1-8, XP002560506, Retrieved from the Internet:URL:http://www.stop-project.eu/Portals/1/publications/ICE07_StoP_ProdAuth.pdf [retrieved on 2009-12-15], the whole document

(57) В изобретении описан способ маркирования промышленного изделия, включающий в себя создание уникального идентификатора продукта для промышленного изделия; создание одного или нескольких ключей шифрования; генерирование тайного ключа с помощью уникального идентификатора продукта и одного или нескольких ключей шифрования; генерирование значения системного шума путем выполнения хеш-функции на тайном ключе и уникальном идентификаторе продукта; генерирование физического ключа из измеренного физического признака промышленного изделия; генерирование значения физического шума путем выполнения хеш-функции на физическом ключе и уникальном идентификаторе продукта; генерирование защищенного идентификатора, полученного из или включающего в себя значение системного шума и значение физического шума; и размещение отметки на промышленном изделии, отметка содержит защищенный идентификатор или идентификатор, полученный из защищенного идентификатора. Также описаны способы установления подлинности изделий, маркированных согласно способу.

B1

034481

034481 B1

Настоящее изобретение относится к способам и устройству для маркирования промышленных изделий. В частности, настоящее изобретение относится к маркированию упакованных товаров.

Поддельные и контрабандные товары представляют собой глобальную проблему для потребителей, изготовителей и правительственных органов. Поддельные товары, которые представляют собой неразрешенные изделия товаров, как правило, более низкого качества, нелегально продают по всему миру. Эти товары наносят вред потребителю, поскольку они могут быть более низкого качества, что может быть опасно (это особенно важно для таких продуктов, как лекарственные препараты или другие потребительские товары). Поддельные товары наносят вред изготовителям, поскольку они могут пострадать от потери репутации, увеличения конкуренции со стороны нелегальных изготовителей, производящих их продукты, и нарушения других юридических прав. Контрабандные товары, которые представляют собой товары, изготовленные с целью ухода от налогов или правительственного регулирования, также являются существенной проблемой для изготовителей и правительственных органов. Эти товары нелегально перевозят, импортируют или ими нелегально торгуют, что приводит к существенным потерям доходов правительственных органов вследствие неправильного сбора пошлин или налогов.

Преимущественно иметь возможность установить подлинность промышленных изделий, используя уникальные маркировки на изделиях, без необходимости хранить каждую уникальную маркировку в месте, где необходимо установить подлинность изделий. Также желательно иметь возможность обнаруживать поддельные изделия, или изделия, для которых была скопирована уникальная маркировка продукта установленной подлинности, без необходимости хранить запись установления подлинности каждой уникальной маркировки.

В одной особенности изобретения предусмотрен способ маркирования промышленного изделия, включающий в себя

- создание уникального идентификатора продукта для промышленного изделия;
- создание одного или нескольких ключей шифрования;
- генерирование тайного ключа с помощью уникального идентификатора продукта и одного или нескольких ключей шифрования;
- генерирование физического ключа из измеренного физического признака промышленного изделия;
- генерирование защищенного идентификатора, полученного из или включающего в себя тайный ключ и физический ключ; и
- размещение отметки на промышленном изделии, при этом отметка содержит защищенный идентификатор или идентификатор, полученный из защищенного идентификатора.

Защищенный идентификатор может включать в себя уникальный идентификатор продукта.

Предпочтительно способ дополнительно включает в себя этап генерирования значения системного шума с помощью тайного ключа и уникального идентификатора продукта, причем защищенный идентификатор получают из или защищенный идентификатор включает в себя значение системного шума. Предпочтительно этап генерирования значения системного шума включает в себя выполнение хеш-функции на тайном ключе и уникальном идентификаторе продукта.

Предпочтительно способ дополнительно включает в себя генерирование значения физического шума с помощью физического ключа и уникального идентификатора продукта, причем защищенный идентификатор получают из или включает в себя значение системного шума. Предпочтительно этап генерирования значения физического шума включает в себя выполнение хеш-функции на физическом ключе и уникальном идентификаторе продукта.

Как используется в данном документе, "уникальный идентификатор продукта" означает идентификатор, который уникальным образом идентифицирует промышленное изделие. Каждому промышленному изделию дают разный уникальный идентификатор продукта. Уникальный идентификатор продукта, как правило, представляет собой цифровую или буквенно-цифровую последовательность или значение.

Как используется в данном документе, "шифрование" означает процесс преобразования информации с помощью алгоритма, чтобы сделать эту информацию нечитаемой для кого бы то ни было, кроме тех, кто обладает особым знанием в форме ключа шифрования. Дешифрование представляет собой обратный процесс. "Ключ шифрования" представляет собой блок информации, который используют вместе с алгоритмом шифрования для шифрования или дешифрования информации. Ключ шифрования, как правило, представляет собой цифровую или буквенно-цифровую последовательность или значение.

Как используется в данном документе, термин "тайный ключ" используют для описания ключа, используемого в хеше с ключом, который генерируют с помощью уникального идентификатора продукта и одного или нескольких дополнительных ключей или блоков данных. Во время, когда его генерируют, тайный ключ неизвестен никакой стороне, кроме той стороны, которая создала тайный ключ. Термин "тайный ключ" в этом контексте не ограничен значением закрытого ключа в контексте схемы асимметричного шифрования.

Как используется в данном документе, хеш-функция представляет собой функцию, которая ставит в соответствие входные данные выходу фиксированного размера (обычно меньшего, чем входные данные), называемому значением хеша. Хеш-функция, как правило, замещает или перемещает или замещает и перемещает информацию, чтобы создавать значение хеша или значение шума. Предпочтительно хеш-

функция представляет собой криптографическую хеш-функцию. Криптографическая хеш-функция производит отпечаток или контрольную сумму входных данных. Два блока данных могут считаться идентичными, если при использовании одной и той же криптографической хеш-функции они производят одинаковое значение хеша. Преимущественно хеш-функция представляет собой одностороннюю хеш-функцию, что означает, что численно невозможно получить входные данные из значения хеша. Эти признаки могут быть использованы в процессе установления подлинности, как будет описано. Хеш-функция может быть снабжена ключом путем сочетания тайного ключа и входного сообщения, чтобы создавать значение хеша с ключом или шум.

Как используется в данном документе, термин "значение шума" означает значение хеша или значение хеша с ключом, или значение или последовательность символов, полученные непосредственно из значения хеша и тайного ключа.

Измеренный физический признак промышленного изделия может представлять собой любой измеренный физический признак и может быть основан на массе, размере, форме, текстуре или узоре поверхности, цвете, химическом составе или ответе на входной сигнал, таком как ответ на электрический, магнитный или оптический сигнал. Измеренный физический признак предпочтительно выбирают и измеряют до некоторого разрешения, так что он, вероятно, будет уникальным для каждого изготовленного изделия или, по меньшей мере, более вероятно, будет другим, чем он же для любых двух промышленных изделий. Измеренный физический признак предпочтительно предусматривает физическую сигнатуру для промышленного изделия. В предпочтительном варианте осуществления измеренный физический признак представляет собой изображение части упаковки промышленного изделия.

Защищенный идентификатор может представлять собой любой тип идентификатора, но предпочтительно представляет собой цифровую или буквенно-цифровую последовательность или значение. Отметка также может представлять собой последовательность символов или чисел или может представлять собой графическое представление, такое как одномерный или двумерный штрих-код.

В одном варианте осуществления этап генерирования защищенного идентификатора включает в себя генерирование первого идентификатора путем шифрования уникального идентификатора продукта вместе со значением системного шума и генерирование защищенного идентификатора путем шифрования первого идентификатора вместе со значением физического шума.

В этом варианте осуществления способ может дополнительно включать в себя установление подлинности изготовленного изделия в проверочном центре, при этом этап установления подлинности включает в себя идентификацию отметки на изделии; дешифрование отметки для получения первого идентификатора и значения физического шума; дешифрование первого идентификатора для получения уникального идентификатора продукта и значения системного шума; генерирование нового физического ключа из измеренного физического признака изготовленного изделия; генерирование новой копии значения физического шума путем выполнения хеш-функции на новом физическом ключе и полученном уникальном идентификаторе продукта; сравнение новой копии значения физического шума с полученным значением физического шума и предоставление указания, идентично ли или коррелирует ли полученное значение физического шума новой копии значения физического шума.

Этап сравнения может включать в себя получение степени корреляции, а этап предоставления указания включает в себя предоставление указания, превышает ли степень корреляции пороговое значение.

В этом варианте осуществления этап установления подлинности может дополнительно включать в себя генерирование новой копии тайного ключа из уникального идентификатора продукта и одного или нескольких ключей шифрования; генерирование новой копии значения системного шума путем выполнения хеш-функции на новой копии тайного ключа и уникальном идентификаторе продукта; сравнение новой копии значения системного шума с полученным значением системного шума; и предоставление указания, являются ли идентичными новая копия значения системного шума и полученное значение системного шума.

В другом варианте осуществления этап генерирования защищенного идентификатора включает в себя генерирование первого защищенного идентификатора путем шифрования уникального идентификатора продукта вместе со значением системного шума; генерирование второго защищенного идентификатора путем шифрования уникального идентификатора продукта вместе со значением физического шума; и размещение отметки на изготовленном изделии, отметка содержит первый и второй защищенные идентификаторы или идентификатор или идентификаторы, полученные из первого и второго защищенных идентификаторов.

В этом варианте осуществления способ может дополнительно включать в себя установление подлинности изготовленного изделия в проверочном центре, при этом этап установления подлинности включает в себя идентификацию отметки на изделии; дешифрование отметки для получения уникального идентификатора продукта, значения системного шума и значения физического шума; генерирование новой копии тайного ключа из уникального идентификатора продукта и одного или нескольких ключей шифрования; генерирование новой копии значения системного шума путем выполнения хеш-функции на новой копии тайного ключа и уникальном идентификаторе продукта; сравнение новой копии значения системного шума с полученным значением системного шума; генерирование нового физического ключа

из измеренного физического признака промышленного изделия; генерирование новой копии значения физического шума путем выполнения хеш-функции на новом физическом ключе и полученном уникальном идентификаторе продукта; сравнение новой копии значения физического шума с полученным значением физического шума; и предоставлением указания, идентична ли новая копия значения системного шума полученному значению системного шума и идентична ли или коррелирует ли новая копия значения физического шума полученному значению физического шума.

В любом из этих вариантов осуществления этап генерирования первого защищенного идентификатора может включать в себя шифрование уникального идентификатора продукта и значения системного шума с помощью ключа генератора кода, причем этап генерирования второго защищенного идентификатора включает в себя сочетание первого защищенного идентификатора и значения физического шума вместе с ID генератора кода, причем ключ генератора кода может быть получен или добыт из справочной таблицы в проверочном центре с помощью ID генератора кода.

В любом из этих вариантов осуществления способ может дополнительно включать в себя этап сохранения одного или нескольких ключей шифрования в проверочном центре. Один или несколько ключей шифрования могут содержать статический ключ и динамический ключ, причем новый динамический ключ создают для каждой партии промышленных изделий, тогда как один и тот же статический ключ используют для нескольких партий промышленных изделий.

Уникальный идентификатор продукта может включать в себя информацию, идентифицирующую партию изделий, к которой принадлежит изделие.

Изобретение предусматривает способность устанавливать подлинность как на основании информации от изготовителя, т.е. различных ключей шифрования, так и на основании физического признака изделия. Это предусматривает два уровня установления подлинности и обеспечивает обнаружение клонирования идентификаторов на подлинных изделиях, но не требует крупномасштабного хранилища кодов установления подлинности.

В другой особенности изобретения предусмотрено устройство для маркирования промышленного изделия, содержащее

- генератор ключа, выполненный с возможностью генерировать ключи шифрования;
- генератор кода, выполненный с возможностью генерировать уникальный идентификатор продукта для каждого промышленного изделия;
- генератор физического ключа, выполненный с возможностью генерировать физические ключи из измеренного физического признака каждого промышленного изделия;
- средство обработки, выполненное с возможностью генерировать тайный ключ для каждого промышленного изделия с помощью уникального идентификатора продукта и одного или нескольких ключей шифрования;
- генерировать защищенный идентификатор, полученный из или включающий в себя тайный ключ и физический ключ; и
- маркер для маркирования каждого промышленного изделия защищенным идентификатором или идентификатором, полученным из защищенного идентификатора.

Предпочтительно процессор выполнен с возможностью генерировать значение системного шума для каждого промышленного изделия с помощью тайного ключа и уникального идентификатора продукта, причем защищенный идентификатор получают из или защищенный идентификатор включает в себя значение системного шума. Предпочтительно процессор выполнен с возможностью генерировать значение системного шума для каждого промышленного изделия путем выполнения хеш-функции на тайном ключе и уникальном идентификаторе продукта.

Предпочтительно процессор выполнен с возможностью генерировать значение физического шума для каждого промышленного изделия с помощью физического ключа и уникального идентификатора продукта, причем защищенный идентификатор получают из или защищенный идентификатор включает в себя значение физического шума. Предпочтительно процессор выполнен с возможностью генерировать значение физического шума для каждого промышленного изделия путем выполнения хеш-функции на физическом ключе и уникальном идентификаторе продукта.

В одном варианте осуществления средство обработки выполнено с возможностью генерировать первый идентификатор для каждого промышленного изделия путем шифрования уникального идентификатора продукта вместе с тайным ключом или значением системного шума; и генерировать защищенный идентификатор для каждого изготовленного изделия путем шифрования первого идентификатора вместе со значением физического шума.

В другом варианте осуществления средство обработки выполнено с возможностью генерировать первый защищенный идентификатор для каждого промышленного изделия путем шифрования уникального идентификатора продукта вместе с тайным ключом или значением системного шума и генерировать второй защищенный идентификатор для каждого промышленного изделия путем шифрования уникального идентификатора продукта вместе с физическим ключом или значением физического шума; и маркер выполнен с возможностью маркировать каждое изготовленное изделие первым защищенным идентификатором и вторым защищенным или идентификатором или идентификаторами, полученными из первого

и второго защищенных идентификаторов.

Промышленное изделие может представлять собой тару, содержащую табачный продукт. Примерами табачных продуктов являются сигареты, листовая табак, сигары и картриджи или заправки для электрически нагреваемых курительных систем или других систем электронных сигарет.

Изобретение позволяет устанавливать подлинность промышленных изделий без требования хранения больших объемов информации. Это является важным для любой практической системы, подходящей для установления подлинности изделий, производимых в больших объемах. Кроме того, использование физического ключа в сочетании с уникальным идентификатором продукта (УИП) повышает защищенность и делает производство поддельных и контрабандных товаров более сложным. Добавление физического ключа предусматривает систему, которая может обнаруживать клонирование и является сложной для копирования. Даже если фальсификатор обладает знанием о конкретном инструменте, используемом для генерирования физического ключа, сочетание физического ключа с УИП для производства идентификатора делает клонирование почти невозможным. Изобретение также позволяет проводить установление подлинности в режиме онлайн, т. е. подключенное к проверочному центру по сети связи на основании значения системного шума, а также позволяет проводить установление подлинности в автономном режиме на основании значения физического шума. Маркирование, требующееся на каждом изделии, представляет собой просто один или несколько кодов, и таким образом очень мало увеличивает затраты на каждое изделие, по сравнению с некоторыми другими решениями, которые полагаются на дорогие этикетки, которые технически сложно воспроизвести.

Далее изобретение будет описано исключительно на примерах со ссылками на сопроводительные графические материалы, в которых:

фиг. 1 - схематический вид системы маркирования согласно одному варианту осуществления изобретения;

фиг. 2 представляет, как получают значение системного шума и значение физического шума;

фиг. 3 - блок-схема, представляющая способ маркирования одного варианта осуществления изобретения, который может быть реализован на системе, представленной на фиг. 1;

фиг. 4 - блок-схема, представляющая способ установления подлинности для варианта осуществления изобретения, представленного на фиг. 3, который может быть реализован на системе, представленной на фиг. 1;

фиг. 5 - блок-схема, представляющая способ маркирования согласно другому варианту осуществления изобретения, который может быть реализован на системе, представленной на фиг. 1; и

фиг. 6 - блок-схема, представляющая способ установления подлинности для варианта осуществления изобретения, представленного на фиг. 5, который может быть реализован на системе, представленной на фиг. 1.

Уникальные маркировки на промышленных изделиях могут быть использованы для отслеживания изделий. Например, заказ потребителя может быть связан с идентифицирующей этикеткой или этикетками конкретного транспортного ящика или ящиков, содержащих заказанные товары. "Товары" в этом контексте означает промышленные изделия или другие изделия, предназначенные для распределения или продажи потребителям. Это позволяет потребителю, изготовителю и любым посредникам постоянно отслеживать местоположение требующихся товаров. Это может быть достигнуто с помощью сканеров для сканирования идентификаторов и осуществления связи с проверочным центром. Альтернативно, идентификаторы могут быть считаны человеком, который может затем вручную осуществлять связь с проверочным центром. Идентификаторы также могут быть использованы потребителями, национальными органами и другими сторонами для проверки того, что конкретное изделие содержит подлинный продукт. Например, одна сторона может использовать сканер для считывания идентификатора на транспортном ящике (или идентификатор может быть считан человеком, как указано выше). Детали идентификатора могут быть отправлены в проверочный центр. Проверочный центр затем может просматривать или иным образом обрабатывать детали идентификатора, определять детали производства транспортного ящика и отправлять эти детали на сканер, таким образом позволяя стороне подтверждать, что транспортный ящик и продукты, содержащиеся в нем, являются подлинными. В случае, когда центральная база данных не распознает идентификатор, сторона может полагать, что рассматриваемые изделия являются поддельными. Идентификаторы также могут быть использованы для отслеживания изделий. Например, если изготовителю нужно отозвать продукты из выбранного количества транспортных ящиков, эти транспортные ящики могут быть отслежены с помощью их идентификаторов.

На фиг. 1 представлен схематический вид системы маркирования согласно одному варианту осуществления изобретения. В этом варианте осуществления система 101 содержит один или несколько производственных центров 103, 105, 107 для производства промышленных изделий 109. Каждый производственный центр может содержать производственную линию или оборудование, которое может представлять собой линию изготовления и упаковки сигарет. Предпочтительно производство осуществляют партиями, каждая партия предназначена для производства определенного количества отдельных промышленных изделий. Если имеется два или несколько производственных центров, они могут быть физически расположены на одной и той же или различных промышленных площадках. В этом предпочтительном

варианте осуществления система включает в себя производственные центры 103, 105, 107, но изобретение может на самом деле быть осуществлено в пункте импорта, пункте распределения, у покупателя, оптового торговца или любом другом пункте в цепи поставки.

Каждый производственный центр включает в себя генератор 111 кода для генерации кодов для промышленных изделий 109. Предпочтительно генератор 111 кода представляет собой полностью автономный компьютер или микроконтроллер, предназначенный для конкретного производственного центра. Каждый производственный центр также включает в себя генератор 112 физического ключа, который измеряет или шифрует физический признак каждого промышленного изделия и преобразует его в физический ключ 207. Генератор 111 кода использует физические ключи для генерирования кодов для маркирования на изделиях.

В этом варианте осуществления генератор физического ключа имеет такой тип, который описан в WO2007/071788. Часть упаковки каждого изделия освещают, и цифровой датчик изображения захватывает изображение освещенной части. Часть упаковки выбирают за ее стабильную во времени беспорядочную микроструктуру. Материалы, такие как бумага и картон, обладают беспорядочной микроструктурой, которая может быть использована в качестве "отпечатка" изделия. Изображение микроструктуры части изделия преобразуют в физический ключ или сигнатуру, как описано в WO2007/071788, в форме буквенно-цифрового значения или матрицы. Генератор физического ключа этого типа доступен у Signoptic Technologies, Savoie Technolac, 5 allée Lac d'Aiguebelette BP340 F-73375, LE BOURGET-DU-LAC, Франция. Однако может быть использован любой тип генератора физического ключа, и он может быть основан на других физических признаках изделия, таких как масса или форма, или может даже быть основан на химических или биологических признаках изделия.

В этом варианте осуществления каждый производственный центр также включает в себя маркер 113 для маркирования сгенерированных кодов на промышленные изделия 109. Маркер 113 может содержать любое подходящее маркировочное средство, например, помимо прочего, струйный принтер непрерывного действия, капельно-импульсный струйный принтер, голографический принтер, лазерный принтер или любой другой принтер или маркер, который позволяет печатать или маркировать сгенерированные коды на отдельных промышленных изделиях. Печатание или маркирование сгенерированных кодов может быть осуществлено на каждом изделии, на внешней упаковке, на этикетках или любым другим удобным образом. В одном варианте осуществления сгенерированные коды печатают на клейких метках или этикетках, которые должны быть наложены на промышленные изделия, предпочтительно без возможности съема. В одном варианте осуществления сгенерированные коды печатают лазерным лучом на слое чувствительного к лазеру материала, нанесенного на производственное изделие на упаковке изделия. Этот способ позволяет отпечатывать код через прозрачный оберточный слой.

Система 101 дополнительно содержит проверочный центр 114, который включает в себя генератор 115 ключа для генерации ключей 209, 211 для использования в маркировании и установлении подлинности промышленных изделий и центральный сервер 117. В этом варианте осуществления генератор 111 кода может осуществлять связь с проверочным центром 114 через защищенное Интернет-соединение 119 и сервер 121, локальный для производственного центра, или с помощью других способов передачи данных. Альтернативно, генератор 111 кода может осуществлять связь с проверочным центром через производственный портал, предназначенный для одного или нескольких производственных центров.

Генератор 115 ключа генерирует криптографический ключ, в данном документе называемый статическим ключом. Генератор 115 ключа генерирует незашифрованную версию статического ключа и зашифрованную версию статического ключа. Незашифрованная версия статического ключа, в данном документе называемая активным статическим ключом 209, представлена на фиг. 1 сплошной границей. Зашифрованная версия статического ключа, в данном документе называемая пассивным статическим ключом 211, представлена на фиг. 1 пунктирной границей. Активный статический ключ 209, т.е. незашифрованную версию статического ключа, генерируют в генераторе 115 ключа, и поэтому он доступен центральному серверу 117. Генератор 115 ключа отправляет пассивный статический ключ 211 генератору 111 кода в производственном центре 103, 105, 107.

Пассивный статический ключ 211 может быть отправлен из генератора 115 ключа генератору 111 кода на постоянном запоминающем устройстве, например CD-диске, DVD-диске или съемном жестком диске. Запоминающее устройство физически переносят на генератор 111 кода в производственном центре 103, 105, 107. Альтернативно, пассивный статический ключ 211 может быть отправлен из генератора 115 ключа генератору 111 кода через защищенное Интернет-соединение, например, действующее шифрование. Это может быть по запросу от генератора 111 кода. Это гарантирует подлинность, конфиденциальность и целостность статического ключа.

Генератор 115 ключа также генерирует код 213 активации, который содержит ключ или код для дешифрования пассивного статического ключа 211 для формирования активного статического ключа 209. Этот код 213 активации также доступен центральному серверу 117. Предпочтительно активный статический ключ 209 и код 213 активации хранят вместе с идентификацией производственного центра 103, 105, 107, которому их выделяют.

В одном варианте осуществления статический ключ содержит ряд частей. Основная часть может

представлять собой несколько тайных кодов, например сложное выражение. Сложное выражение может представлять собой, например, длинную строку случайных или псевдослучайных цифр или символов. Ряд частей могут дополнительно включать в себя уникальный идентификатор для статического ключа, упорядоченный код, определяющий, как статический ключ необходимо совмещать с динамическим ключом (обсуждается ниже), цифровой криптографический сертификат, связанный с уникальным идентификатором статического ключа, и правила или лицензию статического ключа, которая содержит цифровой криптографический сертификат, сгенерированный выше.

Предпочтительно пассивный статический ключ, т.е. зашифрованную версию статического ключа, и особенно несколько тайных кодов, шифруют с помощью стойкого шифра. Примером подходящего шифра является блочный шифр тройной DES (Стандарт шифрования данных) или блочный шифр тройной DES/Рендал. Оба применяют алгоритм шифрования Стандарта шифрования данных три раза к каждому блоку данных, и тройной DES/Рендал является младшим вариантом тройного DES, который был разработан IBM. В этом случае ключ тройного DES или тройного DES/Рендал содержит код 213 активации. Таким образом, в предпочтительном варианте осуществления, активный статический ключ 209 незашифрован, пассивный ключ 211 зашифрован с помощью ключа тройного DES или тройного DES/Рендал, и код 213 активации содержит этот ключ тройного DES или тройного DES/Рендал.

На следующем этапе 203 регистрируют пассивный статический ключ 211, полученный генератором 111 кода. Это осуществляется генератором 111 кода, отправляющим в проверочный центр 114 информацию 215 о полученном статическом ключе и любую связанную машинную информацию (не показано). Ее предпочтительно отправляют через защищенное Интернет-соединение 119, как представлено на фиг. 1, но могут отправлять другим подходящим способом. Проверочный центр 114 отправляет назад генератору 111 кода код 213 активации. Код 213 активации позволяет активировать пассивный статический ключ 211, и это схематически представлено на 217. Код 213 активации предпочтительно также отправляют по защищенному Интернет-соединению 119, как представлено на фиг. 1. Процедура регистрации предпочтительно организована так, что активный статический ключ 209 никогда не передают по Интернет.

Процедура регистрации может иметь форму обычного механизма обмена пары открытый/закрытый ключ. Она может использовать асимметричную пару ключей, связанную с цифровым криптографическим сертификатом, образующим часть статического ключа, как обсуждалось выше. В этом случае открытый ключ асимметричной пары ключей может иметь форму ключа, выданного третьей стороной, например правительственным органом. Информация 215 о полученном статическом ключе, которая отправлена с генератора 111 кода в проверочный центр 114, может содержать уникальный идентификатор для статического ключа, который образует часть статического ключа, как обсуждалось выше. Соответствующая машинная информация (не показана), которую также отправляют с генератора 111 кода в проверочный центр 114, может содержать уникальный идентификатор или сертификат для генератора 111 кода или производственного центра. Этот уникальный идентификатор может включать в себя информацию о местоположении и идентичности генератора кода или производственного центра, который предварительно получил разрешение на производство. Предпочтительно уникальный идентификатор статического ключа и идентификатор генератора кода или производственного центра шифруют с помощью открытого ключа асимметричной пары ключей, связанной с сертификатом статического ключа.

Когда проверочный центр 114 получает зашифрованный уникальный идентификатор статического ключа и идентификатор генератора кода или производственного центра, проверочный центр 114 может дешифровать с помощью закрытого ключа асимметричной пары ключей, связанной с сертификатом статического ключа. Проверочный центр затем может проверять, что уникальный идентификатор статического ключа и идентификатор генератора кода или производственного центра являются действительными. Затем проверочный центр 114 отправляет назад на генератор 111 кода код 213 активации. Как уже упомянуто, предпочтительно код 213 активации имеет форму шифра тройного DES или тройного DES/Рендал. Проверочный центр шифрует код активации (например, шифр тройного DES или тройного DES/Рендал) с открытым ключом асимметричной пары ключей, связанной с сертификатом статического ключа. Это позволяет генератору кода дешифровать код активации (например, шифр тройного DES или тройного DES/Рендал) с помощью закрытого ключа асимметричной пары ключей, связанной с сертификатом статического ключа. Затем пассивный статический ключ 211 может быть активирован с помощью дешифрованного кода 213 активации, чтобы сформировать активный статический ключ 209.

Когда пассивный статический ключ 211 в генераторе 111 кода был активирован, производственный центр может изготавливать изделия и производить коды для промышленных изделий в генераторе 111 кода.

Генератор 111 кода генерирует новый ключ, в данном документе называемый динамическим ключом 219, для каждой партии промышленных изделий. Динамический ключ 219 предпочтительно представляет собой случайный тайный код, такой как случайное число. Генератор кода использует динамический ключ 219 для партии, вместе с активным статическим ключом 209, чтобы генерировать тайный ключ 223. Тайный ключ 223 представляет собой n , используемое в сочетании с физическими ключами и уникальным идентификатором продукта (УИП) для каждого изделия, чтобы генерировать коды 221 (на-

пример, буквенно-цифровые коды), которые должны быть маркированы на промышленных изделиях в этой партии. В этом варианте осуществления УИП для каждого изделия содержит детали производства, идентифицирующие время производства вместе со значением суммирующего счетчика, чтобы различать изделия, произведенные в один период времени одним производственным центром.

Генератор кода использует криптографическую хеш-функцию на сочетании УИП с тайным ключом и сочетании УИП с физическим ключом. Это создает цифровые отпечатки, называемые в данном документе "значениями шума", для изделия, и эти значения шума используют для генерирования кодов 221, которые маркируют на изделиях маркером 113. В дополнение к обычно используемым криптографическим хеш-функциям, для генерирования значений хеша или значений шума доступно множество способов, включая, помимо прочего, преобразование, замещение, табличное замещение и индексирование.

Фиг. 2 представляет способ генерирования значений шума, реализуемый генератором 111 кода. Для генерирования значения 225 системного шума сначала получают тайный ключ из активного статического ключа 209, динамического ключа 219 и УИП 221. Динамический ключ 219 и активный статический ключ 209 известны только проверочному центру 114 и генератору 111 кода. На этапе 301 динамический ключ и УИП используют для извлечения тайного ключа из сложного выражения, содержащегося в статическом ключе, согласно упорядоченному коду в статическом ключе. Тайный ключ 223 и УИП 221 затем хешируют на этапе 303, чтобы производить системный шум для изделия. Для генерирования значения 227 физического шума физический ключ 207 хешируют с УИП 221 на этапе 305. Хеш-функция, используемая для генерирования значения системного шума, может быть той же или отличной от хеш-функции, используемой для генерирования значения физического шума.

Фиг. 3 представляет способ использования значения системного шума и значения физического шума для генерирования защищенного идентификатора для каждого изделия согласно первому варианту осуществления изобретения. На этапе 311 значение 225 системного шума и УИП 221 соединяют. На этапе 313 соединенные значение системного шума и УИП шифруют ключом 231 обфускации генератора кода (КОГК) для производства первого идентификатора 241. КОГК является конкретным для генератора кода и предварительно загружается в генератор кода. Первый идентификатор 241 затем соединяют со значением 227 физического шума и идентификатором 233 генератора кода. Идентификатор генератора кода (ИГК) 233 позволит получить КОГК во время установления подлинности. Сочетание первого идентификатора, значения физического шума и ИГК затем шифруют с помощью глобального ключа 235 на этапе 317 для производства защищенного идентификатора 251. Глобальный ключ 235 является общим для всех производственных центров и может быть частью симметрической или асимметрической пары ключей, известной проверочному центру. Защищенный идентификатор 251 затем маркируют на изделии на этапе 319 маркером 113.

Генератор 111 кода или производственный центр 103, 105, 107 ведет подсчет кодов, которые маркируют на промышленных изделиях. Кроме того, генератор 111 кода отправляет динамический ключ 219 для каждой партии, вместе с информацией о партии (не показана), в проверочный центр 114. Это может быть выполнено через защищенное Интернет-соединение 119. Информация о партии может включать в себя различные блоки информации, например, помимо прочего, бренд, рынок назначения или пункт назначения. Динамические ключи 219 нет необходимости отправлять в проверочный центр 114 в реальном времени, и они могут быть переданы в проверочный центр в любое подходящее время, например ежемесячно. Динамические ключи 219, отправленные в проверочный центр 114, хранят в базе данных (например, на центральном сервере 117) в проверочном центре 114 или в доступности для него. Динамический ключ 219 для каждой партии предпочтительно хранят вместе с информацией о партии, отправленной в проверочный центр 114 в одно и то же время.

Предпочтительно активный статический ключ 209 удаляют, когда генератор 111 кода в конкретном производственном центре 103, 105, 107 выводят из работы. Это предотвращает получение доступа к активному статическому ключу 209 со стороны злонамеренного пользователя без надлежащей регистрации. Могут быть предусмотрены дополнительные средства для отключения генератора 111 кода и предотвращения неавторизованного использования генератора 111 кода и производственного центра.

Фиг. 4 представляет этапы, выполняемые проверочным центром 114 и пользователем 601, когда пользователь 601 желает установить подлинность отдельного промышленного изделия, маркированного согласно процессу, представленному на фиг. 3. Пользователь 601 считывает код 221 на изделии и отправляет его в проверочный центр 114. Это представлено на фиг. 1. Пользователь 601 может отправить код в проверочный центр 114 любым подходящим способом, таким как защищенное или незащищенное Интернет-соединение.

Проверочный центр получает защищенный идентификатор на этапе 321. Защищенный идентификатор дешифруют с помощью глобального ключа 235 (или соответствующего ключа в паре ключей, если используют асимметричные ключи) на этапе 323, чтобы выявить значение 227 физического шума и первый идентификатор 241. Также выявляют ИГК. С помощью справочной таблицы затем получают КОГК 231 из ИГК. Первый ID затем дешифруют на этапе 325 с помощью КОГК 231, чтобы выявить системный шум 225 и УИП 221. С этой информацией, вместе с активным статическим ключом 209 и динамическим ключом 219, и новым физическим ключом, могут быть восстановлены и значение физического шума, и

значение системного шума для установления подлинности изделия.

Для воссоздания значения физического шума новый физический ключ должен быть получен пользователем 601 на этапе 327 путем записи изображения части изделия таким же образом и в тех же условиях, которые использованы для генерирования оригинального физического ключа 207. УИП и новый физический ключ затем хешируют для генерирования нового значения физического шума на этапе 329. На этапе 331 новый физический шум сравнивают с извлеченным значением физического шума, выявленным на этапе 323. Если новое значение физического шума в значительной мере подобно извлеченному значению физического шума, то одна часть процесса установления подлинности завершена. Если новое значение физического шума не в значительной мере подобно извлеченному значению физического шума, то изделие определяют как ненастоящее на этапе 339.

Для того чтобы считать изделие подлинным, может потребоваться, чтобы новое значение физического шума было идентичным извлеченному значению физического шума. Однако, чтобы считать изделие подлинным, можно допустить некоторые различия между новым значением физического шума и извлеченным значением физического шума путем использования степени корреляции и требования пороговой степени корреляции. US2005/0257064 описывает подходящий статистический метод для расчета степени корреляции или подобия между двумя цифровыми сигнатурами, полученными из измеренных физических признаков волокнистой среды.

Возможно, чтобы этап 329 и 331 выполнял или пользователь 601, или проверочный центр 114. Если проверочный центр предоставил пользователю 601 УИП, конечный пользователь может установить подлинность изделия на основе значения физического шума. Аналогично, если проверочному центру 114 предоставлен новый физический ключ, проверочный центр может установить подлинность изделия на основании значения физического шума.

Для воссоздания значения системного шума должен быть восстановлен тайный ключ, на этапе 333, с помощью УИП и ИГК, проверочный центр 114 способен извлечь динамический ключ 219 и активный статический ключ 209 из записей, хранимых в проверочном центре. Тайный ключ может затем быть восстановлен с помощью УИП 221, динамического ключа 219 и активного статического ключа 209. На этапе 335 новое значение системного шума воссоздают путем хеширования УИП и тайного ключа. На этапе 337 новое значение системного шума сравнивают со значением системного шума, извлеченным на этапе 325. Если новое значение системного шума и извлеченное значение системного шума идентичны, изделие может быть определено как подлинное на этапе 339.

В одном варианте осуществления для того, чтобы изделие считать подлинным, требуются сравнения как значения физического шума, так и значения системного шума. Однако, при желании, можно разрешить установление подлинности на основании только одной из этих проверок.

Из полученного активного статического ключа 209 может быть определен производственный центр 103, 105, 107, в котором было изготовлено изделие, поскольку активные статические ключи предпочтительно хранят в проверочном центре вместе с деталями их связанных производственных центров. Из полученного динамического ключа 219 может быть определена информация о партии для изделия, поскольку динамические ключи предпочтительно хранят в проверочном центре вместе со связанной информацией о партии. Таким образом, проверочный центр 114 может получать, из кода 221, отправленного от пользователя 601, различные блоки информации 603 об отдельном изделии, а также проверять подлинность изделия. Затем вся информация 603, или избранные ее части, включая указание того, является или нет изделие подлинным, может быть отправлена пользователю 601. Это представлено на фиг. 1. Информацию 603 предпочтительно отправляют пользователю 601 тем же способом, которым был отправлен оригинальный код.

Фиг. 5 представляет процесс маркирования согласно второму варианту осуществления изобретения. В способе, представленном на фиг. 5, производят два защищенных идентификатора, один, основанный на значении 225 системного шума, и другой, основанный на значении 227 физического шума. Значение 225 системного шума соединяют с УИП 221 на этапе 341. Сочетание значения системного шума и значения физического шума затем шифруют с КОГК 231 на этапе 343, чтобы производить первый ID 241, как в первом варианте осуществления, представленном на фиг. 3. Первый ID 241 затем соединяют с ИГК на этапе 345 и шифруют с глобальным ключом 235 на этапе 347, чтобы производить первый защищенный ID 271. Значение 227 физического шума соединяют с УИП на этапе 221, чтобы производить второй ID 261. Второй ID шифруют с глобальным ключом 235 на этапе 353, чтобы производить второй защищенный ID. Изделие затем может быть маркировано на этапе 355 первым защищенным ID 271 и вторым защищенным ID 281 или отметкой или отметками, полученными из сочетания первого защищенного ID 271 и второго защищенного ID 281.

Фиг. 6 представляет этапы, выполняемые для установления подлинности изделия, маркированного с помощью процесса, представленного на фиг. 5. На этапе 401 отметка или отметки считывает пользователь, и пользователь получает первый защищенный идентификатор 271 и второй защищенный идентификатор 281. На этапе 403, глобальный ключ 235 используют для получения значения 227 физического шума, первой копии УИП 221, первого ID 241 и ИГК 233. Если пользователь имеет глобальный ключ 235, пользователь может установить подлинность изделия на основании второго защищенного иденти-

фикатора автономно, т. е. не требуя соединения с проверочным центром. Пользователь генерирует новый физический ключ на этапе 407 и его хешируют с УИП для генерирования нового значения физического шума на этапе 409. Пользователь может сравнивать новое значение физического шума со значением физического шума, извлеченным на этапе 403, на этапе 411. Как описано со ссылкой на фиг. 3, изделие может считаться подлинным на этапе 419, если новое значение физического шума равно, или в значительной мере подобно, извлеченному значению физического шума.

На этапе 405 ИГК используется проверочным центром для получения КОГК 231, и КОГК используется для дешифрования первого ID 241, чтобы выявить системный шум и вторую копию УИП. На этапе 408 вторая копия УИП необязательно может быть сравнена со второй копией УИП в качестве проверки. На этапе 423 проверочный центр 114 получает динамический ключ 219 и активный статический ключ 209 с помощью ИГК и УИП. На этапе 415 новое значение системного шума генерируют путем сначала восстановления тайного ключа из УИП, динамического ключа и статического ключа, и затем путем хеширования тайного ключа с УИП. На этапе 417 новое значение системного шума сравнивают со значением системного шума, извлеченным на этапе 405. Если они идентичны, подлинность изделия может быть установлена на этапе 419. Как и в случае варианта осуществления, представленного на фиг. 3, для того, чтобы изделие считалось подлинным, может потребоваться установление подлинности, основанное как на значении системного шума, так и на значении физического шума.

Хотя изобретение было описано со ссылкой на изготовление сигарет, следует понимать, что изобретение применимо для любых продуктов, которые требуют установления подлинности, таких как лекарственные препараты, алкогольные напитки и предметы роскоши.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Способ маркирования промышленного изделия, включающий в себя
 - создание уникального идентификатора продукта для промышленного изделия;
 - создание одного или нескольких ключей шифрования;
 - генерирование тайного ключа с помощью уникального идентификатора продукта и одного или нескольких ключей шифрования, причем уникальный идентификатор продукта включает в себя информацию, идентифицирующую партию изделий, к которой принадлежит изделие;
 - генерирование значения (225) системного шума с помощью тайного ключа и уникального идентификатора продукта;
 - генерирование второго ключа шифрования из измеренного физического свойства промышленного изделия;
 - генерирование значения (227) физического шума с помощью второго ключа шифрования и уникального идентификатора продукта,
 - при этом для создания значения системного шума и значения физического шума способ использует преобразование, замещение, табличное замещение и индексирование или криптографическую хеш-функцию на сочетании уникального идентификатора продукта с тайным ключом и сочетании уникального идентификатора продукта со вторым ключом шифрования;
 - генерирование защитного идентификатора, полученного из тайного ключа и второго ключа шифрования или включающего в себя тайный ключ и второй ключ шифрования, при этом защитный идентификатор получают из значения системного шума и значения физического шума или он включает в себя значение системного шума и значение физического шума;
 - размещение отметки на промышленном изделии, при этом отметка содержит защитный идентификатор или идентификатор, полученный из защитного идентификатора.
2. Способ по п.1, отличающийся тем, что защитный идентификатор включает в себя уникальный идентификатор продукта.
3. Способ по п.2, отличающийся тем, что этап генерирования защитного идентификатора включает в себя генерирование первого идентификатора путем шифрования уникального идентификатора продукта вместе со значением системного шума и генерирование защитного идентификатора путем шифрования первого идентификатора вместе со значением физического шума.
4. Способ по п.3, отличающийся тем, что
 - этап генерирования первого идентификатора шифрованием уникального идентификатора продукта вместе со значением системного шума выполняют шифрованием (313) ключом обфускации генератора кода (ЗКГК);
 - первый идентификатор затем сочетают со значением физического шума и идентификатором генератора кода (233);
 - сочетание первого идентификатора, значения физического шума и идентификатора генератора кода затем шифруют (317) с помощью глобального ключа (235) для производства защитного идентификатора.
5. Способ по п.4, отличающийся тем, что ключ обфускации генератора кода является конкретным для генератора кода (111), на который он предварительно загружен, и при этом глобальный ключ является общим для всех производственных центров.

6. Способ по п.2, отличающийся тем, что этап генерирования защитного идентификатора включает в себя

генерирование первого защитного идентификатора путем шифрования уникального идентификатора продукта вместе со значением системного шума;

генерирование второго защитного идентификатора путем шифрования уникального идентификатора продукта вместе со значением физического шума и

размещение отметки на промышленном изделии, при этом отметка содержит первый и второй защитные идентификаторы или идентификатор или идентификаторы, полученные из первого и второго защитных идентификаторов.

7. Способ по п.6, в котором

значение системного шума сочетают с уникальным идентификатором продукта;

сочетание значения системного шума и уникального идентификатора продукта затем шифруют (343) с помощью ключа обфускации генератора кода (ЗКГК) для производства (241) первого идентификатора;

первый идентификатор затем сочетают с идентификатором генератора кода (ИГК) и шифруют (347) с помощью глобального ключа (235) для производства первого защитного идентификатора;

значение физического шума сочетают (351) с уникальным идентификатором продукта для производства второго идентификатора (261);

второй идентификатор шифруют с помощью глобального ключа (235) для производства второго защитного идентификатора (281).

8. Способ по п.6, дополнительно включающий в себя установление подлинности промышленного изделия в проверочном центре, при этом этап установления подлинности включает в себя

идентификацию отметки на изделии;

дешифрование отметки для получения уникального идентификатора продукта, системного шума и физического шума;

генерирование новой копии тайного ключа из уникального идентификатора продукта и одного или нескольких ключей шифрования;

генерирование новой копии значения системного шума путем выполнения хеш-функции на новой копии тайного ключа и уникальном идентификаторе продукта;

сравнение новой копии значения системного шума с полученным значением системного шума;

генерирование нового второго ключа шифрования из измеренного физического свойства промышленного изделия;

генерирование новой копии значения физического шума путем выполнения хеш-функции на новом втором ключе шифрования и полученном уникальном идентификаторе продукта;

сравнение новой копии значения физического шума с полученным значением физического шума и предоставление указания, идентична ли новая копия значения системного шума полученному значению системного шума и идентична ли или коррелирует ли новая копия значения физического шума полученному значению физического шума.

9. Способ по любому из предыдущих пунктов, отличающийся тем, что один или несколько ключей шифрования содержат статический ключ и динамический ключ, при этом новый динамический ключ создают для каждой партии промышленных изделий.

10. Способ по любому из предыдущих пунктов, отличающийся тем, что уникальный идентификатор продукта включает в себя информацию, идентифицирующую партию изделий, которой принадлежит изделие.

11. Способ по любому из предыдущих пунктов, в котором значение шума представляет собой значение хеша, или значение хеша с ключом, или значение или последовательность символов, полученные непосредственно из значения хеша и тайного ключа.

12. Способ по любому из предыдущих пунктов, в котором измеренное физическое свойство промышленного изделия основано на текстуре поверхности промышленного изделия.

13. Способ установления подлинности промышленного изделия, маркированного согласно способу по п.1, в проверочном центре, включающий в себя

идентификацию отметки на изделии;

дешифрование отметки для получения первого идентификатора и значения физического шума;

дешифрование первого идентификатора для получения уникального идентификатора продукта и значения системного шума;

генерирование нового второго ключа шифрования из измеренного физического свойства промышленного изделия;

генерирование новой копии значения физического шума путем выполнения хеш-функции на новом втором ключе шифрования и полученном уникальном идентификаторе продукта;

сравнение новой копии значения физического шума с полученным значением физического шума и предоставление указания, идентично или коррелирует ли полученное значение физического шума новой копии значения физического шума.

14. Способ по п.13, отличающийся тем, что установление подлинности дополнительно включает в себя

генерирование новой копии тайного ключа из уникального идентификатора продукта и одного или нескольких ключей шифрования;

генерирование новой копии значения системного шума путем выполнения хеш-функции на новой копии тайного ключа и уникальном идентификаторе продукта;

сравнение новой копии значения системного шума с полученным значением системного шума и предоставление указания, идентичны ли новая копия значения системного шума и полученное значение системного шума.

15. Устройство для маркирования промышленного изделия согласно способу по п.1, содержащее

генератор ключа, выполненный с возможностью генерировать ключи шифрования;

генератор кода, выполненный с возможностью генерировать уникальный идентификатор продукта для каждого промышленного изделия, причем уникальный идентификатор продукта включает в себя информацию, идентифицирующую партию изделий, к которой принадлежит изделие;

генератор второго ключа шифрования, выполненный с возможностью генерировать вторые ключи шифрования из измеренного физического свойства каждого промышленного изделия;

средство обработки, выполненное с возможностью

генерировать тайный ключ для каждого промышленного изделия с помощью уникального идентификатора продукта и одного или нескольких ключей шифрования;

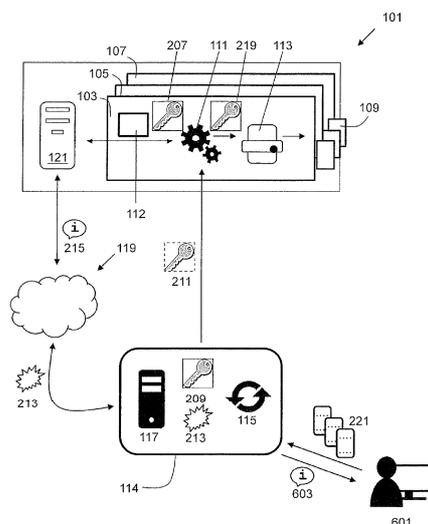
генерировать значение (225) системного шума для каждого промышленного изделия путем выполнения хеш-функции на тайном ключе и уникальном идентификаторе продукта;

генерировать значение (227) физического шума для каждого промышленного изделия путем выполнения хеш-функции на втором ключе шифрования и уникальном идентификаторе продукта, при этом для создания значения системного шума и значения физического шума способ использует преобразование, замещение, табличное замещение и индексирование или криптографическую хеш-функцию на сочетании уникального идентификатора продукта с тайным ключом и сочетании уникального идентификатора продукта со вторым ключом шифрования;

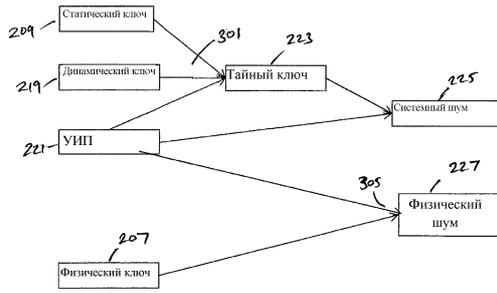
генерировать защитный идентификатор, полученный из тайного ключа и второго ключа шифрования или включающий в себя тайный ключ и второй ключ шифрования, при этом защитный идентификатор получен из значения системного шума и значения физического шума или он включает в себя значение системного шума и значение физического шума; и

маркер для маркирования каждого промышленного изделия защитным идентификатором или идентификатором, полученным из защитного идентификатора.

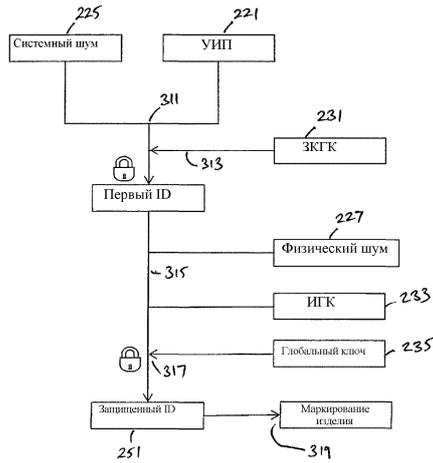
16. Устройство по п.15, в котором измеренное физическое свойство промышленного изделия основано на текстуре поверхности промышленного изделия.



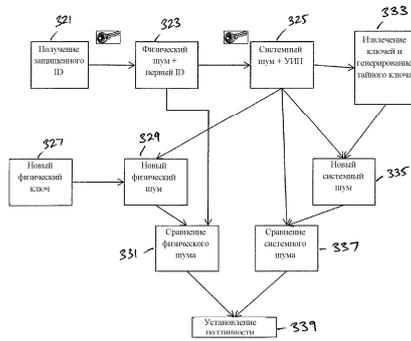
Фиг. 1



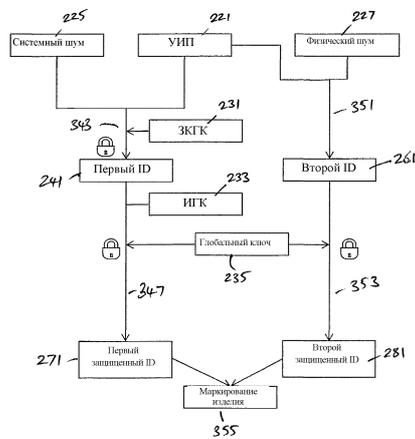
Фиг. 2



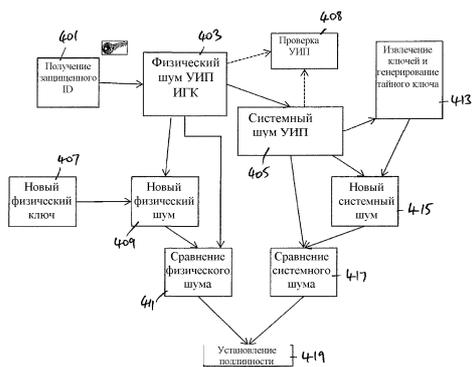
Фиг. 3



Фиг. 4



Фиг. 5



Фиг. 6

