РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2 452 009** (13) **C1**

(51) МПК
G06F 21/20 (2006.01)
H04L 9/14 (2006.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: **2010136824/08, 25.02.2009**

(24) Дата начала отсчета срока действия патента:
25.02.2009

Приоритет(ы):
(30) Конвенционный приоритет:
03.03.2008 KR 10-2008-0019844
30.06.2008 KR 10-2008-0063071

(45) Опубликовано: **27.05.2012** Бюл. № **15**

(56) Список документов, цитированных в отчете о поиске: **US 2006/0136989 A1, 22.06.2006. US 7286772 B2, 23.10.2007. US 2007/0160204 A1, 12.07.2007. US 2006/0133831 A1, 22.06.2006. RU 2289835 C2, 20.12.2006.**

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **02.09.2010**

(86) Заявка PCT:
KR 2009/000895 (25.02.2009)

(87) Публикация заявки PCT:
WO 2009/110693 (11.09.2009)

Адрес для переписки:
129090, Москва, ул. Б. Спасская, 25, стр.3, ООО "Юридическая фирма Городисский и Партнеры"

(72) Автор(ы):
ЛИ Дзае-Сунг (KR),
ЛИ Йоон-Тае (KR),
ЧО Вон-Ил (KR)

(73) Патентообладатель(и):
САМСУНГ ЭЛЕКТРОНИКС КО., ЛТД. (KR)

RU 2452009 C1

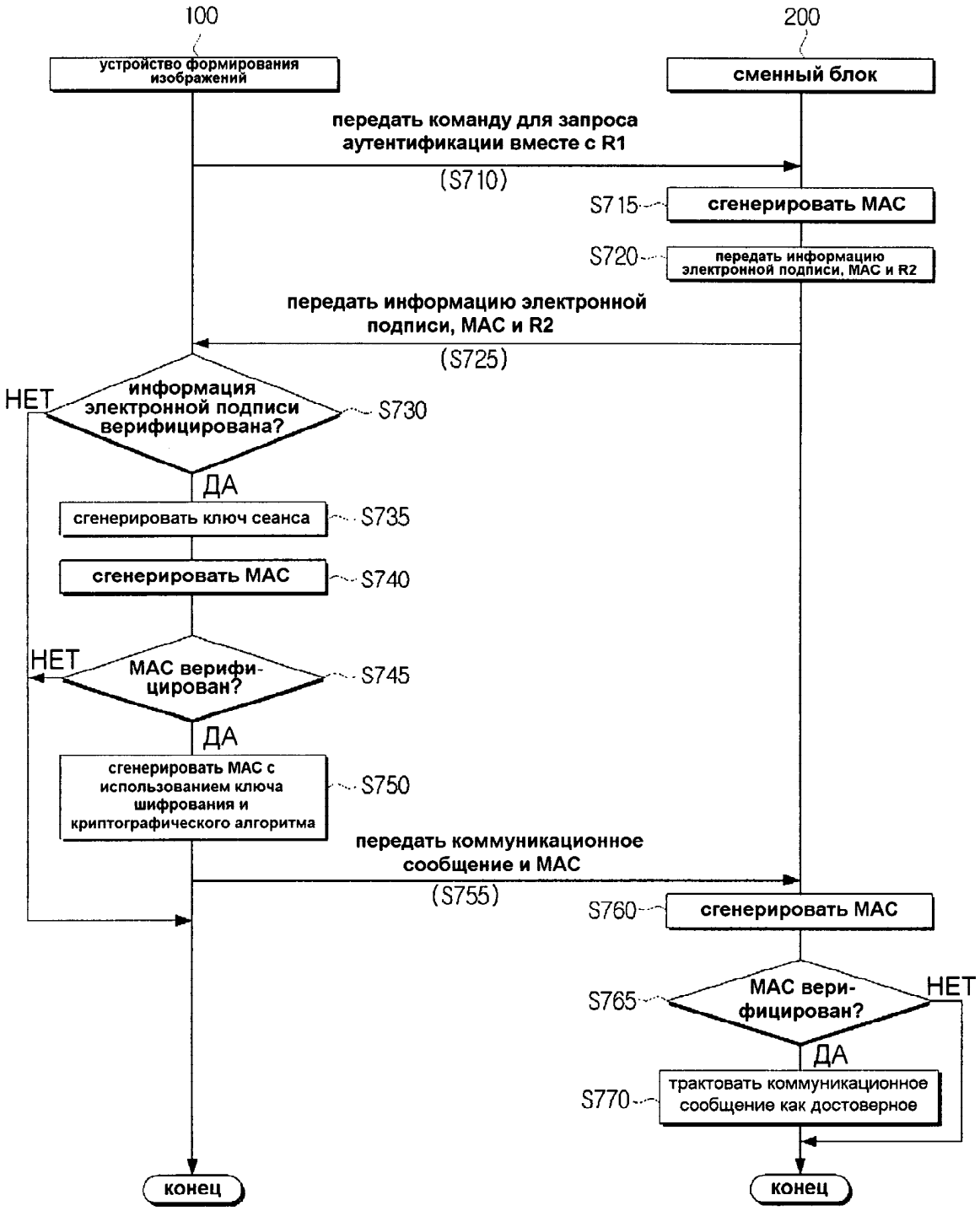
(54) БЛОК, ИСПОЛЬЗУЮЩИЙ ОПЕРАЦИОННУЮ СИСТЕМУ, И УСТРОЙСТВО ФОРМИРОВАНИЯ ИЗОБРАЖЕНИЙ, ИСПОЛЬЗУЮЩЕЕ ЕЕ

(57) Реферат:

Изобретение относится к блоку, включающему в себя встроенный центральный процессор (CPU), и устройству формирования изображений, использующему встроенный центральный процессор. Техническим результатом является повышение надежности данных, хранимых в блоке памяти, встроенном в блоке устройства формирования изображений. Кроме того, пользователи защищены от использования несертифицированного блока. Устройство формирования изображений содержит: основной корпус и сменный блок. Основной корпус содержит основной контроллер, который управляет операцией устройства формирования изображений. Сменный блок присоединен к основному корпусу и выполнен с возможностью выполнения операции формирования изображений с основным корпусом. При этом сменный блок содержит: блок памяти и центральный процессор (CPU). Блок памяти хранит программу инициализации, уникальную информацию, связанную со сменным блоком, и информацию о состоянии по использованию сменного

RU 2452009 C1

блока. CPU выполняет инициализацию, используя программу инициализации независимо от основного корпуса. Основной контроллер выполняет процесс аутентификации сменного блока. 5 н. и 37 з.п. ф-лы, 7 ил., 1 табл.



ФИГ.7

RU 2452009 C1

RU 2452009 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 452 009** (13) **C1**

(51) Int. Cl.
G06F 21/20 (2006.01)
H04L 9/14 (2006.01)

(12) ABSTRACT OF INVENTION

(21)(22) Application: **2010136824/08, 25.02.2009**

(24) Effective date for property rights:
25.02.2009

Priority:
(30) Convention priority:
03.03.2008 KR 10-2008-0019844
30.06.2008 KR 10-2008-0063071

(45) Date of publication: **27.05.2012 Bull. 15**

(85) Commencement of national phase: **02.09.2010**

(86) PCT application:
KR 2009/000895 (25.02.2009)

(87) PCT publication:
WO 2009/110693 (11.09.2009)

Mail address:
129090, Moskva, ul. B. Spasskaja, 25, str.3, OOO "Juridicheskaja firma Gorodisskij i Partnery"

(72) Inventor(s):
LI Dzae-Sung (KR),
LI Joon-Tae (KR),
ChO Von-Il (KR)

(73) Proprietor(s):
SAMSUNG EhLEKTRONIKS KO., LTD. (KR)

RU 2452009 C1

(54) UNIT USING OPERATING SYSTEM AND IMAGE FORMING APPARATUS USING SAID UNIT

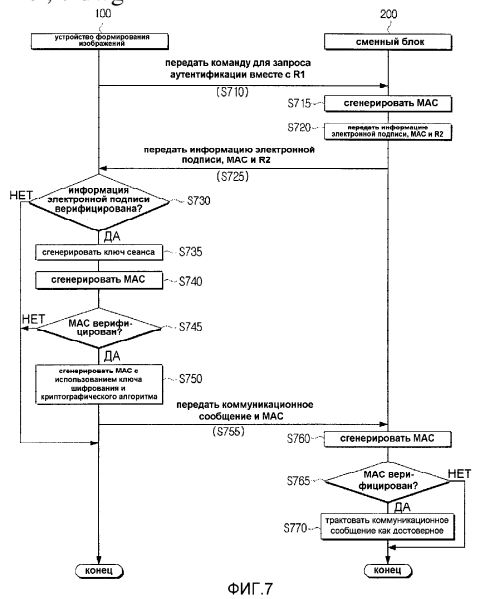
(57) Abstract:

FIELD: information technology.

SUBSTANCE: image forming apparatus comprises: a main housing and a detachable unit. The main housing has a main controller which controls operation of the image forming apparatus. The detachable unit is connected to the main housing and is configured to perform the image forming operation with the main housing. The detachable unit comprises: a memory unit and a central processing unit (CPU). The memory unit stores an initialisation program, unique information associated with the detachable unit, and status information on use of the detachable unit. The CPU performs initialisation using the initialisation program independent of the main housing. The main controller carries out a process of authenticating the detachable unit.

EFFECT: high reliability of data stored in the memory unit built into image forming apparatus; users are protected from use of an uncertified unit.

42 cl, 7 dwg



ФИГ.7

RU 2452009 C1

ОБЛАСТЬ ТЕХНИКИ

Данная общая идея изобретения относится к блоку, включающему в себя встроенный центральный процессор (CPU), и устройству формирования изображений, использующему встроенный центральный процессор. Более конкретно, данная общая идея изобретения относится к блоку, который становится более надежным, так как имеет CPU с операционной системой (OS), и устройству формирования изображений, использующему операционную систему.

УРОВЕНЬ ТЕХНИКИ

По мере того как компьютеры стали широко использоваться, периферийные устройства также стали широко распространенными. Примерами периферийных устройств являются устройства формирования изображений, такие как принтеры, сканеры, копиры и многофункциональные устройства.

Устройства формирования изображений используют чернила или тонер для печати изображений на бумагу. Чернила и тонер используются всякий раз, когда выполняются операции формирования изображений, пока красящий тонер не будет окончательно исчерпан. Если чернила или тонер пуст, то пользователь должен заменить блок для хранения чернил или тонера. Такие компоненты, которые являются сменными при использовании устройств формирования изображений, называются расходными материалами или сменными блоками.

Среди сменных блоков некоторые блоки, отличные от блоков, которые должны быть заменены при исчерпании чернил или тонера, должны быть заменены после использования в течение заданного периода времени. Это происходит, даже если чернила или тонер не исчерпаны, так как свойства этих блоков изменяются после заданного периода времени, и качество печати, таким образом, снижается.

Например, устройство формирования лазерных изображений включает в себя зарядное устройство, блок обмена, термофиксатор и т.д., и разные виды роликов и лент, используемые в каждом блоке, могут изнашиваться или повреждаться из-за использования сверх ограниченного срока службы. В результате, качество печати может заметно ухудшиться. Следовательно, пользователь должен заменять такие сменные блоки в соответствующее время.

Время для замены сменных блоков может быть определено с использованием показателя состояния использования. Показатель состояния использования представляет показатель для указания степеней использования устройства формирования изображений, например число листов бумаги, напечатанных устройством формирования изображений, и число точек, формирующих изображение. Устройство формирования изображений может определять время для замены сменных блоков посредством измерения числа листов бумаги, напечатанных устройством формирования изображений, или числа точек.

В последнее время, для того чтобы пользователь мог точно определить время для замены каждого сменного блока, каждый сменный блок включал в себя встроенную память контроля пользовательского сменного блока (CRUM память). Показатель состояния использования каждого сменного блока сохраняется в CRUM памяти. Соответственно, даже если каждый сменный блок является отдельным и используется в различных устройствах формирования изображений, состояние использования каждого сменного блока может быть точно определено.

Однако стандартный сменный блок, имеющий CRUM память, имеет проблему, что пользователи могут легко получить доступ к CRUM памяти. Информация, хранимая в CRUM памяти, является очень разнообразной, простираясь от базовой информации,

касающейся производителя, до информации, касающейся недавнего состояния использования. Если эта информация модифицирована, то сложно принять послепродажное обслуживание и вычислить адекватное время для замены сменного блока, что приводит к деградации операций формирования изображений. В частности, если информация, касающаяся производителя, модифицирована, то невозможно определить, является ли она аутентичной, и, таким образом, сложно управлять сменным блоком.

ОПИСАНИЕ ИЗОБРЕТЕНИЯ

ТЕХНИЧЕСКАЯ ЗАДАЧА

Данная общая идея изобретения обеспечивает блок, который становится более надежным, так как имеет встроенный CPU с операционной системой (OS) и устройство формирования изображений, использующее то же.

ТЕХНИЧЕСКОЕ РЕШЕНИЕ

Дополнительные особенности и полезности данной общей идеи изобретения будут изложены частично в описании, которое следует, и частично явствуют из этого описания, или могут быть изучены посредством применения на практике этой общей идеи изобретения.

Некоторый вариант осуществления данной общей идеи изобретения может быть достигнут посредством обеспечения микросхемы, которая может быть смонтирована на сменном блоке, используемом в устройстве формирования изображений, причем эта микросхема включает в себя центральный процессор (CPU) с операционной системой (OS) этого CPU, которая работает отдельно от OS устройства формирования изображений, для осуществления аутентичной связи с основным корпусом устройства формирования изображений, использующего OS этого CPU.

Этот CPU может осуществлять инициализацию с использованием OS этого CPU, работающую отдельно от основного корпуса устройства формирования изображений.

Эта инициализация может включать в себя по меньшей мере одну задачу среди начального запуска прикладных программ, вычисления секретной информации, необходимой для обмена данными с основным корпусом устройства формирования изображений после инициализации, установки канала связи, инициализации значений памяти, проверки своего собственного периода замены, установки внутренних значений регистров и установки внутренних/внешних синхросигналов.

Этот CPU может осуществлять обмен криптографическими данными по завершении аутентификации.

При принятии запроса аутентификации от основного корпуса устройства формирования изображений CPU может сгенерировать код аутентификации сообщения (MAC) и передать сгенерированный MAC и уникальную информацию цифровой подписи к основному корпусу устройства формирования изображений.

При принятии запроса аутентификации и первого случайного значения от основного корпуса устройства формирования изображений CPU может независимо сгенерировать второе случайное значение и сгенерировать ключ сеанса, использующий первое случайное значение, и после генерации кода аутентификации сообщения (MAC), использующего сгенерированный ключ сеанса, CPU может передать сгенерированный MAC, второе случайное значение и уникальную информацию цифровой подписи к основному корпусу устройства формирования изображений.

Когда устройство формирования изображений включается, или когда сменный блок с этой микросхемой смонтирован на устройстве формирования изображений, CPU

может выполнить инициализацию согласно OS этого CPU и не отвечает на команду от основного корпуса устройства формирования изображений перед завершением инициализации и выполняет аутентификацию при завершении инициализации.

Микросхема может дополнительно включать в себя блок памяти для хранения информации, касающейся по меньшей мере одной из микросхем, сменного блока, блока памяти контроля пользователем сменного блока (CRUM), смонтированного на сменном блоке, в котором может быть смонтирована эта микросхема, и OS этого CPU.

OS этого CPU может запускать по меньшей мере одно из микросхемы, CRUM блока и сменного блока, и OS этого CPU может быть программным обеспечением, которое выполняет по меньшей мере одно из операции инициализации для независимой инициализации одного состояния микросхемы, CRUM блока и сменного блока, операции обработки для выполнения общедоступного криптографического алгоритма и операции взаимной аутентификации с основным корпусом устройства формирования изображений.

Микросхема может дополнительно включать в себя детектор фальсификации для ответа на попытки хакерства и криптоблок для того, чтобы позволить CPU выполнить аутентификацию на основном корпусе устройства формирования изображений посредством применения предварительно заданного криптографического алгоритма среди некоторого множества криптографических алгоритмов.

Криптографический алгоритм, применяемый для аутентификации, может быть изменяемым.

CPU может принять значения степеней расходных материалов, используемых для задания формирования изображений от основного корпуса устройства формирования изображений, когда задание формирования изображений выполняется с использованием сменного блока, и CPU добавляет эти значения к информации по использованию расходных материалов, хранимой в блоке памяти, и затем обновляет информацию по использованию расходных материалов, хранимую в блоке памяти.

Некоторый вариант осуществления данной общей идеи изобретения может быть достигнут посредством обеспечения CRUM блока, который может использоваться для устройства формирования изображений, причем этот CRUM блок включает в себя блок памяти для хранения информации, касающейся блока, на котором смонтирован этот CRUM блок, и CPU для управления этим блоком памяти, использующий операционную систему (OS) этого CPU, которая работает отдельно от OS устройства формирования изображений, и для осуществления аутентичной связи с основным корпусом устройства формирования изображений.

Этот CPU может осуществлять инициализацию с использованием OS этого CPU, работающую отдельно от основного корпуса устройства формирования изображений.

Эта инициализация может включать в себя по меньшей мере одну задачу среди начального запуска прикладных программ, вычисления секретной информации, необходимой для обмена данными с основным корпусом устройства формирования изображений после инициализации, установки канала связи, инициализации значений памяти, проверки своего собственного периода замены, установки внутренних значений регистров и установки внутренних/внешних синхросигналов.

OS этого CPU может запускать CRUM блок или сменный блок, и OS этого CPU может быть программным обеспечением, которое выполняет по меньшей мере одно из операции инициализации для независимой инициализации одного состояния микросхемы, CRUM блока или сменного блока, операции обработки для выполнения

общедоступного криптографического алгоритма и операции взаимной аутентификации с основным корпусом устройства формирования изображений.

CPU может выполнять аутентификацию и выполняет обмен криптографическими данными по завершении аутентификации.

При принятии запроса аутентификации от основного корпуса устройства формирования изображений CPU может сгенерировать код аутентификации сообщения (MAC) и передать сгенерированный MAC и уникальную информацию цифровой подписи к основному корпусу устройства формирования изображений.

При принятии запроса аутентификации и первого случайного значения от основного корпуса устройства формирования изображений CPU может независимо сгенерировать второе случайное значение и сгенерировать ключ сеанса, использующий первое случайное значение, и после генерации кода аутентификации сообщения (MAC), использующего сгенерированный ключ сеанса, CPU может передать сгенерированный MAC, второе случайное значение и уникальную информацию цифровой подписи к основному корпусу устройства формирования изображений.

Когда устройство формирования изображений включено, или блок, смонтированный с CRUM блоком, смонтирован на устройстве формирования изображений, OS этого CPU может выполнить инициализацию и не отвечает на команду от основного корпуса устройства формирования изображений перед завершением инициализации.

CRUM блок может дополнительно включать в себя интерфейсный блок для подключения устройства формирования изображений к CPU, детектор фальсификации для ответа на попытки физического хакерства и криптоблок для того, чтобы позволить CPU выполнить аутентификацию на устройстве формирования изображений посредством применения предварительно заданного криптографического алгоритма среди некоторого множества криптографических алгоритмов.

Криптографический алгоритм, применяемый для аутентификации, может быть изменяемым.

CPU может принять значения степеней расходных материалов, используемых для задания формирования изображений, когда задание формирования изображений выполняется от основного корпуса устройства формирования изображений, и CPU добавляет эти значения к информации по использованию расходных материалов, хранимой в блоке памяти, и затем обновляет информацию по использованию расходных материалов, хранимую в блоке памяти.

Некоторый вариант осуществления данной общей идеи изобретения может быть достигнут посредством обеспечения сменного блока, который также может быть смонтирован на устройстве формирования изображений, причем этот сменный блок включает в себя блок памяти для хранения информации на этом сменном блоке, и CPU для управления этим блоком памяти, использующий операционную систему (OS) этого CPU, которая работает отдельно от OS устройства формирования изображений, и для осуществления аутентичной связи с основным корпусом устройства формирования изображений.

Этот CPU может осуществлять инициализацию с использованием OS этого CPU, работающую отдельно от основного корпуса устройства формирования изображений.

Эта инициализация может включать в себя по меньшей мере одну задачу среди начального запуска прикладных программ, вычисления секретной информации,

необходимой для обмена данными с основным корпусом устройства формирования изображений после инициализации, установки канала связи, инициализации значений памяти, проверки своего собственного периода замены, установки внутренних значений регистров и установки внутренних/внешних синхросигналов.

OS этого CPU может запускать CRUM блок или сменный блок, и OS этого CPU может быть программным обеспечением, которое выполняет по меньшей мере одно из операции инициализации для независимой инициализации одного состояния микросхемы, CRUM блока или сменного блока, операции обработки для выполнения общедоступного криптографического алгоритма и операции взаимной аутентификации с основным корпусом устройства формирования изображений.

CPU может выполнять обмен криптографическими данными, когда аутентификация между основным корпусом устройства формирования изображений и сменным блоком завершена.

При принятии запроса аутентификации от основного корпуса устройства формирования изображений CPU может сгенерировать код аутентификации сообщения (MAC) и передать сгенерированный MAC и уникальную информацию цифровой подписи к основному корпусу устройства формирования изображений.

При принятии запроса аутентификации и первого случайного значения от основного корпуса устройства формирования изображений CPU может независимо сгенерировать второе случайное значение и сгенерировать ключ сеанса, использующий первое случайное значение, и после генерации кода аутентификации сообщения (MAC), использующего сгенерированный ключ сеанса, CPU может передать сгенерированный MAC, второе случайное значение и уникальную информацию цифровой подписи к основному корпусу устройства формирования изображений.

Когда устройство формирования изображений включено, или сменный блок смонтирован на устройстве формирования изображений, OS этого CPU может выполнить инициализацию согласно своей собственной OS и не отвечает на команду от основного корпуса устройства формирования изображений перед завершением инициализации.

Сменный блок может дополнительно включать в себя интерфейсный блок для подключения устройства формирования изображений к CPU, детектор фальсификации для ответа на попытки физического хакерства и криптоблок для того, чтобы позволить CPU выполнить аутентификацию или обмен криптографическими данными с устройством формирования изображений посредством применения предварительно заданного криптографического алгоритма среди некоторого множества криптографических алгоритмов.

Криптографический алгоритм, применяемый для аутентификации, может быть изменяемым.

CPU может принять значения степеней расходных материалов, используемых для задания формирования изображений, когда задание формирования изображений выполняется от основного корпуса устройства формирования изображений, и CPU добавляет эти значения к информации по использованию расходных материалов, хранимой в блоке памяти, и затем обновляет информацию по использованию расходных материалов, хранимую в блоке памяти.

Некоторый вариант осуществления данной общей идеи изобретения может быть достигнут посредством обеспечения устройства формирования изображений, включающего в себя основной контроллер, и по меньшей мере одного блока, который

включает в себя блок памяти для хранения информации и CPU для управления этим блоком памяти с использованием операционной системы (OS) этого CPU, работающей отдельно от OS основного контроллера, и для выполнения по меньшей мере одного из аутентификации и обмена криптографическими данными с основным контроллером.

CPU может выполнять инициализацию с использованием OS этого CPU, работающей отдельно от основного контроллера.

Эта инициализация может включать в себя по меньшей мере одну задачу среди начального запуска прикладных программ, вычисления секретной информации, необходимой для обмена данными с основным корпусом устройства формирования изображений после инициализации, установки канала связи, инициализации значений памяти, проверки своего собственного периода замены, установки внутренних значений регистров и установки внутренних/внешних синхросигналов.

Этот по меньшей мере один блок может выполнять аутентификацию на основном контроллере с использованием предварительно заданного криптографического алгоритма, причем этот криптографический алгоритм является изменяемым.

Основной контроллер может запросить аутентификацию к CPU по меньшей мере одного блока, и когда информация цифровой подписи и MAC передаются от CPU, основной контроллер может детектировать эту информацию цифровой подписи и MAC для выполнения аутентификации.

Основной контроллер может сгенерировать первое случайное значение и затем передать это первое случайное значение и запрос аутентификации к CPU по меньшей мере одного блока, детектировать информацию цифровой подписи, когда информация цифровой подписи принята, принять первый MAC и второе случайное значение от CPU в качестве реакции на запрос аутентификации, независимо сгенерировать ключ сеанса и второй MAC с использованием первого и второго случайных значений и сравнить и детектировать сгенерированный второй MAC и принятый первый MAC.

Основной контроллер может принять уникальную информацию цифровой подписи, установленную для каждого блока из по меньшей мере одного блока, и выполнить аутентификацию и выполнить обмен криптографическими данными с соответствующими CPU каждого блока, когда аутентификация имела успех.

Основной контроллер может выполнить аутентификацию посредством применения RSA алгоритма с асимметричным ключом и алгоритма ARIA, алгоритмов с симметричным ключом стандартов тройного шифрования данных (TDES), SEED и усовершенствованных стандартов шифрования (AES), и CPU блока может выполнить аутентификацию посредством применения одного из ARIA, TDES, SEED, AES алгоритмов с симметричным ключом.

Этот блок может дополнительно включать в себя криптоблок для того, чтобы позволить CPU выполнить аутентификацию или обмен криптографическими данными с основным контроллером устройства формирования изображений посредством применения установленного криптографического алгоритма среди множества криптографических алгоритмов, и детектор фальсификации для ответа на попытки физического хакерства.

Основной контроллер может быть подключен по меньшей мере к одному блоку через один последовательный I/O канал и может быть доступен по меньшей мере для одного блока с использованием индивидуальных адресов, данных каждому блоку.

Когда это задание выполнено, основной контроллер может измерить значения степеней расходных материалов, используемых для этого задания, передать измеренные значения к каждому CPU по меньшей мере одного блока, добавить эти

значения к информации по использованию расходных материалов, предварительно сохраненной в каждом CPU, и затем обновить информацию по использованию расходных материалов, хранимую в блоке памяти.

OS этого CPU может запустить этот блок, и OS этого CPU может быть программным обеспечением, которое выполняет по меньшей мере одно из операции инициализации, операции обработки для выполнения общедоступного криптографического алгоритма и операции взаимной аутентификации с основным корпусом устройства формирования изображений.

Этим блоком может быть одно из сменного блока, непосредственно связанного с заданием формирования изображений устройства формирования изображений, CRUM блока, монтируемой на сменном блоке, и микросхемы, монтируемой на CRUM блоке.

Некоторый вариант осуществления данной общей идеи изобретения может быть также достигнут посредством обеспечения считываемого компьютером носителя для содержания считываемых компьютером кодов как некоторой программы для выполнения некоторого способа, причем этот способ включает в себя выполнение аутентичной связи с основным корпусом устройства формирования изображений, использующего операционную систему (OS) некоторого центрального процессора (CPU), которая работает отдельно от OS устройства формирования изображений.

Некоторый вариант осуществления данной общей идеи изобретения может быть также достигнут посредством обеспечения микросхемы, которая является монтируемой на сменном блоке, используемом в устройстве формирования изображений, причем эта микросхема включает в себя центральный процессор (CPU) с операционной системой (OS) этого CPU, которая работает отдельно от OS устройства формирования изображений, для выполнения аутентичной связи с основным корпусом устройства формирования изображений, использующего OS этого CPU, и блок памяти для хранения информации, касающейся по меньшей мере одного из этой микросхемы, блока контроля пользователем сменного блока (CRUM), сменного блока с CRUM блоком, и OS этого CPU, где OS этого CPU обеспечена в этом блоке памяти в пределах этой микросхемы или в памяти, внешней к этой микросхеме.

Согласно примерным вариантам осуществления данной общей идеи изобретения, CPU со своей собственной операционной системой (OS) смонтирован в этом блоке, так что этот блок может управлять блоком памяти независимо. Этим блоком может быть микросхема, CRUM блок или сменный блок. Эта OS запускается таким образом, что могут быть выполнены инициализация, запуск криптографического алгоритма и аутентификация с основным корпусом устройства формирования изображений.

Даже когда основной ключ не сохранен в устройстве формирования изображений, имеющем этот блок, устройство формирования изображений может выполнить аутентификацию или обмен криптографическими данными с этим блоком. Следовательно, может быть предотвращено рассеяние основного ключа. Аутентификация или обмен криптографическими данными могут быть выполнены с использованием MAC, сгенерированного на основе некоторого случайного значения, и информации электронной подписи. Эта аутентификация выполняется посредством применения алгоритмов как с симметричным, так и с асимметричным ключом, так что эта криптография обеспечивает надежность данных высокого уровня.

Некоторое множество криптографических алгоритмов может быть избирательно применено для аутентификации и обмена криптографическими данными. Даже если используемый в настоящее время криптографический алгоритм атакован посредством

физического хакерства, этой атаке можно воспрепятствовать посредством замены используемого в настоящее время ключа на ключ, применяющий другой криптографический алгоритм, без замены этого блока на новый блок.

Если используется некоторое множество блоков, то информация электронной подписи устанавливается для каждого блока. Индивидуальные адреса даются каждому блоку, и, таким образом, этот блок может быть подключен к устройству формирования изображений через некоторый последовательный интерфейс. Аутентификация и обмен криптографическими данными между этим множеством блоков эффективно достигаются.

Если задание формирования изображений завершено, то устройство формирования изображений измеряет степени расходных материалов, используемых для этого задания формирования изображений, и передает измеренные значения к каждому из множества блоков. Следовательно, препятствуют записи некорректной информации, касающейся степеней используемых расходных материалов, из-за ошибок.

ТЕХНИЧЕСКИЙ РЕЗУЛЬТАТ

В результате, препятствуют копированию или дублированию данных, хранимых в блоке памяти, встроенном в блоке устройства формирования изображений, и надежность этих данных повышается. Пользователи также защищены от использования несертифицированного блока.

КРАТКОЕ ОПИСАНИЕ ЧЕРТЕЖЕЙ

Эти и/или другие особенности и полезности данной общей идеи изобретения явствуют и легко понятны из соответствующего описания вариантов осуществления, взятого вместе с сопутствующими чертежами, из которых:

Фиг.1 является схематичной блок-схемой, иллюстрирующей некоторую конфигурацию устройства формирования изображений, включающую в себя сменный блок согласно некоторому примерному варианту осуществления данной общей идеи изобретения;

Фиг.2 является подробной блок-схемой, иллюстрирующей некоторую конфигурацию сменного блока согласно некоторому примерному варианту осуществления данной общей идеи изобретения;

Фиг.3 является схематичной блок-схемой, иллюстрирующей некоторую конфигурацию устройства формирования изображений согласно некоторому примерному варианту осуществления данной общей идеи изобретения;

Фиг.4 является схематичной блок-схемой, иллюстрирующей некоторую конфигурацию программного обеспечения, которая встроена в устройство формирования изображений и сменный блок согласно некоторому примерному варианту осуществления данной общей идеи изобретения;

Фиг.5 является блок-схемой, иллюстрирующей способ управления сменным блоком и устройством формирования изображений согласно некоторому примерному варианту осуществления данной общей идеи изобретения;

Фиг.6 является блок-схемой, иллюстрирующей процесс изменения криптографических алгоритмов посредством сменного блока согласно некоторому примерному варианту осуществления данной общей идеи изобретения; и

Фиг.7 является блок-схемой, иллюстрирующей способ выполнения аутентификации и обмена криптографическими данными между устройством формирования изображений и сменным блоком согласно некоторому примерному варианту осуществления данной общей идеи изобретения.

СПОСОБ ОСУЩЕСТВЛЕНИЯ ИЗОБРЕТЕНИЯ

Теперь будет сделана подробная ссылка на варианты осуществления данной общей идеи изобретения, примеры которых показаны в сопутствующих чертежах, где подобные ссылочные позиции относятся к подобным элементам везде. Эти варианты осуществления описаны ниже для того, чтобы объяснить данную общую идею изобретения посредством ссылки на эти чертежи.

Фиг.1 является схематичной блок-схемой, иллюстрирующей некоторую конфигурацию устройства формирования изображений, включающую в себя сменный блок согласно некоторому примерному варианту осуществления данной общей идеи изобретения. Как показано на фиг.1, устройство 100 формирования изображений включает в себя основной контроллер 110, и блок 200 может быть встроен в устройство 100 формирования изображений. Устройством 100 формирования изображений может быть копир, принтер, многофункциональное периферийное устройство, факсимильная машина или сканер.

Устройство 100 формирования изображений может включать в себя OS 115 для управления операциями устройства 100 формирования изображений. Блок 200 представляет компонент, который сконструирован с возможностью независимой установки и использования. Более конкретно, блоком 200 может быть сменный блок, включающий в себя по меньшей мере один сменный элемент 215, который образован в устройстве формирования изображений и непосредственно вмешивается в операцию формирования изображения. Например, по меньшей мере одним сменным элементом 215 сменного блока 200 может быть тонер или красящий картридж, зарядное устройство, блок обмена, термофиксатор, органический фотопроводник (OPC), подающий блок или подающий ролик и т.д.

Кроме того, блоком 200 может быть другой компонент, который является необходимым для устройства 100 формирования изображений и является сменным во время использования. А именно, блоком 200 может быть устройство контроля пользователем сменного блока (CRUM), которое может контролировать и управлять состоянием некоторого компонента, будучи включенным в сменный блок, или может быть микросхема, встроенная в CRUM. Блок 200 может быть реализован в разных формах, но для удобства описания блок 200 описывается ниже как реализованный в виде сменного блока.

Основной контроллер 110 может иметь некоторый интерфейс для связи с внешним устройством (не показано) для принятия данных и может выполнять операцию формирования изображения с использованием принятых данных. Основной контроллер 110 может быть также подключен к факсимильному устройству или сканирующему устройству, например, для принятия или передачи данных, соответствующих операции формирования изображения.

Устройство 100 формирования изображений может включать в себя блок 150 формирования изображений для выполнения операции формирования изображения с использованием блока 200. Блок 200 может быть частью блока 150 формирования изображений, когда он установлен в корпусе устройства 100 формирования изображений. Основной контроллер 110 может управлять блоком 210 памяти и блоком 150 формирования изображений для подачи носителя в устройство формирования изображений для формирования изображения на этом носителе и для выгрузки этого носителя.

Как показано на фиг.1, блок 200 включает в себя блок 210 памяти и центральный процессор (CPU) 220.

Блок 210 памяти хранит разные типы информации, касающейся блока 200 и, более

конкретно, хранит уникальную информацию, такую как информация, касающаяся производителя блока 200, информация, касающаяся времени изготовления, порядковый номер или номер модели, разнообразные программы, информация, касающаяся электронной подписи, информация о состоянии, касающаяся состояния использования (например, сколько листов бумаги было отпечатано до настоящего времени, какова остающаяся способность печати, или сколько тонера осталось).

Например, блок 210 памяти может хранить информацию, показанную в следующей Таблице 1.

Таблица 1

Общая информация	
Версия OS Версия SPL-C Версия машины Порядковый номер USB Установленная модель Дата начала обслуживания	CLP300_V1.30.12.35 02-22-20075.24 06-28-20066.01.00(55)BH45BAIP914466 B.DOM2007-09-29
Вариант	
Размер ЗУПВ Размер ЭСППЗУ Подключенный USB (высокий)	32 мегабайта 4096 байтов
Срок службы расходных материалов	
Общий счетчик страниц Срок службы термофиксатора Срок службы роликов лотка 1 Общий счетчик изображений Срок службы блока формирования изображений/роликов носителя Срок службы ленты обмена Счетчик изображений тонера	774/93 страниц (цветн./монохр.) 1636 страниц 864 страницы 867 страниц 3251 изображений 61 изображение/19 страниц 3251 изображение 14/9/14/19 изображений (C/M/Y/K)
Информация о тонере	
Процент остающегося тонера Среднее покрытие тонера	99%/91%/92%/100% (C/M/Y/K)5%/53%/31%/3%(C/M/Y/K)
Информация о расходных материалах	
Бирюзовый тонер Малиновый тонер Желтый тонер Черный тонер Блок формирования изображений	SAMSUNG(DOM) SAMSUNG(DOM) SAMSUNG(DOM) SAMSUNG(DOM) SAMSUNG(DOM)
Цветовое меню	
Чистый цвет	Ручная регулировка(CMYK:0,0,0,0)
Меню настройки	
Экономия энергии Автопродолжение Регулировка высоты	20 минут Включено Обыкновенная

Как показано в вышеприведенной Таблице 1, блок 210 памяти может хранить разнообразную информацию, касающуюся срока службы расходных материалов, и меню настройки, а также схематичную информацию, касающуюся блока 200. Блок 210 памяти может также хранить информацию операционной системы (OS) для обработки данных, хранящихся в нем таким образом, что основной контроллер 110 может управлять блоком 150 формирования изображений и блоком 200 для выполнения операции формирования изображения.

CPU 220 управляет блоком 210 памяти с использованием операционной системы (OS) CPU 220. Эта OS, которая обеспечена для управления блоком 200, представляет собой программное обеспечение для управления общими прикладными программами. Соответственно, CPU 220 может выполнять самоинициализацию с использованием OS.

Более подробно, CPU 220 выполняет инициализацию во время конкретных событий, например, когда устройство 100 формирования изображений, включающее в себя блок 200, включается, или когда блок 200 или компонент, включающий в себя блок 200, такой как сменный блок, присоединяется к устройству 100 формирования изображений или отсоединяется от него. Инициализация включает в себя начальный запуск разнообразных прикладных программ, используемых в блоке 200, вычисление секретной информации, необходимой для обмена данными с устройством формирования изображений после инициализации, настройку канала связи, инициализацию значения памяти, подтверждение времени замены, установку значений регистров в блоке 200 и установку внутренних и внешних синхросигналов.

Установка значений регистров представляет собой установку функциональных

значений регистров в блоке 200 для того, чтобы блок 200 работал в том же самом состоянии, которое ранее установил пользователь. Кроме того, установка внутренних и внешних синхросигналов представляет собой настройку частоты внешнего синхросигнала, обеспечиваемого от основного контроллера 110 устройства 100 формирования изображений, на частоту внутреннего синхросигнала, подлежащего использованию в CPU 220 блока 200.

Подтверждение времени замены представляет собой проверку оставшейся величины тонера или чернил в использовании, что предупреждает о времени, когда тонер или чернила будут исчерпаны, и уведомляет основной контроллер 110 об этом времени. Если во время инициализации определено, что тонер уже был исчерпан, то после завершения инициализации блок 200 может быть реализован с возможностью автоматического уведомления основного контроллера 110 о том, что операция не может быть выполнена. В других случаях, поскольку блок 200 включает в себя OS CPU 220, разнообразные формы инициализации могут быть выполнены согласно типу или характеристике блока 200.

Такая инициализация выполняется самим блоком 200 и, таким образом, выполняется отдельно от инициализации, выполняемой основным контроллером 110 устройства 100 формирования изображений.

Как описано выше, CPU 220 встроено в блок 200, и блок 200 имеет свою собственную OS, так что если устройство 100 включается, то основной контроллер 110 может проверить оставшуюся величину расходных материалов и число повторных заполнений, которые хранятся в блоке 210 памяти, перед запрашиванием связи с блоком 200. Следовательно, информирование основного контроллера 110 о том, что расходные материалы не должны быть заменены, занимает более короткое время. Например, если тонера недостаточно, то пользователь может включить устройство 100 формирования изображений и преобразовать устройство 100 непосредственно в режим экономии тонера. Пользователь может также выполнить ту же самую операцию, даже когда недостаточно только одного конкретного тонера.

CPU 220 не отвечает на команды основного контроллера 110, пока не завершится инициализация. Основной контроллер 110 периодически передает команды к CPU 220, пока основной контроллер 110 не примет ответ от CPU 220.

Если основной контроллер 110 принимает ответ, а именно подтверждение, то между основным контроллером 110 и CPU 220 инициируется аутентификация.

В этом случае OS в блоке 200 позволяет осуществить аутентификацию посредством взаимодействия между блоком 200 и устройством 100 формирования изображений. Однако для того, чтобы устройство формирования изображений выполнило аутентификацию, основной контроллер устройства формирования изображений односторонним образом получает доступ к этому блоку, идентифицирует уникальную информацию для аутентификации и сравнивает эту уникальную информацию с сохраненной информацией.

Однако, в данной общей идее изобретения, основной контроллер 110 в устройстве 100 формирования изображений выполняет свою собственную инициализацию отдельно от инициализации блока 200. Инициализация блока 200 завершается первой из-за различий в размере этих систем. Если инициализация блока 200 завершена, то блок 200 может запустить криптографический алгоритм, использующий OS. Более конкретно, блок 200 может запустить криптографический алгоритм в качестве реакции на команду основного контроллера 110 таким образом, что может быть выполнена интерактивная аутентификация между основным

контроллером 110 и блоком 200, а не односторонняя аутентификация основного контроллера 110. Следовательно, повышается надежность аутентификации.

Такая аутентификация не ограничена примером, описанным выше, и может быть выполнена в разных формах. Например, основной контроллер 110 может принять ответ от CPU 220 и передать команду к CPU 220, запрашивающую аутентификацию. В этом случае, как показано на фиг.1 и 7, случайное значение R1 может быть передано к CPU 220 сменного блока 200 вместе с этой командой. CPU 220 принимает этот запрос аутентификации и случайное значение R1, генерирует ключ сеанса, использующий случайное значение R1, генерирует первый код аутентификации сообщения (MAC), использующий сгенерированный ключ сеанса, и передает сгенерированный первый MAC, предварительно сохраненную информацию электронной подписи и случайное значение R2 к основному контроллеру 110.

Если основной контроллер 110 идентифицирует аутентичность посредством верификации первого MAC, принятой информации электронной подписи, то основной контроллер 110 генерирует ключ сеанса, использующий принятое случайное значение R2 и предварительно сгенерированное случайное значение R1, и генерирует второй MAC, использующий этот ключ сеанса. Наконец, основной контроллер 110 верифицирует второй MAC посредством идентификации того, является ли сгенерированный второй MAC тем же самым, что и принятый первый MAC. В результате, основной контроллер 110 может определить, была ли аутентификация успешно выполнена. Как описано выше, поскольку случайные значения используются после передачи информации или команд для аутентификации, враждебное хакерство третьей стороны может быть предотвращено.

Если аутентификация успешно выполнена, то между основным контроллером 110 и CPU блока 200 выполняется обмен криптографическими данными. Как описано выше, поскольку блок 200 имеет свою собственную OS, может быть выполнен криптографический алгоритм. Следовательно, достоверность данных может быть определена посредством применения криптографического алгоритма к данным, принятым от устройства 100 формирования изображений. В результате этого определения, если данные достоверны, то блок 200 принимает эти данные и выполняет операцию по обработке этих данных. Если данные не достоверны, то блок 200 может отбросить эти данные при их принятии. В этом случае блок 200 может уведомить основной контроллер 110 о том, что существует проблема в обмене данными.

Криптографический алгоритм может использовать общедоступный стандартный криптографический алгоритм. Такой криптографический алгоритм может быть модифицирован, когда ключ шифрования открывается, или когда необходимо усиление надежности.

В вышеприведенном варианте осуществления данной общей идеи изобретения, поскольку блок 200 имеет свою собственную OS и свою собственную инициализацию, аутентификация и обмен криптографическими данными между блоком 200 и устройством 100 формирования изображений могут быть эффективно выполнены.

Фиг.2 является подробной блок-схемой, иллюстрирующей сменный блок 200 устройства 100 формирования изображений, иллюстрированного на фиг.1. Сменный блок 200 фиг.2 включает в себя криптоблок 230, детектор 240 фальсификации и интерфейсный блок 250 в дополнение к ранее обсужденному блоку 210 памяти и CPU 220. Кроме того, сменный блок 200 может дополнительно включать в себя блок синхронизации (не показан) для вывода синхросигнала или генератор случайных значений (не показан) для генерации случайных значений для аутентификации.

Сменный блок 200, обсуждаемый здесь, может включать в себя меньшее или большее число компонентов, в зависимости от приложения. Далее, если сменный блок 200 реализован как полупроводниковая микросхема или блок полупроводниковых микросхем, то эта микросхема или блок микросхем может включать в себя либо CPU 220 сам по себе, либо может включать в себя как блок 210 памяти, так и CPU 220. Если микросхема включает в себя только CPU 220, то OS, исполняемая посредством CPU 220, может быть обеспечена посредством внешней памяти.

Криптоблок 230 поддерживает некоторый криптографический алгоритм и вызывает выполнение CPU 220 аутентификации или обмена криптографическими данными с основным контроллером 110. Конкретно, криптоблок 230 может поддерживать один из четырех криптографических алгоритмов, включающих в себя алгоритмы с симметричным ключом стандарта ARIA, стандарта тройного шифрования данных (TDES), SEED и усовершенствованного стандарта шифрования (AES).

Для выполнения аутентификации или обмена криптографическими данными основной контроллер 110 также поддерживает эти четыре криптографических алгоритма. Соответственно, основной контроллер 110 может определить, какой криптографический алгоритм применяется сменным блоком 200, может выполнить аутентификацию с использованием этого определенного криптографического алгоритма и может затем выполнить обмен криптографическими данными с CPU 220. В результате, сменный блок 200 может быть легко смонтирован в устройстве 100 формирования изображений таким образом, что обмен криптографическими данными может быть выполнен, даже когда сгенерирован ключ, к которому применяется некоторый криптографический алгоритм.

Детектор 240 фальсификации препятствует различным атакам физического хакерства, а именно фальсификации. Более конкретно, если некоторая атака детектирована посредством контроля рабочих условий, таких как напряжение, температура, давление, свет или частота, то детектор 240 фальсификации может удалить данные, относящиеся к этой атаке, или может физически воспрепятствовать этой атаке. В этой ситуации детектор 240 фальсификации может включать в себя дополнительный источник питания для подачи энергии для поддержания его работы. Этой атакой может быть атака нарушения способности, которая может быть потенциально повреждающей атакой на CRUM блок 200, например.

Как описано выше, сменный блок 200 включает в себя криптоблок 230 и детектор 240 фальсификации, так что можно систематически предохранять данные с использованием либо аппаратного, либо программного обеспечения, либо обоих.

Со ссылкой на фиг.2 блок 210 памяти может включать в себя по меньшей мере одно из OS памяти 211, энергонезависимой памяти 212 и энергозависимой памяти 213.

OS память 211 хранит OS для управления сменным блоком 200. Энергонезависимая память 212 хранит данные в энергонезависимой форме, и энергозависимая память 213 используется как временное пространство хранения, необходимое для операций. Хотя блок 210 памяти включает в себя OS память 211, энергонезависимую память 212 и энергозависимую память 213, как показано на фиг.2, некоторые из этих ЗУ могут быть встроены в CPU 220 как внутренние ЗУ. OS память 211, энергонезависимая память 212 и энергозависимая память 213 могут быть реализованы согласно некоторой конструкции для надежности, такой как скремблирование адресов/линий данных или шифрование битов, отличным образом от общих ЗУ.

Энергонезависимая память 212 может хранить разнообразие информации, такой как информация цифровой подписи, информация, касающаяся различных

криптографических алгоритмов, информация, касающаяся состояния использования сменного блока 200 (например, информация, касающаяся остающегося уровня тонера, времени, в которое тонер необходимо заменить, или числа остающихся листов, подлежащих печати), уникальная информация (например, информация, касающаяся производителя сменного блока 200, информация, касающаяся даты и времени изготовления, порядковый номер или номер модели), или информация о ремонтном обслуживании.

Интерфейсный блок 250 соединяет CPU 220 и основной контроллер 110. Интерфейсный блок 250 может быть реализован как последовательный интерфейс или беспроводной интерфейс. Например, последовательный интерфейс имеет преимущество уменьшения стоимости из-за использования меньшего числа сигналов, чем параллельный интерфейс, и последовательный интерфейс является подходящим для рабочих условий, когда происходит большое количество шума, как, например, в принтере.

Компоненты, показанные на фиг.2, подключены друг к другу через шину, но это просто пример. Соответственно, следует понимать, что компоненты согласно аспектам данной общей идеи изобретения могут быть подключены непосредственно без этой шины.

Фиг.3 является блок-схемой, иллюстрирующей устройство 100 формирования изображений согласно некоторому примерному варианту осуществления данной общей идеи изобретения. Устройство 100 формирования изображений фиг.3 может включать в себя OS 115, основной контроллер 110, блок 120 памяти, блок 150 формирования изображений и множество блоков 200-1, 200-2, …, 200-n. Множеством блоков 200-1, 200-2, …, 200-n фиг.3 могут быть CRUM блоки, полупроводниковые микросхемы, блоки полупроводниковых микросхем или сменные блоки. Только с целью иллюстрации, множество блоков 200-1, 200-2, …, 200-n описаны здесь как сменные блоки.

Если единственной системе требуются различные расходные материалы, то также требуется множество блоков. Например, если устройство 100 формирования изображений является цветным принтером, то четыре цветных картриджа, а именно бирюзовый (C), малиновый (M), желтый (Y) и черный (K) картриджи смонтированы в этом цветном принтере для того, чтобы выразить желаемые цвета. Кроме того, цветной принтер может включать в себя и другие расходные материалы. Соответственно, если требуется большое число блоков, то каждый из блоков требует своего собственного канала ввода/вывода (I/O), так что компоновка может быть неэффективной. Следовательно, как показано на фиг.3, единственный последовательный I/O канал может использоваться для подключения каждого из множества блоков 200-1, 200-2, …, 200-n к основному контроллеру 110. Основной контроллер 110 может получить доступ к каждому из множества блоков 200-1, 200-2, …, 200-n с использованием различных адресов, назначенных каждому из множества блоков 200-1, 200-2, …, 200-n.

Когда основной контроллер 110 включен, или когда множество блоков 200-1, 200-2, …, 200-n смонтированы в устройстве 100 формирования изображений, если каждый из множества блоков 200-1, 200-2, …, 200-n полностью инициализирован, то аутентификация выполняется с использованием уникальной информации цифровой подписи для каждого из множества блоков 200-1, 200-2, …, 200-n.

Если аутентификация является успешной, то основной контроллер 110 выполняет обмен криптографическими данными с множеством CPU (не показаны) во множестве

блоков 200-1, 200-2, …, 200-n и сохраняет информацию, касающуюся истории использования во множестве блоков памяти (не показаны) во множестве блоков 200-1, 200-2, …, 200-n. Основной контроллер 110 и множество CPU могут действовать как ведущее устройство и управляемое устройство.

Здесь, обмен криптографическими данными выполняется посредством передачи данных, которые пользователь желает передать, вместе с MAC, сгенерированным посредством шифрования этих данных с использованием предварительно заданного криптографического алгоритма и ключа. Поскольку эти данные изменяются каждый раз, когда они передаются, MAC может также измениться. Соответственно, даже когда третья сторона вмешивается в операцию обмена данными и находит MAC, для этой третьей стороны невозможно осуществить несанкционированный доступ к последующим операциям обмена данными с использованием этого MAC. Следовательно, надежность обмена данными может быть повышена.

Если обмен криптографическими данными завершен, то канал, соединенный между основным контроллером 110 и CPU, обрезан.

Блок 120 памяти хранит разнообразие информации, включающей в себя значения ключей и множество криптографических алгоритмов, необходимых для аутентификации каждого из множества блоков 200-1, 200-2, …, 200-n.

Основной контроллер 110 выполняет аутентификацию и обмен криптографическими данными с использованием информации, хранимой в блоке 120 памяти. Конкретно, основной контроллер 110 выполняет аутентификацию и обмен криптографическими данными посредством применения RSA алгоритма с асимметричным ключом и одного из алгоритмов с симметричным ключом ARIA, TDES, SEED, AES, например. Следовательно, выполняются как асимметричные, так и симметричные процессы аутентификации, так что можно увеличить криптографический уровень относительно стандартного уровня техники.

Хотя фиг.3 показывает блок 120 памяти как единственный блок, блок 120 памяти может включать в себя блок памяти для хранения разнообразия данных криптографического алгоритма, блок памяти, необходимый для других операций основного контроллера 110, блок памяти для хранения информации, касающейся множества блоков 200-1, 200-2, …, 200-n, или блок памяти для хранения информации, касающейся использования множества блоков 200-1, 200-2, …, 200-n (например, листы, подлежащие печати, или уровень оставшегося тонера).

Множество блоков 200-1, 200-2, …, 200-n, смонтированных в устройстве 100 формирования изображений фиг.3, могут иметь конфигурации, показанные на фиг.1 или фиг.2. Соответственно, после посылки команд доступа ко множеству CPU множества блоков 200-1, 200-2, …, 200-n и принятия сигналов подтверждения, основной контроллер 110 может получить доступ ко множеству блоков 200-1, 200-2, …, 200-n. Следовательно, множество блоков согласно некоторому примерному варианту осуществления данной общей идеи изобретения отличается от стандартной схемы, способной осуществлять доступ к CRUM данным, которая использует простые операции записи и считывания данных.

Если устройство 100 формирования изображений начинает задание формирования изображений, то основной контроллер 110 может измерить степени расходных материалов, используемых для этого задания, и может передать измеренные степени к каждому из множества блоков 200-1, 200-2, …, 200-n. Более подробно, устройство 100 формирования изображений может добавить измеренные степени используемых расходных материалов к ранее сохраненной информации по использованию

расходных материалов, может передать результирующее значение ко множеству блоков 200-1, 200-2, …, 200-n и может обновить информацию по использованию расходных материалов. Когда операция передачи результирующего значения происходит в предшествующем уровне техники, если некорректные данные передаются из-за ошибок, то некорректная информация по степеням используемых расходных материалов может быть записана на каждом из множества блоков 200-1, 200-2, …, 200-n. Например, если задание печати 10 новых листов завершено после того, как 1000 листов напечатаны с использованием смонтированного в настоящее время картриджа носителя, то общее значение равно 1010 листов. Однако если происходят некоторые ошибки, и если передано значение в 0 листов, то запись задания печати 0 листов может быть сделана на множестве блоков 200-1, 200-2, …, 200-n. В результате, было бы невозможно для пользователя точно знать время, в которое необходимо заменить этот расходный материал.

Для решения этой проблемы, в некотором варианте осуществления общей идеи изобретения, основной контроллер 110 может измерить степени расходных материалов, используемых для этого задания, и может передать только измеренные степени используемых расходных материалов к каждому из множества блоков 200-1, 200-2, …, 200-n. В этой ситуации основной контроллер 110 может передать значение в 10 листов, так что множество блоков 200-1, 200-2, …, 200-n могут, через использование своих собственных CPU, добавить заново принятое значение «10» к значению «1000», а именно к ранее сохраненному значению. Соответственно, информация по использованию расходных материалов, хранимая в памяти, может быть корректно обновлена на «1010».

В ином случае основной контроллер 110 может управлять информацией по степеням используемых расходных материалов сам посредством добавления измеренных величин к информации по использованию расходных материалов, хранимой в блоке 120 памяти, отдельно от множества блоков 200-1, 200-2, …, 200-n.

В некотором варианте осуществления данной общей идеи изобретения основной контроллер 110 может автоматически обновлять информацию по использованию расходных материалов, хранимую в блоке 120 памяти, при передаче информации по степеням используемых расходных материалов ко множеству блоков 200-1, 200-2, …, 200-n каждый раз, когда выполняется это задание.

Например, при печати 100 листов с использованием множества блоков 200-1, 200-2, …, 200-n, смонтированных в устройстве 100 формирования изображений, если 10 листов дополнительно печатаются в то время, как выполняется единственное задание, основной контроллер 110 может послать значение «10» ко множеству блоков 200-1, 200-2, …, 200-n и может добавить значение «10» к значению «100», ранее сохраненному в блоке 120 памяти, чтобы сохранить историческую информацию, указывающую, что «110» листов было напечатано. Соответственно, если происходит специфическое событие (например, если устройство 100 формирования изображений установлено на «0», или если тонер или чернила полностью исчерпаны), или если происходит предварительно заданный период, то основной контроллер 110 и множество блоков 200-1, 200-2, …, 200-n могут сравнить их соответствующую историческую информацию через использование их собственных CPU, так что можно проверить, записаны ли нормально данные в каждый из множества блоков 200-1, 200-2, …, 200-n.

Другими словами, точность или неточность сохраненной информации по использованию расходных материалов может быть определена посредством

сравнения информации по использованию расходных материалов, хранимой в блоке 120 памяти, с информацией по использованию расходных материалов, хранимой во множестве блоков 200-1, 200-2, …, 200-n. Более подробно, если происходят эти события, или если происходит предварительно заданный период, то основной контроллер 110 может передать команду для запроса информации по использованию расходных материалов ко множеству блоков 200-1, 200-2, …, 200-n. В ответ на команду запроса CPU множества блоков 200-1, 200-2, …, 200-n могут передать информацию по использованию расходных материалов, хранимую в них, к основному контроллеру 110.

Если информация по использованию расходных материалов, хранимая в блоке 120 памяти, отличается от информации по использованию расходных материалов, хранимой во множестве блоков 200-1, 200-2, …, 200-n, то основной контроллер 110 может выдать сообщение об ошибке, или может гармонизировать информацию, определенную быть корректной, и может обновить информацию по использованию расходных материалов.

Кроме того, если информация по использованию расходных материалов, хранимая в блоке 120 памяти, отличается от информации по использованию расходных материалов, хранимой во множестве блоков 200-1, 200-2, …, 200-n, то основной контроллер 110 может передать команду изменить информацию по использованию расходных материалов, хранимую в блоке 120 памяти, так как существует возможность, что могли бы произойти ошибки при передаче данных к блоку 120 памяти.

Устройство 100 формирования изображений может также включать в себя блок 150 формирования изображений для выполнения операции формирования изображения с использованием блоков 200-1, 200-2, …, 200-n. Блоки 200-1, 200-2, …, 200-n могут быть частью блока 150 формирования изображений, будучи установленными в корпусе устройства 100 формирования изображений. Основной контроллер 110 может управлять блоками 120 и 210 памяти и блоком 150 формирования изображений для подачи носителя в устройство формирования изображений для формирования некоторого изображения на этом носителе и выгрузки этого носителя.

Фиг.4 является иерархической схемой, иллюстрирующей блок 200 и ведущее устройство, использующее блок 200, а именно конфигурацию программного обеспечения устройства формирования изображений согласно некоторому примерному варианту осуществления данной общей идеи изобретения.

Со ссылкой на фиг.1 и 4, программное обеспечение (a) устройства 100 формирования изображений может включать в себя область механизма обеспечения безопасности для выполнения аутентификации и криптографии с блоком 200 и программную область криптографической операции для выполнения программной криптографии в дополнение к общим прикладным программам, приложение для управления данными каждого блока, драйвер устройства, который выполняет свое собственное управление, и программу для обработки команд.

Программное обеспечение (b) блока 200 может включать в себя область полупроводниковой микросхемы, имеющую различные блоки для предохранения данных, область приложения для сопряжения с программным обеспечением ведущего устройства и OS область для управления этими областями.

Область программного обеспечения устройства фиг.4 может включать в себя базовые элементы OS, такие как программы управления файлами и целостности данных. OS область может дополнительно включать в себя рабочие блоки,

необходимые для предохранения данных, включающие в себя механизм обеспечения безопасности, программные криптографические операции и операции контрмер для надежности. OS может включать в себя программы для управления аппаратным обеспечением для системы безопасности, включающей в себя аппаратное управление памятью и аппаратное криптографическое управление. Как показано, OS может включать в себя, с использованием функции аппаратного управления вводом/выводом, а также стандартного протокола, обработку команд и программы выполнения приложений. Область приложений (App) области программного обеспечения устройства включает в себя некоторое приложение для управления сменными блоками и приложение обеспечения общей безопасности. Область полупроводниковой микросхемы может размещать CPU, физическую память и клеммы ввода/вывода и может дополнительно включать в себя программу для препятствования фальсификации другими программами, программу генерации случайных чисел, управления рабочими условиями, программу криптографического процесса, а также вероятностный механизм обеспечения безопасности. Поскольку прикладная программа для реализации функции CRUM установлена на программах, объясненных выше, невозможно проверить информацию, хранимую на данных, через некоторый канал связи. Эти программы могут быть воплощены в структурах, отличных от тех, которые показаны на фиг.4, для включения этих базовых блоков. Однако для эффективного предохранения данных необходимо, чтобы эти программы были тщательно запрограммированы таким образом, чтобы OS была безопасной.

OS область в программной структуре фиг.4 включает в себя область 410 восстановления памяти. Область 410 восстановления памяти обеспечена для того, чтобы гарантировать, что обновление успешно достигнуто согласно процессу обновления информации состояния блока 200.

Со ссылкой на фиг.1 и 2, при записи данных на блок 210 памяти, CPU 220 блока 200 копирует ранее записанные значения в пределах области 410 восстановления памяти и устанавливает флаг старта.

Например, когда задание формирования изображений с использованием блока 200 завершено, основной контроллер 110 получает доступ к CPU 220 блока 200, чтобы заново записать информацию состояния, такую как величина подач или число потребленных листов, при выполнении задания печати. Если энергия отключена, или если задание печати завершилось аварийно из-за внешнего шума перед тем, как завершилась запись, то стандартный CRUM может быть не в состоянии определить, записана ли нормально информация нового состояния. Если такие аномальные условия повторяются, то может быть сложно доверять этой информации и управлять этим блоком даже с использованием CRUM.

Для предотвращения таких случаев OS, согласно некоторому примерному варианту осуществления данной общей идеи изобретения, обеспечивает область 410 восстановления памяти в OS. В этом случае CPU копирует ранее записанные данные в область 410 восстановления памяти перед записью данных и устанавливает флаг старта на 0. Если обрабатывается операция записи данных, то флаг старта непрерывно обновляется согласно операции записи данных.

В этом состоянии, если операция записи данных завершилась аварийно, то CPU проверяет флаг старта после включения энергии, или после того, как система стабилизировалась. CPU, таким образом, определяет, записаны ли данные нормально, согласно условиям изменения значения флага старта. Если разница между значением флага старта и первоначально установленным значением не является значительной,

то CPU определяет, что запись данных потерпела неудачу и возвращает данные на ранее записанные значения. С другой стороны, если значение флага старта приблизительно совпадает с финальным значением, то CPU определяет, что записанные в настоящее время данные являются корректными. Следовательно, даже когда энергия отключается, или когда система работает аварийно, данным, записанным в блоке 200, можно доверять.

Фиг.5 является блок-схемой, иллюстрирующей способ работы сменного блока и устройства формирования изображений согласно некоторому примерному варианту осуществления данной общей идеи изобретения. Со ссылкой на фиг.1 и 5 CPU блока 200 определяет, сгенерировано ли некоторое специфическое событие в операции S510. Это специфическое событие может включать в себя случай, в котором устройство 100 формирования изображений включается, или случай, в котором блок 200 или компоненты, включающие в себя блок 200, смонтированы в устройстве 100 формирования изображений.

Если определено, что произошло некоторое специфическое событие, то блок 200 выполняет свою собственную инициализацию в операции S520. Эта инициализация включает в себя вычисление секретной информации, необходимой для обмена данными с устройством формирования изображений после инициализации, настройки канала связи, инициализации значений памяти, проверки остающейся величины тонера или чернил, подтверждения времени замены или различных других процессов.

Основной контроллер 110 устройства 100 формирования изображений передает команду для осуществления попытки аутентификации между основным контроллером 110 и CPU 220 в операции S530. Если основной контроллер 110 не принимает ответ от CPU 220 в операции S540, то основной контроллер 110 повторно передает эту команду, пока не будет принят ответ.

При получении ответа основной контроллер 110 аутентифицирует связь с CPU 220 в операции S550, как объяснено выше.

Если аутентификация успешно выполнена в операции S560, то обмен криптографическими данными с основным контроллером 110 выполняется с использованием криптографического алгоритма в операции S570.

Фиг.6 является схематичным видом, обеспеченным для объяснения процесса изменения криптографического алгоритма посредством блока 200 согласно некоторому примерному варианту осуществления данной общей идеи изобретения. Со ссылкой на фиг.6 блок 200 может поддерживать алгоритмы с симметричным ключом стандарта ARIA, стандарта тройного шифрования данных (TDES), SEED и усовершенствованного стандарта шифрования (AES), например. Определение процесса, какой алгоритм следует использовать, может иметь место, когда система записи ключа в системе управления ключами (KMS) 600 генерирует данные, генерирующие ключ.

Если выполняется взлом криптографического алгоритма, то криптографический алгоритм может быть изменен посредством приобретения нового ключа от KMS, к которому применяется другой из четырех криптографических алгоритмов вместо изготовления нового блока 200.

Как описано выше, устройство 100 формирования изображений может также поддерживать алгоритмы с симметричным ключом ARIA, TDES, SEED и AES в дополнение к RSA алгоритму с асимметричным ключом. Соответственно, даже если криптографический алгоритм, применяемый к блоку 200, изменен, устройство 100 формирования изображений изменяет криптографический алгоритм в ответ и

выполняет аутентификацию и обмен криптографическими данными.

Следовательно, криптографические алгоритмы могут быть удобно изменены посредством изменения значения ключа по контрасту со стандартным уровнем техники, который требует замены микросхемы.

Фиг.7 является блок-схемой, обеспеченной для объяснения способа выполнения аутентификации и обмена криптографическими данными согласно некоторому примерному варианту осуществления данной общей идеи изобретения. Со ссылкой на фиг.1 и 7 устройство 100 формирования изображений передает команду запроса аутентификации вместе со случайным значением R1 в операции S710.

Если запрос на выполнение аутентификации принят, то блок 200 генерирует ключ сеанса, использующий принятое случайное значение R1 и случайное значение R2, сгенерированное блоком 200 в операции S715, и генерирует код аутентификации сообщения (MAC), использующий сгенерированный ключ сеанса в операции S720.

Первый MAC, сгенерированный блоком 200, является предварительно сохраненной информацией электронной подписи и вместе со случайным значением R2 передается к устройству 100 формирования изображений в операции S725.

Устройство 100 формирования изображений верифицирует принятую электронную подпись первого MAC, сгенерированного блоком 200, посредством сравнения принятой информации электронной подписи с предварительно сохраненной информацией электронной подписи в операции S730. Для верификации принятой электронной подписи устройство 100 формирования изображений может сохранить информацию электронной подписи каждого блока, если множество блоков смонтированы в устройстве 100 формирования изображений.

Если принятая электронная подпись верифицирована, то устройство 100 формирования изображений генерирует ключ сеанса посредством комбинирования предварительно сгенерированного случайного значения R1 с принятым случайным значением R2 в операции S735, и второй MAC генерируется устройством 100 формирования изображений с использованием сгенерированного ключа сеанса в операции S740.

Устройство 100 формирования изображений затем сравнивает сгенерированный второй MAC устройства 100 формирования изображений с принятым первым MAC сменного блока 200 для того, чтобы определить, совпадают ли эти два различных MAC в операции S745. Аутентификация завершается согласно верификации принятого первого MAC сменного блока 200. Если аутентификация успешно выполнена, то может быть выполнен обмен криптографическими данными.

Для выполнения обмена криптографическими данными предполагается, что устройство 100 формирования изображений использует тот же самый ключ и криптографический алгоритм, что и блок 200. Этим ключом может быть ключ сеанса, описанный выше.

Если принятый первый MAC сменного блока 200 полностью верифицирован, то устройство 100 формирования изображений генерирует третий MAC посредством применения этого ключа и криптографического алгоритма к данным при генерации коммуникационного сообщения в операции S750.

Устройство 100 формирования изображений передает это коммуникационное сообщение, включающее в себя третий MAC, к блоку 200 в операции S755.

Блок 200 извлекает эту часть данных из принятого коммуникационного сообщения и генерирует четвертый MAC посредством применения вышеупомянутого ключа и криптографического алгоритма к данным в операции S760.

Блок 200 извлекает часть третьего MAC из принятого коммуникационного сообщения и выполняет аутентификацию посредством сравнения извлеченной части третьего MAC с четвертым MAC, вычисленным блоком 200 в операции S765.

Если извлеченная часть третьего MAC совместима с четвертым MAC, вычисленным блоком 200, то коммуникационное сообщение трактуется как достоверное коммуникационное сообщение, и, таким образом, операция, соответствующая этому сообщению, выполняется в операции S770. С другой стороны, если третий и четвертый MAC не совместимы друг с другом, то коммуникационное сообщение трактуется как ошибочное коммуникационное сообщение и отбрасывается.

Некоторый способ выполнения аутентификации и обмена криптографическими данными может быть также применен к примерным вариантам осуществления, объясненным со ссылкой на эти чертежи. Блок 200 может быть реализован в разнообразных формах, таких как полупроводниковая микросхема или блок микросхем, обычный блок или сменный блок.

Данная общая идея изобретения может быть также воплощена как считываемые компьютером коды на считываемом компьютером носителе. Считываемый компьютером носитель может включать в себя считываемый компьютером носитель записи и считываемую компьютером среду передачи данных. Считываемый компьютером носитель записи является любым устройством хранения данных, которое может хранить данные, как, например, программу, которая может быть после этого считана компьютерной системой. Примеры считываемого компьютером носителя записи включают в себя ПЗУ (ROM), ЗУПВ (RAM), ПЗУ на компакт-дисках, магнитные ленты, флоппи-диски и оптические устройства хранения данных. Считываемый компьютером носитель записи может быть также распределен по связанным в сеть компьютерным системам таким образом, что считываемый компьютером код хранится и исполняется распределенным образом. Считываемая компьютером среда передачи данных может передавать волны несущей или сигналы (например, проводная или беспроводная передача данных через Интернет). Также функциональные программы, коды и сегменты кода для выполнения данной общей идеи изобретения могут быть легко истолкованы программистами с квалификацией в данной области техники, к которой имеет отношение данная общая идея изобретения.

Хотя немногие варианты осуществления данной общей идеи изобретения были показаны и описаны, специалистам в данной области техники будет ясно, что изменения могут быть сделаны в этих вариантах осуществления, не выходя за рамки принципов и сущности общей идеи изобретения, объем которого задан в прилагаемой формуле изобретения и ее эквивалентах.

Формула изобретения

1. Устройство формирования изображений, содержащее:

основной корпус, имеющий основной контроллер, который управляет операцией устройства формирования изображений; и

сменный блок, который присоединен к основному корпусу и выполнен с возможностью выполнения операции формирования изображений с основным корпусом,

причем сменный блок содержит:

блок памяти, хранящий вторую программу инициализации, отличную от первой программы инициализации, используемой в основном корпусе устройства формирования изображений, уникальную информацию, связанную со сменным

блоком, и информацию о состоянии по использованию сменного блока; и

центральный процессор (CPU), который соединен с блоком памяти,

причем CPU, если требуется инициализация, выполняет инициализацию, используя вторую программу инициализации независимо от основного корпуса, и, если первое число принимается из основного контроллера, генерирует второе число, генерирует код (MAC) аутентификации сообщения, используя первое число и второе число, и передает второе число и первый MAC основному контроллеру,

причем основной контроллер генерирует второй MAC, используя первое число и второе число, выполняет процесс аутентификации сменного блока посредством сравнения второго MAC с первым MAC и выполняет криптографический обмен данными посредством генерации третьего MAC и передачи сообщения обмена данными, в том числе зашифрованных данных обмена и третьего MAC, сменному блоку,

причем CPU принимает сообщение обмена данными от основного контроллера для того, чтобы изменить информацию о состоянии, хранящуюся в блоке памяти сменного блока.

2. Устройство по п.1, в котором основной корпус подсоединен к сменному блоку через последовательный интерфейс, и сообщение обмена данными передается сменному блоку от основного корпуса через последовательный интерфейс.

3. Устройство по п.2, в котором криптографический обмен данными выполняется с использованием алгоритма шифрования, хранящегося в основном корпусе и сменном блоке соответственно.

4. Устройство по п.3, в котором зашифрованные данные обмена шифруются с использованием алгоритма шифрования, хранящегося в основном корпусе, и зашифрованные данные обмена выполнены с возможностью дешифрования с использованием алгоритма шифрования, хранящегося в сменном блоке.

5. Устройство по п.4, в котором, если принято сообщение обмена данными, CPU сменного блока выделяет зашифрованные данные обмена из сообщения обмена данными.

6. Устройство по п.2, в котором основной корпус и сменный блок хранят множество программ алгоритмов шифрования соответственно и выполняют криптографический обмен данными с использованием соответствующего алгоритма шифрования из множества алгоритмов шифрования.

7. Устройство по п.5, в котором основной корпус имеет блок хранения, хранящий информацию по использованию расходных материалов, используемых в операции формирования изображения, причем основной контроллер включает в себя информацию по использованию расходных материалов в сообщении обмена данными и передает сообщение обмена данными сменному блоку.

8. Устройство по п.1, в котором CPU сменного блока выделяет информацию по использованию расходных материалов, включенных в состав сообщения обмена данными, и изменяет информацию о состоянии, хранящуюся в блоке памяти.

9. Устройство по любому из пп.1-8, в котором основной корпус выполняет аутентификацию или криптографический обмен данными посредством применения RSA алгоритма с асимметричным ключом и одного из ARIA, TDES, SEED и AES алгоритмов с симметричным ключом, причем CPU выполняет аутентификацию или криптографический обмен данными посредством применения одного из ARIA, TDES, SEED и AES алгоритмов с симметричным ключом.

10. Устройство по любому из пп.1-8, в котором по меньшей мере один сменный

блок включает в себя блок контроля пользовательского сменного блока (CRUM), причем блок памяти и CPU интегрированы в CRUM блоке.

11. Блок CRUM, используемый в сменном блоке, который прикреплен к основному корпусу устройства формирования изображений и выполнен с возможностью выполнения операции формирования изображения с главным корпусом устройства формирования изображения, CRUM блок содержит:

блок памяти, хранящий вторую программу инициализации, отличную от первой программы инициализации, используемой в основном корпусе устройства формирования изображений, уникальную информацию, связанную со сменным блоком, и информацию о состоянии по использованию сменного блока; и CPU, соединенный с блоком памяти,

причем CPU, если требуется инициализация, выполняет инициализацию, используя вторую программу инициализации независимо от основного корпуса, и, если первое число принимается из основного корпуса устройства формирования изображений, генерирует второе число, генерирует первый MAC, используя первое число и второе число, и передает второе число и первый MAC основному контроллеру, причем, если основной корпус генерирует второй MAC, используя первое число и второе число, и выполняет процесс аутентификации CRUM блока посредством сравнения второго MAC с первым MAC, CPU обновляет информацию о состоянии, хранящуюся в блоке памяти посредством выполнения криптографического обмена данными с основным корпусом, чтобы принимать сообщения обмена данными, в том числе зашифрованные данные обмена и третий MAC от основного корпуса.

12. Блок CRUM по п.11, в котором сменный блок подсоединен к основному корпусу устройства формирования изображений через последовательный интерфейс,

причем CPU принимает сообщение обмена данными от основного корпуса через последовательный интерфейс.

13. Блок CRUM по п.12, в котором криптографический обмен данными выполняется с использованием алгоритма шифрования, хранящегося в основном корпусе и CRUM блоке соответственно.

14. Блок CRUM по п.13, в котором зашифрованные данные обмена шифруются с использованием алгоритма шифрования, хранящегося в основном корпусе,

причем, если принимаются зашифрованные данные обмена, CPU выполняет дешифрование с использованием алгоритма шифрования, хранящегося в CRUM блоке.

15. Блок CRUM по п.14, в котором, если принимается сообщение обмена данными, CPU выделяет зашифрованные данные обмена из сообщения обмена данными.

16. Блок CRUM по п.12, в котором основной корпус и блок памяти хранят множество алгоритмов шифрования соответственно и выполняют криптографический обмен данными, используя соответствующий алгоритм шифрования из множества алгоритмов шифрования.

17. Блок CRUM по любому из пп.12-15, в котором CPU принимает сообщение обмена данными, в том числе информацию по использованию расходных материалов, используемых в операции формирования изображения.

18. Блок CRUM по п.17, в котором CPU обновляет информацию о состоянии по использованию сменного блока, хранящегося в блоке памяти, на основании информации по использованию расходных материалов, включенных в состав сообщения обмена данными.

19. Блок CRUM по п.18, в котором CPU выполняет аутентификацию или криптографический обмен данными посредством одного из ARIA, TDES, SEED и AES

алгоритмов с симметричным ключом.

20. Сменный блок, который прикреплен к основному корпусу устройства формирования изображения и выполнен с возможностью выполнения операции формирования изображения с главным корпусом устройства формирования изображений, причем сменный блок содержит:

блок памяти, хранящий вторую программу инициализации, отличную от первой программы инициализации, используемой в основном корпусе устройства формирования изображений, уникальную информацию, связанную со сменным блоком, и информацию о состоянии по использованию сменного блока; и

CPU, соединенный с блоком памяти,

причем CPU, если требуется инициализация, выполняет инициализацию, используя вторую программу инициализации независимо от основного корпуса, и, если первое число принимается из основного корпуса устройства формирования изображений, генерирует второе число, генерирует первый MAC, используя первое число и второе число, и передает второе число и первый MAC основному контроллеру,

причем, если основной корпус генерирует второй MAC, используя первое число и второе число, и выполняет процесс аутентификации CRUM блока посредством сравнения второго MAC с первым MAC, CPU обновляет информацию о состоянии, хранящуюся в блоке памяти посредством выполнения криптографического обмена данными с основным корпусом, чтобы принимать сообщения обмена данными, в том числе зашифрованные данные обмена и третий MAC от основного корпуса.

21. Сменный блок по п.20, в котором сменный блок подсоединен к основному корпусу устройства формирования изображений через последовательную шину, причем CPU принимает сообщение обмена данными от основного корпуса через последовательный интерфейс.

22. Сменный блок по п.21, в котором криптографический обмен данными выполняется с использованием алгоритма шифрования, хранящегося в основном корпусе и сменном блоке соответственно.

23. Сменный блок по п.22, в котором зашифрованные данные обмена шифруются с использованием алгоритма шифрования, хранящегося в основном корпусе,

причем, если принимаются зашифрованные данные обмена, CPU выполняет дешифрование с использованием алгоритма шифрования, хранящегося в сменном блоке.

24. Сменный блок по п.23, в котором, если принимаются зашифрованные данные обмена, CPU выделяет зашифрованные данные обмена из сообщения обмена данными.

25. Сменный блок по п.21, в котором основной корпус и блок памяти хранят множество алгоритмов шифрования соответственно и выполняют криптографический обмен данными, используя соответствующий алгоритм шифрования из множества алгоритмов шифрования.

26. Сменный блок по любому из пп.20-24, в котором, если основной блок включает в себя информацию по использованию расходных материалов, используемых в операции формирования изображения в сообщении обмена данными, и передает сообщение обмена данными сменному блоку, CPU обновляет информацию о состоянии по использованию сменного блока, хранящегося в блоке памяти, на основании информации по использованию расходных материалов, включенных в состав сообщения обмена данными.

27. Сменный блок по п.26, в котором CPU выполняет аутентификацию или криптографический обмен данными посредством одного из ARIA, TDES, SEED и AES

алгоритмов с симметричным ключом.

28. Сменный блок по п.26, в котором сменный блок включает в себя CRUM блок, причем блок памяти и CPU интегрированы в CRUM блоке.

29. Способ выполнения криптографического обмена данными в устройстве, которое выполняет криптографический обмен данными с CRUM блоком, имеющим блок памяти, хранящий программу инициализации и информацию о состоянии по использованию сменного блока устройства формирования изображений, и CPU, подсоединенного к блоку памяти, причем блок памяти содержит этапы, на которых:

генерируют шифрование данных обмена;

генерируют MAC;

генерируют сообщение обмена данными посредством объединения зашифрованных данных обмена и MAC; и

выполняют криптографический обмен данными посредством передачи сообщения обмена данными CRUM блоку.

30. Способ по п.29, в котором сообщение обмена данными используется для того, чтобы изменить информацию о состоянии, хранящуюся в блоке памяти CRUM блока.

31. Способ по п.30, в котором устройство соединено с CRUM блоком через последовательный интерфейс, и сообщение обмена данными передается CRUM блоку через последовательный интерфейс.

32. Способ по п.31, в котором криптографический обмен данными выполняется с использованием алгоритма шифрования, хранящегося в устройстве и CRUM блоке соответственно.

33. Способ по п.32, в котором зашифрованные данные обмена шифруются с использованием алгоритма шифрования, хранящегося в устройстве, причем, если принимаются зашифрованные данные обмена, CPU выполняет дешифрование с использованием алгоритма шифрования, хранящегося в CRUM блоке.

34. Способ по п.29, в котором устройство и блок памяти хранят множество алгоритмов шифрования соответственно, и устройство и блок памяти выполняют криптографический обмен данными, используя соответствующий алгоритм шифрования из множества алгоритмов шифрования.

35. Способ по любому из пп.29-34, в котором устройство выполняет криптографический обмен данными посредством применения RSA алгоритма с асимметричным ключом и одного из ARIA, TDES, SEED и AES алгоритмов с симметричным ключом,

причем CPU выполняет криптографический обмен данными посредством применения одного из ARIA, TDES, SEED и AES алгоритмов с симметричным ключом.

36. Устройство, которое выполняет криптографический обмен данными с CRUM блоком, имеющим блок памяти, хранящий программу инициализации и информацию о состоянии по использованию сменного блока устройства формирования изображений, и CPU, соединенный с блоком памяти, причем устройство содержит:

контроллер, который генерирует зашифрованные данные обмена и MAC и генерирует сообщение обмена данными; и

интерфейс, который передает сообщение обмена данными CRUM блоку.

37. Устройство по п.36, в котором сообщение обмена данными используется для того, чтобы изменить информацию о состоянии, хранящуюся в блоке памяти CRUM блока.

38. Устройство по п.37, в котором устройство соединено с CRUM блоком через последовательный интерфейс, и сообщение обмена данными передается CRUM блоку

через последовательный интерфейс.

39. Устройство по п.38, в котором сообщение обмена данными шифруется с использованием алгоритма шифрования, хранящегося в устройстве и CRUM блоке соответственно.

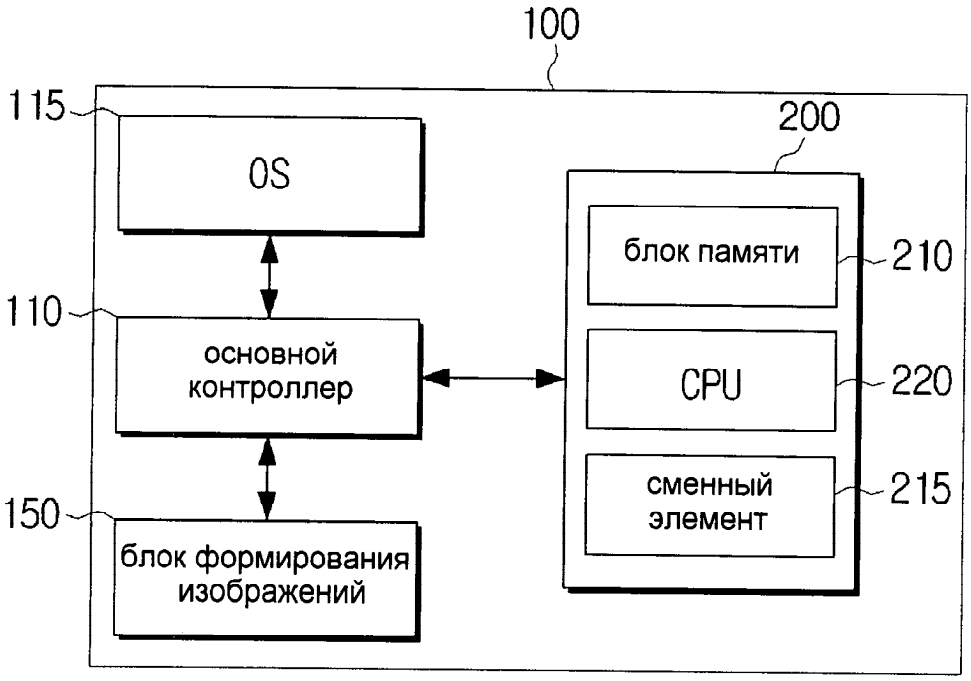
40. Устройство по п.38, в котором сообщение обмена данными включает в себя данные обмена, зашифрованные с использованием алгоритма шифрования, хранящегося в устройстве, и MAC,

причем если принимаются зашифрованные данные обмена, CPU выполняет дешифрование с использованием алгоритма шифрования, хранящегося в CRUM блоке.

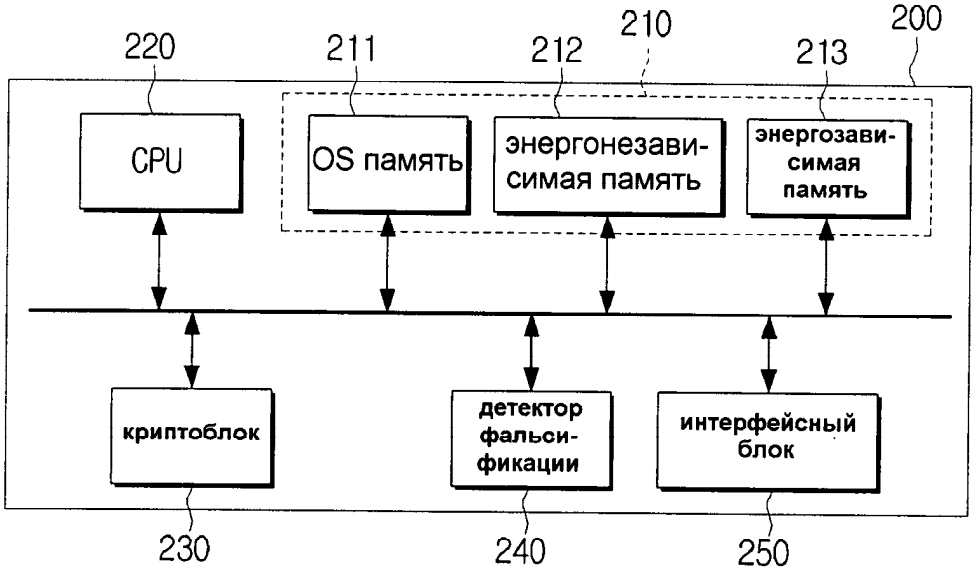
41. Устройство по п.39, в котором устройство и блок памяти хранят множество алгоритмов шифрования соответственно, и устройство и CRUM блок выполняют криптографический обмен данными, используя соответствующий алгоритм шифрования из множества алгоритмов шифрования.

42. Устройство по любому из пп.36-41, в котором устройство выполняет криптографический обмен данными посредством применения RSA алгоритма с асимметричным ключом и одного из ARIA, TDES, SEED и AES алгоритмов с симметричным ключом,

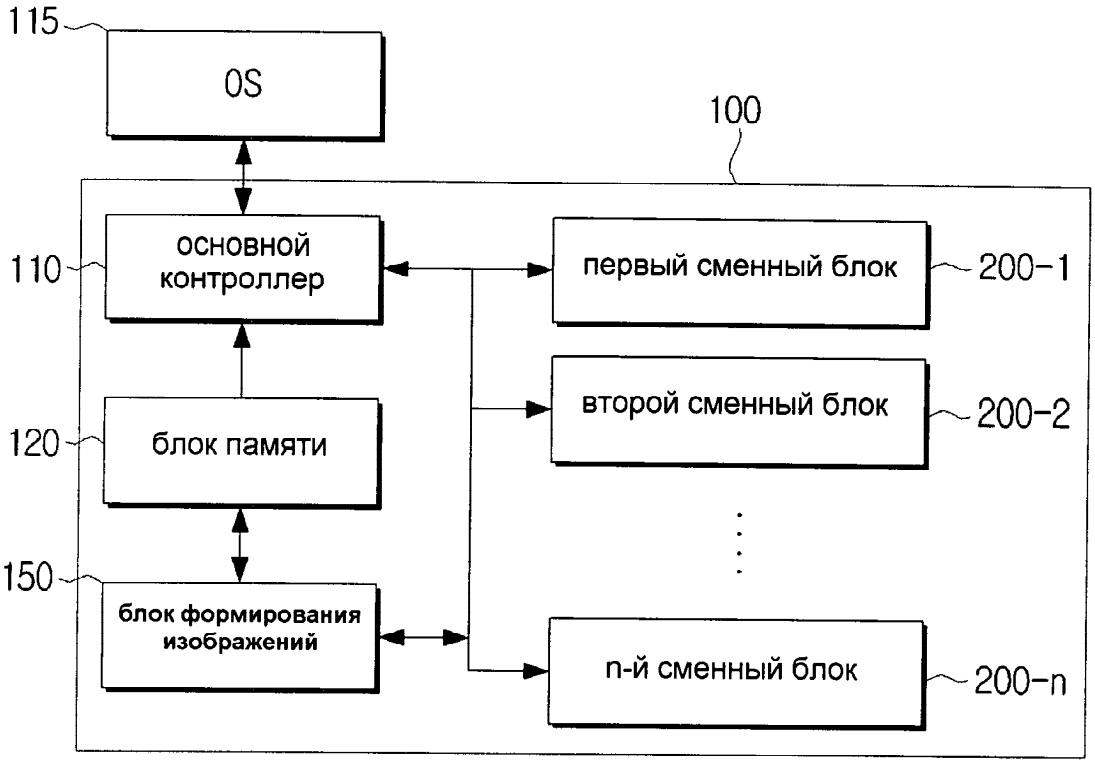
причем CPU выполняет криптографический обмен данными посредством применения одного из ARIA, TDES, SEED и AES алгоритмов с симметричным ключом.


100
115
OS
200
блок памяти
210
110
основной контроллер
CPU
220
сменный элемент
215
150
блок формирования изображений

ФИГ.1


220
211
212
210
213
200
CPU
OS память
энергонезависимая память
энергозависимая память
криптоблок
детектор фальсификации
интерфейсный блок
230
240
250

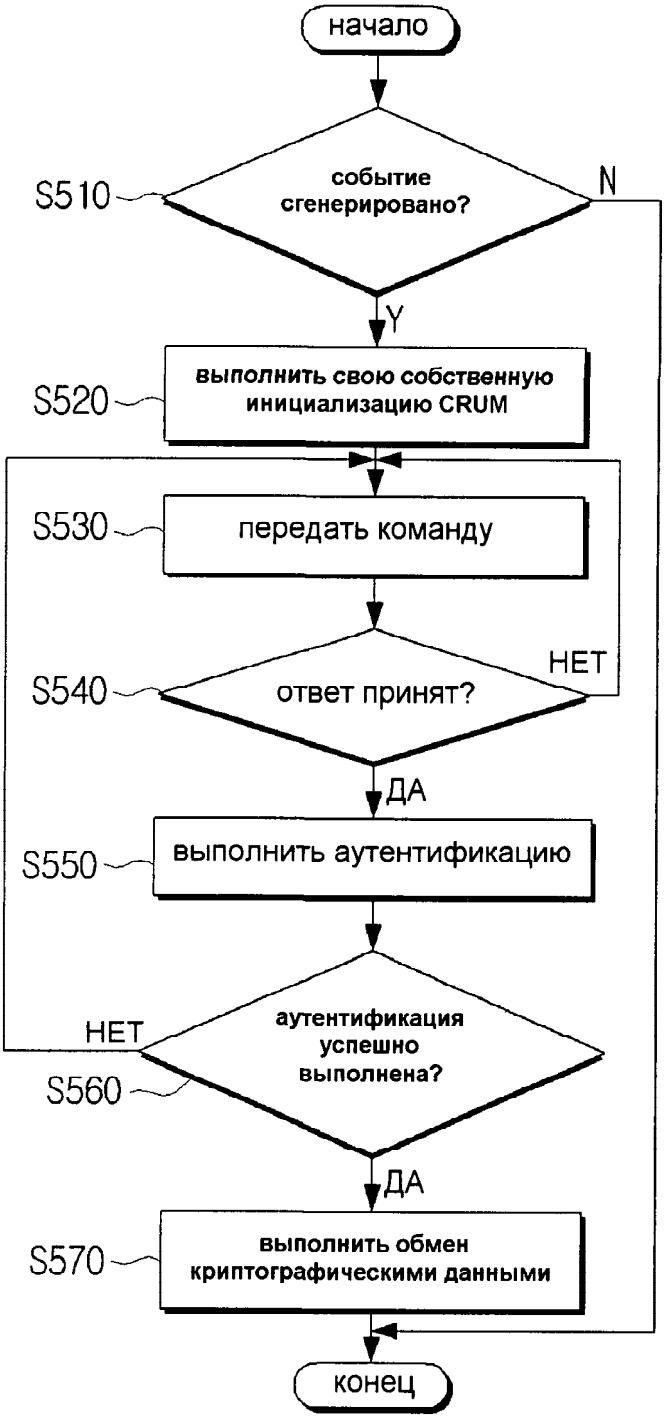
ФИГ.2


115
OS
100
110
основной контроллер
120
блок памяти
150
блок формирования изображений
первый сменный блок
200-1
второй сменный блок
200-2
n-й сменный блок
200-n

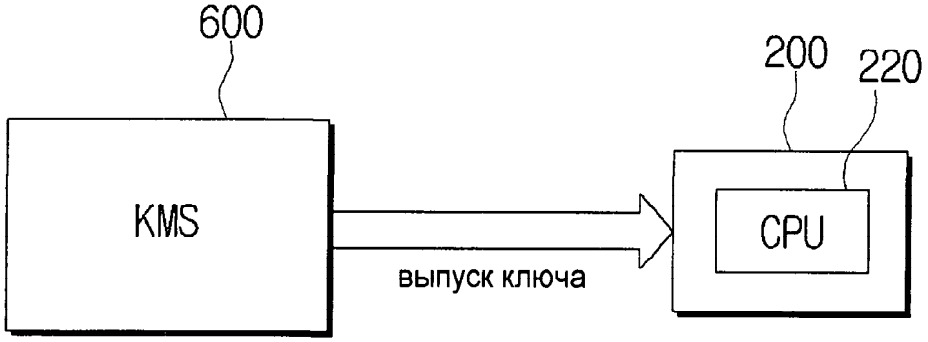
ФИГ.3


программное обеспечение ведущего устройства
прикладная программа
драйвер устройства и сменные блоки приложения
обработка команд
механизм обеспечения безопасности
S/W криптографические операции
a
App
программное обеспечение устройства
O/S
приложение для сменных блоков
приложение безопасности
выполнение приложения
управление файлами
механизм обеспечения безопасности
стандартный протокол
обработка команд
целостность данных
восстановление памяти
S/W криптографические операции
контрмеры безопасности
H/W I/O управление
управление H/W памятью
H/W криптографическое управление
микросхема
генерация случайных чисел
криптографический процесс
управления рабочими условиями
защита от физической фальсификации
вероятностный механизм обеспечения безопасности
CPU, память, физический I/O
410
b

ФИГ.4


начало
S510
событие сгенерировано?
N
Y
S520
выполнить свою собственную инициализацию CRUM
S530
передать команду
S540
ответ принят?
НЕТ
ДА
S550
выполнить аутентификацию
НЕТ
аутентификация успешно выполнена?
S560
ДА
S570
выполнить обмен криптографическими данными
конец

ФИГ.5


600
KMS
200
220
CPU
выпуск ключа

ФИГ.6