РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **225 635**(13) **U1**

(51) МПК
G06F 21/57 (2013.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ПОЛЕЗНОЙ МОДЕЛИ К ПАТЕНТУ

(52) СПК
G06F 21/575 (2024.01)

(21)(22) Заявка: **2024108403, 29.03.2024**

(24) Дата начала отсчета срока действия патента:
29.03.2024

Дата регистрации:
26.04.2024

Приоритет(ы):
(22) Дата подачи заявки: **29.03.2024**

(45) Опубликовано: **26.04.2024** Бюл. № **12**

Адрес для переписки:
121309, Москва, ул. Большая Филёвская, 19/18, корп. 1, кв. 8, Разбегаев Павел Викторович

(72) Автор(ы):
Винокуров Андрей Владимирович (RU),
Аверин Иван Александрович (RU),
Беляев Максим Михайлович (RU)

(73) Патентообладатель(и):
Общество с ограниченной ответственностью "Производственная компания Аквариус" (RU)

(56) Список документов, цитированных в отчете о поиске: **US 20190377583 A1, 12.12.2019. EP 3547194 B1, 06.09.2023. US 20090327741 A1, 31.12.2009. US 7921303 B2, 05.04.2011. RU 2773456 C1, 03.06.2022. RU 2748575 C1, 27.05.2021.**

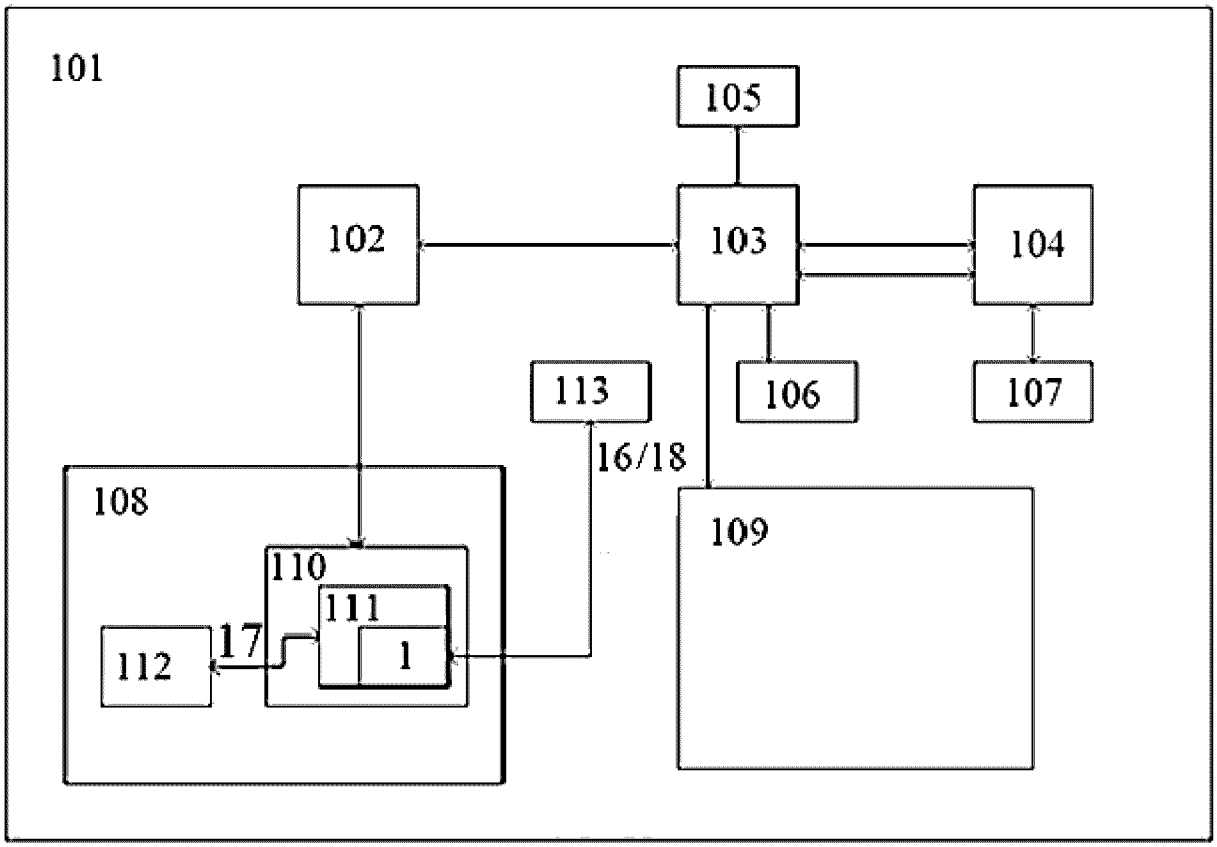
(54) **Интегрированный модуль доверенной загрузки периферийного устройства**

(57) Реферат:

Полезная модель относится к вычислительной технике. Технический результат заключается в повышении степени защиты вычислительной системы. Интегрированный модуль доверенной загрузки периферийного устройства, в котором вычислительное ядро дополнительно соединено с блоком ввода-вывода GPIO, снабжённым третьим интерфейсом, блоком генерации случайного числа, блоком ускорителей симметричных алгоритмов шифрования, блоком ускорителей асимметричных алгоритмов шифрования, блоком однократно программируемого постоянного запоминающего устройства, блоком установки и контроля временных интервалов, блоком контроля параметров напряжения и температуры и блоком безопасного обмена данными для взаимодействия вычислительного ядра с основным вычислительным ядром микросхемы периферийного устройства через четвёртый интерфейс. 2 ил.

RU 225635 U1

RU 225635 U1



Фиг.1

RU 225635 U1

RU 225635 U1

Полезная модель относится к специализированным средствам вычислительной техники и используется в качестве аппаратно-программного модуля, как части кристалла микросхемы периферийного устройства обработки и передачи данных, для обеспечения функции доверенной загрузки и проверки идентичности загружаемого программного кода и микросхемы устройства.

Несанкционированный доступ к информации и получение злоумышленником доступа к конфиденциальной информации может привести к утечке защищаемой важной информации или к нарушению работоспособности информационной системы, что может повлиять на работу средств вычислительной техники и привести к серьёзным потерям.

Известно портативное вычислительное устройство, в частности флэш-накопитель с универсальной последовательной шиной (USB), загруженному операционной системой и прикладными программами для загрузки компьютера при подключении к нему, при этом память флэш-накопителя разделена на активную область только для чтения и записываемые данные, в область хранения, а операционная система и прикладные программы хранятся в активной области; и операционная система выполняется независимо от аппаратного обеспечения, причём данное периферийное устройство обеспечивает возможность загрузки операционной системы и прикладных программ из собственной памяти, когда оно подключено к компьютеру, что позволяет снизить вероятность перехвата вредоносным программным обеспечением, хранящимся на жёстком диске вычислительного устройства, конфиденциальной информации пользователя (см., например опубликованную заявку US2009/0094447A1, кл. G06F 9/00, опубл. 09.04.2009).

Однако данное устройство не обеспечивает возможности однозначной аутентификации пользователя, загружающего указанную операционную систему, в нем отсутствует криптографическая защита информации в процессе использования указанного устройства, а также отсутствует возможность безопасной передачи информации по каналам связи, при этом данное устройство не содержит средств контроля целостности собственных компонентов, что снижает безопасность его эксплуатации.

Наиболее близким к полезной модели по технической сущности и достигаемому результату является интегрированный модуль доверенной загрузки периферийного устройства, содержащий вычислительное ядро, соединённое с блоком неизменяемой памяти, содержащим неизменяемый код корня доверия, блоком изменяемой памяти, блоком ввода-вывода SMBUS/I2C, снабжённым первым интерфейсом, и соединённое с блоком ввода-вывода QSPI/SPI, снабжённым вторым интерфейсом (см. патент US11675602B2, кл. G06F 21/57, опубл. 13.06.2023).

Данное техническое решение по контролю целостности загружаемого программного кода для периферийных устройств с помощью отдельного специализированного чипа, который осуществляет загрузку программного кода с удалённого сервера и после проверки осуществляет ее передачу периферийному устройству. Однако для хранения программного кода не используется микросхема памяти периферийного устройства, а хранение загружаемого программного кода производится на удалённом сервере, что не обеспечивает требуемую степень защиты периферийного устройства.

Технической проблемой, на решение которой направлена настоящая полезная модель, является преодоление выявленных недостатков известных технических решений.

Технический результат, на достижение которого направлена настоящая полезная модель, заключается в повышении степени защиты периферийных устройств и, как

следствие, повышение степени защиты вычислительной системы в целом от подмены программного кода микросхемы устройства и от подмены интегральной микросхемы устройства.

Указанная техническая проблема решается, а технический результат достигается за счёт того, что интегрированный модуль доверенной загрузки периферийного устройства содержит вычислительное ядро, соединённое с блоком неизменяемой памяти, содержащим неизменяемый код корня доверия, блоком изменяемой памяти, блоком ввода-вывода SMBUS/I^2C, снабжённым первым интерфейсом, и соединённое с блоком ввода-вывода QSPI/SPI, снабжённым вторым интерфейсом, при этом вычислительное ядро дополнительно соединено с блоком ввода-вывода GPIO, снабжённым третьим интерфейсом, блоком генерации случайного числа, блоком ускорителей симметричных алгоритмов шифрования, блоком ускорителей асимметричных алгоритмов шифрования, блоком однократно программируемого постоянного запоминающего устройства, блоком установки и контроля временных интервалов, блоком контроля параметров напряжения и температуры и блоком безопасного обмена данными для взаимодействия вычислительного ядра с основным вычислительным ядром микросхемы периферийного устройства через четвёртый интерфейс, при этом неизменяемый код корня доверия, находящийся в блоке неизменяемой памяти, обеспечивает функции загрузки, проверки целостности и аутентичности программного кода расширения функционала аппаратного модуля доверенной загрузки с использованием криптографических алгоритмов при подключении вычислительного ядра к внешней микросхеме хранения данных через второй интерфейс, при этом обеспечена возможность генерации информации для аутентификации микросхемы периферийного устройства с использованием криптографических алгоритмов, и через любой первый и третий интерфейсы её передачи контроллеру безопасности, при этом модуль интегрирован в кристалл микросхемы периферийного устройства.

Таким образом, достигается обеспечение доверенной загрузки и обеспечение аутентичности устройства, за счёт того, что в содержащем вычислительное ядро устройстве, интегрирован защищённый, неизменяемый код, представляющий собой неизвлекаемый корень доверия. В результате выполняется функционал загрузки, проверки целостности и аутентичности кода расширения функционала аппаратного модуля, считываемого с внешнего источника через интерфейс ввода-вывода, а также неизменяемый код выполняет функционал генерации информации для аутентификации самого устройства и последующей передачи её через интерфейс ввода-вывода 17 или интерфейс ввода-вывода 18 устройству следующего звена цепочки доверия.

На фиг. 1 представлена схема вычислительной системы (сервера) с периферийным устройством с интегрированным в микросхему модулем доверенной загрузки.

На фиг. 2 представлена функциональная схема описываемого интегрированного модуля доверенной загрузки периферийного устройства.

На фиг. 1 представлены следующие компоненты вычислительной системы с периферийным устройством.

101 - вычислительное устройство, например, сервер;

102 - ЦПУ (центральное процессорное устройство - центральный процессор);

103 - чипсет (набор микросхем на плате, который отвечает за работу всех компонентов компьютера);

104 - BMC - контроллер управления материнской платы (Baseboard management controller);

105 - АПМДЗ (Аппаратно-программный модуль доверенной загрузки);

106 - микросхема Flash (перепрограммируемой) памяти, содержащая BIOS (базовая система ввода - вывода);

107 - микросхема Flash памяти, содержащая Firmware (прошивка) BMC;

108 и 109 - периферийные устройства

110 - интегральная микросхема контроллера периферийного устройства;

111 - кристалл микросхемы контроллера периферийного устройства;

112 - микросхема Flash памяти содержащая Firmware контроллера периферийного устройства;

113 - Контроллер безопасности вычислительной платформы

1 - интегрированный в кристалл микросхемы периферийного устройства модуль доверенной загрузки контроллера периферийного устройства.

На фиг. 2 представлены следующие компоненты интегрированного модуля доверенной загрузки периферийного устройства

1 - интегрированный в кристалл микросхемы модуль доверенной загрузки контроллера периферийного устройства;

2 - вычислительное ядро;

3 - блок неизменяемой памяти (ПЗУ), относящийся к вычислительному ядру, содержащий программный код, представляющий собой неизвлекаемый корень доверия;

4 - блок изменяемой памяти, относящийся к вычислительному ядру;

5 - блок ввода-вывода SMBUS/I^2C;

6 - блок ввода-вывода QSPI/SPI;

7 - блок ввода-вывода GPIO;

8 - блок генерации случайного числа;

9 - блок ускорителей симметричных алгоритмов шифрования;

10 - блок ускорителей асимметричных алгоритмов шифрования;

11 - блок однократно программируемого постоянного запоминающего устройства ОППЗУ (однократно программируемое постоянное запоминающее устройство);

12 - блок установки и контроля временных интервалов;

13 - блок контроля параметров напряжения и температуры устройства;

14 - блок безопасного обмена данными. Интерфейсы интегрированного модуля:

15 - интерфейс связи с основным вычислительным ядром микросхемы периферийного устройства;

16 - интерфейс SMBUS/I^2C (последовательный протокол обмена данными для устройств питания, основан на шине PC);

17 - интерфейс QSPI/SPI (последовательный периферийный интерфейс);

18 - интерфейс GPIO (интерфейс ввода/вывода общего назначения. GPIO обычно подключены напрямую к «процессору». SoC (System-on-a-Chip - система на кристалле).

Интегрированный модуль доверенной загрузки 1 периферийного устройства содержит вычислительное ядро 2, соединённое с блоком неизменяемой памяти 3, содержащим неизменяемый код корня доверия, блоком изменяемой памяти 4, блоком ввода-вывода SMBUS/I^2C 5, снабжённым первым интерфейсом 16 и соединённое с блоком ввода-вывода QSPI/SPI 6, снабжённым вторым интерфейсом 17.

Вычислительное ядро 2 дополнительно соединено с блоком ввода-вывода GPIO 7, снабжённым третьим интерфейсом 18, блоком генерации случайного числа 8, блоком ускорителей симметричных алгоритмов шифрования 9, блоком ускорителей асимметричных алгоритмов шифрования 10, блоком однократно программируемого постоянного запоминающего устройства 11, блоком установки и контроля временных

интервалов 12, блоком контроля параметров напряжения и температуры 13 и блоком безопасного обмена данными 14 для взаимодействия вычислительного ядра 2 с основным вычислительным ядром микросхемы периферийного устройства через четвёртый интерфейс 15, при этом неизменяемый код корня доверия, находящийся в блоке неизменяемой памяти 3, обеспечивает функции загрузки, проверки целостности и аутентичности программного кода расширения функционала аппаратного модуля доверенной загрузки с использованием криптографических алгоритмов при подключении вычислительного ядра 2 к внешней микросхеме хранения данных 112 через второй интерфейс 17, при этом обеспечена возможность генерации информации для аутентификации микросхемы периферийного устройства с использованием криптографических алгоритмов, и через любой первый и третий интерфейсы 16 и 18 её передачи контроллеру безопасности 113, при этом модуль интегрирован в кристалл микросхемы периферийного устройства.

Основными функциями предлагаемой модели являются: проверка считываемого с внешнего источника 112 программного кода на его целостность и аутентичность, а также генерация и выдача идентифицирующей интегральную микросхему периферийного устройства ПО информации для его последующей аутентификации на уровне системы контроллером безопасности вычислительной платформы 113.

Функционирование интегрированного модуля доверенной загрузки 1 периферийного устройства осуществляется следующим образом:

1. Производится проверка целостности неизвлекаемого корня доверия, находящегося в блоке ПЗУ 3.

2. Производится аутентификация считываемого с внешнего носителя данных 112 программного кода.

3. Производится проверка целостности считываемого с внешнего носителя данных 112 программного кода.

4. Производится генерация и передача идентифицирующей устройство информации и статус загрузки следующему звену системной цепи доверия - контроллеру безопасности вычислительной платформы 113.

Проверка целостности неизвлекаемого корня доверия: исполняемая из ПЗУ 3 программа считывает данные из ПЗУ 3, производит вычисление хэш-функции и сравнивает результат с эталонным значением в ОППЗУ 11, установленного на этапе производства.

Аутентификация кода: исполняемая из ПЗУ 3 программа считывает подтверждающую подлинность информацию с внешнего носителя 112 и используя блок ускорителей асимметричных алгоритмов шифрования 10 выполняет процедуру аутентификации путём проверки электронной подписи считываемого кода. Далее программа передаёт управление процедуре проверки целостности считываемого кода расширения функционала устройства.

Проверка целостности считываемого кода: исполняемая из ПЗУ 3 программа считывает данные программного кода расширения функционала устройства и, используя блок ускорителей симметричных алгоритмов шифрования 9 путём вычисления значения хеш-функции, производит процедуру проверки целостности. Далее программа переходит на выполнение процедуры передачи статуса загрузки и информации для аутентификации устройства.

Передача статуса загрузки и информации для аутентификации: исполняемая из ПЗУ 3 программа на основе зафиксированного в ОППЗУ 11 на этапе производства уникального кода, используя блок ускорителей симметричных алгоритмов шифрования

9 и блок асимметричных алгоритмов шифрования 10, формирует информацию для аутентификации микросхемы устройства. Далее, используя интерфейс I^2C 16 или GPIO 18, интегральная микросхема устройства 110 передаёт информацию для аутентификации следующему звену цепи доверенной загрузки - внешнему устройству, производящему аутентификацию - контроллеру безопасности вычислительной платформы. Информация для аутентификации представляет собой значение криптографической хеш-функции идентификатора устройства, программного кода, хранящегося в ПЗУ 3, и программного кода, загружаемого с внешнего носителя 112.

Блок ускорителей симметричных алгоритмов шифрования 9 поддерживает следующие стандарты:

Зарубежные:

AES с режимами ECB, CBC, OFB, CTR и CTS, размер ключа 128, 192, и256-бит.

XTS-AES, размер ключа 256 и 512 бит.

AES MAC, размер ключа 128, 192, и 256-бит.

Triple-DES режимами ECB и CBC.

Генерации хеш-функции SHA-1, SHA-256, и SHA-512.

Генерации HMAC SHA-256

Отечественные:

ГОСТ Р 34.12 ("кузнечик" и "магма")

ГОСТ Р 34.13 режимы работы блочных шифров ("кузнечик" и "магма")

ГОСТ Р 34.11

Блок ускорителей асимметричных алгоритмов шифрования 10 поддерживает следующие стандарты: Зарубежные:

RSA для генерации и проверки цифровой подписи с 2048-битным ключом

ECDSA генерации и проверки цифровой подписи используя P-256 кривую, с SHA-256 цифровой подписью.

Отечественные:

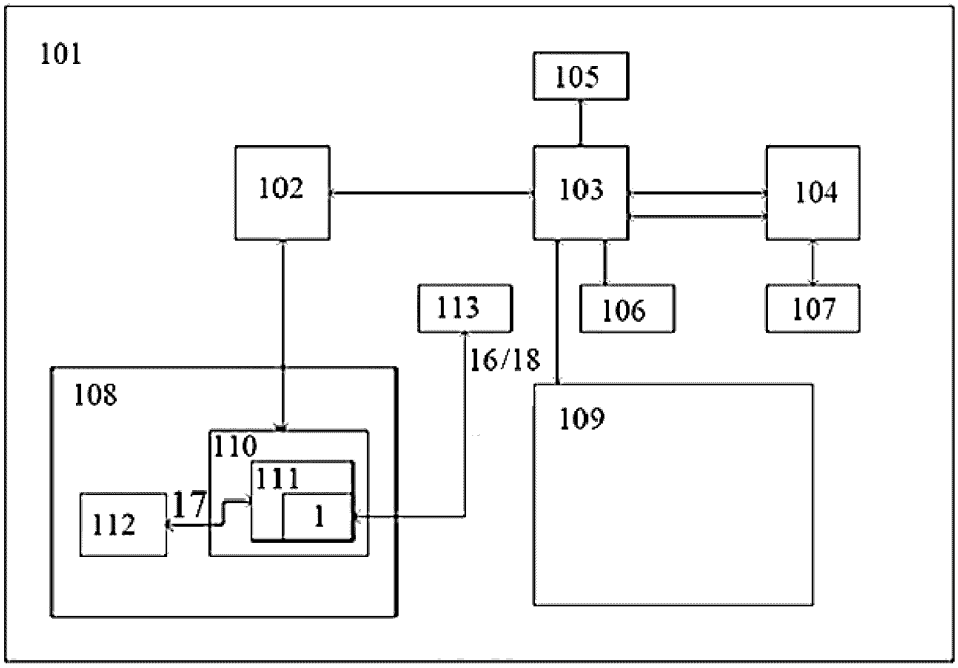
ГОСТ Р 34.10.

(57) Формула полезной модели

Интегрированный модуль доверенной загрузки периферийного устройства, содержащий вычислительное ядро, соединенное с блоком неизменяемой памяти, содержащим неизменяемый код корня доверия, блоком изменяемой памяти, блоком ввода-вывода SMBUS/I2C, снабженным первым интерфейсом, и соединенное с блоком ввода-вывода QSPI/SPI, снабженным вторым интерфейсом, отличающийся тем, что вычислительное ядро дополнительно соединено с блоком ввода-вывода GPIO, снабженным третьим интерфейсом, блоком генерации случайного числа, блоком ускорителей симметричных алгоритмов шифрования, блоком ускорителей асимметричных алгоритмов шифрования, блоком однократно программируемого постоянного запоминающего устройства, блоком установки и контроля временных интервалов, блоком контроля параметров напряжения и температуры и блоком безопасного обмена данными для взаимодействия вычислительного ядра с основным вычислительным ядром микросхемы периферийного устройства через четвёртый интерфейс, при этом неизменяемый код корня доверия находящийся в блоке неизменяемой памяти обеспечивает функции загрузки, проверки целостности и аутентичности программного кода расширения функционала аппаратного модуля доверенной загрузки с использованием криптографических алгоритмов при подключении вычислительного ядра к внешней микросхеме хранения данных через второй интерфейс,

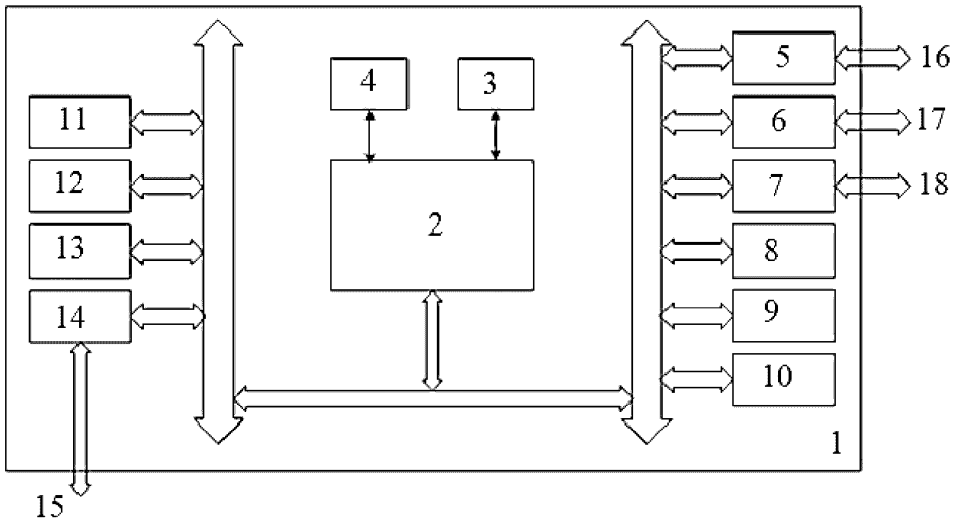
при этом обеспечена возможность генерации информации для аутентификации микросхемы периферийного устройства с использованием криптографических алгоритмов, и через любой первый и третий интерфейсы ее передачи контроллеру безопасности, при этом модуль интегрирован в кристалл микросхемы периферийного устройства.

1



Фиг.1

2



Фиг.2