РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 670 414**(13) **C1**

(51) МПК
B41J 2/175 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК
B41J 2/175 (2006.01)

(21)(22) Заявка: **2017121978, 22.06.2017**

(24) Дата начала отсчета срока действия патента:
30.08.2013

Дата регистрации:
22.10.2018

Приоритет(ы):
Номер и дата приоритета первоначальной заявки, из которой данная заявка выделена:
2016106349 30.08.2013

(45) Опубликовано: **22.10.2018** Бюл. № **30**

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

(72) Автор(ы):
УОРД Джефферсон П (US),
ПАНШИН Стефен Д (US)

(73) Патентообладатель(и):
ХЬЮЛЕТТ-ПАККАРД ДИВЕЛОПМЕНТ КОМПАНИ, Л.П. (US)

(56) Список документов, цитированных в отчете о поиске: **WO 2013048430 A1, 04.04.2013. US 2010224682 A1, 09.09.2010. WO 2006052111 A1, 18.05.2006. US 2004223011 A1, 11.11.2004.**

(54) АУТЕНТИФИКАЦИЯ ПОСТАВКИ ЧЕРЕЗ ОТВЕТ НА ЗАПРОС СОГЛАСОВАНИЯ ПО ВРЕМЕНИ

(57) Реферат:

Устройство предназначено для облегчения аутентификации печатающего картриджа, содержит память и логическую схему для приема запроса согласования по времени от хост-устройства и обеспечения возможности аутентификации картриджа при предоставлении ответа на запрос во время ответа на запрос, которое попадает в ожидаемое временное окно, при этом логическая схема предназначена для выполнения математического вычисления в ответ на запрос согласования по времени, при этом вычисление выдает ответ на запрос в ожидаемом временном окне. 5 н. и 10 з.п. ф-лы, 5 ил.

RU 2670414 C1

RU 2670414 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 670 414**(13) **C1**

(51) Int. Cl.
B41J 2/175 (2006.01)

(12) ABSTRACT OF INVENTION

(52) CPC
B41J 2/175 (2006.01)

(21)(22) Application: **2017121978, 22.06.2017**

(24) Effective date for property rights:
30.08.2013

Registration date:
22.10.2018

Priority:
Number and date of priority of the initial application, from which the given application is allocated:
2016106349 30.08.2013

(45) Date of publication: **22.10.2018** Bull. № **30**

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

(72) Inventor(s):
PANSHIN, Stephen D (US),
WARD, Jefferson P (US)

(73) Proprietor(s):
HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P. (US)

RU 2670414 C1

(54) AUTHENTICATION OF DELIVERY THROUGH RESPONSE TO TIME MATCHING REQUEST

(57) Abstract:

FIELD: information technology.

SUBSTANCE: device is designed to facilitate the authentication of the print cartridge, comprises a memory and a logic circuit for receiving the time-matching request from the host device and enabling the cartridge to be authenticated upon providing a response to the request during the response to the request, which falls into the expected time window, wherein the logic circuit is designed to perform the mathematical calculation in response to the time matching request, wherein the calculation issues a response to the request in the expected time window.

EFFECT: facilitating the authentication of the print cartridge.

15 cl, 5 dwg

RU 2670414 C1

Уровень техники

[0001] Многие системы имеют заменяемые компоненты, которые являются неотъемлемой частью для функционирования системы. Заменяемые компоненты зачастую являются устройствами, которые содержат расходный материал, который убывает с каждым использованием системы. Такие системы могут включать в себя, например, сотовые телефоны, которые используют заменяемые аккумуляторы, медицинские системы, которые распределяют лекарства из заменяемых поставляемых устройств, системы печати, которые распределяют текучие среды (например, чернила) или тонеры из заменяемых поставляемых картриджей и т.д. Проверка того, что заменяемое поставляемое устройство является подлинным устройством от легального производителя, может помогать пользователю системы избегать проблем, связанных с непреднамеренным использованием дефектного и/или поддельного устройства.

Краткое описание чертежей

[0002] Настоящие варианты осуществления будут теперь описаны посредством примера со ссылкой на прилагаемые чертежи, на которых:

[0003] Фиг. 1 показывает блок-схему, иллюстрирующую компоненты примера, характерной системы аутентификации, подходящей для аутентификации (проверки подлинности) заменяемого поставляемого устройства;

[0004] Фиг. 2 показывает пример характеристических данных, сохраненных в заменяемом поставляемом устройстве;

[0005] Фиг. 3 показывает пример системы аутентификации, осуществленной в качестве системы струйной печати;

[0006] Фиг. 4 показывает перспективный вид примерного поставляемого картриджа для струйной печати;

[0007] Фиг. 5 показывает блок-схему примерного процесса аутентификации поставки.

[0008] Повсюду на чертежах идентичные ссылочные номера обозначают аналогичные, но не обязательно идентичные, элементы.

Подробное описание изобретения

Обзор

[0009] Как отмечено выше, подтверждение подлинности заменяемых поставляемых устройств для использования в некоторых системах может помогать пользователям системы избегать проблем, связанных с непреднамеренным использованием дефектных и/или поддельных устройств. Например, в системах печати, которые применяют расходуемые картриджи с тонером или чернилами, непреднамеренная замена картриджей поддельными картриджами может приводить в результате к различным проблемам, простирающимся в диапазоне от отпечатков плохого качества до протекающих картриджей, которые могут повреждать систему печати.

[0010] Предшествующие способы аутентификации заменяемого устройства включали в себя применение строгой аутентификации, которая подразумевает использование секретного ключа, известного смарт-карте, или микроконтроллера безопасности на заменяемом устройстве (например, расходуемом картридже с чернилами/тонером) и хост-устройстве (например, принтере). Если заменяемое устройство может предоставлять ответ на запрос, выданный хостом, который доказывает, что оно содержит соответствующий ключ, хост сделает вывод, что устройство оригинального производства, и затем аутентифицирует устройство. Одним слабым местом с этим способом аутентификации является то, что он полагается на способность системы сохранять секретный ключ. Если злоумышленник может восстанавливать ключ или ключи либо с хоста, либо заменяемого устройства, он может сохранять украденный

ключ(и) в смарт-карте или микроконтроллере, предоставляя возможность им затем создавать заменяемые устройства, которые будут отвечать на запросы, как если бы такие устройства были подлинными устройствами от оригинального производителя. Типично, после того как ключ(и) компрометируется, ответ на запрос и другая функциональность неподлинного (т.е. поддельного) заменяемого устройства может быть сымитирована с помощью микропрограммного обеспечения, работающего на недорогом, стандартном микроконтроллере.

[0011] Здесь раскрываются система аутентификации и процессы аутентификации поставки, которые обеспечивают надежную аутентификацию заменяемых устройств системы, в целом, через ответ на запрос согласования по времени. Хост, такой как принтер, выдает криптографический запрос согласования по времени микроконтроллеру безопасности, присоединенному к заменяемому устройству, такому как расходуемый картридж с чернилами или тонером. Запрос требует, чтобы расходное устройство (т.е. микроконтроллер на расходном устройстве) выполняло ряд математических операций на основе данных, предоставленных хостом/принтером. Принтер контролирует интервал времени, который затрачивается, чтобы расходное устройство выполнило задачу, и независимо подтверждает ответ, предоставленный устройством. Если и ответ, и прошедшее время при вычислении ответа удовлетворяют ожиданиям принтера, принтер сделает вывод, что устройство является подлинным устройством. Если либо ответ, либо время, прошедшее во время вычисления ответа (или и то, и другое), не удовлетворяет ожиданиям принтера, принтер сделает вывод, что устройство не является подлинным устройством.

[0012] Математические операции из запроса выполняются в микроконтроллере расходного устройства посредством специализированной аппаратной логической схемы, специально разработанной для таких операций. Специализированная логическая схема способна выполнять ответ на запрос, выполняя математические вычисления значительно быстрее, чем может быть в ином случае выполнено посредством стандартного микроконтроллера, исполняющего микропрограммное обеспечение. Таким образом, неподлинное/поддельное заменяемое устройство, в котором микроконтроллер содержит украденный ключ(и), может иметь возможность выдавать правильный ответ на запрос. Однако такое поддельное устройство не имеет возможности выдавать ответ на запрос во временных рамках, ожидаемых хост-устройством.

[0013] В примерной реализации печатающий поставляемый картридж включает в себя микроконтроллер для приема запроса согласования по времени и обеспечения возможности аутентификации картриджа при предоставлении ответа на запрос во время ответа на запрос, которое попадает в ожидаемое временное окно. В другой реализации картридж дополнительно включает в себя специализированную аппаратную логическую схему на микроконтроллере для выполнения математического вычисления в ответ на запрос согласования по времени. Выполнение математического вычисления выдает ответ на запрос в ожидаемом временном окне.

[0014] В другой примерной реализации заменяемое поставляемое устройство включает в себя микроконтроллер. Микроконтроллер должен получать ключ сеанса с хост-устройством и принимать времязависимый запрос от хост-устройства, который указывает случайное начальное число, ключ сеанса и цикл вычисления. Заменяемое устройство дополнительно включает в себя специализированную логическую схему в микроконтроллере для выполнения вычисления запроса число раз, равное циклу вычисления, при этом первое вычисление использует случайное начальное число и ключ сеанса для создания выходных данных, а каждое последующее вычисление

использует выходные данные предшествующего вычисления.

[0015] В другой примерной реализации система аутентификации включает в себя хост-устройство, контроллер, интегрированный в хост-устройство, и алгоритм аутентификации, исполняемый в контроллере, для выдачи криптографического запроса согласования по времени и аутентификации поставляемого устройства, когда поставляемое устройство предоставляет ответ на запрос во время ответа на запрос, которое попадает в ожидаемое временное окно.

[0016] В другой примерной реализации система аутентификации включает в себя принтер, который имеет контроллер и память. Система аутентификации также включает в себя алгоритм аутентификации, сохраненный в памяти и исполняемый в контроллере, для выдачи криптографического запроса согласования по времени и аутентификации печатающего поставляемого картриджа, когда картридж предоставляет ответ на запрос, соответствующий ожидаемому ответу, в ожидаемом временном окне.

[0017] В другой примерной реализации невременный, считываемый процессором носитель хранит код, представляющий команды, которые, при исполнении процессором, заставляют процессор распознавать поставляемое устройство и выдавать криптографический запрос согласования по времени поставляемому устройству. Запрос согласования по времени требует, чтобы математическое вычисление было выполнено по данным, которые включают в себя ключ сеанса, случайное начальное число и счет вычислений. Команды дополнительно заставляют процессор принимать ответ на запрос во время ответа на запрос от поставляемого устройства и аутентифицировать поставляемое устройство, когда ответ на запрос соответствует ожидаемому ответу, и время ответа на запрос попадает в ожидаемое временное окно.

Примерные реализации

[0018] Фиг. 1 показывает блок-схему, иллюстрирующую компоненты примерной, характерной системы 100 аутентификации, подходящей для аутентификации заменяемого поставляемого устройства. Система 100 аутентификации включает в себя хост-устройство 102 и заменяемое поставляемое устройство 104. Хост-устройство 102 содержит контроллер 106, который типично включает в себя компоненты стандартной вычислительной системы, такие как центральный процессор (ЦПУ) 108, память 110, микропрограммное обеспечение и другие электронные устройства для управления общими функциями системы 100 аутентификации и для связи и управления поставляемым устройством 104. Память 110 может включать в себя как энергозависимые (т.е. RAM), так и энергонезависимые (например, ROM, жесткий диск, гибкий диск, CD-ROM и т.д.) компоненты памяти, содержащие невременные компьютерные/считываемые процессором носители, которые обеспечивают хранение компьютерных/считываемых процессором закодированных команд и/или данных в форме алгоритмов, программных модулей, структур данных, JDF и т.д. Поставляемое устройство 104 содержит микроконтроллер 112 (т.е. смарт-карту), которое также включает в себя центральный процессор (ЦПУ) 114 и память 116.

[0019] В целом, при включении питания хост-устройства 102, хост-устройство 102 и поставляемое устройство 104 устанавливают безопасные связи посредством стандартных криптографических методов с помощью стандартных криптографических алгоритмов 118. Например, выполняя криптографический алгоритм 118 (т.е. на процессоре 108), хост-устройство 102 может запрашивать уникальный идентификационный код 120 поставляемого устройства 104 и определять "базовый ключ" 122 устройства через криптографическую связь. С помощью базового ключа 122 хост-устройство и поставляемое устройство могут получать секретный "ключ сеанса" 124,

предоставляющий возможность безопасной связи для текущего обмена информацией. Хост-устройство 102 определяет базовый ключ 122 таким образом каждый раз, когда оно включается, и каждый раз, когда устанавливается новое поставляемое устройство 104. Базовый ключ 122 остается одним и тем же и не меняется. Однако новый и отличающийся ключ 124 сеанса получается каждый раз, когда между хост-устройством 102 и поставляемым устройством 104 выполняется обмен информацией.

[0020] В одной реализации память 110 включает в себя алгоритм 126 аутентификации, исполняемый на процессоре 108 контроллера 106 для определения подлинности заменяемого поставляемого устройства 104. Поставляемое устройство 104 определяется как подлинное, когда оно отвечает правильно на криптографический запрос 128 согласования по времени, выданный посредством алгоритма 126 аутентификации, и когда его ответ 130 на запрос выполняется в ожидаемом окне времени. Таким образом, поставляемое устройство 104, значение 130 ответа на запрос которого является правильным, но время 131 ответа на запрос которого не попадает в ожидаемое окно времени, определяется как неподлинное. Аналогично, поставляемое устройство 104, время 131 ответа на запрос которого попадает в ожидаемое окно времени, но значение 130 ответа на запрос которого является неправильным, определяется как неподлинное. Подлинность поставляемого устройства 104, следовательно, зависит от того, предоставляет ли оно правильный ответ 130 на криптографический запрос 128 согласования по времени в интервал времени 131 ответа на запрос (т.е. времени, которое оно затрачивает для предоставления ответа 130), который попадает в ожидаемое окно времени.

[0021] Криптографический запрос 128 согласования по времени, выданный посредством алгоритма 126 аутентификации на хост-устройстве 102, содержит запрос выполнения специального математического вычисления, объединяющего некоторые параметры запроса. Математическое вычисление должно выполняться конкретное число раз. Криптографический запрос 128 согласования по времени включает в себя или сопровождается такими параметрами запроса, которые включают в себя полученный ключ сеанса, случайное начальное число, сгенерированное на хост-устройстве 102 контроллером 106, и счет вычислений или цикл, который указывает число раз, которое вычисление должно быть выполнено. Математическое вычисление использует ключ сеанса и начинает с операции над случайным начальным числом. Результат или выходные данные каждого вычисления повторно подаются обратно в следующее вычисление до тех пор, пока не будет достигнут счет вычислений. Последний результат или выходные данные математического вычисления предоставляют ответ 130 на запрос, который должен быть достигнут или вычислен в конкретное время 131 ответа на запрос. Время 131 ответа на запрос измеряется посредством алгоритма 126 аутентификации, например, начиная последовательность согласования по времени, когда запрос выдается, и останавливая последовательность согласования по времени, после того как поставляемое устройство 104 заканчивает и возвращает ответ 130 на запрос хост-устройству 102. Время 131 ответа на запрос является временным значением, которое в некоторых реализациях может недолго находиться на хост-устройстве 102 в энергозависимом компоненте памяти 110 и/или в процессоре 108 перед или во время сравнения с временным окном, определенным посредством хоста. Алгоритм 126 аутентификации на хосте 102 определяет, являются или нет ответ 130 на запрос и время 131 ответа на запрос правильными (т.е. ожидаемыми), и затем аутентифицирует поставляемое устройство 104 соответствующим образом.

[0022] Обращаясь все еще к фиг. 1, микроконтроллер 112 на поставляемом устройстве

104 содержит специализированную аппаратную логическую схему 132 запроса для выполнения математического вычисления из криптографического запроса 128 согласования по времени. Специализированная логическая схема 132 запроса специально разрабатывается и изготавливается на микроконтроллере 112 для оптимального выполнения конкретного математического вычисления.

В одной примерной реализации математическое вычисление содержит базовую функцию, которая определяет последовательность операций, оптимизированных для очень быстрой работы в специализированной логической схеме 132. Математическое вычисление или функция повторяется множество раз с выходными данными каждой итерации, являющимися частью входных данных для следующей итерации. Таким образом, в то время как один или более операндов изменяются с каждой итерацией математического вычисления, само математическое вычисление не изменяется. Кроме того, значения параметров запроса, сопровождающие запрос 128 согласования по времени, могут изменяться с каждым запросом 128 согласования по времени. Каждый запрос 128 согласования по времени, выданный посредством алгоритма 126 аутентификации поставляемому устройству 104, может иметь различные значения для ключа сеанса, случайного начального числа, сгенерированного на хост-устройстве 102 контроллером 106, и счета или цикла вычислений. Соответственно, для каждого запроса 128 согласования по времени, ответ 130 на запрос и время 131 ответа на запрос определяются по значениям параметра запроса. Более конкретно, ключ сеанса, случайное начальное число и счет вычислений, все отрицательно влияют на значение 130 ответа на запрос, в то время как счет вычислений также отрицательно влияет на время 131 ответа на запрос, изменяя число итераций математического вычисления посредством специализированной логической схемы 132 запроса.

[0023] Как отмечено выше, алгоритм 126 аутентификации определяет, являются ли ответ 130 на запрос и время 131 ответа на запрос правильными или ожидаемыми. Это выполняется посредством сравнения ответа 130 на запрос и времени 131 ответа с правильными или ожидаемыми значениями. В различных реализациях алгоритм 126 определяет правильные или ожидаемые значения различными способами. В одной реализации, например, алгоритм 126 извлекает и осуществляет доступ к характеристическим данным 134, сохраненным на поставляемом устройстве 104. Характеристические данные 134 могут быть защищены цифровой подписью и подтверждены с помощью стандартных криптографических операций. Характеристические данные 134 предоставляют ожидаемые временные окна, в которые время 131 ответа на запрос должно попадать в зависимости от счета вычислений, снабженного запросом 128 согласования по времени. Таким образом, в одном примере, как показано на фиг. 2, характеристические данные 134 могут включать в себя таблицу данных, которая связывает различные значения счета вычислений с различными временными окнами. Только в качестве примера, такая связь может указывать, что для счета вычислений, равного 10000 (т.е. когда математическое вычисление должно быть выполнено 10000 раз), время 131 ответа на запрос ожидается попадающим во временное окно 50-55 миллисекунд. В другом примере характеристические данные 134 могут быть предоставлены через математическое отношение, такое как формула прямой с угловым коэффициентом, $y=mx+b$. Таким образом, для данного значения счета вычислений, x, может быть определено ожидаемое время, y. Временное окно может затем быть определено посредством алгоритма 126 аутентификации на хосте 102, например, с помощью ожидаемого времени y, +/-5%.

[0024] В другой примерной реализации алгоритм 126 аутентификации определяет

правильные или ожидаемые значения для ответа 130 на запрос, выдавая криптографический запрос 128 согласования по времени специализированной эталонной логической схеме 136 на контроллере 106 хост-устройства. Эталонная логическая схема 136 на контроллере 106 зеркально отражает специализированную аппаратную логическую схему 132 на поставляемом устройстве 104 и, следовательно, специально разработана и изготавливается на контроллере 106 для оптимального выполнения математического вычисления из запроса 128 согласования по времени. Таким образом, когда алгоритм 126 аутентификации выдает запрос 128 согласования по времени поставляемому устройству 104, он также выдает запрос 128 согласования по времени эталонной логической схеме 136. Эталонная логическая схема 136 выполняет математические вычисления из запроса тем же образом, который обсужден выше относительно специализированной аппаратной логической схемы 132 на поставляемом устройстве 104. В ответ на запрос 128 согласования по времени эталонная логическая схема 136 завершает запрос и предоставляет эталонный ответ в эталонное время. Эталонное временное окно ответа может быть определено, например, как находящееся в пределах определенного процента (например, +/-5%, +/-10%) эталонного времени. Алгоритм 126 аутентификации может затем использовать эталонный ответ и эталонное временное окно ответа в качестве значений для сравнения с ответом 130 на запрос и временем 131 ответа на запрос. Если ответ 130 на запрос совпадает с эталонным ответом, а время 131 ответа на запрос попадает в эталонное временное окно ответа, алгоритм 126 определяет, что поставляемое устройство 104 является подлинным устройством.

[0025] Фиг. 3 показывает пример системы 100 аутентификации, осуществленной в качестве системы 300 струйной печати. В целом, система 300 печати содержит те же или аналогичные компоненты, что и общая система 100 аутентификации, и функционирует тем же или аналогичным образом относительно аутентификации заменяемых струйных поставляемых картриджей. В примерной реализации система 300 струйной печати включает в себя механизм 302 печати, имеющий контроллер 106, сборочный узел 304, одно или более заменяемых поставляемых устройств 104, осуществленных как картриджи 306 для подачи чернил, и по меньшей мере один источник 308 питания, который снабжает питанием различные электрические компоненты системы 300 струйной печати. Система 300 печати дополнительно включает в себя узел 310 транспортировки носителей.

[0026] Фиг. 4 показывает перспективный вид примерного струйного поставляемого картриджа 306, который представляет заменяемое поставляемое устройство 104. В дополнение к одной или более печатающим головкам 312, струйный картридж 306 включает в себя микроконтроллер 112, группу электрических контактов 400 и камеру 402 для подачи чернил (или другой текучей среды). В некоторых реализациях картридж 306 может иметь камеру 402 для подачи, которая хранит один цвет чернил, а в других реализациях он может иметь ряд камер 402, каждая из которых хранит различный цвет чернил. Электрические контакты 400 передают электрические сигналы от контроллера 106 к соплам 314 на печатающей головке 312, чтобы обусловить выброс капель текучей среды. Электрические контакты 400 также передают электрические сигналы между контроллером 106 и микроконтроллером 112 для облегчения аутентификации картриджа 306 в системе 300 струйной печати. В одной примерной реализации микроконтроллер 112 располагается на кремниевой подложке, совместно используемой с печатающей головкой 312. В другой примерной реализации микроконтроллер 112 располагается где-либо еще на картридже 306 в качестве обособленной смарт-карты. Микроконтроллер 112 аналогичен микроконтроллеру 112, показанному на фиг. 1 и обсужденному выше,

и включает в себя те же общие компоненты (не все показаны на фиг. 4). Таким образом, микроконтроллер 112 на картридже 306 содержит память 116 и специализированную логическую схему 132 запроса, которая функционирует тем же общим образом, который обсужден выше относительно системы 100 аутентификации по фиг. 1 и 2.

[0027] Обращаясь к фиг. 3 и 4, печатающая головка 312 выбрасывает капли чернил или другой текучей среды через множество отверстий или сопел 314 по направлению к печатному носителю 316 с тем, чтобы печатать на печатном носителе 316. Печатные носители 316 могут быть любым типом подходящего листового или рулонного материала, такого как бумага, стопка карточек, слайды, майлар, полиэстер, фанера, вспененный картон, полотно, холст и т.п. Печатающая головка 312 может быть выполнена с возможностью выброса чернил через сопла 314 множеством способов. Например, термическая струйная печатающая головка выбрасывает капли из сопла при пропускании электрического тока через нагревательный элемент с образованием тепла и испарением небольшой части чернил в камере сгорания. Пузырьки пара подталкивают каплю чернил через сопло 314. В другом примере пьезоэлектрическая струйная печатающая головка использует привод из пьезоэлектрического материала с образованием импульсов давления, которые подталкивают капли чернил из сопла. Сопла 314 типично размещаются в одном или более рядах или матрицах по печатающей головке 312, так что правильно упорядоченный выброс чернил из сопел 314 вызывает печать букв, символов и/или других графических знаков или изображений на печатных носителях 316, в то время как струйный картридж 306 и печатные носители 316 движутся относительно друг друга.

[0028] Монтажный узел 304 позиционирует струйный картридж 306 относительно узла 310 транспортировки носителей, а узел 310 транспортировки носителей позиционирует печатные носители 316 относительно струйного картриджа 306. Таким образом, зона 318 печати определяется рядом с соплами 314 в области между струйным картриджем 306 и печатными носителями 316. В одной реализации механизм 302 печати является механизмом 302 печати сканирующего типа. По существу, монтажный узел 304 включает в себя каретку для перемещения струйного картриджа 306 относительно узла 310 транспортировки носителей, чтобы сканировать печатные носители 316. В другой реализации механизм 302 печати является механизмом 302 печати несканирующего типа. По существу, сборочный узел 304 фиксирует струйный картридж 306 в предписанном положении относительно узла 310 транспортировки носителей, в то время как узел 310 транспортировки носителей позиционирует печатные носители 316 относительно струйного картриджа 306.

[0029] Как отмечено выше относительно системы 100 аутентификации по фиг. 1, контроллер 106 типично включает в себя компоненты стандартной вычислительной системы, такие как центральный процессор (ЦПУ) 108, память 110, микропрограммное обеспечение и другие электронные устройства. В системе 300 струйной печати по фиг. 3 контроллер 106 аналогично применяет такие компоненты для управления общими функциями системы 300 печати и для связи и управления струйным картриджем 306, монтажным узлом 304 и узлом 310 транспортировки носителей. Соответственно, контроллер 106 принимает данные 320 от хост-системы, такой как компьютер, и временно сохраняет данные 320 в памяти 110. Типично, данные 320 отправляются системе 300 струйной печати по электронному, инфракрасному, оптическому или другому пути передачи информации. Данные 320 представляют, например, документ и/или файл, который должен быть напечатан. По существу, данные 320 формируют задание печати для системы 300 струйной печати, которые включают в себя одну или

более команд задания печати и/или параметров команды. С помощью данных 320 контроллер 106 управляет струйным картриджем 306 для выброса капель чернил из сопел 314. Таким образом, контроллер 106 определяет рисунок выбрасываемых капель чернил, которые формируют буквы, символы и/или другие графические знаки или изображения на печатном носителе 316. Рисунок выбрасываемых капель чернил определяется командами задания печати и/или параметрами команды из данных 320.

[0030] В дополнение к управлению общими функциями печати системы 300 струйной печати, контроллер 106 выполняет алгоритм 126 аутентификации для определения, является ли струйный поставляемый картридж 306 подлинным устройством. Этот процесс аутентификации в системе 300 печати аналогичен процессу, описанному выше относительно общей системы 100 аутентификации по фиг. 1. Фиг. 5 - это блок-схема примерного процесса 500 аутентификации в системе 300 печати или другой системе 100 аутентификации, который определяет, является ли заменяемое поставляемое устройство 104, такое как струйный поставляемый картридж 306, подлинным устройством. Процесс 500 соответствует примерным реализациям, обсужденным выше относительно фиг. 1-4, и подробности этапов, показанных в процессе 500, могут быть найдены в связанном обсуждении таких реализаций. Этапы процесса 500 могут быть осуществлены в виде алгоритма, содержащего программно-ориентированные команды, сохраненные на невременном компьютерном/считываемом процессором носителе, таком как память 110 по фиг. 1 и 3. В различных примерах реализация этапов процесса 500 выполняется посредством считывания и выполнения таких программно-ориентированных команд процессором, таким как процессор 108 по фиг. 1 и 3. Процесс 500 может включать в себя более чем одну реализацию, и различные реализации процесса 500 могут не применять каждый этап, представленный в блок-схеме по фиг. 5. Следовательно, в то время как этапы процесса 500 представляются в конкретном порядке в блок-схеме, порядок их представления не предназначается быть ограничением относительно порядка, в котором этапы могут фактически быть реализованы, или относительно того, могут ли все из этапов быть реализованы. Например, одна реализация процесса 500 может быть осуществлена посредством выполнения ряда первоначальных этапов, без выполнения одного или более последующих этапов, в то время как другая реализация процесса 500 может быть осуществлена посредством выполнения всех этапов.

[0031] Обращаясь теперь, прежде всего, к фиг. 1, 3 и 5, процесс 500 аутентификации начинается на этапе 502, где первый показанный этап должен распознавать заменяемое поставляемое устройство. Распознавание заменяемого поставляемого устройства типично происходит при включении питания хост-устройства или вставке нового поставляемого устройства в хост-устройство, например, когда система печати включается или когда печатающий поставляемый картридж с чернилами или тонером заменяется в системе печати. Заменяемое поставляемое устройство может также быть распознано, когда поставляемое устройство включается в начале каждого задания печати. Процесс 500 аутентификации продолжается на этапе 504, где выдается криптографический запрос согласования по времени. Запрос согласования по времени выдается из хост-устройства, такого как печатающее устройство, и отправляется поставляемому устройству, такому как печатающий поставляемый картридж. Запрос согласования по времени содержит запрос на выполнение специального математического вычисления, затрагивающего некоторые параметры запроса, которые включают в себя ключ сеанса, полученный между хост-устройством и поставляемым устройством, случайное начальное число, сгенерированное хост-устройством, и счет или цикл вычислений, который указывает число раз, которое вычисление должно быть выполнено.

При выдаче запроса согласования по времени, хост-устройство может начинать последовательность согласования по времени для контроля времени, которое затрачивается для приема ответа на запрос, как показано на этапе 506.

[0032] В некоторых реализациях запрос согласования по времени может также быть отправлен эталонной логической схеме на хост-устройстве, как показано на этапе 508. Когда запрос согласования по времени отправляется эталонной логической схеме в хост-устройстве, эталонный ответ принимается от логической схемы в определенном интервале прошедшего эталонного времени, как показано на этапе 510. На этапе 512 может быть определено эталонное временное окно при включении в него диапазона около эталонного времени, равного определенному проценту. Например, эталонное временное окно может быть определено как эталонное время плюс или минус 5% от эталонного времени. В некоторых реализациях, в качестве альтернативы отправке запроса согласования по времени эталонной логической схеме на хост-устройстве, хост-устройство извлекает и осуществляет доступ к характеристическим данным, сохраненным на поставляемом устройстве, как показано на этапе 514. В другой реализации характеристические данные могут быть жестко закодированы в память хост-устройства. Характеристические данные включают в себя ожидаемые временные окна для приема ответа на запрос от поставляемого устройства, которые связаны с различными значениями счета вычислений.

[0033] Как показано на этапе 516, процесс 500 аутентификации включает в себя прием ответа на запрос от поставляемого устройства. Ответ на запрос принимается в определенное время ответа на запрос, которое может быть определено, например, при измерении времени на хост-устройстве. Процесс 500 продолжается на этапе 518 сравнением ответа на запрос с ожидаемым ответом. Ожидаемый ответ может быть эталонным ответом, принятым от эталонной логической схемы на хост-устройстве. На этапе 520 время ответа на запрос также сравнивается с ожидаемым временным окном ответа для определения, попадает ли время ответа на запрос в ожидаемое временное окно. Ожидаемое временное окно может быть эталонным временным окном или ожидаемым временным окном, извлеченным из характеристических данных, сохраненных на поставляемом устройстве или где-либо еще.

[0034] Процесс 500 аутентификации продолжается на этапе 522 аутентификацией хост-устройством поставляемого устройства, когда ответ на запрос от поставляемого устройства совпадает с ожидаемым значением, и время ответа на запрос попадает в ожидаемое временное окно. На этапе 524 процесса 500 хост-устройство определяет, что поставляемое устройство не является подлинным, когда или ответ на запрос не совпадает с ожидаемым значением, или время ответа на запрос попадает за пределы ожидаемого временного окна, либо в обоих случаях.

[0035] Теперь будут описаны дополнительные варианты осуществления.

[0036] Первый вариант осуществления обеспечивает печатающий поставляемый картридж, содержащий микроконтроллер для приема запроса согласования по времени и предоставления возможности аутентификации картриджа при предоставлении ответа на запрос во время ответа на запрос, которое попадает в ожидаемое временное окно.

[0037] Второй вариант осуществления обеспечивает картридж по первому варианту осуществления, дополнительно содержащий специализированную аппаратную логическую схему на микроконтроллере для выполнения математического вычисления в ответ на запрос согласования по времени, при этом вычисление выдает ответ на запрос в ожидаемом временном окне.

[0038] Третий вариант осуществления обеспечивает картридж по первому варианту

осуществления, дополнительно содержащий характеристические данные, сохраненные в микроконтроллере, которые включают в себя ожидаемые временные окна для выполнения ответа на запрос.

[0039] Четвертый вариант осуществления обеспечивает картридж по третьему варианту осуществления, при этом каждое ожидаемое временное окно связано со счетом вычислений, который указывает число раз выполнения математического вычисления из запроса согласования по времени.

[0040] Пятый вариант осуществления обеспечивает картридж по второму варианту осуществления, при этом запрос согласования по времени включает в себя параметры запроса, содержащие ключ сеанса, случайное начальное число и счет вычислений, который указывает число раз выполнения математического вычисления.

[0041] Шестой вариант осуществления обеспечивает картридж по пятому варианту осуществления, при этом математическое вычисление работает по ключу сеанса, случайному начальному числу и счету вычислений для определения ответа на запрос.

[0042] Седьмой вариант осуществления обеспечивает картридж по пятому варианту осуществления, при этом время ответа на запрос зависит от счета вычислений.

[0043] Восьмой вариант осуществления обеспечивает картридж по пятому варианту осуществления, дополнительно содержащий уникальный идентификационный код и базовый ключ, из которого получен ключ сеанса.

[0044] Девятый вариант осуществления обеспечивает картридж по первому варианту осуществления, дополнительно содержащий печатающий материал, выбранный из группы, состоящей из чернил и тонера.

[0045] Десятый вариант осуществления обеспечивает заменяемое поставляемое устройство, содержащее микроконтроллер для получения ключа сеанса с хост-устройством и приема времязависимого запроса от хост-устройства, который указывает случайное начальное число, ключ сеанса и цикл вычисления; и специализированную логическую схему в микроконтроллере для выполнения вычисления запроса число раз, равное циклу вычисления, при этом первое вычисление использует случайное начальное число и ключ сеанса для создания выходных данных, а каждое последующее вычисление использует выходные данные предшествующего вычисления.

[0046] Одиннадцатый вариант осуществления обеспечивает поставляемое устройство по десятому варианту осуществления, дополнительно содержащее характеристические данные, сохраненные в памяти микроконтроллера, которые включают в себя различные временные окна для выполнения времязависимых запросов в зависимости от указанных циклов вычислений.

[0047] Двенадцатый вариант осуществления обеспечивает поставляемое устройство по десятому варианту осуществления, дополнительно содержащее печатающий материал, который должен наноситься на печатные носители хост-устройством.

[0048] Тринадцатый вариант осуществления обеспечивает поставляемое устройство по двенадцатому варианту осуществления, при этом печатающий материал выбирается из группы, состоящей из тонера и чернил.

[0049] Четырнадцатый вариант осуществления обеспечивает поставляемое устройство по одиннадцатому варианту осуществления, при этом вычисление запроса содержит ряд математических операций в конкретной последовательности.

[0050] Пятнадцатый вариант осуществления обеспечивает устройство, предназначенное для облегчения аутентификации печатающего картриджа, содержащего память и логическую схему для приема запроса согласования по времени от хост-устройства и обеспечения возможности аутентификации картриджа при предоставлении

ответа на запрос во время ответа на запрос, которое попадает в ожидаемое временное окно.

[0051] Шестнадцатый вариант осуществления обеспечивает устройство по пятнадцатому варианту осуществления, дополнительно содержащее логическую схему для выполнения вычисления в ответ на запрос согласования по времени, при этом вычисление выдает ответ на запрос в ожидаемом временном окне.

[0052] Семнадцатый вариант осуществления обеспечивает устройство по пятнадцатому варианту осуществления, дополнительно содержащее характеристические данные, сохраненные в памяти, которые включают в себя ожидаемые временные окна для выполнения ответа на запрос.

[0053] Восемнадцатый вариант осуществления обеспечивает устройство по пятнадцатому варианту осуществления, дополнительно содержащее характеристические данные, сохраненные в памяти, причем характеристические данные включают в себя счет вычислений и обеспечивают ожидаемые временные окна в зависимости от счета вычислений.

[0054] Девятнадцатый вариант осуществления обеспечивает устройство по пятнадцатому варианту осуществления, при этом время ответа на запрос зависит от счета вычислений, принятого от хост-устройства.

[0055] Двадцатый вариант осуществления обеспечивает устройство по пятнадцатому варианту осуществления, при этом каждое ожидаемое временное окно связано со счетом вычислений, принятым от хост-устройства.

[0056] Двадцать первый вариант осуществления обеспечивает устройство по девятнадцатому варианту осуществления, при этом счет указывает число раз выполнения вычисления из запроса согласования по времени.

[0057] Двадцать второй вариант осуществления обеспечивает устройство по пятнадцатому варианту осуществления, при этом запрос согласования по времени включает в себя параметры запроса, содержащие ключ сеанса, случайное начальное число и счет вычислений, который указывает число раз выполнения вычисления.

[0058] Двадцать третий вариант осуществления обеспечивает устройство по двадцать второму варианту осуществления, при этом вычисление работает по ключу сеанса, случайному начальному числу и счету вычислений для определения ответа на запрос.

[0059] Двадцать четвертый вариант осуществления обеспечивает устройство по пятнадцатому варианту осуществления, дополнительно содержащее уникальный идентификационный код и базовый ключ.

[0060] Двадцать пятый вариант осуществления обеспечивает устройство по пятнадцатому варианту осуществления, содержащее микроконтроллер, который содержит логическую схему и память.

[0061] Двадцать шестой вариант осуществления обеспечивает устройство по пятнадцатому варианту осуществления, дополнительно содержащее печатающий материал, выбранный из группы, состоящей из чернил и тонера.

[0062] Двадцать седьмой вариант осуществления обеспечивает заменяемое устройство, содержащее устройство по одному из вариантов осуществления с пятнадцатого по двадцать шестой.

[0063] Двадцать восьмой вариант осуществления обеспечивает заменяемое устройство по двадцать седьмому варианту осуществления, при этом логическая схема предназначена для приема времязависимого запроса от хост-устройства, которое указывает случайное начальное число, ключ сеанса и счет вычислений; выполнения вычисления запроса на основе случайного начального числа, ключа сеанса и счета

вычислений.

[0064] Двадцать девятый вариант осуществления обеспечивает заменяемое устройство по двадцать седьмому варианту осуществления, при этом логическая схема предназначена для ответа во время ответа на запрос, которое зависит от счета вычислений.

[0065] Тридцатый вариант осуществления обеспечивает заменяемое устройство по двадцать седьмому варианту осуществления, дополнительно содержащее характеристические данные, сохраненные в памяти, которые включают в себя различные временные окна для выполнения времязависимых запросов в зависимости от указанных счетов вычислений.

[0066] Тридцать первый вариант осуществления обеспечивает заменяемое устройство по двадцать седьмому варианту осуществления, при этом память хранит идентификационный код и базовый ключ.

[0067] Тридцать второй вариант осуществления обеспечивает заменяемое устройство по двадцать седьмому варианту осуществления, дополнительно содержащее процессор для получения ключа сеанса при каждой связи с хост-устройством.

[0068] Тридцать третий вариант осуществления обеспечивает заменяемое устройство по двадцать седьмому варианту осуществления, при этом логическая схема предназначена для выполнения вычисления запроса число раз, равное циклу вычисления, при этом первое вычисление использует случайное начальное число и ключ сеанса для создания выходных данных, а каждое последующее вычисление использует выходные данные предшествующего вычисления.

[0069] Тридцать четвертый вариант осуществления обеспечивает заменяемое устройство по двадцать седьмому варианту осуществления, содержащее микроконтроллер, который включает в себя логическую схему, память и процессор.

[0070] Тридцать пятый вариант осуществления обеспечивает заменяемое устройство по двадцать седьмому варианту осуществления, дополнительно содержащее печатающий материал, который должен наноситься на печатные носители хост-устройством.

[0071] Тридцать шестой вариант осуществления обеспечивает заменяемое устройство по двадцать седьмому варианту осуществления, при этом печатающий материал выбран из группы, состоящей из тонера и чернил.

[0072] Тридцать седьмой вариант осуществления обеспечивает заменяемое устройство по двадцать седьмому варианту осуществления, при этом вычисление запроса содержит ряд операций, которое соответствует счету вычислений, в конкретной последовательности.

(57) Формула изобретения

1. Заменяемое поставляемое устройство, содержащее

центральный процессор (ЦП) (114) и память (116), хранящую базовый ключ (122),

специализированную аппаратную логическую схему (132), предназначенную для ответа на криптографический запрос (128) согласования по времени, причем специализированная аппаратная логическая схема (132) выполнена с возможностью

вычислять ответ (130) на основе параметров, включающих счет вычислений, ключ сеанса, связанный с базовым ключом, и случайное начальное число, и

предоставлять ответ (130) в пределах заданного времени (131) ответа на запрос,

при этом счет вычислений отрицательно влияет на время (131) ответа на запрос для ответа (130).

2. Устройство по п. 1, при этом память дополнительно содержит характеристические

данные (134) для предоставления ожидаемых временных окон, в которые время (131) ответа на запрос должно попадать в зависимости от счета вычислений.

3. Устройство по п. 2, при этом характеристические данные (134) защищены с использованием цифровой подписи.

4. Устройство по п. 2 или 3, при этом характеристические данные являются такими, что для данного счета вычислений x ожидаемое временное окно y может быть определено с помощью формулы прямой с угловым коэффициентом (y=mx+b).

5. Устройство по одному из пп. 1-4, при этом вычисление содержит базовую функцию, которая определяет последовательность операций, оптимизированных для очень быстрой работы в специализированной аппаратной логической схеме (132).

6. Устройство по одному из пп. 1-5, при этом специализированная аппаратная логическая схема (132) предназначена для выполнения вычисления запроса число раз, равного счету или циклу вычислений, и при этом первое вычисление использует случайное начальное число и ключ сеанса для создания выходных данных, а каждое последующее вычисление использует выходные данные предшествующего вычисления.

7. Устройство по п. 6, при этом последние выходные данные вычисления предоставляют ответ (130) в пределах времени (131) ответа на запрос.

8. Устройство по одному из пп. 1-7, при этом в то время как один или более операндов изменяются с каждой итерацией вычисления, само вычисление не изменяется.

9. Печатающий поставляемый картридж, содержащий:

устройство по одному из предыдущих пунктов и

электрические контакты (400) для передачи сигналов на контроллер (116) хост-устройства для способствования аутентификации печатающего поставляемого картриджа (306).

10. Система аутентификации, содержащая:

хост-устройство (102); и

заменяемое поставляемое устройство (104) по одному из пп. 1-7,

при этом хост-устройство (102) выполнено с возможностью

выдавать криптографический запрос (128) согласования по времени,

принимать ответ (130) на запрос от заменяемого поставляемого устройства (104),

определять время (131) ответа на запрос, и

аутентифицировать заменяемое поставляемое устройство (104) с использованием ответа (130) на запрос и времени (131) ответа на запрос.

11. Система аутентификации по п. 10, при этом для определения времени (131) ответа на запрос хост-устройство (102) выполнено с возможностью

измерять время (131) ответа на запрос, начиная последовательность согласования по времени, когда криптографический запрос (128) согласования по времени выдается, и останавливая последовательность согласования по времени после того, как заменяемое поставляемое устройство (104) заканчивает и возвращает ответ (130) на запрос хост-устройству (102).

12. Система печати, содержащая систему аутентификации по п. 10 или 11.

13. Способ аутентификации заменяемого поставляемого устройства, содержащий:

в ответ на криптографический запрос (128) согласования по времени

вычисление заменяемым поставляемым устройством ответа (130) на основе параметров, включающих в себя счет вычислений, ключ сеанса, связанный с базовым ключом, и случайное начальное число, и

предоставление заменяемым поставляемым устройством ответа (130) в пределах заданного времени (131) ответа на запрос,

при этом счет вычислений отрицательно влияет на время (131) ответа на запрос для ответа (130).

14. Способ по п. 13, содержащий:

выдачу хост-устройством (102) криптографического запроса (128) согласования по времени,

прием хост-устройством (102) ответа (130) на запрос от заменяемого поставляемого устройства (104),

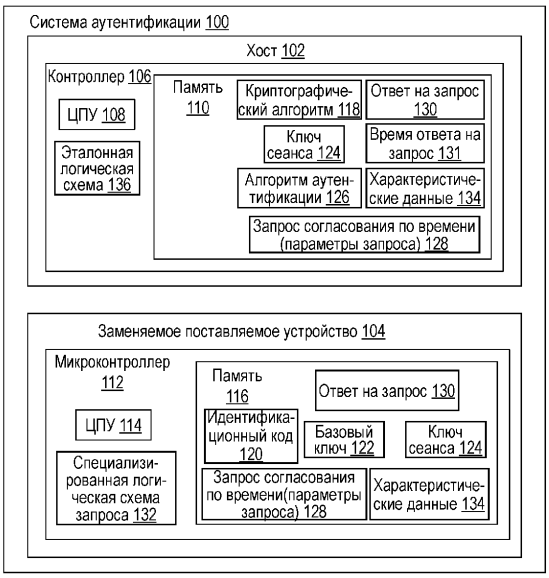
определение времени (131) ответа на запрос, и

аутентификацию заменяемого поставляемого устройства (104) с использованием ответа (130) на запрос и времени (131) ответа на запрос.

15. Способ по п. 14, при этом определение времени (131) ответа на запрос содержит:

измерение времени (131) ответа на запрос, начиная последовательность согласования по времени, когда криптографический запрос (128) согласования по времени выдается, и останавливая последовательность согласования по времени после того, как заменяемое поставляемое устройство (104) заканчивает и возвращает ответ (130) на запрос хост-устройству (102).

1



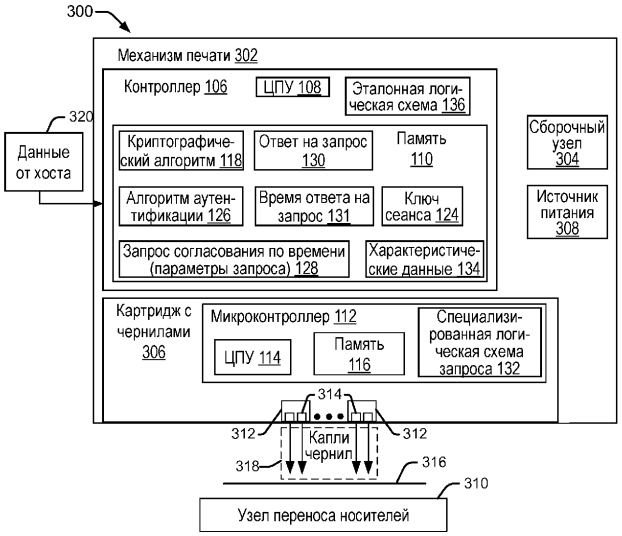
ФИГ. 1

134

Счет вычислений	Временное окно ответа на запрос
A	Q - R мс
B	S - T мс
10,000	50 - 55 мс
C	U - V мс
•	•
•	•
•	•

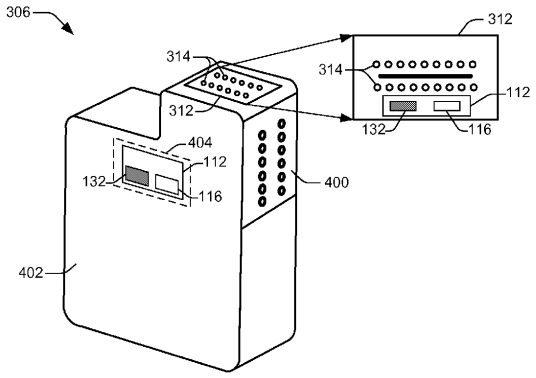
ФИГ. 2

2


300
Механизм печати 302
Контроллер 106
ЦПУ 108
Эталонная логическая схема 136
320
Данные от хоста
Криптографический алгоритм 118
Ответ на запрос 130
Память 110
Алгоритм аутентификации 126
Время ответа на запрос 131
Ключ сеанса 124
Запрос согласования по времени (параметры запроса) 128
Характеристические данные 134
Сборочный узел 304
Источник питания 308
Картридж с чернилами 306
Микроконтроллер 112
ЦПУ 114
Память 116
Специализированная логическая схема запроса 132
314
312
312
Капли чернил
318
316
310
Узел переноса носителей

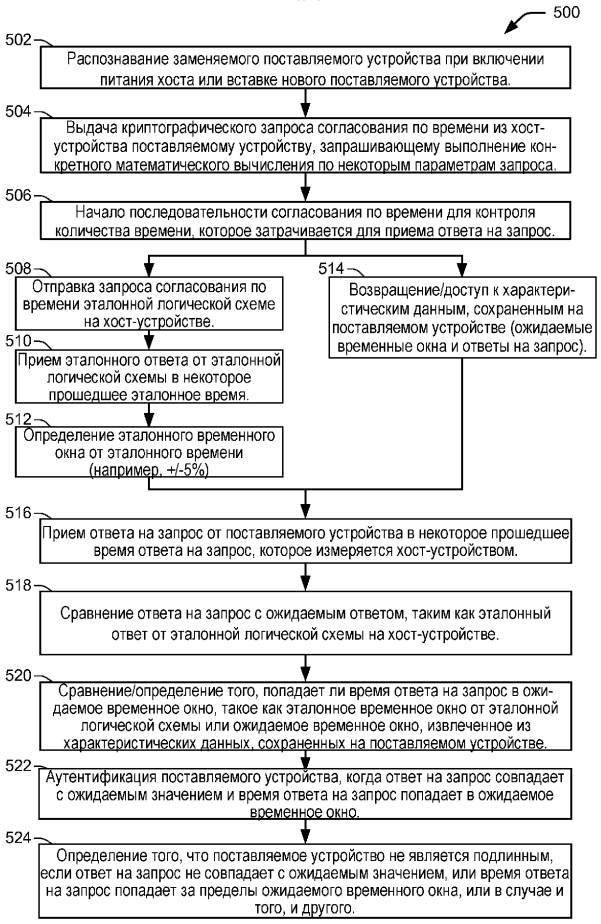
ФИГ. 3

3



ФИГ. 4

4


500
502
Распознавание заменяемого поставляемого устройства при включении питания хоста или вставке нового поставляемого устройства.
504
Выдача криптографического запроса согласования по времени из хост-устройства поставляемому устройству, запрашивающему выполнение конкретного математического вычисления по некоторым параметрам запроса.
506
Начало последовательности согласования по времени для контроля количества времени, которое затрачивается для приема ответа на запрос.
508
Отправка запроса согласования по времени эталонной логической схеме на хост-устройстве.
510
Прием эталонного ответа от эталонной логической схемы в некоторое прошедшее эталонное время.
512
Определение эталонного временного окна от эталонного времени (например, +/-5%)
514
Возвращение/доступ к характеристическим данным, сохраненным на поставляемом устройстве (ожидаемые временные окна и ответы на запрос).
516
Прием ответа на запрос от поставляемого устройства в некоторое прошедшее время ответа на запрос, которое измеряется хост-устройством.
518
Сравнение ответа на запрос с ожидаемым ответом, таким как эталонный ответ от эталонной логической схемы на хост-устройстве.
520
Сравнение/определение того, попадает ли время ответа на запрос в ожидаемое временное окно, такое как эталонное временное окно от эталонной логической схемы или ожидаемое временное окно, извлеченное из характеристических данных, сохраненных на поставляемом устройстве.
522
Аутентификация поставляемого устройства, когда ответ на запрос совпадает с ожидаемым значением и время ответа на запрос попадает в ожидаемое временное окно.
524
Определение того, что поставляемое устройство не является подлинным, если ответ на запрос не совпадает с ожидаемым значением, или время ответа на запрос попадает за пределы ожидаемого временного окна, или в случае и того, и другого.

ФИГ. 5