РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2 728 519**(13) **C1**

(51) МПК
H04L 9/08 (2006.01)
H04L 9/30 (2006.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК
H04L 9/0866 *(2020.02);* ***H04L 9/3073*** *(2020.02);* ***H04L 9/0643*** *(2020.02);* ***H04L 9/0841*** *(2020.02);* ***G06F 7/725*** *(2020.02)*

(21)(22) Заявка: **2019130501, 12.02.2018**

(24) Дата начала отсчета срока действия патента:
12.02.2018

Дата регистрации:
30.07.2020

Приоритет(ы):
(30) Конвенционный приоритет:
28.02.2017 EP 17158508.6

(45) Опубликовано: **30.07.2020** Бюл. № **22**

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **30.09.2019**

(86) Заявка PCT:
EP 2018/053389 (12.02.2018)

(87) Публикация заявки PCT:
WO 2018/158065 (07.09.2018)

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

(72) Автор(ы):
ГАРСИЯ МОРЧОН, Оскар (NL),
БХАТТАЧАРЯ, Саувик (NL),
ТОЛХЭЙЗЕН, Людовикус, Маринус, Герардус, Мария (NL),
РИТМАН, Рональд (NL)

(73) Патентообладатель(и):
КОНИНКЛЕЙКЕ ФИЛИПС Н.В. (NL)

(56) Список документов, цитированных в отчете о поиске: **US 2005/094806 A1, 05.05.2005. RU 2376651 C2, 20.12.2009. EP 1528705 B1, 04.05.2005. CA 2483486 A1, 01.10.2004.**

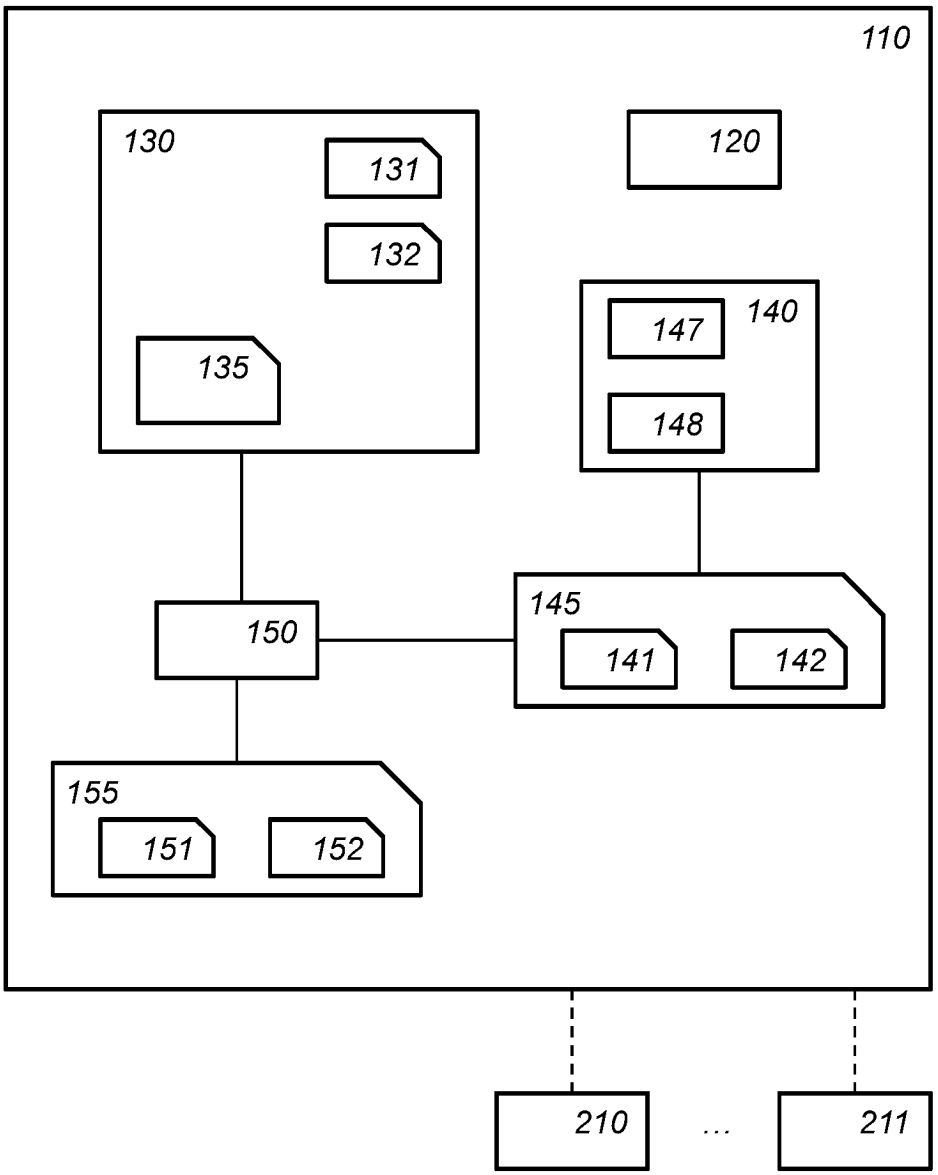
(54) ПРОТОКОЛ СОГЛАСОВАНИЯ КЛЮЧЕЙ НА ОСНОВЕ ИЗОГЕНИИ ЭЛЛИПТИЧЕСКИХ КРИВЫХ

(57) Реферат:

Изобретение относится к шифрованию, в частности, к предварительному распределению ключей для конфигурирования множества сетевых узлов информацией локальных ключей. Технический результат заключается в повышении устойчивости криптографических систем. Указанный результат достигается за счет того, что применяют, по меньшей мере, первую хеш–функцию (147) и вторую хеш–функцию (148) к цифровому идентификатору сетевого узла. Первая и вторая хеш–функции отображают цифровой идентификатор в первую открытую точку (141; $H_1(ID)$) и вторую открытую точку (142; $H_2(ID)$) на первой эллиптической кривой (131) и второй эллиптической кривой (132). Первая и вторая секретные изогении (135) применяются к первой и второй открытым точкам (141, 142) эллиптической кривой, чтобы получать первую закрытую точку (151) эллиптической кривой и вторую закрытую точку (152) эллиптической кривой, составляющие часть материала (155) закрытых ключей для сетевого узла (210). 5 н. и 8 з.п. ф-лы, 11 ил.

RU 2728519 C1

RU 2728519 C1



ФИГ. 1

RU 2728519 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 728 519**(13) **C1**

(51) Int. Cl.
H04L 9/08 (2006.01)
H04L 9/30 (2006.01)

(12) ABSTRACT OF INVENTION

(52) CPC
H04L 9/0866 *(2020.02);* ***H04L 9/3073*** *(2020.02);* ***H04L 9/0643*** *(2020.02);* ***H04L 9/0841*** *(2020.02);* ***G06F 7/725*** *(2020.02)*

(21)(22) Application: **2019130501, 12.02.2018**

(24) Effective date for property rights:
12.02.2018

Registration date:
30.07.2020

Priority:
(30) Convention priority:
28.02.2017 EP 17158508.6

(45) Date of publication: **30.07.2020** Bull. № **22**

(85) Commencement of national phase: **30.09.2019**

(86) PCT application:
EP 2018/053389 (12.02.2018)

(87) PCT publication:
WO 2018/158065 (07.09.2018)

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

(72) Inventor(s):
GARCIA MORCHON, Oscar (NL),
BHATTACHARYA, Sauvik (NL),
TOLHUIZEN, Ludovicus, Marinus, Gerardus, Maria (NL),
RIETMAN, Ronald (NL)

(73) Proprietor(s):
Koninklijke Philips N.V. (NL)

RU 2728519 C1

(54) KEY MATCHING PROTOCOL BASED ON ELLIPTIC CURVE ISOGENY

(57) Abstract:

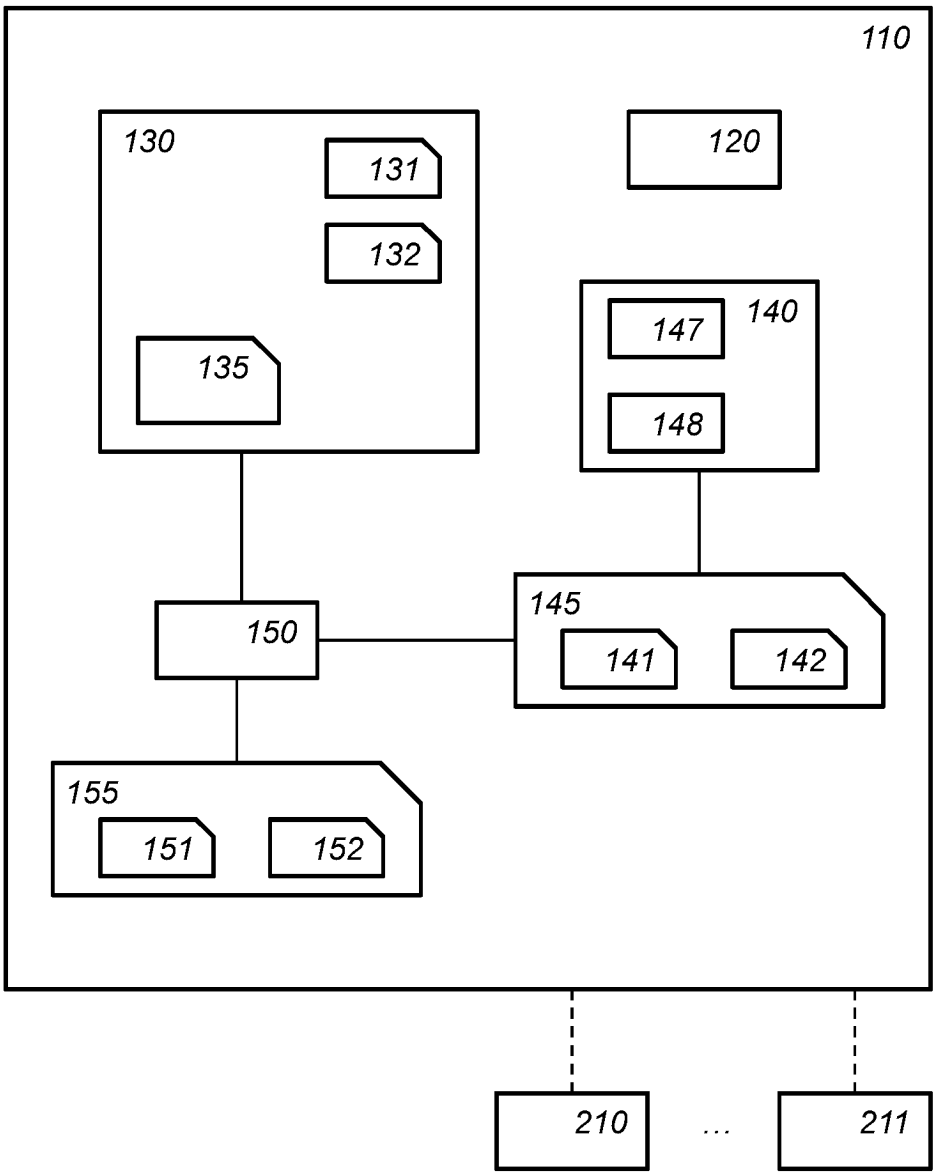
FIELD: physics.

SUBSTANCE: invention relates to encryption, in particular, to preliminary distribution of keys for configuration of multiple network nodes with information of local keys. Said result is achieved by using at least first hash function (147) and second hash function (148) to digital identifier of network node. First and second hash functions map the digital identifier to the first open point (141; $H_1(ID)$) and the second open point (142; $H_2(ID)$) on the first elliptic curve (131) and the second elliptic curve (132). First and second secret isogenies (135) are applied to the first and second open points (141, 142) of the ellipsoidal curve in order to obtain the first closed point (151) of the elliptic curve and the second closed point (152) of the ellipsoidal curve, which form part of closed (155) material switches for network node (210).

EFFECT: technical result consists in improvement of cryptographic systems stability.

13 cl, 11 dwg

RU 2728519 C1



ФИГ. 1

RU 2728519 C1

Область техники, к которой относится изобретение

Изобретение относится к электронному устройству предварительного распределения ключей для конфигурирования множества сетевых узлов информацией локальных ключей, к первому электронному сетевому узлу, сконфигурированному для протокола согласования ключей со вторым сетевым узлом, к электронному способу для предварительного распределения ключей, конфигурирующему множество сетевых узлов информацией локальных ключей, к электронному способу для установления совместно используемого ключа между первым сетевым узлом и вторым сетевым узлом, и к машиночитаемому носителю.

Уровень техники

Согласование ключей, например, в беспроводных сенсорных сетях, представляет собой важный криптографический примитив. После того, как две стороны согласуют общий совместно используемый ключ, они могут использовать упомянутый ключ для того, чтобы защищать связь между собой, например, с использованием шифрования и аутентификации. Так называемые схемы предварительного распределения ключей на основе идентификационных данных обеспечивают возможный способ упрощать согласование ключей. Схема предварительного распределения ключей на основе идентификационных данных имеет две фазы: предварительное распределение ключей и извлечение ключей. С двумя фазами схемы предварительного распределения ключей на основе идентификационных данных ассоциированы два алгоритма: алгоритм формирования материала локальных ключей и алгоритм установления ключей, соответственно.

С использованием схем предварительного распределения ключей на основе идентификационных данных, два сетевых узла могут согласовывать совместно используемый ключ, который основан на их идентификационных данных. Традиционный подход, в котором ключ определяется для каждой пары сетевых узлов, должен расти квадратично. Тем не менее, схема предварительного распределения ключей на основе идентификационных данных должна распределять только один набор материала локальных ключей для каждого узла и в силу этого растет линейно.

Схема предварительного распределения ключей на основе идентификационных данных устанавливается посредством предоставления доверенной третьей стороне материала корневых ключей. Доверенная третья сторона может представлять собой изготовителя устройства и, например, может инициализировать устройства во время их изготовления или в некотором другом доверенном окружении. Альтернативно, доверенная третья сторона может представлять собой устройство центра сертификации, например, устройство, которое инициализирует устройства, например, с использованием некоторого онлайнового протокола.

Во время предварительного распределения ключей материал локальных ключей формируется для каждого сетевого узла и сохраняется в сетевом узле посредством применения алгоритма формирования материала локальных ключей к материалу корневых ключей и идентификатору каждого сетевого узла. В течение фазы извлечения ключей два сетевых узла могут извлекать совместно используемый ключ посредством применения алгоритма установления ключей к их материалу локальных ключей и идентификатору другого сетевого узла. Например, первый узел может применять алгоритм установления ключей ко второму идентификатору второго сетевого узла и собственному первому материалу локальных ключей, в то время как второй узел может применять алгоритм установления ключей к первому идентификатору первого сетевого узла и своему второму материалу локальных ключей. Результат алгоритма установления

ключей представляет собой ключ на основе идентификационных данных, совместно используемый двумя сетевыми узлами.

Существует большое количество схем предварительного распределения ключей на основе идентификационных данных. Например, схема предварительного распределения ключей на основе идентификационных данных описывается в работе "HIMMO: A lightweight collusion–resistant key pre–distribution scheme", авторов Oscar Garcia–Morchon, Domingo Gomez–Perez, Jaime Gutierrez, Ronald Rietman, Berry Schoenmakers и Ludo Tolhuizen, опубликованной в Cryptology ePrint Archive, Report 2014/698. Улучшенная версия HIMMO описывается в заявке на патент (Европа) "Improved system for key sharing", поданной в EPO, с адвокатской выпиской 2015PF001725, от идентичного заявителя, которая содержится по ссылке. HIMMO, аналогично некоторым другим схемам распределения ключей на основе идентификационных данных, имеет такой недостаток, что необработанные ключи могут быть немного устаревшими. Это может быть приемлемым, либо дополнительные сверочные данные ключей (также называемые "вспомогательными данными") используются для того, чтобы добиваться совместно используемого ключа. Сверочные данные ключей обычно формируются первым сетевым узлом, который имеет доступ к обоим идентификационным данным, например, второго сетевого узла, если первой сетевой узел инициирует согласование ключей.

В варианте осуществления, материал корневых ключей содержит бивариативный полином, и материал локальных ключей содержит унивариативный полином. Например, в схеме предварительного распределения ключей на основе идентификационных данных Бландо, материал корневых ключей формируется посредством бивариативного полинома $f(x,y)$. Материал g локальных ключей для первого узла с идентификатором ID_1 формируется посредством сворачивания бивариативного в унивариативный полином $g(y) = f(ID_1,y)$. Узел с материалом g локальных ключей и идентификатором ID_2 второго узла получает совместно используемый ключ посредством вычисления $g(ID_2)$. Все полиномиальные вычисления могут проводиться по модулю математический модуль m.

Недавно начаты исследования касательно того, может или нет билинейное отображение, заданное в эллиптической кривой, использоваться для создания системы перераспределения ключей на основе идентификационных данных. Проблемы возникают, даже если такие подходы обеспечивают достаточное разнообразие в своих базовых криптографических объектах и в силу этого являются достаточно защищенными от криптографического анализа. Кроме того, имеется такая потребность, что криптографические протоколы должны быть устойчивыми к новой угрозе квантовых компьютеров.

Сущность изобретения

Предусмотрено электронное устройство предварительного распределения ключей для конфигурирования множества сетевых узлов информацией локальных ключей. Устройство предварительного распределения ключей содержит:

устройство хранения данных, содержащее информацию, представляющую первую секретную изогению для первой эллиптической кривой и вторую секретную изогению для второй эллиптической кривой, причем изогения приспособлена принимать точку на эллиптической кривой и формировать точку на эллиптической кривой в качестве вывода,

процессорную схему, выполненную с возможностью:

– получать цифровой идентификатор для сетевого узла,

– применять, по меньшей мере, первую хеш–функцию и вторую хеш–функцию к

цифровому идентификатору, причем первая и вторая хеш–функции отображают цифровой идентификатор в первую открытую точку и вторую открытую точку на первой эллиптической кривой и второй эллиптической кривой, причем первая эллиптическая кривая отличается от второй эллиптической кривой, причем первая и вторая открытые точки составляют часть материала открытых (общедоступных) ключей для сетевого узла,

– применять первую и вторую секретные изогении к первой и второй открытым точкам эллиптической кривой, за счет этого получая первую закрытую точку эллиптической кривой и вторую закрытую точку эллиптической кривой, составляющие часть материала закрытых (конфиденциальных) ключей для сетевого узла, и

интерфейс связи, выполненный с возможностью конфигурировать сетевой узел закрытой точкой эллиптической кривой.

Кроме того, предусмотрен электронный сетевой узел, сконфигурированный для протокола согласования ключей со вторым сетевым узлом. Для простоты ссылки, сетевой узел идентифицируется в качестве первого сетевого узла, что отличает его из второго сетевого узла, с которым он обменивается данными. Прилагательные "первый" и "второй" не имеют дополнительного смысла. Первый сетевой узел может представлять собой инициирующий сетевой узел, который инициирует протокол со вторым сетевым узлом, и второй сетевой узел может представлять собой отвечающий сетевой узел. Тем не менее, это также может быть наоборот.

Сетевой узел содержит:

устройство хранения данных, содержащее:

цифровой идентификатор для первого сетевого узла и/или первую и вторую открытые точки эллиптической кривой, причем первая и вторая открытые точки эллиптической кривой находятся на первой и второй эллиптических кривых, и

причем первая закрытая точка эллиптической кривой и вторая закрытая точка эллиптической кривой соответствуют первой открытой точке эллиптической кривой и второй открытой точке эллиптической кривой через первую и вторую секретные изогении, причем первая открытая точка эллиптической кривой и вторая открытая точка эллиптической кривой соответствуют цифровому идентификатору сетевого узла через первую и вторую хеш–функции, причем первая и вторая закрытые точки эллиптической кривой вычисляются посредством устройства предварительного распределения ключей,

процессорная схема выполнена с возможностью:

– получать открытую точку эллиптической кривой для второго сетевого узла, причем открытая точка эллиптической кривой находится на первой из первой и второй эллиптических кривых,

– выбирать закрытую точку эллиптической кривой из первой и второй закрытых точек эллиптической кривой, находящихся на второй из первой и второй эллиптических кривых, причем первая и вторая кривые отличаются,

– применять билинейное отображение к выбранной закрытой точке первого сетевого узла и полученной открытой точке эллиптической кривой второго сетевого узла или открытой точке эллиптической кривой второго сетевого узла, к которому применяется открытая изогения посредством первого узла,

– извлекать криптографический ключ из результата билинейного отображения.

Включение изогений на эллиптических кривых в криптографический протокол является преимущественным, поскольку они предположительно имеют повышенную квантовую устойчивость. В частности, отсутствует эффективный известный квантовый

алгоритм для того, чтобы реконструировать изогению между двумя суперсингулярными эллиптическими кривыми. Кроме того, изогении увеличивают варианты выбора, который осуществляется в алгоритмах, и в силу этого затрудняют атаку на систему. Преимущество протокола, реализованного в сетевом узле, состоит в том, что совместно используемые ключи могут вычисляться при обмене только небольшим числом простых сообщений. Фактически, если цифровой идентификатор другого узла может получаться без сообщения, то не требуется вообще обмениваться сообщениями для получения совместно используемого ключа. Извлеченный ключ затем может использоваться для того, чтобы извлекать ключ для симметричного шифрования и т.д. Точки эллиптической кривой также охватывают сжатые точки, например, только координату X или координату X с дополнительным битом, чтобы определять знак координаты Y.

Сетевой узел представляет собой электронное устройство. Например, он может представлять собой мобильное электронное устройство, такое как мобильный телефон. Сетевой узел может представлять собой абонентскую приставку, смарт–карту, компьютер и т.д. Устройство предварительного распределения ключей может представлять собой компьютер, сервер и т.д. Устройство предварительного распределения ключей также может представлять собой устройство связи, такое как телефон, например, выполненный с возможностью устанавливать так называемую произвольно организующуюся сеть беспроводной связи, например, ячеистую сеть. Способы, описанные в данном документе, могут применяться в широком диапазоне практических вариантов применения. Такие практические варианты применения включают в себя финансовые приложения, например, чтобы совместно использовать информацию кредитных карт, приложения для повышения конфиденциальности, например, приложения для обмена сообщениями, медицинские приложения и т.д.

Способ согласно изобретению может реализовываться на компьютере в качестве машинореализованного способа или в выделенных аппаратных средствах либо в комбинации вышеозначенного. Исполняемый код для способа согласно изобретению может сохраняться на компьютерном программном продукте. Примеры компьютерных программных продуктов включают в себя запоминающие устройства, оптические устройства хранения данных, интегральные схемы, серверы, онлайновое программное обеспечение и т.д. Предпочтительно, компьютерный программный продукт содержит энергонезависимый программный код, сохраненный на машиночитаемом носителе для осуществления способа согласно изобретению, когда упомянутый программный продукт выполняется на компьютере.

В предпочтительном варианте осуществления, компьютерная программа содержит компьютерный программный код, выполненный с возможностью осуществлять все этапы способа согласно изобретению, когда компьютерная программа выполняется на компьютере. Предпочтительно, компьютерная программа осуществляется на машиночитаемом носителе.

Другой аспект изобретения предоставляет способ обеспечения доступности компьютерной программы для загрузки. Этот аспект используется, когда компьютерная программа выгружается, например, в Apple App Store, Google Play Store или Microsoft Windows Store, и когда компьютерная программа доступна для загрузки из такого магазина.

Краткое описание чертежей

В дальнейшем описываются дополнительные подробности, аспекты и варианты осуществления изобретения, только в качестве примера, со ссылкой на чертежи. Элементы на чертежах проиллюстрированы для простоты и ясности и не обязательно

нарисованы в масштабе. На чертежах, элементы, которые соответствуют уже описанным элементам, могут иметь идентичные номера ссылок. На чертежах:

Фиг. 1 схематично показывает пример варианта осуществления системы предварительного распределения ключей,

Фиг. 2a–2c схематично показывают примеры варианта осуществления устройства хранения данных устройства предварительного распределения ключей,

Фиг. 3a схематично показывает пример варианта осуществления системы согласования ключей,

Фиг. 3b схематично показывает пример варианта осуществления системы согласования ключей,

Фиг. 4 схематично показывает пример варианта осуществления системы согласования ключей,

Фиг. 5 схематично показывает пример варианта осуществления способа предварительного распределения ключей,

Фиг. 6 схематично показывает пример варианта осуществления способа согласования ключей,

Фиг. 7a схематично показывает машиночитаемый носитель, имеющий записываемую часть, содержащую компьютерную программу согласно варианту осуществления,

Фиг. 7b схематично показывает представление процессорной системы согласно варианту осуществления.

Список ссылок с номерами на фиг. 1–3b:

100 – система предварительного распределения ключей
110 – электронное устройство предварительного распределения ключей
120 – интерфейс связи
130 – устройство хранения данных
131 – первая эллиптическая кривая
132 – вторая эллиптическая кривая
135 – первая секретная изогения
140 – модуль обработки эллиптических хеш–функций
141 – первая открытая точка
142 – вторая открытая точка
145 – материал открытых ключей
147 – первая хеш–функция
148 – вторая хеш–функция
150 – модуль обработки изогений
151 – первая закрытая точка эллиптической кривой
152 – вторая закрытая точка эллиптической кривой
155 – материал закрытых ключей
161, 167, 168 – устройство хранения данных
162 – первая изогения
163 – вторая изогения
164 – секретное целое число
165 – первое секретное целое число
166 – второе секретное целое число
200, 201 – система согласования ключей
210, 211 – сетевой узел
215, 216 – первый сетевой узел
220 – интерфейс связи

230 – устройство хранения данных
231 – первая эллиптическая кривая
232 – вторая эллиптическая кривая
234 – цифровой идентификатор
235 – открытая изогения
241 – первая открытая точка эллиптической кривой
242 – вторая открытая точка эллиптической кривой
251 – первая закрытая точка эллиптической кривой
252 – вторая закрытая точка эллиптической кривой
260 – модуль обработки совместно используемых ключей
270 – модуль обработки изогений
280 – модуль подтверждения правильности ключей

Осуществление изобретения

Хотя это изобретение допускает вариант осуществления во многих различных формах, один или более конкретных вариантов осуществления показаны на чертежах и подробно описываются в данном документе с пониманием того, что настоящее раскрытие должно рассматриваться в качестве примера принципов изобретения и не имеет намерение ограничивать изобретение конкретными показанными и описанными вариантами осуществления.

Далее, для понимания, элементы вариантов осуществления описываются при работе. Тем не менее, должно быть очевидным то, что соответствующие элементы выполнены с возможностью осуществлять функции, описанные как выполняемые посредством них.

Дополнительно, изобретение не ограничено вариантами осуществления, и изобретение заключается в каждом новом признаке или в комбинации признаков, описанных в данном документе или изложенных во взаимно различных зависимых пунктах формулы изобретения.

Рост Интернета вещей (IoT) и подход квантовой эры приводят к необходимости в облегченных быстрых (квантовых) защищенных протоколов для IoT–сетей, даже в случае множества компрометаций IoT–устройств. Варианты осуществления, описанные ниже, предоставляют схемы неинтерактивного распределения ключей (NIKD) на основе открытых и/или секретных изогений, соответственно. Включение изогений на эллиптических кривых в криптографический протокол является преимущественным, поскольку они предполагаются квантово–устойчивыми, в частности, при использовании с суперсингулярными эллиптическими кривыми. В частности, варианты осуществления, в которых предоставляются секретные изогении, имеют повышенную устойчивость к атаке даже в случае атаки с использованием квантового компьютера. Помимо этого, варианты осуществления являются облегченными и классически защищенными от тайного сговора/компрометации любого числа устройств. Облегченная и высокопроизводительная работа обеих схем обеспечивает то, что они являются подходящими для IoT–примеров использования.

Ниже обобщаются некоторые математические основы.

Для текущих криптографических целей, эллиптическая кривая может задаваться посредством канонического уравнения $y^2 = x^3 + ax + b$, где a, b являются элементами из конечного поля с характеристикой, большей трех. Эллиптические кривые над конечными полями с характеристикой в два или три могут описываться посредством аналогичного, но другого типа уравнения. Точки на кривой могут идентифицироваться посредством пары координат, например, координат X и Y, которая удовлетворяет формуле задания

эллиптической кривой. Обычно, точка на кривой представляется в сжатом формате. Например, точка на кривой может уникально идентифицироваться посредством только своей координаты X, одного бита, чтобы определять знак прилагаемой координаты Y. Фактически, зачастую координата Y вообще пропускается. Хотя это вводит небольшую неоднозначность в точке, для большинства вариантов применения это не является релевантным. Для целей этого документа, такие представления также считаются точками на кривой.

Спаривания (также известные как билинейные формы): Спаривание представляет собой отображение из прямого произведения двух циклических (аддитивных) групп G_1 и G_2в группу G_T таким образом, что для всех $P \in G_1, Q \in G_2$и всех положительных целых чисел *a, b*, предусмотрено, что $(aP,bQ) = [e(P,Q)]^{ab}$, и $e(P,Q) \neq 1$ для некоторых $(P,Q) \in G_1 \times G_2$. Важное спаривание в криптографии представляет собой так называемое спаривание Вейля. В этом случае, кривая $E(K)$ выбирается над конечным полем K, которое содержит *m*–ый корень единицы. Спаривание e Вейля принимает в качестве вводов точки $P,Q \in E(K)(m) = \{T \in E(K) | mT = O\}$ и формирует *m*–ый корень из единицы в K, т.е. $e(P,Q) \in \{x \in K | x^m = 1\}$. Если точки *P* и *Q* задаются в сжатой форме, с битом указания знаков, можно вычислять соответствующие координаты Y и затем вычислять спаривания. Альтернативно, можно вычислять, по меньшей мере, для определенных спариваний, таких как спаривание Вейля и спаривание Тейта, значение z таким образом, что для всех точек *P* и *Q*, $z = (e(P,Q))^{a(P,Q)}$, где экспонента $a(P,Q)$равна 1 или –1. Это поясняется в работе "Computing pairings using x–coordinates only" авторов S. Galbraith и X.Lin, Designs, Codes and Cryptography, издание 50, выпуск 3, стр. 305–324, март 2009 года. В идентичном ссылочном документе, поясняется то, что только из значений координат X, можно вычислять след $e(P,Q)$, т.е. значение $T(P,Q) = e(P,Q) + (e(P,Q))^{-1}$.

Изогении: Неформально, изогении представляют собой отображения между эллиптическими кривыми. Изогения может задаваться как непостоянная функция, заданная на первой эллиптической кривой, которая принимает значения на второй эллиптической кривой и сохраняет добавление точек, т.е. она сохраняет структуру эллиптических кривых. См. диссертацию автора D. Shumow "Isogenies of Elliptic Curves: A Computational Approach". Более формально, пусть E1/K и E2/K представляют собой две эллиптические кривые, изогения может задаваться как рациональное отображение эллиптических кривых $\phi: E1(\overline{K}) \rightarrow E2(\overline{K})$ с координатами из $\overline{K}$, которое сохраняет точку в бесконечности, т.е. $\phi(\infty) = \infty$. Из этого следует, что такое отображение сохраняет групповую структуру. См. диссертацию автора A. Sankar "Classical and Quantum Algorithms for Isogeny–based Cryptography".

Типично, изогения задается как отображение между двумя разными кривыми; тем не менее, также рассматриваются изогении между кривой и ей самой. Во втором случае, изогении могут задаваться, например, в качестве умножений по эллиптической кривой с фиксированным целым числом, например, в качестве отображения точки P эллиптической кривой в точки *sP* эллиптической кривой. Следует отметить, что это отображение сохраняет добавление. Изогении между разными кривыми имеют намного более насыщенную структуру, чем может задаваться посредством одного целого числа.

Стандартный способ представлять изогению φ состоит в том, чтобы предоставлять 3 гомогенных полинома $f_1, f_2, f_3 \in \overline{K}[X,Y,Z]$, удовлетворяющих $\varphi(x:y:z) = (f_1(x,y,z): f_2(x,y,z): f_3(x,y,z)) \in P^2(\overline{K})$ для поля K. Если *l* обозначает степень φ, то обычно один из этих полиномов должен иметь степень примерно в *l*. Следует обратиться

к работе "Evaluating large degree isogenies and applications to pairing based cryptography" авторов Reinier Bröker, Denis Charles и Kristin Lauter. В разделе 2 этой работы, содержится альтернативное представление изогений между эллиптическими кривыми по конечным полям, длина которых представляет собой полином в $log\ l$. Кроме того, работа представляет алгоритм, который оценивает изогении между эллиптическими кривыми по конечным полям.

В этой патентной заявке предлагаются различные варианты осуществления сетевых узлов и устройств предварительного распределения ключей. Эти варианты осуществления включают в себя NIKD–схемы на основе изогений. Сначала приводится введение, и дополнительные варианты осуществления и подробности описываются в отношении чертежей.

Узлы в сети регистрируют себя в доверенной третьей стороне (TTP), чтобы принимать материал(ы) секретных ключей и, в необязательном порядке, открытый идентификатор (ы) (например, открытый идентификатор). С их помощью, любые два узла могут устанавливать секретный ключ, который является уникальным для них и является известным только для этой пары узлов, причем он затем может использоваться этой парой для защищенного обмена данными друг с другом.

Варианты осуществления используют две эллиптические кривые E_1, E_2. TTP хеширует идентификатор сетевого узла в точки на этих двух эллиптических кривых $H_1(ID)$ и $H_2(ID)$. Последние представляют собой открытые точки и могут сохраняться в сетевом узле или могут вычисляться сетевым узлом непосредственно из идентификатора. TTP отображает две открытые точки в две закрытые точки посредством отображения открытых точек на своих соответствующих эллиптических кривых в две закрытые точки также на двух разных эллиптических кривых. Варианты осуществления могут разделяться на два основных типа.

В первом типе, TTP поддерживает секретную изогению и ее так называемую двойственную изогению, связанную с вышеуказанными двумя кривыми. Изогения отображает из первой эллиптической кривой во вторую эллиптическую кривую, тогда как двойственная изогения отображает из второй эллиптической кривой в первую эллиптическую кривую. Во время регистрации узлов, они используются посредством TTP для того, чтобы вычислять два уникальных материала секретных ключей для узла после вычисления двух открытых точек для него. Установление ключей между двумя узлами может осуществляться с использованием одной из (открытых) точек равноправного узла и одного из двух собственных материалов секретных ключей узла, которые представляют собой образы собственных идентификаторов узла в секретной изогении и секретной двойственной изогении, соответственно, в спаривании Вейля. Следует отметить, что спаривание Вейля представляет собой пример билинейного отображения. В случае спаривания Вейля требуется, чтобы все точки имели указанный порядок, скажем, m. Следует отметить, что в первом типе открытая точка и ее соответствующая закрытая точка находятся на разных эллиптических кривых.

Во втором типе, TTP поддерживает изогению для каждой эллиптической кривой, но эти изогении отображаются из эллиптической кривой в саму себя. Например, TTP может иметь одно целое число s и выполнять точечное умножение с целым числом s для каждой кривой. TTP также может иметь два целых числа s_1 и s_2, с использованием первого целого числа для точечного умножения на первой кривой и второго целого числа для точечного умножения на второй кривой. С другой стороны, во время регистрации узлов две изогении используются посредством TTP для того, чтобы вычислять два уникальных

материала секретных ключей для узла, после вычисления двух открытых точек для него. Установление ключей между двумя узлами может осуществляться с использованием одной из (открытых) точек равноправного узла и одного из двух собственных материалов секретных ключей узла. В завершение, билинейное отображение, например, спаривание Вейля, применяется к двум точкам. Здесь, открытая изогения между двумя эллиптическими кривыми используется в качестве системного параметра.

Математически, вариант осуществления первого типа может работать следующим образом. Первый и второй сетевые узлы называются "инициатором" и "ответчиком" в зависимости от того, кто инициирует протокол согласования ключей.

TTP имеет:

– Две обычные эллиптические кривые E1 и E2 над полем F_p с изоморфными кольцами эндоморфизмов дискриминанта $\Delta<-4$,

– Секретный ключ, который представляет собой изогению φ: E1 → E2, указываемой посредством идеала L.

– Открытые спаривания e':G1xG2–>GT и e:G'1xG' 2–>GT, где G1 и G2 являются подгруппами точек на E1, и G'1 G'2 являются подгруппами точек E1 и E2, соответственно, φ' является двойственной изогенией, также секретной, т.е. для всей $P \in G_1', Q \in G_2$, справедливо, что $e(\varphi(P),Q) = e'(P,\varphi'(Q))$.. Кроме того, предполагается, что φ отображает G2 в G'2, и φ' отображает G'1 в G1.

Во время извлечения ключевого материала, каждый субъект с идентификационными данными ID получает H1(ID), точку в G2, и H2(ID), точку в G'1, которые служат в качестве ее двух открытых идентификаторов. Он дополнительно получает из TTP два материала секретных ключей:

Материал секретных ключей S1=φ(H1(ID))

Материал секретных ключей S2=φ'(H2(ID))

Во время формирования ключей, две стороны, инициатор (I) и ответчик (R), которые хотят формировать общий ключ, выполняют следующее:

Инициатор вычисляет: K_IR=e(H2(R), φ(H1(I)))

Инициатор использует K_IR, чтобы шифровать сообщение, и отправляет его в R.

Ответчик вычисляет K_RI=e'(φ'(H2(R)), H1(I)) и дешифрует с использованием ключа K_RI.

Функциональная корректность для первого типа продемонстрирована посредством отмечания того, что вследствие примыкающего свойства изогении φ и ее двойственной φ' относительно спариваний Вейля: K_IR=e(H2(R), φ(H1(I)))=e'(φ'(H2(R)), H1(I))=K_RI.

В варианте осуществления, G1=G2=E1[m], G'1=G'2=E2[m], и e, e' являются спариваниями Вейля на E1 и E2. В альтернативном варианте осуществления, материал открытых ключей и материал секретных ключей сжимаются. Хеш–функции H1 и H2 могут предоставлять только координату X точки на E1 и E2, соответственно. Из H1 (ID) и H2(ID), TTP может вычислять координаты Y y1(ID), y2(ID) таким образом, что U1(D)=(H1(ID), y1(ID)) находится на E1, и U2(ID)=(H2(ID), y2(ID)) находится на E2. Материал S1(ID) секретных ключей может быть равным координате X $\varphi(U1(D))$ и $\varphi'(U2(ID))$, соответственно. Во время формирования ключей две стороны, инициатор (I) и ответчик (R), которые хотят формировать общий ключ, выполняют следующее:

Из собственного секретного ключа S2(I) и открытого ключа H2(R), инициатор вычисляет значение T_{IR} , удовлетворяющее $T_{IR} = e(U2(R),\varphi(U1(I)) + e(U2(R),\varphi(U1(I))^{-1}$, например, как пояснено в работе авторов Galbraith и Lin.

Инициатор использует T_{IR} в качестве ключа для шифрования сообщения M и отправляет его в R.

Ответчик R использует собственный секретный ключ S1(R) и открытый ключ H1(I) для вычисления значения T_{RI} , удовлетворяющее $T_{RI} = e'(U2(R),H1(I)) + e'(U2(R),H1(I))^{-1}$ и дешифрует сообщение с использованием T_{RI}в качестве ключа.

Функциональная корректность вытекает из примыкающего свойства φ'. Очевидно, что возможны варьирования этих вариантов осуществления, например, со сжатым открытым ключом и несжатым секретным ключом, или наоборот, со сжатыми ключами с дополнительными битами, чтобы определять знаки и т.д.

Обобщая, можно иметь: подгруппы G1, G2 для E1, e': G1xG2–>GT; и подгруппы G1', G2' для E2, e: G1'xG2'–>GT; и φ (G1)=G1', φ' (G2')=G2. Для спариваний Вейля: можно требовать отображений в точки на E1, E2, для которых порядок делится на m, и GT состоит из m–ого корня из единицы в конечном поле. Спаривание не должно обязательно задаваться для всех точек на E1.

Математически, вариант осуществления во втором типе может работать следующим образом:

TTP имеет секрет *s.*

Во время извлечения ключей, каждый субъект с идентификационными данными ID получает $H_1(ID) \in E_1, H_2(ID) \in E_2$, и $sH_1(ID) \in E1, sH_2(ID)$, где H_1 является хеш–функцией в E_1 , и $H_2^{H_2}$является хеш–функцией в $E_2.H_1(ID)$, и $H_2(ID)$служит в качестве открытых идентификаторов субъекта, тогда как $sH_1(ID), sH_2(ID)$ служит в качестве его материала секретных ключей.

Во время работы, субъект–инициатор (I), желающий говорить с ответчиком (R), вычисляет K_IR=e($\varphi(H_1(R)), sH_2(I)$, где e является спариванием на E2. Затем идентификационные данные I отправляют сообщение M, зашифрованное с помощью K_IR, в R, R вычисляет K_RI=e($\varphi(H_1(R)), sH_2(I)$).

Функциональная корректность для второго типа продемонстрирована посредством отмечания того, что: K_IR e($\varphi(H(R))$, sH(I))= e($\varphi(H(R))$, H(I)) ^s=e($\varphi(sH(R))$, H(I))=K_RI. Вариант осуществления второго типа, в необязательном порядке, может иметь сжатые точки и использовать вычисление следа операции спаривания посредством использования только координат X и использовать след в качестве ключа или в качестве ввода в функцию извлечения ключей.

Для вариантов осуществления с использованием первого типа, использование секретных изогений: Анализ возможных атак на эту схему, которые подробно описываются ниже, является применимым независимо от того, являются используемые эллиптические кривые обычными или суперсингулярными. Чтобы восстанавливать главный секрет TTP, т.е. секретную изогению φ: E1→E2 и ее двойственную φ', взломщик, который компрометирует множество узлов (и за счет этого получает доступ к их материалам секретных ключей формы φ(H1(ID)) и φ'(H2(ID)), где ID является идентификатором скомпрометированного узла), должен пытаться реконструировать две секретные изогении, упомянутые выше, с использованием оценок этих изогений, которые представляют собой точно материалы секретных ключей скомпрометированных узлов. Восстановление секретного ключа K_IR, вычисленного узлом–инициатором I для узла–ответчика R из открытых параметров H1(I), H2(I), H1 (R) и H2(R), считается трудной проблемой.

Для суперсингулярных эллиптических кривых, безопасность этой разновидности

связана с проблемой суперсингулярной изогении Диффи–Хеллмана (SIDH). Безопасность SIDH основана только на таком допущении, что с учетом пары суперсингулярных кривых E1 и E2, нахождение изогении φ таким образом, что φ:E1→E2, является и классической и квантово–трудной проблемой. Оно представляет собой варьирование классической проблемы абелева скрытого сдвига; тем не менее, группа классов общего кольца эндоморфизмов суперсингулярных кривых не является абелевой, вследствие чего единственный известный эффективный квантовый алгоритм для нахождения секретных изогений не работает в суперсингулярном случае. Можно использовать эллиптические кривые по полю с характеристикой p, для которых группа геометрических точек p является тривиальной, в качестве суперсингулярных.

Фактически, даже этого может быть недостаточным для взломщика, чтобы решать случай проблемы дискретного логарифма, поскольку непонятно то, существует или нет точка Q на E_2 таким образом, что для любого инициатора I, материал φ(H1(I)) секретных ключей узла–инициатора I может представляться как кратное q. В случае если материал φ(H1(I)) секретных ключей узла–инициатора I не может представляться как точка на эллиптической кривой, то варианты осуществления типа 1 имеют повышенную квантовую устойчивость. Фактически, вопрос состоит в том, может или нет φ(H1(I)) записываться в качестве скалярного кратного числа известной точки на E2. Если да, проблема дискретного логарифма является релевантной. E2(m) не должен обязательно иметь один генератор.

Если проблема дискретного логарифма предположительно является трудной (т.е. предполагается, что взломщика, обладающего квантовыми вычислительными возможностями, не существует), то предполагается, что взломщик не может восстанавливать секретный ключ K_IR.

Для вариантов осуществления с использованием второго типа, с использованием открытой изогении: В этой схеме, чтобы восстанавливать секретный ключ K_IR, вычисленный посредством узла–инициатора I с узлом–ответчиком R, взломщик должен решать задачу дискретного логарифма для получения s из открытого ключа H(I) инициатора с идентификационными данными I, и sH(I) является секретным ключом узла–инициатора с идентификационными данными I. Если он добивается успеха, взломщик также восстанавливает главный секрет s TTP и затем может восстанавливать ключи, принадлежащие любому узлу, который регистрируется в TTP. Даже если взломщик имеет возможность компрометировать множество узлов и получать доступ к их материалу sH(ID) секретных ключей, где ID является идентификатором скомпрометированного узла, предполагается, что взломщик по–прежнему неспособен восстанавливать главный секрет TTP s, при условии, что один случай задачи дискретного логарифма остается трудным для решения.

В отсутствие квантовых компьютеров, если предполагается, что взломщика, допускающего эффективное решение задачи дискретного логарифма, не существует, то оба предложенных типа являются защищенными и функционально корректными. Тем не менее, если такой взломщик существует, второй тип может быть скомпрометирован. Тем не менее, варианты осуществления согласно первому типу не затрагиваются напрямую в том смысле, что секрет TTP (изогения) не может восстанавливаться.

Криптографические операции на стороне узла в варианте осуществления с использованием первого типа содержат только оценку спариваний Вейля по эллиптическим кривым, которые являются функционально относительно эффективными. Это имеет желательные последствия для узлов, которые типично представляют собой

IoT–устройства с ограниченными вычислительными характеристиками и характеристиками запоминающего устройства. Вычисление изогении между двумя эллиптическими кривыми и оценка изогении для точки эллиптической кривой являются сравнительно более интенсивными, но в этой разновидности такая изогения вычисляется только в TTP.

Фиг. 1 схематично показывает пример варианта осуществления системы 100 предварительного распределения ключей. Система 100 содержит электронное устройство 110 предварительного распределения ключей и множество сетевых узлов. На фиг. 1 показаны сетевые узлы 210 и 211. Число сетевых узлов типично составляет гораздо больше, например, больше 1000, 10000 и т.д. Устройство 110 предварительного распределения ключей конфигурирует множество сетевых узлов для протокола согласования ключей. В частности, устройство 110 предварительного распределения ключей может выполнять фазу предварительного распределения ключей в схеме предварительного распределения ключей на основе идентификационных данных и конфигурирует сетевые узлы 210, 211 с материалом локальных ключей таким образом, что позднее любые два из множества сетевых узлов могут защищенно согласовывать совместно используемый ключ между собой. Материал локальных ключей включает в себя, по меньшей мере, две закрытые точки на двух эллиптических кривых. Эти закрытые точки являются закрытыми для сетевого узла и/или для всех доверенных устройств, таких как устройство 110. Материал локальных ключей также может включать в себя незакрытые элементы, например, идентификатор устройства, открытые точки эллиптической кривой и необязательно открытую изогению. Инициализация описывается главным образом относительно узла 210, но другие узлы могут инициализироваться аналогично.

Устройство 110 предварительного распределения ключей содержит интерфейс 120 связи, выполненный с возможностью конфигурировать сетевой узел закрытой точкой эллиптической кривой. Интерфейс связи может иметь тип, идентичный типу, используемому между сетевыми узлами (см. ниже), но также может иметь другой тип. Например, интерфейс 120 связи может представлять собой проводной интерфейс, например, проводное соединение, задаваемое при тестировании и инициализации устройства во время изготовления сетевых узлов 210, 211 и т.д. Например, интерфейс 120 связи может содержать соединительную панель или соединительный порт. Интерфейс 120 связи также может представлять собой цифровое проводное сетевое соединение или беспроводное сетевое соединение, или гибридное соединение и т.д. Например, интерфейс 120 связи может содержать антенну.

Устройство 110 предварительного распределения ключей содержит устройство 130 хранения данных. Устройство 130 хранения данных содержит представление первой эллиптической кривой 131 и второй эллиптической кривой 132. Эллиптические кривые 131 и 132 представляют собой разные кривые, например, они могут задаваться разными формулами. Эллиптическая кривая может задаваться посредством коэффициентов формулы, которая задает ее, например, в некоторой канонической форме. Одна такая форма представляет собой $Y^2 = X^3 + AX + B$, при этом A и B являются целыми числами, которые задают эллиптическую кривую. Например, устройство 130 хранения данных может сохранять коэффициенты A и B для двух эллиптических кривых. Альтернативно, два числа могут жестко кодироваться в алгоритмах, которые используют их, например, умножение по кривой или эллиптические хеш–функции (см. дополнительно ниже).

В варианте осуществления, первая и вторая эллиптические кривые задаются над

полем F_q с характеристикой p. Например, можно принимать q=p^k. В варианте осуществления, p=2. Наряду с кривыми 131, 132, может сохраняться информация по полю, для которого они задаются. Следует отметить, что две кривые задаются по идентичному полю.

В варианте осуществления, эллиптические кривые 131 и 132 представляют собой так называемые обычные (не суперсингулярные) кривые. Например, можно рассматривать эллиптические кривые из документа "Recommended Elliptic Curves For Federal Government Use", совокупность эллиптических кривых рекомендуется для использования Федеральным правительством. В варианте осуществления, эллиптические кривые 131 и 132 представляют собой так называемые суперсингулярные кривые. Примеры суперсингулярных кривых включают в себя следующее: если K является полем с характеристикой 2, каждая кривая задана посредством уравнения формы $y^2 + a_3 y = x^3 + a_4 x + a_0$, с ненулевым a_3 ; если K является полем с характеристикой 3, каждая кривая задана посредством уравнения формы $y^2 = x^3 + a_4 x + a_6$, с ненулевым a_4. Известны другие примеры.

Устройство 110 распределения ключей содержит модуль 140 обработки эллиптических хеш–функций. Модуль 140 обработки эллиптических хеш–функций выполнен с возможностью получать цифровой идентификатор (ID) для сетевого узла 210. Цифровой идентификатор может приниматься из сетевого узла 210, например, через интерфейс 120 связи. Например, сетевой узел 210 может отправлять в устройство 110 предварительного распределения ключей идентификатор. Идентификатор также может назначаться посредством устройства 110 предварительного распределения ключей, например, посредством модуля 140 обработки хеш–функций. Например, идентификатор может содержать порядковый номер сетевого узла 210, случайное число, одноразовый номер и т.д. Например, идентификатор может содержать цифровой адрес компьютера сетевого узла, например, IP–адрес, MAC–адрес и т.д. Идентификатор может содержать общее имя сетевого узла 210 или имя пользователя сетевого узла 210. Идентификатор может содержать информацию относительно ролей или авторизаций пользователя. Вторые опции являются полезными для неявной аутентификации; например, устройство 110 может назначать или верифицировать роли.

Модуль 140 обработки хеш–функций сконфигурирован с двумя хеш–функциями: первой хеш–функцией 147 и второй хеш–функцией 148. Первая хеш–функция 147, H_1 , отображает цифровой идентификатор сетевого узла 210 в первую открытую точку 141, $H_1(ID)$, на первой эллиптической кривой 131. Вторая хеш–функция 148, H_2, отображает цифровой идентификатор сетевого узла 210 во вторую открытую точку 142, $H_2(ID)$, на второй эллиптической кривой 132. Хеш–функции могут включать в себя дополнительную информацию вместе с идентификатором, например, идентификацию устройства 110 предварительного распределения ключей, например, соль, например, дополнительную информацию относительно сетевого узла 210, например, временную метку времени создания материала локальных ключей.

Открытые точки 141 и 142 составляют часть материала 145 открытых ключей для сетевого узла 210. Вообще говоря, предусмотрено два подхода к материалу 145 открытых ключей. Материал 145 открытых ключей может сохраняться в сетевом узле 210, например, вместе с материалом закрытых ключей. В этом случае, узлы могут использовать открытую точку другого узла и закрытую точку себя, чтобы получать совместно используемый ключ. Это исключает необходимость вычислять эллиптические

хеш–функции 147 и 148 в узле. Фактически, идентификатор сетевого узла даже не требуется в узле в этом случае; устройство 110 предварительного распределения ключей может просто рассматривать случайное число для означенного. С другой стороны, сетевые узлы также могут быть выполнены с возможностью вычислять открытые точки 141 и 142 для другого узла из идентификатора этого узла. Если какая–либо дополнительная информация используется, в дополнение к идентификатору, то эта дополнительная информация должна быть известна для узла, который вычисляет открытые точки 141 и 142. Эти варианты осуществления могут предоставлять неявную аутентификацию, но требуют дополнительных вычислений. Оба подхода могут комбинироваться, например, некоторые узлы вычисляют непосредственно хеши, некоторые узлы используют предварительно вычисленную открытую точку. В варианте осуществления, открытая информация содержит идентификатор и необязательно любую дополнительную информацию, которая может составлять часть материала открытых ключей, но не открытые точки 141 и 142. В варианте осуществления, открытая информация содержит открытые точки 141 и 142, но не идентификатор. В варианте осуществления, открытая информация содержит открытые точки 141 и 142, а также идентификатор и необязательно любую дополнительную информацию.

Хеш–функции 147 и 148 отображают битовую строку, к примеру, цифровой идентификатор, в точку на эллиптической кривой. Предпочтительно, хеш–функции являются криптографически устойчивой к коллизиям, т.е. трудно находить два идентификатора, которые отображаются в идентичную точку эллиптической кривой, но статистическая устойчивость к коллизиям может быть достаточной в вариантах осуществления, т.е. маловероятно, что два случайных идентификатора отображаются в идентичную точку эллиптической кривой. Эллиптические хеши могут конструироваться из традиционных хеш–функций, таких как хеш–функция из SHA–семейства, например, SHA–256 и т.д. Например, можно хешировать идентификатор и отображать его в значение в поле, над которым задается эллиптическая кривая. После этого, заменять значение в качестве значения X в каноническом представлении эллиптической кривой (например, координаты с кубической степенью) и в завершение вычислять значение Y. То, какое значение Y следует выбирать (в общем, предусмотрено два решения), может определяться посредством некоторого бита хеша идентификатора или посредством бита из дополнительного хеша идентификатора и т.д. Хеши могут отличаться для первой и второй кривых посредством добавления идентификатора кривой в идентификатор, например, магическое число, например, 1 для кривой 131 и 2 для кривой 132. Две открытые точки 141 и 142 находятся на разных первой и второй эллиптических кривых. Например, точка 141 может находиться на кривой 131, а точка 142 – на кривой 132.

Устройство 110 предварительного распределения ключей содержит модуль 150 обработки изогений. Модуль 150 обработки изогений принимает открытые точки, вычисленные посредством модуля 140 обработки хеш–функций, и вычисляет закрытые точки эллиптической кривой из них посредством применения изогений к ним. Устройство 130 хранения данных дополнительно содержит информацию 135, представляющую первую секретную изогению для первой эллиптической кривой 131 и вторую секретную изогению для второй эллиптической кривой 132. Знание этих изогений должно приводить к бреши во всей системе. По этой причине, они держатся в секрете от любого, кто не может быть доверенным, чтобы защищать систему.

Модуль 150 обработки изогений выполнен с возможностью применять первую секретную изогению к первой открытой точке 141 эллиптической кривой, получая

первую закрытую точку 151 эллиптической кривой, и применять вторую секретную изогению ко второй открытой точке 142 эллиптической кривой, получая вторую закрытую точку 152 эллиптической кривой. Первая закрытая точка 151 эллиптической кривой находится на одной из эллиптических кривых 131, 132, и вторая закрытая точка 152 эллиптической кривой находится на другой из эллиптических кривых 131, 132. В некоторых вариантах осуществления, точки 141 и 151 эллиптической кривой находятся на идентичной кривой, в некоторых вариантах осуществления точки 141 и 151 эллиптической кривой находятся на разной эллиптической кривой. Секретные изогении отображают точку в эллиптическую кривую в точку на эллиптической кривой. Различные примеры устройства 130 хранения данных и модуля 150 обработки изогений проиллюстрированы относительно фиг. 2a–2c.

Фиг. 2a схематично показывает пример варианта осуществления устройства 161 хранения данных устройства предварительного распределения ключей. Устройство 161 хранения данных может использоваться в устройстве 110 предварительного распределения ключей вместо устройства 130 хранения данных. Устройство 161 хранения данных может использоваться в варианте осуществления первого типа, как пояснено выше. В устройстве 161 хранения данных, информация 135 изогений содержит первую изогению 162 и вторую изогению 163.

Первая изогения 162, φ, представляет собой отображение из первой эллиптической кривой 131 во вторую эллиптическую кривую 132. Вторая изогения 163 является двойственной относительно первой изогении 162, φ', и обеспечивает отображение из второй эллиптической кривой 132 в первую эллиптическую кривую 131. Можно рассматривать двойственную изогению в качестве уникальной изогении таким образом, что конструкция $\varphi'*\varphi$ представляет собой умножение на первой эллиптической кривой со степенью первой изогении. В варианте осуществления, степень первой изогении 162 составляет, по меньшей мере, 2^{90} , по меньшей мере, 2^{128} или, по меньшей мере, 2^{256} и т.д. Значительная степень изогении исключает атаки методом исчерпывающего поиска, поскольку эллиптические кривые, которые используются, являются открытыми.

В этом варианте осуществления, точки 141 и 151 эллиптической кривой находятся на разных кривых, как и точки 142 и 152. Модуль 150 обработки изогений применяет первую изогению 162 к точке 141 и вторую двойственную изогению 163 к точке 142. Этот вариант осуществления, в частности, может использовать технологии, раскрытые в работе "Evaluating large degree isogenies and applications to pairing based cryptography" авторов Reinier Bröker, Denis Charles и Kristin Lauter.

Фиг. 2b схематично показывает пример варианта осуществления устройства 167 хранения данных устройства предварительного распределения ключей. Устройство 167 хранения данных может использоваться в устройстве 110 предварительного распределения ключей вместо устройства 130 хранения данных. Устройство 167 хранения данных может использоваться в варианте осуществления согласно второму типу. Устройство 167 хранения данных сохраняет секретное целое число 164, s. Первая изогения может задаваться как точечное умножение на первой кривой 131 на s. Вторая изогения может задаваться как точечное умножение на второй кривой 132 также на s. В этом варианте осуществления, точки 141 и 151 эллиптической кривой находятся на идентичной кривой, как и точки 142 и 152. Этот вариант осуществления может использовать традиционные алгоритмы точечного умножения.

Фиг. 2c схематично показывает пример варианта осуществления устройства 168 хранения данных из состава устройства предварительного распределения ключей. Устройство 168 хранения данных может использоваться в устройстве 110

предварительного распределения ключей вместо устройства 130 хранения данных. Устройство 168 хранения данных может использоваться в варианте осуществления согласно второму типу. Устройство 168 хранения данных сохраняет два секретных целых числа 165, 166, s_1,s_2. Первая изогения может задаваться как точечное умножение на первой кривой 131 на s_1. Вторая изогения может задаваться как точечное умножение на второй кривой 132 на s_2. В этом варианте осуществления, точки 141 и 151 эллиптической кривой находятся на идентичной кривой, как и точки 142 и 152. Этот вариант осуществления может использовать традиционные алгоритмы точечного умножения.

В варианте осуществления, модуль 140 обработки хеш–функций модифицируется таким образом, что он также включает в себя точечное умножение. Первая открытая точка 141 вычисляется в качестве $a_1\, H_1\,(ID)$, а вторая открытая точка – в качестве $a_2\, H_2\,(ID)$. Параметры выбираются таким образом, что $a_1 s_2 = a_2 s_1$. В варианте осуществления, целые числа a_1 и a_2 могут быть открытыми, хотя это может исключаться посредством использования открытых точек вместо хеш–функций в сетевых узлах; то, что узел принимает одну из открытых точек другой стороны вместо ее идентификатора.

В варианте осуществления, все точки, которые могут использоваться, имеют порядок, который делится на общее число m. В этом случае, случай по фиг. 2c может уменьшаться посредством переопределения H1, H2 и задания $s = s_1/a_1 = s_2/a_2$, где / является делением по модулю m.

Вернемся к фиг. 1. Первая закрытая точка 151 эллиптической кривой и вторая закрытая точка 152 эллиптической кривой составляют часть материала 155 закрытых ключей для сетевого узла 210. Устройство 110 предварительного распределения ключей выполнено с возможностью записывать, по меньшей мере, материал 155 закрытых ключей в сетевой узел 210. Помимо этого, или идентификатор для сетевого узла 210 или открытые точки 141 и 142, например, материал 145 открытых ключей записывается в сетевой узел 210. Запись обоих из них также является возможной.

Фиг. 3a схематично показывает пример варианта осуществления системы 200 согласования ключей. Система 200 согласования ключей содержит множество узлов, которые выполнены с возможностью совместного использования ключей посредством устройства предварительного распределения ключей, такого как устройство 110 предварительного распределения ключей. Множество узлов в системе 200 могут обмениваться данными между собой через защищенную связь, защищенную с использованием совместно используемого ключа, который каждый узел может вычислять для любого из других узлов. Устройство 110 предварительного распределения ключей также может составлять часть системы 200, например, чтобы динамически добавлять новые узлы даже после того, как система 200 работает. Это не является обязательным. В варианте осуществления, устройство 110 предварительного распределения ключей отбрасывается после того, как все узлы инициализируются с материалом локальных ключей.

Относительно фиг. 3a, проиллюстрированы варианты осуществления первого типа. Первый сетевой узел 210 сконфигурирован для протокола согласования ключей с множеством сетевых узлов. Протокол согласования ключей проиллюстрирован относительно второго сетевого узла 211. Структура второго сетевого узла 211 в основном является идентичной структуре первого сетевого узла 210 за исключением того, что они имеют взаимосвязь "отправитель/приемник".

Сетевой узел 210 содержит устройство 230 хранения данных. Устройство 230 хранения данных содержит некоторое средство, с помощью которого второй узел 211 может получать открытую точку для сетевого узла 210. Например, устройство 230 хранения данных может сохранять цифровой идентификатор 234, ID_1, для первого сетевого узла. Цифровой идентификатор является идентичным идентификатору, используемому для того, чтобы вычислять материал закрытых ключей для узла 210. Вместо цифрового идентификатора устройство 230 хранения данных может сохранять первую открытую точку 241 эллиптической кривой и вторую открытую точку 242 эллиптической кривой. Точки могут соответствовать открытым точкам 141 и 142. Использование идентификатора имеет такое преимущество, что неявная аутентификация является возможной. Использование открытых точек имеет такое преимущество, что некоторые вычисления исключаются в узлах. Первая и вторая открытые точки 241, 242 эллиптической кривой находятся на первой и второй эллиптических кривых, соответственно.

Устройство 230 хранения данных также сохраняет первую закрытую точку 251 эллиптической кривой и вторую закрытую точку 252 эллиптической кривой. Первая закрытая точка 251 эллиптической кривой и вторая закрытая точка 252 эллиптической кривой соответствуют первой открытой точке 241 эллиптической кривой и второй открытой точке 242 эллиптической кривой через первую и вторую секретные изогении. Первая открытая точка 241 эллиптической кривой и вторая открытая точка 242 эллиптической кривой в свою очередь соответствуют цифровому идентификатору 234 через первую и вторую хеш–функции 147, 148.

В этом варианте осуществления, первая изогения может представлять собой изогению 162, и вторая изогения может представлять собой изогению 163. Точки 241 и 251 не находятся на идентичной кривой, так же, как и точки 242 и 252.

Устройство 230 хранения данных может сохранять первую эллиптическую кривую 231 и вторую эллиптическую кривую 232, на которой находятся точки в открытых и закрытых данных. Кривые могут представляться, например, посредством коэффициентов уравнения для кривой. Кривая также может присутствовать неявно, например, жестко кодироваться в алгоритме билинейного отображения и т.п.

Первый и второй сетевые узлы 210, 211 содержат интерфейс 220 связи. Интерфейс 220 связи первого сетевого узла 210 выполнен с возможностью цифровой связи со вторым сетевым узлом 211. Типично, интерфейс 120 связи выполнен с возможностью обмениваться данными со многими из других узлов в системе 200.

Интерфейсы связи могут быть выполнены с возможностью цифровой связи с другими узлами в системе согласования ключей. Тем не менее, необязательно, что все узлы в системе могут достигаться в любой момент времени. Интерфейс 220 связи выполнен с возможностью цифровой связи. Например, интерфейсы связи могут быть выполнены с возможностью обмениваться данными по компьютерной сети. Например, интерфейс связи может быть выполнен с возможностью беспроводной связи, например, Wi–Fi, ZigBee, Bluetooth и т.п., и/или проводной связи, например, Ethernet, USB и т.п. Связь между узлами 210 и 211 также может представлять собой комбинацию проводных и беспроводных соединений. Например, узлы в системе 200, включающей в себя узлы 210 и 211, могут содержать электронное устройство хранения данных, которое содержит идентификатор связи, который уникально идентифицирует узел в системе 200. Например, идентификатор связи может быть включен в цифровые сообщения, которыми обмениваются между узлами 210 и 211, например, чтобы адресовать сообщение. Например, идентификатор связи может представлять собой IP–адрес, MAC–адрес и т.п.

Преимущественно, идентичный идентификатор связи может содержаться в цифровом идентификаторе 234 и использоваться для того, чтобы вычислять материал локальных ключей.

Сетевой узел 210 содержит модуль 260 обработки совместно используемых ключей. Модуль 260 обработки совместно используемых ключей выполнен с возможностью получать открытую точку эллиптической кривой для второго сетевого узла (например, точку $H_2(ID_2)$, где ID_2 является идентификатором второго сетевого узла), причем открытая точка эллиптической кривой находится на первой из первой и второй эллиптических кривых. Как указано, для этой цели предусмотрены различные варианты. Например, второй сетевой узел 210 может отправлять открытую точку эллиптической кривой ($H_2(ID_2)$) непосредственно в первый сетевой узел 210, например, через интерфейс 220 связи. С другой стороны, второй сетевой узел 211 может отправлять свой идентификатор ID_2 вместо этого. В этом случае модуль 260 обработки совместно используемых ключей может применять одну из хеш–функций 147 и 148, например, вторую хеш–функцию 148, чтобы получать открытую точку для второго сетевого узла 211. Модуль 260 обработки совместно используемых ключей также выбирает закрытую точку эллиптической кривой из первой и второй закрытых точек эллиптической кривой, находящихся на эллиптической кривой, идентичной эллиптической кривой принимаемой открытой точки, например, $\varphi(H_1(ID_1))$. В конечном счете, модуль 260 обработки совместно используемых ключей получает две точки эллиптической кривой на идентичной кривой: например, одну открытую точку, полученную из второго узла 211, и одну закрытую точку, выбранную из устройства 230 хранения данных. Например, точки, используемые посредством модуля 260 обработки совместно используемых ключей, могут представлять собой $H_2(ID_2)$ и $\varphi(H_1(ID_1))$. К этим двумя точкам, билинейное отображение e применяется посредством модуля 260 обработки совместно используемых ключей, например, $e(H_2(ID_2), \varphi(H_1(ID_1)))$. Билинейное отображение может представлять собой спаривание Вейля или спаривание Тейта и т.д. Результат билинейного отображения может использоваться в качестве совместно используемого ключа. Вывод также дополнительно может обрабатываться, например, с использованием функции извлечения ключей (KDF). В варианте осуществления, все выходные биты билинейных отображений вводятся в функцию извлечения ключей (KDF), например, в криптографическую хеш–функцию. Пример KDF, например, представлен в CMLA_KDF из CMLA Technical Specification, Version: V1.43–20131218, либо в KDF–функции, заданной в "DRM specification", OMA–TS–DRM–DRM–V2_0_2–20080723–A, Open Mobile Alliance™, Version 2.0.2, section 7.1.2, и т.д.

Второй сетевой узел 211 также имеет модуль обработки совместно используемых ключей, который проводит соответствующее вычисление $e'(H_1(ID_1), \varphi'(H_2(ID_2)))$. То, какое вычисление следует использовать, может жестко кодироваться на стороне, которая инициирует или отвечает. Например, может быть согласовано, что инициирующий узел использует открытую точку для отвечающего узла на второй кривой, а также закрытую точку на второй кривой; тогда как отвечающая сторона принимает открытую точку для инициирующего узла на первой кривой и секретную закрытую точку на первой кривой. Это также может быть наоборот. В варианте осуществления этого типа, один узел вычисляет билинейное отображение e' на первой кривой, в то время как другой узел вычисляет билинейное отображение e на второй кривой. Это работает, поскольку, с учетом двух билинейных отображений на двух кривых и изогении, получается двойственная изогения.

В необязательном порядке, сетевой узел 210 может содержать модуль 280 подтверждения правильности ключей. Модуль 280 подтверждения правильности ключей выполнен с возможностью вычислять данные подтверждения правильности ключей из криптографического ключа и отправлять данные подтверждения правильности ключей во второй сетевой узел. Данные подтверждения правильности ключей могут представлять собой некоторый аутентификационный маркер, например, зашифрованную временную метку, например, зашифрованный оклик из второго узла и т.д. Данные подтверждения правильности ключей обеспечивают неявную аутентификацию, в том смысле, что она доказывает для второго сетевого узла то, что первый сетевой узел должен иметь допустимый материал ключей, что, в свою очередь означает то, что оно зарегистрировано в устройстве 110 предварительного распределения ключей. Альтернативно или помимо этого, модуль 280 подтверждения правильности ключей может быть выполнен с возможностью принимать данные подтверждения правильности ключей для криптографического ключа из второго узла и верифицировать данные подтверждения правильности ключей с использованием извлеченного совместно используемого ключа. Это верифицирует то, что второй сетевой узел корректно вычисляет криптографический ключ, и в силу этого предоставляет неявную аутентификацию.

Схема согласования/распределения ключей, проиллюстрированная относительно фиг. 3a, является подходящей для такого варианта применения, как Интернет вещей, вследствие неинтерактивного характера установления ключей между узлами и облегченных операций на основе криптографических спариваний по эллиптическим кривым. Изогении выполняются только посредством TTP, которая может обладать большим количеством ресурсов и в силу этого допускает проведение таких операций. Материалы секретных ключей каждого узла могут защищенно предоставляться посредством TTP в узлы, например, во время самоинициализации узлов. Модель обеспечения безопасности, рассматриваемая при оценке атак, представляет собой модель обеспечения безопасности на основе тайных сговоров по умолчанию и учитывает взломщиков, которые могут компрометировать IoT–узлы в поле и использовать их скомпрометированные материалы ключей для того, чтобы предпринимать атаки на остальную часть сети и, в частности, на TTP.

Преимущество протокола, реализованного в узле 210, состоит в том, что совместно используемый ключ может вычисляться без обмена сообщениями при условии, что цифровой идентификатор другого узла известен. Извлеченный ключ затем может использоваться для того, чтобы извлекать ключ для симметричного шифрования.

Фиг. 3b схематично показывает пример варианта осуществления системы 201 согласования ключей. Система 201 является аналогичной системе 200 за исключением того, что она использует предварительное распределение ключей второго типа. Система 201 содержит множество сетевых узлов; показаны узлы 215 и 216.

Аналогично сетевому узлу 210, узел 215 содержит устройство 230 хранения данных. Устройство 230 хранения данных содержит материал 245 открытых ключей, материал 255 закрытых ключей, первую эллиптическую кривую 231, вторую эллиптическую кривую 232 и цифровой идентификатор 234. Аналогично узлу 210, часть из указанного является необязательной, например, требуется только одно из цифрового идентификатора 234 и открытого материала 245. Первая эллиптическая кривая 231 и вторая эллиптическая кривая 232 не должны обязательно быть явными, но могут быть неявными, например, жестко кодироваться в алгоритмах для точечного умножения, билинейных отображений и т.п.

Отличие от узла 210 заключается в том, что в узле 215, первая открытая точка 241 и первая закрытая точка 251 находятся на одной и той же эллиптической кривой, и в том, что вторая открытая точка 242 и вторая закрытая точка 252 находятся на другой эллиптической кривой. Кроме того, устройство 230 хранения данных по фиг. 3b содержит открытую изогению 235. Открытая изогения 235 представляет собой отображение из первой эллиптической кривой во вторую эллиптическую кривую (или наоборот). Предпочтительно, открытая изогения 235 представляет собой изогению низкой степени. Интересно, что степень изогении практически ничего не привносит в безопасность, поскольку изогения является открытой; тем не менее, более низкая степень обеспечивает упрощенную реализацию в узлах. В вариантах осуществления этого типа, открытая изогения обеспечивает то, что каждый узел выполняет билинейное отображение на идентичной кривой; в случае, если открытая изогения отображает сначала во вторую кривую, как первый, так и второй узлы вычисляют билинейное отображение на второй кривой.

Узел 215 содержит модуль 270 обработки изогений, выполненный с возможностью применять открытую изогению, заданную посредством информации 235, к точке на первой кривой 231. В частности, модуль 270 обработки изогений должен применяться к открытой точке на первой кривой, которая принимается из второго узла или вычисляется для второго узла из его цифрового идентификатора, или модуль 270 обработки изогений должен применяться к закрытой точке 251 самого узла 215 на первой кривой. Модуль 270 обработки изогений в варианте осуществления второго типа может использовать аналогичное проектное решение с модулем 150 обработки изогений в варианте осуществления первого типа, за исключением того, что модуль 270 обработки изогений не должен обязательно оценивать двойственные изогении.

Модуль 260 обработки совместно используемых ключей выполнен с возможностью получать открытую точку эллиптической кривой для второго сетевого узла, открытая точка эллиптической кривой может находиться на любой из первой и второй эллиптических кривых. Модуль 260 обработки совместно используемых ключей может вычислять открытую точку эллиптической кривой для второго сетевого узла или принимать ее. Модуль 260 обработки совместно используемых ключей также выбирает закрытую точку эллиптической кривой из устройства 230 хранения данных по фиг. 3b, которая находится на другой эллиптической кривой относительно открытой точки для узла 216. В этот момент, модуль 260 обработки совместно используемых ключей получает две точки эллиптической кривой, по одной на каждой из двух кривых, одна из которых является закрытой для узла 215, и одна из которых является открытой для узла 216. Следующий модуль 260 обработки совместно используемых ключей применяет модуль 270 обработки изогений к точке, которая находится на первой эллиптической кривой, она может представлять собой открытую или закрытую точку. Результат заключается в том, что две точки теперь получаются на второй эллиптической кривой. В завершение, модуль 270 обработки совместно используемых ключей оценивает билинейное отображение e для второй эллиптической кривой и двух точек на ней.

Что касается узла 210, из результата билинейного отображения, совместно используемый ключ может извлекаться, например, с использованием KDF. В случае точечного сжатия, след результата билинейного отображения может использоваться для извлечения совместно используемого ключа.

Узлы могут быть сконфигурированы в зависимости от того, какой из них представляет собой инициирующий узел, того, какую точку следует использовать. Например, инициатор может использовать первую открытую точку для отвечающего узла, тогда

как ответчик использует вторую открытую точку инициатора.

В различных вариантах осуществления, например, относительно устройства 110 предварительного распределения ключей или сетевого узла 210, 215 интерфейс связи может выбираться из различных альтернатив. Например, интерфейс связи может представлять собой сетевой интерфейс с локальной или глобальной вычислительной сетью, например, с Интернетом, интерфейс хранения данных с внутренним или внешним устройством хранения данных. Интерфейс связи может представлять собой считыватель карт и т.д.

Устройство 130, 230 хранения данных может реализовываться как электронное запоминающее устройство, скажем, флэш–память, или магнитное запоминающее устройство, скажем, жесткий диск и т.п.

Устройство 130, 230 хранения данных может содержать множество дискретных запоминающих устройств, вместе составляющих устройство хранения данных. Устройство 130, 230 хранения данных также может представлять собой временное запоминающее устройство, скажем, RAM, но в случае устройства временного хранения данных, устройство хранения данных содержит некоторое средство для того, чтобы получать параметры перед использованием, скажем, посредством их получения по необязательному сетевому соединению (не показано).

Типично, устройства 110, 210 и 215 содержат микропроцессор (отдельно не показан), который выполняет надлежащее программное обеспечение, сохраненное в устройствах 110, 210 и 215; например, это программное обеспечение, возможно, загружено и/или сохранено в соответствующем запоминающем устройстве, например, в энергозависимом запоминающем устройстве, к примеру, в RAM, или в энергонезависимом запоминающем устройстве, к примеру, во флэш–памяти (отдельно не показана). Альтернативно, устройства 110, 210 и 215 могут, полностью или частично, реализовываться в программируемой логике, например, в качестве программируемой пользователем вентильной матрицы (FPGA). Устройства 110, 210 и 215 могут реализовываться, полностью или частично, в качестве так называемой специализированной интегральной схемы (ASIC), т.е. интегральной схемы (IC), специально разработанной для конкретного использования. Например, схемы могут реализовываться в CMOS, например, с использованием языка описания аппаратных средств, такого как Verilog, VHDL и т.д.

В варианте осуществления, устройство 110 предварительного распределения ключей содержит интерфейсную схему связи, схему хранения данных, схему модуля обработки эллиптических хеш–функций, схему модуля обработки изогений. В варианте осуществления, сетевой узел 210 содержит интерфейсную схему связи, схему хранения данных, схему модуля обработки совместно используемых ключей и необязательную схему модуля подтверждения правильности ключей. Сетевой узел 215 также может содержать схему модуля обработки изогений. Схемы могут представлять собой процессорную схему и схему хранения данных, причем процессорная схема выполняет инструкции, представленные электронно в схемах хранения.

Процессорная схема может реализовываться распределенным способом, например, в качестве множества подпроцессорных схем. Устройство хранения данных может быть распределено по множеству распределенных субустройств хранения данных. Часть или все запоминающее устройство может представлять собой электронное запоминающее устройство, магнитное запоминающее устройство и т.д. Например, устройство хранения данных может иметь энергозависимую и энергонезависимую часть. Часть устройства хранения данных может быть неперезаписываемой.

Фиг. 4 схематично является упрощенной схемой последовательности операций,

которая иллюстрирует пример варианта осуществления способа согласования ключей. Совместно используемый ключ устанавливается между сетевыми узлами 210 и 211, как показано на фиг. 3a. Тем не менее, аналогичный способ является применимым к узлам 215 и 215 по фиг. 3b. Последовательность 400 сообщений, которая показана на фиг. 4, содержит множество сообщений, которыми обмениваются между узлами, показаны сообщения 410, 420 и 430.

В первом сообщении 410, узел 210 отправляет запрос согласования ключей в узел 211. Запрос включает в себя цифровой идентификатор ID_1 узла 210. Второе сообщение 420, отправленное из узла 211 в узел 210, содержит цифровой идентификатор ID_2 узла 211.

В этот момент, узел 210 вычисляет вторую открытую точку узла 211: $H_2(ID_2)$ и выбирает собственную первую закрытую точку $\varphi(H_1(ID_1))$. Узел 210 вычисляет билинейное отображение $e(H_2(ID_2), \varphi(H_1(ID_1)))$ и извлекает совместно используемый ключ из результата.

Все или часть сообщения 430, отправленного из узла 210 до 211, защищается, например, шифруется/или аутентифицируется, например, с использованием блочного шифра или кода аутентификации сообщений (MAC) с использованием полученного совместно используемого ключа. Содержимое защищенной части может быть не связано с протоколом согласования ключей, например, чтобы удовлетворять некоторую дополнительную потребность в связи узлов 210 и 211, например, обмениваться значениями датчика и т.д.

Перед или после приема сообщения 430, узел 211 вычисляет первую открытую точку узла 210: $H_1(ID_1)$ и выбирает собственную вторую закрытую точку $\varphi'(H_2(ID_2))$. Узел 210 вычисляет билинейное отображение $e(H_1(ID_1), \varphi'(H_2(ID_2)))$ и извлекает совместно используемый ключ из результата. Совместно используемый ключ затем может использоваться узлом 211 для того, чтобы дешифровать и/или верифицировать сообщение 430 либо его часть.

Если узлы 210 и 211 уже знают цифровой идентификатор другого узла, то сообщения 410 и 420 могут отменяться. Сообщение 430 может содержать маркер подтверждения правильности ключей, вычисленный узлом 210. Сообщение 420 может содержать оклик (challenge) из узла 211, например, одноразовый номер, который должен шифроваться узлом 210. Сообщение 430 может содержать оклик в узел 211. Дополнительное сообщение из узла 211 в узел 210 может содержать маркер подтверждения правильности ключей, вычисленный посредством узла 211.

Вариант применения протокола согласования ключей заключается в приложениях для обмена сообщениями. Например, в таком варианте применения можно предполагать, что отправитель уже имеет идентификатор приемного устройства. Например, первый сетевой узел может отправлять сообщение во второй сетевой узел, включающее в себя: идентификатор первого сетевого узла, защищенное сообщение. Например, идентификатор первого сетевого узла может представлять собой (мобильный) телефонный номер, адрес электронной почты, адрес компьютера, например, IP–адрес и т.п. Первый узел имеет возможность вычислять совместно используемый ключ заранее, поскольку он знает идентификатор, например, телефонный номер, второго узла, для которого предназначено сообщение. Сообщение может непосредственно отправляться в идентификатор второго узла посредством идентификатора, например, в случае адреса электронной почты или адреса компьютера. Сообщение также может отправляться посредством посредника, например, услуги маршрутизации, которая отправляет

сообщение по компьютерной сети в устройство, ассоциированное с идентификатором, например, телефонным номером. Во втором случае, узлы могут использовать телефонный номер во время регистрации, чтобы получать материал локальных ключей, и включать адрес компьютера для маршрутизации сообщений. Интересно, что первый узел может отправлять сообщение, даже если второй узел в данный момент оффлайн и не может интерактивно участвовать в протоколе согласования ключей. Сообщение первого узла может сохраняться в буфере, например, посредством устройства маршрутизации до тех пор, пока второе устройство не становится онлайн.

Фиг. 5 схематично показывает пример варианта осуществления способа 500 предварительного распределения ключей. Способ 500 для предварительного распределения ключей конфигурирует множество сетевых узлов, таких как узлы 210 и 211 или узлы 215 и 216, с информацией локальных ключей. Способ 500 предварительного распределения ключей содержит:– сохранение 510 информации 135, представляющей первую секретную изогению φ; s, для первой эллиптической кривой 131; E_1 , и вторую секретную изогению φ'; s, для второй эллиптической кривой 132; E_2, причем изогения приспособлена принимать точку на эллиптической кривой и формировать точку на эллиптической кривой в качестве вывода,

– получение 520 цифрового идентификатора ID для сетевого узла 210,

– применение 530, по меньшей мере, первой хеш–функции 147 и второй хеш–функции 148 к цифровому идентификатору, причем первая и вторая хеш–функции отображают цифровой идентификатор в первую открытую точку 141; H1(ID) и вторую открытую точку 142; H1(ID) на первой эллиптической кривой 131 и второй эллиптической кривой 132, причем первая эллиптическая кривая отличается от второй эллиптической кривой, причем первая и вторая открытые точки составляют часть материала 145 открытых ключей для сетевого узла 210,

– применение 540 первой и второй секретных изогений 135 к первой и второй открытым точкам 141, 142 эллиптической кривой, за счет этого получая первую закрытую точку 151 эллиптической кривой и вторую закрытую точку 152 эллиптической кривой, составляющие часть материала 155 закрытых ключей для сетевого узла 210, и

– конфигурирование 550 сетевого узла с закрытой точкой эллиптической кривой по интерфейсу связи.

Фиг. 6 схематично показывает пример варианта осуществления способа 600 согласования ключей. Способ 600 устанавливает совместно используемый ключ между двумя сетевыми узлами, такими как первый сетевой узел 210 и вторая сеть; или первый сетевой узел 215 и второй сетевой узел 216. Способ 600 содержит:

– сохранение 610 цифрового идентификатора 234; ID, для первого сетевого узла и/или первую и вторую открытые точки эллиптической кривой, причем первая и вторая открытые точки эллиптической кривой находятся на первой и второй эллиптических кривых, и

– причем первая закрытая точка 251 эллиптической кривой и вторая закрытая точка 252 эллиптической кривой соответствуют первой открытой точке 241 эллиптической кривой и второй открытой точке 242 эллиптической кривой через первую и вторую секретные изогении 135, причем первая открытая точка 241 эллиптической кривой и вторая открытая точка 242 эллиптической кривой соответствуют цифровому идентификатору 234 сетевого узла 210 через первую и вторую хеш–функции 147, 148, причем первая и вторая закрытые точки эллиптической кривой вычисляются посредством устройства 110 предварительного распределения ключей,

– получение 620 открытой точки эллиптической кривой $H_2(ID_2)$ для второго сетевого узла, причем открытая точка эллиптической кривой находится на первой из первой и второй эллиптических кривых,

– выбор 630 закрытой точки эллиптической кривой из первой и второй закрытых точек эллиптической кривой, находящихся на второй из первой и второй эллиптических кривых, причем первая и вторая кривые отличаются,

– применение 640 билинейного отображения e к выбранной закрытой точке первого сетевого узла и полученной открытой точке эллиптической кривой второго сетевого узла или открытой точке эллиптической кривой второго сетевого узла, к которому применяется открытая изогения посредством первого узла,

– извлечение 650 криптографического ключа из результата билинейного отображения.

Специалистам в данной области техники должно быть очевидным, что возможно множество различных вариантов осуществления способов 500 и 500. Например, порядок этапов может варьироваться, либо некоторые этапы могут выполняться параллельно. Кроме того, между этапами могут вставляться другие этапы способа. Вставленные этапы могут представлять уточнения способа, к примеру, как описано в данном документе, либо могут быть не связаны со способом. Кроме того, данный этап может не заканчиваться полностью до того, как начинается следующий этап.

Способ согласно изобретению может осуществляться с использованием программного обеспечения, которое содержит инструкции для инструктирования процессорной системе осуществлять способ 500 или 600. Программное обеспечение может включать в себя только этапы, выполняемые посредством конкретного подобъекта системы. Программное обеспечение может сохраняться на подходящем носителе хранения данных, к примеру, на жестком диске, на дискете, в запоминающем устройстве, на оптическом диске и т.д. Программное обеспечение может отправляться в качестве сигнала проводным или беспроводным способом либо с использованием сети передачи данных, например, Интернета. Программное обеспечение может становиться доступным для скачивания и/или для удаленного использования на сервере. Способ согласно изобретению может осуществляться с использованием потока битов, выполненного с возможностью конфигурировать программируемую логику, например, программируемую пользователем вентильную матрицу (FPGA), с тем чтобы осуществлять способ.

Следует принимать во внимание, что изобретение также применимо к компьютерным программам, в частности, к компьютерным программам на носителе, приспособленном для осуществления изобретения на практике. Программа может иметь форму исходного кода, объектного кода, кода, промежуточного между исходным и объектным кодом, к примеру, частично компилированную форму, либо любую другую форму, подходящую для использования при реализации способа согласно изобретению. Вариант осуществления, связанный с компьютерным программным продуктом, содержит машиноисполняемые инструкции, соответствующие каждому из этапов обработки, по меньшей мере, одного из изложенных способов. Эти инструкции могут подразделяться на подпрограммы и/или сохраняться в одном или более файлов, которые могут быть связаны статически или динамически. Другой вариант осуществления, связанный с компьютерным программным продуктом, содержит машиноисполняемые инструкции, соответствующие каждому из средств, по меньшей мере, одной из изложенных систем и/или продуктов.

Фиг. 7a показывает машиночитаемый носитель 1000, имеющий записываемую часть 1010, содержащую компьютерную программу 1020, причем компьютерная программа

1020 содержит инструкции для инструктирования процессорной системе осуществлять способ предварительного распределения ключей или согласования ключей согласно варианту осуществления. Компьютерная программа 1020 может быть осуществлена на машиночитаемом носителе 1000 в качестве физических меток либо посредством намагничивания машиночитаемого носителя 1000. Тем не менее, также возможен любой другой подходящий вариант осуществления. Кроме того, следует принимать во внимание, что, хотя машиночитаемый носитель 1000 показан здесь в качестве оптического диска, машиночитаемый носитель 1000 может представлять собой любой подходящий машиночитаемый носитель, такой как жесткий диск, полупроводниковое запоминающее устройство, флэш–память и т.д., и может быть незаписываемым или записываемым. Компьютерная программа 1020 содержит инструкции для инструктирования процессорной системе осуществлять упомянутый способ предварительного распределения ключей или согласования ключей.

Фиг. 7b показывает схематичное представление процессорной системы 1140 согласно варианту осуществления. Процессорная система содержит одну или более интегральных схем 1110. Архитектура одной или более интегральных схем 1110 схематично показана на фиг. 7b. Схема 1110 содержит модуль 1120 обработки, например, CPU, для выполнения компьютерных программных компонентов, чтобы осуществлять способ согласно варианту осуществления и/или реализовывать его модули или блоки. Схема 1110 содержит запоминающее устройство 1122 для сохранения программного кода, данных и т.д. Часть запоминающего устройства 1122 может быть неперезаписываемой. Схема 1110 может содержать элемент 1126 связи, например, антенну, разъемы либо и то, и другое и т.п. Схема 1110 может содержать специализированную интегральную схему 1124 для выполнения части или всей обработки, заданной в способе. Процессор 1120, запоминающее устройство 1122, специализированная IC 1124 и элемент 1126 связи могут соединяться между собой через межкомпонентное соединение 1130, скажем, шину. Процессорная система 1110 может быть выполнена с возможностью контактной и/или бесконтактной связи, с использованием антенны и/или разъемов, соответственно.

Например, в варианте осуществления, устройство предварительного распределения ключей или устройство согласования ключей, например, сетевой узел, может содержать процессорную схему и запоминающую схему, причем процессор выполнен с возможностью выполнять программное обеспечение, сохраненное в запоминающей схеме. Например, процессорная схема может представлять собой процессор Intel Core i7, ARM Cortex–R8 и т.д. В варианте осуществления, процессорная схема может представлять собой ARM Cortex M0. Запоминающая схема может представлять собой ROM–схему или энергонезависимое запоминающее устройство, например, флэш–память. Запоминающая схема может представлять собой энергозависимое запоминающее устройство, например, запоминающее SRAM–устройство. Во втором случае, устройство может содержать энергонезависимый программный интерфейс, например, жесткий диск, сетевой интерфейс и т.д., выполненный с возможностью предоставления программного обеспечения.

Следует отметить, что вышеуказанные варианты осуществления иллюстрируют, а не ограничивают изобретение, и что специалисты в данной области техники должны иметь возможность разрабатывать множество альтернативных вариантов осуществления.

В формуле изобретения, все ссылки с номерами, помещенные в круглые скобки, не должны рассматриваться как ограничивающие формулу изобретения. Использование глагола "содержит" и его спряжений не исключает наличия элементов или этапов,

отличных от элементов или этапов, изложенных в формуле изобретения. Упоминание элемента в единственном числе не исключает наличия множества таких элементов. Изобретение может реализовываться посредством аппаратных средств, содержащих несколько отдельных элементов, и посредством надлежащим образом запрограммированного компьютера. В пункте формулы изобретения на устройство, перечисляющем несколько средств, некоторые из этих средств могут быть осуществлены посредством идентичного элемента аппаратных средств. Простой факт того, что определенные меры упомянуты в различных зависимых пунктах формулы изобретения, не означает того, что комбинация этих мер не может использоваться с выгодой.

В формуле изобретения, ссылки в круглых скобках означают ссылки с номерами на чертежах примерных вариантов осуществления либо формулы вариантов осуществления, за счет этого повышая понятность формулы изобретения. Эти ссылки не должны истолковываться как ограничивающие формулу изобретения.

(57) Формула изобретения

1. Электронное устройство (110) предварительного распределения ключей для конфигурирования множества сетевых узлов (210, 211) информацией локальных ключей, причем устройство предварительного распределения ключей содержит:

устройство (130) хранения данных, содержащее информацию (135), представляющую первую секретную изогению (ϕ; s) для первой эллиптической кривой (131; E_1) и вторую секретную изогению (ϕ'; s) для второй эллиптической кривой (132; E_2), причем изогения приспособлена принимать точку на эллиптической кривой и формировать точку на эллиптической кривой в качестве вывода,

процессорную схему, выполненную с возможностью:

– получать цифровой идентификатор (*ID*) для сетевого узла (210),

– применять по меньшей мере первую хеш–функцию (147) и вторую хеш–функцию (148) к цифровому идентификатору, причем первая и вторая хеш–функции отображают цифровой идентификатор в первую открытую точку (141; $H_1(ID)$) и вторую открытую точку (142; $H_2(ID)$) на первой эллиптической кривой (131) и второй эллиптической кривой (132), при этом первая эллиптическая кривая отличается от второй эллиптической кривой, причем первая и вторая открытые точки составляют часть материала (145) общедоступных ключей для сетевого узла (210),

– применять первую и вторую секретные изогении (135) к первой и второй открытым точкам (141, 142) эллиптической кривой, за счет этого получая первую закрытую точку (151) эллиптической кривой и вторую закрытую точку (152) эллиптической кривой, составляющие часть материала (155) конфиденциальных ключей для сетевого узла (210), и

интерфейс (120) связи, выполненный с возможностью конфигурировать сетевой узел с первой и второй закрытыми точками эллиптической кривой.

2. Устройство предварительного распределения ключей по п.1, при этом первая и вторая открытые точки находятся на разных из первой и второй эллиптических кривых, причем первая и вторая закрытые точки находятся на разных из первой и второй эллиптических кривых.

3. Устройство предварительного распределения ключей по п.1 или 2, при этом первая изогения (162) представляет собой отображение из первой эллиптической кривой (131, E_1) во вторую эллиптическую кривую (132, E_2), причем вторая изогения (163) является двойственной относительно первой изогении, при этом первая открытая точка

представляет собой точку на первой эллиптической кривой, причем первая закрытая точка представляет собой точку на второй эллиптической кривой, при этом вторая открытая точка представляет собой точку на второй эллиптической кривой, причем вторая закрытая точка представляет собой точку на первой эллиптической кривой.

4. Устройство предварительного распределения ключей по любому из предшествующих пунктов, при этом первая и вторая эллиптические кривые задаются посредством разных формул.

5. Устройство предварительного распределения ключей по п.1, при этом первая и вторая секретные изогении (164; 165, 166) обеспечивают отображение из эллиптической кривой в саму себя, первая и вторая секретные изогении содержат скалярное умножение по эллиптической кривой входной точки (P) на эллиптической кривой с секретным целым числом (s;s_1,s_2), причем упомянутая информация представляет секретные изогении, содержащие секретное целое число.

6. Первый электронный сетевой узел (210; 215), сконфигурированный для протокола согласования ключей со вторым сетевым узлом (211), содержащий:

устройство хранения данных, содержащее цифровой идентификатор (234; *ID*) для первого сетевого узла и/или первую и вторую открытые точки эллиптической кривой, причем первая и вторая открытые точки эллиптической кривой находятся на первой и второй эллиптических кривых, при этом первая закрытая точка (251) эллиптической кривой и вторая закрытая точка (252) эллиптической кривой соответствуют первой открытой точке (241) эллиптической кривой и второй открытой точке (242) эллиптической кривой через первую и вторую секретные изогении (135), причем первая открытая точка (241) эллиптической кривой и вторая открытая точка (242) эллиптической кривой соответствуют цифровому идентификатору (234) сетевого узла (210) через первую и вторую хеш–функции (147, 148), при этом первая и вторая закрытые точки эллиптической кривой вычисляются посредством устройства (110) предварительного распределения ключей,

процессорную схему, выполненную с возможностью:

– получать открытую точку эллиптической кривой ($H_2(ID_R)$) для второго сетевого узла, причем открытая точка эллиптической кривой находится на первой одной из первой и второй эллиптических кривых,

– выбирать закрытую точку эллиптической кривой из первой и второй закрытых точек эллиптической кривой, находящихся на второй одной из первой и второй эллиптических кривых, причем упомянутые первая одна и вторая одна из кривых отличаются,

– применять билинейное отображение (e) к выбранной закрытой точке первого сетевого узла и полученной открытой точке эллиптической кривой второго сетевого узла или открытой точке эллиптической кривой второго сетевого узла, к которой первым узлом применена открытая изогения,

– извлекать криптографический ключ из результата билинейного отображения.

7. Первый электронный сетевой узел по п.6, в котором процессорная схема выполнена с возможностью:

– получать для второго сетевого узла открытую точку эллиптической кривой на первой эллиптической кривой ($H_1(ID)$) или открытую точку эллиптической кривой на второй эллиптической кривой ($H_2(ID)$),

– применять билинейное отображение (e) к:

открытой точке эллиптической кривой на первой эллиптической кривой ($H_1(ID)$) для

второго сетевого узла и второй закрытой точке эллиптической кривой на первой эллиптической кривой, или к

открытой точке эллиптической кривой на второй эллиптической кривой ($H_1(ID)$) для второго сетевого узла и первой закрытой точке эллиптической кривой на второй эллиптической кривой.

8. Первый электронный сетевой узел по п.6, при этом первая открытая точка и первые закрытые точки находятся на первой эллиптической кривой, и вторая открытая точка и вторые закрытые точки находятся на второй эллиптической кривой, причем процессорная схема выполнена с возможностью применять открытую изогению к открытой точке эллиптической кривой до применения билинейного отображения (e), при этом упомянутая открытая изогения обеспечивает отображение из первой эллиптической кривой во вторую эллиптическую кривую или из второй эллиптической кривой в первую эллиптическую кривую.

9. Первый электронный сетевой узел по любому из пп.6–8, в котором процессорная схема выполнена с возможностью:

– вычислять данные подтверждения правильности ключей из криптографического ключа, чтобы обеспечивать второму узлу возможность верифицировать то, что первый сетевой узел корректно вычислил криптографический ключ, и/или

– принимать данные подтверждения правильности ключей для криптографического ключа из второго узла и верифицировать данные подтверждения правильности ключей, чтобы верифицировать то, что второй сетевой узел корректно вычислил криптографический ключ.

10. Первый электронный сетевой узел по любому из пп.6–9, в котором процессорная схема выполнена с возможностью шифровать цифровое сообщение с помощью криптографического ключа и отправлять зашифрованное сообщение во второй узел и/или дешифровать зашифрованное сообщение с помощью криптографического ключа, который принимается из второго узла.

11. Электронный способ 500 предварительного распределения ключей, конфигурирующий множество сетевых узлов (210, 211) информацией локальных ключей, при этом способ предварительного распределения ключей содержит этапы, на которых:

сохраняют (510) информацию (135), представляющую первую секретную изогению (ϕ; s) для первой эллиптической кривой (131; E_1) и вторую секретную изогению (ϕ'; s) для второй эллиптической кривой (132; E_2), причем изогения приспособлена принимать точку на эллиптической кривой и формировать точку на эллиптической кривой в качестве вывода,

получают (520) цифровой идентификатор (ID) для сетевого узла (210),

применяют (530) по меньшей мере первую хеш–функцию (147) и вторую хеш–функцию (148) к цифровому идентификатору, причем первая и вторая хеш–функции отображают цифровой идентификатор в первую открытую точку (141; $H_1(ID)$) и вторую открытую точку (142; $H_2(ID)$) на первой эллиптической кривой (131) и второй эллиптической кривой (132), при этом первая эллиптическая кривая отличается от второй эллиптической кривой, причем первая и вторая открытые точки составляют часть материала (145) общедоступных ключей для сетевого узла (210),

применяют (540) первую и вторую секретные изогении (135) к первой и второй открытым точкам (141, 142) эллиптической кривой, за счет этого получая первую закрытую точку (151) эллиптической кривой и вторую закрытую точку (152) эллиптической кривой, составляющие часть материала (155) конфиденциальных ключей

для сетевого узла (210), и

конфигурируют (550) сетевой узел с закрытой точкой эллиптической кривой по интерфейсу связи.

12. Электронный способ (600) установления совместно используемого ключа между первым сетевым узлом (210; 215) и вторым сетевым узлом (211; 216), содержащий этапы, на которых:

сохраняют (610) цифровой идентификатор (234; ID) для первого сетевого узла и/или первую и вторую открытые точки эллиптической кривой, причем первая и вторая открытые точки эллиптической кривой находятся на первой и второй эллиптических кривых, и первую закрытую точку (251) эллиптической кривой и вторую закрытую точку (252) эллиптической кривой, соответствующие первой открытой точке (241) эллиптической кривой и второй открытой точке (242) эллиптической кривой через первую и вторую секретные изогении (135), причем первая открытая точка (241) эллиптической кривой и вторая открытая точка (242) эллиптической кривой соответствуют цифровому идентификатору (234) сетевого узла (210) через первую и вторую хеш–функции (147, 148), при этом первая и вторая закрытые точки эллиптической кривой вычисляются посредством устройства (110) предварительного распределения ключей,

получают (620) открытую точку эллиптической кривой ($H_2(ID_R)$) для второго сетевого узла, причем открытая точка эллиптической кривой находится на первой одной из первой и второй эллиптических кривых,

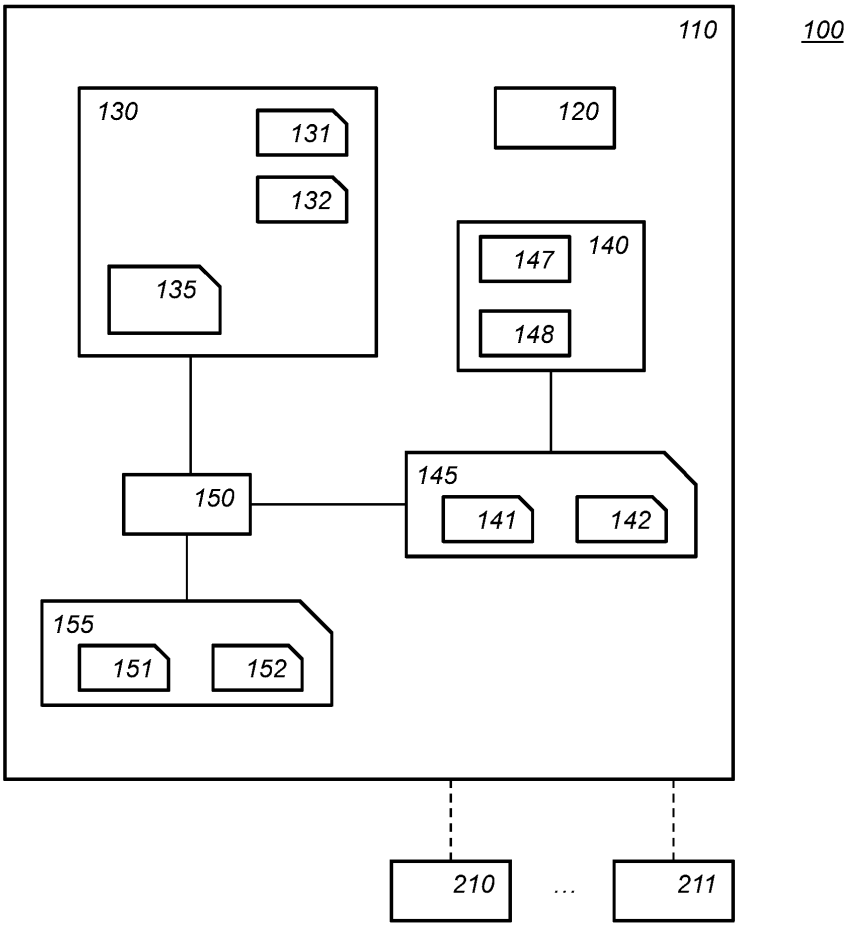
выбирают (630) закрытую точку эллиптической кривой из первой и второй закрытых точек эллиптической кривой, находящихся на второй одной из первой и второй эллиптических кривых, причем упомянутые первая одна и вторая одна из кривых отличаются,

применяют (640) билинейное отображение (e) к выбранной закрытой точке первого сетевого узла и полученной открытой точке эллиптической кривой второго сетевого узла или открытой точке эллиптической кривой второго сетевого узла, к которой первым узлом применена открытая изогения,

извлекают (650) криптографический ключ из результата билинейного отображения.

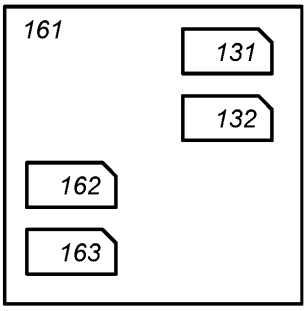
13. Машиночитаемый носитель (1000), содержащий долговременные или краткосрочные данные (1020), представляющие инструкции для предписания процессорной системе осуществлять способ по п.11 или 12.

1

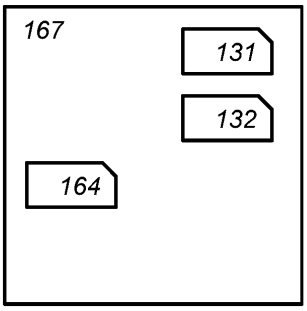

110
100
130
131
132
135
120
140
147
148
145
141
142
150
155
151
152
210
...
211

ФИГ. 1

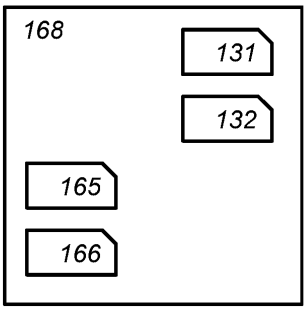
2



ФИГ. 2a

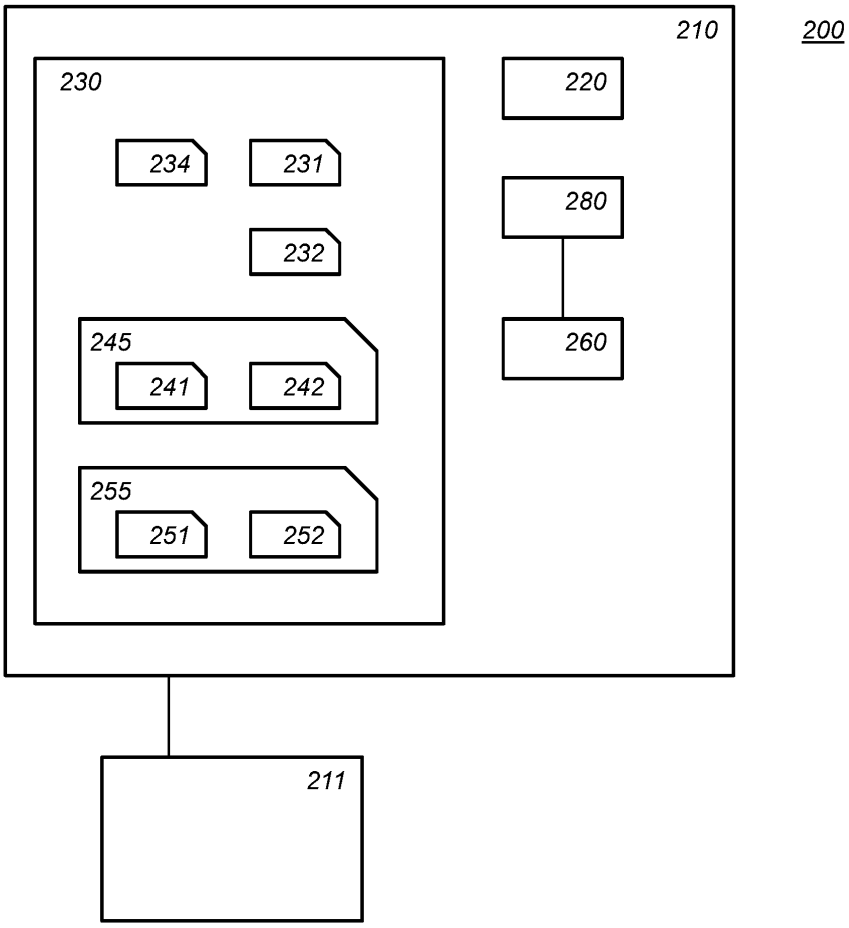


ФИГ. 2b



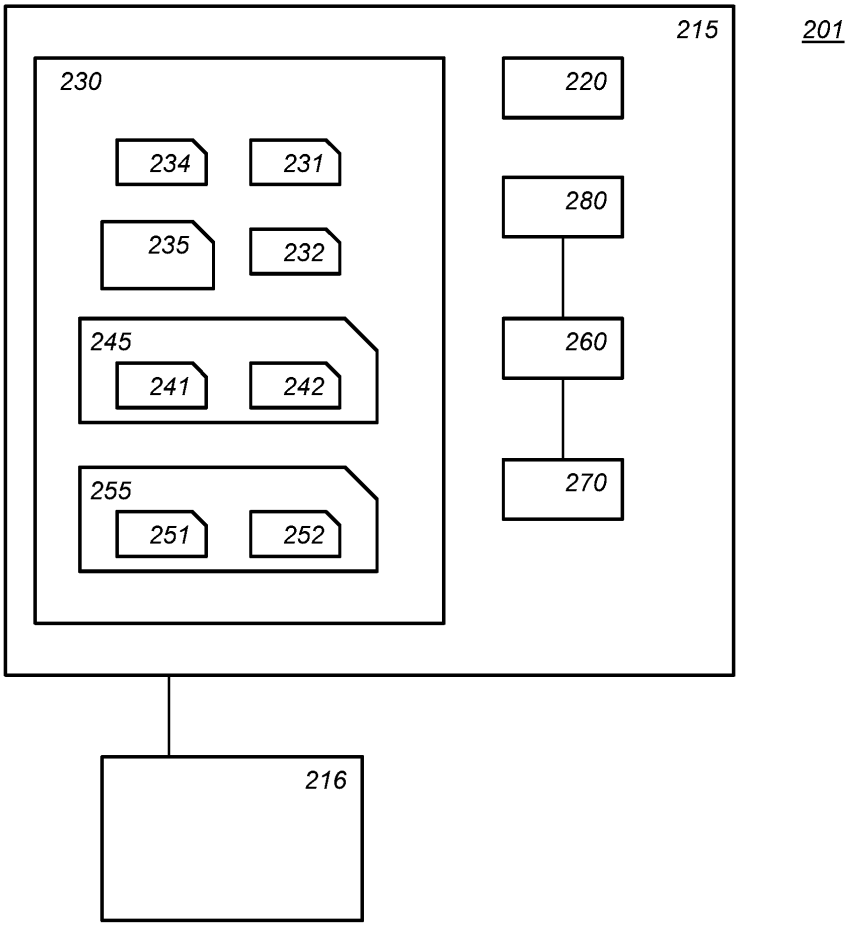
ФИГ. 2c

3

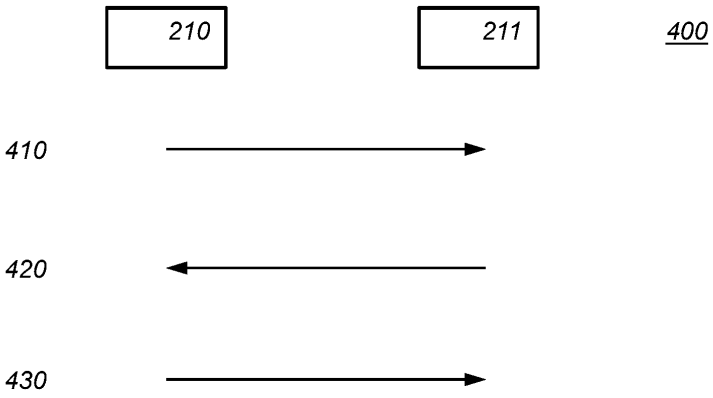


ФИГ. 3а

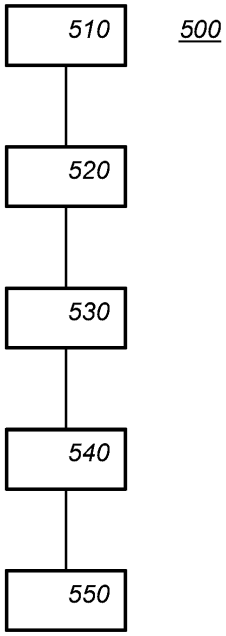
4


215
201
230
220
234
231
280
235
232
245
260
241
242
255
270
251
252
216

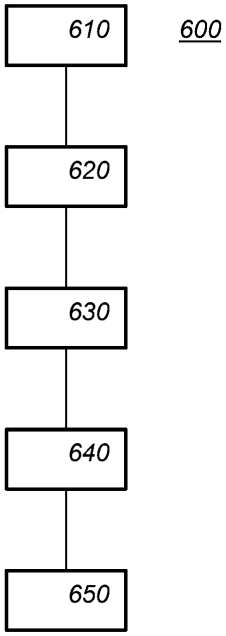
ФИГ. 3b



ФИГ. 4

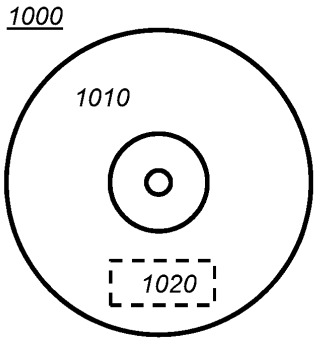


ФИГ. 5

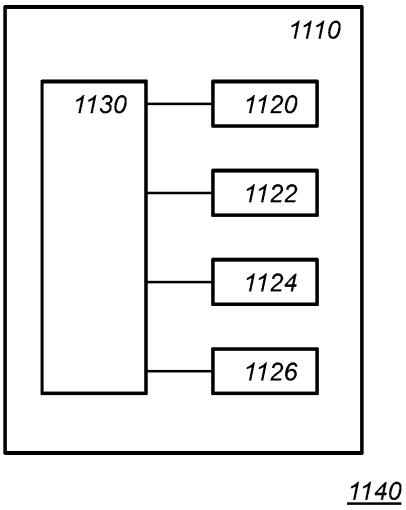


ФИГ. 6

7



ФИГ. 7a



ФИГ. 7b