РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2015 129 778**(13) **A**

(51) МПК
H04L 9/08 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ЗАЯВКА НА ИЗОБРЕТЕНИЕ

(21)(22) Заявка: **2015129778, 20.12.2013**

Приоритет(ы):
(30) Конвенционный приоритет:
21.12.2012 EP 12198794.5;
21.12.2012 US 61/740,488

(43) Дата публикации заявки: **27.01.2017** Бюл. № 03

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **21.07.2015**

(86) Заявка PCT:
EP 2013/077842 (20.12.2013)

(87) Публикация заявки PCT:
WO 2014/096420 (26.06.2014)

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

(71) Заявитель(и):
КОНИНКЛЕЙКЕ ФИЛИПС Н.В. (NL)

(72) Автор(ы):
ГОМЕС Доминго (NL),
ГАРСИЯ МОРЧОН Оскар (NL),
ТОЛХЭЙЗЕН Людовикус Маринус Герардус Мария (NL),
ГУТЬЕРРЕС Хайме (NL)

(54) ИСПОЛЬЗУЮЩЕЕ ОБЩИЙ КЛЮЧ СЕТЕВОЕ УСТРОЙСТВО И ЕГО КОНФИГУРИРОВАНИЕ

(57) Формула изобретения

1. Способ конфигурирования сетевого устройства для использования общего ключа, содержащий этапы, на которых:

- получают в электронной форме по меньшей мере два набора параметров, каждый набор параметров содержит частный модуль, публичный модуль и двумерный полином, имеющий целые коэффициенты, бинарное представление публичного модуля и бинарное представление частного модуля являются одинаковыми в имеющих по меньшей мере длину ключа последовательных разрядах,

- генерируют материал локального ключа для сетевого устройства, что содержит этапы, на которых

- получают в электронной форме идентификационный номер для сетевого устройства и

- для каждого набора параметров получают соответствующий одномерный полином посредством определения, используя устройство манипулирования полиномом, одномерного полинома из двумерного полинома набора параметров посредством подстановки идентификационного номера в упомянутый двумерный полином и приведения результата подстановки по модулю частного модуля набора параметров, и

- электронным образом сохраняют на сетевом устройстве сгенерированный материал локального ключа, содержащий публичный модуль упомянутого каждого набора

RU 2015129778 A

RU 2015129778 A

параметров и соответствующий одномерный полином упомянутого каждого набора параметров.

2. Способ по п. 1, в котором генерирование материала локального ключа для сетевого устройства содержит этапы, на которых для по меньшей мере двух из по меньшей мере двух наборов параметров

- генерируют ненулевой запутывающий полином, соответствующий упомянутому набору параметров,

- прибавляют (440), используя устройство для манипулирования полиномом, ненулевой запутывающий полином к одномерному полиному, который соответствует упомянутому набору параметров, чтобы получить запутанный одномерный полином,

- при этом сгенерированный материал локального ключа содержит запутанный одномерный полином.

3. Способ по п. 2, в котором каждый коэффициент суммы запутывающих полиномов кратен 2 в степени длины ключа.

4. Способ по п. 2, в котором каждый коэффициент суммы запутывающих полиномов, разделенный на степень двойки, округленный вниз до целого числа, кратен 2 в степени длины ключа.

5. Способ по п. 1, в котором все двумерные полиномы во всех наборах параметров являются симметричными полиномами.

6. Способ по п. 1, в котором, во всех наборах параметров одинаковые, имеющие по меньшей мере длину ключа последовательные разряды бинарного представления публичного модуля соответствующего набора параметров такие же, как и самые младшие имеющие длину ключа разряды частного модуля соответствующего набора параметров.

7. Способ по п. 6, в котором имеющие по меньшей мере длину ключа последовательные разряды являются самыми младшими имеющими длину ключа разрядами.

8. Способ по п. 1, содержащий этапы, на которых:

- генерируют частный модуль, используя электронный генератор случайных чисел, или

- генерируют двумерный полином, используя электронный генератор случайных чисел, посредством генерирования одного или более случайных коэффициентов для двумерного полинома.

9. Способ по п. 1, в котором один или все публичные модули удовлетворяют $2^{(a+2)}{}^{b-1} \leq N$, где N представляет публичный модуль, а представляет степень двумерного полинома, a b представляет длину ключа.

10. Способ по п. 1, в котором по меньшей мере два набора параметров содержат множество частных модулей и множество двумерных полиномов, имеющих коэффициенты по модулю, таких, что имеется набор имеющих длину ключа последовательных позиций, в которых бинарное представление публичного модуля согласуется с бинарным представлением всех частных модулей, и способ дополнительно содержит определение одномерного полинома, которое содержит подстановку идентификационного номера в каждый из множества двумерных полиномов, приведение по модулю частного модуля из множества частных модулей, соответствующих одному симметричному двумерному полиному, и сложение множества результатов множества приведений.

11. Способ по п. 1, в котором запутывающее число генерируется так, что

$|\epsilon^{A}_{i,k}| < 2^{(a+2-k)b-2}$, где $\in A, i$ обозначает запутывающее число, i обозначает степень

RU 2015129778 A

RU 2015129778 A

одночлена, соответствующего коэффициенту, а представляет степень двумерного полинома и b представляет длину ключа.

12. Способ определения общего ключа для первого сетевого устройства, причем ключ является криптографическим ключом, и способ содержит этапы, на которых

- получают материал локального ключа для первого сетевого устройства в электронной форме, материал локального ключа содержит по меньшей мере два одномерных полинома и соответствующие публичные модули,

- получают идентификационный номер для второго сетевого устройства, причем второе сетевое устройство отлично от первого сетевого устройства,

- для каждого из по меньшей мере двух одномерных полиномов подставляют (530) идентификационный номер второго сетевого устройства в упомянутый одномерный полином и приводят результат подстановки по модулю публичного модуля, соответствующего упомянутому одномерному полиному, и

- суммируют результаты приведений по модулю публичного модуля и приводят по модулю ключевого модуля, и

- получают общий ключ из результата приведения по модулю ключевого модуля.

13. Способ по п. 12, содержащий этапы, на которых

- определяют, получили ли первое сетевое устройство и второе сетевое устройство одинаковый общий ключ или нет, и если нет, получают дополнительный общий ключ из результата приведения по модулю ключевого модуля.

14. Способ по п. 12, содержащий деление результата подстановки по модулю публичного модуля на делитель строки нулевого разряда, который является степенью двойки, при этом делитель строки нулевого разряда больше чем 1, и округление вниз результата деления до целого числа.

15. Сетевое устройство, сконфигурированное, чтобы определять общий ключ, являющийся криптографическим ключом, причем сетевое устройство содержит

- узел получения материала локального ключа, сконфигурированный, чтобы получать материал локального ключа для сетевого устройства в электронной форме, материал локального ключа содержит по меньшей мере два одномерных полинома и соответствующие публичные модули,

- приемник, сконфигурированный, чтобы получать идентификационный номер для другого дополнительного сетевого устройства,

- устройство манипулирования полиномом, сконфигурированное, чтобы, для каждого из по меньшей мере двух одномерных полиномов, подставлять идентификационный номер второго сетевого устройства в упомянутый одномерный полином, приводить результат подстановки по модулю публичного модуля, соответствующего упомянутому одномерному полиному, и суммировать результаты приведений по модулю публичного модуля и приводить по модулю ключевого модуля, и

- устройство получения ключа, сконфигурированное, чтобы получать общий ключ из результата приведения по модулю ключевого модуля.

16. Система для конфигурирования сетевого устройства для использования общего ключа, содержащая

- узел получения материала ключа для получения в электронной форме по меньшей мере двух наборов параметров, набор параметров, содержащий частный модуль, публичный модуль и двумерный полином, имеющий целые коэффициенты, бинарное представление публичного модуля и бинарное представление частного модуля являются одинаковыми в имеющих по меньшей мере длину ключа последовательных разрядах,

- генератор для генерирования материала локального ключа для сетевого устройства, генератор, содержащий

- узел управления сетевым устройством для получения в электронной форме

RU 2015129778 A

RU 2015129778 A

идентификационного номера для сетевого устройства и для электронного сохранения сгенерированного материала локального ключа на сетевом устройстве,

- устройство манипулирования полиномом, сконфигурированное для получения для каждого набора параметров соответствующего одномерного полинома посредством определения одномерного полинома из двумерного полинома набора параметров посредством подстановки идентификационного номера в упомянутый двумерный полином и приведения результата подстановки по модулю частного модуля набора параметров.

17. Невременный машиночитаемый носитель данных, содержащий программу, содержащую команды для предписания процессору выполнять способ конфигурирования сетевого устройства для использования общего ключа, содержащий этапы, на которых:

- получают в электронной форме по меньшей мере два набора параметров, каждый набор параметров содержит частный модуль, публичный модуль и двумерный полином, имеющий целые коэффициенты, бинарное представление публичного модуля и бинарное представление частного модуля являются одинаковыми в имеющих по меньшей мере длину ключа последовательных разрядах,

- генерируют материал локального ключа для сетевого устройства, что содержит этапы, на которых

- получают в электронной форме идентификационный номер для сетевого устройства, и

- для каждого набора параметров получают соответствующий одномерный полином посредством определения, используя устройство манипулирования полиномом, одномерного полинома из двумерного полинома набора параметров посредством подстановки идентификационного номера в упомянутый двумерный полином и приведения результата подстановки по модулю частного модуля набора параметров, и

- электронным образом сохраняют на сетевом устройстве сгенерированный материал локального ключа, содержащий публичный модуль упомянутого каждого набора параметров и соответствующий одномерный полином упомянутого каждого набора параметров.

RU 2015129778 A

RU 2015129778 A