(19) **RU** (11) **2 236 760** (13) **C2**

(51) МПК[7] **H 04 L 9/32, G 07 F 7/12**

РОССИЙСКОЕ АГЕНТСТВО
ПО ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ РОССИЙСКОЙ ФЕДЕРАЦИИ

(21), (22) Заявка: 2002123875/09, 26.01.2001

(24) Дата начала действия патента: 26.01.2001

(30) Приоритет: 08.02.2000 EP 00102634.3

(43) Дата публикации заявки: 27.01.2004

(46) Дата публикации: 20.09.2004

(56) Ссылки: EP 0440158 A1, 07.08.1991. GB 2144564 A, 06.03.1985. RU 2040117 C1, 20.07.1995. RU 2126170 C1, 10.02.1999. EP 0782115 A, 02.07.1997.

(85) Дата перевода заявки PCT на национальную фазу: 09.09.2002

(86) Заявка PCT:
DE 01/00335 (26.01.2001)

(87) Публикация PCT:
WO 01/59728 (16.08.2001)

(98) Адрес для переписки:
129010, Москва, ул. Б. Спасская, 25, стр.3, ООО "Юридическая фирма Городисский и Партнеры", пат.пов. Ю.Д.Кузнецову, рег.№ 595

(72) Изобретатель: ХЕСС Эрвин (DE), ПОКРАНДТ Вольфганг (DE)

(73) Патентообладатель:
ИНФИНЕОН ТЕКНОЛОДЖИЗ АГ (DE)

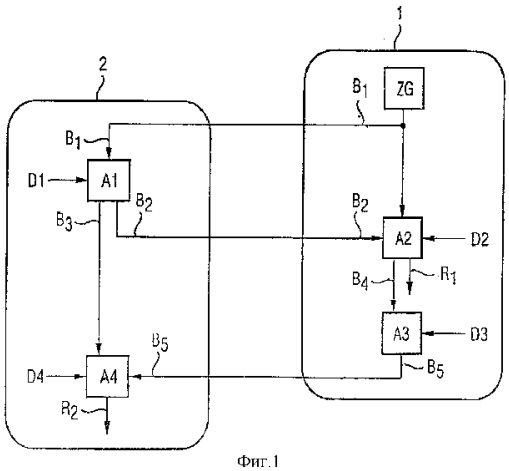
(74) Патентный поверенный:
Кузнецов Юрий Дмитриевич

RU 2236760 C2

(54) СПОСОБ И УСТРОЙСТВО ДЛЯ ВЗАИМНОЙ АУТЕНТИФИКАЦИИ ДВУХ БЛОКОВ ОБРАБОТКИ ДАННЫХ

(57)

Изобретение относится к устройствам для взаимной аутентификации двух блоков обработки данных. Техническим результатом является упрощение взаимной аутентификации двух блоков обработки данных. Для этого первый запрос от первого блока обработки данных пересылается ко второму блоку обработки данных, который передает назад ответ, при этом второй ответ вырабатывается первым блоком обработки данных и пересылается ко второму блоку обработки данных. 2 с. и 7 з.п. ф-лы, 2 ил.



Фиг.1

RU 2236760 C2

(19) **RU** (11) **2 236 760** (13) **C2**

(51) Int. Cl.[7] **H 04 L 9/32, G 07 F 7/12**

RUSSIAN AGENCY
FOR PATENTS AND TRADEMARKS

(12) ABSTRACT OF INVENTION

(21), (22) Application: 2002123875/09, 26.01.2001

(24) Effective date for property rights: 26.01.2001

(30) Priority: 08.02.2000 EP 00102634.3

(43) Application published: 27.01.2004

(46) Date of publication: 20.09.2004

(85) Commencement of national phase: 09.09.2002

(86) PCT application:
DE 01/00335 (26.01.2001)

(87) PCT publication:
WO 01/59728 (16.08.2001)

(98) Mail address:
129010, Moskva, ul. B. Spasskaja, 25, str.3,
OOO "Juridicheskaja firma Gorodisskij i
Partnery", pat.pov. Ju.D.Kuznetsovu, reg.№ 595

(72) Inventor: KhESS Ehrvin (DE),
POKRANDT Vol'fgang (DE)

(73) Proprietor:
INFINEON TEKNOLODZhIZ AG (DE)

(74) Representative:
Kuznetsov Jurij Dmitrievich

(54) METHOD AND APPARATUS FOR AUTHENTICATION OF TWO BLOCKS OF PROCESSED DATA

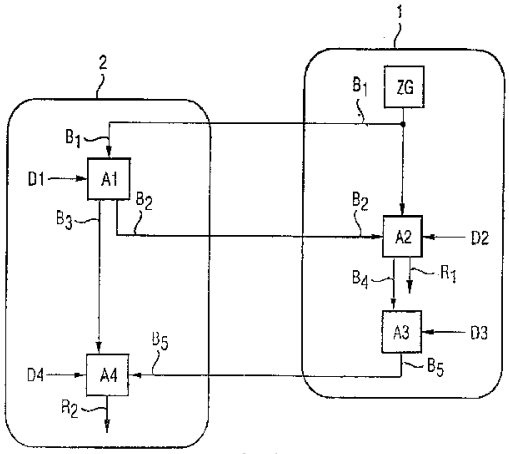
(57) Abstract:

FIELD: systems for authentication of two data blocks.

SUBSTANCE: first demand of first unit for data processing is transmitted to second unit for data processing which sends back response. Second response is formed by means of first unit for data processing and said response is transmitted to second unit for data processing.

EFFECT: simplified authentication system of two blocks of processed data.

9 cl, 2 dwg



Фиг.1

RU 2236760 C2

RU 2236760 C2

Настоящее изобретение относится к способу и устройству для взаимной аутентификации двух блоков обработки данных по процедуре запроса-ответа.

Аутентификация блоков обработки данных приобрела большое экономическое значение в связи с применением электронной передачи данных, электронной подписи, чип-карт, таких как телефонные карты и платежные карты. Аутентификация блоков обработки данных имеет большое значение в тех случаях, когда только правомочным пользователям или блокам обработки данных разрешено считывать данные или модифицировать их.

Известные способы для аутентификации блоков обработки данных основываются на процедурах запроса-ответа, базирующихся на криптографических процедурах, таких как DES (Стандарт шифрования данных), RSA (алгоритм цифровой подписи Райвеста-Шамира-Адлемана) или так называемые методы с нулевым знанием Fiat Schamir, Guillou Quisquater или Schnorr.

Общим для процедур запроса-ответа является то, что вырабатывается случайное число (запрос), которое пересылается на проверяемый блок обработки данных. Проверяемый блок обработки данных вырабатывает из него с помощью соответствующего криптографического способа ответное число (ответ), которое пересылается обратно в проверяющий блок обработки данных. С помощью запроса и ответа проверяющий блок обработки данных проверяет аутентичность проверяемого блока обработки данных.

При взаимной аутентификации процедура запроса-ответа проводится дважды, причем при втором ее проведении проверяющий и проверяемый блоки обработки данных меняются ролями, так что каждый блок обработки данных проверяет другой блок.

Задачей настоящего изобретения является создание упрощенного способа взаимной аутентификации двух блоков обработки данных. Кроме того, задачей изобретения является создание устройства, посредством которого может быть осуществлен вышеупомянутый способ.

В соответствии с изобретением поставленная задача решается в способе взаимной аутентификации первого блока обработки данных и второго блока обработки данных, включающем следующие этапы: выработка первой битовой последовательности в первом блоке обработки данных, передача первой битовой последовательности во второй блок обработки данных; выработка второй битовой последовательности и третьей битовой последовательности из первой битовой последовательности и первых данных посредством первого алгоритма во втором блоке обработки данных; передача второй битовой последовательности в первый блок обработки данных; выработка первого результата аутентификации и четвертой битовой последовательности из первой битовой последовательности, второй битовой последовательности и вторых данных посредством второго алгоритма в первом блоке обработки данных; выработка пятой битовой последовательности из четвертой битовой последовательности и третьих данных посредством третьего алгоритма в первом блоке обработки данных; передача пятой битовой последовательности к второму блоку обработки данных; выработка второго результата аутентификации из третьей битовой последовательности, пятой битовой последовательности и четвертых данных посредством четвертого алгоритма во втором блоке обработки данных.

Преимущество соответствующего изобретению способа состоит в том, что первая битовая последовательность применяется для аутентификации второго устройства обработки данных первым устройством обработки данных и для вычисления третьей и четвертой битовых последовательностей. Посредством заявленного способа становится возможным предусмотреть второй блок обработки данных без генератора случайных чисел. За счет экономии затрат на генератор случайных чисел второй блок обработки данных выполняется существенно более компактно, проще и, следовательно, экономичнее. Это является, например, решающим, когда при применении в условиях массового рынка карт с микросхемами необходимо использовать надежный способ аутентификации. Экономия на одном генераторе случайных чисел означает огромное упрощение блока обработки данных, так как к генератору случайных чисел предъявляются очень высокие требования, связанные со случайностью генерируемых чисел и нечувствительностью по отношению к внешним манипуляциям. Несмотря на это весьма значительное упрощение, могут применяться криптографические способы, зарекомендовавшие себя как надежные, такие как DES, RSA или методы с нулевым знанием, причем эти способы сохраняют свою надежность. Тем самым соответствующий изобретению способ достигает уровня тех же стандартов защищенности, которые обеспечиваются способами, известными из предшествующего уровня техники.

Предпочтительный вариант осуществления соответствующего изобретению способа предусматривает, что третья битовая последовательность передается от второго блока обработки данных к первому блоку обработки данных и используется во втором алгоритме, чтобы выработать первый результат аутентификации и/или четвертую битовую последовательность. За счет такого выполнения может использоваться более широкое разнообразие способов вычислений во втором алгоритме, что может упростить второй алгоритм.

Кроме того, является предпочтительным, что третья битовая последовательность является промежуточным результатом расчета второй битовой последовательности. За счет такого выполнения в первом алгоритме можно избежать дополнительных вычислительных затрат, так что выполнение первого алгоритма может быть реализовано с большей скоростью.

Еще один предпочтительный вариант выполнения способа предусматривает, что первая битовая последовательность вырабатывается случайным образом. Выработка случайной первой битовой последовательности повышает надежность способа.

RU 2236760 C2

RU 2236760 C2

Предпочтительным является то, что первая битовая последовательность выбирается таким образом, что она отличается от всех ранее применявшихся первых битовых последовательностей. Тем самым гарантируется, что потенциальный взломщик не сможет спрогнозировать ни первую битовую последовательность, ни вычисленную из нее вторую битовую последовательность. Благодаря этому повышается надежность способа.

Устройство для осуществления соответствующего изобретению способа содержит первый блок обработки данных и второй блок обработки данных, причем в первом блоке обработки данных размещен формирователь битовой последовательности для выработки первой битовой последовательности, а во втором блоке обработки данных размещен первый блок обработки битовой последовательности, предназначенный для выработки второй битовой последовательности и третьей битовой последовательности из первой битовой последовательности и первых данных, при этом в первом блоке обработки данных предусмотрен второй блок обработки битовой последовательности для выработки первого результата аутентификации и четвертой битовой последовательности из первой битовой последовательности, второй битовой последовательности и вторых данных; кроме того, в первом блоке обработки данных размещен третий блок обработки битовой последовательности для выработки пятой битовой последовательности, при этом во втором блоке обработки данных размещен четвертый блок обработки битовой последовательности для выработки второго результата аутентификации из третьей битовой последовательности, пятой битовой последовательности и четвертых данных.

Блоки обработки данных могут быть выполнены, например, в виде компьютера, компактного портативного компьютера, миниатюрного портативного компьютера, карманного компьютера, ручного компьютера, чип-карты, телефонной карты, карты медицинского страхования и т.д., которые могут прямо или косвенно осуществлять связь с другим блоком обработки данных.

В предпочтительном варианте осуществления соответствующего изобретению устройства по меньшей мере один из блоков обработки данных выполнен в виде интегральной схемы. Тем самым может быть реализован блок обработки данных, характеризуемый высокой компактностью, малыми габаритами и хорошей воспроизводимостью.

В еще одном варианте осуществления один из блоков обработки данных выполнен мобильным. Тем самым обеспечивается простая транспортировка блока обработки данных.

Кроме того, предпочтительным является то, что один из блоков обработки данных содержит сдвиговый регистр, который связан обратной связью по меньшей мере с одной логической схемой ИСКЛЮЧАЮЩЕЕ ИЛИ. Логическая схема ИСКЛЮЧАЮЩЕЕ ИЛИ выполнена в виде одного конструктивного элемента, называемого вентилем. Благодаря такому выполнению обеспечивается создание очень малогабаритного криптографически защищенного блока обработки данных. Сдвиговый регистр при этом представляет собой часть блока, в которой реализуется один из четырех алгоритмов.

В еще одном варианте осуществления предусматривается, что один блок обработки данных выполнен в виде чип-карты, а другой блок обработки данных представляет собой терминал для чип-карт.

Другие варианты осуществления настоящего изобретения охарактеризованы в зависимых пунктах.

Примеры осуществления настоящего изобретения представлены на чертежах и рассматриваются ниже более подробно.

На чертежах представлено следующее:

Фиг.1 - первый соответствующий изобретению способ взаимной аутентификации двух блоков обработки данных;

Фиг.2 - другой соответствующий изобретению способ взаимной аутентификации двух блоков обработки данных.

На фиг.1 представлена система, содержащая первый блок 1 обработки данных и второй блок 2 обработки данных. Кроме того, показана диаграмма потока, в соответствии с которой некоторые этапы способа выполняются в первом блоке 1 обработки данных, а другие этапы обработки данных - в блоке 2 обработки данных. Способ начинается с выработки первой битовой последовательности B_1, которая в первом блоке 1 обработки данных в данном варианте осуществления вырабатывается с помощью генератора ZG случайных чисел. Первая битовая последовательность B_1 передается от первого блока 1 обработки данных к второму блоку 2 обработки данных, и во втором блоке 2 обработки данных с помощью алгоритма A1 вырабатываются вторая битовая последовательность B_2 и третья битовая последовательность B_3 из первой битовой последовательности B_1 и первых данных D1.

В случае алгоритма речь может идти об одном из известных из предшествующего уровня техники алгоритмов, таких как DES, RSA. В случае данных D1 речь идет, например, о секретном ключе и/или о других данных, необходимых для вычисления второй битовой последовательности B_2 и/или третьей битовой последовательности B_3.

Затем вторая битовая последовательность B_2 передается от второго блока 2 обработки данных к первому блоку 1 обработки данных. В первом блоке 1 обработки данных вырабатываются первый результат аутентификации R1 как результат аутентификации второго блока 2 обработки данных первым блоком 1 обработки данных и четвертая битовая последовательность с помощью второго алгоритма A2 из первой битовой последовательности B_1, второй битовой последовательности и вторых данных D2. Второй алгоритм A2 выбирается в соответствии с применяемым алгоритмом шифрования (DES, RSA и т.д.), причем он согласован с первым алгоритмом A1. При этом данные D2 включают в себя, например, секретный ключ или секретный первичный ключ, из которого может рассчитываться секретный ключ. В случае RSA речь идет,

RU 2236760 C2

RU 2236760 C2

например, о ключе индивидуального пользования и/или о ключе открытого пользования.

В первом блоке 1 обработки данных вырабатывается пятая битовая последовательность B_5 с использованием третьего алгоритма A3 из четвертой битовой последовательности B_4 и третьих данных D3.

Пятая битовая последовательность B_5 передается от первого блока 1 обработки данных ко второму блоку 2 обработки данных.

Во втором блоке 2 обработки данных вырабатывается второй результат аутентификации R2 как результат аутентификации первого блока 1 обработки данных посредством второго блока 2 обработки данных с использованием четвертого алгоритма из третьей битовой последовательности B_3, пятой битовой последовательности B_5 и четвертых данных D4.

В качестве алгоритмов A3 и A4 могут использоваться, например, известные из уровня техники алгоритмы (DES, RSA и т.д.). В качестве данных D3, D4 могут использоваться, например, секретные ключи. Алгоритм A1 может, например, совпадать с алгоритмом A3.

Если оба результата аутентификации положительны, то это означает, что первый блок 1 обработки данных и второй блок 2 обработки данных аутентифицировали друг друга. В качестве алгоритмов A1, A2, A3 и A4 могут использоваться, например, криптографические способы. В качестве данных D1, D2, D3 и D4 могут использоваться, например, ключи индивидуального или открытого использования, с помощью которых модифицируются битовые последовательности B_1, B_2, B_3 и B_4. Преимущество этого способа состоит в том, что во втором блоке 2 обработки данных нет необходимости использовать генератор случайных чисел. Дополнительное преимущество данного способа заключается в том, что между первым блоком 1 обработки данных и вторым блоком 2 обработки данных требуется только три передачи данных. В известных способах требовалось четыре передачи данных.

На фиг.2 представлен другой вариант осуществления соответствующего изобретению способа взаимной аутентификации двух блоков обработки данных. Способ аутентификации, иллюстрируемый на фиг.2, отличается от показанного на фиг.1 способа аутентификации передачей третьей битовой последовательности B_3 от второго блока 2 обработки данных к первому блоку 1 обработки данных. Еще одно различие по отношению к способу, представленному на фиг.1, состоит в том, что третья битовая последовательность B_3 применяется во втором алгоритме A2, чтобы выработать четвертую битовую последовательность и/или первый результат аутентификации R1. Остальные этапы способа выполняются аналогично тому, как описано выше со ссылками на фиг.1.

Формула изобретения:

1. Способ взаимной аутентификации первого блока обработки данных (1) и второго блока обработки данных (2), включающий следующие этапы: выработка первой битовой последовательности (B1) в первом блоке обработки данных (1), передача первой битовой последовательности (B1) во второй блок обработки данных (2), выработка второй битовой последовательности (B2) и третьей битовой последовательности (B3) из первой битовой последовательности (B1) и первых данных (D1) посредством первого алгоритма шифрования (A1) во втором блоке обработки данных (2), передача второй битовой последовательности (B2) в первый блок обработки данных (1); выработка первого результата аутентификации (A1) и четвертой битовой последовательности (B4) из первой битовой последовательности (B1), второй битовой последовательности (B2) и вторых данных (D2) посредством второго алгоритма шифрования (A2) в первом блоке обработки данных (1), выработка пятой битовой последовательности (B5) из четвертой битовой последовательности (B4) и третьих данных (D3) посредством третьего алгоритма шифрования (A3) в первом блоке обработки данных (1), передача пятой битовой последовательности (B5) к второму блоку обработки данных (2), выработка второго результата аутентификации (R2) из третьей битовой последовательности (B3), пятой битовой последовательности (B5) и четвертых данных (D4) посредством четвертого алгоритма шифрования (A4) во втором блоке обработки данных (2).

2. Способ по п.1, отличающийся тем, что третью битовую последовательность (B3) передают от второго блока обработки данных (2) к первому блоку обработки данных (1) и используют во втором алгоритме шифрования (A2), чтобы выработать первый результат аутентификации (R1) и/или четвертую битовую последовательность (B4).

3. Способ по п.1 или 2, отличающийся тем, что третья битовая последовательность (B3) является промежуточным результатом расчета второй битовой последовательности (B2).

4. Способ по любому из пп.1-3, отличающийся тем, что первую битовую последовательность (B1) вырабатывают случайным образом.

5. Способ по любому из пп.1-4, отличающийся тем, что первую битовую последовательность (B1) выбирают таким образом, чтобы она отличалась от всех ранее применявшихся первых битовых последовательностей (B1).

6. Устройство для осуществления способа по любому из пп.1-5, содержащее первый блок обработки данных (1) и второй блок обработки данных (2), причем в первом блоке обработки данных (1) размещен формирователь битовой последовательности (ZG) для выработки первой битовой последовательности (B1), во втором блоке обработки (2) данных размещен первый блок обработки битовой последовательности (A1), предназначенный для выработки второй битовой последовательности (B2) и третьей битовой последовательности (B3) из первой битовой последовательности (B1) и первых данных (D1), при этом в первом блоке обработки данных (1) предусмотрен второй блок обработки битовой последовательности (A2), предназначенный для выработки первого результата аутентификации (R1) и

RU 2236760 C2

RU 2236760 C2

четвертой битовой последовательности (B4) из первой битовой последовательности (B1), второй битовой последовательности (B2) и вторых данных (D2), кроме того, в первом блоке обработки данных (1) размещен третий блок обработки битовой последовательности (A3) для выработки пятой битовой последовательности (B5), при этом во втором блоке обработки данных (2) размещен четвертый блок обработки битовой последовательности (A4) для выработки второго результата аутентификации (R2) из третьей битовой последовательности (B3), пятой битовой последовательности (B5) и четвертых данных (D4).

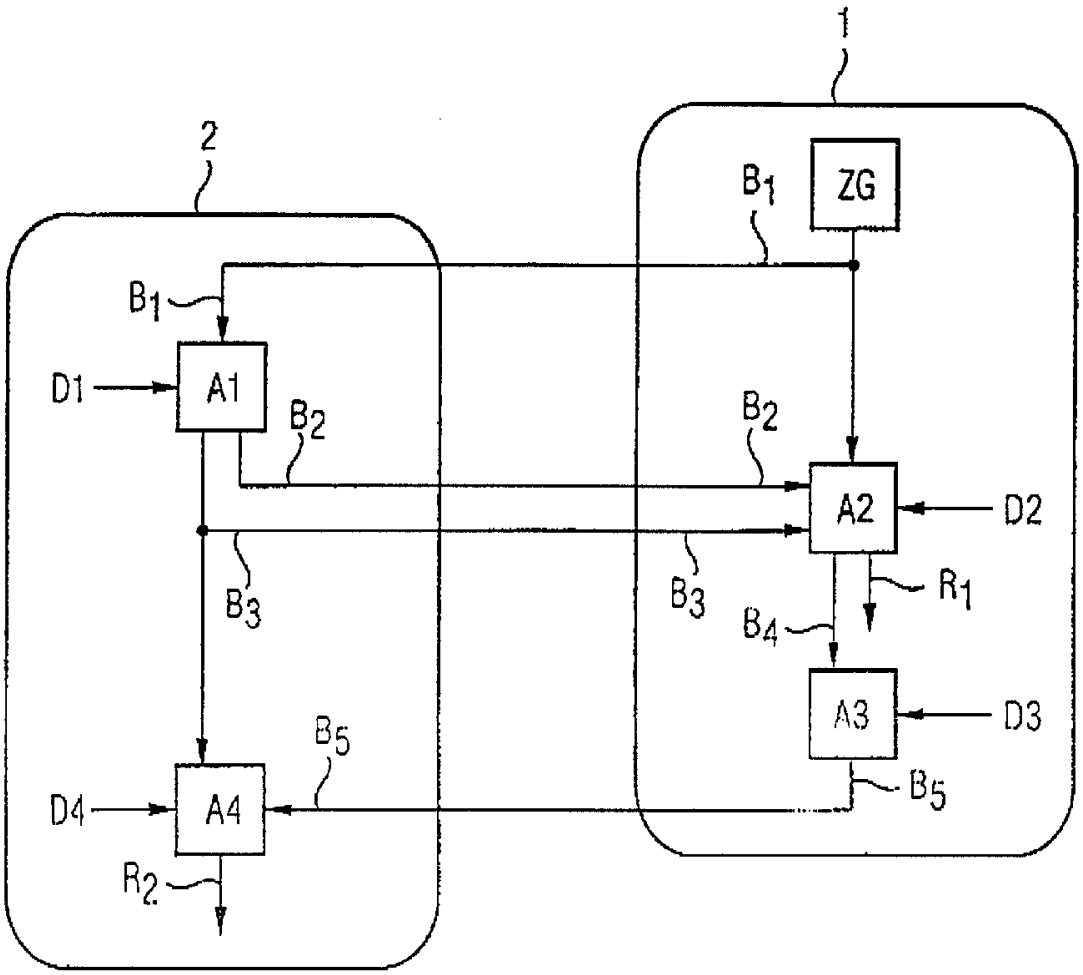
7. Устройство по п.6, отличающееся тем, что по меньшей мере один из блоков обработки данных (1) или (2) выполнен в виде интегральной схемы.

8. Устройство по п.6 или 7, отличающееся тем, что один из блоков обработки данных (1) или (2) содержит сдвиговый регистр, который связан обратной связью по меньшей мере с одной логической схемой исключающее ИЛИ.

9. Устройство по любому из пп.6-8, отличающееся тем, что один блок обработки данных выполнен в виде чип-карты, а другой блок обработки данных представляет собой терминал для чип-карт.

RU 2236760 C2

RU 2236760 C2



Фиг.2

RU 2236760 C2

RU 2236760 C2