(19) C2 (11) 72579 (13) UA

(98) вул.Пушкінська, 9, кв. 11, м.Київ, 01034
(85) 2002-09-08
(74) Пахаренко Олександр Володимирович, (UA)
(45) [2005-03-15]
(43) [2002-10-15]
(24) 2005-03-15
(22) 2001-01-26
(12) null
(21) 2002086590
(46) 2005-03-15

(86) 2001-01-26 PCT/DE01/00335
(30) 00102634.3 2000-02-08 EP
(54) СПОСІБ І ПРИСТРІЙ ДЛЯ ВЗАЄМНОЇ ІДЕНТИФІКАЦІЇ ДВОХ ПРИСТРОЇВ ОБРОБКИ ДАНИХ СПОСОБ И УСТРОЙСТВО ДЛЯ ВЗАИМНОЙ ИДЕНТИФИКАЦИИ ДВУХ УСТРОЙСТВ ОБРАБОТКИ ДАННЫХ METHOD AND DEVICE FOR MUTUAL AUTHENTICATION OF TWO DATA PROCESSING UNITS
(56) EP 0440158, 07.08.1991 2 GB 2144564, 06.03.1985 2 EP 0782115, 02.07.1997 2
(71)
(72) DE Хесс Ервін DE Хесс Ервін DE Хесс Ервін DE Поккрандт Вольфганг DE Поккрандт Вольфганг DE Поккрандт Вольфганг
(73) DE ІНФІНЕОН ТЕКНОЛОДЖІС АГ DE ИНФИНЕОН ТЕКНОЛОДЖИС АГ DE INFINEON TECHNOLOGIES AG

Настоящее изобретение относится к способу и устройству для взаимной идентификации двух устройств обработки данных. Обычно для взаимной идентификации двух устройств требуется последовательное выполнение двух отдельных процедур идентификации. Как правило, для этого используется проверка правильности ответа устройства на посылаемый запрос. Первый запрос передается из первого устройства 1 обработки данных во второе устройство 2, которое посылает первое ответное сообщение. В соответствии с изобретением, второе ответное сообщение формируется первым устройством 1 и передается во второе устройство 2.

Винахід стосується способу і пристрою для взаємної ідентифікації двох пристроїв обробки даних. Взаємна ідентифікація двох пристроїв обробки даних здійснюється звичайно двома кроками, що виконуються один за одним. Використовують звичайно метод "виклик-відгук". Для цього перший виклик від першого пристрою (1) обробки даних передають до другого пристрою (2) обробки даних, який відсилає назад перший відгук. Згідно з винаходом, перший пристрій (1) обробки даних формує другий відгук і передає його до другого пристрою (2) обробки даних.

The invention relates to a method and device for mutual authentication of two data processing units. The mutual authentication of two data processing units is normally carried out in two separate successive authentications. A challenge-response method is normally used. A first challenge is transmitted from a first data processing unit (1) to a second data processing unit (2) which sends back a first response. According to the invention, a second response is generated by the first data processing unit (1) and transmitted to the second data processing unit (2).

1. Спосіб взаємної ідентифікації першого пристрою (1) обробки даних і другого пристрою (2) обробки даних, який включає такі операції:
- формування першої біт-послідовності (B_1) у першому пристрої (1) обробки даних;
- передача першої біт-послідовності (B_1) до другого пристрою (2) обробки даних;
- формування другої біт-послідовності (B2) і третьої біт-послідовності (B_3) із першої біт-послідовності (B_1) і першого блока даних (D1) з використанням першого алгоритму (A1) у другому пристрої (2) обробки даних;
- передача другої біт-послідовності (B_2) до першого пристрою (1) обробки даних;
- формування першого результату (R_1) ідентифікації і четвертої біт-послідовності (B_4) із першої біт-послідовності (B_1), другої біт-послідовності (B_2) і другого блоку даних (D_2) з використанням другого алгоритму (A2) у першому пристрої (1) обробки даних;
- формування п'ятої біт-послідовності (B_5) із четвертої біт-послідовності (B_4) і третього блока даних (D_3) з використанням третього алгоритму (A3) у першому пристрої (1) обробки даних;
- передача п'ятої біт-послідовності (B5) до другого пристрою (2) обробки даних;
- формування другого результату ідентифікації (R_2) із третьої біт-послідовності (B3), п'ятої біт-послідовності (B_5) і четвертого блока даних (D_4) з використанням четвертого алгоритму (A4) в другому пристрої (2) обробки даних.
2. Спосіб за п. 1, який **відрізняється** тим, що третю біт-послідовність (B_3) від другого пристрою (2) обробки даних передають до першого пристрою (1) обробки даних і використовують другим алгоритмом (A2) для формування першого результату (R_1) ідентифікації і/або четвертої біт-послідовності (B_4).
3. Спосіб за п. 1 або 2, який **відрізняється** тим, що третя біт-послідовність (B_3) є проміжним результатом при обчисленні другої біт-послідовності (B_2).
4. Спосіб за будь-яким з пп. 1-3, який **відрізняється** тим, що першу біт-послідовність (B_1) формують випадковим чином.
5. Спосіб за будь-яким з пп. 1-4, який **відрізняється** тим, що першу біт-послідовність (B_1) вибирають таким чином, що вона відрізняється від усіх уже використаних перших біт-послідовностей (B1).
6. Пристрій для взаємної ідентифікації двох пристроїв обробки даних, який містить
- перший пристрій (1) обробки даних і
- другий пристрій (2) обробки даних,
- причому перший пристрій (1) обробки даних містить генератор (ZG) випадкових послідовностей для формування першої біт-послідовності (B_1),
- другий пристрій (2) обробки даних містить перший вузол (A1) обробки послідовностей, виконаний з можливістю формування другої біт-послідовності (B_2) і третьої біт-послідовності (B_3) із першої біт-послідовності (B_1) і першого блока даних (D_1),
- перший пристрій (1) обробки даних містить другий вузол (A2) обробки послідовностей, виконаний з можливістю формування першого результату (R1) ідентифікації і четвертої біт-послідовності (B_4) із першої біт-послідовності (B1), другої біт-послідовності і другого блока даних (D_2),
- перший пристрій (1) обробки даних містить третій вузол (A3) обробки послідовностей для формування п'ятої біт-послідовності (B_5),
- а другий пристрій (2) обробки даних містить четвертий вузол (A4) обробки послідовностей, виконаний з можливістю формування другого результату (R_2) ідентифікації із третьої біт-послідовності (B_3), п'ятої біт-послідовності (B_5) і четвертого блока даних (D_4).
7. Пристрій за п. 6, який **відрізняється** тим, що принаймні один із пристроїв (1) або (2) обробки даних виконаний у вигляді інтегральної мікросхеми.
8. Пристрій за п. 6 або 7, який **відрізняється** тим, що один із пристроїв (1) або (2) обробки даних містить зсувний регістр, охоплений зворотним зв'язком зі щонайменше одним логічним елементом "виключне АБО".
9. Пристрій за будь-яким з пп. 6-8, який **відрізняється** тим, що один пристрій обробки даних є чіп-карткою, а другий пристрій обробки даних є терміналом для чіп-карток.

Винахід стосується способу і пристрою для взаємної ідентифікації двох пристроїв обробки даних з використанням методу "виклик-відгук".

Ідентифікація пристроїв обробки даних у зв'язку з використанням систем електронної передачі даних, електронного підпису, чіп-карток, як, наприклад, телефонні картки і кредитні картки, набула великого економічного значення. Ідентифікація пристроїв обробки даних має велике значення, коли необхідно забезпечити, щоб зчитування чи модифікацію даних могли здійснювати лише вповноважені користувачі або пристрої обробки даних.

Відомі способи ідентифікації пристроїв обробки даних здійснюються з використанням методу "виклик-відгук" на основі криптографічних методів, таких як стандарт кодування даних (Data Encoding Standard, DES), метод Рівеста-Шаміра-Адельмана (Rivest-Shamer-Adelman, RSA) або так званий метод нульового знання (Zero-Knowledge) авторів Фіата Шаміра, Гіллоу Квісквотера або Шнорра (Fiat Schamir, Guillou Quisquarter, Schnorf.

Метод "виклик-відгук" передбачає формування випадкового числа (виклику) і передачу його на пристрій обробки даних, що підлягає перевірці. На його основі пристрій обробки даних, що підлягає перевірці, формує за допомогою певного криптографічного методу число-відповідь (відгук), яке передається на пристрій обробки даних, що здійснює перевірку. За допомогою виклику і відгуку пристрій обробки даних, що здійснює перевірку, перевіряє автентичність пристрою обробки даних.

При взаємній ідентифікації процедура виклик-відгук виконується двічі, причому при другому виконанні пристрій обробки даних, що здійснює перевірку, і пристрій обробки даних, що підлягає перевірці, міняються ролями, тобто кожен пристрій перевіряє інший пристрій.

Задача винаходу полягає в розробці спрощеного способу взаємної ідентифікації двох пристроїв обробки даних, додатково задачею винаходу є також розробка пристрою, який може здійснити спосіб.

Відповідно до винаходу поставлена задача вирішена у способі взаємної ідентифікації першого пристрою обробки даних і другого пристрою обробки даних, який включає такі операції:

формування першої біт-послідовності у першому пристрої обробки даних;

передача першої біт-послідовності до другого пристрою обробки даних;

формування другої біт-послідовності і третьої біт-послідовності із першої біт-послідовності і першого блоку даних з використанням першого алгоритму у другому пристрої обробки даних; передача другої біт-послідовності до першого пристрою обробки даних;

формування першого результату ідентифікації і четвертої біт-послідовності із першої біт-послідовності, другої біт-послідовності і другого блоку даних з використанням другого алгоритму у першому пристрої обробки даних;

формування п'ятої біт-послідовності із четвертої біт-послідовності і третього блоку даних з використанням третього алгоритму у першому пристрої обробки даних;

передача п'ятої біт-послідовності до другого пристрою обробки даних;

формування другого результату ідентифікації із третьої біт-послідовності, п'ятої біт-послідовності І четвертого блоку даних з використанням четвертого алгоритму в другому пристрої обробки даних.

Перевага відповідного винаходові способу полягає в тому, що перша біт-послідовність використовується першим пристроєм обробки даних для ідентифікації другого пристрою обробки даних, а також для обчислення третьої і четвертої біт-послідовностей. Завдяки цьому способу другий пристрій обробки даних може обходитися без генератора випадкових чисел. Завдяки економії на генераторі випадкових чисел другий пристрій обробки даних може бути виконаний значно компактнішим, простішим і тому дешевшим. Це може мати вирішальне значення, наприклад, в разі необхідності забезпечення надійної ідентифікації в такій масовій галузі ринку, як чіп-картки. Економія на генераторі випадкових чисел означає значне спрощення пристрою обробки даних, тому що до генератора випадкових чисел висуваються строгі вимоги стосовно випадковості і несприйнятливості щодо зовнішніх спроб маніпулювання. Незважаючи на значне спрощення, можуть бути використані і зберегти свою надійність криптографічні методи, що зарекомендували себе як надійні - такі як DES, RSA або ж Zero-Knowledg. Таким чином відповідний винаходові спосіб досягає такої ж надійності, як і способи згідно з рівнем техніки.

Вигідне вдосконалення відповідного винаходові способу передбачає, що третя біт-послідовність від другого пристрою обробки даних передається до першого пристрою обробки даних і використовується другим алгоритмом для формування першого результату ідентифікації і/або четвертої біт-послідовності. Завдяки цьому підходу у другому алгоритмі може бути використана більша кількість методів обчислення, що може спростити другий алгоритм. Крім того, вигідним є те, що третя біт-послідовність є проміжним результатом обчислення другої біт-послідовності. Завдяки цьому можна уникнути додаткових витрат у першому алгоритмі, тому виконання першого алгоритму може бути здійснене швидше.

Інше вигідне вдосконалення способу передбачає, що перша біт-послідовність формується випадковим чином. Формування випадкової першої біт-послідовності підвищує надійність способу.

Перевагу має те, що перша біт-послідовність вибирається таким чином, що вона відрізняється від усіх уже використаних перших послідовностей. Таким чином забезпечується, що зловмисник не зможе передбачити ні першої біт-послідовності, ні обрахованої на її основі другої біт-послідовності. Завдяки цьому підвищується надійність способу.

Пристрій для здійснення відповідного винаходові способу складається із першого пристрою обробки даних і другого пристрою обробки даних, причому перший пристрій обробки даних містить генератор випадкових послідовностей для формування першої біт-послідовності, причому другий пристрій обробки даних містить перший пристрій обробки послідовностей, виконаний з можливістю формування другої біт-послідовності і третьої біт-послідовності із першої біт-послідовності і першого блоку даних, причому перший пристрій обробки даних містить другий пристрій обробки послідовностей, виконаний з можливістю формування першого результату ідентифікації і четвертої біт-послідовності із першої біт-послідовності, другої біт-послідовності і другого блоку даних, причому перший пристрій обробки даних містить третій пристрій обробки послідовностей

для формування п'ятої біт-послідовності, причому другий пристрій обробки даних містить четвертий пристрій обробки послідовностей, виконаний з можливістю формування другого результату ідентифікації із третьої біт-послідовності, п'ятої біт-послідовності і четвертого блоку даних.

При цьому пристрої обробки даних можуть бути виконані у. вигляді комп'ютера, переносного комп'ютера, кишенькового комп'ютера, чіп-картки, кредитної картки, телефонної картки, лікарняної картки, і ряду інших виробів, які безпосередньо або опосередковано можуть бути з'єднані з іншим пристроєм обробки даних.

У вигідному прикладі виконання відповідного винаходові пристрою принаймні один із пристроїв обробки даних виконаний у вигляді інтегральної мікросхеми. В такому разі пристрій обробки даних є дуже компактним і придатним для масового виробництва.

В іншій вигідній формі виконання винаходу пристрій обробки даних є мобільним. Цим забезпечується просте його транспортування.

Крім того, доцільною є форма виконання винаходу, згідно з якою один із пристроїв обробки даних містить зсувний регістр, охоплений зворотним зв'язком зі щонайменше одним логічним елементом "виключне АБО". Завдяки цьому пристрою можливе створення компактного, криптографічно надійного пристрою обробки даних. При цьому зсувний регістр представляє частину функціонального вузла, в якому виконується один із чотирьох алгоритмів.

В іншій вигідній формі виконання винаходу один пристрій обробки даних є чіп-карткою, а другий пристрій обробки даних є терміналом для чіп-карток.

Інші ознаки винаходу наведені в додаткових пунктах формули винаходу.

Нижче приклади виконання винаходу детальніше пояснюються з використанням фігур. На них схематично зображено:

Фіг.1. перший відповідний винаходові спосіб взаємної ідентифікації двох пристроїв
обробки даних;

Фіг.2. другий відповідний винаходові спосіб взаємної ідентифікації двох пристроїв обробки даних.

На Фіг.1 зображена система, що складається із першого пристрою 1 обробки даних і другого пристрою 2 обробки даних. Кожен з пристроїв 1, 2 обробки даних представлений у вигляді блок-схеми, причому деякі операції способу здійснюються в першому пристрої 1 обробки даних, а інші операції обробки даних здійснюються у другому пристрої 2 обробки даних. Процес починається з формування першої біт-послідовності B1, яка в цьому прикладі виконання винаходу формується генератором ZG випадкових чисел першого пристрою 1 обробки даних. Перша біт-послідовність B1 від першого пристрою 1 обробки даних передається до другого пристрою 2 обробки даних і в ньому із першої біт-послідовності B1 і першого блоку даних D1 з використанням алгоритму A1 формуються друга біт-послідовність B2 і третя біт-послідовність B3.

Під алгоритмом мається на увазі один із відомих із рівня техніки алгоритмів - DES, RSA і т.п. Під блоком даних D1 мається на увазі, наприклад, секретний ключ і/або інші дані, необхідні для вирахування другої біт-послідовності B2 і третьої біт-послідовності B3.

Потім від другого пристрою 2 обробки даних на перший пристрій 1 обробки даних передається друга біт-послідовність B2. У першому пристрої 1 обробки даних формуються перший результат R1 ідентифікації як наслідок ідентифікації другого пристрою 2 обробки даних першим пристроєм 1 обробки даних і - з використанням алгоритму A2 - четверта біт-послідовність B4 на основі першої біт-послідовності B1, другої біт-послідовності B2 і другого блоку даних D2. Другий алгоритм A2 вибраний відповідно до використовуваного алгоритму кодування (DES, RSA і т.п.) і кореспондує з першим алгоритмом A1. При цьому блок даних D2 є, наприклад, секретний ключ або секретний майстер-ключ, з якого може бути вирахуваний секретний ключ. Під ключем мається на увазі, наприклад, особистий і/або відкритий ключ.

У першому пристрої 1 обробки даних з використанням третього алгоритму A3 із четвертої біт-послідовності B4 і третього блоку даних D3 формується п'ята біт-послідовність B5.

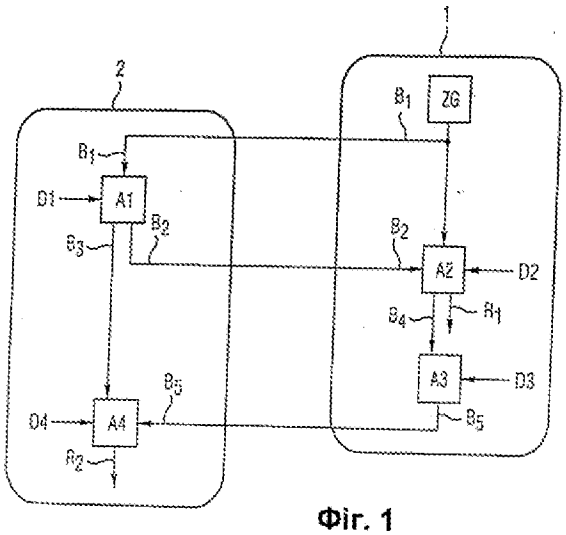
П'ята біт-послідовність B5 передається від першого пристрою 1 обробки даних до другого пристрою 2 обробки даних.

У другому пристрої 2 обробки даних як наслідок ідентифікації першого пристрою 1 обробки даних другим пристроєм 2 обробки даних з використанням четвертого алгоритму A4 із третьої біт-послідовності B3, п'ятої біт-послідовності B5 і четвертого блоку даних D4 формується другий результат R2 ідентифікації.

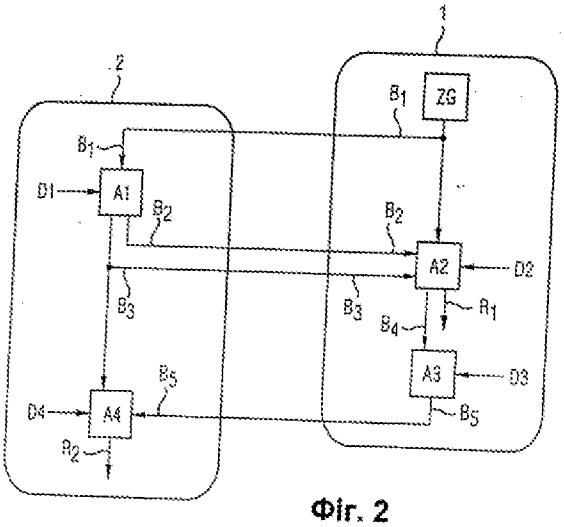
Алгоритми A3 і A4 можуть бути відомими із рівня техніки алгоритмами (DES, RSA і т.п.). Блоки даних D3 і D4 є, наприклад, секретними ключами. Алгоритм A1 можу, наприклад, співпадати з алгоритмом A3.

Якщо обидва результати ідентифікації співпадають, це означає, що перший пристрій 1 обробки даних і другий пристрій 2 обробки даних взаємно ідентифікувалися. В разі алгоритмів A1, A2, A3 і A4 йдеться, наприклад, про криптографічні методи. В разі блоків даних D1, D2, D3 і D4 йдеться, наприклад, про секретні або відкриті ключі, якими модифікуються біт-послідовності B1, B2, B3 і B4. Перевага цього способу полягає в тому, що відсутній генератор випадкових чисел у другому пристрої 2 обробки даних. Наступною перевагою цього способу є те, що для ідентифікації між першим пристроєм 1 обробки даних і другим пристроєм 2 обробки даних здійснюється лише три передачі даних. Зазвичай необхідні чотири операції передачі даних.

На Фіг.2 представлений другий приклад здійснення відповідного винаходові способу взаємної ідентифікації двох пристроїв обробки даних. Представлений на фіг. 2 спосіб ідентифікації відрізняється тим, що здійснюється передача третьої біт-послідовності B3 від другого пристрою 2 обробки даних до першого пристрою 1 обробки динах. Інша відмінність порівняно з Фіг.1 полягає в тому, що третя біт-послідовність B3 використовується у другому алгоритмі A2 для формування четвертої біт-послідовності і/або першого результату R1 ідентифікації. Решта операцій способу виконуються таким же чином, як описано стосовно Фіг.1.


1
2
ZG
A1
A2
A3
A4
D1
D2
D3
D4
B1
B2
B3
B4
B5
R1
R2

Фіг. 1


1
2
ZG
A1
A2
A3
A4
D1
D2
D3
D4
B1
B2
B3
B4
B5
R1
R2

Фіг. 2