



УКРАЇНА

(19) UA

(11) 55469

(13) C2

(51) 7 G06K19/07

МІНІСТЕРСТВО ОСВІТИ  
І НАУКИ УКРАЇНИДЕРЖАВНИЙ ДЕПАРТАМЕНТ  
ІНТЕЛЕКТУАЛЬНОЇ  
ВЛАСНОСТІОПИС  
ДО ПАТЕНТУ НА ВІНАХІД

## (54) СПОСІБ ПЕРЕВІРКИ АВТЕНТИЧНОСТІ НОСІЯ ДАНИХ

1

(21) 2000020649  
(22) 29 07 1998  
(24) 15 04 2003  
(86) PCT/DE98/02147, 29 07 1998  
(31) 197 34 507 7  
(32) 08 08 1997  
(33) DE  
(46) 15 04 2003, Бюл. № 4, 2003 р.  
(72) Зедлак Хольгер, DE, Брюкльмайр Франц-Йозеф, DE  
(73) ІНФІНЕОН ТЕКНОЛОДЖІС АГ, DE  
(56) EP 0112461, 1984  
EP 0583709, 1994  
GB 2211643, 1989  
(57) Спосіб перевірки автентичності носія даних (1), зокрема чіп-картки, що містить принаймні один пристрій (2) пам'яті, причому у цьому пристрої (2) пам'яті записаний специфічний фізичний параметр (X) носія даних (1) у закодованій формі ( $K_{s, s} [X]$ ), а параметр (X) закодований за допомогою першого таємного спеціального ключа ( $K_{s, s}$ ), причому у носії даних (1) додатково записані другий спеціальний загальнодоступний ключ ( $K_{s, p}$ ), що відповідає першому спеціальному таємному ключу ( $K_{s, s}$ ), а також закодований за допомогою

2

третього глобального таємного ключа ( $K_{g, s}$ ) другий ключ ( $K_{g, s} [K_{s, p}]$ ), який виконується за такими етапами

а) термінал зчитування/запису (3) зчитує другий ключ та закодовану форму другого ключа ( $K_{s, s} [X]$ ,  $K_{s, p}$ ,  $K_{g, s} [K_{s, p}]$ ) з носія даних і за допомогою записаного у терміналі (3) четвертого глобального загальнодоступного ключа ( $K_{g, p}$ ) обчислює другий ключ ( $K_{s, p} = K_{g, p} [K_{g, s} [K_{s, p}]]$ ) та порівнює його із зчитаним другим ключем,

б) якщо результат перевірки позитивний, виконуються етапи від с) до е), якщо негативний - процес припиняється,

с) термінал зчитування/запису (3) зчитує закодований параметр ( $K_{s, s} [X]$ ) з пристрою (2) пам'яті носія даних (1) і визначає фізичний параметр (X) шляхом вимірювання,

д) термінал зчитування/запису (3) за допомогою другого ключа ( $K_{s, p}$ ) обчислює параметр ( $X = K_{s, p} [K_{s, s} [X]]$ ) та порівнює його з виміряним параметром (X),

е) якщо результат позитивний, носій даних (1) визнається автентичним, якщо негативний - процес припиняється

Винахід стосується способу перевірки автентичності носія даних, зокрема чіп-картки, що має принаймні пристрій пам'яті, причому в цьому пристрої пам'яті у закодованій формі записаний специфічний фізичний параметр носія даних

Такий спосіб відомий з опису до Європейського патенту EP 0 112 461 A1. За цим способом, характеристики антени, інтегрованої в ідентифікаційну картку, у закодованій формі записані у картці і порівнюються з характеристиками, що вимірюються. Проте, при цьому процес порівняння здійснюється у картці, причому важливим секретом є алгоритм кодування.

Європейський патент EP 0 112 461 A1 залишає відкритим питання щодо того, де саме слід здійснювати порівняння та утворення числового коду у картці чи у терміналі. У першому

випадку виникає проблема, пов'язана з тим, що підроблена картка може завжди повідомляти позитивний результат порівняння незалежно від справжнього результату, так що справжня перевірка автентичності неможлива. В іншому випадку таємний алгоритм та таємний ключ мають бути записані також у вимірювальному терміналі, що представляє ризик несанкціонованого доступу до даних. Крім того, алгоритм і таємний ключ для всіх карток мають бути записані в усіх терміналах.

Європейський патент EP 0 583 709 A1 також описує спосіб перевірки автентичності, у якому фізичні характеристики, що підлягають вимірюванню, записуються у закодованій формі і пізніше порівнюються із тими, що підлягають вимірюванню після декодування. При цьому можна застосовувати також асиметричний спосіб кодування та декодування. Проте, при цьому

(13) C2

(11) 55469

(19) UA

виникає проблема, пов'язана з великими витратами на зберігання записаних даних та управлінські витрати у терміналі для численних загальнодоступних ключів для окремих носіїв даних однієї системи

Носії даних, які підлягають перевірці автентичності, найчастіше мають лічильник, показання якого відображають наявність грошових сум, тому ці носії є об'єктами спроб копіювання чи підроблення. Проте, застосування таких носіїв даних у системах контролю доступу або у галузі соціального страхування також може провокувати аналогічні спроби

Можна створити ідентичну копію напівпровідникового чіпа, навіть не розуміючи принцип побудови схеми, так що копія буде містити також усі таємні ключі і закодовані дані у вигляді закодованого фізичного параметра, тобто існує ризик несанкціонованого доступу до даних. Проте, проведення перевірки автентичності на підставі фізичного параметру, який для кожного носія даних є іншим і за можливістю складним, внаслідок чого процес копіювання значно ускладнюється, є лише першим кроком на шляху забезпечення високої надійності захисту від фальшування, оскільки, хоча зловмисник і може скопіювати конструкцію чіпа, але навряд чи - відповідну картку з потрібним фізичним параметром

У відомих способах у кожному терміналі мали би бути записані алгоритми кодування і декодування, а також кодове число, яке має бути секретним, або загальнодоступне кодове число, щоб або кодувати також і вимірювані дані та порівнювати закодовані форми, або декодувати дані, зчитані з картки у закодованій формі, і порівнювати з даними оригіналу. Проте, це пов'язано зі значним ризиком несанкціонованого доступу до даних, оскільки зловмисника спокушатиме можливість вкрати та проаналізувати термінал

Таким чином, в основу винаходу було покладено задачу створення способу перевірки автентичності носіїв даних, що забезпечував би високу надійність захисту даних і був би позбавлений вищезгаданих недоліків

Ця задача вирішується за допомогою способу згідно з п1 формули винаходу. Переважні варіанти реалізації винаходу наведені у залежних пунктах формули винаходу. У способі згідно з винаходом порівняння здійснюється у терміналі, причому немає необхідності у зберіганні таємного ключа в терміналі, оскільки застосовується асиметричне кодування. Асиметричне кодування означає, що для кодування використовується інший ключ, ніж для декодування, і навіть якщо відомий один з цих ключів, на його підставі неможливо обчислити інший. Ключ декодування може бути загальновідомим, і зазвичай його можна одержати з доступних кожному файлів - наприклад, з мережі Internet

При цьому загальнодоступний ключ підпорядкований певним власникам систем застосування карток, наприклад компаніям, що випускають кредитні картки, чи банкам. Важливою ознакою способу згідно з винаходом є те, що

таємний, відомий лише власнику ключ не можна обчислити на підставі загальнодоступного ключа. Прикладом способу асиметричного кодування є спосіб RSA

Якщо на термінал передається лише закодований параметр, необхідно, щоб у терміналі були записані загальнодоступні ключі усіх власників систем, або щоб для тих, хто бажає користуватись послугами цих терміналів, доступ до цих ключів забезпечувався, наприклад, через підключення до мережі Intranet. Щоб уникнути цього недоліку, у вдосконаленому варіанті реалізації винаходу на картку у закодованій формі записується загальнодоступний спеціальний ключ, причому для його кодування застосовувався таємний глобальний ключ. Цей таємний глобальний ключ відомий, наприклад, лише центральному банку або іншим владним структурам. Він застосовується для кодування будь-яких загальнодоступних спеціальних ключів. Крім того, на картку записується незакодований загальнодоступний спеціальний ключ

Отже, у терміналі зберігається лише загальнодоступний глобальний ключ, що відповідає таємному глобальному ключу, за допомогою якого декодується закодована форма загальнодоступного спеціального ключа і порівнюється з оригінальним ключем, який також записаний у пам'ять. У тому разі, коли результат порівняння виявляється позитивним, це свідчить про те, що для кодування загальнодоступного спеціального ключа був застосований належний таємний глобальний ключ, і означає підтвердження, наприклад, центрального банку, який таким чином ручається, що загальнодоступний спеціальний ключ є автентичним і його можна застосувати для декодування фізичного параметру

Як фізичний параметр для ідентифікації безконтактних носіїв даних можна використовувати характеристику антени, наприклад добротність, або комбінацію аналогічних характеристик. Інші варіанти використання фізичних характеристик наведені в описах до європейських патентів EP 0 676 073 B1 та EP 0 602 643 A2. У цих патентах пропонується використовувати як характерний для картки фізичний параметр регульований резистивний контур або характеристики комірки EEPROM

Суть винаходу пояснюється далі на прикладі реалізації за допомогою креслення. На кресленні показано схему чіп-картки та терміналу зчитування/запису, а також алгоритм способу згідно з винаходом

На кресленні показано чіп-картку 1, що містить пристрій 2 пам'яті, який може бути реалізований на підставі напівпровідникового чіпа, а також фізичний параметр X

Незалежно від наведеної схеми чіп-картки, винахід у жодному разі не обмежений виключно такою структурою, його можна застосовувати для будь-яких типів носіїв даних

У пристрої 2 пам'яті записана принаймні форма  $K_{s_s}[X]$  параметра  $X$ , закодована за допомогою першого таємного спеціального ключа  $K_{s_s}$ . Як показано за допомогою зазначеної

штриховою лінією збільшеної площі пристрою 2 пам'яті, у вдосконаленому варіанті реалізації винаходу у ньому, крім того, може бути записаний другий загальнодоступний спеціальний ключ  $K_{sp}$ , а також цей другий ключ у закодованій формі  $K_{gs}$  [ $K_{sp}$ ]. Для кодування другого ключа  $K_{sp}$  був використаний третій таємний глобальний ключ  $K_{gs}$ .

На кресленні термінал 3 відділений від чіп-картки 1 вертикальною штриховою лінією. Цей термінал містить приймальний відсік 4 для чіп-картки 1, а також клавіатуру 5 та дисплей 6. Крім того, у терміналі передбачений пристрій пам'яті 7, у якому принаймні тимчасово записаний другий загальнодоступний спеціальний ключ  $K_{sp}$ . Цей ключ може бути або постійно записаний у терміналі 3, або можна також під час кожного сеансу перевірки автентичності одержувати його за запитом від центральної станції або з мережі передачі даних через лінію передачі даних. Оскільки другий ключ  $K_{sp}$  є спеціальним ключем, підпорядкованим певному власнику системи, наприклад, фірмі, що працює з кредитними картками, проте, має існувати можливість використання терміналу 3 для роботи з картками власників різних систем, тому довелося б зберігати записані у пристрої пам'яті різні загальнодоступні спеціальні ключі. Замість цього, як пропонується в іншому варіанті реалізації винаходу, можна записати у пам'ять і зберігати четвертий загальнодоступний глобальний ключ  $K_{gp}$ , тобто розширити пристрій 7 пам'яті, як показано на кресленні штриховою лінією.

Як чіп-картка 1, так і термінал 3 можуть містити інші пристрої, наприклад мікро- чи криптопроцесори. Передача від чіп-картки 1 до терміналу 3 може здійснюватись як контактним, так і безконтактним способом, наприклад, з використанням індуктивного зв'язку. Крім того, у терміналі 3 передбачений вимірювальний пристрій для визначення фізичного параметру  $X$  чіп-картки 1. Усі ці деталі не показані на кресленні, оскільки вони на сучасному рівні розвитку техніки вже добре відомі, тому їх не треба детально описувати у винаході.

На кресленні під зображенням чіп-картки 1 та терміналу 3 показаний алгоритм процесу згідно з винаходом. Між горизонтальними штриховими лініями наведений варіант реалізації винаходу,

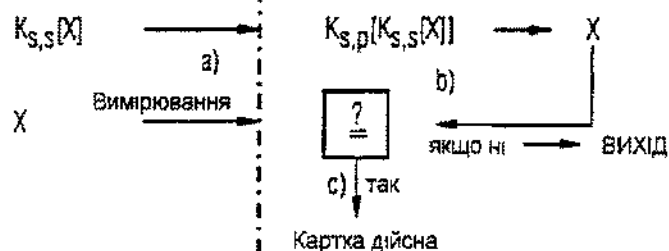
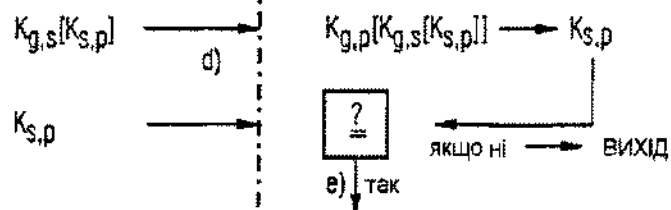
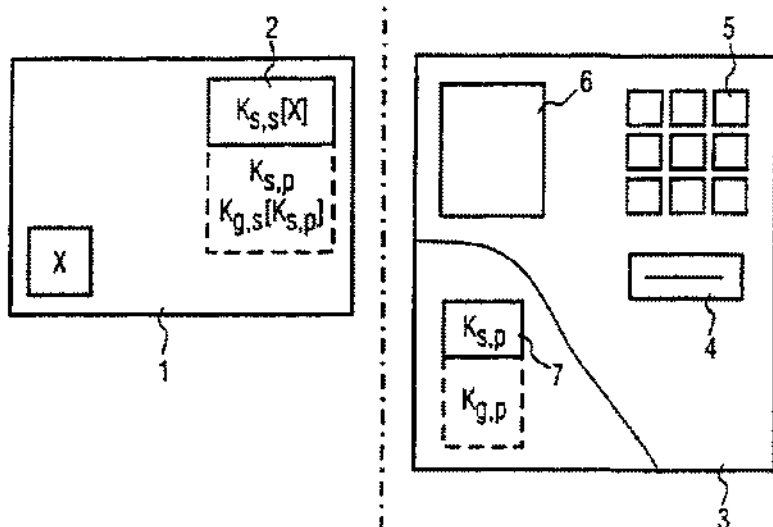
коли у терміналі 3 зберігається лише один загальнодоступний глобальний ключ. У цьому разі на етапі d) загальнодоступний спеціальний ключ у закодованій формі, а також власне цей загальнодоступний спеціальний ключ передаються з чіп-картки 1 на термінал 3, у терміналі 3 на підставі загальнодоступного глобального ключа обчислюється загальнодоступний спеціальний ключ і на етапі e) порівнюється з переданим загальнодоступним спеціальним ключем. Якщо результат порівняння виявиться негативним, процес припиняється.

Якщо результат порівняння виявиться позитивним, на етапі a) фізичний параметр у закодованій формі передається від чіп-картки 1 на термінал 3, а також у терміналі 3 вимірюється власне цей фізичний параметр. Потім у терміналі за допомогою переданого раніше і визнаного правильним загальнодоступного спеціального ключа  $K_{sp}$  декодується закодований фізичний параметр і порівнюється з виміряним.

Якщо результат порівняння виявляється позитивним, картка на етапі c) визнається автентичною. Якщо результат негативний, процес припиняється.

При застосуванні способу згідно з винаходом у чіп-картці 1 мають бути записані лише закодовані форми параметра  $X$  та загальнодоступного спеціального ключа, а також власне цей загальнодоступний спеціальний ключ. Немає потреби у тому, щоб таємний спеціальний і таємний глобальний ключі були записані у чіп-картці 1, вони мають бути відомі лише власнику системи або установі, що видає сертифікати. Оскільки таємні ключі все рівно однозначно підпорядковані відповідним загальнодоступним ключам, неможливо підробити картку, у якій були б записані належні закодовані форми даних, потрібних для перевірки автентичності.

Злочинне викрадення та аналіз терміналу 3 не призводять до бажаного успіху, оскільки у ньому також записані лише загальнодоступні ключі, тобто такі, що можна одержати також іншим способом. Як у носії даних, так і у терміналі можуть зберігатись таємні спеціальні та таємний глобальний ключі, хоча це не потрібно, проте це призвело б до втрати надійності захисту інформації.



Фіг.