

Винахід стосується способу аутентифікації щонайменше одного абонента при обміні даними між щонайменше двома абонентами, згідно з яким першому абоненту від другого абонента передається перша інформація, перший абонент цю першу інформацію за допомогою певного алгоритму перетворює у другу інформацію і відправляє другому абоненту, а другий абонент перевіряє другу інформацію на її правильність.

Такі методи відомі зі статті Ханнса-Петера Кьоніга "Способи криптографічної ідентифікації для "інтелектуальних" карток в процесі стандартизації" [Hanns-Peter König "Cryptographic Identification Methods for Smart Card in the Process of Standardization"] в журналі IEEE Communications Magazine, том 29, №6, червень 1991, сс. 42-48. У викладеному в ній способі як першу інформацію від терміналу запису/зчитування на смарт-картку передають випадкове число, яке в картці кодується за допомогою секретного алгоритму і щонайменше одного секретного числа. Закодований результат пересилають назад від смарт-картки до терміналу і там або декодують або таким же чином кодують. Отриманий результат порівнюють з початково переданим випадковим числом або з прийнятою другою інформацією. Позитивний результат порівняння свідчить, що обидва абоненти процесу обміну даними користуються правильним алгоритмом і правильним секретним числом або правильним кодом і тому є аутентичними.

Способи аутентифікації використовують, передовсім тоді, коли йдеться про операції з грошима або про критичну з точки зору безпеки інформацію. Такі операції часто зазнають небажаного втручання. Перед зловмисником стоїть задача визначити задіяні коди, секретні числа і алгоритми. Контролюючи хід обміну даними, можна зробити висновок про вид використовуваної аутентифікації і таким чином цілеспрямовано здійснити втручання.

Задачею винаходу є якомога краще приховання виду здійснюваного способу аутентифікації.

Задача вирішена способом згідно з п.1 формули винаходу. Вигідні вдосконалення винаходу є предметами додаткових пунктів формули винаходу.

Завдяки необхідності одночасного здійснення щонайменше двох операцій обробки, зловмиснику значно утруднюється задача розпізнавання внутрішнього ходу аутентифікації шляхом дослідження, наприклад, зміни споживаної потужності в часі.

Нижче винахід докладніше пояснюється з використанням прикладу виконання, зображеного на ілюстрації.

Представлена на фіг. система обміну даними включає першого абонента 1, який може бути, наприклад, терміналом запису/зчитування, і другого абонента 2, який може бути, наприклад, смарт-карткою або чіп-карткою. У поясненому нижче прикладі другий абонент, тобто, картка, має бути аутентифікована першим абонентом - терміналом. Тому на фігурі зображені лише потрібні для цієї операції функціональні вузли картки. Для випадку, коли термінал має бути аутентифікований карткою 2, термінал мусить містити відповідні функціональні вузли.

Спочатку термінал 1 передає на картку 2 першу інформацію, так званий виклик. Згідно з винаходом виклик підводиться як до першого обробного пристрою VE1, так і до другого обробного пристрою VE2. Для виконання обробки виклику, необхідної для аутентифікації, до обробних пристроїв VE1, VE2 із запам'ятовуючого пристрою SP підводиться необхідна інформація, така як секретне число чи ключ.

Власне обробка може здійснюватися або шляхом простого порівняння виклику з очікуваним, записаним у запам'ятовуючому пристрої SP значенням, або ж шляхом складного декодування, наприклад, відповідно з алгоритмами DES (Data Encryption Standard = стандарт шифрування США) або RSA. Для цієї мети обробні пристрої VE1, VE2 можуть бути виконані у вигляді складних мікропроцесорів з відповідними крипто-співпроцесорами. Часто застосовують апаратно реалізовані пристрої однонапрявленого кодування, виконані, наприклад, з використанням охоплених зворотним зв'язком зсувних регістрів.

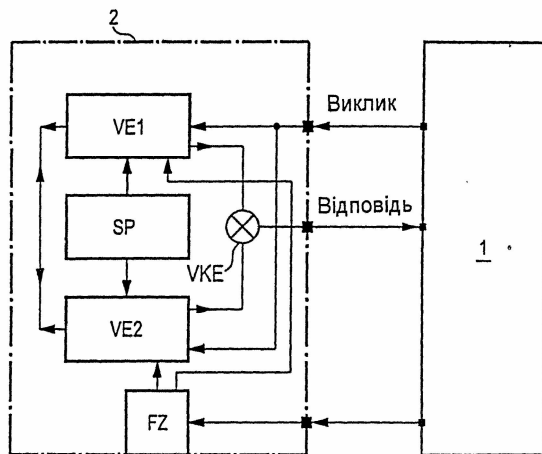
Інформація з виходів обробних пристроїв VE1, VE2 подається на пристрій логічного об'єднання VKE, вихідний сигнал якого як відповідь передається на термінал 1. Пристрій логічного об'єднання VKE не обов'язково мусить здійснювати логічне об'єднання вихідних даних обробних пристроїв VE1, VE2; він може також лише передавати вихідну інформацію першого обробного пристрою VE1 як відповідь, а вихідну інформацію другого обробного пристрою VE2 блокувати, оскільки суттєвим аспектом винаходу є одночасне виконання щонайменше двох, переважно різних процесів обробки з метою унеможливлення розпізнавання внутрішньої структури і відповідних даних абонента 2 за змінами споживаної потужності.

Однак доцільним є логічне об'єднання вихідних даних обробних пристроїв VE1, VE2, наприклад, за допомогою логічного елемента "Виключне АБО", на якому виконаний пристрій логічного об'єднання VKE.

На блок-схемі зображено логічне об'єднання виходів обох обробних пристроїв VE1, VE2. В даному разі логічне об'єднання означає залучення проміжного або кінцевого результату обробки даних в одному обробному пристрої до обробки в іншому обробному пристрої. При цьому в першому вдосконаленому варіанті винаходу вихідні дані лише одного обробного пристрою враховуються в іншому обробному пристрої, а в іншому варіанті вихідні дані кожного з обробних пристроїв використовуються в іншому обробному пристрої.

Як уже було сказано у вступній частині опису, правильність відповіді може перевірятися в терміналі 1 різними способами. Деякі можливі рішення такого типу вичерпно описані у згаданому друкованому виданні і тому на фігурі детальніше не показані.

В іншому варіанті виконання винаходу передбачено лічильник помилок FZ, який фіксує кількість негативних результатів порівняння і при певній попередньо заданій їх кількості блокує обробні пристрої VE1, VE2, внаслідок чого подальше виконання аутентифікації і, тим самим, подальший обмін даними між терміналом 1 і карткою 2 стають неможливими. Таким чином гарантується, що не може бути здійснена довільна кількість спроб дослідження процесу аутентифікації.



1	перший абонент термінал
2	другий абонент картка
VE1	першого обробного пристрою
VE2	другого обробного пристрою
SP	запам'ятовуючого пристрою
VKE	пристрій логічного об'єднання
FZ	лічильник помилок