HU 0002195 34 B

(19) Országkód

HU

MAGYAR KÖZTÁRSASÁG

MAGYAR SZABADALMI HIVATAL

SZABADALMI LEÍRÁS

(11) Lajstromszám:

219 534 B

(21) A bejelentés ügyszáma: P 96 02255
(22) A bejelentés napja: 1996. 08. 15.
(30) Elsőbbségi adatok:
1000988 1995. 08. 16. NL

(51) Int. Cl.[7]

G 06 K 19/00

(40) A közzététel napja: 1997. 05. 28.
(45) A megadás meghirdetésének dátuma a Szabadalmi Közlönyben: 2001. 05. 28.

(72) Feltaláló:
Hekstra, Andries Pieter, Voorschoten (NL)

(73) Szabadalmas:
Koninklijke KPN N. V., Hága (NL)

(74) Képviselő:
Komáromi Judit, DANUBIA Szabadalmi és Védjegy Iroda Kft., Budapest

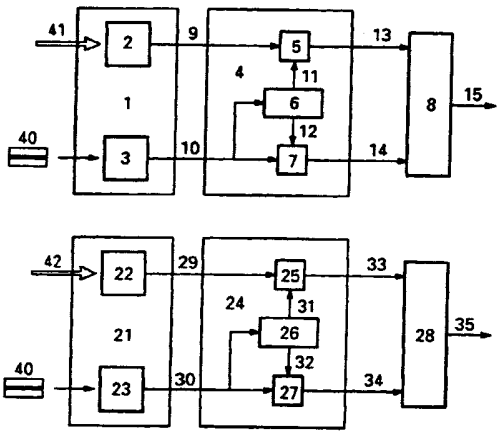
(54) ## Eljárás és rendszer azonos adathordozóval különböző azonosítási eljárások végrehajtására

KIVONAT

A találmány tárgya eljárás és rendszer azonos adathordozóval különböző azonosítási eljárások végrehajtására.

Az ismert módszerek, melyek ugyanazon adathordozóval alkalmasak különböző azonosítási eljárások végrehajtására, nem szabványosított adathordozókra (intelligens mikrokártyákra) alapulnak, melyeken két különböző hozzáférési kódot tárolnak.

A találmány szerint az első azonosítási eljárással az első felhasználó első kódot állít elő, melyet egy, az adathordozón tárolt első hozzáférési kód átalakított változatával hasonlítanak össze. A második azonosítási eljárással a második felhasználó második felhasználói kódot állít elő, melyet az adathordozón tárolt második hozzáférési kód átalakított változatával hasonlítanak össze. Mivel a másik azonosítási eljárás más átalakítással történik, ugyanazt a világszerte szabványosított adathordozót lehet használni különböző azonosítási eljárásokhoz, melyen csupán egyetlen hozzáférési kód van tárolva. Az első/második felhasználó első/második felhasználói kódot állít elő, amelyet az adathordozón tárolt egyetlen hozzáférési kód első/második átalakításával átalakított változattal hasonlítanak össze.



1. ábra

HU 219 534 B

A találmány tárgya eljárás azonos adathordozóval különböző azonosítási eljárások végrehajtására, mely adathordozón legalább egy kódot tárolunk, az eljárás első azonosítási eljárási folyamata a következő lépésekből áll:

- az adathordozón tárolt első kódot és egy felhasználótól származó második kódot veszünk,
- a következő kódátalakítások közül legalább egyet végrehajtunk,
  - az első kódot első átalakítással átalakított első kóddá alakítjuk át, és
  - a második kód második átalakításával átalakított második kódot állítunk elő,
- a kódokat összehasonlítjuk, és azok eredményétől függően az első azonosítási eljárást lezárjuk,

és az eljárás második azonosítási eljárása a következő lépésekből áll:

- az adathordozón tárolt harmadik kódot és egy felhasználótól származó negyedik kódot veszünk,
- a következő kódátalakítások közül legalább egyet végrehajtunk:
  - a harmadik kód harmadik kódátalakításával átalakított harmadik kódot állítunk elő, és
  - a negyedik kód negyedik kódátalakításával átalakított negyedik kódot állítunk elő,
- a kódokat összehasonlítjuk és azok eredményétől függően a második azonosítási eljárást lezárjuk.

A találmány tárgya továbbá a fenti eljárás végrehajtására alkalmas rendszer.

Egy ilyen eljárást ismertetnek az US 4 837 422 lajstromszámú szabadalmi leírásban. Ebben egy intelligens mikrokártya formájában kialakított adathordozót mutatnak be (az US 4 837 422 lajstromszámú szabadalmi leírás 2. ábráján), melyen egy első kódot [az US 4 837 422 2. ábráján 210 hivatkozási számmal jelölt memóriában tárolt PIN-kód (személyi azonosítószám)], és amelyen egy harmadik kódot tárolnak (az US 4 837 422 számú leírás 2. ábráján 207 memóriában tárolt SUBPIN-kód, azaz kiegészítő személyi azonosítószám). Általánosságban véve a PIN-kód és a SUBPIN-kód sifrírozott formában van tárolva.

Egy első azonosítási eljárás esetében, mely például egy első rendszerre és például egy első felhasználóra vonatkozik, a felhasználó előállítja a valós PIN-kódot (a második kódot), melyet az első rendszer vesz, ezután a sifrírozott módon tárolt PIN-kódot (az első kódot) kiolvassák és (az első kódátalakítás segítségével) desifrírozzák, amivel előállítják a PIN-kódot (az átalakított első kódot). Ezt azután összehasonlítják az előállított valós PIN-kóddal (a második kóddal), és erre válaszképp az első azonosítási eljárás pozitívan fejeződik be (megegyezés esetében), vagy pedig negatívan (ha a két kód nem egyezik meg). A sifrírozott PIN-kód desifrírozása (az első kódátalakítás segítségével az első kódot átalakított első kóddá alakítják át) helyett vagy annak kiegészítéseképp az egyik lehetőség az, hogy az első felhasználó által előállított valós PIN-kódot (a második kódot) a második kódátalakítás segítségével átalakított második kóddá alakíthatják át, majd ezután vagy az átalakított második kódot hasonlítják össze, vagy pedig az első kódot, vagy pedig az átalakított első kódot, az adott esetnek megfelelően stb.

Egy második azonosítási eljárás esetében, mely például egy második rendszerre és például egy második felhasználóra vonatkozik, a második felhasználó létrehozza a valós SUBPIN-kódot (a negyedik kódot), melyet a második rendszer vesz, ezután a sifrírozott módon tárolt SUBPIN-kódot (a harmadik kódot) kiolvassák és (a harmadik kódátalakítás segítségével) desifrírozzák, amellyel megkapják a SUBPIN-kódot (az átalakított harmadik kódot). Ezt azután összehasonlítják az előállított valós SUBPIN-kóddal (a negyedik kóddal), és erre válaszképp a második azonosítási eljárás pozitívan zárul (megegyezés esetén), vagy pedig negatívan (ha a két kód nem egyezik meg). Az adott esettől függően a sifrírozott SUBPIN-kód desifrírozása (a harmadik kódátalakítás segítségével a harmadik kódot átalakítják az átalakított harmadik kóddá) helyett vagy annak kiegészítéseképp az egyik lehetőség az, hogy a második felhasználó által előállított valós SUBPIN-kódot (a negyedik kódot) a negyedik kódátalakítás segítségével átalakítják az átalakított negyedik kóddá, majd ezután vagy az átalakított negyedik kódot hasonlítják össze, vagy pedig a harmadik kódot, vagy az átalakított harmadik kódot az adott esettől függően stb.

Mindkét azonosítási eljárás vonatkozhat továbbá olyan különböző rendszerekre, melyeknek egy felhasználója van, vagy pedig olyan rendszerre, amelynek különböző felhasználói vannak (mint például az US 4 837 422 lajstromszámú szabadalmi leírás esetében).

Ezeknek az eljárásoknak többek között az a hátránya, hogy az első azonosítási eljárás kedvéért az első kódot az adathordozón kell tárolni, a második azonosítási eljárás kedvéért pedig a harmadik kódot ugyanazon az adathordozón kell tárolni. Ennek eredményeképp nem lehetséges olyan, már gyakran forgalomban lévő adathordozók előnyeinek kihasználása, amelyeken nem lehet tárolni a következő azonosítási eljárások következő kódját.

A találmány egyik célja egy, a bevezetőben említett olyan eljárás kidolgozása, mellyel lehetővé válik már gyakran forgalomban lévő olyan adathordozók előnyeinek kihasználása, amelyeken nem lehet tárolni a következő azonosítási eljárásokhoz szükséges következő kódokat.

Ebből a célból a találmány szerinti eljárás új jellemzője, hogy az első kód és a harmadik kód egyenlő, míg a második kód és a negyedik kód különböző, és az első és harmadik, illetve a második és negyedik kódátalakítások közül legalább az első és a harmadik vagy a második és a negyedik kódátalakítások eltérőek.

Mivel az első és a második kódátalakítások közül legalább az egyik különbözik a harmadik, illetve a negyedik kódátalakítástól, az első és a harmadik kód egyenlő lehet és teljesen egybeeshet, miközben a második kód és a negyedik kód eltérő egymástól. Felmerül tehát annak a lehetősége, hogy olyan adathordozókat használjunk, amelyen csak az első kódot tároltuk (mely első kód megegyezik és egybeesik a harmadik kóddal), és ezeket az adathordozókat két különböző azonosítási

eljáráshoz is lehet használni, melyekhez akkor a második kódot, illetve a negyedik kódot kell előállítani.

A találmány többek között abból az elgondolásból indul ki, hogy az első azonosítási eljárás legalább három paraméterre alapul, nevezetesen az első kódra, a második kódra és legalább egy (az első vagy a második) kódalakításra, a második azonosítási eljárás pedig legalább három paraméterre alapul, nevezetesen a harmadik kódra, a negyedik kódra és legalább egy (a harmadik vagy negyedik) kódátalakításra, továbbá abból az elgondolásból, hogy ha legalább három paraméterre alapulnak az azonosítási eljárások, az egyik paraméter állandó értéket kap, a legalább két paraméter közül pedig a másodikat még mindig szabadon meg lehet választani.

Tehát a gyakran már forgalomban lévő adathordozók felhasználhatóságát akadályozó problémát, azaz azt, hogy azokon a következő azonosítási eljáráshoz nem lehet egy további kódot tárolni, úgy oldottuk meg, hogy legalább az egyik rendszerben legalább az egyik kódátalakítást szabályozzuk.

Előnyös, ha az első kódátalakítás eltér a harmadik kódátalakítástól, ugyanakkor a második kódátalakítás megegyezik a negyedik kódátalakítással.

Tehát az első eljárásra és az első felhasználóra vonatkozó első azonosítási eljárás esetében az első felhasználó a második kódot állítja elő, melyet az első rendszer vesz, ezután az első, sifrírozva tárolt kódot vagy a harmadik, sifrírozva tárolt kódot kiolvassuk és az első kódátalakítással desifrírozzuk, amellyel megkapjuk az első kódot, egy első módon átalakítva, vagy pedig a harmadik kódot, egy első módon átalakítva, melyet azután összehasonlítunk a második (és esetleg egy második módon átalakított) előállított kóddal, és arra válaszképp az első azonosítási eljárást pozitívan zárjuk le (megegyezés esetén), vagy pedig negatívan (meg nem egyezés esetén). A második rendszerre és a második felhasználóra vonatkozó második azonosítási eljárás esetében a második felhasználó előállítja a negyedik kódot, melyet a második rendszerrel veszünk, azután az első, sifrírozott formában tárolt kódot vagy a harmadik, sifrírozott formában tárolt kódot kiolvassuk és a harmadik kódátalakítással desifrírozzuk, amellyel megkapjuk az első kódot, harmadik módon átalakítva, vagy pedig a harmadik kódot harmadik módon átalakítva, melyet azután összehasonlítunk az előállított (és esetleg egy negyedik módon átalakított) negyedik kóddal, és erre válaszképp a második azonosítási eljárást pozitívan zárjuk le (megegyezés esetén), vagy pedig negatívan zárjuk le (meg nem egyezés esetén). Mivel az első kódátalakítás és a harmadik kódátalakítás egymástól eltérő, a felhasználónak ennélfogva minden rendszerhez másik kódot kell előállítania (a másodikat vagy a negyediket), ugyanakkor az adathordozón csak egyetlen kódot helyezünk el (az elsőt vagy a harmadikat). A második kódátalakítás és a negyedik kódátalakítás kölcsönösen egyforma, és a legegyszerűbb esetben ezeket el is lehet hagyni, ami természetesen általában véve nem növeli a biztonságot.

Előnyös, ha a második kódátalakítás eltér a negyedik kódátalakítástól, ugyanakkor az első kódátalakítás megegyezik a harmadik kódátalakítással.

Ebben a változatban egy, az első rendszerre és az első felhasználóra vonatkozó első azonosítási eljárás esetében az első felhasználó létrehozza a második kódot, amelyet az első rendszer vesz és egy második módon átalakított második kóddá alakítja át, ezután az (esetleg sifrírozott módon tárolt) első kódot vagy az (esetleg sifrírozott módon tárolt) harmadik kódot kiolvassuk és adott esetben az első kódátalakítással desifrírozzuk, mellyel megkapjuk az első (és esetleg egy első módon átalakított) első kódot, vagy a harmadik (esetleg egy első módon átalakított) kódot, melyet azután a második, egy második módon előállított és átalakított kóddal hasonlítunk össze, és erre válaszképp az első azonosítási eljárás pozitívan zárul (megegyezés esetén), vagy negatívan (meg nem egyezés esetében). A második rendszerre és a második felhasználóra vonatkozó második azonosítási eljárás esetében a második felhasználó előállítja a negyedik kódot, melyet a második rendszer vesz, és egy negyedik módon átalakít a negyedik kóddá, ezután pedig az első (esetleg sifrírozott módon tárolt) kódot vagy a harmadik (esetleg sifrírozott módon tárolt) kódot kiolvassuk és adott esetben a harmadik kódátalakítás segítségével desifrírozzuk, mellyel megkapjuk az első (esetleg egy harmadik módon átalakított) kódot, vagy a harmadik (esetleg egy harmadik módon átalakított) kódot, melyet azután összehasonlítunk egy negyedik módon előállított és átalakított kóddal, és erre válaszképp a második azonosítási eljárást pozitívan zárjuk le (megegyezés esetében), vagy pedig negatívan (meg nem egyezés esetében). Mivel a második kódátalakítás és a negyedik kódátalakítás különbözőek, ennélfogva a felhasználónak minden rendszerhez más-más kódot (a másodikat és a negyediket) kell előállítania, ugyanakkor az adathordozón csupán egyetlen kód (az első vagy a harmadik) van elhelyezve. Az első kódátalakítás és a harmadik kódátalakítás kölcsönösen egyenlőek, és a legegyszerűbb esetben ezek elhagyhatóak, ami azonban általánosságban nem javítja a biztonságot.

Előnyös, ha az első kódátalakítás eltér a harmadik kódátalakítástól, és a második kódátalakítás is eltér a negyedik kódátalakítástól.

Ebben a változatban egy, az első rendszerre és az első felhasználóra vonatkozó első azonosítási eljárás esetében az első felhasználó létrehozza a második kódot, amelyet az első rendszer vesz és egy második módon átalakított második kóddá alakítja át, ezután az (esetleg sifrírozott módon tárolt) első kódot vagy az (esetleg sifrírozott módon tárolt) harmadik kódot kiolvassuk és adott esetben az első kódátalakítással desifrírozzuk, mellyel megkapjuk az első (és esetleg egy első módon átalakított) első kódot, vagy a harmadik (esetleg egy első módon átalakított) harmadik kódot, melyet azután a második, egy második módon előállított és átalakított kóddal hasonlítunk össze, és erre válaszképp az első azonosítási eljárás pozitívan zárul (megegyezés esetén), vagy negatívan (meg nem egyezés esetében). A második rendszerre és a második felhasználóra vonatkozó második azonosítási eljárás esetében a második felhasználó előállítja a negyedik kódot, melyet a második rendszer vesz, és egy negyedik módon átalakít a ne-

gyedik kóddá, ezután pedig az első (esetleg sifrírozott módon tárolt) kódot vagy a harmadik (esetleg sifrírozott módon tárolt) kódot kiolvassuk és adott esetben a harmadik kódátalakítás segítségével desifrírozzuk, mellyel megkapjuk az első (esetleg egy harmadik módon átalakított) kódot vagy a harmadik (esetleg egy harmadik módon átalakított) kódot, melyet azután összehasonlítunk egy negyedik módon előállított és átalakított kóddal, és erre válaszképp a második azonosítási eljárást pozitívan zárjuk le (megegyezés esetében), vagy pedig negatívan (meg nem egyezés esetében). Mivel a második kódátalakítás és a negyedik kódátalakítás különbözőek, ennélfogva a felhasználónak minden rendszerhez más-más kódot (a másodikat és a negyediket) kell előállítania, ugyanakkor az adathordozón csupán egyetlen kód (az első vagy a harmadik) van elhelyezve. Az első kódátalakítás és a harmadik kódátalakítás kölcsönösen egyenlőek, és a legegyszerűbb esetben ezek elhagyhatóak, ami azonban általánosságban nem javítja a biztonságot. Mivel nemcsak az első kódátalakítás és a harmadik kódátalakítás különbözik egymástól, hanem a második kódátalakítás és a negyedik kódátalakítás is különbözik, a felhasználónak mindegyik rendszerhez más kódot (másodikat vagy a negyediket) kell előállítania, az adathordozón azonban csak egy kód (az első vagy a harmadik) van elhelyezve, így egy jól védett rendszerről beszélhetünk.

Előnyös, ha a kódátalakítások közül legalább egyet az adathordozón tárolt ötödik kódtól függően hajtunk végre.

Mivel a kódátalakítások közül legalább egy az adathordozón tárolt ötödik kódtól függ, például egy (zsíró- vagy bankszámla-) számtól vagy születési dátumtól, sokkal bonyolultabb lesz a találmány szerinti eljárást felderíteni, ami annak biztonságát javítja.

A találmány tárgya továbbá rendszer azonos adathordozóval különböző azonosítási eljárások végrehajtására, ahol az adathordozón legalább egy kód van tárolva, mely rendszer egy első azonosítási eljárás esetében el van látva:

- az adathordozón tárolt első kód és egy felhasználótól származó második kód vételére első vevőegységgel,
- a következő kódátalakítások közül legalább egynek a végrehajtására első kódátalakítóval,
  - az első kódnak átalakított első kóddá való első átalakítása, és
  - a második kódnak átalakított második kóddá való második kódátalakítása,
- az első azonosítási eljárás lezárására válaszképp kódok összehasonlítására első összehasonlító egységgel,

és amely rendszer egy második azonosítási eljárás esetében el van látva:

- az adathordozón tárolt harmadik kód és egy felhasználótól származó negyedik kód vételére második vevőegységgel,
- a következő kódátalakítások közül legalább egynek a végrehajtására második kódátalakítóval,
  - a harmadik kódnak átalakított harmadik kóddá való harmadik átalakítása, és
  - a negyedik kódnak átalakított negyedik kóddá való negyedik kódátalakítása,
- a második azonosítási eljárás lezárására válaszképp kódok összehasonlítására második összehasonlító egységgel,

ahol a találmány szerint az első kód és a harmadik kód egyenlőek, míg a második kód és a negyedik kód különbözőek, és az első és harmadik, illetve a második és negyedik kódátalakítások közül legalább az első és a harmadik vagy a második és a negyedik kódátalakítások eltérőek.

Előnyös, ha az első kódátalakítás eltér a harmadik kódátalakítástól, ugyanakkor a második kódátalakítás megegyezik a negyedik kódátalakítással.

Célszerű, ha a második kódátalakítás eltér a negyedik kódátalakítástól, ugyanakkor az első kódátalakítás megegyezik a harmadik kódátalakítással.

Előnyös, ha az első kódátalakítás eltér a harmadik kódátalakítástól, és a második kódátalakítás is eltér a negyedik kódátalakítástól.

Célszerű, ha a kódátalakítások közül legalább egyet az adathordozón tárolt ötödik kódtól függően hajtunk végre.

A találmány szerinti megoldás kidolgozásánál felhasználtuk a

- „Contemporary Cryptology" („Korszerű rejtjelezés") [The Science of Information Integrity (Az információ egységességének tudománya), edited by Gustavus J. Simmons, IEEE Press, 1992] és a
- „Cryptography: a new dimension in computer data security" („Rejtjelezés: új dimenzió a számítógépes adatvédelemben") [A guide for the Design and Implementation of Secure Systems (Kézikönyv biztonsági rendszerek tervezéséhez és megvalósításához), by Carl H. Meyer and Stephen M. Matyas, Wiley-Interscience Publication, John Wiley & Sons, 1982] könyveket és az
- NL 1000988 számú holland szabadalmi bejelentést.

A találmány szerinti eljárást és rendszert az alábbiakban kiviteli példa kapcsán a mellékelt rajzra való hivatkozással ismertetjük részletesebben, ahol az

ábrán a találmány szerinti eljárás alkalmazására alkalmas találmány szerinti rendszer tömbvázlatát szemléltetjük.

Az 1. ábrán látható találmány szerinti rendszer első 1 vevőegységet tartalmaz, mely például 2 billentyűzettel és 3 kártyaolvasóval van ellátva, és tartalmaz egy 4 kódátalakítót, mely az 1 vevőegységhez van csatlakoztatva, a 4 kódátalakító például 5 sifrírozóegységgel, 6 processzorral és egy második 7 sifrírozóegységgel van ellátva. Az 5 sifrírozóegység első bemenete 9 összeköttetésen keresztül a 2 billentyűzet egyik kimenetével, a 7 sifrírozóegység első bemenete és a 6 processzor bemenete 10 összeköttetésen keresztül a 3 kártyaolvasó kimenetével vannak összekötve. A 6 processzor első kimenete 11 összeköttetés segítségével az 5 sifrírozóegység második bemenetével, a 6 processzor második kimenete pedig 12 összeköttetésen keresztül a 7 sifrírozóegység második bemenetével van összekötve. Az 5 sifrírozóegység kimenete 13 összeköttetésen kereszt-

tül első 8 összehasonlító egység első bemenetével, a 7 sifrírozóegység kimenete pedig 14 összeköttetésen keresztül a 8 összehasonlító egység második bemenetével van összekapcsolva, melynek 15 kimenete van.

Az 1. ábrán szemléltetett találmány szerinti rendszer második 21 vevőegységet tartalmaz, mely például 22 billentyűzettel és 23 kártyaolvasóval van ellátva, és a rendszer tartalmaz egy második 24 kódátalakítót, mely a második 21 vevőegységhez van csatlakoztatva, mely például 25 sifrírozóegységgel, 26 processzorral és egy további 27 sifrírozóegységgel van ellátva. A 25 sifrírozóegység első bemenete 29 összeköttetésen keresztül a 22 billentyűzet kimenetével, a 27 sifrírozóegység első bemenete és a 26 processzor bemenete 30 összeköttetésen keresztül a 23 kártyaolvasó kimenetével, a 26 processzor első kimenete 31 összeköttetésen keresztül a 25 sifrírozóegység második bemenetével, a 26 processzor második kimenete pedig 32 összeköttetésen keresztül a 27 sifrírozóegység második bemenetével van összekötve. A 25 sifrírozóegység kimenete 33 összeköttetésen keresztül a második 28 összehasonlító egység első bemenetével, a 27 sifrírozóegység kimenete pedig 34 összeköttetésen keresztül a második 28 összehasonlító egység második bemenetével van összekötve, melynek 35 kimenete van.

A találmány szerinti rendszer a következőképpen működik. Egy első felhasználó, akinek egy adott időpontban van egy adathordozója, például egy mágneskártyája, amelyen első 40 kód van tárolva, mágneskártyáját behelyezi a 3 kártyaolvasóba, mely az első 40 kódot és a további adatokat (például számlaszámot, nevet és címet) kiolvassa, ezután az első 40 kódot a 10 összeköttetésen keresztül a 7 sifrírozóegységbe továbbítja, a többi adatot pedig a 10 összeköttetésen keresztül a 6 processzorba. Ezenkívül szóban forgó első felhasználó a 2 billentyűzet segítségével előállít egy második 41 kódot, melyet a 9 összeköttetésen keresztül az 5 sifrírozóegységbe ad be. A további adatokra válaszképp a 6 processzor egy első kulcsszót állít elő, melyet a 12 összeköttetésen keresztül a 7 sifrírozóegységbe ad be, mely az első kulcsszóra válaszképp az első 40 kódot átalakított első kóddá alakítja át, és azt a 14 összeköttetésen keresztül az első 8 összehasonlító egységbe továbbítja. A további adatra válaszképp a 6 processzor második kulcsszót állít elő, melyet a 11 összeköttetésen keresztül az 5 sifrírozóegységre ad, mely ezen második kulcsszóra válaszképp a második 41 kódot átalakított második kóddá alakítja át, és azt a 13 összeköttetés segítségével az első 8 összehasonlító egységre továbbítja. Ez utóbbi az átalakított kódokat összehasonlítja egymással, és megegyezés esetén pozitív azonosítási jelet ad ki a 15 kimeneten, meg nem egyezés esetén pedig negatív azonosítási jelet ad ki a 15 kimeneten. A pozitív azonosítási jelre válaszképp az első felhasználó hozzáférhet például egy automata készpénzkiadóhoz.

Egy második felhasználó, akinek egy adott időpontban birtokában van ugyanez az adathordozó, például a mágneskártya, amelyen az első 40 kód van tárolva, behelyezi mágneskártyáját a 23 kártyaolvasóba, mely kiolvassa az első 40 kódot és a további adatokat (például számlaszámot és nevet és címet), ezután az első 40 kódot a 30 összeköttetésen keresztül a 27 sifrírozóegységbe adja be, a további adatokat pedig a 30 összeköttetésen keresztül a 26 processzorba. Továbbá a szóban forgó második felhasználó a 22 billentyűzet segítségével előállít egy negyedik 42 kódot, melyet 29 összeköttetésen keresztül a 25 sifrírozóegységbe visz be. A további adatokra válaszképp a 26 processzor egy harmadik kulcsszót állít elő, melyet a 32 összeköttetésen keresztül a 27 sifrírozóegységbe ad be, mely erre a harmadik kulcsszóra az első 40 kódot átalakított első kóddá alakítja át, és azt a 34 összeköttetésen keresztül a második 28 összehasonlító egységbe továbbítja. A további adatokra válaszképp a 26 processzor továbbá előállít egy negyedik kulcsszót, melyet a 31 összeköttetésen keresztül a 25 sifrírozóegységbe adunk, mely ezen negyedik kulcsszóra válaszképp a negyedik 42 kódot egy átalakított negyedik kóddá alakítja át, és azt a 33 összeköttetésen keresztül a második 28 összehasonlító egységbe továbbítja. A 28 összehasonlító egység a két átalakított kódot összehasonlítja egymással, és megegyezés esetén pozitív azonosítójelet állít elő a 35 kimeneten, meg nem egyezés esetében pedig egy negatív azonosítási jelet állít elő 35 kimenetén. A pozitív azonosítási jelre válaszképp a második felhasználó hozzáférhet például egy automatikus csomagkezelő egységhez, és a továbbítandó csomag postázási költségei automatikusan határozzák meg és jelölik ki a fizető személyt vagy szervezetet.

Mivel a második felhasználó nem ismeri a második 41 kódot, nem fog sikerülni neki, hogy hozzáférjen az automata készpénzkiadó berendezéshez. Összefoglalva, az első felhasználó, ha ő például a tulajdonosa az adathordozónak vagy egy olyan cégnek a főnöke, akinek a tulajdonába tartozik az adathordozó, és aki a második felhasználót alkalmazza, ismerni fogja a második és a negyedik kódot is, jóllehet, erre nincs szükség. Tehát ugyanazzal az adathordozóval, amelyen az első kód és valamilyen további adatok vannak tárolva, különböző azonosítási eljárásokat lehet végrehajtani oly módon, hogy a felhasználók közül legalább egy, aki a kódok közül legalább egyet nem ismer, nem lesz képes arra, hogy az összes azonosítási eljárást pozitív azonosítási eredménnyel zárja le, azaz legalább egy negatív eredményre fog jutni.

Az adathordozón tárolt első kód tehát egy (esetleg sifrírozott) PIN-kód (személyi azonosítószám), és mivel vagy az történik, hogy legalább az első kód az első kulcsszóval és az első kód a harmadik kulcsszóval különböző módon lesznek átalakítva, vagy pedig az történik, hogy legalább a második kód a második kulcsszóval és a negyedik kód a negyedik kulcsszóval különböző módon lesznek átalakítva, elérjük azt, hogy ezentúl nem kell különböző PIN-kódokat (például egy PIN-kódot és egy SUBPIN-kódot vagy pedig egy első kódot és egy harmadik kódot) tárolni ugyanazon az adathordozón. Ez azt eredményezi, hogy világszerte használt szabványos adathordozókat lehet készíteni (például mágneskártyákat vagy csipkártyákat), aminek természetesen nagy előnye van.

Ha az első kódot az első kulcsszóval és az első kódot a harmadik kulcsszóval különböző módokon alakítjuk át, és ezenkívül a második kódot is a második kulcsszóval és a negyedik kódot a negyedik kulcsszóval különböző módon alakítjuk át, a biztonság a legnagyobb lesz. Ha a kódátalakítások közül legalább az egyiket egy, az adathordozón tárolt ötödik kódtól tesszük függővé (ez az ötödik kód lehet például a további adatoknak legalább egy része), a fent említett biztonságot még tovább növeljük. Ebben az esetben a 6 processzor a további adatok első részére (például a számlaszámra) válaszképp egy táblázatból előállíthat egy első értéket és egy második értéket, ezután az első értéket használjuk az első kulcsszó kiszámítására, a további adat egy második részére (például a névre) válaszképp, és a második értéket pedig a további adatok harmadik részére (például a címre) válaszképp a második kulcsszó kiszámítására használjuk. Ezenkívül a 26 processzor a további adatok első részére (például a számlaszámra) válaszképp előállíthat egy harmadik értéket és egy negyedik értéket egy táblázatból, majd ezután a harmadik értéket használjuk a további adatok egy második részére (például a névre) válaszképp a harmadik kulcsszó kiszámítására, a negyedik értéket pedig a további adatok harmadik részére (például a címre) válaszképp a negyedik kulcsszó kiszámítására használjuk. Vagyis a kódátalakítások közül legalább egyet egy ötödik kódszótól lehet függővé tenni oly módon, hogy ezt az ötödik kódot a szakemberek számára ismert módon kombináljuk a 9, 10, 29 és 30 összeköttetések közül legalább egyen keresztül beérkező kóddal.

A 6 (26) processzorok tartalmaznak például egy érzékelőt a további adatok érzékelésére, egy táblázatmemóriát, melynek legalább három oszlopa van, melyek közül az első oszlopban például a számlaszámokat, a második oszlopban az első (harmadik) kulcsszót vagy egy első (harmadik) értéket, a harmadik oszlopban pedig egy második (negyedik) kulcsszót vagy egy második (negyedik) értéket tárolunk, és a 6 (26) processzorok tartalmaznak egy, az érzékelőt és a táblázatmemóriát vezérlő processzort, mellyel adott esetben az első és második (harmadik és negyedik) kulcsszavakat kiszámítjuk, az első és második (harmadik és negyedik) értékek alapján, és például a nevek és címek alapján. Az 5 és 7 (25 és 27) sifrírozóegységek például a szakemberek által ismert sifrírozó áramkörök, melyek egy x bites bemenőszót egy y bites kulcsszó függvényében z bites kimenőszóvá alakítanak át, az x=y=z összefüggés alapján, ami általában megfelel, de nem feltétlenül szükségszerű. A 8 (28) összehasonlító egység például egy, a szakterületen ismert összehasonlító áramkör.

A 4 kódátalakító tehát a 7 sifrírozóegység segítségével az első 40 kódon első kódátalakítást hajt végre, amelyből az első kulcsszó segítségével egy átalakított első kódot állít elő, és az 5 sifrírozóegység segítségével pedig második kódátalakítást hajt végre a második 41 kódon, melyből a második kulcsszó segítségével egy átalakított második kódot állít elő. A második 24 kódátalakító tehát a 27 sifrírozóegység segítségével az első (egyenlő harmadik) 40 kód harmadik átalakítását hajtja végre, és abból a harmadik kulcsszó segítségével átalakított első (=átalakított harmadik) kódot állít elő, és ezenkívül a 25 sifrírozóegység segítségével a negyedik 42 kódon egy negyedik átalakítást hajt végre, melyből a negyedik kulcsszó segítségével átalakított negyedik kódot állít elő. Természetesen a szakemberek számára ismert módon sok más kódátalakítást is lehet alkalmazni, például olyanokat, melyek nem kulcsszavakra alapulnak.

SZABADALMI IGÉNYPONTOK

1. Eljárás azonos adathordozóval különböző azonosítási eljárások végrehajtására, mely adathordozón legalább egy kódot tárolunk, az eljárás első azonosítási eljárási folyamata a következő lépésekből áll:
- az adathordozón tárolt első kódot és egy felhasználótól származó második kódot veszünk,
- a következő kódátalakítások közül legalább egyet végrehajtunk,
  - az első kódot első átalakítással átalakított első kóddá alakítjuk át, és
  - a második kód második átalakításával átalakított második kódot állítunk elő,
- a kódokat összehasonlítjuk és azok eredményétől függően az első azonosítási eljárást lezárjuk,

és az eljárás második azonosítási eljárása a következő lépésekből áll:
- az adathordozón tárolt harmadik kódot és egy felhasználótól származó negyedik kódot veszünk,
- a következő kódátalakítások közül legalább egyet végrehajtunk:
  - a harmadik kód harmadik kódátalakításával átalakított harmadik kódot állítunk elő, és
  - a negyedik kód negyedik kódátalakításával átalakított negyedik kódot állítunk elő,
- a kódokat összehasonlítjuk és azok eredményétől függően a második azonosítási eljárást lezárjuk,

azzal jellemezve, hogy az első (40) kód és a harmadik (40) kód egyenlő, míg a második (41) kód és a negyedik (42) kód különböző, és az első és harmadik, illetve a második és negyedik kódátalakítások közül legalább az első és a harmadik vagy a második és a negyedik kódátalakítások eltérőek.

2. Az 1. igénypont szerinti eljárás, *azzal jellemezve,* hogy az első kódátalakítás eltér a harmadik kódátalakítástól, ugyanakkor a második kódátalakítás megegyezik a negyedik kódátalakítással.

3. Az 1. igénypont szerinti eljárás, *azzal jellemezve,* hogy a második kódátalakítás eltér a negyedik kódátalakítástól, ugyanakkor az első kódátalakítás megegyezik a harmadik kódátalakítással.

4. Az 1. igénypont szerinti eljárás, *azzal jellemezve,* hogy az első kódátalakítás eltér a harmadik kódátalakítástól, és a második kódátalakítás is eltér a negyedik kódátalakítástól.

5. Az 1., 2., 3. vagy 4. igénypont szerinti eljárás, *azzal jellemezve,* hogy a kódátalakítások közül legalább egyet az adathordozón tárolt ötödik kódtól függően hajtunk végre.

6. Rendszer azonos adathordozóval különböző azonosítási eljárások végrehajtására, ahol az adathordozón legalább egy kód van tárolva, mely rendszer egy első azonosítási eljárás esetében el van látva:
- az adathordozón tárolt első kód és egy felhasználótól származó második kód vételére első vevőegységgel,
- a következő kódátalakítások közül legalább egynek a végrehajtására első kódátalakítóval,
  - az első kódnak átalakított első kóddá való első átalakítása, és
  - a második kódnak átalakított második kóddá való második kódátalakítása,
- az első azonosítási eljárás lezárására válaszképp kódok összehasonlítására első összehasonlító egységgel,

és amely rendszer egy második azonosítási eljárás esetében el van látva:
- az adathordozón tárolt harmadik kód és egy felhasználótól származó negyedik kód vételére második vevőegységgel,
- a következő kódátalakítások közül legalább egynek a végrehajtására második kódátalakítóval,
  - a harmadik kódnak átalakított harmadik kóddá való harmadik átalakítása, és
  - a negyedik kódnak átalakított negyedik kóddá való negyedik kódátalakítása,
- a második azonosítási eljárás lezárására válaszképp kódok összehasonlítására második összehasonlító egységgel.

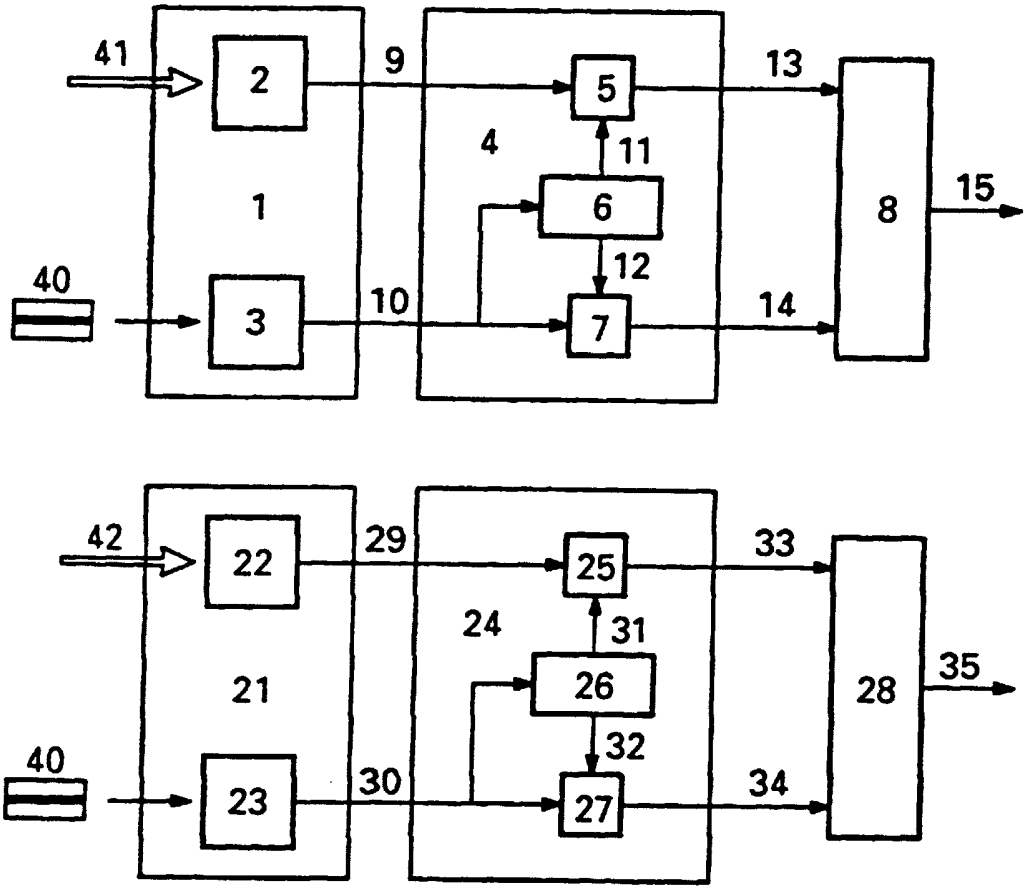
azzal jellemezve, hogy az első kód (40) és a harmadik kód (40) egyenlőek, míg a második kód (41) és a negyedik kód (42) különbözőek, és az első és harmadik, illetve a második és negyedik kódátalakítások közül legalább az első és a harmadik vagy a második és a negyedik kódátalakítások eltérőek.

7. A 6. igénypont szerinti rendszer, *azzal jellemezve,* hogy az első kódátalakítás eltér a harmadik kódátalakítástól, ugyanakkor a második kódátalakítás megegyezik a negyedik kódátalakítással.

8. A 6. igénypont szerinti rendszer, *azzal jellemezve,* hogy a második kódátalakítás eltér a negyedik kódátalakítástól, ugyanakkor az első kódátalakítás megegyezik a harmadik kódátalakítással.

9. A 6. igénypont szerinti rendszer, *azzal jellemezve,* hogy az első kódátalakítás eltér a harmadik kódátalakítástól, és a második kódátalakítás is eltér a negyedik kódátalakítástól.

10. A 6., 7., 8. vagy 9. igénypont szerinti rendszer, *azzal jellemezve,* hogy a kódátalakítások közül legalább egyet az adathordozón tárolt ötödik kódtól függően hajtunk végre.



1. ÁBRA

Kiadja a Magyar Szabadalmi Hivatal, Budapest
A kiadásért felel: Törőcsik Zsuzsanna főosztályvezető-helyettes
Windor Bt., Budapest