(19) Országkód

HU

MAGYAR KÖZTÁRSASÁG

MAGYAR SZABADALMI HIVATAL

SZABADALMI LEÍRÁS

(11) Lajstromszám:

220 210 B

(21) A bejelentés ügyszáma: P 99 03552
(22) A bejelentés napja: 1996. 11. 14.
(30) Elsőbbségi adatok:
1001659 1995. 11. 15. NL
(86) Nemzetközi bejelentési szám: PCT/EP 96/05028
(87) Nemzetközi közzétételi szám: WO 97/18537

(51) Int. Cl.[7]

G 07 F 7/10

(40) A közzététel napja: 2000. 02. 28.
(45) A megadás meghirdetésének dátuma a Szabadalmi Közlönyben: 2001. 11. 28.

(72) Feltalálók:
Pieterse, Rob; Aerdenhout (NL)
Rombaut, Willem; Hága (NL)

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

(74) Képviselő:
Kis Kovács Ferencné, DANUBIA Szabadalmi és Védjegy Iroda Kft., Budapest

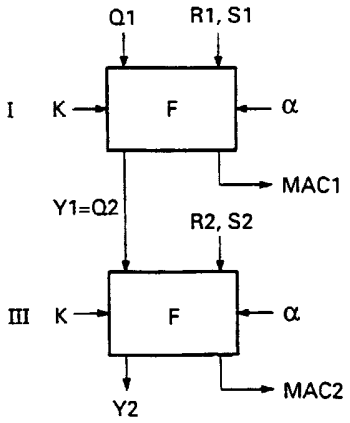
(54) Eljárás tranzakció védett módon történő végrehajtására

KIVONAT

A találmány tárgya eljárás tranzakció védett módon történő végrehajtására, amelyhez elektronikus fizetőeszközt és fizetési állomást alkalmazunk, ahol az eljárás során

- egy kezdeti lépést (I) hajtunk végre, amelynek során:
  - a fizetési állomásról egy első véletlen számot (R1) a fizetőeszközre viszünk át,
  - a fizetőeszközről az említett első véletlen számra (R1) reagálva a fizetési állomásra első hitelesítőkódot (MAC1) viszünk át, amely hitelesítőkódot előre meghatározott folyamat alkalmazásával legalább egy első kezdeti érték (Q1), az első véletlen szám (R1) és egy, a fizetőeszköznek egy első tranzakcióadata alapján határozzuk meg,
- egy további lépést (III) hajtunk végre, amelynek során:
  - adott esetben a fizetési állomásról a fizetőeszközre egy második véletlen számot (R2) viszünk át,
  - a fizetőeszközről a fizetési állomásra egy második hitelesítőkódot (MAC2) viszünk át, amely második hitelesítőkódot az említett folyamat alkalmazásával legalább egy második kezdeti érték (Q2), a második véletlen szám (R2) és a fizetőeszköznek egy második tranzakcióadata alapján határozzuk meg,

ahol a találmány szerint a kezdeti lépés során a folyamat segítségével továbbá egy első végértéket (Y1) állítunk elő, ahol a második kezdeti érték (Q2) az első végértéken (Y1) alapul.



3. ábra

HU 220 210 B

A találmány tárgya eljárás tranzakció védett módon történő végrehajtására, amelyhez elektronikus fizetőeszközt és fizetési állomást alkalmazunk, és az eljárás során egy kezdeti lépést hajtunk végre, amelynek során a fizetési állomásról egy első véletlen számot a fizetőeszközre viszünk át, a fizetőeszközről az említett első véletlen számra reagálva a fizetési állomásra első hitelesítőkódot viszünk át, amely hitelesítőkódot egy előre meghatározott folyamat alkalmazásával legalább egy első kezdeti érték, az első véletlen szám és egy, a fizetőeszköznek egy első tranzakcióadata alapján határozzuk meg, egy további lépést hajtunk végre, amelynek során a fizetési állomásról a fizetőeszközre egy második véletlen számot viszünk át, a fizetőeszközről a fizetési állomásra egy második hitelesítőkódot viszünk át, amely második hitelesítőkódot az említett folyamat alkalmazásával legalább egy második kezdeti érték, a második véletlen szám és a fizetőeszköznek egy második tranzakcióadata alapján határozzuk meg.

A találmány különösen, de nem kizárólag előre kifizetett elektronikus fizetőkártya (előfizetett kártya) védett módon történő terhelésére szolgál, amilyen előre kifizetett elektronikus fizetőkártyát például a telefonfülkékben alkalmaznak. A jelen leírásban a fizetőeszköz fogalmát a speciális fizetőeszköz alakjától és típusától elvonatkoztatva alkalmazzuk. A fizetőeszközt így tehát például újratölthető kártya (azaz olyan fizetőkártya, amelynek egyenlege megnövelhető) vagy nem kártya alakú elektronikus fizetőeszköz képezheti.

Az utóbbi években az elektronikus fizetőeszközök egyre nagyobb mértékben terjedtek el, nemcsak a nyilvános telefonfülkék használatáért történő fizetésre, hanem számos más fizetési célra is. Mivel az ilyen fizetőeszközök általában pénzösszeget képviselő egyenleget (hitelt) tartalmaznak, szükséges, hogy az ilyen fizetőeszközök és a fizetési állomás (mint például elektronikus fizetéssel működő távbeszélő készülékek vagy elektronikus pénztár) közötti adatcserét védett eljárás (fizetési jegyzőkönyv) segítségével kell lebonyolítani. Ebben az esetben biztosítani kell, hogy például a fizetőeszközt terhelő összeg (pénzösszeg vagy számítási egységek száma) máshol hitelezett összegnek (pénzösszeg vagy számítási egységek) feleljen meg: a felhasználó által fizetett összegnek az ellátó által fogadott összegnek kell megfelelnie. A hitelezett összeg tárolható, például a fizetési állomáson jelen lévő védett modulban.

A technika állásához tartozó fizetési eljárások, mint amilyet például az EP 0 637 004 lajstromszámú európai szabadalmi bejelentés ismertet, magukba foglalnak: egy első lépést, amelynek során a fizetési állomás által a fizetőeszköz egyenlegét keressük vissza; egy második lépést, amelynek során a fizetőeszköz egyenlegét csökkentjük (a fizetőeszköz terhelése); és egy harmadik lépést, amelynek során a fizetőeszköz egyenlegének újbóli visszakeresését hajtjuk végre. Az első és a harmadik lépés során megállapított egyenlegek különbsége alapján meghatározható a terhelt összeg és ezáltal a fizetési állomáson hitelezendő összeg. Csalások megelőzése érdekében az első lépésben véletlen számot alkalmazunk, amelyet a fizetési állomás által állítunk elő, és ezt a véletlen számot a fizetőeszközre visszük át. Az első véletlen szám alapján a fizetőeszköz első válaszként egy hitelesítőkódot állít elő, amely többek között a véletlen szám és az egyenleg (például kriptográfiailag) feldolgozott alakját tartalmazhatja. Eltérő véletlen számoknak az egyes tranzakciókhoz való alkalmazásával megelőzhető, hogy a tranzakciót visszajátszással utánozzák. Ezenkívül a harmadik lépés alatt második véletlen számot alkalmaznak, amelyet szintén a fizetési állomás állít elő és juttat a fizetőeszközhöz. A második véletlen szám alapján a fizetőeszköz második válaszként egy második és új hitelesítőkódot állít elő, amely többek közt a második véletlen szám és az új egyenleg feldolgozott alakját tartalmazhatja. A két átvitt egyenleg közötti különbség alapján a fizetési állomás (vagy a fizetési állomásnak egy védett modulja) meghatározza, hogy milyen összeget kell a fizetési állomás egyenlegének jóváírni.

Az ismertetett eljárás csalás ellen alapvetően jól véd, amennyiben a fizetőeszköz egyetlenegy fizetési állomással (vagy védett modullal) kommunikál. Az ismert megoldás hátránya viszont azon a tényen alapul, hogy az első és a második hitelesítőkód egymástól független. Amennyiben egy második vagy harmadik fizetési állomás (vagy védett modul) a fizetőeszközzel kommunikál, úgy az említett függetlenség miatt lehetséges, hogy az első lépés a második és harmadik lépéstől elkülönül. Ennek az a következménye, hogy a vonatkozó fizetőeszköz terhelése nélkül egy látszólag teljes tranzakció megy végbe. Magától értetődő, hogy ez nem kívánatos.

Az US 5 495 098 lajstromszámú szabadalmi leírás és a megfelelő EP 0 621 570 lajstromszámú szabadalmi bejelentés olyan megoldást ismertet, amelynél a fizetési állomás biztonsági moduljának azonosságát (identitását) használják fel annak biztosítása érdekében, hogy az adatcsere a kártya és csupán egyetlenegy végkészülék (terminál) között valósuljon meg. A biztonsági modul, az állomás és a kártya közötti adatcsere védése viszonylag bonyolult és külső kriptográfiai (titkosított) számításokat igényel.

Más ismert megoldások például az EP 0 223 213 és az EP 0 570 924 lajstromszámú bejelentésekben vannak leírva, viszont ezek a leírások sem tartalmaznak javaslatot a fentiekben említett problémák megoldására.

A találmány révén megoldandó feladat, hogy a technika állásához tartozó megoldások fentiekben ismertetett és más hátrányait kiküszöböljük, és olyan eljárást hozzunk létre, amely a terhelési tranzakció nagyobb fokú védelmét biztosítja. A találmány feladata különösen, hogy olyan eljárást hozzunk létre, amely biztosítja, hogy egy tranzakció alatt csak egyetlenegy fizetési állomással bonyolíthassuk le az ügyletet.

Ennek megfelelően a jelen találmány tranzakció végrehajtására olyan eljárást javasol, amelyhez elektronikus fizetőeszközt és fizetési állomást alkalmazunk, ahol az eljárás során ismételten lekérdezési lépést hajtunk végre, amelynek során a fizetési állomás a fizetőeszközt lekérdezi és válaszként a fizetőeszköztől adatot fogad, ahol a fizetőeszköz adata előre meghatározott folyamat által előállított hitelesítőkódot és ugyanennek a

tranzakciónak egy megelőző hitelesítőkóddal az említett folyamatállapotai által kapcsolatba hozott következő hitelesítőkódot tartalmaz.

A hitelesítőkódok közötti kapcsolat létrehozásával biztosítható, hogy a fizetési állomás által fogadott adatok erre az állomásra jellemző egyedi adatok legyenek. Annak érdekében, hogy a különböző lépések hitelesítőkódjait összekapcsoljuk, a folyamat egy lekérdezési lépésben az előző lekérdezési lépésben végrehajtott folyamat végső állapotából levezetett kezdeti értéket alkalmazza.

A jelen találmány tehát tranzakciók védett módon történő végrehajtására olyan eljárást javasol, amelyhez elektronikus fizetőeszközt és fizetési állomást alkalmazunk, ahol az eljárás során az alábbi lépéseket hajtjuk végre:

- egy kezdeti lépést hajtunk végre, amelynek során:
  - a fizetési állomásról egy első véletlen számot a fizetőeszközre viszünk át,
  - a fizetőeszközről az említett első véletlen számra reagálva a fizetési állomásra első hitelesítőkódot viszünk át, amely hitelesítőkódot előre meghatározott folyamat alkalmazásával legalább egy első kezdeti érték, az első véletlen szám és egy, a fizetőeszköznek egy első tranzakcióadata alapján határozzuk meg, és
- egy további lépést hajtunk végre, amelynek során:
  - adott esetben a fizetési állomásról a fizetőeszközre egy második véletlen számot viszünk át,
  - a fizetőeszközről a fizetési állomásra egy második hitelesítőkódot viszünk át, amely második hitelesítőkódot az említett folyamat alkalmazásával legalább egy második kezdeti érték, a második véletlen szám és a fizetőeszköznek egy második tranzakcióadata alapján határozzuk meg,

ahol a találmány szerint a kezdeti lépés során a folyamat segítségével továbbá egy első végértéket állítunk elő, ahol a második kezdeti érték az első végértéken alapul.

A találmány szerinti eljárás szempontjából így tehát lényeges, hogy a második kezdeti érték az első végértéken alapul.

Azáltal, hogy a második kezdeti érték az első végértéken alapul, azaz a folyamatnak az első azonosító kód összeállítását követő állapotán a kezdeti (első) lépés és a további lépések között közvetlen kapcsolatot hoztunk létre, az eljárás észrevétlenül történő megszakítására vagy más fizetési állomásokkal észrevétlenül történő adatcserére már nincs lehetőség. Ebben az esetben a második kezdeti érték, amely például egy kriptográfiai folyamatnak egy kezdeti vektorát képezheti, az első végértékkel azonos lehet, vagy az első végértékből lehet levezetve. Az első esetben az első végértéket tárolhatjuk, a második esetben a második kezdeti érték egy olyan folyamatnak a (kriptográfiai) állapotát képviselheti, amely folyamatot az első végértéktől kiindulva többször végrehajtottunk. Mindkét esetben a második kezdeti értéket az első végérték alapján reprodukálhatjuk, aminek köszönhetően a hitelesség ellenőrzése és így az eljárás folyamatossága is biztosítható.

Az eljárás során egy további (harmadik) lépésben egy második végértéket állíthatunk elő, amelyet lehetséges további lépések számára kezdeti értékek levezetésére használhatunk fel. Az eljárás opcionálisan a kezdeti és a további lépés között egy közbenső lépést is magában foglalhat, amelynek során a fizetési állomásról a fizetőeszközre egy parancsot viszünk át, és a fizetőeszköz egyenlegét a parancs alapján változtatjuk.

A találmány tehát azon a felismerésen alapul, hogy terhelési tranzakció egymást követő lépéseiben a hitelesítésre vonatkozó több független kezdeti érték alkalmazása lehetővé teszi, hogy a tranzakciónak ne az összes lépése kerüljön ugyanazon fizetőeszköz–fizetési állomás pár között végrehajtásra.

A találmány továbbá azt az előnyt biztosítja, hogy a találmány szerinti eljárást meglévő elektronikus fizetőeszközökben is alkalmazzuk.

A fentiekben olyan fizetési állomásra hivatkoztunk, amellyel a fizetőeszköz (kártya) kommunikál. A fizetőeszköz magában foglalhatja a tranzakcióadatokhoz való tárolót vagy egy különálló modult. A fizetőeszköz a gyakorlatban fizetési állomáson keresztül a védett modullal (biztonsági modul) kommunikálhat, abban az esetben, ha a fizetési állomás ilyen modult a tranzakcióadatok biztonságos tárolásához alkalmaz.

A találmányt az alábbiakban előnyös kiviteli példák kapcsán a mellékelt rajzra való hivatkozással részletesebben is ismertetjük, ahol a rajzon az

- 1. ábrán olyan fizetési rendszer látható vázlatosan, amelyben a találmány alkalmazható, a
- 2. ábra vázlatosan olyan eljárást mutat, amelyben a találmány kerül alkalmazásra, a
- 3. ábra vázlatosan olyan eljárás további részleteit szemlélteti, amely eljárásban a találmány kerül alkalmazásra, a
- 4. ábrán a 3. ábra szerinti eljárásnak egy alternatív foganatosítási módja látható vázlatosan, és az
- 5. ábrán egy fizetőeszköz integrált áramköre látható vázlatosan, amely fizetőeszköz segítségével a találmány alkalmazható.

Az 1. ábrán vázlatosan látható, elektronikus fizetésre szolgáló 10 rendszernek egy kiviteli alakja, amely 11 fizetőeszközt, mint például úgynevezett chipkártyát vagy memóriakártyát, 12 fizetési állomást, első 13 fizetési intézményt és második 14 fizetési intézményt tartalmaz. A 12 fizetési állomás (terminál) az 1. ábrán pénztárgépként van bemutatva, de tartalmazhat például (nyilvános) telefonkészüléket is. A 13, 14 fizetési intézmények, amelyeket az 1. ábrán bankként jelöltünk, nem csak bankokat, hanem más intézményeket is képviselhetnek, amelyek fizetések teljesítésére szolgáló eszközökkel (számítógépekkel) rendelkeznek. A gyakorlatban a 13 és 14 fizetési intézmények egyetlenegy fizetési intézményt képezhetnek. A bemutatott kiviteli példa esetén a 11 fizetőeszköz hordozót és érintkezőkkel ellátott 15 integrált áramkört tartalmaz, amely áramkör tranzakciók lebonyolítására (fizetések teljesítése) alkalmasan van kiképezve. A 11 fizetőeszköz elektronikus pénztárcaként is ki lehet képezve.

A tranzakció során a 11 fizetőeszköz és a 12 fizetési állomás között PD1 fizetési adatok vonatkozásában adatcsere valósul meg. A 11 fizetőeszközhöz a 13 fizetési intézmény, a 12 fizetési állomáshoz pedig a 14 fizetési intézmény van társítva. A 13 és 14 fizetési intézmények között a tranzakció után PD2 fizetési adat cseréjével elszámolás valósul meg, ahol a PD2 fizetési adat a PD1 fizetési adatból van levezetve. A tranzakció során a 12 fizetési állomás és a 14 fizetési intézmény között az ügyre vonatkozóan lényegében nem valósul meg kommunikáció (úgynevezett offline rendszer). Ezért a tranzakciókat ellenőrzött feltételek mellett kell végrehajtani a rendszerrel való visszaélés megakadályozása érdekében. Az ilyen visszaélés például a 11 fizetőeszköz (kártya) egyenlegének növelése lehet, amely a 13 fizetési intézménynél lévő hozzárendelt számla egyenlegváltoztatásával nincs összhangban.

A 2. ábrán adatcserét szemléltetünk a kártyaként jelölt 11 fizetőeszköz (1. ábra) (annak integrált áramköre) és a terminálként jelölt 12 fizetési állomás (1. ábra) biztonsági modulja között, ahol az egymást követő eseményeket egymás alatt tüntettük fel.

Egy első I lépésben a terminál egy első R1 véletlen számot állít elő, és ezt a számot a kártyára viszi át. A kártya az R1 véletlen szám és más adat, előnyösen a kártya egy S1 egyenlegét magában foglaló tranzakcióadat alapján MAC1 hitelesítőkódot állít elő: MAC1= =F(R1, S1,...), ahol F funkció egy önmagában ismert kriptográfiai funkció lehet. Erre a későbbiekben a 3. és 4. ábra kapcsán még részletesebben is kitérünk. Az MAC1 hitelesítőkódot (Message Authentication Code) a terminálra visszük át legalább az S1 egyenleggel együtt. Az MAC1 hitelesítőkód ellenőrzését követően a terminál az S1 egyenleget rögzíti (feljegyzi).

Egy második II lépés alatt a terminál terhelési D parancsot állít elő, amely a kártya terhelésére szánt értéket (összeget) tartalmazza. A terhelő D parancsot a kártyára visszük át, ahol a kártya S1 egyenlegét a terhelendő összeggel csökkentjük, aminek eredményeként új S1 egyenleget kapunk. A II lépés végrehajtása a találmány szempontjából nem lényeges. A gyakorlatban a II lépés a 0-t is magában foglaló, tetszőleges számú alkalommal megismételhető.

Egy harmadik III lépésben a terminál egy második R2 véletlen számot állít elő, és ezt a kártyára viszi át. A kártya az R2 véletlen szám és új S2 egyenlegét is magában foglaló tranzakcióadatok alapján MAC2 hitelesítőkódot állít elő: MAC2=F(R2, S2,...), ahol F funkció egy önmagában ismert kriptográfiai funkció lehet. Az új S2 egyenleget és az MAC2 hitelesítőkódot a terminálra visszük át. A terminál az MAC2 hitelesítőkódot ellenőrzi, például a kódnak az R2 véletlen szám és S2 egyenleg felhasználásával történő regenerálásával és a regenerált és fogadott kód összehasonlításával. Alternatív módon a terminál az MAC2 kódot meg is fejtheti, hogy az R2 véletlen számot és az S2 egyenleget megállapítsa. Az ilyen megfejtés például az F funkció fordítottjának az alkalmazásával történhet.

Az MAC2 hitelesítőkód pozitív eredménnyel történő ellenőrzését követően a terminál az új S2 egyenleget rögzíti. Magától értetődő, hogy az egyenlegnek a terminálhoz való megismételt átvitele a jelen találmány esetében nem lényeges. Ezt figyelembe véve a kártya egyenlegének átvitelét magában foglaló lépés elhagyható és például a harmadik lépésben egy csökkenés visszaigazolásával helyettesíthető, ami után a csökkenés összege (ahogy a II lépés alatt a kártyára történő adatátvitel mutatja) a terminálban rögzítésre kerül. Az első és harmadik lépésben a kártya egyenlegéhez kiegészítésképpen vagy ehelyett a terminálra egy kártyaazonosítás vihető át.

Egy negyedik IV lépésben a terminálban az S1 és S2 egyenlegek közötti különbséget határozzuk meg és rögzítjük. Ezzel kapcsolatban megemlítendő, hogy az ilyen különbség vagy külön tárolható, vagy egy később teljesítendő meglévő összeghez (a fizetési állomás egyenlege) hozzáadható. Az említett negyedik IV lépés ugyanúgy, mint a lehetséges soron következő lépések, a találmány szempontjából nem lényegesek. A 2. ábrán bemutatott lépéseket egy hitelesítési vagy ellenőrzési lépés előzheti meg, amelynek során a hitelesítőkódok előállítására alkalmazandó kulcsot azonosítjuk. Célszerű, ha az egyes kártyacsoportokhoz vagy akár minden egyes kártyához különböző kulcsot alkalmazunk. Ez például a technika állásából ismert és a kártyaazonosítási számon alapuló, különböző kulcsváltozatok alkalmazásával történhet.

A fentiekben ismertetett diagramon az R1 és R2 véletlen számok különbözőek. Az R2 és R1 véletlen számok azonosak is lehetnek (R1=R2=R), úgyhogy a III lépés alatt ellenőrizhető, hogy az MAC2 hitelesítőkódban ugyanazt az R véletlen számot (R=R1) használtuk-e.

A technika állásának megfelelően az MAC1 és MAC2 hitelesítőkódok alapvetően egymástól függetlenek. Megemlítendő, hogy amennyiben az R1 és R2 véletlen számok különböznek, úgy az MAC1 és MAC2 hitelesítőkódok között nincs közvetlen vagy közvetett kapcsolat, mivel a folyamat (F funkció), amellyel a hitelesítőkódot határozzuk meg, mindenkor ugyanazt a kezdeti értéket feltételezi, éspedig a zéró kezdeti értéket. E miatt a függetlenség miatt alapvetően nincs garantálva, hogy az I lépés és a III lépés ugyanazon kártya és fizetési állomás között kerül végrehajtásra.

A találmány értelmében viszont a második MAC2 hitelesítőkód meghatározásakor feltételezünk egy olyan kezdeti értéket, amely az első MAC1 hitelesítőkód meghatározásának eredményeként képződik. Második kezdeti értékként például a (kriptográfiai) folyamatnak az első hitelesítőkód meghatározása utáni állapotát használhatjuk fel. Ezzel kapcsolatban nem lényeges, hogy a folyamat az első hitelesítőkód meghatározását követően egy meghatározott számú folyamatlépésen túl van-e már, mivel a második kezdeti érték függősége és reprodukálhatósága biztosítva van.

A kezdeti értékeknek az említett függősége a találmány értelmében biztosítja, hogy azon tranzakció összes lépése, amelyben a találmány szerinti eljárást alkalmazzuk, ugyanaz a kártya és ugyanaz a fizetési állomás között kerüljön végrehajtásra.

A kezdeti értékek közötti összefüggést az alábbiakban a 3. ábrára való hivatkozással ismertetjük rész-

letesebben, ahol az I és III lépések a 2. ábrán látható I és III lépésekkel azonosak lehetnek. Az I lépésben az első MAC1 hitelesítőkódot F funkció alkalmazásával állítjuk elő, ahol az F funkció egy önmagában ismert kriptográfiai funkció lehet, mint például az úgynevezett DES (Data Encription Standard) funkció vagy egy viszonylag egyszerű kombinatorikus funkció (lásd 5. ábrát is) vagy tördelő függvény (Hash funkció) lehet. Ez az F funkció bemeneti paraméterekként az első R1 véletlenszámot, az első (régi) S1 egyenleget, egy K kulcsot és egy első Q1 kezdeti értéket tartalmaz. Opcionálisan bemeneti paraméterként egy terhelő parancs azonosítása (ahogy a II lépésben kerül alkalmazásra) is alkalmazható. A folyamat vezérlésére α órajel alkalmazható, amely az 5. ábrán bemutatott α órajellel azonos lehet.

Az első Q1 kezdeti érték (kezdeti vektor) nullával vagy egy másik előre megadott kezdeti értékkel lehet egyenlő, ha az F funkciót alkalmazó folyamat korábban, a kártya aktiválása előtt (az aktiválás a kártyának a terminálba való behelyezésével történhet) nem valósult meg.

Az F funkció MAC1 hitelesítőkódot állít elő. Ezenkívül az F funkció állapota első Y1 végértékként is rögzítve van. Az első Y1 végérték később a III lépésben második Q2 kezdeti értékként (Q2=Y1) kerül felhasználásra, így valósul meg az I és a III lépés összekapcsolása.

A III lépésben F funkció felhasználásával a második MAC2 hitelesítőkódot állítjuk elő, ahol ez az F funkció előnyösen az I lépésben alkalmazott F funkcióval azonos. Ebben az esetben az F funkció bemeneti paramétereit a második R2 véletlen szám, a második (új) S2 egyenleg, a K kulcs és a második Q2 kezdeti érték képezi. Az F funkció a második MAC2 hitelesítőkódot szolgáltatja és járulékosan a második Y2 végértéket, amely az F funkciónak a folyamat utáni állapotát képviseli. A második Y2 végérték elmenthető, hogy harmadik Q3 kezdeti értékként abban az esetben kerülhessen alkalmazásra, amennyiben ugyanezt a kártyát és biztonsági modult (terminált) alkalmazva harmadik MAC3 hitelesítőkódra van szükség. Általában a kártya deaktiválása (például a kártyának a terminálból való eltávolítása) ahhoz vezet, hogy az aktuális végérték (például Y2) elvész. Ez biztosítja a tranzakció egyediségét.

A 4. ábrán azt az esetet szemléltetjük, amelynél az F funkció feldolgozása a II és a III lépés között α órajel vezérlésével történik. Az I lépés eredményeként MAC1 hitelesítőkódot és egy első Y1 végértéket nyerünk, ahogy a 3. ábrán feltüntettük. Ez az Y1 végérték az F funkció bemeneti paraméterét kezdeti értékként képezi. Ahogy a fentiekben ismertettük, az Y1 végérték az F funkciónak az MAC1 hitelesítőkód előállítása utáni állapotát képviseli, így ha a funkció feldolgozása folytatódik, az említett állapot kezdeti értékként vehető figyelembe. A 4. ábrán a II lépésben F' funkció van jelölve, amely az R1 véletlen szám, az S1 egyenleg és a K kulcs által képzett bemeneti paraméterekkel nem rendelkezik.

A III lépésben az F' funkció állapotát (végértékét) Q2 kezdeti értékként alkalmazzuk. Ezt követően az F funkció és az R2 véletlen szám, az S2 egyenleg és a K kulcs bemeneti paraméterek felhasználásával MAC2 hitelesítőkódot állítunk elő.

A 4. ábra szerinti példa esetén a Q2 kezdeti érték az Y1 végértékkel nem azonos, viszont a Q2 kezdeti érték és Y1 végérték az F' funkció révén egymással összefüggésben állnak. Ez lehetővé teszi, hogy az I és a III lépés közötti kapcsolatot (megfelelést) ellenőrizzük.

Magától értetődő, hogy a 3. és 4. ábra szerinti lépéseket mind a kártyában, mind a terminálban (a terminál biztonsági moduljában) hajtjuk végre, azaz mind a kártya, mind a terminál állítja elő az MAC1 és MAC2 hitelesítőkódot, ahogy a 3. vagy 4. ábrán látható. A fogadott kódnak a terminálban előállított párjával való összehasonlítása révén lehetővé válik, hogy a terminál a fogadott adat hitelességét megállapítsa, és biztosítsa, hogy a tranzakcióban kizárólag egyetlenegy kártya vegyen részt.

Az 5. ábra alapján az alábbiakban ismertetjük, hogy hogyan alkalmazható a találmány szerinti eljárás a hagyományos, rendelkezésre álló fizetőkártyákban.

Az 5. ábrán látható és alapvetően az 1. ábra szerinti 11 fizetőeszközben lévő 15 integrált áramkörnek megfelelő 100 integrált áramkör első 101 memóriát és 102 címregisztert tartalmaz. A 101 memória számos memóriahellyel rendelkezik, amelyeket a számlálóként kialakított 102 címregiszter segítségével címzünk meg. Egy, a 11 fizetőeszközön kívül előállított α órajel hatására a 102 címregiszter egy címtartományon fut végig. A 101 memória úgynevezett EPROM memóriaként vagy EEPROM memóriaként van kiképezve, és (külső) R/W olvasó-író jelek hatására opcionálisan írható vagy olvasható. Az adatoknak, például az S1, S2 egyenlegeknek stb. a 100 integrált áramkör más részeivel való adatcseréje 103 adatbuszon keresztül történik.

Egy második 104 memória visszacsatolással ellátott léptetőregiszterként van kiképezve, sok esetben a 104 memória dinamikus memóriaként van kiképezve, aminek következtében a memóriában tárolt információ elvész, ha az említett információt rendszeresen fel nem frissítik. Erre a pontra a későbbiekben még részletesebben is kitérünk. Az R véletlen szám (ideiglenesen) egy (opcionális) 105 regiszterben tárolható. Mind az R véletlen szám, mind az S egyenleg a 105 regiszterből, illetve a 101 memóriából egy opcionális 106 kombinációs áramkör (logikai áramkör) útján a második 104 memóriába van bevezetve. A kombinációba (kapcsolatba) természetesen további paraméterek, mint például a 101 memóriában tárolt K kulcs is bevonhatók. A 104 memória (léptetőregiszter) (visszacsatolt) kimenetén MAC (azaz MAC1, MAC2,...) hitelesítőkódok jelennek meg, amelyek az S egyenleg, az R véletlen szám és esetlegesen más paraméterek, mint például azonosító kód (például kártyaszám), K kulcs és hasonlók rejtjelezett kombinációjaként kerülnek előállításra. A visszacsatolás több 2-modulusú összegző és a 106 kombinációs áramkör útján van megvalósítva. A 104 memória és a 106 kombinációs áramkör és az erre csatlakoztatott összegzők a 3. és 4. ábra szerinti F és F' funkciókat képezik.

A gyakorlatban a 100 integrált áramkör számos más részt is tartalmazhat, amelyek viszont a jelen találmány szempontjából nem játszanak lényeges szerepet.

A meglévő eljárások és azok megvalósítása esetén az a probléma merül fel, hogy az adatnak (ebben az esetben egyenleg) a 101 memóriába (EEPROM) való beírásához viszonylag hosszú írási idő szükséges, például legalább 5 ms. Az írás során a memóriába órajel és írójelek kerülnek betáplálásra (az α órajel és az R/W olvasó-író jelek). Meglévő fizetőkártyák esetén az EEPROM memóriába való beírás során nincs lehetőség arra, hogy a 100 integrált áramkör más részeihez más órajelet juttassunk. Ennek következtében a dinamikus 104 memóriatartalma elvész, mivel ebbe a memóriába a memóriatartalom felfrissítése céljából rendszeresen és rövid időintervallumokban, például legalább 0,1 ms-os időintervallumokban, órajelet kell juttatni. Az egyenlegnek az EEPROM-ként kialakított 101 memóriába (a 2. ábrán a II lépés alatt) való beírását követően ezért a dinamikus 104 memória tartalma elvész, és ezt a memóriát a memória meghatározott kezdeti állapotának beállítása érdekében visszaállításnak kell alávetni. Ez a visszaállítás a 104 memória bemenetére juttatott 0-sorozatok (vagy 1-sorozatok) segítségével történhet. Erre a célra a 106 kombinációs áramkör úgy lehet kialakítva, hogy kimenetén, egy meghatározott vezérlőjel alapján, kizárólag 0-kat (vagy 1-eket) bocsát ki.

A 104 memória visszaállításának az a hátránya, hogy ezáltal az eljárás korábbi lépéseire (a 2. ábrán az I lépés) vonatkozó információ elvész. A találmány szerint a 104 memóriában lévő információ viszont megmarad. Ezt előnyösen azzal érjük el, hogy az adatoknak az EEPROM-ként kialakított 101 memóriába való beírását oly módon valósítjuk meg, hogy a dinamikus 104 memóriának és lehetséges más dinamikus memóriaelemeknek, például a 105 regiszternek a felfrissítési folyamatát nem zavarjuk. Ennek érdekében az α órajel frekvenciáját mindenkor olyan értéken tartjuk, amely a dinamikus memóriák felfrissítését nem veszélyezteti. Az alkalmazott dinamikus memóriaelemektől függően az ütemfrekvencia előnyösen például legalább 100 kHz-et tesz ki. Mivel az impulzustartam (óraimpulzus-időtartam) az ilyen ütemfrekvenciával történő írás során túl alacsony (például 0,05 ms 100 kHz esetén, miközben a bizonyos EEPROM memória esetén legalább 5 ms-ot kitevő impulzustartam szükséges), az írást ismétlődően hajtjuk végre. Másképpen kifejezve, ugyanazt az értéket (egyenleget) a 101 memóriának ugyanarra a címére többször írjuk, amíg végül a teljes előírt időtartamot el nem érjük. Az adott példa esetén, amelynél az ütemfrekvencia 100 kHz és a minimális írási idő 5 ms, ez azt jelenti, hogy legalább százszor kell ugyanarra a címre írásműveletet végrehajtani.

A fentiekben említett ismételt írásművelet bonyolult lehet, jóllehet számos meglévő fizetőkártyában a címregiszter eggyel növekszik (vagy csökken) minden egyes óraimpulzus hatására. Az aktuális írás így tehát a sok cím közül csupán egyre történhet, úgyhogy a teljes címtartományon mindenkor végig kell futni, hogy egy (viszonylag rövid) óraimpulzus alatt írhassunk. Ennek az a következménye, hogy az íráshoz szükséges időtartam növekszik.

Ennek megoldására a találmánynak egy további gondolata szerint úgy járunk el, hogy az α órajel frekvenciáját oly módon változtatjuk, hogy a címregiszteren való végigfutás során és így az írójel távolléte esetén az α órajel frekvenciáját a végigfutás gyorsítása érdekében megnöveljük, majd közvetlenül az írás előtt vagy az írás alatt az ütemfrekvenciát csökkentjük, hogy az írásimpulzus hosszabb ideig tarthasson. Magától értetődő, hogy az ütemfrekvencia csak olyan mértékben csökkenthető, amely mértéket a dinamikus memória szükséges felfrissítése megenged.

Ezenkívül az órajel alakja előnyösen úgy választható meg (állítható be), hogy az I/O viszont ne legyen 50/50, hanem például 70/30 vagy 90/10. Ennek eredményeként hosszabb írásimpulzust nyerünk (amennyiben az írást eggyel egyenlő órajellel hajtjuk végre) és így a teljes írási idő rövidebbé válik anélkül, hogy a dinamikus memória felfrissítési műveletét zavarná.

Az óraimpulzus alakjának beállítását előnyösen az ütemfrekvencia változtatásával kombinálhatjuk. Ezenkívül a címregiszter előnyösen úgy lehet kiképezve, hogy ne állítson elő több különböző címet, mint amennyi feltétlenül szükséges. A lehetséges címek számának korlátozásával a címregiszteren való végigfutáshoz szükséges idő hatásosan korlátozható.

Ahogy a fentiekben kifejtettük, a találmány azon a tényen alapul, hogy az eljárás különböző lépései között hitelesítő információ nem vész el. Erre a célra biztosítva van, hogy a dinamikus regiszterek és memóriák tartalmukat megőrzik azon időtartamon keresztül is, amikor viszonylag hosszú írási időt igénylő memóriába, mint például EEPROM memóriába írunk.

A gyakorlatban az eljárás a fizetési állomáson, különösen a fizetési állomás úgynevezett kártyaolvasójában elrendezett szoftver alakjában valósítható meg.

Magától értetődő a szakterületen jártas szakember számára, hogy a találmány nem korlátozódik a bemutatott kiviteli példára, és hogy számos változat és módosítás lehetséges a találmány keretén belül. Így a találmány elvét a fentiekben fizetőeszköz terhelésére vonatkozóan ismertettük, jóllehet az ilyen elv fizetőeszköz számára végrehajtott jóváíráshoz (hitelnyújtáshoz) is alkalmazható.

SZABADALMI IGÉNYPONTOK

1. Eljárás tranzakció védett módon történő végrehajtására, amelyhez elektronikus fizetőeszközt (11) és fizetési állomást (12) alkalmazunk, és az eljárás során
   - egy kezdeti lépést (I) hajtunk végre, amelynek során:
     - a fizetési állomásról (12) egy első véletlen számot (R1) a fizetőeszközre (11) viszünk át,
     - a fizetőeszközről (11) az említett első véletlen számra (R1) reagálva a fizetési állomásra (12) első hitelesítőkódot (MAC1) viszünk át, amely hitelesítőkódot egy előre meghatározott folyamat alkalmazásával legalább egy első kezdeti érték (Q1), az első véletlen szám (R1) és egy, a fizető-

eszköznek (11) egy első tranzakcióadata alapján határozzuk meg,

– egy további lépést (III) hajtunk végre, amelynek során:

– adott esetben a fizetési állomásról (12) a fizetőeszközre (11) egy második véletlen számot (R2) viszünk át,

– a fizetőeszközről (11) a fizetési állomásra (12) egy második hitelesítőkódot (MAC2) viszünk át, amely második hitelesítőkódot az említett folyamat alkalmazásával legalább egy második kezdeti érték (Q2), a második véletlen szám (R2) és a fizetőeszköznek (11) egy második tranzakcióadata alapján határozzuk meg,

azzal jellemezve, hogy a kezdeti lépés (I) során a folyamat segítségével egy első végértéket (Y1) állítunk elő, ahol a második kezdeti érték (Q2) az első végértéken (Y1) alapul.

2. Az 1. igénypont szerinti eljárás, *azzal jellemezve,* hogy a második kezdeti érték (Q2) az első végértékkel (Y1) azonos.

3. Az 1. vagy 2. igénypont szerinti eljárás, *azzal jellemezve,* hogy hitelesítőkód (például MAC1) meghatározása során egy kulcsot (K) és/vagy egy azonosító kódot is figyelembe veszünk.

4. Az 1–3. igénypontok bármelyike szerinti eljárás, *azzal jellemezve,* hogy a kezdeti lépés (I) és a további lépések (III) között egy opcionális közbenső lépést (II) hajtunk végre, amelynek során

– a fizetési állomásról (12) a fizetőeszközre (11) parancsot (D) viszünk át, és a fizetőeszköz (11) egyenlegét a parancs (D) alapján változtatjuk.

5. Az 1–4. igénypontok bármelyike szerinti eljárás, *azzal jellemezve,* hogy az első véletlen szám (R1) és a második véletlen szám (R2) azonosak, ahol a fizetési állomásról (12) a fizetőeszközre (11) történő, a második véletlen szám (R2) átvitelét magában foglaló allépést kihagyjuk.

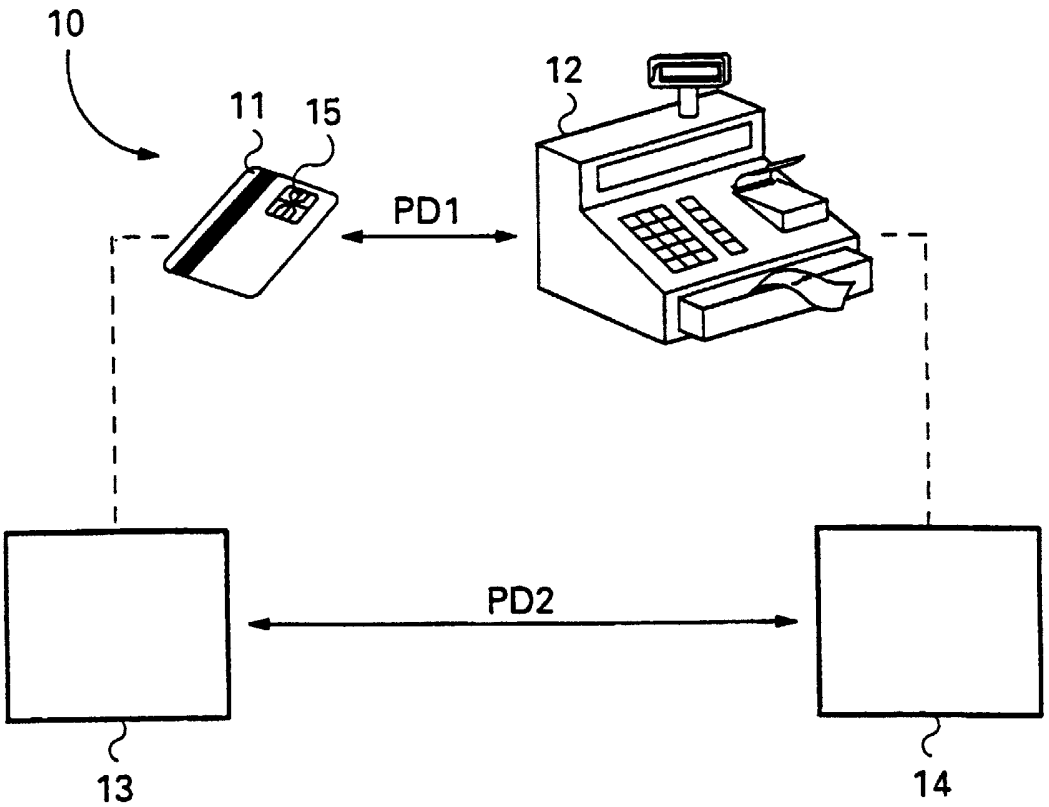
6. Az 1–5. igénypontok bármelyike szerinti eljárás, *azzal jellemezve,* hogy kriptográfiai funkciót (F) magában foglaló folyamatot alkalmazunk.

7. Az 1–6. igénypontok bármelyike szerinti eljárás, *azzal jellemezve,* hogy további negyedik lépést (IV) hajtunk végre, amelynek során:

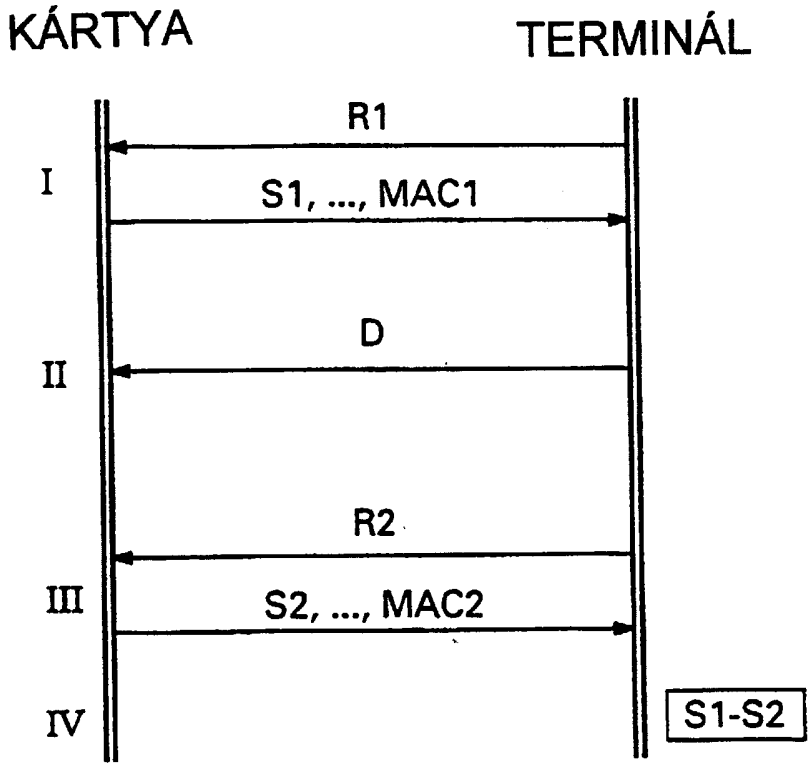
– a fizetési állomáson (12) az első és a harmadik lépés egyenlegei közötti különbséget (S1–S2) rögzítjük.

8. Az 1–7. igénypontok bármelyike szerinti eljárás, *azzal jellemezve,* hogy a harmadik lépést (III) ismételten végrehajtjuk.

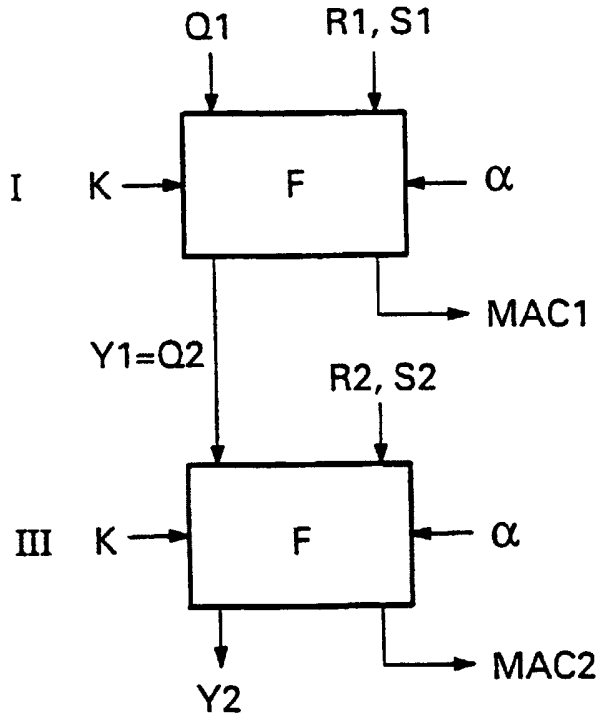
9. Az 1–8. igénypontok bármelyike szerinti eljárás, *azzal jellemezve,* hogy védett adatrögzítésre alkalmas modult tartalmazó fizetési állomást (12) alkalmazunk.



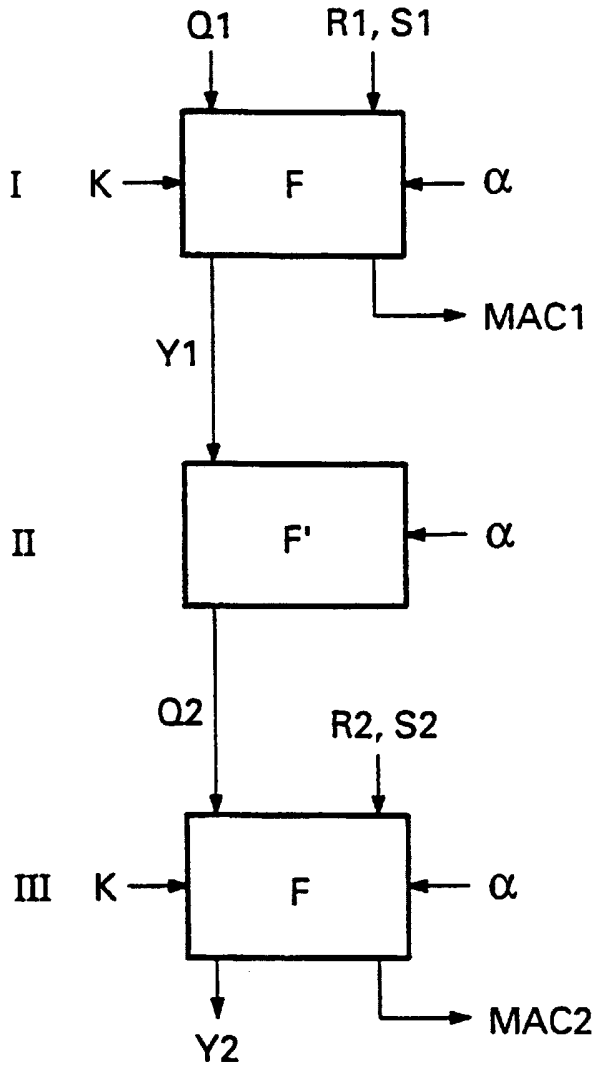
1. ÁBRA



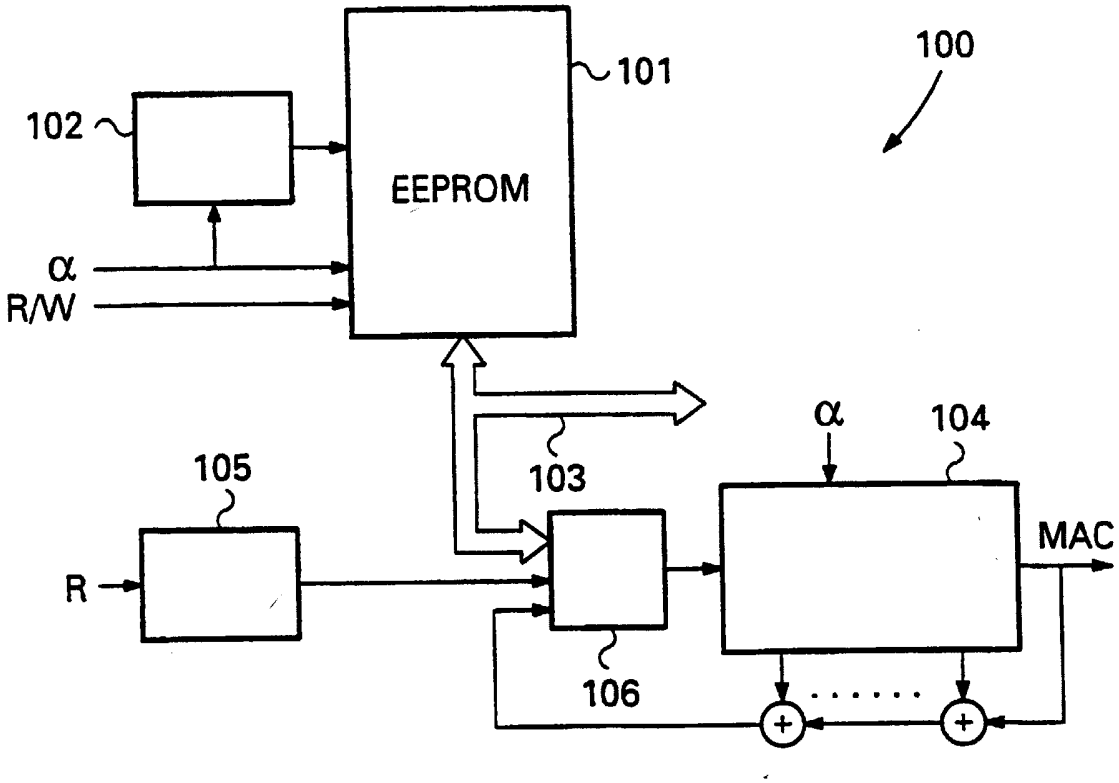
2. ÁBRA



3. ÁBRA



4. ÁBRA



5. ÁBRA

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