SLOVENSKÁ REPUBLIKA

(19) **SK**

ÚRAD
PRIEMYSELNÉHO
VLASTNÍCTVA
SLOVENSKEJ REPUBLIKY

ZVEREJNENÁ PRIHLÁŠKA VYNÁLEZU

(22) Dátum podania: 14.11.96

(31) Číslo prioritnej prihlášky: 1001659

(32) Dátum priority: 15.11.95

(33) Krajina priority: NL

(40) Dátum zverejnenia: 13.04.99

(86) Číslo PCT: PCT/EP96/05028, 14.11.96

(21) Číslo dokumentu:

600-98

(13) Druh dokumentu: **A3**

(51) Int. Cl.[6] :

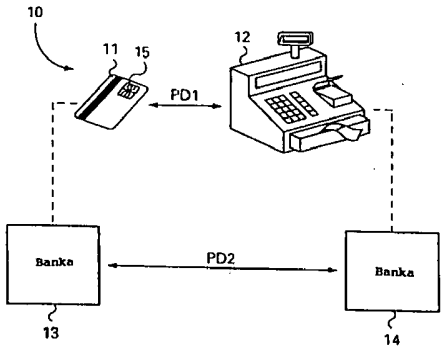
G 07F 7/10

(71) Prihlasovateľ: KONINKLIJKE PTT NEDERLAND N.V., The Hague, NL;

(72) Pôvodca vynálezu: Pieterse Rob, Aerdenhout, NL;
Rombaut Willem, The Hague, NL;

(54) Názov prihlášky vynálezu: **Spôsob debetovania elektronického platobného prostriedku**

(57) Anotácia:
Spôsob umožňuje ochranné debetovanie elektronického platobného prostriedku (11), napríklad telefónnej karty. V komunikačnom protokole medzi platobným prostriedkom (11) a platobným terminálom (12) sa používa proces overovania, ktorý identifikuje platobný prostriedok v priebehu rôznych krokov protokolu. Podľa tohto vynálezu sú overovacie kroky navzájom spriahnuté pomocou stavov (Y1, Q2) šifrovacieho procesu (F), aby sa dosiahla možnosť zistiť rušivý zásah do protokolu. Tento spôsob sa môže aplikovať na terajších platobných kartách s dynamickou pamäťou, pričom je zaistené, že obsah dynamickej pamäte, v ktorej je uložená informácia týkajúca sa overovania, sa počas protokolu nestratí.



PV 600-98

Spôsob debitovania elektronického platobného prostriedku

Oblasť techniky

Vynález sa týka spôsobu debitovania elektronického platobného prostriedku, napríklad elektronickej platobnej karty s integrovaným obvodom ("čipová karta"). Zvlášť sa potom vynález týka (nie však výhradne) spôsobu ochranného debitovania predplatených platobných kariet ("predplatené karty"), napríklad tých, ktoré sa používajú na telefonovanie z telefónnych búdok. V ďalšom texte sa výraz platobný prostriedok bude používať bez ohľadu na formu alebo typ konkrétneho platobného prostriedku. Platobným prostriedkom môže byť napríklad valorizovaná platobná karta (platobná karta, ktorej bilancia sa môže zvýšiť) alebo platobný prostriedok, ktorý nemá tvar platobnej karty.

Doterajší stav techniky

V posledných rokoch sa používanie platobných kariet stalo omnoho častejšie, a to nielen na platbu pri telefonovaní z verejných automatov, ale aj na iné platobné účely. Keďže taký platobný prostriedok obyčajne zahŕňa (kreditné) saldo, ktoré predstavuje peňažnú hodnotu, je nutné mať zaistenú výmenu dát medzi takým platobným prostriedkom a platobným terminálom (napríklad telefónnym prístrojom prispôsobeným na elektronickú platbu alebo elektronickou pokladňou), ktorá prebieha chráneným spôsobom (podľa platobného protokolu). Malo by byť napríklad zaistené, aby každá čiastka (peňažná hodnota alebo kalkulačná čiastka), debitovaná platobnému prostriedku, zodpovedala čiastke (peňažnej hodnote alebo kalkulačnej čiastke) kreditovanej inde: čiastka platená zákazníkom by mala zodpovedať čiastke prijatej dodávateľom. Kreditovaná čiastka by mala byť uložená napríklad v chránenom module umiestnenom v platobnom termináli.

Spôsoby platenia podľa doterajšieho stavu techniky, tak ako sú uvedené v európskej patentovej prihláške EP 0637004,

zahŕňajú: prvý krok, v ktorom je saldo platobného prostriedku vyhľadané platobným terminálom; druhý krok, v ktorom je saldo platobného prostriedku znížené (debitovanie platobného prostriedku); tretí krok, v ktorom je saldo platobného prostriedku opäť vyhľadané. Z rozdielu medzi saldom v prvom kroku a treťom kroku možno stanoviť debitovanú čiastku a tým aj čiastku kreditovanú v platobnom termináli. Aby sa zabránilo možnému podvodu, používa sa v prvom kroku náhodné číslo generované platobným terminálom, ktoré je následne prenesené na platobný prostriedok. Na základe prvého náhodného čísla platobný prostriedok generuje ako prvú odozvu overovací kód, ktorý môže zahŕňať (zašifrovane) spracovaný tvar, okrem iného, náhodného čísla a salda. Použitím rôzneho náhodného čísla pre každú transakciu je zabránené tomu, aby transakcia mohla byť imitovaná opätovnou realizáciou. Okrem toho sa v treťom kroku používa druhé náhodné číslo, ktoré sa rovnako generuje v platobnom termináli, a ktoré je prenášané na platobný prostriedok. Na základe druhého náhodného čísla platobný prostriedok generuje ako druhú odozvu druhý a nový overovací kód, ktorý môže zahŕňať spracovaný tvar, okrem iného, druhého náhodného čísla a nového salda. Podľa rozdielu medzi dvoma prenesenými saldami platobný terminál (alebo chránený modul platobného terminálu) stanoví, akou čiastkou má byť saldo platobného terminálu kreditované.

Uvedený známy spôsob platby je v podstate veľmi odolný proti podvodu, pokiaľ platobný prostriedok komunikuje s jedným platobným terminálom (alebo chráneným modulom). Nevýhoda známeho spôsobu spočíva v tom, že prvý a druhý overovací kód sú navzájom nezávislé. Ak s platobným terminálom komunikuje druhý alebo tretí platobný terminál, potom je možné vplyvom uvedenej nezávislosti oddeliť prvý krok od druhého a tretieho kroku. Výsledkom môže byť realizácia zdanlivo úplnej transakcie bez toho, aby došlo k debitovaniu platobného prostriedku. Tento spôsob transakcie je pochopiteľne nežiaduci.

Patent US 5495098 a zodpovedajúca európska patentová prihláška EP 0621570 uvádzajú spôsob, pri ktorom je na zaistenie ~~toho, aby výmena dát prebehla len medzi kartou a terminálom~~

toho, aby výmena dát prebehla len medzi kartou a terminálom, použitá identita bezpečnostného modulu platobného terminálu. Ochrana výmeny dát medzi bezpečnostným bezpečnostným modulom, terminálom a kartou je pomerne komplikovaná záležitosť a vyžaduje si extenzívne šifrovacie výpočty.

Ďalšie spôsoby, podľa doterajšieho stavu techniky, sú uvedené v európskej patentovej prihláške EP 0223213 a EP 0570924, ale tieto dokumenty riešenie uvedeného problému neponúkajú.

Podstata vynálezu

Cieľom tohto vynálezu je vylúčiť uvedené a iné nedostatky doterajšieho stavu techniky a poskytnúť spôsob, ktorý ponúka dokonca vyšší stupeň ochrany debetnej transakcie. Zvlášť je potom cieľom tohto vynálezu poskytnúť spôsob, ktorý zaisťuje, že počas transakcie je kreditovaný len jeden terminál.

Tento vynález poskytuje spôsob vykonávania transakcie, ktorý používa elektronický platobný prostriedok a platobný terminál, pričom tento spôsob zahŕňa opakované vykonávanie dopytovacieho kroku, pri ktorom sa platobný terminál dopytuje platobného prostriedku a ako odozvu prijíma dáta platobného prostriedku, kedy platobný prostriedok zahŕňa overovací kód vytvorený vopred stanoveným procesom, kedy následný overovací kód je pripojený k predchádzajúcemu overovaciemu kódu rovnakej transakcie pomocou stavov uvedených procesov.

Poskytnutím spojenia medzi overovacími kódmi možno zaistiť, že dáta prijaté platobným terminálom budú pre terminál jednoznačné. Aby sa spojili overovacie kódy rôznych krokov, proces v dopytovacom kroku používa počiatočnú hodnotu odvodenú z konečného stavu procesu predchádzajúceho dopytovacieho kroku.

Tento vynález konkrétnejšie poskytuje spôsob chráneného vykonávania transakcií pri použití elektronických platobných prostriedkov a platobných terminálov, pričom tento spôsob zahŕňa:

- počiatočný krok, pri ktorom:

- platobný terminál prenáša prvú náhodnú hodnotu do platobného prostriedku,

- platobný prostriedok, ako odozva na uvedenú prvú náhodnú hodnotu, prenáša do platobného terminálu prvý overovací kód, kedy tento overovací kód je stanovený na základe aspoň prvej počiatočnej hodnoty, prvej náhodnej hodnoty a prvého dáta transakcie platobného prostriedku použitím vopred stanoveného procesu, pričom proces ďalej produkuje prvú konečnú hodnotu,
- ďalší krok, pri ktorom:

- platobný terminál prenáša druhú náhodnú hodnotu na platobný prostriedok,

- platobný prostriedok prenáša druhý overovací kód do platobného terminálu, pričom overovací kód je stanovený na základe aspoň druhej počiatočnej hodnoty, druhej náhodnej hodnote a druhých dát prenosu platobného prostriedku, ktorý tento proces používa, pričom druhá počiatočná hodnota je založená na prvej konečnej hodnote.

Spôsob podľa tohto vynálezu je charakterizovaný tým, že druhá počiatočná hodnota je založená na prvej konečnej hodnote.

Tým, že je druhá počiatočná hodnota založená na prvej konečnej hodnote, to znamená na stave procesu po dokončení prvého overovacieho kódu, získa sa priame spojenie medzi prvým krokom a zostávajúcimi krokmi, pričom už nie je nutné spôsob prerušovať alebo si vymieňať dáta s inými platobnými terminálmi bez toho, aby to bolo zaznamenané. Druhá počiatočná hodnota, ktorá môže napríklad tvoriť inicializačný vektor šifrovacieho procesu, môže byť identická s prvou konečnou hodnotou alebo môže byť odvodená z prvej konečnej hodnoty. V prvom prípade sa môže prvá konečná hodnota uložiť, v druhom prípade môže byť druhá počiatočná hodnota napríklad stavom (šifrovacieho) procesu, ktorý, ak začína od prvej konečnej hodnoty, sa môže niekoľkokrát opakovať. V oboch prípadoch môže byť druhá počiatočná hodnota obnovená z prvej konečnej hodnoty, výsledkom čoho je ponuka kontroly autenticity a pokračovania spôsobu.

Proces môže v ďalšom (treťom) kroku produkovať druhú konečnú hodnotu, ktorá sa môže použiť na odvodenie počiatočných

hodnôt ďalších možných krokov. Spôsob zahŕňa, a to nepovinne, medziľahlý krok, ktorý sa vykonáva medzi počiatočným a ďalším krokom, a v ktorom platobný terminál prenáša príkaz do platobného prostriedku, pričom sa mení saldo platobného prostriedku na základe uvedeného príkazu.

Vynález je založený na pochopení skutočnosti, že aplikácia niekoľkonásobných krokov pre autentizáciu následných krokov debetných transakcií vytvára za istých okolností možnosť nevykonávať všetky kroky transakcie medzi rovnakým párom platobného prostriedku a platobného terminálu.

Vynález ďalej poskytuje výhodnú možnosť realizácie uvedeného spôsobu pri existujúcich platobných prostriedkoch.

V uvedených dokumentoch je odkaz na platobný terminál, s ktorým platobný prostriedok (karta) komunikuje. Platobný terminál môže zahŕňať integrovanú pamäť dát transakcie alebo samostatný modul. Ľahko možno pochopiť, že platobný prostriedok môže v praxi komunikovať s chráneným modulom ("bezpečnostným modulom"), a to cez platobný terminál v prípade, že platobný terminál používa taký modul na bezpečné uloženie dát transakcie.

Prehľad obrázkov na výkrese

Vynález bude ďalej popísaný omnoho podrobnejšie s použitím výkresov, na ktorých:

obr.1 schematicky znázorňuje platobný systém, v ktorom sa môže tento vynález použiť,

obr.2 schematicky znázorňuje spôsob aplikácie tohto vynálezu,

obr.3 schematicky znázorňuje ďalšie podrobnosti spôsobu aplikácie tohto vynálezu,

obr.4 schematicky znázorňuje alternatívne stvárnenie spôsobu z obr.3,

obr.5 schematicky znázorňuje integrovaný obvod platobného prostriedku, v ktorom sa tento vynález môže použiť.

obr.5 schematicky znázorňuje integrovaný obvod platobného prostriedku, v ktorom sa tento vynález môže použiť.

Príklady stvárnenia vynálezu

Systém 10 elektronických platieb, znázornený na obr.1 ako príklad, zahŕňa elektronický platobný prostriedok vo forme napríklad tzv. čipovej karty 11, ďalej platobný terminál 12 a prvú platobnú inštitúciu 13 a druhú platobnú inštitúciu 14. Platobným terminálom 12 na obr.1 je pokladňa, ale môže to takisto byť napríklad telefónny automat. Platobné inštitúcie 13 a 14, označené na obr.1 ako banky, nemusia byť len bankami, ale môžu to byť aj iné inštitúcie, ktoré majú k dispozícii prostriedky na zúčtovanie platieb. V praxi môžu inštitúcie 13 a 14 tvoriť jednu platobnú inštitúciu. Na zobrazenom príklade zahŕňa platobný prostriedok 11 podkladovú vrstvu a integrovaný obvod s kontaktmi 15, ktorý je konštruovaný na realizáciu platobných transakcií. Platobný prostriedok môže rovnako zahŕňať elektronickú schránku.

Medzi platobným prostriedkom 11 a platobným terminálom 12 existuje v priebehu transakcie výmena platobných dát PD1. Platobný prostriedok 11 je spojený s platobnou inštitúciou 13 a platobný terminál s platobnou inštitúciou 14. Medzi oboma inštitúciami 13 a 14 dochádza po vykonaní transakcie k zúčtovaniu na základe výmeny dát PD2, ktoré sú odvodené od platobných dát PD1. Počas transakcie v podstate nedochádza ku komunikácii medzi platobným terminálom 12 a platobnou inštitúciou 14 (tzv. off-line systém). Transakcia preto musí prebiehať za riadených podmienok, aby sa zaistilo, že systém nebude zneužívaný. K takému zneužívaniu môže napríklad dochádzať zvyšovaním salda na platobnom prostriedku (karte) 11, kedy saldo nesúhlasí so saldom na protiúčte platobnej inštitúcie 13.

Diagram na obr.2 znázorňuje výmenu dát medzi integrovaným obvodom platobného prostriedku, ktorý je označený ako "Karta" (11 na obr.1) a bezpečnostným modulom platobného terminálu,

ktorý je označený ako "Terminál" (12 na obr.1), pričom následné kroky sú zobrazené pod sebou.

V prvom kroku, označenom ako I, vytvára terminál prvé náhodné číslo R1 a prenáša toto číslo na kartu (medzikrok Ia). Na základe náhodného čísla R1 a iných dát, ktoré zahŕňajú napr. saldo karty S1, karta vytvorí overovací kód MAC1=F(R1, S1,...), kde F môže byť šifrovou funkciou. Toto bude ďalej vysvetlené s odkazom na obr.3 a 4. Kód MAC1 ("Message Authentication Code") je prenesený do terminálu spoločne aspoň so saldom S1 (medzikrok Ib). Po kontrole overovacieho kódu MAC1 terminál zaznamená saldo S1.

V druhom kroku, označenom ako II, vytvára terminál debetný príkaz D, ktorý obsahuje hodnotu (čiastku), ktorá má byť debitovaná na karte. Debetný príkaz D je prenesený na kartu, kde je saldo S1 znížené o debitovanú čiastku, výsledkom čoho je nové saldo S2. Vykonanie kroku II nie je pre vynález podstatné. V praxi sa krok II môže vykonať podľa ľubovôle niekoľkokrát (alebo vôbec).

V treťom kroku, označenom ako III, vytvára terminál druhé náhodné číslo R2 a prenáša ho na kartu (medzikrok IIIa). Na základe náhodného čísla R2 a iných dát, vrátane nového salda S2 na karte, vytvorí karta overovací kód MAC2=F(R2, S2,...), kde F môže byť šifrovou funkciou. Nové saldo a overovací kód MAC2 sa prenesie do terminálu (medzikrok IIIb). Terminál skontroluje overovací kód MAC2 napríklad novým generovaním kódu použitím R2 a S2 a porovnaním novo generovaného a prijatého kódu. Alternatívne môže terminál kód MAC2 dešifrovať a tým získať R2 a S2. Toto dešifrovanie sa môže realizovať vykonaním inverzie funkcie F. Po vykonaní kontroly kódu MAC2 s kladným výsledkom zaznamená terminál nové saldo S2. Rozumie sa, že opakovaný prenos sáld do terminálu nie je pre tento vynález podstatný. V tomto ohľade sa môže prenos salda karty vynechať a môže sa nahradiť napríklad potvrdením poklesu v treťom kroku, po ktorom je čiastka poklesu (prenášaná na kartu v kroku II) terminálom zaznamenaná. Identifikácia karty môže byť do terminálu zaslaná v prvom a treťom kroku, a to ako dodatok (alebo namiesto) salda karty.

V štvrtom kroku, označenom ako IV, je terminálom stanovený rozdiel sáld S1 a S2 a je tu zaznamenaný. Zistený rozdiel sa môže uložiť oddelene alebo sa môže pridať k existujúcej hodnote (saldu platobného terminálu) a zúčtovať neskôr. Uvedený štvrtý krok a možné ďalšie kroky nie sú pre realizáciu tohto vynálezu podstatné. Krokom, znázorneným na obr.2, môže predchádzať overovací krok, v ktorom sa identifikuje kľúč, ktorý sa použije na vytvorenie overovacích kódov. Pre každú dávku kariet, ale aj pre každú jednotlivú kartu, sa použije iný kľúč. Môže sa to realizovať pomocou diverzifikácie na základe čísla totožnosti a technických postupov, ktoré už odborníci dobre poznajú.

V diagrame, ktorý bol už popísaný, sú náhodné hodnoty R1 a R2 rôzne. Náhodné hodnoty R1 a R2 môžu byť rovnaké (R1=R2=R), čo znamená, že v kroku III sa môže kontrolovať, či sa v overovacom kóde MAC2 používa náhodné číslo R (=R1).

Podľa doterajšieho stavu techniky sú hodnoty overovacích kódov v podstate nezávislé. Je treba uviesť, že pokiaľ sa náhodné čísla R1 a R2 od seba líšia, neexistuje priamy a nepriamy vzťah medzi hodnotami MAC1 a MAC2, keďže proces (funkcia F), ktorým je overovací kód stanovený, vždy prijíma rovnakú počiatočnú hodnotu, menovite nulovú počiatočnú hodnotu. Vplyvom tejto nezávislosti tu neexistuje garancia, že krok I a III sa vykonáva medzi rovnakým párom karty a platobného terminálu.

Podľa tohto vynálezu je pri určovaní overovacieho kódu (MAC2) prijímaná počiatočná hodnota, ktorá je výsledkom stanovenia prvého overovacieho kódu (MAC1). Ako druhú počiatočnú hodnotu možno napríklad použiť stav (šifrovacieho) procesu po stanovení prvého overovacieho kódu. V tejto súvislosti nie je podstatné, či proces, po stanovení prvého overovacieho kódu, bude prechádzať počtom krokov procesu, keďže závislosť a reprodukovateľnosť druhej počiatočnej hodnoty bude zaručená.

Menovaná závislosť počiatočnej hodnoty, v súlade s vynálezom, zaručuje, že všetky kroky transakcie, v ktorých je spôsob fungovania podľa tohto vynálezu aplikovaný, sa uskutočnia medzi rovnakou kartou a rovnakým platobným terminálom.

Vzťah medzi počiatočnými hodnotami bude teraz vysvetlený s odkazom na obr.3, na ktorom môžu byť kroky I a III identické s krokmi I a III na obr.2. V kroku I je prvý overovací kód MAC1 generovaný použitím funkcie F, ktorá môže byť šifrovou funkciou, napríklad funkciou DES ("Data Encryption Standard"), alebo relatívne jednoduchšou kombinatorickou funkciou (viď tiež obr.5), alebo transformačnou "hašovacou" funkciou. Funkcia F má ako vstupné parametre prvú náhodnú hodnotu R1, prvé (staré) saldo S1, kľúč K a prvú počiatočnú hodnotu Q1. Ako vstupný parameter sa môže nepovinne použiť identifikácia debetného príkazu (použitého v kroku II). Hodinový impulz alfa, ktorý môže byť identický s impulzom na obr.5, je určený na riadenie procesu spracovania.

Prvá počiatočná hodnota (inicializačný vektor) Q1 sa môže rovnať nule alebo inej vopred nastavenej počiatočnej hodnote, ak sa nekonalo žiadne spracovávanie, zahŕňajúce funkciu F, a to pred aktiváciou karty (aktivácia sa môže vykonávať vložením karty do terminálu).

Funkcia F vytvára overovací kód MAC1. Dodatočne je stav (zostatkový) funkcie F uložený ako prvá konečná hodnota Y1. Prvá konečná hodnota Y1 bude neskôr použitá v kroku III ako druhá počiatočná hodnota Q2 (Q2=Y1), čím spája prvý a tretí krok.

V kroku III je generovaný druhý overovací kód MAC2 použitím funkcie F, ktorá je identická s funkciou F v kroku I. Funkcia F zahŕňa ako vstupné parametre druhú náhodnú hodnotu R2, druhé (nové) saldo S2, kľúč K a druhú počiatočnú hodnotu Q2. Funkcia F vytvára druhý overovací kód MAC2 a dodatočne druhú konečnú hodnotu Y2, ktorá je stavom funkcie F po spracovaní. Druhá konečná hodnota Y2 sa môže uložiť a použiť ako tretia počiatočná hodnota (Q3) v prípade, že sa vyžaduje tretí overovací kód MAC3 zahŕňajúci rovnakú kartu a bezpečnostný modul (terminál). Výsledkom dezaktivácie karty, vyňatím z terminálu, bude strata aktuálnej konečnej hodnoty (napríklad Y2). Táto skutočnosť je garantom jednoznačnosti transakcie.

Obr.4 znázorňuje prípad, v ktorom spracovávanie funkcie pokračuje medzi krokmi I a III, a to pri riadení hodinovým

impulzom alfa. Výsledkom kroku I je kód MAC1 a prvá konečná hodnota Y1, tak ako na obr.3. Táto konečná hodnota Y1 "vstupuje" do funkcie F' ako počiatočná hodnota. Ako to už bolo uvedené, je konečná hodnota Y1 stavom funkcie F po dokončení kódu MAC1, takže ak pokračuje funkcia F v spracovávaní, môže byť zmienený stav považovaný za počiatočnú hodnotu. Na obr.4 je funkcia F označená v kroku II ako F', keďže by funkcia nemusela prijať vstupné parametre R1, S1 a K.

V kroku III je stav (konečná hodnota) funkcie F' použitý ako počiatočná hodnota Q2. Následne je vytvorený kód MAC2 použitím F a vstupných parametrov R2, S2, K. V príklade na obr.4 nie je počiatočná hodnota Q2 identická s konečnou hodnotou Y1, hoci hodnoty Q2 a Y1 sú prostredníctvom hodnoty F' vo vzájomnom vzťahu. Umožňuje to kontrolu korešpondencie medzi krokmi I a III.

Je zrejmé, že kroky na obr.3 a 4 sa vykonávajú ako na karte, tak i v bezpečnostnom module terminálu. Znamená to, že karta aj terminál vytvárajú kódy MAC1 a MAC2, ako je to znázornené na obr.3 alebo 4. Porovnaním získaných kódov s ich náprotivkami vytvorenými v termináli je terminálu umožnené zistiť autenticitu prijatých dát a potvrdiť, že v transakcii je prítomná len jedna karta.

Na základe obr.5 bude ďalej vysvetlené, akým spôsobom môže byť spôsob realizácie, podľa tohto vynálezu, aplikovaný pri použití platobných kariet bežne dostupných na trhu.

Integrovaný obvod 100, schematicky znázornený na obr.5, ktorý v podstate zodpovedá integrovanému obvodu 15 platobného prostriedku 11 na obr.1, zahŕňa prvú pamäť 101 a adresový register 102. Pamäť 101 zahŕňa viac pamäťových miest, ktoré sú adresované pomocou adresového registra 102, ktorý je konštruovaný ako čítač. V odpovedi na hodinový impulz alfa, ktorý sa generuje mimo platobný prostriedok, prehľadáva adresový register 102 celý rozsah adries. Pamäť 101 je konštruovaná ako tzv. EPROM alebo EEPROM (meniteľná programovateľná permanentná pamäť - elektronicky mazateľná programovateľná permanentná pamäť), z ktorej sa môže, ako odpoveď na (vonkajšie) signály čítanie/zápis R/W, čítať a môže sa do nej aj zapisovať. Dáta,

napríklad saldá S1, S2 atď., sa vymieňajú pomocou dátovej zbernice 103 s ostatnými časťami integrovaného obvodu 100.

Druhá pamäť je konštruovaná ako posúvací register so spätnou väzbou. V mnohých prípadoch je táto pamäť tvorená dynamickou pamäťou, čo má za následok, že informácia uložená v pamäti sa stratí, ak nie je pravidelne aktualizovaná. Tento bod bude rozvedený neskôr. Náhodné číslo R sa môže ukladať (dočasne) v registri 105 (nepovinne). Do druhej pamäti 104 sa cez kombinačný obvod 106 z registra 105 a pamäti 101 ukladá ako náhodné číslo R, tak i saldo S. V kombinácii sa môžu vyskytovať aj iné parametre, napríklad kľúč K uložený v pamäti 101. Na výstupe (spätnej väzby) pamäti (posúvacieho registra) 104 vzniká overovací kód MAC (MAC1, MAC2), ktorý vznikol zo zakódovanej kombinácie salda S, náhodného čísla R a iných možných parametrov, napríklad identifikačného kódu (čísla karty), kľúča K a pod. Spätná väzba existuje vďaka množstvu sčítačov modulo-2 a kombinačného obvodu 106. Obvody 104 a 106 a k nim pripojené sčítače vytvárajú funkcie F a F'(obr.3 a 4).

V praxi môže integrovaný obvod 100 zahŕňať mnoho ďalších častí, ktoré nie sú pre fungovanie tohto vynálezu podstatné.

V prípade existujúcich spôsobov a ich implementácií vzniká problém v tom, že na zápis dát (v tomto prípade zápis sáld) do pamäti EPROM 101 sa požaduje pomerne dlhý čas zápisu, t.j. najmenej 5 ms. Počas zápisu sa dodávajú do pamäti hodinové a zápisové signály (znázornené ako signály α a R/W). V prípade existujúcich platobných kariet nie je možné počas zápisu do pamäti EEPROM dodávať do ostatných častí integrovaného obvodu 100 ďalší hodinový impulz. Výsledkom je strata obsahu dynamickej pamäti 104, keďže táto pamäť musí pravidelne a v rámci krátkeho časového intervalu, aspoň 0.1 ms, dostávať hodinový impulz, ktorý "osviežuje" obsah pamäti. Po zápise salda do pamäti EEPROM 101 (krok II na obr.2) sa obsah dynamickej pamäti 104 stratil a pamäť by mala byť resetovaná, aby sa dosiahol definovaný počiatočný stav pamäti. Návrat do pôvodného stavu sa môže uskutočniť zavedením série núl (alebo jednej) na vstup pamäti 104. Kombinačný obvod môže

byť na tento účel skonštruovaný tak, že na základe istých riadiacich signálov obvod pošle na svoj výstup len nuly.

Resetovanie pamäti 104 má však nevýhodu v tom, že informácia so vzťahom k predchádzajúcim krokom tohto spôsobu (krok I na obr.2) sa tým stráca. Podľa tohto vynálezu sa však informácia v pamäti 104 zachováva. Dosahuje sa to tým, že zápis dát do pamäti EEPROM 101 sa vykonáva tak, že osviežovanie dynamickej pamäti 104 a iných možných dynamických pamäťových prvkov, napríklad registra 105, nie je narušené. Na tento účel je frekvencia hodinového impulzu alfa udržiavaná na takej hodnote, že osviežovanie dynamických pamätí nie je ohrozené. V závislosti na používaných dynamických pamäťových prvkoch môže frekvencia hodinového impulzu dosiahnuť hodnotu najmenej 10 kHz. Keďže je trvanie hodinového impulzu počas zápisu pri takej frekvencii príliš malé (napr. 0.05 ms pri 10 kHz, zatiaľ čo pri istých pamätiach EEPROM sa vyžaduje trvanie impulzov po dobu najmenej 5 ms), vykonáva sa zápis opakovane. Inými slovami, rovnaká hodnota salda sa na rovnakú adresu pamäti 101 zapisuje niekoľkokrát, a to do doby, kedy sa dosiahla predpísaná doba trvania. V príklade s hodinovou frekvenciou 10 kHz a minimálnou dobou zápisu 5 ms to znamená, že zápis na rovnakú adresu sa bude opakovať aspoň stokrát.

Opakovaný zápis by mohol vyvolať ťažkosti v tom, že každým hodinovým impulzom na existujúcich kartách sa hodnota adresového registra zvýši (zníži) o jednotku. Platný zápis sa môže vykonať len na jednu z mnohých adries tak, že celkový rozsah adries by mal na uskutočnenie zápisu prejsť počas jedného (relatívne krátkeho) hodinového impulzu. Výsledkom by malo byť predĺženie požadovaného trvania zápisu.

Podľa iného aspektu tohto vynálezu sa ponúka riešenie, a to menením frekvencie hodinového impulzu alfa takým spôsobom, že počas prechodu adresového registra, to znamená bez záznamového signálu, sa zvýši frekvencia hodinového impulzu alfa, aby sa tým urýchlil priebeh, pričom ihneď pred zápisom alebo počas neho sa frekvencia zníži, aby záznamový impulz trval dlhšie. Je zrejmé, že sa frekvencia hodinového impulzu

môže znížiť len v rozsahu, ktorý požadované "osvieženie" dynamickej pamäti dovoľuje.

Tvar hodinového impulzu sa môže tiež výhodne nastaviť tak, že pomer 1/0 sa nedostane na hodnotu 50/50, ale napríklad na hodnoty 70/30 alebo 90/10. Výsledkom bude dlhší záznamový impulz (ak záznam prebieha pri hodinovom impulze rovnom 1), a tým aj kratší celkový čas záznamu bez toho, aby sa tým narúšalo osviežovanie dynamickej pamäti.

Nastavovanie tvaru hodinového impulzu sa môže výhodne kombinovať so zmenou frekvencie hodinového impulzu. Okrem toho môže byť adresový register konštruovaný tak, že negeneruje viac rôznych adries, než je skutočné nutné. Obmedzením počtu možných adries sa tiež obmedzí čas nevyhnutný na prehľadanie adresového registra.

Ako už bolo vysvetlené skôr, vynález je založený na skutočnosti, že sa medzi rôznymi krokmi tohto spôsobu nestráca žiadna overovacia informácia. Na tento účel je zaistené, že si dynamické registre a pamäte zachovávajú svoj obsah, a to dokonca i pri zápise do pamäti, napríklad do pamäti EEPROM, ktorý vyžaduje relatívne dlhý záznamový čas.

V praxi to znamená, že tento spôsob môže byť realizovaný vo forme softwaru v platobnom termináli, obzvlášť potom v tzv. čítacom zariadení kariet platobného terminálu.

Odborníci ľahko pochopia, že tento vynález nie je obmedzený na uvedené stvárnenia, ale že sú možné rôzne modifikácie a doplnky bez toho, aby tým bol narušený rozsah tohto vynálezu. Princíp tohto vynálezu je popísaný pre debitovací platobný prostriedok, ale rovnaké princípy sa môžu tiež aplikovať na kreditné a platobné prostriedky.

P A T E N T O V É N Á R O K Y

1. Spôsob vykonávania transakcií použitím elektronických platobných prostriedkov /11/ a platobných terminálov /12/, pričom tento spôsob zahŕňa:

- prvý krok /I/, v ktorom:

platobný terminál /12/ prenáša prvú náhodnú hodnotu /R1/ do platobného prostriedku /11/,

platobný prostriedok /11/ ako odpoveď na prvú náhodnú hodnotu /R1/ prenáša prvý overovací kód /MAC1/ do platobného terminálu /12/, kedy tento overovací kód je stanovený na základe aspoň prvej počiatočnej hodnoty /Q1/, prvej náhodnej hodnoty /R1/ a bežného salda /S1/ platobného prostriedku /11/ a pri použití vopred stanoveného procesu /F/, pričom tento proces vytvára prvú konečnú hodnotu /Y1/,

- ďalší krok /II/, v ktorom:

platobný terminál /12/ prenáša druhú náhodnú hodnotu /R2/ do platobného prostriedku /11/,

platobný prostriedok /11/ prenáša druhý overovací kód /MAC2/ do platobného modulu /12/, kedy tento overovací kód je stanovený na základe aspoň druhej počiatočnej hodnoty /Q2/, druhej náhodnej hodnote /R2/ a druhých prenosových dát /S2/ platobného prostriedku /11/, ktorý tento proces /F/ používa, kde je druhá počiatočná hodnota založená na prvej konečnej hodnote /Y1/

2. Spôsob podľa nároku 1, v y z n a č u j ú c i s a t ý m, že druhá počiatočná hodnota /Q2/ je identická s prvou konečnou hodnotou /Y1/.

3. Spôsob podľa nároku 1 alebo 2, v y z n a č u j ú c i s a t ý m, že overovací kód /MAC1/ je tiež stanovený na základe kľúča /K/ a identifikačného kódu.

4. Spôsob podľa nároku 1, 2 a 3, v y z n a č u j ú c i s a t ý m, že zahŕňa nepovinný medziľahlý krok /II/, ktorý sa vykonáva medzi počiatočným /I/ krokom a ďalšími krokmi /III/, v ktorých:

- platobný terminál /12/ prenáša príkaz /D/ do platobného prostriedku /11/, kde sa saldo platobného prostriedku /11/ mení na základe uvedeného príkazu /D/.

5. Spôsob podľa ktoréhokoľvek predchádzajúceho nároku, v y z n a č u j ú c i s a t ý m, že prvá náhodná hodnota /R1/ a druhá náhodná hodnota /R2/ sú identické, kde medzikrok platobného terminálu /12/, prenášajúci druhú náhodnú hodnotu /R2/ do platobného prostriedku, je vynechaný.

6. Spôsob podľa ktoréhokoľvek predchádzajúceho nároku, v y z n a č u j ú c i s a t ý m, že proces /F/ zahŕňa šifrovaciu funkciu.

Spôsob podľa ktoréhokoľvek predchádzajúceho nároku,

v y z n a č u j ú c i s a t ý m, že ďalej zahŕňa štvrtý krok /IV/, v ktorom:

- platobný terminál /12/ zaznamenáva rozdiel /S1-S2/ medzi saldami prvého a tretieho kroku.

8. Spôsob podľa ktoréhokoľvek predchádzajúceho nároku, v y z n a č u j ú c i s a t ý m, že tretí krok /III/ je vykonávaný opakovane.

9. Spôsob podľa ktoréhokoľvek predchádzajúceho nároku, v y z n a č u j ú c i s a t ý m, že platobný terminál /12/ zahŕňa modul dát zaznamenaných chráneným spôsobom.

10. Platobný prostriedok aplikácie tohto spôsobu podľa ktoréhokoľvek predchádzajúceho nároku, v y z n a č u j ú c i s a t ý m, že platobný prostriedok /11/ zahŕňa integrovaný obvod /100/ s prvou prepisovateľnou pamäťou /101/ na uchovávanie sáld, a ďalej s druhou dynamickou pamäťou /104/ na generovanie overovacieho kódu /MAC/ ako funkciu náhodného čísla /R/, kedy je integrovaný obvod /100/ prispôsobený na zápis salda /S/ do prvej pamäti /101/, ktorý prebieha opakovane a s hodinovými impulzmi /alfa/ tak, že obsah druhej dynamickej pamäti /104/ je zachovaný.

11. Platobný prostriedok podľa nároku 10, v y z n a č u j ú c i s a t ý m, že počet zapisovacích akcií na jednu zapisovanú jednotku salda dosahuje hodnoty 50 až 150.

12. Spôsob podľa nároku 10 alebo 11, v y z n a č u j ú c i s a t ý m, že frekvencia hodinového impulzu /alfa/ sa počas zápisu zvyšuje.

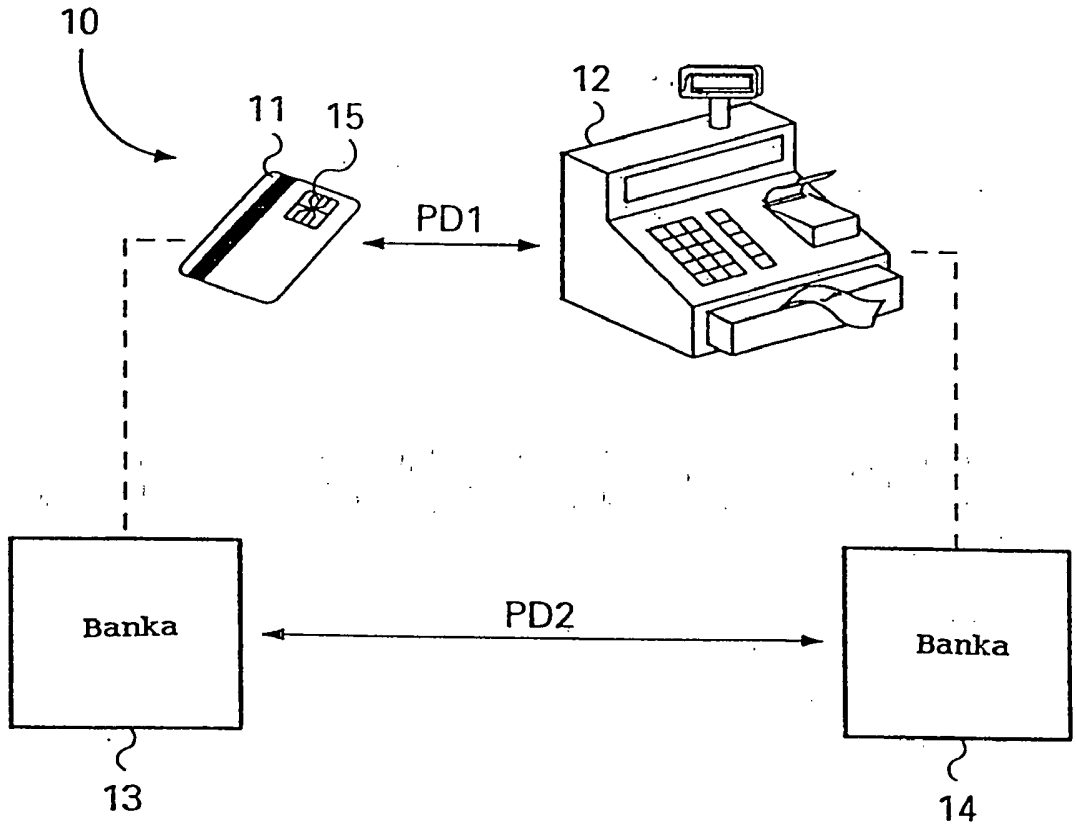
13. Platobný prostriedok podľa nároku 10, 11 alebo 12, v y z n a č u j ú c i s a t ý m, že hodinové impulzy /alfa/ majú asymetrický pomer 1/0.

14. Platobný prostriedok podľa ktoréhokoľvek nároku 10 až 14, v y z n a č u j ú c i s a t ý m, že ďalej zahŕňa prostriedok na zmenu pomeru hodinového impulzu.

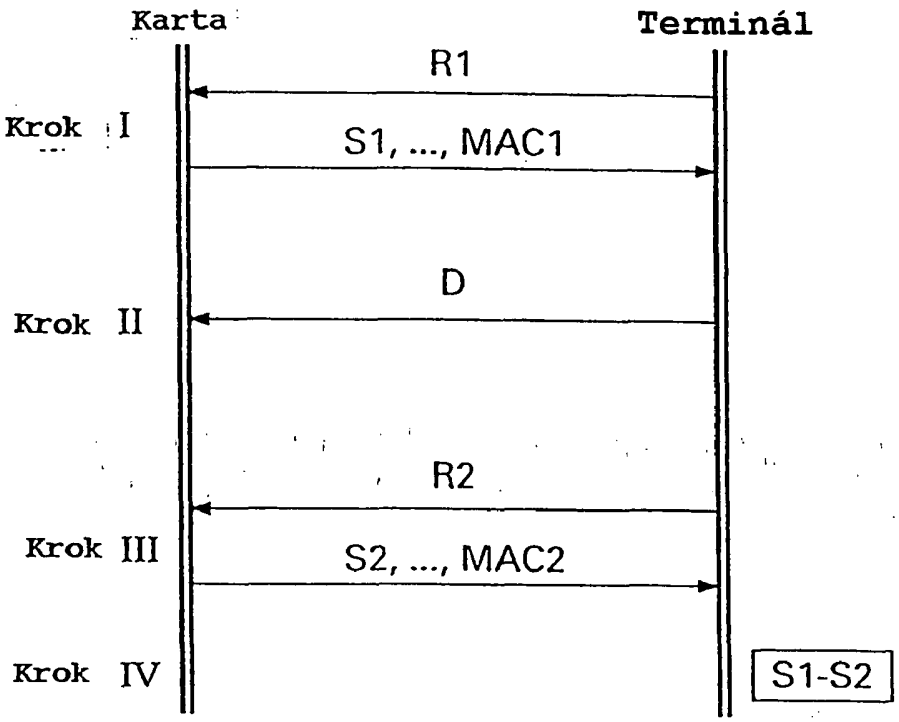
15. Platobný prostriedok podľa ktoréhokoľvek nároku 10 až 14, v y z n a č u j ú c i s a t ý m, že ďalej zahŕňa logický prostriedok /106/, operatívne pripojený k prvej pamäti /101/ a druhej pamäti /104/, a to s cieľom kombinovania dát z prvej pamäti s dátami spätnej väzby z druhej pamäti, a ďa-

lej s cieľom vloženia uvedených kombinovaných dát do druhej pamäti /104/.

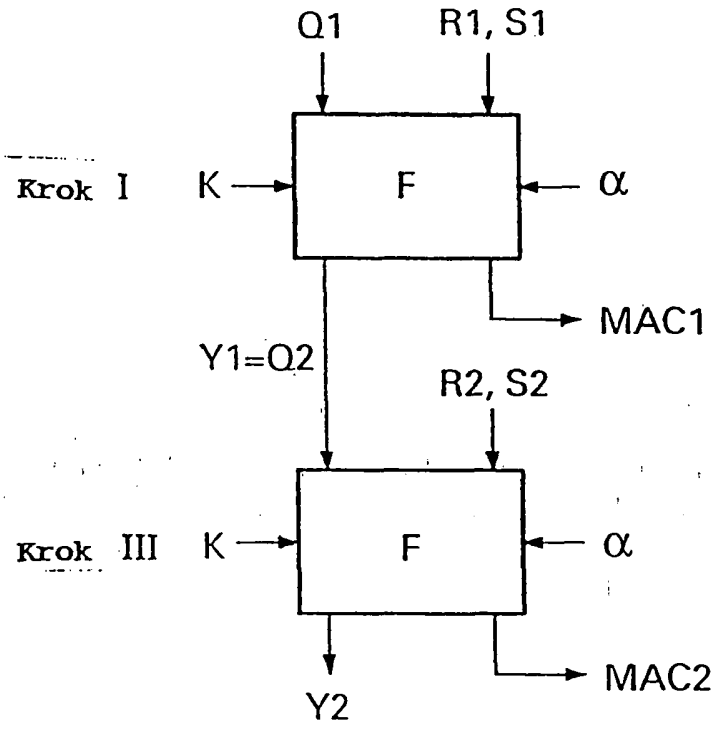
16. Platobný prostriedok podľa ktoréhokoľvek nároku 10 až 15, v y z n a č u j ú c i s a t ý m, že ďalej zahŕňa register /105/, ktorý je pripojený k logickému prostriedku /106/ s cieľom uloženia náhodnej hodnoty /R/.



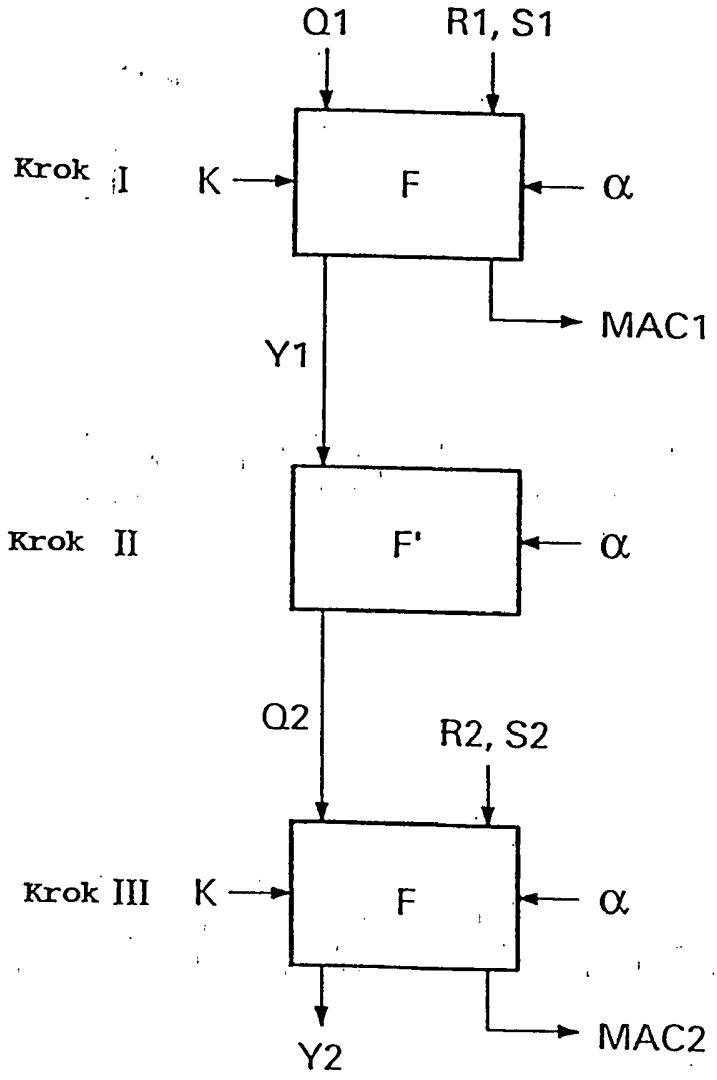
Obr. 1


Karta
Terminál
R1
Krok I
S1, ..., MAC1
D
Krok II
R2
Krok III
S2, ..., MAC2
Krok IV
S1-S2

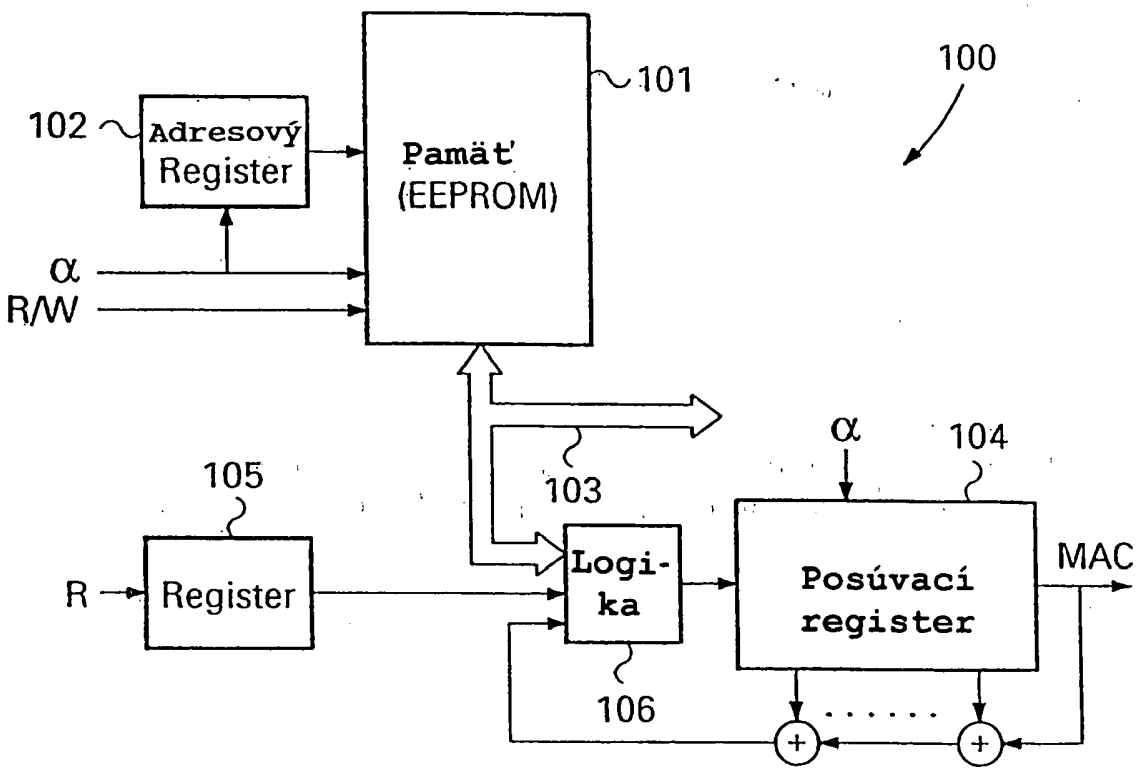
Obr. 2



Obr. 3


Q1
R1, S1
Krok I
K
F
α
MAC1
Y1
Krok II
F'
α
Q2
R2, S2
Krok III
K
F
α
Y2
MAC2

Obr. 4


100
101
102
Adresový Register
Pamäť (EEPROM)
α
R/W
103
104
105
R
Register
Logi-ka
Posúvací register
MAC
106

Obr. 5