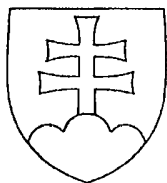


SLOVENSKÁ REPUBLIKA

(19) SK



ÚRAD
PRIEMYSELNÉHO
VLASTNÍCTVA
SLOVENSKEJ REPUBLIKY

ZVEREJNENÁ PRIHLÁŠKA VYNÁLEZU

(22) 03.12.93
(31) 07/710 875
(32) 06.06.91
(33) US
(43) 10.08.94
(86) PCT/EP92/00926

(21)

1361-93

(13) A3

(51)

G 06 F 12/14

(71) International Business Machines Corporation, Armonk, NY, US;

(72) CLARK Carl Edward, Poughkeepsie, NY, US;
SCALZI Casper Anthony, Poughkeepsie, NY, US;
MALL Michael Gerard, Lagrangeville, NY, US;
SINHA Bhaskar, Wappingers Falls, NY, US;

(54) Spôsob zaistenia ochrany prístupu pre bloky dát a
prostriedok na vykonávanie tohto spôsobu

(57) Spôsob zaistenia ochrany prístupu pre bloky dát zaisťujú tri úrovne prístupu ochrany ukladacími kľúčmi zahrňujúcimi supervizorovú úroveň, strednú úroveň neverejných a nesupervizorových kľúčov, a jedinou verejnú úroveň. Programové rutiny pracujúce s prístupovým kľúčom supervizorovej úrovne môžu pristupovať k verejnej úrovni a k strednej úrovni blokov uloženia. Hoci programová rutina pracujúca s prístupovým kľúčom v strednej úrovni prístupu nemôže pristúpiť k bloku uloženia na supervizorovej úrovni, môže pristúpiť k nejakému bloku priradenému ukladaciemu kľúčovi verejnej úrovne, ako i k nejakému bloku uloženia priradenému príslušnému kľúčovi strednej úrovne. Môže byť vytvorený jeden alebo niekoľko verejných ukladacích kľúčov VUK tretej úrovne. Prístupový kľúč programu používajúci jednu z hodnôt VUK môže pristúpiť len k bloku majúcim rovnakú hodnotu VUK a nemôže pristúpiť k blokom majúcim inú kľúčovú hodnotu.

SPÔSOB ZAISTENIA OCHRANY PRÍSTUPU PRE BLOKY DÁT A PROSTRIEDOK NA VYKONÁVANIE TOHTO SPÔSOBU

Oblasť techniky

Vynález sa týka spôsobu zaistenia ochrany prístupu pre bloky dát v uložení systému spracovania dát, v ktorom môžu rôzne programy pristúpiť k blokom. Vynález sa ďalej týka prostriedkov na vykonávanie spôsobu definovaného vyššie.

Vynález zvyšuje použitie ochranných kľúčov uloženia na ochranu programov a dát v rozličných častiach pamäti počítača požiadavkou na každý program, aby použil ochranný kľúč priradený bloku uloženia pamäti, ktorý musí byť sprístupnený programom. Takáto ochrana prístupu chráni kód a dáta v jednom bloku uloženia proti divokým uloženiám vyplývajúcim z realizácie kódu v inej oblasti uloženia, i keď práve tieto bloky uloženia sú v rovnakom priestore virtuálnych adries.

Doterajší stav techniky

Ochranné kľúče uloženia pre bloky uloženia pamäti boli popísané v patentových spisoch Spojených štátov amerických 3,576,544 s názvom "Storage protection system" od autorov H. Cordero a spol. 4,093,987 s názvom "Hardware Control Storage Area Protection Method and Means" od autorov C. M. Gaudette a spol. a 4,472,790 s názvom "Storage Fetch Protect Override Controls" od autorov J. L. Burk a spol., ktoré majú rovnakého prihlasovateľa ako táto prihláška vynálezu. Ochranné kľúče uloženia boli použité v komerčných systémoch IBM S/360, S/370 a S/390 a v ich kompatibilných systémoch.

Bežná architektúra IBM S/390 obsahuje ukladacie kľúče 0-15 a prístupové kľúče 0-15, ako sú popísané v pojednaní Enterprise System Architecture S/390 Principles of Operation, od čísla SA22-7201-00, vydanom spoločnosťou IBM. V bežných systémoch IBM kľúče 0-15 zaisťujú dve úrovne ochrany, jednu pre supervizorovú

triedu kľúča, implementovanú s kľúčom 0 a užívateľskú triedu kľúčov, implementovanú s kľúčom 1-15. Supervizorový kľúč 0 môže sprístupniť dáta v akomkoľvek bloku uloženia v pamäti bez ohľadu na ukladací kľúč priradený bloku. Nesupervizorový prístupový kľúč z kľúčov 1-15 však môže získať prístup k uloženiu len vtedy, keď bola rovnosť medzi niektorým prístupovým kľúčom použitým prístupovým programom a ukladacím kľúčom priradeným bloku, v ktorom sa vykonáva pokus o prístup.

Ukladací kľúč je zaistený s hlavným hardware uložením pre každý blok s veľkosťou 4 KB alebo stránku, v hlavnom zložení systému S/360, S/370 a S/390. Každý prístup k hlavnému uloženiu systému vykonáva skúšku ochranného kľúča niektorého prístupového kľúča zaisteného pre každý prístupový program. Prístupový kľúč je všeobecne zaistený z poľa prístupových kľúčov v stavovom stave programu SSP programu. Prístupový kľúč je združený proti ochrannému kľúčovi uloženia stránky adresovanej v systémovom hardware uložení s použitím skôr komplexnej množiny pravidiel posilnených hardware na určenie, či existuje alebo neexistuje združenie kľúča.

Združovacie pravidlá zahrňujú použitie ochranného bitu privádzania OP v každom ukladacom kľúči. Prístupy na uloženie nie sú ovplyvnené nastavením OP bitu a rovnosť medzi prístupovým kľúčom a ukladacím kľúčom je potrebná pred akýmkoľvek povolením prístupu na uloženie pre akýkoľvek nesupervizorový prístupový kľúč 1-15. Kvôli nejakej žiadosti o privedenie OP bit kontroluje, či je alebo nie je potrebná rovnosť na dovolenie prístupu pre akýkoľvek nesupervizorový prístupový kľúč 1-15. Ak je OP bit nulový, nie je nutná rovnosť na dovolenie prístupu privedenia, ktorý je dovoľený bez ohľadu na hodnotu prístupového kľúča alebo na hodnotu ukladacieho kľúča. Ak je však OP bit rovný jednej, je nutná rovnosť na dovolenie prístupu privedenia pre akýkoľvek nesupervizorový kľúč 1-15.

Supervizorovému prístupovému kľúčovi 0 je dovoľený prístup, či je alebo nie je rovný niektorému z ukladacích kľúčov 1-15.

Spôsob ochrany ukladacieho kľúča v súčasnosti nájdený v systémoch používajúcich architektúru IBM S/390 je dvojúrovňová štruktúra ochrany pozostávajúca zo supervizorovej úrovne kľúča 0 a z nesupervizorovej úrovne kľúčov 1-15. Supervizorové programy môžu prístupit' k nesupervizorovo priradeným blokom uloženia, avšak nesupervizorové programy nemôžu prístupit' k supervizorovo priradeným blokom uloženia.

Spôsob ochrany kľúča je zaistený v kritickej ceste každého prístupu uloženia v systéme, lebo je vyhotovený pre každý prístup k uloženiu. Hardware kontroly kľúčov v systéme S/390 a tiež v predchádzajúcich systémoch S/360 a S/370 sa tiež vykonával paralelným spôsobom s prekrývaním iných riadiacich operácií v každom prístupe, takže sa nezväčšovala doba každého prístupu k uloženiu.

Nie sú známe iné typy architektúr počítačov ako IBM, ktoré vo svojich schémach ochrany uloženia používajú ochranné kľúče uloženia implementovania v hardware. Napríklad skôr známy systém Multics používal schému okruhov ochrany, ktorá nepoužívala ochranné kľúče uloženia. Nie je známe, že Multics priraduje ukladacie kľúče blokom v uložení. Tento systém priradzoval číslo okruhu ku každému procesu vykonanému programovými inštrukciami volanie/návrat pri použití segmentového virtuálneho adresovania. Akýkoľvek proces mohol prístupit' k virtuálnemu uloženiu priradenému k niektorému inému procesu priradenému nižšie číslovanému okruhu v hierarchii čísiel okruhov. V tomto vynáleze nie sú nutné chránené okruhy.

Ochranné kľúče chránia prístupy k reálnemu uloženiu v systéme a zaistujú adresovaciú ochranu prídavne k iným spôsobom ochrany zaisteným v systémoch S/390, ako je virtuálne adresovanie a priestory virtuálnych adries, čo zaistuje ochranu prístupu mimo ochranu zaistenú ukladacími kľúčmi. Virtuálne adresovanie akejkoľvek programovej adresy túto mapuje na ktorékoľvek miesto stránky v reálnom hlavnom uložení, čo je skutočne miesto

premenlivé a neznáme pre užívateľa adresy od jedného okamihu k nasledujúcemu pri použití systému. Ak nejaký program bežiaci v jednom adresovom priestore nesmie prístupit' k inému adresovému priestoru, potom sú dáta a programy v druhom adresovom priestore chránené z programu. Ukladacie kľúče sú použité na zaistenie ochrany v nejakom adresovom priestore z programov, ktoré majú adresovaciú schopnosť k tomuto priestoru, avšak nemajú poverenie pre niektoré dáta v tomto priestore.

V doterajšom stave techniky sú popísané i iné spôsoby ochrany, ktoré súvisia len nepatrne alebo vôbec nie s vyššie uvedeným spôsobom ochrany kľúčmi, ako je použitie porovnania s hornou a spodnou okrajovou adresou, čo môže byť reálna adresa alebo absolútna adresa.

Jednako však rôzne typy spôsobov ochrany možné v nejakom systéme nie sú navzájom porovnateľné, pretože chovanie systému neprebíha zhodne.

Ochrana kľúčmi vyžaduje inicializáciu prístupu a zavedené ukladacie kľúče. Prístupový kľúč programu je určený poľom v stavovom slove programu SSP, po ktorom je program vykonávaný. Ukladací kľúč je združený s každým blokom reálneho uloženia. Ochrana kľúčmi môže pripustiť viac úrovní hodnotí prístupu použitých v jednom programe. Program môže mať schopnosť prístupu k viac ako jednému kľúču. Táto schopnosť je zaistená poľom riadiaceho registra nazvaným maska programového kľúča MPK a inicializovaným operačným systémom pre úlohu, ktorá má byť vykonávaná. Jednako však všeobecne má pôsobiť v ktoromkoľvek čase len jedna hodnota prístupového kľúča. V architektúre S/390 je obsiahnutá malá sada inštrukcií pre pohyb dát z jedného miesta v uložení do iného, čo dovoľuje oddelený ochranný kľúč pre každý operand. Jeden z kľúčov je SSP kľúč. Iný kľúč musí byť ohodnotený od MPK, ak SSP nie je v supervizorovom stave, teda bit 15 SSP je nulový, viď obr. 3. Program, ktorý smie použiť viac ako jeden kľúč, musí ovládať hodnotu prístupového kľúča PSS použitím inštrukcie v S/390, ktorá má text Nastav SSP Kľúč Z Adresy

(NSKA), ako je požadované jej zamýšľanými prístupmi na uloženie v ktoromkoľvek okamihu. Len supervizorový prístupový kľúč umožňuje schopnosť súčasných prístupov k viac ako jednému kľúču a bez pôsobenia na špecifický SSP prístupový kľúč.

Iné techniky ochrany však vyžadujú vykonávanie špeciálne programovaných inštrukcií v ich kritických cestách, čo zhoršuje ich chovanie, ako je použitie programových inštrukcií volanie/návrat za účelom použitia ochranných techník virtuálneho adresovania, ktoré zavádza chovanie nad spínaním adresového priestoru, ktoré nie je potrebné pri ochrane kľúča.

Napríklad môže byť do jedného adresového priestoru zavedený podsystém v software a jeho použitie v rozličných adresových priestoroch na zaistenie oddelenia priestoru virtuálnych adres. Teraz dochádza k významnej strate výsledkov chovania v tom, že je treba spínať adresové priestory pri pohybe medzi podsystémom k aplikácii a takéto nadradené spínanie adresového priestoru je vylúčené týmto vynálezom, pričom sa získajú všetky potrebné výhody ochrany priradením iného ukladacieho kľúča aplikačnému programu ako dátam podsystému, avšak pripustením prístupu podsystémom k dátam aplikačného programu bez pôsobenia prístupového kľúča.

Podstata vynálezu

Predložený vynález pridáva tretiu jednosmernú úroveň prístupu k spôsobu kľúčovej ochrany uloženia v súčasnosti obsiahnutej v systémoch používajúcich architektúru IBM S/390, ktorá má dvojúrovňovú štruktúru ochrany, zahrňujúcu supervizorovú úroveň, kľúč 0 a nesupervizorovú úroveň, kľúče 1-15. Programové rutiny pracujúce na supervizorovej úrovni môžu pristupovať k blokom uloženia nesupervizorovej úrovne, avšak programové rutiny pracujúce na nesupervizorovej úrovni nemôžu pristupovať k blokom uloženia supervizorovej úrovne.

Vynález zachováva dve jednosmerné úrovne ochrany prístupu skoršieho spôsobu kľúčovej ochrany S/390, zatiaľ čo oddeľuje tretiu jednosmernú úroveň ochrany prístupu z druhej úrovne pre použitie ako verejnej prístupnej úrovne. Vynález zachováva výhody chovania kľúčovej ochrany pre všetky tri úrovne bez zvýšenia požiadaviek programového kódu na umožnenie krátkej dĺžky cesty inštrukcie a bez požiadaviek akéhokoľvek spínania adresového priestoru. Tretia úroveň riadenia ukladacích kľúčov je tu označená ako úroveň verejného ukladacieho kľúča VUK. Tieto tri úrovne zaistujú tri triedy ochranných kľúčov, ktoré sú tieto: supervizorová trieda, stredná trieda a verejná trieda. Všetkým triedam sú pridelené špecifické hodnoty mimo kódovaných množinu ochranných kľúčov. Napríklad keď sa použije štvorbitový kód zaistujúci 16 kľúčov, sú kľúče vo všetkých triedach umiestnené z týchto 16 kódov. Priradenie zvláštnych hodnôt kódu príslušným triedam je na začiatku ľubovoľné, avšak keď sa už raz priradia, kódy sa musia používať bez zmeny. Každá z troch tried môže obsahovať jeden alebo niekoľko ochranných kľúčov. Supervizorová trieda, to je najvyššia trieda, má podľa predpokladu jeden ochranný kľúč, čo môže byť kľúč 0. Trieda VUK, to je najnižšia trieda, môže obsahovať jeden alebo niekoľko kľúčov. Ak je priradených niekoľko VUK hodnôt, potom prístup používajúci niektorých z VUK môže pristúpiť len k blokom majúcim inú VUK hodnotu. Tie zo 16 kódov, ktoré nie sú priradené k supervizorovej triede a k VUK triede, sú dostupné na použitie strednou triedou. Prístupový kľúč strednej triedy môže pristúpiť nielen k blokom uloženia jemu priradených, avšak i k blokom priradeným VUK.

Prvou úlohou vynálezu teda je vytvoriť systém ochrany uloženia, ktorý obsahuje verejnú triedu kľúčov, ktoré môžu pracovať so zvyčajným supervizorovým kľúčom a jednu strednú triedu ochranných kľúčov.

Ďalej je úlohou vynálezu chrániť všetky bloky uloženia nepriradené verejnému kľúču pred divokým ukladaním spôsobeným inštrukciami vykonávanými pod hodnotou prístupu verejného

ukladacieho kľúča, ak sú inštrukcie vykonávané v rovnakom adresovom priestore alebo v inom adresovom priestore.

Ďalšou úlohou vynálezu je chrániť bloky uloženia ktorejkoľvek jednej hodnoty VUK pred prístupom inštrukciami bežiacimi pod nejakou inou hodnotou VUK, zatiaľ čo v rovnakom čase môžu byť voľne prístupné bez kľúča ovládaných krokov programu inštrukciami vykonávanými s hodnotou prístupu akejkoľvek hodnoty v supervizorovej triede kľúča alebo v strednej triede kľúča, buď v rovnakom adresovom priestore alebo v inom adresovom priestore.

Prvá, supervizorová trieda môže byť zvolená, napríklad ako kľúč 0, kvôli zachovaniu kompatibility so skoršími programami, ktoré používali kľúč 0 ako supervizorový kľúč. Potom môže byť tretia, verejná trieda ľubovoľne zvolená ako jeden alebo niekoľko zostávajúcich kľúčov 1-15. Napríklad kľúč 9 môže byť zvolený ako VUK. To ponecháva kľúče 1-8 a 10-15 pre druhú, strednú triedu.

Zvyčajný ochranný kľúč uloženia má pole bitov ochrany privedenia OP a pole ACC, ktoré sú použité s novým usporiadaním kľúčov vytvoreným predloženým vynálezom, avšak s určitou obmenou v činnosti. Ďalej, zhodná podmienka alebo nezhodná podmienka označuje rovnosť alebo nerovnosť medzi obsahom poľa ACC v adresovanom ochrannom kľúči uloženia a poľom prístupového kľúča, zvyčajne poľom kľúča získaným zo SSP.

Pravidlá činnosti novej tretej, verejnej triedy sú také, že verejný prístupový kľúč môže ukladať do niektorého bloku len vtedy, keď je nájdená rovnaká podmienka s verejným ukladacím kľúčom bloku, bez ohľadu na nastavenie OP bitu v ukladaacom kľúči. Privádzanie verejným prístupovým kľúčom je však riadené nastavením OP bitu. Ak je v ukladaacom kľúči OP rovné 1, je privedenie dovolené len keď je rovnosť medzi verejným prístupovým kľúčom a verejným ukladacím kľúčom. Ak je však OP rovné 0 v ukladaacom kľúči, privedenie je dovolené bez rovnosti medzi verejným prístupovým kľúčom a verejným ukladacím kľúčom.

Pravidlá pre kľúče 1-8 a 10-15 druhej, strednej triedy sú predloženým vynálezom pozmenené na prispôsobenie novej VUK triede. Prv bola vždy vyžadovaná rovnosť pre ukladanie do niektorého bloku majúceho nesupervizorový kľúč. To je zmenené predloženým vynálezom, ktorý dovoľuje, aby ktorýkoľvek kľúč strednej triedy, ako i kľúč supervizorovej triedy, ukladal alebo privádzal do nejakého VUK bloku bez rovnosti, bez ohľadu na stav OP bitu.

Ako dôsledok je rozšírená schopnosť stredného kľúča pristupovať k blokom majúcim rôzne ukladacie kľúče bez použitia zvláštneho programovania ovládania kľúčov, čo prv bolo možné len u supervizorových kľúčov. Teda s predloženým vynálezom program používajúci stredný kľúč môže pristupovať nielen k blokom uloženia priradeným k strednému kľúču, ale aj k blokom zloženia priradených niektorému verejnému kľúču. Predložený vynález teda odstraňuje skoršiu požiadavku mať možnosť použitia prídavných programových inštrukcií pre zmenu niektorého nesupervizorového kľúča, napríklad v SSP, pred tým, ako niektorý nesupervizorový kľúč by mohol prísť k bloku s iným kľúčom. Napríklad program bežiaci s niektorým stredným prístupovým kľúčom môže vykonať zavádzaciu inštrukciu zo slova v bloku chránenom proti privádzaniu a ukladacím kľúčom rovným rovnakému strednému kľúču a v bezprostredne nasledujúcej inštrukcii môže použiť inštrukciu uloženia do bloku uloženia s ukladacím kľúčom verejnej triedy.

Okrem rovnosti zostáva požiadavka pre niektorý kľúč strednej triedy ukladať do bloku používajúceho kľúč strednej triedy, bez ohľadu na nastavenie OP. A privádzanie je riadené nastavením OP. Ak je OP rovné 1 v ukladacom kľúči, privedenie je dovolené len keď je rovnosť medzi stredným prístupovým kľúčom a iným stredným ukladacím kľúčom. Ak je však OP rovné 0 v ukladacom kľúči, privedenie je dovolené bez rovnosti medzi stredným prístupovým kľúčom a stredným ukladacím kľúčom.

Pravidlá pre supervizorovú triedu kľúča 0 nie sú predloženým vynálezom zmenené, avšak sú rozšírené na VUK bloky - žiadna rovnosť kľúčov nie je žiadaná pre prístup k niektorému bloku uloženia, včítane niektorého VUK bloku, programom používajúcim prístupový kľúč 0 okrem s blokmi priradenými ukladaciemu kľúču 0.

Ktorýkoľvek stredný kľúč 0 - 8 a 10-15 môže pri použití pristúpiť k bloku uloženia ktoréhokoľvek verejného kľúča 9. Žiaden verejný kľúč 9 pri použití nemôže uložiť alebo priviesť, keď ochrana privedenia je zapnutá do nejakého bloku uloženia chráneného supervizorovým kľúčom 0 alebo stredným ukladacím kľúčom 0-8 a 10-15.

Prehľad obrázkov na výkresoch

Vynález je znázornený na výkresoch, kde:

- obr. 1 znázorňuje hardware obsahujúci jedno vyhotovenie vynálezu,
- obr. 2 znázorňuje zvyčajný ochranný kľúč uloženia,
- obr. 3 znázorňuje prístupový kľúč a P bit v stavovom slove programu SSP,
- obr. 4 znázorňuje prístupový kľúč v registri všeobecného účelu RU použitom niekoľkými rozličnými inštrukciami,
- obr. 5 znázorňuje prístupový kľúč v bloku požiadavky operácie BPO použitom pre operáciu vstup/výstup,
- obr. 6 znázorňuje pole masky bitu SSP kľúča v kontrolnom registri KR 3,
- obr. 7 znázorňuje vstupný kľúč a pole masky kľúča použité pri riadení adresového priestoru,
- obr. 8 znázorňuje riadiace pole módu verejného ukladacieho kľúča VUK používané v prednostnom vyhotovení vynálezu,
- obr. 9 znázorňuje vývojový diagram prednostného vyhotovenie vynálezu,
- obr. 10 znázorňuje stavový diagram činnosti vynálezu, a
- obr. 11 je znázornenie hardware prednostného vyhotovenia vynálezu.

Príklad vyhotovenia vynálezu

Obr. 1 znázorňuje hardware obsahujúci prednostné vyhotovenie vynálezu. Má množstvo centrálnych procesorov CP-0 až CP-N a množstvo vstupných/výstupných prístrojov I/O-0 až I/O-K s ich podkanálmi, riadiacimi jednotkami a kanálmi. Centrálné procesory a vstupné/výstupné prístroje dávajú požiadavky na prístup do pamäti hlavnému kontrolóru 20 uloženia, ktorý riadi privedenie a uloženie dátových jednotiek v hlavnom uložení HU 21. HU 21 obsahuje množstvo radov DRAM pre dátové jednotky HU. Každá žiadosť o prístup HU obsahuje absolútnu adresu dátovej jednotky privedenej alebo uloženej v HU. Centrálné procesory vyvíjajú logické adresy, čo sú zvyčajne virtuálne adresy, môžu to však byť reálne adresy, v súhlase s architektúrou S/390. Každá virtuálna adresa vyvinutá niektorým centrálnym procesorom je v ňom preložená na absolútnu adresu, ktorá je poslaná so žiadosťou o prístup do HU spolu s prístupovým kľúčom žiadateľa.

Každá vyžiadaná absolútna adresa má časť vyššieho radu, ktorá predstavuje adresu 4 KB bloku zvaného "stránka" v HU obsahujúcom žiadanú dátovú jednotku.

Rad 22 ochranných kľúčov pozostáva z jednej alebo niekoľkých DRAM, ktoré obsahujú ochranné kľúče uloženia typu definovaného v architektúre S/390.

Kľúče v rade 22 sú združené s príslušnými stránkami zloženia dát v HU 21 na báze jedna pre jednu. Keď je do HU 21 poslaná adresa niektorej dátovej jednotky, je súčasne do radu 22 kľúčov poslaná adresa stránka dátovej jednotky na umiestnenie ochranného kľúča uloženia v rade 22, ktorá je združená s dátovou jednotkou prístupnou v HU 21. Tento spôsob adresovania HU a radu kľúčov je dobre známy v doterajšom stave techniky.

Obr. 2 znázorňuje formu každého ochranného kľúča uloženia v rade 23, ktorá je definovaná architektúrou S/390. Každý

ochranný kľúč uloženia zaberá jednu slabiku uloženia v rade kľúčov a má určitý počet polí obsahujúci štvorbitové pole ACC, ktoré býva označené ako "ochranný kľúč uloženia", keď presnejšie celá slabika je ochranný kľúč uloženia. Iné pole v ochrannom kľúči uloženia sú jednobitové pole OP ochrana uloženia, R referencie a Z zmena. Obsah ACC poľa "kľúča" v ochrannom kľúči uloženia je združený so štvorbitovým "prístupovým kľúčom" zaisteným programom žiadajúcim prístup do HU. Vynález kontroluje, ako združenie pracuje a môže byť ovplyvnené nastavením poľa OP bitu.

Skúšobný hardware 23 ochranných kľúčov dostane každý ochranný kľúč uloženia privedený do radu 22 kľúčov. Skúšobný hardware 23 skúša privedený "ochranný kľúč uloženia" proti niektorému "prístupovému kľúču" zaistenému bežnou žiadosťou vykonanou niektorým CP alebo I/O.

"Prístupový kľúč" je získaný z riadiaceho prvku, ktorý je definovaný architektúrou S/390 v doterajšom stave techniky. Prístupový kľúč je zaistený príslušným vyhotovením CP alebo I/O požadujúcim operáciu prístupu do HU. Obr. 3, 4 a 5 znázorňujú rozličné zdroje pre prístupový kľúč. Zvláštny zdroj je vybraný jednotkou HP alebo I/O vykonávajúcou žiadosť HU.

Obr. 3 znázorňuje zdroj SSP (stavové slovo programu) prístupového kľúča v každom centrálnom procesore O-N. SSP v príslušnom CP je zdroj prístupového kľúča pre väčšinu inštrukcií vykonávaných CP, ktorý žiada prístup do HU. Malý počet inštrukcií CP nepoužíva SSP ako zdroj pre prístupový kľúč, v tomto prípade je zdrojom prístupového kľúča register všeobecného účelu RU, v ktorom sa prístupový kľúč nachádza v polohách bitov 24-27, čo je znázornené v obr. 4. Tento malý počet inštrukcií je definovaný v architektúre S/390 ako: pohyb k primáru, pohyb k sekundáru, pohyb s kľúčom, pohyb s určujúcim kľúčom a pohyb so zdrojovým kľúčom.

Na obr. 3 P pole v SSP v bitovej polohe 15 kontroluje, či príslušný CP je činný v probléme alebo je v supervizorovom stave. Keď je v problémovom stave, bit 15 v SSP je rovný jednej, maska kľúča SSP v KR3, viď obr. 6, je použitá na určenie, či žiadateľ je oprávnený použiť prístupový kľúč špecifikovaný v RU. Keď je v supervizorovom stave, kľúč špecifikovaný v RU je použitý bez ohľadu na MPK.

Obr. 5 znázorňuje blok požiadavky operácie BPO používajúci väčšinou žiadosť I/O o prístup, od I/O-O do I/O-K, ako jeho zdroj prístupového kľúča pre prístup do HU žiadaný I/O. BPO je kontrolný blok v HU, ktorý sa získa štartom inštrukcie podkanálu, ktorá štartuje ktorýkoľvek I/O prístroj v architektúre S/390. Bitové polohy 0-3 v BPO obsahujú prístupový kľúč.

Volacia inštrukcia zlučovacieho programu VP v architektúre S/390 používa prístupový kľúč odvodený zo vstupu vstupnej tabuľky VVT, v ktorej sa prístupový kľúč nazýva vstupný kľúč VK znázornený v obr. 7. Použitie prístupového kľúča VK pracuje s poľom masky kľúča SSP v kontrolnom registri KR3 znázornenom na obr. 6. Účinnou maskou môže byť modifikácia poľa masky kľúča SSP v kontrolnom registri KR3, modifikovaná poľom masky kľúča oprávnenia poľom masky vstupného kľúča pri kontrole M poľa vo VVT znázorneného v obr. 7, ako je definované v architektúre S/390.

Činnosť vyhotovenia vynálezu je kontrolovaná nastavením poľa módu verejného ukladacieho kľúča VUK znázorneného v obr. 8 v KR s bitovou polohou 7 označenou ako KR 0.7. Činnosť vynálezu je vyvolaná, keď bit KR 0.7 je nastavená na 1 a zvyčajná činnosť kľúča sa získa, keď KR 0.7 je nastavená na 0.

Obr. 9 znázorňuje činnosť prednostného vyhotovenia vynálezu, ktorá je vykonávaná pre každú žiadosť o prístup na uloženie z niektorého CP alebo I/O v systéme keď KR 0.7 je nastavený do stavu 1 pre dovoľenie operácie verejného ukladacieho kľúča PSK.

Na obr. 9 je zavedený krok 31 na žiadosť o prístup na uloženie dostanúce priority k vykonaniu hlavným kontrolórom uloženia v obr. 1 zvyčajným spôsobom.

Ak krok 31 zistí, že zaistený prístupový kľúč je supervizorový kľúč, to je kľúč 0, potom je zvolená dráha áno ku kroku 32 na dokončenie prístupu a v obr. 1 je vyslaný signál "prístup možný" do HU 21 skúšobným hardware 23 ochranných kľúčov, aby sa HU umožnilo dokončiť žiadaný prístup k zavedeniu alebo uloženiu v HU. Ak krok 31 zistí, že prístupový kľúč nie je v supervizorovej triede, je zvolená dráha nie ku kroku 33.

Krok 33 skúša prístupový kľúč, aby zistil, či je zhodný s polom ACC v ochrannom kľúči uloženia, vid' obr. 2. Keď áno, je zvolená dráha ku kroku 32 pre dokončenie privedenia alebo uloženia. Ak nie je však prístupový kľúč zhodný s ukľadacím kľúčom, je zvolená dráha nie ku kroku 34, ktorý skúša stav bitu módu KR 0.7, aby určil, či je vo VUK alebo v konvenčnom móde. Ak je KR 0.7 v stave 0, modus VUK nie je bežne účinný a je zvolený výstup nie ku kroku 38. Teraz sa skúša požiadavka krokom 38, aby sa určilo, či je to požiadavka privedenia alebo nie. Ak zistí krok 38, že nie je, znamená to, že požiadavka prístupu je pre uloženie. Ak sa zistí, že je to prístup pre uloženie, jeho dokončenie nie je dovolené, pretože požiadavka uloženia je pripustená len keď prístupový kľúč bol krokom 33 zistený ako zhodný s ukľadacím kľúčom, čo spôsobuje zvolenie dráhy áno z kroku 33 ku kroku 32. Výstup nie z kroku 33 oznamujúci nerovnosť medzi prístupovým kľúčom a ukľadacím kľúčom však zamedzí dokončenie požiadavky uloženia. Teraz krok 38 zvolí dráhu nie ku kroku 41, ak nie je zistená požiadavka privedenia krokom 38, a krok 41 vyvinie výnimku prístupu pre oznámenie, že pre túto požiadavku uloženia nie je vykonané dokončenie. Linka umožnenia prístupu v obr. 1 tiež nie je aktivovaná, čo zamedzí uskutočnenie prístupu na uloženie v HU.

Ak sa však zistí krokom 34, že KR 0.7 je v stave 1, existuje modus VUK a je zvolená dráha áno ku kroku 36, ktorý určí, či

prístupový kľúč je vo verejnej triede skúšaním jeho zhodnosti s niektorou z hodnôt kódu definovaných ako členovia verejnej triedy. Ak bolo zistené, že prístupový kľúč je zhodný s niektorým kľúčom vo verejnej triede, je zvolená dráha áno ku kroku 38. Napríklad by mohla byť zvolená hodnota 9 alebo 15 ako jediný kľúč vo verejnej triede, alebo by verejná trieda mohla obsahovať niekoľko kľúčov, napríklad 9, 10 a 15.

Ak nie je však prístupový kľúč zhodný so žiadnym kľúčom vo verejnej triede, je zvolená dráha nie z kroku 36 ku kroku 37. Krok 37 určí, či bežný prístupový kľúč je verejný kľúč skúškou, či je zhodný s niektorým kľúčom z verejnej triedy. Ak je prístupový kľúč verejný kľúč, je zvolená dráha áno z kroku 37 ku kroku 32 na dokončenie prístupu privedenia alebo uloženia v HU. Ak však zistí krok 37, že prístupový kľúč nie je verejný kľúč, je vykonaný krok 38, aby sa zistilo, či bežná požiadavka je alebo nie je privedenie, čo je teda uloženie, pretože stav OP bitu je použitý na možné pripustenie len keď ide o požiadavku privedenia.

Ako bolo vyššie vysvetlené, dráha nie z kroku 38 ku kroku 41 je zvolená, keď bolo zistené, že ide o požiadavku uloženia pretože uloženie nie je pripustené, keď predchádzajúci krok 33 zistil, že prístupový kľúč nie je hodný s ukladacím kľúčom. Dráha áno z kroku 38 ku kroku 42 je však volená ak bolo zistené, že ide o požiadavku privedenia. Krok 42 skúša stav poľa OP v bežne adresovanom ochrannom kľúči uloženia, aby sa určilo, či je nastavená ochrana privedenia, to je $OP=1$, v ktorom prípade je privedenie zamedzené a je zvolená dráha áno ku kroku 41, ktorý vyvinie výnimku prístupu, ktorá oznamuje, že bola vykonaná nedovolená akcia, v ktorom prípade sa vykoná prerušenie a vykonávanie bežnej inštrukcie je zastavené. Ak zistí krok 42, že ochrana privedenia je vyradená, to je $OP=0$, privedenie je pripustené a je zvolená dráha nie ku kroku 32.

V stavovom diagrame na obr. 10 je znázornená hierarchia troch tried kľúčov I, II a III, v ktorej I je najvyššia a III najnižšia trieda, pričom kontrola prístupu je postupne viac

obmedzená v poradí tried od I ku II a k III triede. Trieda I je supervizorová trieda, trieda II je stredná trieda a trieda III je verejná trieda. Každá trieda obsahuje jeden alebo niekoľko ochranných kľúčov. Napríklad v systéme špecifikujúcom svoje ochranné kľúče v štvorbitovom poli ochranných kľúčov, kde ochranné kľúče sú špecifikované ako kľúče 0-15, môže byť supervizorová trieda ľubovoľne reprezentovaná kľúčom 0. Verejná trieda III môže byť ľubovoľne reprezentovaná kľúčom 0. Stredná trieda II je potom reprezentovaná zostávajúcimi kľúčmi 1-8 a 10-15.

V diagrame na obr. 10 môže každá trieda pristúpiť k sebe samej, ako je vyznačené kruhovou šipkou, ktorá vystupuje z každého kruhu triedy a vracia sa do toho istého kruhu. To predstavuje prípad zhody porovnania niektorého prístupového kľúča s ukladacím kľúčom. Trieda I môže pristúpiť ku ktorejkoľvek inej triede, k strednej triede II alebo k verejnej triede III. Stredná trieda II môže ako k inej triede pristúpiť len k verejnej triede III. Použitím niektorého verejného kľúča v triede III nie je možné pristúpiť k inej triede a verejné kľúče sú podrobené skúške porovnania zhody prístupového kľúča a ukladacieho kľúča prv ako niektorý kľúč verejnej triedy smie vstúpiť do bloku uloženia priradeného inému ukladaciemu kľúču verejnej triedy.

Nasledujúca schéma predstavuje operácie privádzania a uloženia vyplývajúce z použitia ukladacieho kľúča a niektorého prístupového kľúča pri použití troch stavov znázornených na obr. 10 a riadených spôsobom z obr. 9. Nastavenie bitu OP ochrany privedenia v ukladacom kľúči riadi operáciu privedenia, kde F je znázornené s hviezdičkou (*), to je F^* , v tejto schéme:

Štyri porovnávacie obvody 131, 133, 137 a 136 vykonávajú porovnávacie operácie vyjadrené v obr. 9 krokmi 31, 33, 36 a 37, ktoré súčasne, paralelne vykonávajú porovnanie v obr. 11. Výstupné vedenie 71 zaistuje signál "prístup dovolený" znázornený na obr. 1. Výstupné vedenie 72 zaistuje signál "výnimka prístupu" znázornený na obr. 1. To sú funkcie 32 a 41 znázornené na obr. 9.

Na obr. 11 sú znázornené logické obvody a odborníkovi bude zrejmé, že pre realizáciu znázornených obvodov možno použiť niektoré z množstva logických obvodov I, ALEBO, INVERZIA. Každý z porovnávacích obvodov 131, 133, 137 a 136 vykonáva porovnávacie operácie znázornené na obr. 9 a je znázornený na obr. 11 s doplnkovými výstupmi 1 a 0. Výstup 1 je aktívny, keď sa od obvodu žiada podmienka áno na splnenie podmienok v obr. 9 a výstup 0 je aktívny, keď sa žiada podmienka nie na splnenie podmienok na obr. 9.

Vzťah medzi operáciami v obr. 9 a obr. 11 je tento: Signál z ALEBO obvodu 57 predstavuje dráhu áno z kroku 31 alebo z kroku 33 v obr. 11. Hradlo I 55 predstavuje dráhu nie z kroku 37. Signál z niektorého z hradiel I 61, 64 a 67 predstavuje dráhu nie z kroku 38. Signál z niektorého z hradiel I 62, 64 a 67 predstavuje dráhu áno z kroku 42. Signál z niektorého z hradiel I 63, 65 a 68 predstavuje dráhu nie z kroku 42.

Usporiadanie hardwaru v obr. 11 je jedna cesta pre vyhotovenie procesu znázorneného na obr. 9. Na obvody znázornené na obr. 11 môžu byť aplikované metódy Booleovej algebry pre vytvorenie iných zostáv obvodov vykonávajúcich rovnaké operácie. Napríklad množstvo obvodov I a ich vstupov môže byť zlúčené do jedného hradla I pre sled dráh na obr. 9, kde hradlá I 51, 52, 53 a 54 môžu byť skombinované do hradiel I 61-69 pre obmedzenie operácií hradiel I na jedinú úroveň hradiel I.

Vedenie 71 na obr. 11 vedie množstvo signálov z obvodu ALEBO 57 a z hradiel I 63, 65, 68 a 55, z ktorých len jeden

obvod/hradlo zaistuje signál v niektorom čase na vedení 71 pre vyvinutie a vyslanie na výstup signálu "prístup dokončený". Vedenie 72 vedie množstvo signálov z hradiel I 61, 62, 64, 66 a 69, z ktorých len jedno z týchto hradiel zaistuje signál v niektorom čase na vedenie 72 na vyvinutie a vyslanie na výstup signálu "výnimka prístupu".

Hoci bolo popísané prednostné vyhotovenie vynálezu, odborníkovi bude zrejmé, že v podrobnostiach je možné vykonať rad obmien bez toho, aby sa vybočilo z rámca myšlienky vynálezu.

P A T E N T O V É N Á R O K Y

1. Spôsob zaistenia ochrany prístupu pre bloky dát v uložení systému spracovania dát, v ktorom môžu rôzne programy pristúpiť k blokom, vyznačujúci sa tým, že obsahuje kroky: voľbu jedného alebo niekoľkých verejných kľúčov zo všetkých kľúčov dosiahnuteľných pre systém, z ktorých ostatné kľúče sú neverejné kľúče, priradenie niektorého verejného kľúča z verejných kľúčov k zvláštnemu programu v systéme ako verejného prístupového kľúča a priradenie rovnakého verejného kľúča ako verejného ukladacieho kľúča ku každému bloku, ktorý má byť prvotne uložený zvláštnym programom, avšak blok má byť tiež schopný uloženia programom pracujúcim s neverejným prístupovým kľúčom a akýkoľvek blok priradený neverejnému ukladaciemu kľúču nie je schopný uloženia programom priradeným verejnému prístupovému kľúču.

2. Spôsob podľa bodu 1, vyznačujúci sa tým, že ďalej zahrňuje umožnenie uloženia zvláštnym programom v každom bloku priradenom verejnému ukladaciemu kľúču, keď je získaná rovnosť medzi prístupovým kľúčom programu a verejným ukladacím kľúčom a umožnenie uloženia v bloku priradenom verejnému ukladaciemu kľúču inými programami majúcimi neverejné prístupové kľúče, ktoré sa nerovnajú verejnému kľúču.

3. Spôsob podľa bodu 1 alebo 2, vyznačujúci sa tým, že ďalej zahrňuje umožnenie použitia verejného kľúča ako prístupového kľúča a ako ukladacieho kľúča nastavením stavu v počítači na modus verejného kľúča.

4. Spôsob podľa ktoréhokoľvek z bodov 1 až 3, vyznačujúci sa tým, že ďalej zahrňuje zaistenie privádzacieho ochranného poľa v spojení s verejným ukladacím kľúčom priradeným k niektorému bloku a umožnenie programu priradenému k niektorému verejnému kľúču ako jeho verejnému prístupovému kľúču privedenia, nie však

uloženia v bloku priradenom k neverejnému ukladaciemu kľúču, keď je privádzacie ochranné pole vyradené, avšak privedenie do bloku, keď je privádzacie ochranné pole zaradené a vždy zamedzenie uloženia programom užívajúcim verejný prístupový kľúč v niektorom bloku priradenom neverejnému kľúču.

5. Spôsob podľa ktoréhokoľvek z bodov 1 až 4, vyznačujúci sa tým, že ďalej zahrňuje voľbu supervizorového kľúča a nepripúšťa, aby nejaký program používajúci iný prístupový kľúč vykonal uloženie v nejakom inom bloku v uložení priradenom k supervizorovému kľúču.

6. Spôsob podľa ktoréhokoľvek z bodov 1 až 5, vyznačujúci sa tým, že ďalej zahrňuje voľbu kľúča -0 v rozmedzí 0-15 ako supervizorového kľúča a nedovoľuje žiadnemu programu použitie nejakého prístupového kľúča v rozmedzí 1-15 pre uloženie v niektorom bloku v uložení priradenom ukladaciemu kľúču 0.

7. Spôsob podľa bodu 6, vyznačujúci sa tým, že zahrňuje: voľbu kľúča 9 ako verejného kľúča z rozmedzia 0-15 a priradenie kľúčov 1-8 a 10-15 ako neverejných supervizorových vložených kľúčov, ktoré môžu byť použité na prístup k nejakému bloku priradenému verejnému kľúču 9 ako ukladaciemu kľúču.

8. Spôsob zaistenia ochrany prístupu pre bloky uloženia v systéme majúcom súbežné privádzanie niekoľkých programov, vyznačujúci sa tým, že zahrňuje:

zaistenie množiny kľúčov pre zamedzenie ukladacích a privádzacích prístupov nepoverenými programami k priradeným blokom v uložení, voľbu množstva kľúčov v množine ako verejných kľúčov 3. triedy, voľbu iného kľúča v množine ako supervizorového kľúča I. triedy a voľbu zostávajúcich kľúčov v množine ako vložených kľúčov, pričom supervizorové kľúče a vložené kľúče sú neverejné kľúče, a umožnenie niektorému programu priradenému prístupovému kľúču rovnému niektorému neverejnému kľúču v množine mať čítací a zapisovací prístup k niektorému bloku priradenému k ukladaciemu

klúču rovnému niektorému verejnému klúču, avšak umožnenie programu priradenému prístupovému klúču rovnému niektorému verejnému klúču mať čítací a zapisovací prístup k bloku priradenému ukladaciemu klúču rovnému niektorému neverejnému klúču alebo ukladaciemu klúču rovnému niektorému neverejnému klúču alebo ukladaciemu klúču rovnému verejnému klúču odlišnému od prístupového klúča.

9. Spôsob podľa bodu 8, vyznačujúci sa tým, že ďalej zahrňuje umožnenie niektorému programu priradenému neverejnému prístupovému klúču prístup k niektorému bloku uloženia priradenému verejnému klúču bez rovnosti a nevyžadujúcemu žiadne programové inštrukcie pre zmenu neverejného prístupového klúča pre umožnenie programu prístupu k blokom uloženia priradeným k niektorému verejnému klúču pre umožnenie niektorému neverejnému prístupovému klúču prístupu k blokom uloženia užívajúcim rôzne klúče.

10. Spôsob podľa bodu 8 alebo 9, vyznačujúci sa tým, že ďalej zahrňuje:

zaistenie privádzacieho chráneného módu majúceho stavy zapnutia a vypnutia a pridružený ukladací klúč na umožnenie privedenia do pridruženého bloku, keď je stav vypnutia a umožnenie programu s verejným prístupovým klúčom mať privádzací prístup, nie však ukladací prístup do niektorého bloku majúceho niektorý neverejný klúč ako jeho ukladací klúč, keď jeho privádzací ochranný modus je v stave vypnutia, avšak neumožniť privádzací prístup alebo ukladací prístup do bloku majúceho neverejný klúč, keď jeho ukladací klúč má jeho privádzací ochranný modus v stave zapnutia.

11. Prostriedok na ochranu proti nedovolenému prístupu požiadavky programu pre prístup k dátovým jednotkám v blokoch v uložení počítačového systému, vyznačujúci sa tým, že zahrňuje procesor na zistenie adresy dátovej jednotky, ktorá má byť sprístupnená v bloku uloženia a zaistenie prístupového klúča združeného s programom vyžadujúcim prístup do bloku a zaistenie signálu privedenia/uloženia identifikujúceho spôsob prístupu,

prostriedok na privedenie ukladacieho kľúča združeného s adresovaným blokom v uložení, prostriedok na vyskúšanie, či je prístupový kľúč rovný supervizorovému kľúču na zaistenie signálu supervizorového kľúča, prostriedok pre porovnanie prístupového kľúča a ukladacieho na zaistenie rovnakého kľúčového signálu, prostriedok pre určenie, či ukladací kľúč je rovný verejnému kľúču pre zaistenie signálu verejného ukladacieho kľúča, prostriedok pre zistenie, či prístupový kľúč je rovný verejnému kľúču pre zaistenie signálu verejného prístupového kľúča a obvod na umožnenie prístupu k adresovanej dátovej jednotke a poslanie do žiadajúceho procesoru keď (1) je zaistený signál supervizorového kľúča alebo (2) je zaistený rovnaký signál alebo (3) je zaistený signál verejného ukladacieho kľúča a signál neverejného prístupového kľúča a žiaden rovnaký signál a žiaden supervizorový signál, alebo (4) je zaistený signál žiadajúci privedenie a signál verejného prístupového kľúča a žiaden rovnaký signál a žiaden supervizorový signál kdekoľvek je použitie verejného kľúča umožnené, alebo (5) keď je zaistený signál žiadajúci privedenie a signál verejného prístupového kľúča a žiaden rovnaký signál a alebo žiaden supervizorový signál kedykoľvek je použitie verejného kľúča znemožnené.

12. Prostriedok podľa bodu 11, vyznačujúci sa tým, že ďalej zahrňuje:

obvod na vyvíjanie výnimkového signálu pre procesor a zamedzenie poslania adresovanej dátovej jednotky do žiadajúceho procesoru (1) keď je zaistený signál žiadosti uloženia a žiaden signál verejného prístupového kľúča a žiaden rovnaký signál supervizorového kľúča, kdekoľvek je použitie verejného kľúča umožnené, (2) keď je zaistený signál žiadajúci uloženie a signál verejného prístupového kľúča a žiaden rovnaký signál a žiaden signál supervizorového kľúča, kdekoľvek je umožnené použitie verejného kľúča, alebo (3) je zaistený signál žiadajúci uloženie a signál verejného prístupového kľúča a žiaden rovnaký signál, zatiaľ čo použitie verejného kľúča je zamedzené.

13. Prostriedok podľa bodu 12, vyznačujúci sa tým, že ďalej zahrňuje:

obvod tvoriaci kombináciu obvodov I a ALEBO s prostriedkom pre inverziu signálu zaistený pre nestavové podmienky v obvodoch.

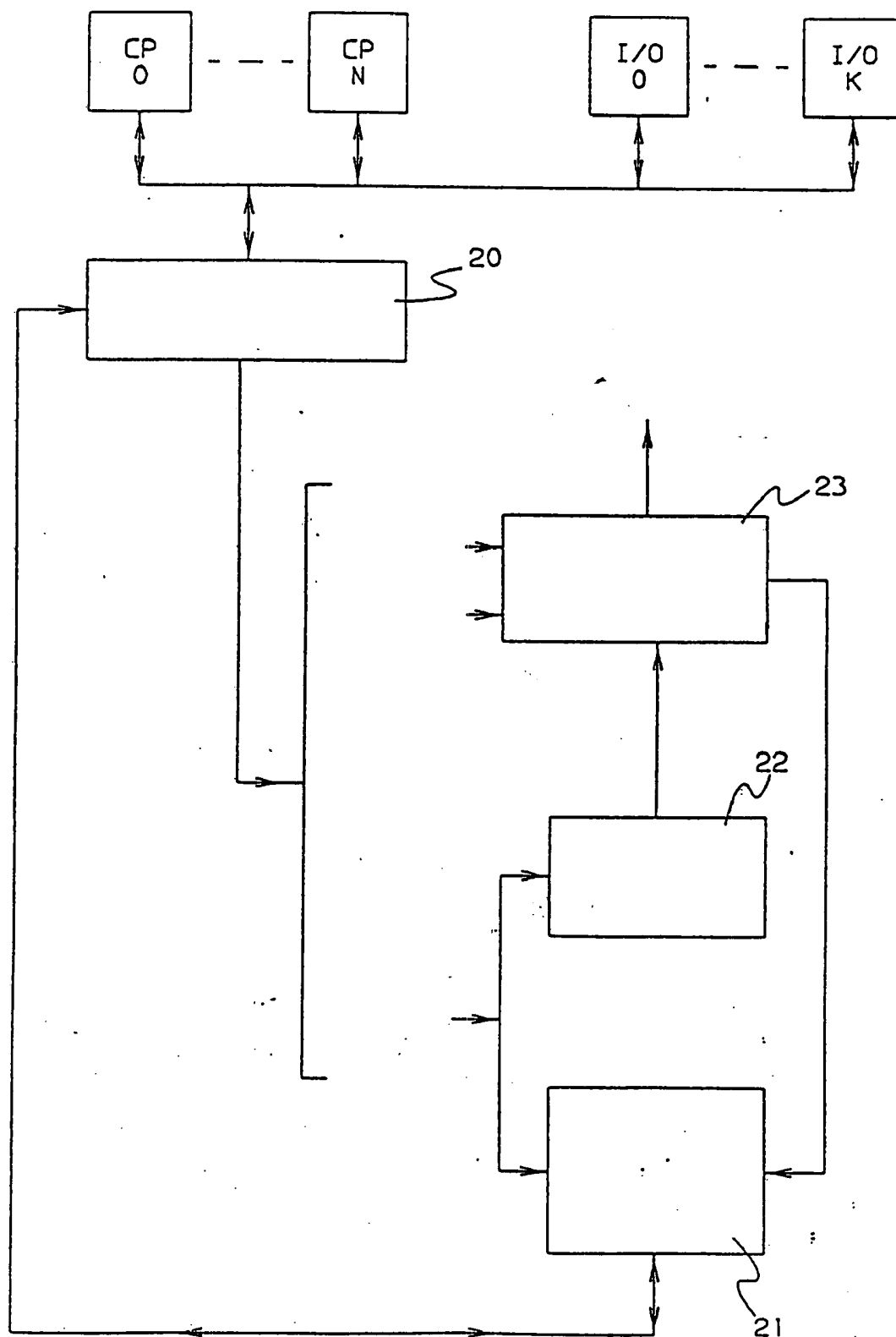
14. Prostriedok podľa ktoréhokoľvek z bodov 11 až 13, vyznačujúci sa tým, že ďalej zahrňuje:

prostriedok pre oznámenie stavu poľa módu verejného kľúča v kontrolnom registri v procesore na oznámenie, či je použitie verejného kľúča umožnené alebo zamedzené.

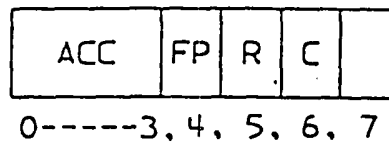
15. Prostriedok podľa bodu 14, vyznačujúci sa tým, že procesor je niektorý z množstva procesorov v počítačovom systéme zahrňujúcim nejaký centrálny procesor alebo nejaký vstupný/výstupný procesor.

1/4

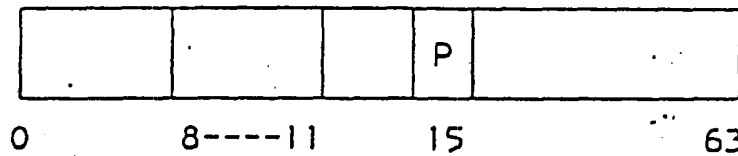
Obr. 1



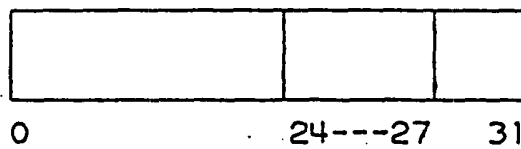
2/4



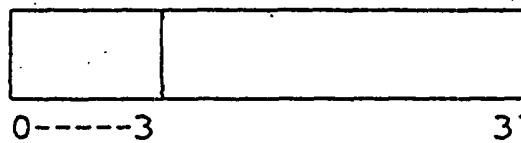
Obr. 2



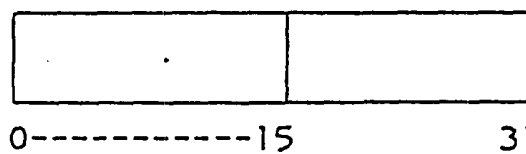
Obr. 3



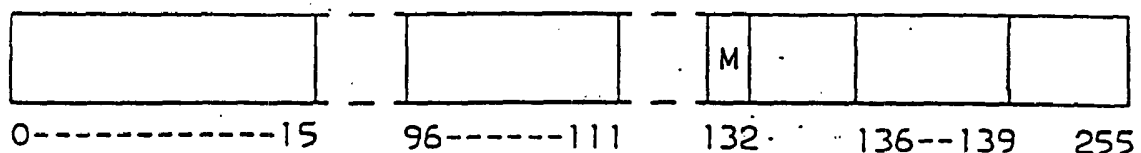
Obr. 4



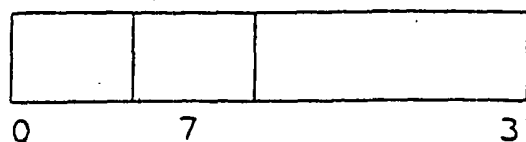
Obr. 5



Obr. 6



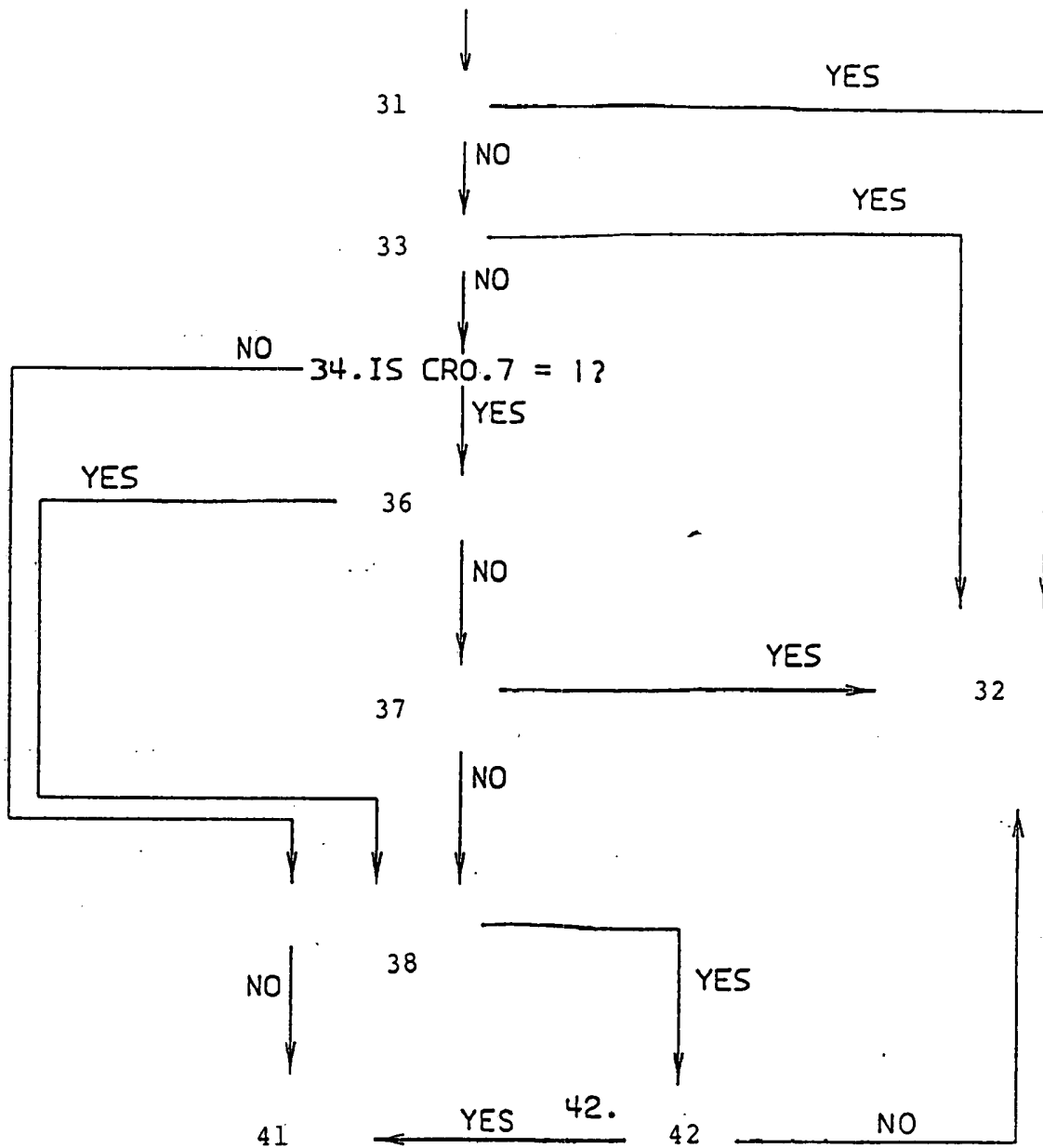
Obr. 7



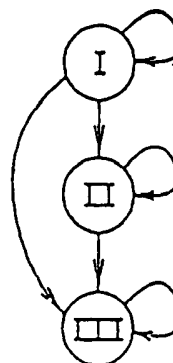
Obr. 8

3/4

Obr. 9



Obr. 10



Obr. 11

