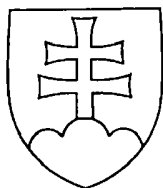


SLOVENSKÁ REPUBLIKA

(19) **SK**



ÚRAD
PRIEMYSELNÉHO
VLASTNÍCTVA
SLOVENSKEJ REPUBLIKY

**ZVEREJNENÁ
PATENTOVÁ PRIHLÁŠKA**

- (22) Dátum podania prihlášky: **24. 1. 2001**
(31) Číslo prioritnej prihlášky: **0166/00
60/226 769**
(32) Dátum podania prioritnej prihlášky: **28. 1. 2000
21. 8. 2000**
(33) Krajina alebo regionálna
organizácia priority: **CH, US**
(40) Dátum zverejnenia prihlášky: **9. 1. 2003**
Vestník ÚPV SR č.: **1/2003**
(62) Číslo pôvodnej prihlášky
v prípade vylúčenej prihlášky:
(86) Číslo podania medzinárodnej prihlášky
podľa PCT: **PCT/IB01/00094**
(87) Číslo zverejnenia medzinárodnej prihlášky
podľa PCT: **WO01/56287**

(11), (21) Číslo dokumentu:

1103-2002

(13) Druh dokumentu: **A3**

(51) Int. Cl.⁷ :

H04N 7/167

(71) Prihlasovateľ: **NAGRACARD S. A., Cheseaux-sur-Lausanne, CH;**

(72) Pôvodca: **Kudelski André, Lutry, CH;
Sasselli Marco, Chardonne, CH;**

(74) Zástupca: **ROTT, RŮŽIČKA & GUTTMANN, v. o. s., Bratislava, SK;**

(54) Názov: **Spôsob a zariadenie na prenos dešifrovacích informácií**

(57) Anotácia:
Každému kanálu na prenos obrazových alebo zvukových signálov vo viackanálovom systéme platenej televízie prislúchajú autorizačné správy (ECM), ktoré umožňujú kanál v súhlase s právami užívateľa dešifrovať. Pri prepínaní kanálov je na overenie práv užívateľa na nový kanál k dispozícii iba veľmi krátky čas. Preto nie je možné na zašifrovanie použiť zložité algoritmy. Vynález prináša systém, ktorý kombinuje autorizačné informácie pre daný kanál (ECM) s autorizačnými informáciami pre skupinu kanálov (MECM). Zatiaľ, čo pre jednokanálové ECM je z hľadiska času nutné použiť rýchly a teda menej zabezpečený šifrovací algoritmus, viackanálové MECM sa môžu zašifrovať zložitejším, časovo náročnejším, ale bezpečnejším algoritmom.

SK 1103-2002 A3

Spôsob a zariadenie na prenos dešifrovacích informácií

Oblasť techniky

Vynález sa týka procesu a systému na prenos dešifrovacích informácií (dát) medzi riadiacim centrom a predplatiteľským dekodérom.

Doterajší stav techniky

Dekodéry, ktoré sú súčasťou zariadenia u predplatiteľov platenej televízie, obsahujú šifrovacie jednotky, ktoré sú schopné spracovávať signály prichádzajúce po káblovej trase alebo rádiovou cestou. Signály môžu byť analógové alebo digitálne.

Signály môžu byť rôznych typov, napríklad hlasové, obrazové alebo riadiace.

Do poslednej kategórie patria administratívne správy (ktoré sa nazývajú EMM správy), ktorými sa prenášajú príkazy k dekodéru alebo skupine dekodérov, a riadiace správy (ECM správy), ktoré okrem iného prenášajú autorizačné informácie potrebné na dešifrovanie dátových signálov.

Vynález sa týka autorizačných správ ECM, ktoré umožňujú dešifrovanie zvukových a obrazových signálov.

Ponuka predložená predplatiteľovi platenej televízie môže zahŕňať mnoho kanálov, z ktorých každý môže byť zašifrovaný pomocou jedného alebo viac konkrétnych kľúčov. Predplatiteľ si teda môže vybrať iba jeden alebo niekoľko kanálov a pritom nemať prístup ku kanálom ostatným, nepožadovaným.

Autorizačné správy ECM sa šifrujú kľúčmi, ktoré zodpovedajú použitému riadiacemu systému. Predplatiteľský dekodér zahrnuje zabezpečovaciu šifrovaciu jednotku, ktorá vie tieto správy dešifrovať. Z bezpečnostných dôvodov sa autorizačné informácie, ktoré umožňujú dešifrovanie užitočných signálov (zvuk

a obraz), periodicky menia. Riadiaci systém ECM správy odosiela v zašifrovanej podobe k šifrovacej jednotke dekodéra, ktorá správy dešifruje, vykoná autorizáciu a podľa prístupových práv predplatiteľa odošle informácie potrebné na dešifrovanie zvuku a obrazu k dekodéru.

Výsledkom dešifrovania v šifrovacej jednotke je "riadiace slovo", ďalej iba CW (control word). Riadiace slovo riadi dekodér a predplatiteľovi sa dostanú požadované dáta v dešifrovanej podobe.

Ako bolo naznačené vyššie, riadiace slová sa pravidelne menia. Bráni sa tým neoprávnenému prístupu k plateným dátam. Riadiace slová sa aktualizujú v pravidelných intervaloch o dĺžke typicky medzi 1 a 20 sekundami. Tento interval sa nazýva kryptoperiódou.

Autorizačné správy ECM sa odosielajú s vyššou frekvenciou, než je kryptoperiódou, napríklad každých 100 milisekúnd. Taký krátky interval je užitočný napríklad pri spúšťaní dekodéra alebo pri prepínaní kanálov.

Riadiace slovo je potrebné na zobrazenie požadovaného programu; prípad, keď by bolo nutné po zapnutí prijímača čakať napríklad 5 sekúnd, než sa obraz objaví, je možné považovať za úplne neprijateľný.

Každý kanál má svoje vlastné riadiace slová, takže pri prepnutí prijímača na iný kanál by bolo nutné čakať do konca kryptoperiódou na prijatie ďalšej autorizačnej správy s dešifrovacími informáciami pre tento kanál. Ako vo vyššie uvedenom prípade, by bolo aj tu niekoľkokundové čakanie na objavenie sa programu veľmi nepríjemné.

Z opísaných dôvodov sa autorizačné správy ECM odosielajú s frekvenciou medzi 5 a 20 za sekundu.

Pri prepnutí kanálu musí byť čas, ktorý uplynie medzi požiadavkou predplatiteľa a zobrazením požadovaného kanálu, krátky. Podľa obvyklých štandardov sa považuje 500 milisekúnd za vyhovujúcu dobu.

Počas tejto doby prebiehajú nasledujúce kroky:

- nastavenie zvukového, obrazového a riadiaceho filtra na nový kanál;
- čakanie na ďalšiu ECM správu so zašifrovaným riadiacim slovom pre tento nový kanál;
- prijatie ECM správy a jej odoslanie k šifrovacej jednotke na dešifrovanie; a
- vykonanie dešifrovacieho algoritmu šifrovacou jednotkou a vrátenie dešifrovaného riadiaceho slova, odoslanie slova k dekodéru;
- zahájenie MPEG dekompresie a čakanie na správu "obraz úplný" od synchronizácie.

Je zrejmé, že kroky sú zretiazené, jeden nadväzuje na druhý, a teda ich nie je možné vykonávať súčasne. Každý z uvedených krokov má teda priamy vplyv na trvanie prepínacej doby pri zmene kanálu.

Vie sa tiež, že čím je šifrovací algoritmus bezpečnejší, tým je dlhší a pribúda operácií potrebných na jeho vypočítanie. Na druhej strane dešifrovanie priamo ovplyvňuje prepínanie doby, ktorá je obmedzená a nie je možné ju ani z dôvodov zlepšeného šifrovania predĺžiť. Preto býva kvalita šifrovacieho algoritmu väčšinou prispôbena dostupnému času na jeho výpočet, aj keď to v dôsledku vedie k menšiemu zabezpečeniu prenášanej informácie.

Známy spôsob riešenia uvedeného problému je opísaný v EP 0 583 202 a spočíva v odosielaní, na danom kanále, autorizačných správ ECM nielen tohto konkrétneho kanála, ale aj kanálov ostatných. ECM ostatných kanálov sa odosiela s nižšou frekvenciou, aby sa zabránilo zahlteniu prenosovej cesty.

Tento známy spôsob má ale niekoľko nedostatkov. Kanál je zaťažovaný väčšinou nepotrebnými správami, okrem toho je nutné tieto autorizačné správy ukladať pre prípad, že budú potrebné pri prepínaní kanálov. Okrem toho sa nerieši možnosť zvýšenia kvality šifrovania (a teda doby trvania dešifrovacej operácie) bez predĺženia prepínacej doby.

Cieľom vynálezu je priniesť spôsob a systém na prenos dešifrovacej informácie, ktoré zaistia väčšiu úroveň zabezpečenia riadiaceho slova pre deko-

dér a to bez predĺženia doby, ktorá je potrebná na spracovanie riadiaceho slova pre konkrétny kanál.

Podstata vynálezu

Uvedený cieľ vynálezu sa v plnom rozsahu dosiahne pomocou riadiaceho slova, ktoré sa získa kombináciou dešifrovania autorizačnej správy ECM, ktorá prislúcha konkrétnemu kanálu, a dešifrovania autorizačnej správy, ktorá je spoločná skupine kanálov.

V ďalšom texte sa budú správy príslušné konkrétnym kanálom označovať ako "jednokanálové autorizačné správy ECM" a správy príslušné celej skupine kanálov ako "viackanálové autorizačné správy MECM (Master ECM)".

Algoritmus spracovania ECM správ je rýchly a preto je jeho bezpečnosť obmedzená. Obmedzujúcim parametrom je predovšetkým prepínacia doba, počas ktorej sa obraz na práve zapnutom kanále musí objaviť.

Podľa vynálezu však výsledné riadiace slovo nezávisí iba na spracovaní jednokanálovej ECM správy. Šifrovacia jednotka, ktorá má spracovávať jednokanálové ECM správy, musí obsahovať už skôr prijaté informácie z viackanálovej MECM správy. Pretože nezávisí na jednotlivých kanáloch, dešifruje sa MECM správa pomocou systémového kľúča.

V okamžiku zmeny alebo prepnutia z jedného kanála na druhý, sa informácia, obsiahnutá v jednokanálovej autorizačnej správe ECM, ktorá prislúcha novo nastavenému kanálu, spojí s informáciou obsiahnutou už vo viackanálovej autorizačnej správe MECM, ktorá je už v šifrovacej jednotke k dispozícii. MECM je spoločná najmenej dvom kanálom. Doba dešifrovania MECM správy neovplyvňuje prepínicu dobu. Teda algoritmus na spracovanie MECM správ môže byť silnejší a môže vyžadovať viac času, avšak neovplyvní prepínicu dobu, pretože sa jeho výpočet vykonáva mimo túto prepínicu dobu a teda ne-spôsobí penalizáciu prepínacieho času. Jednoduchým použitím rôzneho algoritmu sa okrem toho zvyšuje úroveň zabezpečenia systému.

Obsah viackanálovej autorizačnej správy MECM sa môže meniť s rovnakou periódou, ako obsah ECM správ (kryptoperiódou) alebo v násobkoch tejto periódy.

Doba medzi dvoma jednokanálovými ECM správami je dôležitá, pretože priamo ovplyvňuje výpočet maximálnej doby prepnutia medzi dvoma kanálmi. Pre viackanálové MECM správy to ale neplatí. Pretože MECM správa je spoločná skupine kanálov, môže byť doba odosielania týchto správ dlhšia. Jediným okamžikom, keď je periódou MECM dôležitá, je zapnutie dekodéra. Prakticky postačuje odosielať 1 až 2 MECM správy za sekundu.

Prehľad obrázkov

Vynález bude ďalej podrobne opísaný na príkladných uskutočneniach s odkazmi na sprievodné výkresy, na ktorých:

na obr. 1 je znázornené odosielanie ECM a MECM správ na dvoch kanáloch A a B; a

na obr. 2 je bloková schéma zabezpečovacej šifrovacej jednotky.

Príklady uskutočnenia vynálezu

Na obr. 1 sú dvoma čiarami schematicky znázornené správy, ktoré umožňujú dešifrovanie zvukových a obrazových dát, na dvoch kanáloch. Na obr. 1 je možné rozoznať v pravidelných intervaloch prenos jednokanálových autorizačných ECM správ. Na kanále "A" sa v pravidelných intervaloch prenáša jednokanálová autorizačná ECM správa "A", na kanále "B" sa v pravidelných intervaloch prenáša jednokanálová autorizačná ECM správa "B". Obom kanálom "A" a "B" spoločné viackanálové správy MECM sa prenášajú súčasne na oboch kanáloch.

Pokiaľ systém, v ktorom sa vynález použije, používa na prenos dát a informácií analógové vysielanie, prenášajú sa jednokanálové ECM správy aj

viackanálové MECM správy na zvláštnych kanáloch, každému kanálu prislúcha samostatná frekvencia. V digitálnych systémoch frekvencie kanálom priradené nie sú. Viackanálové MECM správy sa môžu pridať k iným správam pre tento kanál alebo sa môžu prenášať v hlavnom dátovom toku bez toho, že by ich bolo nutné opakovať na každom kanále zvlášť.

V príklade podľa obr. 1 je frekvencia odosielania viackanálových MECM správ oproti frekvencii jednokanálových ECM správ polovičná. Frekvencia vysielania viackanálových MECM správ závisí predovšetkým na ešte prijateľnej dešifrovacej dobe pri prvom zapnutí dekodéra. Na zahájenie dešifrovania signálov je nutné mať k dispozícii aspoň jednu jednokanálovú ECM správu a aspoň jednu viackanálovú MECM správu. Opakovanie MECM správy približne každú sekundu je ešte prijateľné a zbytočne nezaťažuje prenosové pásma systému. Po prijatí a spracovaní MECM správy je táto okamžite k dispozícii pri prepínaní kanálov s novou správou (ECM).

Ďalším aspektom vynálezu je, že berie do úvahy zmenšenie kryptoperiody podľa kanálov. Zmenu riadiaceho slova je možné vykonávať v rôznych okamihoch u príslušných kanálov. Napríklad v kanále "A" sa zmení riadiace slovo CW z CW-A1 na CW-A2. Na získanie dešifrovaného riadiaceho slova je potom nutná viackanálová správa MECM-2. Kanál "B" ale pracuje stále s riadiacim slovom CW-B1, na ktorého dešifrovanie je potrebná správa MECM-1. Preto každá viackanálová MECM správa obsahuje informácie príslušné niekoľkým kryptoperiódam, aby neboli rozdiely v synchronizácii kanálov, ktorým je správa spoločná.

Na obr. 2 je naznačené spracovanie informácií z viackanálovej autorizačnej správy MECM. Jednokanálová ECM správa, ktorá obsahuje riadiace slovo CW v zašifrovanej podobe, sa odošle k šifrovacej jednotke CU, ktorá je schopná správu dešifrovať. Na dešifrovanie správy ECM slúžia parametre P_1 , P_2 až P_n , ktoré opisujú práva k systému všeobecne a ku konkrétnemu kanálu zvlášť. Pomocou týchto parametrov jednotka vypočíta riadiace slovo CW. Podľa vynálezu dáta prenášané správou MECM buď menia parametre šifrovacej jednotky alebo jednotkou vypočítané riadiace slovo.

V jednom uskutočnení vynálezu sa konečné riadiace slovo CW získa logickou operáciou, ktorá sa vykoná s informáciami zo správ ECM a MECM. Operáciou môže byť napríklad logické sčítanie, odčítanie, vylučovanie (XOR) alebo násobenie.

V jednom uskutočnení vynálezu sa informácia z viackanálovej správy MECM použije ako sekundárny kľúč na dešifrovanie obsahu jednokanálových správ ECM.

P A T E N T O V É N Á R O K Y

1. Viackanálové prenosové zariadenie zašifrovaných informácií pre platenú televíziu, ktoré zahŕňa riadiace centrum a najmenej jednu predplatiteľskú jednotku, riadiace centrum na vysielanie zašifrovaných signálov a jednokanálových autorizačných správ (ECM) zašifrovaných pre každý kanál, **vyznačujúce sa tým**, že zahŕňa viackanálové autorizačné správy (MECM), ktoré sú spoločné pre skupinu kanálov, pričom tieto správy sú spájané s jednokanálovými autorizačnými správami (ECM) práve prijímaného kanála na dešifrovanie tohto kanála.
2. Viackanálové prenosové zariadenie podľa nároku 1, **vyznačujúce sa tým**, že viackanálové autorizačné správy (MECM) sú zašifrované algoritmom, ktorý je odlišný od algoritmu použitého na zašifrovanie jednokanálových autorizačných správ (ECM).
3. Viackanálové prenosové zariadenie podľa nárokov 1 a 2, **vyznačujúce sa tým**, že viackanálové autorizačné správy (MECM) sú menené s periódou, ktorá je odlišná od periódy jednokanálových autorizačných správ (ECM).
4. Viackanálové prenosové zariadenie podľa nárokov 1 až 3, **vyznačujúce sa tým**, že informácie obsiahnuté vo viackanálovej autorizačnej správe (MECM) sú kombinované s informáciami obsiahnutými v jednokanálových autorizačných správach (ECM) v operácii, akou je sčítanie, odčítanie, vylučovanie (XOR), násobenie alebo kódovanie.

5. Viackanálové prenosové zariadenie podľa nárokov 1 až 3, **vyznačujúce sa tým**, že predplatiteľská jednotka zahrnuje šifrovaciu jednotku (CU), ktorá z jednokanálových autorizačných správ (ECM) určuje riadiace slová (CW), ktoré predplatiteľskej jednotke umožňujú dešifrovať zašifrované signály, kde obsah viackanálových autorizačných správ (MECM) je skombinovaný s parametrami (P1, P2 až Pn) šifrovacieho výpočtu šifrovacej jednotky (CU).

6. Spôsob prenosu viackanálových šifrovaných signálov pre platenú televíziu, ktorý zahrnuje kroky:
 - odoslanie viackanálových zašifrovaných signálov k predplatiteľskej jednotke;
 - odoslanie jednokanálových autorizačných správ (ECM) zašifrovaných pre každý kanál;
 - dešifrovanie autorizačných správ (ECM) pre práve prijímaný kanál v šifrovacej jednotke (CU), pričom dešifrovaná informácia predstavuje riadiace slová (CW), ktoré sú potrebné na dešifrovanie signálov, ktoré zodpovedajú práve prijímanému kanálu;

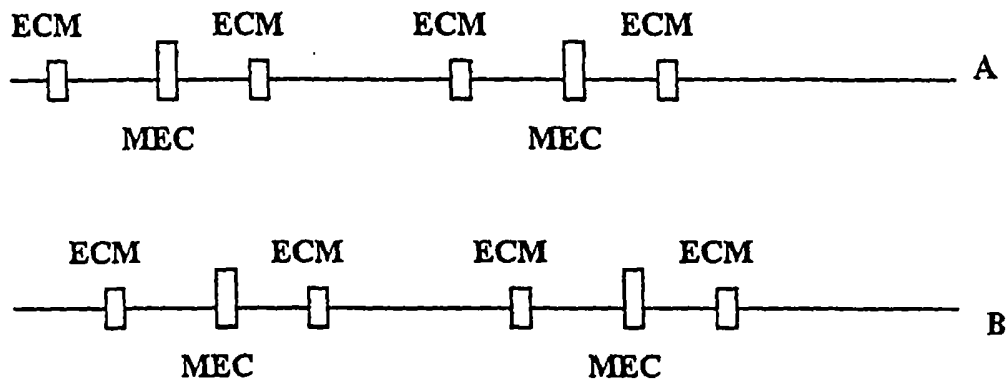
vyznačujúci sa tým, že ďalej zahrnuje kroky:

 - odoslanie viackanálových autorizačných správ (MECM), ktoré sú spoločné pre skupinu kanálov;
 - dešifrovanie viackanálových autorizačných správ (MECM) a spojenie dešifrovanej informácie s informáciou potrebnou na získanie riadiacich slov (CW).

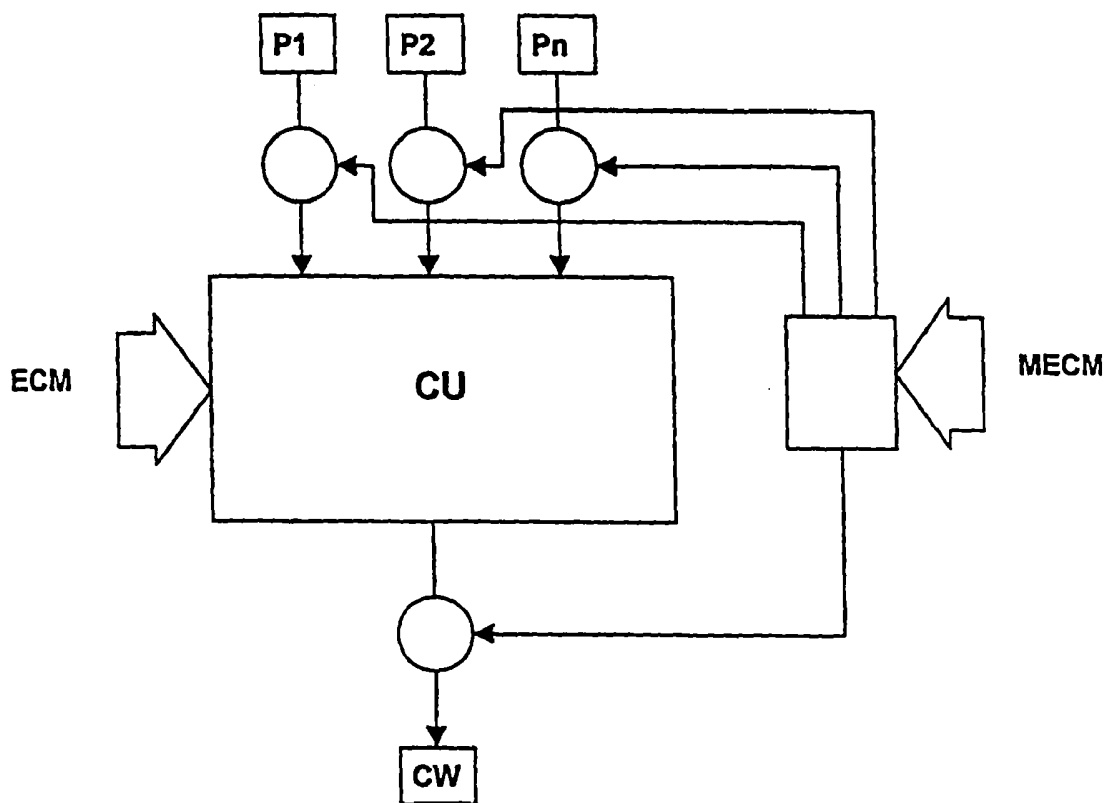
7. Spôsob prenosu viackanálových šifrovaných signálov podľa nároku 6, **vyznačujúci sa tým**, že spojenie sa vykoná na vstupných parametroch (P1, P2 až Pn) šifrovacej jednotky (CU).

8. Spôsob prenosu viackanálových šifrovaných signálov podľa nároku 6, **vyznačujúci sa tým**, že spojenie sa vykoná podľa výsledkov získaných šifrovacou jednotkou (CU).
9. Spôsob prenosu viackanálových šifrovaných signálov podľa nárokov 6 až 8, **vyznačujúci sa tým**, že zahrnuje krok zmeny viackanálových autorizačných správ (MECM) s periódou, ktorá je odlišná od periódy zmeny jednokanálových autorizačných správ (ECM).
10. Spôsob prenosu viackanálových šifrovaných signálov podľa nárokov 6 až 9, **vyznačujúci sa tým**, že zahrnuje krok zašifrovania viackanálových autorizačných správ (MECM) algoritmom, ktorý je odlišný od algoritmu zašifrovania jednokanálových autorizačných správ (ECM).

1/1



Obr. 1



Obr. 2