PATENTOVÝ SPIS

(19) ČESKÁ REPUBLIKA

ÚŘAD PRŮMYSLOVÉHO VLASTNICTVÍ

(21) Číslo přihlášky: **2002-1924**
(22) Přihlášeno: **24.01.2001**
(30) Právo přednosti: **28.01.2000 CH 2000/0166**
21.08.2000 US 2000/226769
(40) Zveřejněno: **13.11.2002**
(Věstník č. 11/2002)
(47) Uděleno: **07.02.2008**
(24) Oznámení o udělení ve Věstníku: **19.03.2008**
(Věstník č. 12/2008)
(86) PCT číslo: **PCT/IB2001/000094**
(87) PCT číslo zveřejnění: **WO 2001/056287**

(11) Číslo dokumentu:
298 949
(13) Druh dokumentu: **B6**
(51) Int. Cl.:
H04N 7/167 (2006.01)

(56) Relevantní dokumenty:
EP 583202; EP 461029.

(73) Majitel patentu:
NAGRACARD S. A., Cheseaux-sur-Lausanne, CH

(72) Původce:
Kudelski André, Lutry, CH
Sasselli Marco, Chardonne, CH

(74) Zástupce:
Ing. Bohuslav Vobořil, Nad Štolou 12, Praha 7, 17000

(54) Název vynálezu:
Způsob a zařízení pro přenos dešifrovacích informací

(57) Anotace:
Každému kanálu pro přenos obrazových nebo zvukových signálů ve vícekanálovém systému placené televize přísluší autorizační zprávy (ECM), které umožňují kanál v souhlasu s právy uživatele kanál dešifrovat. Při přepínání kanálů je pro ověření práv uživatele k novému kanálu k dispozici jen velmi krátký čas. Proto nelze k zašifrování použít složitých algoritmů. Systém kombinuje autorizační informace pro daný kanál (ECM) s autorizačními informacemi pro skupinu kanálů (MECM). Zatímco pro jednokanálové autorizační zprávy (ECM) je z hlediska času nutné použít rychlý a tudíž méně zabezpečený šifrovací algoritmus, vícekanálové autorizační zprávy (MECM) se mohou zašifrovat složitějším, časově náročnějším, ale bezpečnějším algoritmem.

CZ 298949 B6

Způsob a zařízení pro přenos dešifrovacích informací

Oblast techniky

Vynález se týká procesu a systému pro přenos dešifrovacích informací (dat) mezi řídicím centrem a předplatitelským dekodérem.

Dosavadní stav techniky

Dekodéry, které jsou součástí zařízení u předplatitelů placené televize, obsahují šifrovací jednotky, které jsou schopné zpracovávat signály přicházející po kabelové trase nebo rádiovou cestou. Signály mohou být analogové nebo digitální.

Signály mohou být různých typů, například hlasové, obrazové nebo řídicí.

Do poslední kategorie patří správní zprávy (které se nazývají EMM zprávy), kterými se přenáší příkazy k dekodéru nebo skupině dekodérů, a řídicí zprávy (ECM zprávy), které mimo jiné přenáší autorizační informace potřebné pro dešifrování datových signálů.

Vynález se týká, autorizačních zpráv ECM, které umožňují dešifrování zvukových a obrazových signálů.

Nabídka předložená předplatiteli placené televize může zahrnovat mnoho kanálů, z nichž každý může být zašifrován pomocí jednoho nebo více konkrétních klíčů. Předplatitel si tedy může vybrat pouze jeden nebo několik kanálů a přitom nemít přístup ke kanálům ostatním, nepožadovaným.

Autorizační zprávy ECM se šifrují klíči, které odpovídají použitému řídicímu systému. Předplatitelský dekodér zahrnuje zabezpečovací šifrovací jednotku, která umí tyto zprávy dešifrovat. Z bezpečnostních důvodů se autorizační informace, které umožňují dešifrování užitečných signálů (zvuk a obraz), periodicky mění. Řídicí systém ECM zprávy odesílá v zašifrované podobě k šifrovací jednotce dekodéru, která zprávy dešifruje, provede autorizaci a podle přístupových práv předplatitele odešle informace potřebné k dešifrování zvuku a obrazu k dekodéru.

Výsledkem dešifrování v šifrovací jednotce je „řídicí slovo“ , dále jen CW (control word). Řídicí slovo řídí dekodér a předplatiteli se dostane požadovaných dat v dešifrované podobě.

Jak bylo naznačeno výše, řídicí slova se pravidelně mění. Brání se tím neoprávněnému přístupu k placeným datům. Řídicí slova se aktualizují v pravidelných intervalech o délce typicky mezi 1 a 20 sekundami. Tento interval se nazývá kryptoperioda.

Autorizační zprávy ECM se odesílají s vyšší frekvencí než je kryptoperioda, například každých 100 milisekund. Takový krátký interval je užitečný například při spuštění dekodéru nebo při přepínání kanálů.

Řídicí slovo je potřebné pro zobrazení požadovaného programu; případ, kdy by bylo nutné po zapnutí přijímače čekat například 5 sekund, než se obraz objeví, lze považovat za naprosto nepřijatelný.

Každý kanál má svá vlastní řídicí slova, takže při přepnutí přijímače na jiný kanál by bylo nutné čekat do konce kryptoperiody na přijetí další autorizační zprávy s dešifrovacími informacemi pro

tento kanál. Jako ve výše uvedeném případě, by bylo i zde několikasekundové cekání na objevení se programu velmi nepříjemné.

Z popsaných důvodů se autorizační zprávy ECM odesílají s frekvencí mezi 5 a 20 za sekundu.

Při přepnutí kanálu musí být čas, který uplyne mezi požadavkem předplatitele a zobrazením požadovaného kanálu, krátký. Podle obvyklých standardů se považuje 500 milisekund za vyhovující dobu.

V průběhu této doby probíhají následující kroky:

- nastavení zvukového, obrazového a řídicího filtru na nový kanál;

- čekání na další ECM zprávu se zašifrovaným řídicím slovem pro tento nový kanál;

- přijetí ECM zprávy a její odeslání k šifrovací jednotce pro dešifrování; a

- provedení dešifrovacího algoritmu šifrovací jednotkou a vrácení dešifrovaného řídicího slova, odeslání slova k dekodéru;

- zahájení MPEG dekomprese a cekání na zprávu „obraz úplný“ od synchronizace.

Je zřejmé, že kroky jsou zřetězené, jeden navazuje na druhý, a tudíž je nelze provádět současně. Každý z uvedených kroků má tudíž přímý vliv na trvání přepínací doby při změně kanálu.

Ví se také, že čím je šifrovací algoritmus bezpečnější, tím je delší a přibývá operací potřebných k jeho vypočtení. Na druhé straně dešifrování přímo ovlivňuje přepínací dobu, která je omezená a nelze ji ani z důvodů zlepšeného šifrování prodloužit. Proto bývá kvalita šifrovacího algoritmu většinou přizpůsobena dostupnému času na jeho výpočet, i když to v důsledku vede k menšímu zabezpečení přenášené informace.

Známý způsob řešení uvedeného problému je popsán v EP 0 583 202 a spočívá v odesílání, na daném kanále, autorizačních zpráv ECM nejen onoho konkrétního kanálu, ale i kanálů ostatních. ECM ostatních kanálů se odesílají s nižší frekvencí, aby se zabránilo zahlcení přenosové cesty.

Tento známý způsob má ale několik nedostatků. Kanál je zatížen většinou nepotřebnými zprávami, navíc je nutné tyto autorizační zprávy ukládat pro případ, že budou potřebné při přepínání kanálů. Navíc se neřeší možnost zvýšení kvality šifrování (a tudíž doby trvání dešifrovací operace) bez prodloužení přepínací doby.

Cílem vynálezu je přinést způsob a systém pro přenos dešifrovací informace, které zajistí větší úroveň zabezpečení řídicího slova pro dekodér, a to bez prodloužení doby, která je potřebná ke zpracování řídicího slova pro konkrétní kanál.

Podstata vynálezu

Uvedeného cíle vynálezu se v plném rozsahu dosáhne s pomocí řídicího slova, které se získá kombinací dešifrování autorizační zprávy ECM, která přísluší konkrétnímu kanálu, a dešifrování autorizační zprávy, která je společná skupině kanálů.

V dalším textu se budou zprávy příslušné konkrétním kanálům označovat jako „jednokanálové autorizační zprávy ECM“ a zprávy příslušné celé skupině kanálů jako „vícekanálové autorizační

zprávy MECM (Master ECM)".

Algoritmus zpracování ECM zpráv je rychlý a proto je jeho bezpečnost omezená. Omezujícím parametrem je zejména přepínací doba, za kterou se obraz na právě zapnutém kanálu musí objevit.

Podle vynálezu však výsledné řídicí slovo nezávisí jen na zpracování jednokanálové ECM zprávy. Šifrovací jednotka, která má zpracovávat jednokanálové ECM zprávy, musí obsahovat již dříve přijaté informace z vícekanálové MECM zprávy. Protože nezávisí na jednotlivých kanálech, dešifruje se MECM zpráva pomocí systémového klíče.

V okamžiku změny nebo přepnutí z jednoho kanálu na druhý, se informace, obsažená v jednokanálové autorizační zprávě ECM, která přísluší nově nastavenému kanálu, spojí s informací obsaženou už vícekanálové autorizační zprávě MECM, která je již v šifrovací jednotce k dispozici. MECM je společná nejméně dvěma kanálům. Doba dešifrování MECM zprávy neovlivňuje přepínací dobu. Tedy, algoritmus pro zpracování MECM zpráv může být silnější a může vyžadovat více času, avšak neovlivní přepínací dobu, protože se jeho výpočet provádí mimo tuto přepínací dobu a tudíž nezpůsobí penalizaci přepínacího času. Jednoduchým použitím různého algoritmu se navíc zvyšuje úroveň zabezpečení systému.

Obsah vícekanálové autorizační zprávy MECM se může měnit se stejnou periodou jako obsah ECM zpráv (kryptoperioda) nebo v násobcích této periody.

Doba mezi dvěma jednokanálovými ECM zprávami je důležitá, protože přímo ovlivňuje výpočet maximální doby přepnutí mezi dvěma kanály. Pro vícekanálové MECM zprávy to ale neplatí. protože MECM zpráva je společná skupině kanálů, může být doba odesílání těchto zpráv delší. Jediným okamžikem, kdy je perioda MECM důležitá, je zapnutí dekodéru. Prakticky postačuje odesílat 1 až 2 MECM zprávy za sekundu.

Přehled obrázků

Vynález bude dále podrobně popsán na příkladných provedeních s odkazy na doprovodné výkresy, na nichž :

Na obr. 1 je znázorněno odesílání ECM a MECM zpráv na dvou kanálech A a B; a

na obr. 2 je blokové schéma zabezpečovací šifrovací jednotky.

Příklady provedení vynálezu

Na obr. 1 jsou dvěma čarami schematicky znázorněny zprávy, které umožňují dešifrování zvukových a obrazových dat, na dvou kanálech. Na obr. 1 lze seznat v pravidelných intervalech přenos jednokanálových autorizační ECM zpráv. Na kanálu „A" se v pravidelných intervalech přenáší jednokanálová autorizační ECM zpráva „A", na kanálu „B" se v pravidelných intervalech přenáší jednokanálová autorizační ECM zpráva „B". Oběma kanálům „A" a „B" společné vícekanálové zprávy MECM se přenáší současně na obou kanálech.

Pokud systém, v němž se vynález použije, používá pro přenos dat a informací analogového vysílání, přenáší se jednokanálové ECM zprávy i vícekanálové MECM zprávy na zvláštních kanálech, každému kanálu přísluší samostatná frekvence. V digitálních systémech frekvence kanálům přiřazeny nejsou. Vícekanálové MECM zprávy se mohou přidat k jiným zprávám pro

tento kanál nebo se mohou přenášet v hlavním datovém toku bez toho, že by je bylo nutné opakovat na každém kanálu zvlášť.

V příkladě dle obr. 1 je frekvence odesílání vícekanálových MECM zpráv oproti frekvenci jednokanálových ECM zpráv poloviční. Frekvence vysílání vícekanálových MECM zpráv závisí především na ještě přijatelné dešifrovací době při prvním zapnutí dekodéru. K zahájení dešifrování signálů je nutné mít k dispozici alespoň jednu jednokanálovou ECM zprávu a alespoň jednu vícekanálovou MECM zprávu. Opakování MECM zprávy přibližně každou sekundu je ještě přijatelné a zbytečně nezatěžuje přenosová pásma systému. Po přijetí a zpracování MECM zprávy je tato okamžitě k dispozici při přepínání kanálů s novou zprávou (ECM).

Dalším aspektem vynálezu je, že bere v úvahu zmenšení kryptoperiody podle kanálů. Změnu řídicího slova lze provádět v různých okamžicích u příslušných kanálů. Například v kanálu „A" se změní řídicí slovo CW z CW-A1 na CW-A2. K získání dešifrovaného řídicího slova je potom nutná vícekanálová zpráva MECM-2. Kanál „B" ale pracuje stále s řídicím slovem CW-81, k jehož dešifrování je potřebná zpráva MECM-1. Proto každá vícekanálová MECM zpráva obsahuje informace příslušné několika kryptoperiodám, aby nebyly rozdíly v synchronizaci kanálů, kterým je zpráva společná.

Na obr. 2 je naznačeno zpracování informací z vícekanálové autorizační zprávy MECM. Jednokanálová ECM zpráva, která obsahuje řídicí slovo CW v zašifrované podobě, se odešle k šifrovací jednotce CU, která je schopna zprávu dešifrovat. K dešifrování zprávy ECM slouží parametry P1, P2 až Pn, které popisují práva k systému obecně a ke konkrétnímu kanálu zvláště. Pomocí těchto parametrů jednotka vypočte řídicí slovo CW. Podle vynálezu se data přenášená zprávou MECM bud´ mění parametry šifrovací jednotky, nebo jednotkou vypočtené řídicí slovo.

V jednom provedení vynálezu se konečné řídicí slovo CW získá logickou operací, která se provede s informacemi ze zpráv ECM a MECM. Operací může být například logické sčítání, odčítání, vylučování (XOR) nebo násobení.

V jednom provedení vynálezu se informace z vícekanálové zprávy MECM použije jako sekundární klíč pro dešifrování obsahu jednokanálových zpráv ECM.

PATENTOVÉ NÁROKY

1. Vícekanálové přenosové zařízení zašifrovaných informací pro placenou televizi, které zahrnuje řídicí centrum a nejméně jednu předplatitelskou jednotku, řídicí centrum pro vysílání zašifrovaných signálů a jednokanálových autorizačních zpráv (ECM) zašifrovaných pro každý kanál, **vyznačující se tím**, že zahrnuje vícekanálové autorizační zprávy (MECM), které jsou společné pro skupinu kanálů, přičemž tyto zprávy jsou spojovány s jednokanálovými autorizačními zprávami (ECM) právě přijímaného kanálu pro dešifrování tohoto kanálu.

2. Vícekanálové přenosové zařízení podle nároku 1, **vyznačující se tím**, že vícekanálové autorizační zprávy (MECM) jsou zašifrovány algoritmem, který je odlišný od algoritmu použitého k zašifrování jednokanálových autorizačních zpráv (ECM).

3. Vícekanálové přenosové zařízení podle nároků 1 a 2, **vyznačující se tím**, že vícekanálové autorizační zprávy (MECM) jsou měněny s periodou, která je odlišná od periody jednokanálových autorizačních zpráv (ECM).

4. Vícekanálové přenosové zařízení podle nároků 1 až 3, **vyznačující se tím**, že informace obsazené ve vícekanálové autorizační zprávě (MECM) jsou kombinovány s informacemi obsaženými v jednokanálových autorizačních zprávách (ECM) v operaci, jakou je sčítání, odečítání, vylučování (XOR), násobení nebo kódování.

5. Vícekanálové přenosové zařízení podle nároků 1 až 3, **vyznačující se tím**, že předplatitelská jednotka zahrnuje šifrovací jednotku (CU), která z jednokanálových autorizačních zpráv (ECM) určuje řídicí slova (CW), která předplatitelské jednotce umožňují dešifrovat zašifrované signály, kde obsah vícekanálových autorizačních zpráv (MECM) je zkombinován s parametry (P1, P2 až Pn) šifrovacího výpočtu šifrovací jednotky (CU).

6. Způsob přenosu vícekanálových šifrovaných signálů pro placenou televizi, který zahrnuje kroky:

- odeslání vícekanálových zašifrovaných signálů k předplatitelské jednotce;

- odeslání jednokanálových autorizačních zpráv (ECM) zašifrovaných pro každý kanál;

- dešifrování autorizačních zpráv (ECM) pro právě přijímaný kanál v šifrovací jednotce (CU), přičemž dešifrovaná informace představuje řídicí slova (CW), která jsou potřebná pro dešifrování signálů, které odpovídají právě přijímanému kanálu;

vyznačující se tím, že dále zahrnuje kroky:

- odeslání vícekanálových autorizačních zpráv (MECM), které jsou společné pro skupinu kanálů;

- dešifrování vícekanálových autorizačních zpráv (MECM) a spojení dešifrované informace s informací potřebnou pro získání řídicích slov (CW).

7. Způsob přenosu vícekanálových šifrovaných signálů podle nároku 6, **vyznačující se tím**, že spojení se provede na vstupních parametrech (P1, P2 až Pn) šifrovací jednotky (CU).

8. Způsob přenosu vícekanálových šifrovaných signálů podle nároku 6, **vyznačující se tím**, že spojení se provede podle výsledků získaných šifrovací jednotkou (CU).

9. Způsob přenosu vícekanálových šifrovaných signálů podle nároků 6 až 8, **vyznačující se tím**, že zahrnuje krok změny vícekanálových autorizačních zpráv (MECM) s periodou, která je odlišná od periody změny jednokanálových autorizačních zpráv (ECM).

10. Způsob přenosu vícekanálových šifrovaných signálů podle nároků 6 až 9, **vyznačující se tím**, že zahrnuje krok zašifrování vícekanálových autorizačních zpráv (MECM) algoritmem, který je odlišný od algoritmu zašifrování jednokanálových autorizačních zpráv (ECM).

1 výkres

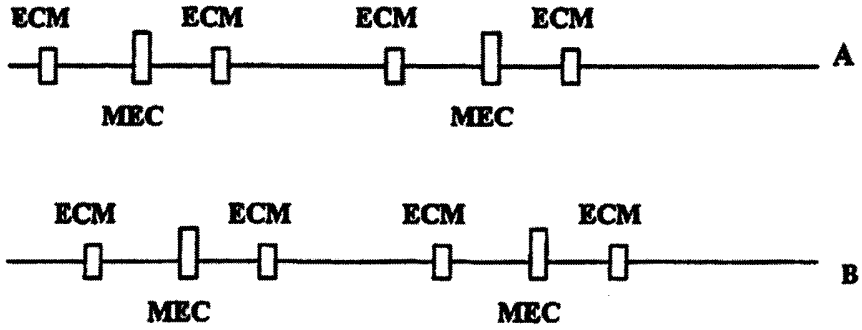

Fig. 1

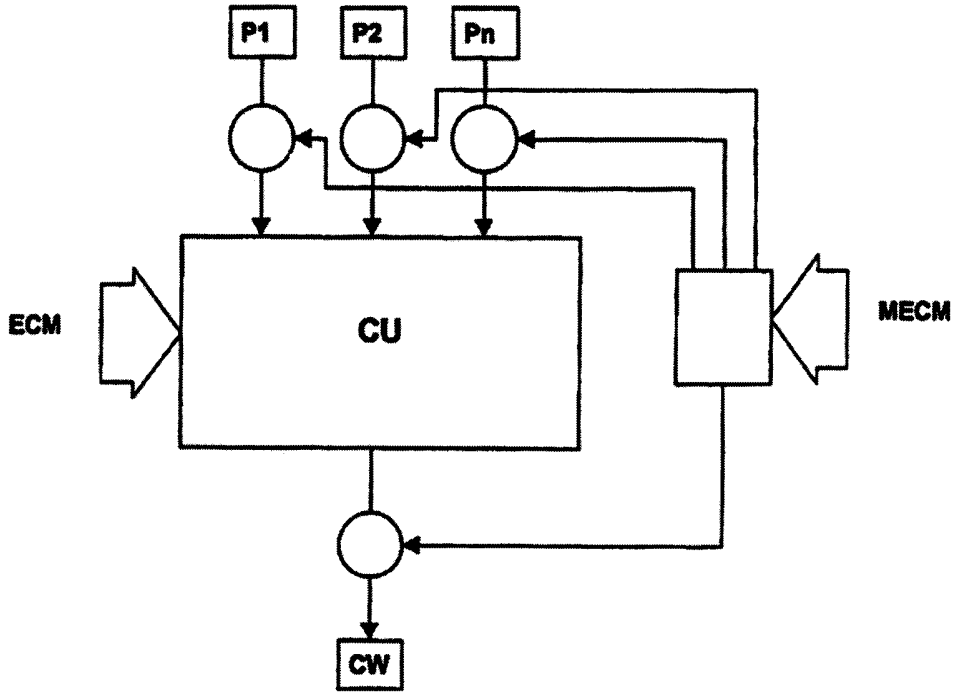

Fig. 2

Konec dokumentu