

Eljárás és dekóder továbbított csomag adatáram feldolgozására, továbbá hordozható biztonsági modul a dekóderhez**Kivonat**

A találmány tárgya egyrészt egy dekóder egy továbbított csomag adatáram feldolgozására, ahol a továbbított adatáram a csomag hasznos részekbe illesztett csomagokra bontott adatokat tartalmaz, másrészt hordozható biztonsági modul a javasolt dekóderben való használatra, harmadrészt egy eljárás a csomag hasznos részben megtalálható csomagokra bontott adatokat tartalmazó továbbított csomagáram feldolgozására. A javasolt eljárás, dekóder és hordozható biztonsági modul a digitális jelátviteli rendszerekben, különösen a digitális televízió rendszerekben használható előnyösen.

A dekóder egyik megoldás szerint egy hordozható biztonsági modultól egy meghatározott biztonsági modul rendszer azonosítót fogadó eszközt, továbbá a dekódert a kapott azonosító függvényében konfiguráló eszközt, továbbá a meghatározott biztonsági modul rendszerrel társított csomagokra bontott adatok szűrésére, szűrési adatokat a hordozható biztonsági modultól fogadó eszközt, valamint a kapott szűrési adatok függvényében csomagokra bontott adatokat szűrő eszközt tartalmaz, másik megoldás szerint a csomagokra bontott adatokból egy meghatározott biztonsági modul rendszerrel társított adatokat kiválasztó első szűrő eszközt, valamint az egy hordozható biztonsági modultól kapott szűrési adatok függvényében a kiválasztott adatokat tovább szűrő második szűrő eszközzel rendelkezik.

A hordozható biztonsági modul egy meghatározott biztonsági modul rendszer azonosító eltárolására szolgáló memória eszközt, valamint az azonosítót a dekóder konfigurálásához a dekóderhez továbbító eszközt tartalmaz.

Az eljárás során egyik megoldás szerint a hordozható biztonsági modultól egy meghatározott biztonsági modul rendszer azonosítóját vesszük, a dekódert a vett azonosító függvényében konfiguráljuk, a hordozható biztonsági modultól vesszük a meghatározott biztonsági modul rendszerrel társított csomagokra bontott adatok szűréséhez szükséges szűrési adatokat, és a csomagokra bontott adatokat a kapott szűrési adatok függvényében szűrjük, másik megoldás szerint a csomagokra bontott adatokból egy meghatározott biztonsági modul rendszerrel társított adatokat választunk ki, és a kiválasztott adatokat egy hordozható biztonsági modultól kapott szűrési adatok függvényében szűrjük.

~~(7. ábra)~~

(—)

2001. 06. 28.

Henry Celuti

Eljárás és dekóder továbbított csomag adatáram feldolgozására, továbbá hordozható biztonsági modul a dekóderhez

A találmány tárgya egyrészt egy dekóder egy továbbított csomag adatáram feldolgozására, ahol a továbbított adatáram a csomag hasznos részekbe illesztett csomagokra bontott adatokat tartalmaz, másrészt hordozható biztonsági modul a javasolt dekóderben való használatra, harmadrészt egy eljárás a csomag hasznos részben megtalálható csomagokra bontott adatokat tartalmazó továbbított csomagáram feldolgozására. A javasolt eljárás, dekóder és hordozható biztonsági modul a digitális jelátviteli rendszerekben, különösen a digitális televízió rendszerekben használható előnyösen.

A hagyományos digitális televízió műsorszóró rendszerek az adatokat különálló szállítási adatáram csomagok formájában továbbítják, amelynek során minden egyes csomag előre meghatározott hosszúságú, és egy élőfejből valamint hasznos adatból áll. Ezen a területen a jelenleg előszeretettel alkalmazott szabvány az MPEG szabvány, amely előre meghatározza többek között a szállító csomagok formátumát.

A csomag élőfej általánosságban a csomagra vonatkozó leíró adatot tartalmaz, míg a hasznos adat a vevőben feldolgozandó adatot jelenti. A csomag élőfej a csomagot azonosító csomagazonosítót foglal magában. A csomagban lévő hasznos adat pedig audio, video vagy egyéb adat lehet, például feltételes hozzáférési rendszerre vonatkozó adat lehet.

Hagyományos esetben a beérkező adatáramot a vevő és dekódoló berendezés az egyes csomagok csomagazonosítója alapján szűri. Az azonnali feldolgozást igénylő adatokat, mint amilyenek a vizuális adatok, szokásos elnevezéssel csomagokra bontott elemi adatáram formájában juttatják el a megfelelő processzorhoz. Ez a folyamatos adatfolyam, amely a továbbított csomagok hasznos adatainak a feldolgozásával alakul ki, olyan csomagsorozatot tartalmaz, amelyben az egyes csomagra bontott elemi adatáram csomagok ugyancsak egy-egy csomag élőfejet, valamint hasznos adatot tartalmaznak.

A csomagokra bontott elemi adatáram adatokon túlmenően a továbbított csomagok hasznos adatai között egyéb, azonnali feldolgozást nem igénylő adatok is elhelyezhetők. Eltérően a csomagokra bontott elemi adatáramok adataitól, amelyeket valósidejű kimenet előállítására céljából egy processzor nyomban feldolgoz, ezeket az adatokat a processzor jellemző módon aszinkron módon dolgozza fel. Ebben az esetben a továbbított csomagok hasznos adatai között található adatokat olyan szekciók vagy táblázatok sorozatává bont-

ják, melyek mindegyike egy élőfejet és külön hasznos adatot tartalmaz, ahol az élőfejekben a táblázatot azonosító táblázat azonosító van elhelyezve.

Olyan esetekben, amikor egy adáshoz korlátozott a hozzáférés, például fizető televízió rendszer esetében (pay TV), a korlátozott hozzáférésre vonatkozó adatokat az adás során a továbbított adatáramban lévő táblázatba vagy szekcióba foglalhatják bele. Ezeket a feltételes hozzáférésre vonatkozó adatokat a dekóderrel tudjuk szűrni, és egy hordozható biztonsági modulhoz, például a dekóderbe behelyezett programozható csipkártyához továbbíthatjuk. Az adatokat ilyen esetben a programozható csipkártyával feldolgozzuk, hogy például olyan ellenőrző szót hozzunk segítségével létre, amelyet azt követően a dekóder használ fel egy adás bitsordekódolásához.

Jelentős problémát jelent az az adatmennyiség, amelyet a dekóderrel veszünk és feldolgozunk, ezen belül különösen a biztonsági modulhoz továbbított feltételes hozzáférésre vonatkozó adatok mennyisége. Ez a kérdés azért lényeges, mert a biztonsági modul processzorának a jelfeldolgozó kapacitása, továbbá a dekóder és a biztonsági modul közötti kommunikációs csatorna kapacitása szűkös lehet egy meghatározott üzenetmennyiség lekezeléséhez és feldolgozásához. Ez a probléma folyton nő, ahogy a több feltételes hozzáférésű üzenetet is tartalmazó programok száma is nő, amelyek lehetővé teszik, hogy különböző kezelők férjenek hozzá ugyanahhoz a programhoz (például futball mérkőzéshez, vagy valamilyen tematikus televíziós csatornához).

A kitűzött feladatot egyrészt egy továbbított csomag adatáram feldolgozására szolgáló dekóderrel oldottuk meg, ahol a továbbított adatáram a csomag hasznos részekbe illesztett csomagokra bontott adatokat tartalmaz. Újszerű módon a dekóder egy hordozható biztonsági modultól egy meghatározott biztonsági modul rendszer azonosítót fogadó eszközt, továbbá a dekódert a kapott azonosító függvényében konfiguráló eszközt, továbbá a meghatározott biztonsági modul rendszerrel társított csomagokra bontott adatok szűrésére, szűrési adatokat a hordozható biztonsági modultól fogadó eszközt, valamint a kapott szűrési adatok függvényében csomagokra bontott adatokat szűrő eszközt tartalmaz.

A különböző biztonsági modulok különböző biztonsági modul rendszerekkel társíthatók, ahol minden egyes biztonsági modul a hozzátartozó meghatározott rendszerre vonatkozó azonosítót tárol. Ha a biztonsági modult először összekötjük a dekóderrel, vagy behelyezzük a dekóderbe, akkor a biztonsági modul ezt a benne eltárolt azonosítót megadja a dekódernek. A javasolt dekóder egy előnyös kiviteli alakja értelmében a konfigurálást vég-

ző eszköz ezután a dekódert a kapott azonosító függvényében tudja konfigurálni annak érdekében, hogy a csomagokra bontott adatokból a meghatározott biztonsági modul rendszerrel társított adatokat válasszon ki. Ezzel a dekódert több különböző biztonsági modul rendszer valamelyikéhez egyszerű, olcsó és hatékony módon tudjuk konfigurálni.

Mint fent jeleztük, a szűrést végző eszköz úgy konfigurálható, hogy a biztonsági modultól kapott szűrési adatok függvényében a csomagokra bontott adatokat szűrni tudja. Ezáltal lehetővé válik a szűrést végző eszköz számára, hogy úgy konfiguráljuk, hogy a kiválasztott csomag adatokból csupán a biztonsági modul számára érdekes csomag adatokat szűrje ki. Ezzel biztosítani tudjuk, hogy a biztonsági modulhoz juttatott adatáramot a biztonsági modul jelfeldolgozó képességeihez igazodóan a lehető legnagyobb mértékben lecsökkentsük.

Egy előnyös kialakítás szerint a biztonsági modul rendszer azonosítóját fogadó, valamint a dekódert konfiguráló eszközök a dekóderben tárolt alkalmazással rendelkeznek, és a szűrési adatok fogadására, valamint a csomagokra bontott adatok szűrésére alkalmas eszközök szűrőt tartalmaznak.

A szűrő eszközt a konfigurálást végző eszközökkel úgy konfigurálhatjuk, hogy a csomagokra bontott adatokból a meghatározott biztonsági modul rendszerrel társított adatokat válasszunk ki, amelyeket azt követően a kapott szűrési adatok függvényében szűrni tudunk.

A javasolt dekóder egy további előnyös kiviteli alakja értelmében az azonosító egy meghatározott feltételes hozzáférési rendszer azonosítóját foglalja magában. A dekódert úgy konfigurálhatjuk, hogy a csomagokra bontott adatokból kizárólag a biztonsági modul által használt feltételes hozzáférési rendszerrel társított adatokat válassza ki. Ezzel a dekódert igen egyszerűen alkalmassá tehetjük számos különböző, az egyes szolgáltatók által használt feltételes hozzáférési rendszerekkel való együttműködésre. Így az előfizetőt nem korlátozzuk le például magával a dekóderrel csupán egy meghatározott feltételes hozzáférési rendszerre.

Ugyancsak előnyös a találmány értelmében, ha a szűrő eszköz a csomagokra bontott adatokból egy program térkép táblázatot és egy feltételes hozzáférés táblázatot tartalmazó továbbított csomagokat kiválasztó eszköz. Ugyancsak előnyös a javasolt dekóder olyan kiviteli alakja, amelynél a konfigurálást végző eszköz a program térkép táblázatot és a feltételes hozzáférés táblázatot a szűrő eszköztől fogadó, és a szűrő eszközt a kapott azonosító és

a program térkép táblázatban és a feltételes hozzáférés táblázatban lévő adatok függvényében konfiguráló eszközként van megvalósítva. Ezáltal a szűrést végző eszközt alkalmassá tudjuk tenni arra, hogy a meghatározott feltételes hozzáférési rendszerrel társított adatok csomag azonosítóját könnyű szerrel be tudja azonosítani.

A találmány szerinti dekóder egy további előnyös kiviteli alakja értelmében a szűrő eszköz a továbbított adatáramból kiválasztott csomag adatokra vonatkozó legalább egy táblázat azonosítót vagy szekció azonosítót tartalmazó szűrési adatok függvényében konfigurálható eszközként van megvalósítva. A biztonsági modultól származó információ függvényében a táblázat vagy szekció szintjén végrehajtott adatszűrés sokkal pontosabb azonosítást és adatkiválasztást tesz lehetővé, például biztosítja, hogy a modulhoz címzett releváns feltételes hozzáférési üzeneteket kiválaszthassuk. A szűrő eszköz hasonlóképpen konfigurálható a hordozható biztonsági modultól kapott egyéb adatokkal kapcsolatosan is.

Ugyancsak előnyös a javasolt dekóder olyan kiviteli alakja, amelyben az azonosító a biztonsági modul által használt meghatározott elszámolási rendszer azonosítót tartalmaz. A különböző biztonsági modulok különböző elszámolási rendszereket használhatnak, például a "nézd és fizess" vagy "töltsd le és fizess" típusú eseményekért. Például a biztonsági modul elektronikus zsetonokat tartalmazó elektronikus pénztárcával látható el, ahol a pénztárcában lévő zsetonok száma egy-egy alkalom, esemény "megvásárlásakor" eggyel-eggyel csökken. Alternatív megoldásként a biztonsági modul hitelkártya tulajdonságokkal is felruházható, amelyek viszont azt teszik szükségessé, hogy a dekóder ki tudja olvasni a hitelkártya adatait, és azokat továbbítani tudja a bankhoz, annak érdekében, hogy egy esemény "megvásárlásakor" a megfelelő összeggel meg tudja terhelni az előfizető számláját. Ha a biztonsági modul adja át az azonosítót a dekódernek, akkor ezzel a biztonsági modulon keresztül tudjuk a dekódert konfigurálni, hogy a biztonsági modul által támogatott módon hajtsa végre a megterhelési műveletet.

Ugyancsak előnyös a javasolt dekóder olyan lehetséges kiviteli alakja, amelynél alternatív módon vagy járulékosan az azonosító a biztonsági modul által használt meghatározott jóváíró rendszer azonosítót tartalmaz. Ebben az esetben szintén igaz, hogy a különböző biztonsági modulok különböző jóváíró rendszereket használhatnak. Például a biztonsági modulban tárolt, elektronikus zsetonokat tartalmazó pénztárca tartalmaz megnövelhető, vagy az előfizető bankszámlája jóváírható valamekkora összeggel a program szolgáltatója részéről olyan esetekben, ha az előfizető például valamilyen reklámozott eseményt, például egy

italreklámot bizonyíthatóan megtekinthet. Ha a biztonsági modullal adjuk meg az azonosítót a dekóder számára, akkor a biztonsági modullal tudjuk a dekódert konfigurálni ahhoz, hogy a biztonsági modul által támogatott módon végrehajtsa a jóváírási műveletet.

Egy további lehetséges és előnyös kiviteli alak értelmében a szűrő eszköz első szűrő eszközt, például első szűrő készletet tartalmaz, a csomagokra bontott adatokból egy meghatározott biztonsági modul rendszerrel társított adatok kiválasztására, valamint második szűrő eszközt, például egy második szűrő készletet tartalmaz, a szűrési adatok függvényében a kiválasztott adatok tovább szűrésére.

A kitűzött feladatot ezen túlmenően egy továbbított csomag adatáram feldolgozására szolgáló dekóderrel oldottuk meg, ahol a továbbított adatáram a csomag hasznos részekbe illesztett csomagokra bontott adatokat tartalmaz. Újszerű módon a dekóder a csomagokra bontott adatokból egy meghatározott biztonsági modul rendszerrel társított adatokat kiválasztó első szűrő eszközt, valamint az egy hordozható biztonsági modultól kapott szűrési adatok függvényében a kiválasztott adatokat tovább szűrő második szűrő eszközzel rendelkezik.

Előnyös a javasolt dekóder olyan kiviteli alakja, amelynél az első szűrő eszköz a biztonsági modultól kapott, a meghatározott biztonsági modul rendszer azonosítója függvényében konfigurálható eszközként van kiképezve.

Ugyancsak előnyös találmányunk értelmében, ha a második szűrő eszköz több szűrőt tartalmaz, melyek közül legalább egy szűrő a szűrési adatok függvényében konfigurálható módon van kiképezve.

Elsősorban ez utóbbi esetben előnyös, ha a második szűrő eszköz a szűrési adatokban található bitminta függvényében konfigurálhatóan van kialakítva.

Előnyös a javasolt dekóder olyan kiviteli alakja, amelyben a második szűrő eszköz a kiválasztott adatokból a szűrési adatokban található bitmintával megegyező adatmintát kiszűrő módon konfigurálhatóan van kialakítva. Egy másik lehetőség értelmében előnyös, ha a második szűrő eszköz a kiválasztott adatokból a szűrési adatokban található bitmintával egyező bitmintát tartalmazó adatokat kiszűrületlenül hagyóan van konfigurálva.

Előnyös a javasolt dekóder olyan kiviteli alakja, amelyben a második szűrő készlet legalább egy szűrője a szűrési adatokban található maszkoló minta függvényében az adatminta legalább egy részét figyelmen kívül hagyó módon van konfigurálva.

A javasolt dekóder egy további előnyös kiviteli alakja értelmében a biztonsági modulhoz a csomagokra bontott adatokban lévő feltételes hozzáférési adatokat továbbító eszközzel van ellátva.

Ugyan jelen találmányunk elsősorban a dekóder és a biztonsági modul között kommunikált feltételes hozzáférési üzenetek mennyiségének a csökkentését lehetővé tevő módon valósul meg, nyilvánvaló, hogy a szűrő eszközt úgy is konfigurálhatjuk, hogy a feltételes hozzáférési adatoktól eltérő adatokat is képes legyen kiválasztani, amelyeknek a biztonsági modultól eltérő a címezési helyük.

A javasolt dekóder egy további előnyös kiviteli alakja értelmében a biztonsági modulhoz továbbított feltételes hozzáférési adatok jogosultság vezérlő üzeneteket és/vagy jogosultság kezelő üzeneteket tartalmaznak.

Még egy egyetlen feltételes hozzáférési rendszerrel társított üzenet csoporton belül is nagy számú olyan üzenet található, amely a rendszer egyes felhasználói számára nem bír jelentőséggel. Például egyetlen feltételes hozzáférési rendszeren belül több különböző felhasználói csoportot definiálhatunk, ami több ilyen jogosultságkezelő üzenet keletkezéséhez vezet, és ezek közül nem mindegyik releváns minden egyes felhasználó számára.

Elsősorban éppen ezért előnyös, ha a biztonsági modul által rendelkezésre bocsátott szűrési adatok a szűrő eszköz által a biztonsági modulhoz címzett csoportos és/vagy egyedi jogosultságkezelő üzenetek kiválasztására használt adatokat tartalmaznak.

Egy további előnyös kiviteli alak értelmében a dekóder a biztonsági modul által a hozzá továbbított feltételes hozzáférési adatok függvényében generált ellenőrző szó vételére alkalmas módon van kialakítva, ahol a dekóder a ellenőrző szót egy bitsorkódolt adás bitsordekódolásához hasznosítja.

Egy további előnyös kiviteli alak értelmében a dekóder a hordozható biztonsági modul felé illetve felől kommunikáció kódolására és/vagy dekódolására alkalmas módon van kialakítva. Ez elsősorban azt jelenti, hogy a biztonsági modul által előállított, és esetenként a dekóderhez továbbított bitsordekódoló ellenőrző szó kódolt lehet.

Jóllehet találmányunk bármilyen csomagokra bontott jeltovábbítási rendszerben használható, különösen alkalmas egy MPEG kompatibilis adatáramot fogadó dekóderben történő felhasználásra, például, amelyben a csomagok hasznos részében táblázatok, szekciók vagy egyéb csomagokra bontott adatok vannak beépítve.

Ebben a vonatkozásban a "táblázat", "szekció", vagy "egyéb csomagokra bontott adat" kifejezés a legszélesebb értelemben tekintendő bármilyen adat táblázatra, önmagában, vagy egymást követően, és egy élőfejet és egy hasznos részt tartalmaz, és egy szállítási csomag áramba van becsomagolva. Mint az előnyös kiviteli alakok kapcsán később bemutatjuk, találmányunk különösen alkalmas egy MPEG táblázatban lévő adatok kiszűrésére, elsősorban egy egyszeres rövid formátumú MPEG táblázatban lévő adatok kiszűrésére.

Az "MPEG" kifejezés alatt a Nemzetközi Szabványügyi Szervezet (International Standards Organisation, ISO) Motion Pictures Expert Group csoportja által kifejlesztett adatátviteli szabványt értjük. Az MPEG-2 szabványt digitális televíziós alkalmazásokhoz fejlesztették ki, és az ISO 13818-1, az ISO 13818-2, az ISO 13818-3 és az ISO 13818-4 sz. dokumentumokban tették közzé. Jelen leírásban az MPEG formátum alatt a digitális adatátvitel területén alkalmazható alap MPEG formátumok összes változatát, módosított vagy továbbfejlesztett változatát egyaránt értjük.

A kitűzött feladatot ezen túlmenően egy találmány szerinti dekóderben használható hordozható biztonsági modullal oldottuk meg, amely javaslatunk értelmében egy meghatározott biztonsági modul rendszer azonosító eltárolására szolgáló memória eszközt, valamint az azonosítót a dekóder konfigurálásához a dekóderhez továbbító eszközt tartalmaz.

A javasolt hordozható biztonsági modul egy előnyös kiviteli alakja értelmében a modulnak szűrési adatot eltároló eszköze, továbbá a szűrési adatokat a dekóderben lévő szűrő eszközhöz továbbító eszköze van. A hordozható biztonsági modul előnyösen programozható csipkártyát foglal magában.

Leírásunkban a "programozható csipkártya" kifejezés alatt nem kizárólagosan bármilyen csip-alapú kártya eszközt, vagy hasonló funkciójú és működésű eszközt értünk, amely például mikroprocesszorral és/vagy valamilyen adattároló résszel, memóriával van ellátva. A kifejezés magában foglalja a kártyától eltérő alternatív kialakításokat is, például a televízió vevő és dekódoló rendszerekben igen gyakran használt kulcs alakú eszközöket, hitelkártyákat, valamint olyan eszközöket, amelyeknél az eszközben tárolt információhoz való hozzáférés nem mindig és minden körülmény között megengedett bárki számára.

A kitűzött feladatot ezen túlmenően a csomag hasznos részben megtalálható csomagokra bontott adatokat tartalmazó továbbított csomagáram feldolgozására szolgáló eljárással oldottuk meg, amelynek során újszerű módon a hordozható biztonsági modultól egy megha-

tározott biztonsági modul rendszer azonosítóját vesszük, a dekódert a vett azonosító függvényében konfiguráljuk, a hordozható biztonsági modultól vesszük a meghatározott biztonsági modul rendszerrel társított csomagokra bontott adatok szűréséhez szükséges szűrési adatokat, és a csomagokra bontott adatokat a kapott szűrési adatok függvényében szűrjük.

A javasolt eljárás egy előnyös foganatosítási módja értelmében a csomagokra bontott adatokat a meghatározott biztonsági modul rendszerrel társított adatok kiválasztásához szűrjük.

Ugyancsak előnyös a javasolt eljárás olyan foganatosítási módja, amelyben az azonosító egy meghatározott feltételes hozzáférési rendszer azonosítóját foglalja magában.

Ugyancsak előnyös a javasolt eljárás olyan foganatosítási módja, ahol az egy program térkép táblázatot és egy feltételes hozzáférési táblázatot tartalmazó továbbított csomagokat a csomagokra bontott adatáramból választjuk ki.

Egy további előnyös foganatosítási mód értelmében a csomagokra bontott adatokat a program térkép táblázatban és a feltételes hozzáférési táblázatban lévő kapott azonosító és adatok függvényében szűrjük.

Ugyancsak előnyös találmányunk értelmében, ha az azonosító a biztonsági modul által használt meghatározott elszámolási rendszer azonosítóját is magában foglalja.

Előnyös a javasolt eljárás olyan foganatosítási módja, ahol az azonosító a biztonsági modul által használt meghatározott jóváíró rendszer azonosítóját is magában foglalja.

Előnyös találmányunk értelmében, ha a szűrési adatok a csomagokra bontott adatokra vonatkozó legalább egy táblázat azonosítót vagy szekció azonosítót foglalnak magukban.

Egy további előnyös megvalósítás értelmében a csomagokra bontott adatokat a szűrési adatokban lévő bitminta szerint szűrjük.

Egy további előnyös foganatosítási mód értelmében a bitmintával megegyező bitmintát tartalmazó adatokat szűrjük ki a csomagokra bontott adatokból.

A kitűzött feladatot ezen túlmenően a csomag hasznos részben megtalálható csomagokra bontott adatokat tartalmazó továbbított csomagáram feldolgozására szolgáló eljárással oldottuk meg, amelynek során a csomagokra bontott adatokból egy meghatározott biztonsági

modul rendszerrel társított adatokat választunk ki, és a kiválasztott adatokat egy hordozható biztonsági modultól kapott szűrési adatok függvényében szűrjük.

Előnyös a javasolt eljárás olyan foganatosítási módja, amelynek során a meghatározott biztonsági modul rendszer azonosítóját a biztonsági modultól fogadjuk.

Előnyös továbbá, ha a kiválasztott adatokban lévő feltételes hozzáférési adatokat a biztonsági modulhoz továbbítjuk.

Előnyös a javasolt eljárás olyan foganatosítási módja, amelynek során a biztonsági modulhoz továbbított feltételes hozzáférési adatok jogosultság vezérlő üzeneteket és/vagy jogosultság kezelő üzeneteket foglalnak magukban.

Ugyancsak előnyös a találmány értelmében, ha a biztonsági modul által rendelkezésre bocsátott szűrési adatok a dekóder által a biztonsági modulhoz címzett csoportos és/vagy egyedi jogosultság kezelő üzenetek kiválasztásához használt adatokat foglalnak magukban.

Ugyancsak előnyös a javasolt eljárás olyan foganatosítási módja, amelynek során a biztonsági modullal a hozzá továbbított feltételes hozzáférési adatok függvényében egy ellenőrző szót állítunk elő, és ezt a ellenőrző szót használjuk a dekóderben a bitsorkódolt adás dekódolásához.

Találmányunk ezen túlmenően kiterjed egy digitális jelátviteli rendszerben használható olyan dekóderre is, amely egy továbbított csomag adatáram csomagjainak hasznos részében lévő táblázatokat, szekciókat vagy egyéb csomagokra bontott adatokat tartalmazó adatáram vételére alkalmas, és a találmányból fakadó újszerűsége abban áll, hogy a dekóder egy hordozható biztonsági modultól kapott szűrési adatok függvényében a jelzett adatok szűrésére konfigurálható eszközt foglal magában. A táblázati vagy szekció szinten végzett szűrésen túlmenően a dekóder ezen túlmenően egy szállítási szintű szűrést is végrehajthat, például annak érdekében, hogy csupán a biztonsági modul által használt meghatározott feltételes hozzáférési rendszerhez tartozó adatokat tartalmazó csomagokat válassza ki. Ennek érdekében a dekóder előnyösen a biztonsági modultól kapott adatok függvényében a továbbított csomagokra bontott adatok kiszűrésére konfigurálható eszközt is tartalmaz. Előnyösen a továbbított csomagokra bontott adatok szűrésére szolgáló eszköz a biztonsági modultól megkapott feltételes hozzáférési rendszer azonosítót jelentő adatok függvényében konfigurálható módon van kialakítva.

A "vevő és dekódoló berendezés" és "dekóder" kifejezés akár kódolt, akár kódolatlan jelek

vételére alkalmas, például televízió és/vagy rádió jelek vételére alkalmas vevőt jelenthet. Egy ilyen dekóder lehetséges kiviteli alakjai kialakíthatók úgy, hogy a dekódert egybeépítjük a vevővel, az utóbbi által vett jelek dekódolására, például egy set top box-ban, vagy egy dekóder egy tőle fizikailag különálló vevővel kombinálva működik, vagy a dekódert más készülékekkel, például egy Web böngészővel, egy videomagnetofonnal, vagy egy televízió készülékkel egybe is integrálhatjuk.

A leírásunkban többször használt "digitális átviteli rendszer" például elsődlegesen audiovizuális vagy multimédia digitális adatok továbbítására vagy sugárzására szolgáló bármilyen jelátviteli rendszert jelenthet. Bár találmányunk elsősorban egy műsort vagy adatot sugárzó digitális televízió rendszerben alkalmazható, hasonlóan eredményesen alkalmazható multimédiás Internetes alkalmazások céljára létrehozott vezetékes távközlési hálózatokban, zártláncú televízió rendszerekben, és így tovább.

A "digitális televízió rendszer" kifejezés például bármilyen műholdas, földi műsorszóró, kábel vagy egyéb rendszert is magában foglalhat.

A találmányt az alábbiakban a csatolt rajz segítségével ismertetjük részletesebben, amelyen a javasolt dekóder, modul és eljárás példakénti kiviteli alakját tüntettük fel. A rajzon az

1. ábra a találmány szerinti digitális televízió rendszer általános vázlata, a
2. ábrán az 1. ábra szerinti rendszer feltételes hozzáférési rendszerének architektúrája látható, a
3. ábrán elsősorban a feltételes hozzáférési üzenetekre vonatkozó MPEG-2 csomagok hierarchiája látható, a
4. ábra MPEG-2 privát szekciók hosszú illetve rövid alakjának felépítését mutatja, az
5. ábra a találmány szerinti vevő és dekódoló berendezés főbb egységeinek vázlata, a
6. ábrán az 5. ábra szerinti vevő és dekódoló berendezés elsősorban feltételes hozzáférési üzenetek vonatkozásában a továbbított adatáramot feldolgozó elemeinek vázlata látható, és a
7. ábrán a 6. ábra szerinti szűrőegység táblázat azonosítójának és szekció szűrőinek felépítése követhető nyomon.

A találmány szerinti 1 digitális televízió rendszer vázlata az 1. ábrán követhető nyomon. A találmány hagyományosan felépített 2 digitális televízió rendszert foglal magában, amely az ismert MPEG-2 tömörítő rendszert használja tömörített digitális jelek kibocsátásához és sugárzásához. Ezt kicsit részletezve, a 3 MPEG-2 tömörítő, amely szokásosan egy műsorszóró központban helyezkedik el, rendszerint videojel adatáram formájában digitális adatáramot kap. A 3 tömörítő 5 vonalon keresztül 4 multiplexerhez és bitsorkódolóhoz van csatlakoztatva. A 4 multiplexer és bitsorkódoló multiplexere további bemenőjelet kap, amelyekből egy vagy több szállítási adatáramot állít össze, és a tömörített digitális jelet a műsorszóró központban lévő 6 adóberendezéshez továbbítja további 7 vonalon keresztül, amely természetesen számos módon megvalósítható, beleértve a szokásos távközlési vezetékes kapcsolatokat is.

A 6 adóberendezés elektromágneses jeleket továbbít 8 földi állomástól műholdra irányuló adatátviteli kapcsolat segítségével 9 transzponderhez, amely azt elektronikusan feldolgozza, és 10 műholdról földi állomás felé irányuló adatátviteli kapcsolaton át egy földi 11 vevőhöz továbbítja, mely 11 vevő általában egy végfelhasználó tulajdonában lévő, vagy általa bérelt parabola antenna. A 11 vevővel fogadott jelek szintén a végfelhasználó tulajdonában álló, vagy általa bérelt integrált 12 dekóderbe kerülnek, amely a tömörített MPEG-2 jelet olyan televízió jellé alakítja vissza, amely minden további nélkül használható 13 televízió készülékben.

A 4 multiplexerhez és a 12 dekóderhez egy 20 feltételes hozzáférési rendszer kapcsolódik, amely részben a műsorszóró központban, részben a 12 dekóderben van kialakítva. A 20 feltételes hozzáférési rendszer lehetővé teszi a felhasználók számára, hogy egy vagy több műsorszóró szolgáltatótól digitális televízió műsorokat fogadjon. A kereskedelmi ajánlatokra vonatkozó üzenetek dekódolására képes programozható csipkártya (ezek az üzenetek tulajdonképpen a műsorszóró szolgáltató által felkínált egy vagy több televízió programot jelentenek) helyezhető a 12 dekóderbe, és a kettő együttes használatával a végfelhasználó vagy előfizetési módon, vagy helyben fizetős módon (pontosabban "nézd- és fizess", angolul pay-per-view módon) műsorok által megtestesülő eseményeket vásárolhat.

Az ugyancsak a 4 multiplexerhez és a 12 dekóderhez csatlakoztatott, és szintén részben a műsorszóró központban, részben a dekóderben kialakított 17 interaktív rendszer lehetővé teszi a végfelhasználó számára, hogy egy 16 modemcsatlakoztatott keresztül interaktív módon kapcsolatba kerüljön számos alkalmazással.

Az alábbiakban az említett 20 feltételes hozzáférési rendszert ismertetjük részletesebben.

Ehhez térjünk át a 2. ábrára, amelyen látható, hogy a 20 feltételes hozzáférési rendszer 21 előfizető azonosítási rendszert tartalmaz. A 21 előfizető azonosítási rendszer egy vagy több 22 előfizető karbantartó rendszerhez csatlakozik, pontosabban minden egyes műsorszóró szolgáltatóhoz tartozik egy 22 előfizető karbantartó rendszer, és a 21 előfizető azonosítási rendszer egy-egy TCP/IP 23 kapcsolaton keresztül csatlakozik (jóllehet más típusú csatlakozás módok is alkalmazhatók). Egy alternatív megoldás értelmében két műsorszóró szolgáltató között egy 22 előfizető karbantartó rendszer is megosztható, vagy fordítva, egy műsorszóró szolgáltató is használhat két 22 előfizető karbantartó rendszert és így tovább.

A 21 előfizető azonosítási rendszerhez 26 vonalon keresztül "anya" 25 programozható csipkártyákat használó 24 kódoló egységek vannak csatlakoztatva, melyek elsődleges 24 kódoló egységként szolgálnak. Ennek megfelelően a rendszer másodlagos 27 kódoló egységeket is tartalmaz, amelyek a 4 multiplexer és bitsorkódolóhoz vannak 29 vonalon keresztül csatlakoztatva, és "anya" 28 programozható csipkártyákat használó 27 kódoló egységek alkotják. A 12 dekóder a terminológiát alkalmazva "gyerek" 30 programozható csipkártyát fogad be, és 31 kommunikációs szerverek révén a modemes 16 válaszcatornán keresztül közvetlenül a 21 előfizető azonosítási rendszerhez csatlakozik. A 21 előfizető azonosítási rendszer egyéb információk mellett külön kérelemre előfizetői jogokat küld a "gyerek" 30 programozható csipkártyának.

A 25, 28, 30 programozható csipkártyák egy vagy több kereskedelmi operátor titkos adatait tartalmazzák. A 25, 28 programozható csipkártya különböző típusú üzeneteket kódol, míg a 30 programozható csipkártya - amennyiben joga van hozzá - ezeket az üzeneteket dekódolja.

Az első és a második, 24, 27 kódoló egység egy elektronikus szekrényben (rack) helyezkedik el, és EEPROM-ban tárolt szoftverrel működő elektronikus VME kártyát, legfeljebb húsz elektronikus kártyát és minden egyes elektronikus kártyához egy-egy 25 programozható csipkártyát illetve 28 programozható csipkártyát tartalmaz valamint egy 28 programozható csipkártyát tartalmaz a jogosultság vezérlő üzenetek kódolására, és egy további 25 programozható csipkártyát tartalmaz a jogosultság kezelési üzenetek kódolására.

Az 1 digitális televízió rendszer 20 feltételes hozzáférési rendszerének a működését egyes egységeik működésének részletesebb bemutatásával és az összefüggések vázolásával is-

mertetjük részletesebben.

4 multiplexer és bitsorkódoló

Amint az az 1. és 2. ábrán megfigyelhető, a műsorszóró központban a digitális videojelet előbb tömörítjük (vagy a bitátvitel sebességét csökkentjük), és ehhez a 3 MPEG-2 tömörítőt használjuk. Ezt a tömörített jelet ezt követően a 5 vonalon át a 4 multiplexer és bitsorkódolóhoz továbbítjuk, hogy ott más adatokkal, például más tömörített adatokkal multiplexeljük.

A 4 multiplexer és bitsorkódolóval előbb előállítunk egy olyan ellenőrző szót, amelyet a bitsorkódolási művelet során használunk, és a 4 multiplexer és bitsorkódolóval beépítjük az MPEG-2 adatáramba. Ezt az ellenőrző szót belsőleg állítjuk elő, és lehetővé tesszük a végfelhasználó integrált 12 dekódere számára, hogy a programokat dekódolja.

Az MPEG-2 áramhoz olyan hozzáférési kritériumokat is csatolunk, amelyek azt jelzik, hogy az egyes programok kereskedelmi értékesítése miképpen történjék. A programok kereskedelmi értékesítése vagy a számos előfizetési módzat valamelyike szerint, vagy pedig a számos fizetős (pay per view) módzat valamelyike szerint történhet. Előfizetés esetén a végfelhasználó egy vagy több kereskedelmi ajánlatra vagy "csomagra" fizet elő, és ezzel megszerzi a jogot arra, hogy a kiválasztott csomagban lévő összes csatornát, programot, eseményt nézze. Találmányunk egy előnyös kiviteli alakja értelmében egy ilyen csatorna csomagból maximum kilencszázhatvan kereskedelmi ajánlat választható ki. Az említett másik módban, vagyis a fizetős módban a végfelhasználó a kívánsága szerinti eseményeket, programokat "megvásárolhatja". Ez történhet akár úgy, hogy a kiválasztott eseményt elővételben megveszi, (ez az elővételi mód), vagy pedig az eseményt közvetlenül annak kisugárzásakor "fogyasztja", veszi meg, (ez az impulzus mód). Az előnyös kiviteli alak esetében az összes felhasználó előfizetőként tekintett, akár előfizetési, akár elővételes, akár prompt fizetési módban fogyasztja a műsorokat, de természetesen a fizetési módot választóknak nem kell egyben előfizetőknek is lenniük, bár lehetnek.

Jogosultság vezérlő üzenetek

Mind az ellenőrző szót, mind a hozzáférési kritériumokat arra használjuk, hogy létrehozunk egy jogosultság vezérlő üzenetet. Ezt az üzenetet egy kódolt program vonatkozásában bocsátjuk ki, és a program dekódolásának lehetővé tételét biztosító ellenőrző szót, valamint a kisugárzott program hozzáférési kritériumait tartalmazza. A hozzáférési kritériumokat és

az ellenőrző szót a 29 vonalon át a második 27 kódoló egységhez továbbítjuk. A 27 kódoló egységben állítjuk elő a jogosultság vezérlő üzenetet kódoljuk, majd továbbítjuk a 4 multiplexer és bitsorkódolóhoz. Egy műsorszóró sugárzás során az ellenőrző szó jellemzően néhány másodperces időközönként változik, így a jogosultság vezérlő üzeneteket szintén megadott időközönként kell kisugározni, hogy lehetővé tegyünk a változó ellenőrző szó bitsordekódolását. Redundancia okokból minden egyes jogosultság vezérlő üzenet általában két ellenőrző szót tartalmaz: az éppen érvényes ellenőrző szót, valamint a következő ellenőrző szót.

Minden egyes, egy műsorszóró szolgáltató által egy adatáramban kibocsátott szolgáltatás több különálló összetevőt foglal magában, például egy televízió műsor egy video összetevőt, egy audio összetevőt, egy alcím összetevőt, és így tovább, tartalmaz. Mindegyike ezeknek a szolgáltatási összetevőknek külön-külön van bitsorkódolva és kódolva, hogy a 9 transzponderen keresztül ki lehessen sugározni. A szolgáltatás minden egyes bitsorkódolt összetevője vonatkozásában egy-egy különálló jogosultság vezérlő üzenetre van szükség. Alternatív megoldásként egy adott szolgáltatás összes bitsorkódolt összetevőjéhez egyetlen jogosultság vezérlő üzenet is elegendő lehet. Olyan esetekben, ahol több feltételes hozzáférési rendszer gondoskodik ugyanahhoz a továbbított programhoz a hozzáférésről, több jogosultság vezérlő üzenetet kell előállítani.

Program továbbítás

A 4 multiplexer és bitsorkódolóval a 21 előfizető azonosítási rendszertől kódolt jogosultság kezelési üzeneteket tartalmazó elektromos jeleket, a második 27 kódoló egységtől kódolt jogosultság vezérlő üzeneteket, a 3 MPEG-2 tömörítőtől pedig tömörített programokat veszünk. A 4 multiplexer és bitsorkódolóval a programokat bitsorkódoljuk, majd a bitsorkódolt programokat a kódolt jogosultság kezelési üzeneteket és a kódolt jogosultság vezérlő üzeneteket villamos jelként a műsorszóró központ 6 adóberendezéséhez továbbítjuk a 7 vonalon keresztül. A 6 adóberendezéssel elektromágneses jeleket lövünk fel a 8 földi állomáson keresztül a műholdas 9 transzponderhez.

Program vétel

A 9 transzponderrel vesszük és feldolgozzuk a 6 adóberendezéssel fellőtt elektromágneses jeleket, és a feldolgozott jeleket visszaküldjük a földi 11 vevőhöz, amely általában a végfelhasználó tulajdonában álló vagy általa bérelt parabola antenna. Erre a célra a 2016 mű-

holdat használjuk. A 11 vevővel vett jeleket a végfelhasználó tulajdonát képező, vagy általa bérelt integrált 12 dekóderhez továbbítjuk, amely a végfelhasználó 13 televízió készülékével áll kapcsolatban. A 12 dekóderrel demultiplexeljük a jeleket, hogy megkapjuk a bitsorkódolt programokat a kódolt jogosultság kezelési üzenetekkel és ugyancsak kódolt jogosultság vezérlő üzenetekkel.

Ha a program nem bitsorkódolt, azaz az MPEG-2 áramban nem továbbítottunk jogosultság vezérlő üzenetet, akkor a 12 dekóderrel a tömörített adatokat visszaállítjuk, és a jeleket videojellé alakítjuk, hogy a 13 televízió készülékbe vezethessük.

Ha a program bitsorkódolt, akkor a 12 dekóderrel az MPEG-2 áramból kivonjuk a hozzátartozó jogosultság vezérlő üzenetet, és azt a végfelhasználó "gyerek" 30 programozható csipkártyájához továbbítjuk. A 30 programozható csipkártya a 12 dekóder házának erre a célra kialakított fészkebe van rendszerint bedugaszolva és azt felügyeli, hogy a végfelhasználónak milyen körülmények között van joga, jogosultsága a jogosultság vezérlő üzenet dekódolására és a programokhoz való hozzáférésre. Ha a végfelhasználónak nincs ilyen joga, úgy a 12 dekódernek negatív állapotjelzést ad, amellyel jelzi, hogy a szóban forgó program nem dekódolható. Ha a végfelhasználónak megvan a joga, akkor a jogosultság vezérlő üzenetet dekódolni tudja, és kivonhatja belőle az ellenőrző szót. Ennek birtokában a 12 dekóder visszaállíthatja a bitsorkódolt programot, az MPEG-2 áramot dekomprimálhatja, és videojellé alakíthatja, amely már továbbítható a 13 televízió készülékhez.

Jogosultság kezelési üzenetek

A jogosultság kezelési üzenet egy egyedi végfelhasználó (előfizető) részére címzett üzenet, vagy akár végfelhasználók meghatározott csoportjának szóló üzenet (ellentétben a jogosultság vezérlő üzenettel, amely egy bitsorkódolt programhoz, vagy ha ugyanannak a kereskedelmi ajánlatnak a részét képezik, egy bitsorkódolt program készlethez tartozik). Minden egyes csoport egy adott számú végfelhasználót tartalmazhat. A csoportokba szervezés a sáv szélesség optimalizálása irányában hat, azaz egyetlen csoporthoz történő hozzáféréssel nagyszámú végfelhasználót tudunk egyidejűleg elérni.

A találmány gyakorlatban történő megvalósításához számos speciális jogosultság kezelési üzenet típust használunk. Egyedi, testre szabott jogosultság kezelési üzeneteket rendelhetünk az egyes előfizetőkhez és ezeket jellemző módon a fizetős szolgáltatások előkészítése során használjuk; ezek a jogosultság kezelési üzenetek tartalmazzák az adott csoportban

lévő előfizető csoport azonosítóját és pozícióját. Úgynevezett "csoportos" előfizetői jogosultság kezelési üzeneteket dedikálhatunk, például 256 felhasználóból álló csoportokhoz, és ezeket jellemző módon bizonyos előfizetői szolgáltatások adminisztrációjában hasznosítjuk. Ez a típusú jogosultság kezelési üzenet egy csoport azonosítót valamint egy előfizetői csoport bittérképét tartalmaz. A nézőközönségi jogosultság kezelési üzeneteket a teljes nézőközönség részére dedikáljuk és ilyeneket használhatunk például arra, hogy egy meghatározott adminisztrátor bizonyos szabad, ingyenes szolgáltatásokat kínálhasson. A "nézőközönség" kifejezés alatt azon összes előfizetőt értjük, aki azonos operátor azonosítójú 25, 28, 30 programozható csipkártyával rendelkezik. Végül, a 25, 28, 30 programozható csipkártya egyedi azonosítójának egy "egyedi" jogosultság kezelési üzenetet címzünk.

22 előfizető karbantartó rendszer

A 22 előfizető karbantartó rendszer olyan 32 adatbázist tartalmaz, amely többek között karbantartja az összes végfelhasználói rekordot, a kereskedelmi ajánlatokat (mint a tarifák és bemutatók), az előfizetéseket, a fizetési mód részleteit, valamint a végfelhasználói fogyasztásra és jogosultságra vonatkozó adatokat. A 22 előfizető karbantartó rendszer fizikailag a 21 előfizető azonosítási rendszertől távol lehet kialakítva.

Minden egyes 22 előfizető karbantartó rendszer egy-egy hozzátartozó TCP/IP 23 kapcsolaton keresztül üzeneteket továbbít a 21 előfizető azonosítási rendszernek, melyek a végfelhasználókhöz továbbítandó jogosultság kezelési üzenet létrehozásokat és módosításokat befolyásolják.

A 22 előfizető karbantartó rendszer olyan üzeneteket is továbbít a 21 előfizető azonosítási rendszernek, amelyek nem a jogosultság kezelési üzenetek létrehozására vagy módosítására vonatkoznak, hanem csupán egy végfelhasználó státuszában bekövetkező változást jelzik (vagyis a végfelhasználó számára megadott jogosultságra vonatkozó információt tartalmazzák, ha a végfelhasználók újabb "árut" vásárol, vagy például a végfelhasználónak kiterhelendő számláról van szó).

Mint a későbbiekben még részletesebben is bemutatjuk, a 21 előfizető azonosítási rendszer jellemző módon információt, például visszahívási információt vagy számlázási információt kérelmező üzeneteket küld a 22 előfizető karbantartó rendszernek, így nyilvánvaló, hogy a közöttük lévő kommunikáció kétirányú kommunikáció.

21 előfizető azonosítási rendszer

A 22 előfizető karbantartó rendszerben előállított üzeneteket a TCP/IP 23 kapcsolaton keresztül a 21 előfizető azonosítási rendszerhez továbbítjuk, amellyel ennek alapján olyan üzeneteket állítunk elő, amelyekkel nyugtázzuk a 22 előfizető karbantartó rendszer által létrehozott üzenetek vételét és ezeket a nyugtázásokat elküldjük a 22 előfizető karbantartó rendszernek.

Általánosságban a 21 előfizető azonosítási rendszer egy előfizetési lánc területet, egy nézd-és-fizess lánc területet és egy jogosultság kezelési üzenet beillesztő területet foglal magában. Az előfizetési lánc terület adja az előfizetési mód jogosultságokat, valamint lehetővé teszi ezen jogosultságoknak a havonta történő automatikus megújítását, a 21 előfizető azonosítási rendszer az egyes nézd-és-fizess eseményekhez ad jogokat, míg a 22 előfizető karbantartó rendszer arra szolgál, hogy az előfizetési lánc terület és a nézd-és-fizess lánc terület által létrehozott jogosultság kezelési üzeneteket eljuttassa a 4 multiplexer és bitsorkódolóba és így az MPEG adatáramot ellássa jogosultság kezelési üzenetekkel. Amennyiben más jogokat kell megadni, például tölts-le-és-fizess jogokat, ha felhasználó saját személyi számítógépére számítógép programokat tölt le, akkor a bemutatotthoz hasonló területeket hozunk létre.

A 21 előfizető azonosítási rendszer egyik feladata azokhoz a televízió programokhoz való hozzáférési jogok adminisztrálása, amelyek kereskedelmi ajánlatként állnak rendelkezésre előfizetési módban, vagy nézd-és-fizess eseményekként kerülnek értékesítésre a kereskedelmi hasznosítás különböző módozataiban (azaz elővételi módon vagy impulzus módon). A 21 előfizető azonosítási rendszer a 22 előfizető karbantartó rendszertől kapott jogok és információk alapján megfelelő jogosultság kezelési üzeneteket állít elő az előfizetők részére.

A jogosultság kezelési üzeneteket a 24 kódoló egységhez továbbítjuk, hogy ott a kezelési és felhasználási kulcsoknak megfelelően kódolhassuk. A 24 kódoló egység elhelyezi aláírását a jogosultság kezelési üzenetben, majd azt visszaküldi a 21 előfizető azonosítási rendszerben lévő üzenet generátorhoz, amely azt egy élőfejjel egészíti ki. Ezt követően a jogosultság kezelési üzeneteket mint hiánytalan, teljes üzeneteket továbbítjuk egy üzenet küldő egységhez. Az üzenet küldő egység határozza meg a kisugárzás kezdési és befejezési időpontját, a jogosultság kezelési üzenetek kibocsátási sűrűségét, és ezeket a jogosultság kezelési üzenetekkel együtt megfelelő utasításokként átadja az üzenet kibocsátóhoz. Az

üzenet generátor egy adott jogosultság kezelési üzenetet csupán egyszer hoz létre, azok ciklikus elküldéseiről a továbbiakban már az üzenet kibocsátó egység fog gondoskodni.

Egy jogosultság kezelési üzenet létrehozása során az üzenet generátor a jogosultság kezelési üzenethez egy egyedi azonosítót rendel hozzá. Ha az üzenet generátor a jogosultság kezelési üzenetet átadja az üzenet kibocsátónak, a létrehozott jogosultság kezelési üzenet azonosítót is átadja. Ez mind az üzenet generátor, mind az üzenet kibocsátó számára lehetővé teszi egy meghatározott jogosultság kezelési üzenet beazonosítását.

Olyan rendszerekben, mint a Simulcrypt, ahol több feltételes hozzáférés rendszer, például több operátorral működhet együtt, az egyes feltételes hozzáférési rendszerekhez tartozó jogosultság kezelési üzenet adatáramokat külön-külön állítják elő, és azokat kibocsátásuk, elküldésük előtt a 4 multiplexerrel multiplexelik.

Feltételes hozzáférési üzenetek a továbbított adatáramban

A jogosultság vezérlő üzenet és a jogosultság kezelési üzenet különböző természete következtében eltérő ezen üzenetek továbbítási módja is az MPEG adatáramban. A jogosultság vezérlő üzeneteket, amelyek egy program bitsordekódolásához szükséges vezérlő szavakat tartalmaznak, szükségszerűen összekötjük a továbbított program video- és adatáramaival. Ettől eltérően a jogosultság kezelési üzenetek általános üzenetek, amelyeket aszinkron módon sugárzunk, hogy egyes fogyasztókhoz, vagy egyes fogyasztói csoportokhoz jogosultsági információkat közvetítsünk. Ez a különbség a jogosultság vezérlő üzenet és a jogosultság kezelési üzenet MPEG továbbított adatáramában történő elhelyezésében mutatkozik meg.

Mint az jól ismert, az MPEG továbbított csomagok 188 bájt hosszúságúak, mely hossz rögzített érték és egy élőfejet tartalmaznak. Egy szabványos csoportban a szinkronizálási adatokat követő 3 bájt az élőfejben az alábbi módon áll össze:

Szállítási hibajelző	1 bit
Hasznos rész egység jelző	1 bit
Szállítási elsőbbség	1 bit
Csomag azonosító	13 bit
Szállítási bitsordekódolási vezérlés	2 bit
Felhasználási mező vezérlés	2 bit

Folytonosság számláló

4 bit

A fenti mezők jellemzőit az MPEG szabvány nagy mértékben meghatározta és rögzítette.

Ha megnézzük a harmadik áramot, amelyen egy továbbított adatáramban az adatok szervezését vázoltuk, látható, hogy ez a továbbított adatáram 40 program hozzáférési táblázatot tartalmaz, és a csomag élőfejében a csomag azonosító az MPEG-2 szabványnak megfelelően rögzített 0x00 értékű. A 40 program hozzáférési táblázat adja meg a program adatok hozzáféréséhez szükséges belépési pontot, és a programokkal társított 41, 42 program térkép táblázatok csomag azonosító értékeire vonatkozó táblázatot tartalmaz. Minden egyes 41, 42 program térkép táblázat hivatkozást tartalmaz a programok 43 audio táblázatainak és 44 video táblázatainak a csomag adatáramainak a csomag azonosító értékeire vonatkozóan.

Mint látható, a 42 program térkép táblázat ezen túlmenően a szóban forgó programokra vonatkozó járulékos adatokat tartalmazó egyéb 45, 46 csomagok csomag azonosító értékeihez is tartalmaz hivatkozást. Jelen esetben a különböző feltételes hozzáférési rendszerek által előállított és a szóban forgó programokkal társított jogosultság vezérlő üzenet adatok ezekben a 45, 46 csomagokban találhatók. A 40 program hozzáférési táblázaton túlmenően az MPEG szállítási adatáram olyan 47 feltételes hozzáférési táblázatot is tartalmaz, amelynek csomag azonosítója rögzítetten 0x01 értékű. Az összes ezt a csomag azonosító értéket tartalmazó csomag élőfejet így automatikusan olyanként azonosítjuk be, mint amely feltételes hozzáférési vezérlő információt tartalmaz. A 47 feltételes hozzáférési táblázat egy vagy több feltételes hozzáférési rendszerrel társított jogosultság kezelési üzenet adatokhoz tartozó MPEG 48, 49, 50 csomagok csomag azonosító értékeire hivatkozik. Hasonlóan, mint a program térkép táblázat csomagoknál láttuk, a jogosultság kezelési üzenet csomagoknak a 47 feltételes hozzáférési táblázatban lévő csomag azonosító értékei nem rögzítettek, így a rendszer operátorának a választása alapján határozhatók meg.

Az MPEG-2 szabvánnyal összhangban az egy csomag hasznos részében található információ a továbbított adat típusának megfelelő további strukturáltságú. Audio, video, teletext, alcím vagy egyéb, ilyen gyorsan kialakuló és szinkronizált adat esetében az információt csomagokra bontott elemi adatáram néven ismert formában készítjük elő. Ez az adatáram, amelyet a továbbított csomagok hasznos részének az összeállításával alakítunk ki, saját maga olyan csomag szekvenciát tartalmaz, ahol minden egyes csomag egy csomag élőfejet

és egy hasznos részt tartalmaz. Eltérően a továbbított adatáramban lévő, továbbított csomagoktól, ezeknek a csomagokra bontott elemi adatáram csomagoknak a hossza változó.

Egyéb adatok esetén, például alkalmazási adatok, vagy mint jelen esetünkben jogosultság vezérlő üzenet, illetve jogosultság kezelési üzenet adatok esetén eltérő csomagokra bontott elemi adatáram formátumra van előírás. Ilyen esetben a továbbított csomag hasznos részben lévő adatokat szekciók vagy táblázatok sorozatára osztják fel, ahol egy táblázat azonosítóval rendelkező táblázat élőfej vagy szekció élőfej azonosítja a szóban forgó táblázatot. Az adatok méretétől függően egy szekció teljes egészében elfér egy csomag hasznos részben, vagy több továbbított csomagon át egy táblázat sorozatban helyezkedik el. Az MPEG-2 szabvány vonatkozásában a "táblázat" kifejezést gyakran használjuk egyetlen adat táblázat kifejezésére, a "szekció" kifejezést pedig ugyanazzal a táblázat azonosító értékkel rendelkező több táblázat esetén használjuk.

A továbbított csomag adatok illetve a csomagokra bontott elemi adatok vonatkozásában egy táblázat vagy szekció adatszerkezetét az MPEG-2 szabvány meghatározza. Ezen belül két lehetséges szintaxis forma létezik privát táblázatokra vagy szekció adatokra: egy úgynevezett hosszú alak és egy úgynevezett rövid alak, amelyeket a 4. ábrán vázoltunk. Mind a hosszú, mind a rövid alak esetében az élőfej legalább az alábbiakat magában foglaló 60 adatot tartalmazza:

Táblázat azonosító	8 bit
Szekció szintaxis jelző	1 bit
Privát jelző/tartalék rész	1 bit
ISO tartalék rész	2 bit
Szekció hossz	12 bit

A privát jelző és a privát szekció hossz az MPEG-2 szabvány által nem rögzített hosszúságú adatot tartalmaz, és a rendszer üzemeltetője saját céljaira használhatja fel.

A rövid alak esetében az élőfej 60 adatot közvetlenül a hasznos rész 61 adat követi. Hosszú alak esetében a 63 hasznos részt megelőzően egy további 62 élőfej szekció található, és az üzenet ezen kívül 64 CRC ellenőrző értéket is magában foglal. A hosszú alak, amelyet általában olyan esetekben alkalmazunk, amikor egy üzenet olyan hosszú, hogy több szekcióra kell felosztanunk, tartalmazza a szekciók összeállításához szükséges információt, így például a szekció számot, a szekciók sorrendjében az utolsó szekció számát, és így tovább.

A hosszú és rövid alakú táblázat adatokra vonatkozó információ az MPEG-2 szabvány leírásaiból ismerhető meg.

Feltételes hozzáférési jogosultság vezérlő üzenet és jogosultság kezelési üzenet esetében az adatokat általában egyetlen táblázatba tudjuk összefoglalni és megfelelő formátumként a fent említett rövid alakot használhatjuk. Ilyen rövid alakú feltételes hozzáférési üzenetek számára a találmányunk értelmében egy alábbi speciális szintaxist javasolunk, nevezetesen:

Táblázat azonosító (szűrési adatok)	8 bit (1 bájt)
Szekció szintaxis jelző	1 bit
Privát jelző/tartalék rész	1 bit
ISO tartalék rész	2 bit
Szekció hossz	12 bit
Feltételes hozzáférési specifikus élőfej mező (szűrési adatok)	56 bit (7 bájt)

Ilyen feltételes hozzáférési üzenetek esetében a táblázat azonosító értéket a rendszer üzemeltetője például 0x80 és 0x81 értékre állíthatja be jogosultság vezérlő üzenetekhez (például páratlan és páros üzenetekhez), illetve 0x82 -0x8F értékre állíthatja be jogosultság kezelési üzenetekhez. Ezeket az értékeket az MPEG-2 szabvány nem rögzíti, így alkalmazásuk és megválasztásuk kizárólag a rendszer üzemeltetőjének a döntésétől függ.

Hasonlóképpen, a feltételes hozzáférésű specifikus élőfej mező esetében, amely az élőfejet követő hasznos rész első 7 bájtja, a paramétereket ugyancsak a rendszer üzemeltetője állíthatja be, például annak a jelzésére, hogy a feltételes hozzáférési üzenet egyedre vonatkozó, csoportos vagy előfizetési információt hordozó jogosultság kezelési üzenet. Ebben az esetben egy ilyen táblázat vagy szekció "élőfeje" ki van terjesztve.

Az ilyen üzenet szintaxis előnyei leírásunk későbbi részében egyértelművé válnak, a vevő és dekódoló berendezés által az üzenet feldolgozására és szűrésére vonatkozóan, elsősorban a táblázat azonosító és a feltételes hozzáférés specifikus mező adatok használata révén.

Az 5. ábrán egy digitális műsorszóró rendszerben használható 12 dekóder vagy Set top box egyes elemeit tüntettük fel. Ezen elemek felépítése, működése messzemenően az ismert, hagyományos módon történik, így a területen jártas szakember számára megvalósításuk nem jelent gondot.

Mint látható, a 12 dekóder különböző interfészekkel rendelkezik adatok vételére és küldésére, ezen belül sugárzott MPEG adások vételére szolgáló MPEG 70 tunert és

demultiplexert, 71 soros interfészt, 72 párhuzamos interfészt, valamint adatok telefonhálózaton keresztül történő adásához és vételéhez 73 modemet. Ebben a kiviteli alakban a 12 dekódernek első és második 74, 75 kártyaolvasója van, ahol az első 74 kártyaolvasó a rendszerrel társított dekódoló kulcsot tartalmazó előfizetői programozható csipkártyát befogadó kártyaolvasó, míg a második 75 kártyaolvasó bankkártyát vagy más hasonló kártyát befogadó és olvasó kártyaolvasó.

A 12 dekódernek 76 vevőfokozata van, amellyel egy kézi 77 távirányítóból származó infravörös vezérlőjeleket fogad, valamint egy PERITEL kimenettel rendelkezik, amelyen keresztül a 12 dekóderhez csatlakoztatott 13 televízió készülékhez audiovizuális jeleket továbbít.

A 12 dekóderen belüli adatfeldolgozást általában a központi 20 processzor végzi. A központi 20 processzor szoftver-architektúrája megfelelhet az ismert dekódolóokban alkalmazott szoftver-architektúrának, ezért ezt a továbbiakban nem részletezzük. A szoftver-architektúra alapulhat például olyan virtuális gépen, amely egy interfész rétegen keresztül a dekódoló hardver-komponenseiben megvalósított, alacsonyabb szintű operációs rendszerrel áll kapcsolatban. A hardver-architektúra szempontjából a 12 dekóder processzort, memóriát – például ROM, RAM, FLASH, stb. memóriát – tartalmaz, akárcsak az ismert dekódoló egységek.

Az alkalmazások vagy úgynevezett rezidens alkalmazások, amelyek a 12 dekóder ROM-jában (vagy Flash, vagy más nem-felejtő tárolójában) vannak eltárolva, vagy a 12 dekóder RAM-jába (vagy Flash ROM-jába) kerülnek kisugárzás és letöltés útján. Az alkalmazások lehetnek műsorfűzet alkalmazások, játékok, interaktív szolgáltatások, távvásárlási alkalmazások, valamint a vevő és dekódoló berendezés bekapcsolást követő azonnali működőképességét lehetővé tevő alkalmazások, vagy például a vevő és dekódoló berendezés egyes paramétereinek konfigurálására szolgáló alkalmazások. Az alkalmazásokat a 12 dekóder memóriahelyein tároljuk és ezek erőforrás fájllokként és adatokként jelennek meg. Az erőforrás fájllok grafikus objektum leíró egység fájllokból, változó blokk egység fájllokból, utasítás sorrend fájllokból, alkalmazás fájllokból és adatfájllokból állnak.

A feltételes hozzáférési adatok szűrése

A 6. ábrán a csomag és táblázat adatok találmány szerinti feldolgozásához szükséges elemeket vázoltuk fel. Látható, hogy az ábrán feltüntetett elemek, összetevők akár hardveresen, akár szoftveresen, akár a kettő kombinációjában megvalósíthatók.

A műholdvevő által vett adás hagyományos 70 tuneren és ahhoz tartozó 79 demodulátor egységen keresztül érkezik be. A 70 tuner általában egy teljes frekvencia tartományt letapogat, és megáll, ha egy kiválasztott hordozó frekvenciát észlel az adott tartományban. A jeleket ezt követően a 79 demodulátor egység veszi át, amely kiválasztja és továbbítja a továbbított csomag adatáramot egy 80 demultiplexer és szűrő egységhez. Ennek a 80 demultiplexer és szűrő egységnek a szűrési struktúráját a későbbiekben a 7. ábra leírása kapcsán érthetjük meg. Mint látható, egy ilyen egység megvalósításához szükséges összetevők aktuális kiválasztása a gyártó szabad választásától függ, és egy ilyen egységgel kapcsolatos legfontosabb megfontolások a megválasztott szűrő konfigurációval kapcsolatosak.

A jelen kiviteli alak szerinti feltételes hozzáférési rendszerrel kódolt adatok esetében a 80 demultiplexer és szűrő egység a 12 dekóderbe helyezett 30 programozható csipkártyával (vagy bármilyen más biztonsági eszközzel), valamint jellemző módon a 12 dekóderben szoftver alkalmazásként megvalósított 81 csatorna paraméter alkalmazással működik együtt.

A 80 demultiplexer és szűrő egység a szállítási csomag adatáramból kiválasztja az adatáramban jelen lévő 41, 42 program térkép táblázatokat és a 47 feltételes hozzáférés táblázatokat. Visszanézve a 3. ábrára látható, hogy ezt a szűrési műveletet egy csomag azonosító szinten hajtjuk végre, ahol a 47 feltételes hozzáférési táblázatot a 0x01 csomag azonosító érték azonosítja be, és a megválasztott műsorszóró csatornának megfelelő 41, 42 program térkép táblázatot a 40 program hozzáférés táblázat segítségével, valamint az abban azonosított megválasztott csatorna program azonosító értékével választjuk ki. A 40 program hozzáférési táblázat csoportazonosító értéke 0x00.

A 81 csatorna paraméter alkalmazás ezen túlmenően a 30 programozható csipkártyától az azzal társított feltételes hozzáférési rendszer azonosítóját is megkapja. Ismét visszanézve a 3. ábrára, megfigyelhetjük, hogy egy első feltételes hozzáférési rendszert a 45 illetve 48 csomagokban lévő jogosultság vezérlő üzenet és jogosultság kezelési üzenet adatokkal van társítva. A 30 programozható csipkártyától megkapott feltételes hozzáférési rendszer azo-

nosítót, valamint a 80 demultiplexer és szűrő egységtől kapott 41, 42 program térkép táblázatokat és 47 feltételes hozzáférési táblázatot felhasználva a 81 csatorna paraméter alkalmazással meghatározzuk a szóban forgó feltételes hozzáférési rendszerrel társított feltételes hozzáférési csomagok csomag azonosító értékét, és ezeket az értékeket visszaadjuk a 80 demultiplexer és szűrő egységnek.

Egy egyszerűsített rendszer esetében, ahol viszonylag kis számú jogosultság vezérlő üzenetet és jogosultság kezelési üzenetet kell kibocsátanunk, nincs szükség más szűrésre, és ezeket a csomag azonosító értékeket használhatjuk a 80 demultiplexer és szűrő egységgel, hogy az azonosított csomagokból kiválasszuk az összes releváns jogosultság vezérlő üzenetet és jogosultság kezelési üzenetet privát szekciót, és hogy ezt követően az ezekben a szekciókban lévő adatokat a 30 programozható csipkártyákhoz továbbítsuk.

A feltételes hozzáférési adatokat ezt követően a 30 programozható csipkártya mikroprocesszorával feldolgozzuk, és az adással társított ellenőrző szót 83 bitsordekódoló egységhez juttatjuk el. A 83 bitsordekódoló egység fogadja a bitsorkódolt audiovizuális vagy egyéb adat információt, amelyet a 80 demultiplexer és szűrő egységgel a szállítási csomag adatáramból választottunk ki, ezt az ellenőrző szó segítségével bitsordekódolja, majd az adatokat egy hagyományos MPEG-2 csiphez küldi el, amely az adatokat felkészíti a hozzátartozó televízió képernyőn történő megjelenítéshez.

Míg azonban egy csomag azonosító szintű szűrés kizárólagosan a szóban forgó feltételes hozzáférési rendszerrel társított jogosultság vezérlő üzenetek és jogosultság kezelési üzenetek kiválasztását teszi lehetővé, nagy mennyiségű, a felhasználó számára érdektelen üzenet is jelen lehet. Ezek az üzenetek tartalmazhatnak más felhasználói csoportoknak szóló csoportos jogosultság kezelési üzeneteket, más egyedi felhasználóknak szóló egyedi jogosultság kezelési üzeneteket, és így tovább. A 30 programozható csipkártyához továbbított feltételes hozzáférési üzenetek mennyisége így igen nagyra nőhet. A feldolgozási teljesítmény és a 30 programozható csipkártya memóriájának korlátai miatt ez a mennyiség a gyakorlatban nagyobb lehet annál, mint amit a 30 programozható csipkártyával fel tudunk dolgozni.

Ennek a problémának a kiküszöbölése érdekében a 30 programozható csipkártyát úgy alakítjuk ki, hogy a 80 demultiplexer és szűrő egységhez további szűrési adatokat legyen képes eljuttatni, egy szekció vagy táblázat szintű szűrési művelet elősegítéséhez. Ha visszatekintünk a legutóbbi táblázatos felsorolásra, látható, hogy a feltételes hozzáférési adat

táblázat olyan táblázat azonosító és feltételes hozzáférés specifikus élőfej mezőket tartalmaz, amelyek arra szolgálnak, hogy jelezzék például egy jogosultság kezelési üzenet vagy jogosultság vezérlő üzenet jelenlétét (0x80 vagy 0x81, és 0x82 - 0x8F táblázat azonosító értékek), és az üzenet típusát (a feltételes hozzáférés specifikus adatok azonosítják az egy csoportos jogosultság kezelési üzenet által érintett csoportot, egy nyilvános jogosultság kezelési üzenet jelenlétét, és így tovább. A szükséges adatok függvényében a 30 programozható csipkártya elküldi a szükséges táblázat azonosító és feltételes hozzáférés specifikus adatokat, hogy úgy konfigurálja a 80 demultiplexer és szűrő egységet, hogy az képes legyen kizárólag a 30 programozható csipkártya számára érdekes feltételes hozzáférési üzeneteket kiválasztani és visszaküldeni. Ily módon a 30 programozható csipkártyához elküldött adatok mennyiségét le tudjuk csökkenteni, hogy a 30 programozható csipkártya mikroprocesszor feldolgozási képességét ne haladjuk meg.

A 7. ábrán a 80 demultiplexer és szűrő egység részleteit tüntettük fel. Ez az egység jellemző módon hardveres erőforrásként valósítható meg, amelyet a 12 dekóderben egy főmverkező alkalmazással hajtunk meg. Mint látható, egy első 85 szűrőkészlet a 81 csatorna paraméter alkalmazástól kapott feltételes hozzáférés csomag azonosító információ felhasználásával egy csomag azonosító szűrési eljárást hajt végre. A csomag azonosító 85 szűrők ugyanígy beállíthatók más releváns csomagok, például a 81 csatorna paraméter alkalmazáshoz küldött 41, 42 program térkép táblázatok vagy 47 feltételes hozzáférés táblázatok kiválasztására is. Az ábrán nem látható egyéb csomag azonosító szűrőket is használhatunk az esetlegesen a bitsordekódolóhoz küldött audiovizuális csomagokra bontott elemi adatáram csomag információ kibontására, és így tovább.

Miután a csomag élőfejtől megszabadítottuk, a privát szekció vagy táblázat adatokat olyan 80 előszűrő készlethez irányítjuk, amelyek egy táblázat kiterjesztett élőfejének 8 bájtnak szűrésére szolgálnak. Mint a legutóbbi kis táblázatban látható, a kiterjesztett élőfej 1 bájtna a táblázat azonosítóhoz tartozik, 7 bájtna pedig a feltételes hozzáférés specifikus információhoz tartozik. A szűrési műveletet úgy hajtjuk végre, hogy a 8 bájtos mintát a 30 programozható csipkártyától kapott szűrési adatokat tartalmazó táblázattal hasonlítjuk össze. Ennek során a 8 bájton belül néhány bitet, például egy 64 bites mintát kimaszkolhatunk, vagy figyelmen kívül hagyhatunk. A bemutatott kiviteli alak esetében harminckét különböző mintát alakítottunk ki, ahol ezen minták egy alkészletét az említett 86 előszűrőkkel használjuk, a 30 programozható csipkártyától kapott információ függvényében. Ha egy minta

egyezést találunk, a szekciót 87 FIFO puffer elemhez küldjük. Ha nincs bitminta egyezés, a szekciót figyelmen kívül hagyjuk. A 86 szűrők egyformán képesek a megfelelő szekciókból a 41, 42 program térkép táblázat és a 47 feltételes hozzáférés táblázat információ kiválasztására, amelyet azután 88 FIFO puffer elemhez továbbítanak.

A szállítási réteg tulajdonságai következtében a szekciók érkezése igen lökészerűen zajlik. A 87, 88 puffer elemek átmeneti tároló kapacitását elegendő nagyra kell választanunk ahhoz, hogy egy 5 Mbit/s átlagos adatsebességet le tudjanak kezelni, úgy, hogy a csomagok behelyezése egy lehetséges $\pm 25\%$ -os túréssal szabályos allokálással történik.

A találmány jobb megértése érdekében az alábbiakban felvázoljuk a 86 előszűrők által lekezelte üzemeltetési utasítások egy-egy lehetséges példáját.

Összes szekció szűrése (szűrő azonosító, cél, maszk, kiváltó feltételek, pozitív/negatív)
Ezzel a paranccsal az összes, a céllal megegyező szekciót ki tudunk választani, kivéve a maszkolt biteket, a kiváltó feltételek bekövetkezése után.

Következő szekció szűrése (szűrő azonosító, cél, maszk, kiváltó feltételek, pozitív/negatív)
Ezzel a paranccsal a céllal megegyező következő szekciót választhatjuk ki, kivéve a maszkolt biteket, a kiváltó feltételek bekövetkezését követően. A kiváltó feltételek az előzőleg egyezőként beazonosított többi szűrőre vonatkoznak.

Szűrő azonosító egy 0 és 31 közötti index, amely egy szűrőre és egy kimeneti várakozási sorra mutat. Ezen túlmenően megadja a várakozási sor prioritást is, ahol a 0 érték jelenti a legmagasabb prioritási szintet.

Cél egy 8 bájtos minta.

Maszk egy 8 bájtos minta, amely megmutatja a célon maszkolandó biteket, és a 0 érték jelenti a maszkolt állapotot.

Kiváltó feltételek: egy 32 bites bittérkép, amely a szűrő azonosítóval vagy viszonylatban gondoskodik az adott szűrő indításáról. 0 értékű bit azt jelenti, hogy nincs kiváltó feltétel. Az önkiváltó feltételt figyelmen kívül hagyjuk.

Pozitív/negatív egy általában 1-re beállított érték, amely a fent leírt normál működés esetén pozitív. Ha az érték 0, az negatív szűrést jelent, vagyis azoknak a szekcióknak a kiválasztását, amelyek nem egyeznek a céllal.

Az alábbiakban néhány használati példát mutatunk be:

1. példa

Összes szekció szűrése (5, 0x8C7C453AA8BBFF00, 0xFF557FFFEFFFFFF00, 0, 1)

Ezzel megkapjuk az egyezési feltételnek megfelelő összes jogosultság kezelési üzenetet.

2. példa

Következő szekció szűrése (0, 0x8000000000000000, 0xFF00000000000000, 0, 1)

Következő szekció szűrése (1, 0x8100000000000000, 0xFF00000000000000, 5, 1)

Következő szekció szűrése (2, 0x8000000000000000, 0xFF00000000000000, 3, 1)

Ezzel egy páros/páratlan átváltással egy jogosultság vezérlő üzenet fogadó műveletet kezdeményezünk.

3. példa

Következő szekció szűrése (8, 0x program térkép táblázat táblázat azonosító 0000 verziószám 00000000, 0xFF00001F00000000, 0, 0)

Következő szekció szűrése (1, 0x8100000000000000, 0xFF00000000000000, 0x14, 1)

Következő szekció szűrése (2, 0x8000000000000000, 0xFF00000000000000, 0x12, 1)

Ezzel páratlan-páros átváltással egy jogosultság vezérlő üzenet fogadó műveletet indítunk abban az esetben, amikor a program térkép táblázatban változás történik.

A 82 programozható csipkártya és a 80 demultiplexer és szűrő egység közötti feltételes hozzáférési üzenet és szűrési adat kommunikáció vonatkozásában valamilyen ismert szabványos protokollt, például az ISO 7816 protokollt használhattunk. Mivel a 82 programozható csipkártya számára nincs szükség az összes, a szűrt privát szekcióban található adatra, ezt a szekciót módosíthatjuk, és a 82 programozható csipkártyához az alábbi formátumú üzenetet küldhetjük el:

Táblázat azonosító	8 bit
0	11 bit
Szűrő azonosító	5 bit
Feltételes hozzáférés specifikus előfej mező	56 bit
Feltételes hozzáférés üzenet	Nx8 bit

Az eddig leírtak alapján a fenti fogalmak értelme nyilvánvaló. A 82 programozható csipkártyától a 80 demultiplexer és szűrő egységhez küldött szűrési adatok vonatkozásában az alábbi formátumot használhatjuk:

Szűrők száma	8 bit
Szűrési utasítás	5 bit
Szűrő azonosító	5 bit
Cél	64 bit
Maszk	64 bit
Kiváltó feltételek	5 bit
Pozitív/negatív	1 bit

Szűrők száma az utasításban beállítandó szűrők számát jelenti.

Szűrési utasítás az utasítás típusát (következő szekció szűrése, vagy összes szekció szűrése) írja le.

Szűrő azonosító egy szűrőre és egy kimeneti várakozási sorra mutató index, amely emellett megadja a várakozási sor prioritást is, ahol 0 érték jelenti a legmagasabb prioritást.

Cél a keresett bitminta.

Maszk a célon kimaszkolandó bitek mintáját mutatja, ahol 0 érték jelenti a maszkolt állapotot.

Kiváltó feltételek egy olyan bittérkép, amelyik a szűrő azonosítóval logikai VAGY kapcsolatban gondoskodik a szűrő indításáról. 0 értékű bit azt jelenti, hogy nincs kiváltó feltétel. Az önkiváltó feltételt itt is figyelmen kívül hagyjuk.

Pozitív/negatív egy általában 1-re beállított érték, amely a fent leírt normál működés esetén pozitív. Ha az érték 0, az negatív szűrést jelent, vagyis azoknak a szekcióknak a kiválasztását, amelyek nem egyeznek a céllal.

A gyakorlatban a 82 programozható csipkártya és a 12 dekóder közötti kommunikáció biztonsági szempontok alapján kódolásnak vagy bitsorkódolásnak vethető alá. Különösen a 82 programozható csipkártya és a 80 demultiplexer és szűrőegység közötti kommunikáció valamint a 83 bitsordekódoló egységhez küldött ellenőrző szó áram kódolható ezen a módon. Erre a célra számos megfelelő kódoló algoritmus ismert széles körben (RSA, DES, és így tovább).

Jóllehet a bemutatott kiviteli alaknál a 12 dekóder konfigurálását írtuk le a 30 programozható csipkártyával társított feltételes hozzáférési rendszer azonosítója függvényében, tálmányunk nem korlátozódik a 12 dekódernek ezzel az egy biztonsági modul rendszerrel összefüggő konfigurálására. A dekóder bármely más biztonsági modul rendszerrel együtt használható és konfigurálható.

Például a 30 programozható csipkártya olyan elszámoló rendszert használhat, amelyben elektronikus zsetonokat tartalmazó elektronikus "pénztárca" található, és ezt egy meghatározott összeggel megterheljük, ha az előfizető valamilyen "fizesd és nézd" eseményt megvásárol. Alternatív módon a 30 programozható csipkártyánál egy a hitelkártyáknál használt elszámolási rendszert is használhatunk, amelyben a 12 dekóder a 30 programozható csipkártyán tárolt banki információt képes kiolvasni, és a 16 modemes válaszcsatornán keresztül az előfizető bankszámlájának a megterhelése céljából kapcsolatot tud felvenni az illető bankkal. Az elszámolási rendszer azonosítójának egy alkalmazáshoz történő eljuttatásával, például a 81 csatorna paraméter alkalmazáshoz vagy hasonlóhoz történő eljuttatásával ez utóbbi a 12 dekódert úgy tudja konfigurálni, hogy az a 30 programozható csipkártya által támogatott módon hajtsa végre a soron következő megterhelést.

Egy másik példában a 30 programozható csipkártyával olyan jóváíró rendszert használhatunk, amelyben a programozható csipkártyán tárolt elektronikus zsetonokat tartalmazó elektronikus pénztárcában egy meghatározott összeget jóváírunk, ha az előfizető valamilyen kiválasztott és meghatározott promóciós eseményt végignézett. Alternatív módon a 30 programozható csipkártyát a hitelkártyáknál használthoz hasonló jóváíró rendszerrel is használhatjuk, amelyben a 12 dekóder kiolvassa a 30 programozható csipkártyán tárolt banki információt, és a bankkal a 16 modemes válaszcsatornán keresztül felveszi a kapcsolatot annak érdekében, hogy jóváírást eszközölhessen az előfizető bankszámláján. A jóváíró rendszer egy azonosítójának egy alkalmazáshoz, például a 81 csatorna paraméter alkalmazáshoz, vagy hasonlóhoz történő eljuttatásával, az alkalmazással a dekódert konfigurálni tudjuk úgy, hogy az a 30 programozható csipkártya által támogatott módon hajtsa végre a jóváíró műveletet.

Szabadalmi igénypontok

1. Dekóder egy továbbított csomag adatáram feldolgozására, ahol a továbbított adatáram a csomag hasznos részekbe illesztett csomagokra bontott adatokat tartalmaz, **azzal jellemezve**, hogy egy hordozható biztonsági modultól egy meghatározott biztonsági modul rendszer azonosítót fogadó eszközt, továbbá a dekódert (12) a kapott azonosító függvényében konfiguráló eszközt, továbbá a meghatározott biztonsági modul rendszerrel társított csomagokra bontott adatok szűrésére, szűrési adatokat a hordozható biztonsági modultól fogadó eszközt, valamint a kapott szűrési adatok függvényében csomagokra bontott adatokat szűrő eszközt tartalmaz.
2. Az 1. igénypont szerinti dekóder, **azzal jellemezve**, hogy a konfigurálást végző eszköz a dekódert (12) a kapott azonosító függvényében a csomagokra bontott adatokból a meghatározott biztonsági modul rendszerrel társított adatok kiválasztásához konfiguráló eszközként van kiképezve.
3. Az 1. vagy 2. igénypont szerinti dekóder, **azzal jellemezve**, hogy az azonosító egy meghatározott feltételes hozzáférési rendszer azonosítóját foglalja magában.
4. A 3. igénypont szerinti dekóder, **azzal jellemezve**, hogy a szűrő eszköz a csomagokra bontott adatokból egy program térkép táblázatot (41, 42) és egy feltételes hozzáférés táblázatot (47) tartalmazó továbbított csomagokat kiválasztó eszköz.
5. A 4. igénypont szerinti dekóder, **azzal jellemezve**, hogy a konfigurálást végző eszköz a program térkép táblázatot (41, 42) és a feltételes hozzáférés táblázatot (47) a szűrő eszköztől fogadó, és a szűrő eszközt a kapott azonosító és a program térkép táblázatban (41, 42) és a feltételes hozzáférés táblázatban (47) lévő adatok függvényében konfiguráló eszközként van megvalósítva.
6. Az 1-5. igénypontok bármelyike szerinti dekóder, **azzal jellemezve**, hogy az azonosító a biztonsági modul által használt meghatározott elszámolási rendszer azonosítót tartalmaz.
7. Az 1-6. igénypontok bármelyike szerinti dekóder, **azzal jellemezve**, hogy az azonosító a biztonsági modul által használt meghatározott jóváírási rendszer azonosítót tartalmaz.
8. Az 1-7. igénypontok bármelyike szerinti dekóder, **azzal jellemezve**, hogy a szűrő eszköz a továbbított adatáramból kiválasztott csomag adatokra vonatkozó legalább egy táblázat

azonosítót vagy szekció azonosítót tartalmazó szűrési adatok függvényében konfigurálható eszközként van megvalósítva.

9. Az 1-8. igénypontok bármelyike szerinti dekóder, **azzal jellemezve**, hogy a szűrő eszköz a csomagokra bontott adatokból egy meghatározott biztonsági modul rendszerrel társított adatok kiválasztására egy első szűrő eszközt, valamint a szűrési adatok függvényében a kiválasztott adatok tovább szűrésére egy második szűrő eszközt tartalmaz.

10. Dekóder egy továbbított csomag adatáram feldolgozására, ahol a továbbított adatáram a csomag hasznos részekbe illesztett csomagokra bontott adatokat tartalmaz, **azzal jellemezve**, hogy a csomagokra bontott adatokból egy meghatározott biztonsági modul rendszerrel társított adatokat kiválasztó első szűrő eszközt, valamint az egy hordozható biztonsági modultól kapott szűrési adatok függvényében a kiválasztott adatokat tovább szűrő második szűrő eszközzel rendelkezik.

11. A 10. igénypont szerinti dekóder, **azzal jellemezve**, hogy az első szűrő eszköz a biztonsági modultól kapott, a meghatározott biztonsági modul rendszer azonosítója függvényében konfigurálható eszközként van kiképezve.

12. A 9-11. igénypontok bármelyike szerinti dekóder, **azzal jellemezve**, hogy a második szűrő eszköz több szűrőt tartalmaz, melyek közül legalább egy szűrő a szűrési adatok függvényében konfigurálható módon van kiképezve.

13. A 9-12. igénypontok bármelyike szerinti dekóder, **azzal jellemezve**, hogy a második szűrő eszköz a szűrési adatokban található bitminta függvényében konfigurálhatóan van kialakítva.

14. A 13. igénypont szerinti dekóder, **azzal jellemezve**, hogy a második szűrő eszköz a kiválasztott adatokból a szűrési adatokban található bitmintával megegyező adatmintát kiszűrő módon konfigurálhatóan van kialakítva.

15. A 13. igénypont szerinti dekóder, **azzal jellemezve**, hogy a második szűrő eszköz a kiválasztott adatokból a szűrési adatokban található bitmintával egyező bitmintát tartalmazó adatokat kiszűrületlenül hagyóan van konfigurálva.

16. A 13-15. igénypontok bármelyike szerinti dekóder, **azzal jellemezve**, hogy a második szűrő készlet legalább egy szűrője a szűrési adatokban található maszkoló minta függvényében az adatminta legalább egy részét figyelmen kívül hagyó módon van konfigurálva.

17. Az 1-16. igénypontok bármelyike szerinti dekóder, **azzal jellemezve**, hogy a biztonsági modulhoz a csomagokra bontott adatokban lévő feltételes hozzáférési adatokat továbbító eszközzel van ellátva.
18. A 18. igénypont szerinti dekóder, **azzal jellemezve**, hogy a biztonsági modulhoz továbbított feltételes hozzáférési adatok jogosultság vezérlő üzeneteket és/vagy jogosultság kezelő üzeneteket tartalmaznak.
19. Az 1-19. igénypontok bármelyike szerinti dekóder, **azzal jellemezve**, hogy a biztonsági modul által rendelkezésre bocsátott szűrési adatok a szűrő eszköz által a biztonsági modulhoz címzett csoportos és/vagy egyedi jogosultságkezelő üzenetek kiválasztására használt adatokat tartalmaznak.
20. A 17-19. igénypontok bármelyike szerinti dekóder, **azzal jellemezve**, hogy a biztonsági modul által a hozzá továbbított feltételes hozzáférési adatok függvényében generált, egy bitsorkódolt adás bitsordekódolásához hasznosított ellenőrző szó vételére alkalmas módon van kialakítva.
21. Az 1-20. igénypontok bármelyike szerinti dekóder, **azzal jellemezve**, hogy a hordozható biztonsági modul felé illetve felől irányuló kommunikáció kódolására és/vagy dekódolására alkalmas módon van kialakítva.
22. Hordozható biztonsági modul az 1-21. igénypontok bármelyike szerinti dekóderben való használatra, **azzal jellemezve**, hogy egy meghatározott biztonsági modul rendszer azonosító eltárolására szolgáló memória eszközt, valamint az azonosítót a dekóder (12) konfigurálásához a dekóderhez (12) továbbító eszközt tartalmaz.
23. A 22. igénypont szerinti hordozható biztonsági modul, **azzal jellemezve**, hogy szűrési adatot eltároló eszköze, továbbá a szűrési adatokat a dekóderben (12) lévő szűrő eszközhöz továbbító eszköze van.
24. A 22 vagy 23. igénypont szerinti hordozható biztonsági modul, **azzal jellemezve**, hogy programozható csipkártyát foglal magában.
25. Eljárás a csomag hasznos részben megtalálható csomagokra bontott adatokat tartalmazó továbbított csomagáram feldolgozására, **azzal jellemezve**, hogy a hordozható biztonsági modultól egy meghatározott biztonsági modul rendszer azonosítóját vesszük, a dekódert (12) a vett azonosító függvényében konfiguráljuk, a hordozható biztonsági modultól vesz-

szük a meghatározott biztonsági modul rendszerrel társított csomagokra bontott adatok szűréséhez szükséges szűrési adatokat, és a csomagokra bontott adatokat a kapott szűrési adatok függvényében szűrjük.

26. A 25. igénypont szerinti eljárás, *azzal jellemezve*, hogy a csomagokra bontott adatokat a meghatározott biztonsági modul rendszerrel társított adatok kiválasztásához szűrjük.

27. A 25. vagy 26. igénypont szerinti eljárás, *azzal jellemezve*, hogy az azonosító egy meghatározott feltételes hozzáférési rendszer azonosítóját foglalja magában.

28. A 27. igénypont szerinti eljárás, *azzal jellemezve*, hogy az egy program térkép táblázat (41, 42) és egy feltételes hozzáférési táblázat (47) tartalmazó továbbított csomagokat a csomagokra bontott adatáramból választjuk ki.

29. A 28. igénypont szerinti eljárás, *azzal jellemezve*, hogy a csomagokra bontott adatokat a program térkép táblázatban (41, 42) és a feltételes hozzáférési táblázatban (47) lévő kapott azonosító és adatok függvényében szűrjük.

30. A 25-29. igénypontok bármelyike szerinti eljárás, *azzal jellemezve*, hogy az azonosító a biztonsági modul által használt meghatározott elszámolási rendszer azonosítóját is magában foglalja.

31. A 25-30. igénypontok bármelyike szerinti eljárás, *azzal jellemezve*, hogy az azonosító a biztonsági modul által használt meghatározott jóváíró rendszer azonosítóját is magában foglalja.

32. A 25-31. igénypontok bármelyike szerinti eljárás, *azzal jellemezve*, hogy a szűrési adatok a csomagokra bontott adatokra vonatkozó legalább egy táblázat azonosítót vagy szekció azonosítót foglalnak magukban.

33. A 25-32. igénypontok bármelyike szerinti eljárás, *azzal jellemezve*, hogy a csomagokra bontott adatokat a szűrési adatokban lévő bitminta szerint szűrjük.

34. A 33. igénypont szerinti eljárás, *azzal jellemezve*, hogy a bitmintával megegyező bitmintát tartalmazó adatokat szűrjük ki a csomagokra bontott adatokból.

35. Eljárás a csomag hasznos részben megtalálható csomagokra bontott adatokat tartalmazó továbbított csomagáram feldolgozására, *azzal jellemezve*, hogy a csomagokra bontott adatokból egy meghatározott biztonsági modul rendszerrel társított adatokat választunk ki,

és a kiválasztott adatokat egy hordozható biztonsági modultól kapott szűrési adatok függvényében szűrjük.

36. A 35. igénypont szerinti eljárás, **azzal jellemezve**, hogy a meghatározott biztonsági modul rendszer azonosítóját a biztonsági modultól fogadjuk.

37. A 25-36. igénypontok bármelyike szerinti eljárás, **azzal jellemezve**, hogy a kiválasztott adatokban lévő feltételes hozzáférési adatokat a biztonsági modulhoz továbbítjuk.

38. A 37. igénypont szerinti eljárás, **azzal jellemezve**, hogy a biztonsági modulhoz továbbított feltételes hozzáférési adatok jogosultság vezérlő üzeneteket és/vagy jogosultság kezelő üzeneteket foglalnak magukban.

39. A 25-38. igénypontok bármelyike szerinti eljárás, **azzal jellemezve**, hogy a biztonsági modul által rendelkezésre bocsátott szűrési adatok a dekóder (12) által a biztonsági modulhoz címzett csoportos és/vagy egyedi jogosultság kezelő üzenetek kiválasztásához használt adatokat foglalnak magukban.

40. A 37-39. igénypontok bármelyike szerinti eljárás, **azzal jellemezve**, hogy a biztonsági modullal a hozzá továbbított feltételes hozzáférési adatok függvényében egy ellenőrző szót állítunk elő, és ezt a ellenőrző szót használjuk a dekóderben (12) a bitsorkódolt adás dekódolásához.



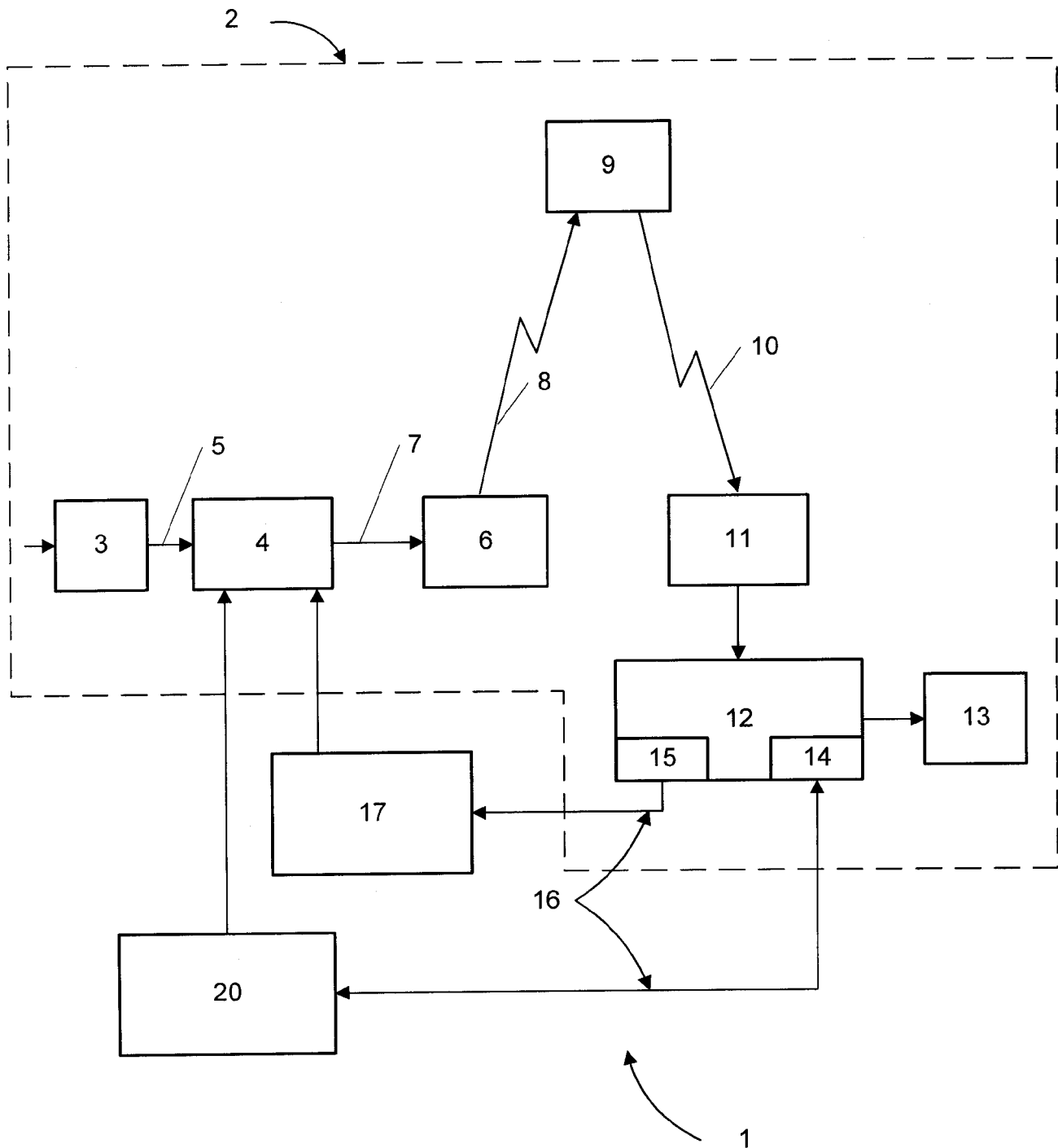
A meghatalmazott:

DANUBIA

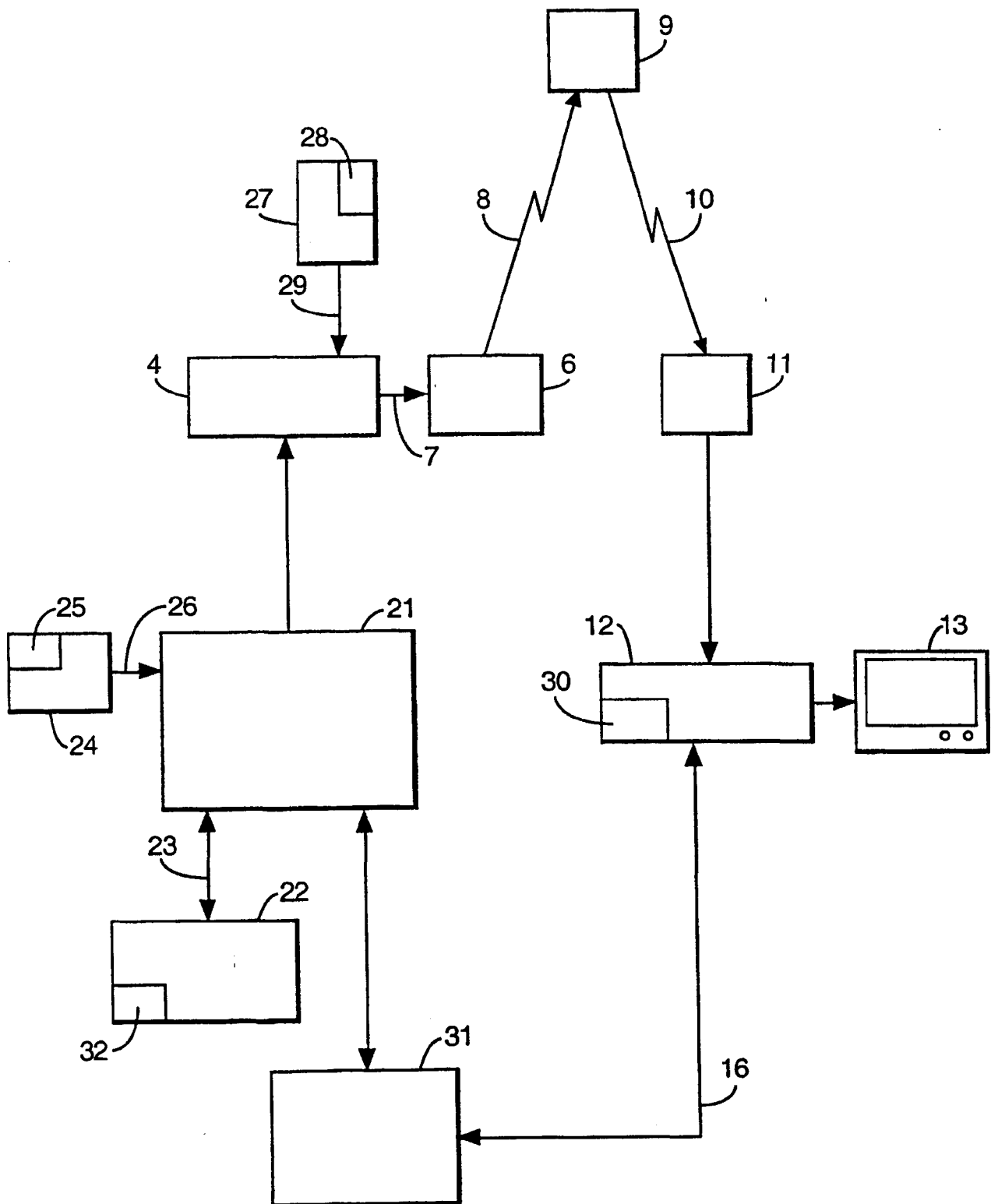
Szabadalmi és Védjegy Iroda Kft.



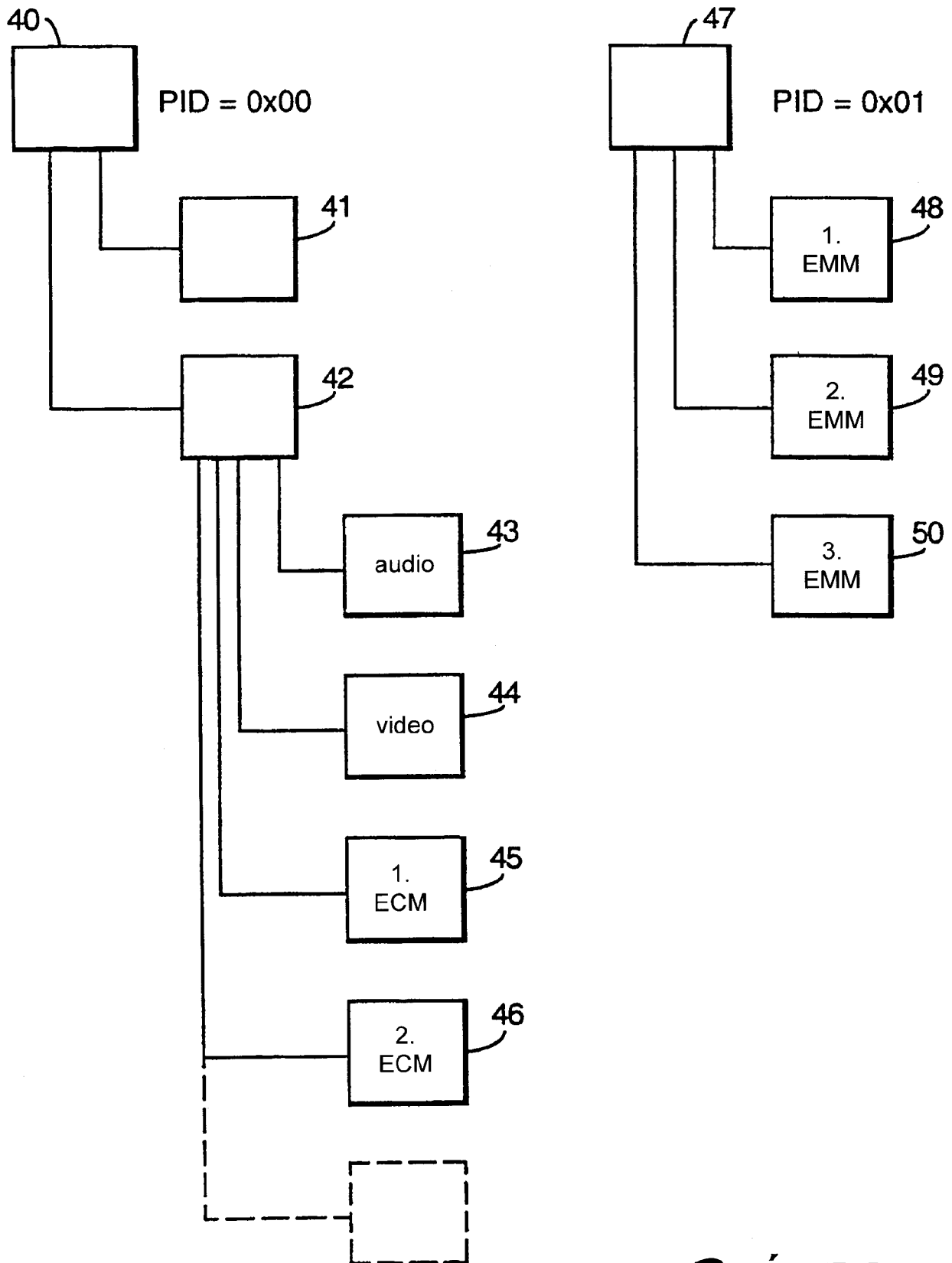
Antalffy-Zsíros András



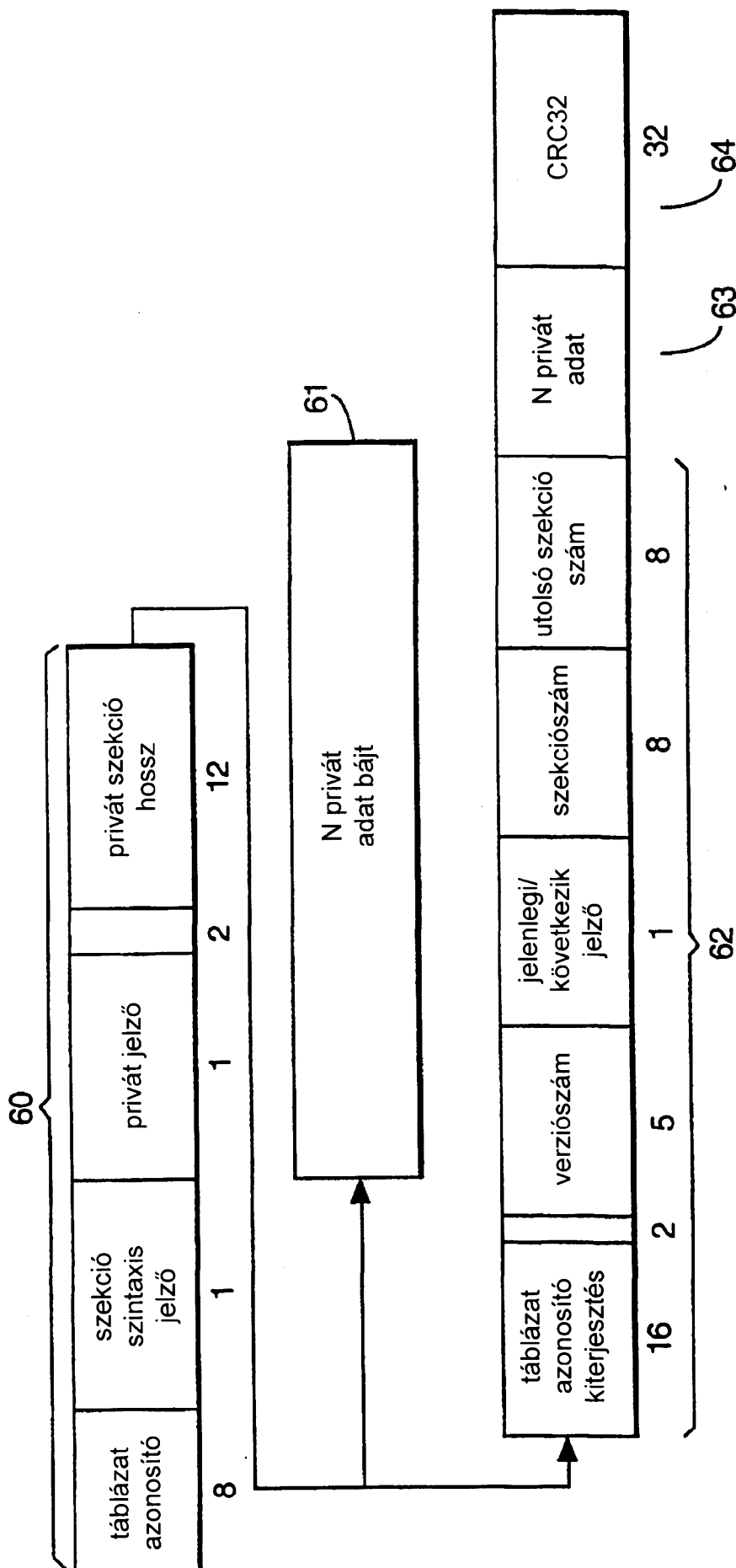
1. ÁBRA



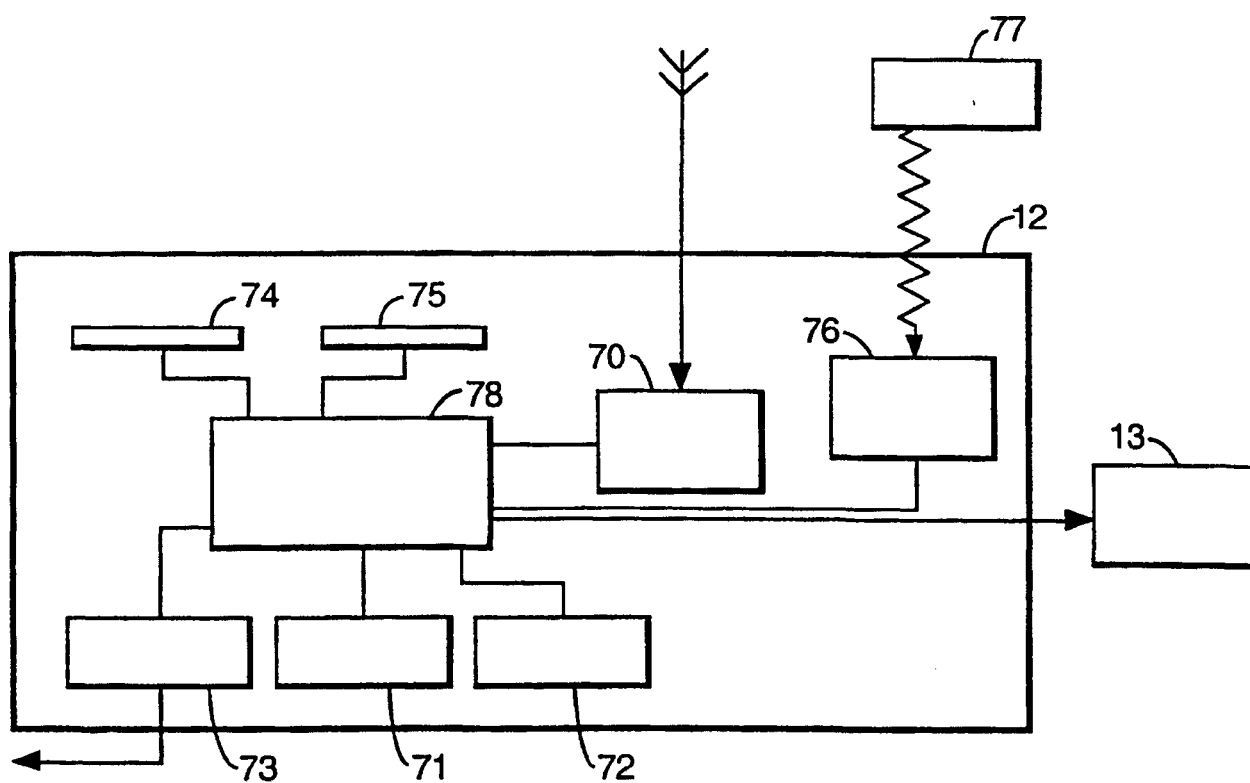
2. ÁBRA



3. ÁBRA

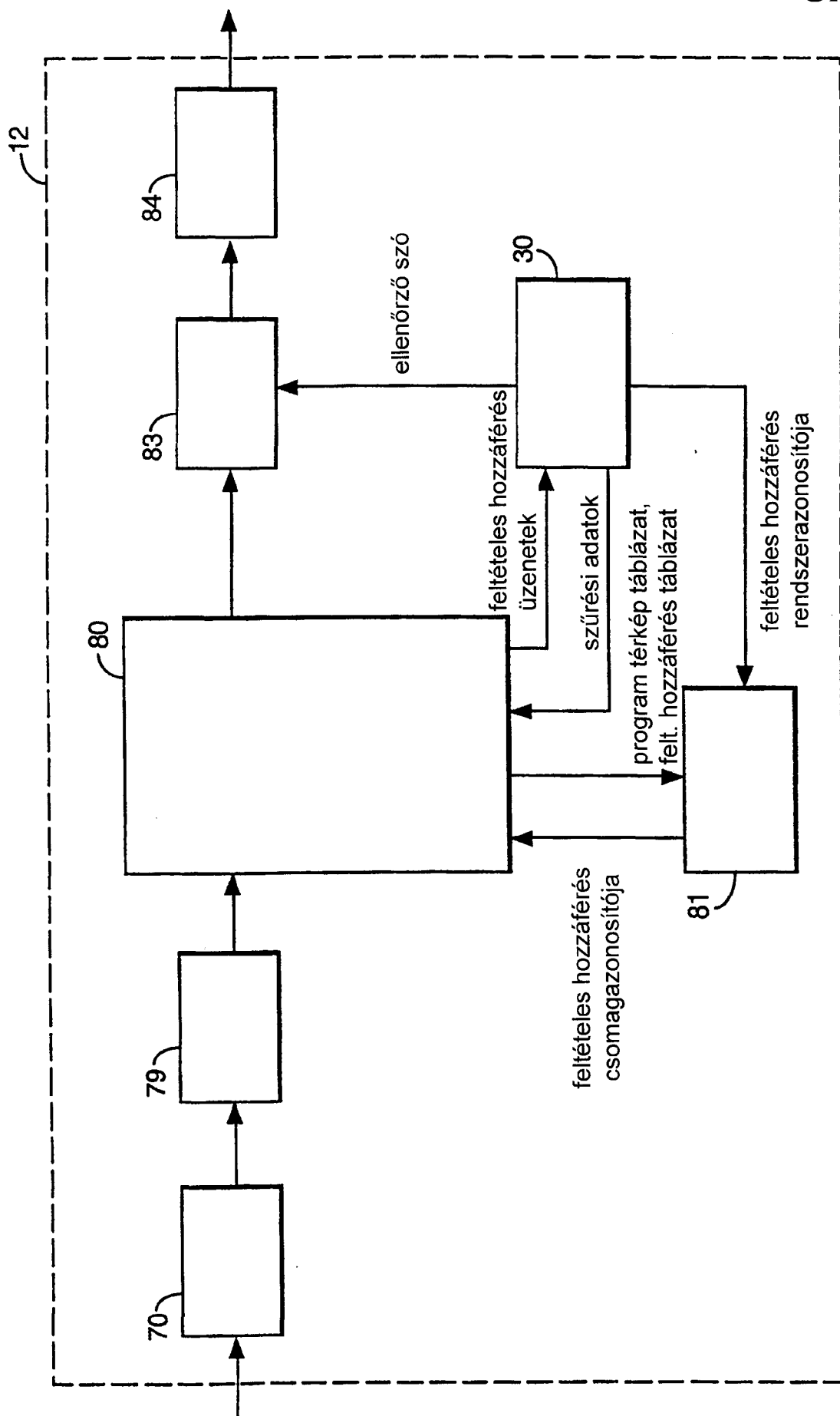


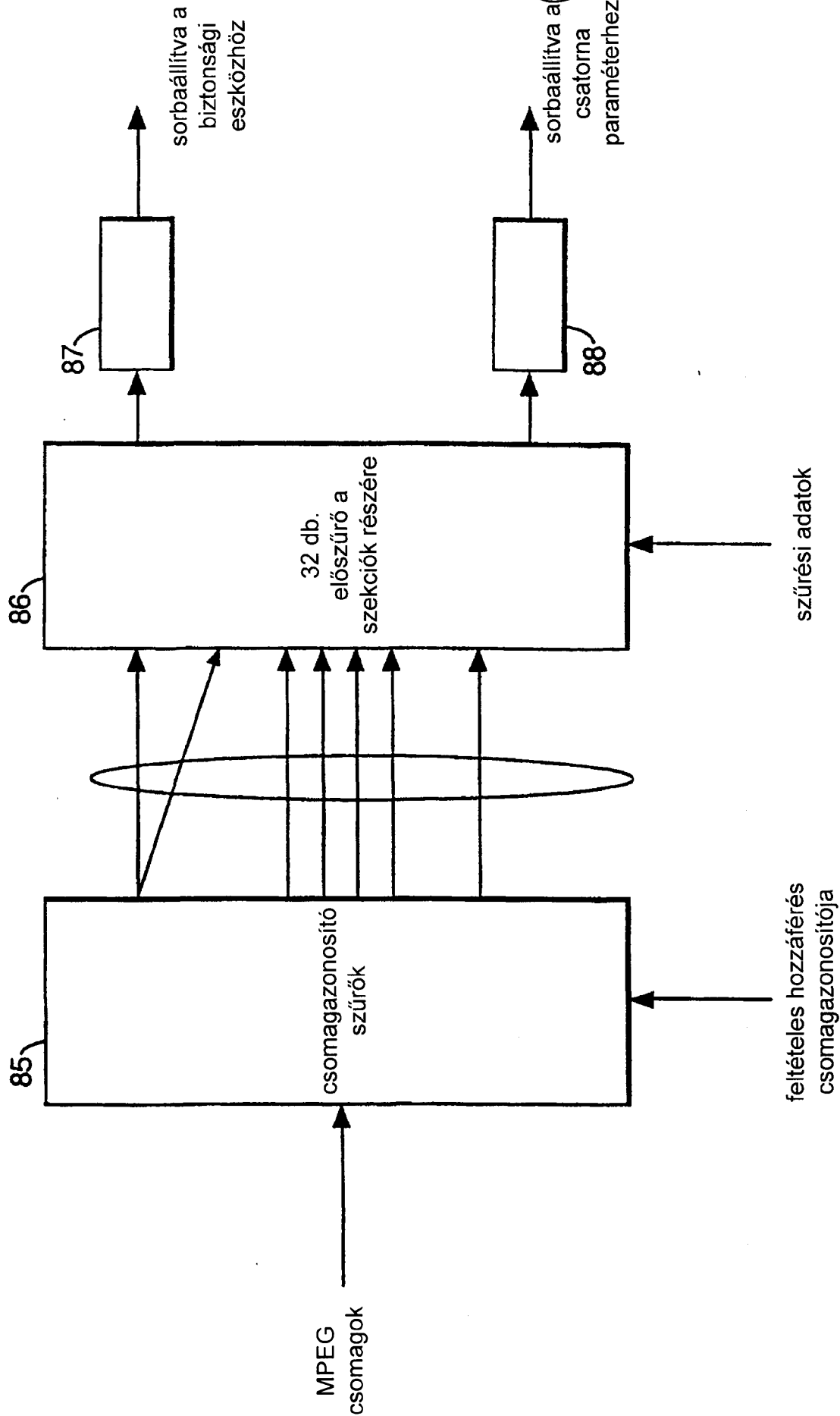
4. ÁBRA



5. ÁBRA

6. ÁBRA





7. ÁBRA