Eljárás első és második eszköz között továbbított adat kódolására, továbbá eszköz az eljárásban történő használatra, valamint rendszer első és második eszköz közötti biztonságos adattovábbításra

Kivonat

Eljárás egy első eszköz és egy második eszköz között továbbított adat kódolására, amelynek során az első eszköz memóriájában legalább egy előre kiszámított kulcspárt eltárolunk, ahol a legalább egy kulcspárba egy eseménykulcsot, valamint egy szállítási kulcs felhasználásával előállított szállítási kulcs kódolt verzióját veszünk, majd az eseménykulcs kódolt verzióját a második eszközhöz továbbítjuk, amelyben az eseménykulcs kódolt verzióját annak memóriájában tárolt ekvivalens szállítási kulcs felhasználásával dekódoljuk, úgy, hogy a legalább a második eszköztől az első eszközhöz továbbított adatokat az egyes eszközökben lévő eseménykulccsal tudjuk kódolni és dekódolni.

Egy első eszköz és egy második eszköz közötti biztonságos adattovábbításra szolgáló rendszer az első eszköz memóriájában legalább egy, egy eseménykulcsot, valamint egy szállítási kulcs felhasználásával előállított szállítási kulcs kódolt verzióját tartalmazó előre kiszámított kulcspárt eltároló, az eseménykulcs kódolt verzióját a második eszközhöz továbbító, és az eseménykulcs kódolt verzióját annak memóriájában tárolt ekvivalens szállítási kulcs felhasználásával, a legalább a második eszköztől az első eszközhöz továbbított adatokat az egyes eszközökben lévő eseménykulccsal kódoló és dekódoló eszközzel rendelkezik.

Egy, a javaslat szerinti eljárásban használt eszköz első eszközként legalább egy előre kiszámolt kulcspárt tároló memóriával rendelkezik, ahol a legalább egy előre számított kulcspár egy eseménykulcs, valamint az eseménykulcs kódolt változata.

Egy, a javaslat szerinti eljárásban használt másik eszköz második eszközként az első eszköz memóriájában tárolt kódolt eseménykulcs érték dekódolásához szükséges kulcsot és algoritmust tároló memóriával van ellátva.

(1. ábra)

Eljárás első és második eszköz között továbbított adat kódolására, továbbá eszköz az eljárásban történő használatra, valamint rendszer első és második eszköz közötti biztonságos adattovábbításra

A találmány tárgya egy eljárás, valamint egy berendezés két eszköz, például egy digitális televízió rendszer dekódere és hordozható biztonsági modulja közötti üzenetek kódolására. A találmány tárgya ezen belül egyrészt egy eljárás egy első eszköz és egy második eszköz között továbbított adat kódolására, másrészt egy eszköz a javasolt eljárásban történő használatra, harmadrészt pedig egy rendszer egy első eszköz és egy második eszköz közötti biztonságos adattovábbításra.

A kódolt adatok továbbítása a fizető televíziós rendszerekben jól ismert módszer. Ennek során a bitsorkódolt audiovizuális információt jellemzően műholdas úton juttatják el a nagyobb számú előfizetőhöz, és minden egyes előfizető rendelkezik olyan dekóder, vagy kombinált vevő és dekódoló berendezéssel, amely alkalmas a továbbító program bitsordekódolására, ezzel tulajdonképpen a kapott műsor megnézésére.

Egy ilyen jellemző rendszerben a bitsorkódolt adatokat az adatok bitsordekódolásához szükséges ellenőrző szóval együtt közvetítik, ahol magát az ellenőrző szót egy úgynevezett megfejtő kulccsal kódolják, és ilyen kódolt formában sugározzák ki. A bitsorkódolt adatokat és a kódolt ellenőrző szót egy olyan dekóderrel veszik, amely a dekóderbe ismert módon behelyezett hordozható biztonsági modulon, például programozható csipkártyán tárolt megfejtő kulcs ekvivalenshez bír hozzáféréssel. A kódolt ellenőrző szó dekódolása a programozható csipkártyán megy végbe, majd a dekóderbe kerül, hogy az a kapott adatokat annak segítségével bitsordekódolja.

Annak érdekében, hogy a rendszer biztonságosságát megnöveljék, vagy legalábbis erre kísérletet tegyenek, a jelenleg szokásos módon az ellenőrző szót hozzávetőlegesen minden 10 másodpercben, vagy ilyen idő érték körül, módosítják. Ezzel elkerülhető egy állandó, vagy csak ritkán változó ellenőrző szó esetén fellépő olyan szituáció, amelyben az ellenőrző szó publikussá válhat. Ilyen körülmények között egy rosszindulatú felhasználó számára viszonylag egyszerű feladat lenne a megismert ellenőrző szót dekóderének bitsordekódoló fokozatának megadnia, hogy ezzel a jogtalanul vett adást bitsordekódolni tudja.

A vázolt biztonsági intézkedés ellenére az utóbbi években olyan gondok jelentkeztek, hogy a például egy film sugárzása során elküldött ellenőrző szó áram publikussá vált. Ezt az in-

formációt aztán bármely, arra fel nem jogosított felhasználó, néző felhasználhatta, aki a bitsorkódolt filmet videomagnetofonra vette. Ha a filmet az ellenőrző szó áram dekóderbe táplálásával egyidejűleg játsszák le, a film nézhetővé, élvezhetővé válik. Az, hogy a felhasználó a filmet és az ellenőrző szó áramot egymással szinkronizálja, nem jelent túlságosan bonyolult műszaki problémát, különösen, amióta a bitsordekódoló felépítéséhez szükséges hardver eszközök, elemek igen könnyen beszerezhetők az Internet elterjedésével, hiszen nem okoz gondot olyan internetes honlapok megkeresése, amelyek az egy adás folyamán kisugárzott ellenőrző szavakat listázzák.

A WO 97/03530 számú nemzetközi szabadalmi leírás a fent vázolt probléma megoldására azt javasolja, hogy a programozható csipkártya és a dekóder közötti interfészen keresztül továbbított ellenőrző szó áramot is egy eseménykulccsal kell kódolni. Az eseménykulcsot a dekóder állítja elő véletlenszerűen, és egy benne tárolt második kulccsal kódolja, egy nyilvános kulcs-privátkulcs kódoló algoritmushoz tartozó nyilvános kulcs szerint. A hozzá tartozó programozható csipkártya az eseménykulcs dekódolása céljából rendelkezik a kulcspár privát kulcsával, amelyet a programozható csipkártyától a dekóderbe küldött ellenőrző szó áram kódolásához használ fel.

Nyilvánvaló, hogy az ellenőrző szó áram kódolásához való eseménykulcs helyi létrehozása azt jelenti, hogy ezt a kódolt jeláramot nem tudjuk másik dekóderbe táplálni az adatok bitsor dekódolásához, hiszen minden egyes dekóder más és más eseménykulcsot fog tartalmazni a programozható csipkártyától kapott ellenőrző szó áram dekódolásához.

Jóllehet a jelzett dokumentumban ismertetett megoldás magasabb biztonsági szintet nyújt a hagyományos rendszereknél alkalmazott biztonsági szintnél, a rendszerrel mégis számos kedvezőtlen hatás jár együtt.

Jelesül, a nyilvános kulcs - privátkulcs algoritmus használata egy ilyen rendszerben gyakorlatilag kötelező, hiszen biztonsági okokból nem célszerű a szimmetrikus kulcsot és az ahhoz tartozó algoritmust a dekóderben eltárolni, hiszen a dekóder memóriájából az információ bármikor és igen könnyen kiszedhető. Ez a probléma a nyilvános kulcs esetében nem jelentkezik, hiszen a nyilvános kulcs ismerete önmagában nem teszi lehetővé a privát kulccsal kódolt üzenetek dekódolását.

A találmánnyal egyik célunk a fent vázolt, ismert rendszerekhez képest egy a gyakorlatban használhatóbb alternatív megoldás létrehozása. Találmányunk azonban nem korlátozódik

egy dekóderrel kapcsolatos biztonsági feladatok megoldására, és mint a leírásból látható, számos olyan helyzetben és területen alkalmazható, ahol szükség van adatok biztonságos továbbítására, kommunikációjára.

A kitűzött feladatot egyrészt egy első eszköz és egy második eszköz között továbbított adat kódolására szolgáló eljárással oldottuk meg, amelynek során a találmány értelmében az első eszköz memóriájában legalább egy előre kiszámított kulcspárt eltárolunk, ahol a legalább egy kulcspárba egy eseménykulcsot, valamint egy szállítási kulcs felhasználásával előállított szállítási kulcs kódolt verzióját veszünk, majd az eseménykulcs kódolt verzióját a második eszközhöz továbbítjuk, amelyben az eseménykulcs kódolt verzióját annak memóriájában tárolt ekvivalens szállítási kulcs felhasználásával dekódoljuk, úgy, hogy a legalább a második eszköztől az első eszközhöz továbbított adatokat az egyes eszközökben lévő eseménykulccsal tudjuk kódolni és dekódolni.

Eltérően a WO 97/03530 számú nemzetközi szabadalmi leírásból megismert rendszertől, az előre kiszámított értékpárok használatával nincs szükség többé arra, hogy az első eszközben, például a dekóderben kódoló algoritmust alkalmazzunk a benne tárolt eseménykulcs kódolásához. Ennek következtében az eseménykulcs kódolásához kiválasztott algoritmusnak nem kell egy nyilvános kulcs/privát kulcs algoritmusra korlátozódnia, hanem szükség esetén egy szimmetrikus típusú algoritmust is kiválaszthatunk. Természetesen az eseménykulcs kódolásához továbbra is használhatunk nyilvános kulcs/privát kulcs algoritmust a későbbiekben leírt módon.

A javasolt eljárás egy előnyös foganatosítási módja értelmében az első eszköz memóriájában több kulcspárt tárolunk és az első eszközzel legalább egy eseménykulcsot kiválasztunk és feldolgozunk, hogy egy meghatározott eseménykulcsot állítsunk elő, és a legalább egy eseménykulcs kódolt, hozzátartozó változatát a második eszközhöz továbbítjuk, hogy azzal dekódoljuk és feldolgozzuk, hogy előállítsuk a meghatározott eseménykulcsot.

Azáltal, hogy az első eszközben több kulcspárt teszünk lehetővé, az első eszköz minden egyes kommunikációhoz ki tud választani és meg tud határozni egy, az előzőtől eltérő eseménykulcsot. Így a javasolt eljárás egy további előnyös foganatosítási módja értelmében több eltárolt eseménykulcsból álló alkészletet választunk ki az első eszközzel a meghatározott eseménykulcs létrehozására, és az eseménykulcs alkészlet hozzátartozó kódolt változatait továbbítjuk a második eszközhöz dekódolás és feldolgozás céljára.

Az alkalmazott művelet típusától függően az eredményül kapott eseménykulcs a kiválasztott eseménykulcsok kombinációjának sorrendjétől függhet. Így a javasolt eljárás egy további előnyös foganatosítási módja értelmében a meghatározott eseménykulcs előállításához használt eseménykulcsok kombinációjának a sorrendjét az első eszköztől a második eszközhöz továbbítjuk.

Például, a javasolt eljárás egy további előnyös foganatosítási módja értelmében az első eszköz számára és a második eszköz számára egyaránt ismert bázis eseménykulcs értéket ismétlődően kódolunk mindkét eszközben, meghatározott sorrendű eseménykulcsokkal, a kódolás sorrendjére érzékeny kódoló algoritmus, például a DES algoritmus alkalmazásával.

Természetesen olyan esetben, amikor az első eszköz egy kiválasztott kulcs alkészletet használ az eseménykulcs előállításához, nem szükséges egy sorrendfüggő algoritmust használnunk a változtatható eseménykulcs előállításához, és a kulcsokat például valamilyen egyszerű matematikai művelettel is kombinálhatjuk.

A javasolt eljárás egy további előnyös foganatosítási módja értelmében a legalább egy előre kiszámított kulcspárt még az első eszközben történő eltárolását megelőzően egy nagyobb előre számított kulcspár készletből választjuk ki. Például a rendszergazda, vagy a rendszert kezelő személy nagy számú előre kiszámított kulcspárt adhat át az első eszköz gyártójának, aki azután az egyes készülékekben ebből az átadott előre kiszámított kulcspárokból véletlenszerűen kiválasztott kulcspárokat tárol el.

Ezen a módon az első eszközben tárolt egy vagy több kulcspár az adott eszköz vonatkozásában teljesen, vagy legalábbis majdnem teljesen egyedinek tekinthető, ami növeli a rendszer biztonságosságát. Ezen túlmenően az eszköz gyártásáért felelős személynek nem kell a kódolt eseménykulcs értékek elkészítéséhez használt algoritmus vagy kulcsok birtokában lennie, hanem egyszerűen táblázatosan kaphatja meg a kulcspárokat.

A javasolt eljárás egy további előnyös foganatosítási módja értelmében a második eszközhöz továbbított eseménykulcs kódolt változat a második eszközzel olvasható aláírás értéket is tartalmaz, hogy az eseménykulcs kódolt változatának hitelességét ellenőrizhessük.

Ilyen aláírás értéket valamilyen hagyományos aláírás rendszerrel generálhatunk és hitelesíthetünk, például tördelő algoritmus, valamint nyilvános kulcs-privát kulcs algoritmus

kombinációjával, mint amilyenek az MD5 és RSA algoritmusok, és ezt az aláírást az első eszközben tárolt kulcspár értékekhez rendeljük hozzá.

Az aláírás értéket előnyösen a kódolt kulcsérték kiszámításának időpontjában is előre kiszámíthatjuk, majd később tárolhatjuk el az első eszközben.

A javasolt eljárás egy további, különösen előnyös foganatosítási módja értelmében egy eseménykulcs kódolásához és dekódolásához használt algoritmusként és szállítási kulcsként egy szimmetrikus algoritmust és ahhoz tartozó szimmetrikus kulcsot használunk. A szimmetrikus algoritmus használatával -- összehasonlítva a nyilvános kulcs-privát kulcs algoritmussal végzett műveletekkel -- meg tudjuk növelni a második eszköz számára az eseménykulcs dekódolásához szükséges feldolgozási időt.

Jóllehet találmányunk egyik fő előnyeként azt tekintjük, hogy a rendszer alkalmas akár szimmetrikus algoritmusok használatára is, szakember számára kézenfekvő, hogy ez ezen a módon nem kötelező. Például egy alternatív megvalósítása esetén az egy vagy több eseménykulcsot e nyilvános kulccsal kódolhatjuk még az első eszközben történő eltárolását megelőzően, valamint a második eszközben egy ekvivalens privát kulccsal dekódolhatjuk.

Ugyancsak előnyös a javasolt eljárás egy további foganatosítási módja, amelynek értelmében az első eszköz és a második eszköz között továbbított adat kódolásához és dekódolásához az eseménykulccsal használt kódoló algoritmusként szimmetrikus algoritmust használunk. Az alkalmazott algoritmus megválasztása többek között a rendszer követelményektől is függhet, például attól, hogy szükség van-e két irányú kommunikációra az egyes eszközök között.

Megfelelő szimmetrikus algoritmusok közé tartozik a DES, vagy valamilyen más alkalmas, ismert algoritmus. A megfelelő nyilvános kulcs - privát kulcs algoritmusok többek között RSA vagy más hasonló algoritmust is magukban foglalhatnak.

Mint arra már korábban utaltunk, találmányunk különösen a digitális televíziózás területén alkalmazható. Így a javasolt eljárás egy további előnyös foganatosítási módja értelmében első eszközként dekódert használunk, míg második eszközként hordozható biztonsági modult használunk, vagy fordítva.

A javasolt eljárás egy további, különösen előnyös foganatosítási módja értelmében hordozható biztonsági modulként programozható csipkártya és feltételes hozzáférési modul egyikét alkalmazzuk. Ilyen esetben az eseménykulccsal kódolt adatok a dekóder által a ka-

pott adatok bitsordekódolásához használt egyszerű ellenőrző szó információnak felelhet meg.

Ugyanezt az elvet alkalmazhatjuk abban az esetben is, amikor a dekóderben lévő bitsordekódoló egységet eltávolítható feltételes hozzáférési modulként valósítjuk meg, és a kapott sugárzott adatokat ebben a feltételes hozzáférési modulban bitsordekódoljuk, majd adjuk át a dekódernek.

Ilyen kiviteli alak esetén az első eszköz egy dekóder, a második eszköz pedig az eltávolítható feltételes hozzáférési modul lehet. Ilyen esetben egy eseménykulccsal kódolt és dekódolt adatként bitsordekódolt sugárzott adatot, például magát a műsort továbbítjuk.

A javasolt eljárás egy további előnyös foganatosítási módja értelmében első eszközként egy feltételes hozzáférési modult, második eszközként pedig egy programozható csipkártyát használunk.

A javasolt eljárás egy további előnyös foganatosítási módja értelmében az egy eseménykulccsal kódolt és dekódolt adataként ellenőrző szó adatot továbbítunk.

Egy feltételes hozzáférési modulként történő megvalósítás esetén egy programozható csipkártya is részét képezheti a rendszernek, amely kártyát ismert módon a feltételes hozzáférési modulba kell helyeznünk az ellenőrző szó dekódolásához, majd a dekódolt ellenőrző szót továbbítjuk, pontosabban adjuk át a programozható csipkártyáról a feltételes hozzáférési modulnak, hogy lehetővé tegyük ezzel a sugárzott és vett programok bitsordekódolását. Ilyen esetben az első eszköz lesz a feltételes hozzáférési modul, a második eszköz lesz a programozható csipkártya, és az eseménykulccsal kódolt adatok töltik be az ellenőrző szó szerepét.

A digitális televíziózás területén találmányunk egy dekóder és más eszköz, például televízió készülék vagy videomagnetofon közötti adatkommunikációra is alkalmazható. Így a javasolt eljárás egy további előnyös foganatosítási módja értelmében első eszközként és második eszközként egy első dekódert és egy második dekódert használunk.

Egy első és egy második dekóderrel is rendelkező háztartásokban számos probléma jelentkezik a tapasztalatok szerint az első, vagy "mester" valamint a második, vagy "szolga" dekóder közötti kapcsolat, pontosabban kommunikáció biztosítása során. Az audiovizuális adatok, ellenőrző szó adatok, vagy éppen az előfizetői jogosultságok és megfejtőkulcsok vonatkozó adatai közléséhez használt biztonságos, kódolt kapcsolat lehetőségét kell ezen a

téren megemlítenünk. Ilyen esetben a javasolt eljárás egy további előnyös foganatosítási módja értelmében házi hálózatban első eszközként és második eszközként valamilyen, például rádiós, infravörös, stb. kommunikációs útvonalon adatok továbbítására alkalmas első és második szórakoztató elektronikai készüléket használunk.

A fenti előnyös megoldások valamilyen adat kódolására szolgáló eljárással kapcsolatosan kerültek bemutatásra.

A kitűzött feladatot másrészt egy, a javasolt eljárásban használható eszközzel oldottuk meg, amely első eszközként legalább egy előre kiszámolt kulcspárt tároló memóriával rendelkezik, ahol a legalább egy előre számított kulcspár egy eseménykulcs, valamint az eseménykulcs kódolt változata.

A kitűzött feladatot harmadrészt egy, a javasolt eljárásban használható eszközzel oldottuk meg, amely második eszközként az első eszköz memóriájában tárolt kódolt eseménykulcs érték dekódolásához szükséges kulcsot és algoritmust tároló memóriával van ellátva.

A javasolt eszközök egy előnyös kiviteli alakja értelmében az első eszköz egy dekóder, a második eszköz pedig hordozható biztonsági modul.

A kitűzött feladatot negyedrészt egy első eszköz és egy második eszköz közötti biztonságos adattovábbításra szolgáló rendszerrel oldottuk meg, amely az első eszköz memóriájában legalább egy, egy eseménykulcsot, valamint egy szállítási kulcs felhasználásával előállított szállítási kulcs kódolt verzióját tartalmazó előre kiszámított kulcspárt eltároló, az eseménykulcs kódolt verzióját a második eszközhöz továbbító, és az eseménykulcs kódolt verzióját annak memóriájában tárolt ekvivalens szállítási kulcs felhasználásával a legalább a második eszköztől az első eszközhöz továbbított adatokat az egyes eszközökben lévő eseménykulccsal kódoló és dekódoló eszközzel rendelkezik.

A javasolt rendszer egy előnyös kiviteli alakja értelmében az első eszköz memóriájában több kulcspárt tároló, az első eszközzel legalább egy eseménykulcsot kiválasztó és egy meghatározott eseménykulcs előállításához feldolgozó, és a legalább egy eseménykulcs kódolt, hozzátartozó változatát a meghatározott eseménykulcs előállításához dekódolás és feldolgozás céljából a második eszközhöz továbbító eszközzel rendelkezik.

A javasolt rendszer egy további előnyös kiviteli alakja értelmében a második eszközhöz továbbított eseménykulcs kódolt változata annak hitelességnek az ellenőrzéséhez egy, a második eszközzel olvasható aláírás értéket is tartalmaz.

A javasolt rendszer egy további előnyös kiviteli alakja értelmében egy eseménykulcs kódolásához és dekódolásához használt algoritmusként és szállítási kulcsként egy szimmetrikus algoritmust és ahhoz tartozó szimmetrikus kulcsot foglal magában.

A javasolt rendszer egy további előnyös kiviteli alakja értelmében az első eszköz és a második eszköz között továbbított adat kódolásához és dekódolásához az eseménykulccsal használt kódoló algoritmusként szimmetrikus algoritmust foglal magában.

A javasolt rendszer egy további előnyös kiviteli alakja értelmében első eszközként dekódert tartalmaz.

A javasolt rendszer egy további előnyös kiviteli alakja értelmében második eszközként hordozható biztonsági modult tartalmaz.

A javasolt rendszer egy további előnyös kiviteli alakja értelmében hordozható biztonsági modulként programozható csipkártya és feltételes hozzáférési modul egyikét tartalmazza.

A javasolt rendszer egy további előnyös kiviteli alakja értelmében első eszközként egy feltételes hozzáférési modult, második eszközként pedig egy programozható csipkártyát foglal magában.

A javasolt rendszer egy további előnyös kiviteli alakja értelmében első eszközként és második eszközként egy első dekódert és egy második dekódert foglal magában.

A javasolt rendszer egy további előnyös kiviteli alakja értelmében házi hálózatban első eszközként és második eszközként egy kommunikációs útvonalon adatok továbbítására alkalmas első és második szórakoztató elektronikai készüléket foglal magában.

A "hordozható biztonsági modul" kifejezés alatt bármilyen hagyományos csipen, vagy programozható csipen alapuló hordozható kártya típusú készüléket értünk, amely például mikroprocesszort, és/vagy tároló memóriát tartalmaz. Ide tartozhatnak a programozható csipkártyák, a PCMCIA kártyák, az SIM kártyák, és így tovább. Ebbe a kifejezésbe vesszük a szokásostól eltérő fizikai kialakítású és megjelenésű, csipet tartalmazó eszközöket, mint amilyenek a jelenlegi fizető televíziós rendszerekben előszeretettel használt kulcs alakú kártyák, és így tovább.

Az ilyen eszközökre példaként egy programozható csipkártya olyan kártyaeszköz lehet, amely az ismert ISO-7816/1, ISO-7816/2 és ISO-7816/3 nemzetközi szabványok szerint készült, míg a feltételes hozzáférési modult a PCMCIA csoport által rögzített szabványok-

nak megfelelő PCMCIA vagy PC kártya alakjában valósíthatjuk meg. Természetesen ettől eltérő fizikai alakokat, kialakításokat is alkalmazhatunk.

A "bitsorkódolt", "kódolt", "ellenőrző szó", "kulcs", "kódoló kulcs" kifejezéseket csupán a használt fogalmak egyszerűsítése érdekében vezettük be és használtuk, és használjuk leírásunkban. Nyilvánvaló azonban, hogy a "bitsorkódolt adatok" és a "kódolt adatok" között, vagy például az "ellenőrző szó" és a "kódoló kulcs" kifejezések között alapvető különbséget nem lehet tenni.

Hasonlóképpen amennyiben a leírásban nem jelezzük, vagy más módon nem nyilvánvaló, egy adott kódolási és/vagy dekódolási művelet céljára sem szimmetrikus, sem nyilvános kulcs-privátkulcs algoritmusok használatát nem tekintjük kizárólagosnak. Hasonló módon, jóllehet a kódoló és dekódoló információban alkalmazott megegyezési kulcsot hasonló néven nevezhetjük (például "szállítási kulcs", "eseménykulcs"), nyilvánvaló, hogy ezeknek mindaddig, amíg feladatukat betöltik, nem kell számszerűen azonos kulcsoknak lenniük. Például az adatok kódolásához és dekódolásához használt megfelelő nyilvános és privát kulcsok általában különböző numerikus értékűek.

Miközben leírásunkban csaknem kizárólagosan "vevő és dekódoló berendezésről" és "dekóderről" beszélünk, nyilvánvaló, hogy találmányunk minden olyan kiviteli alakra vonatkozik, és használható, ahol egy vevő berendezés egy dekóderrel van egybeépítve, vagy ahol a dekóder egy tőle fizikailag különálló vevővel működik együtt. Természetesen találmányunk hasonlóképpen kiterjed mindazon kialakításokra is, ahol az említett egységeket, berendezéseket, készülékeket integráltan, egybeépítve alakítják ki, például a televízió készülékekkel, digitális videomagnetofonokkal, és így tovább.

A leírásunkban többször használt "digitális átviteli rendszer" például elsődlegesen audiovizuális vagy multimédia digitális adatok továbbítására vagy sugárzására szolgáló bármilyen jelátviteli rendszert jelenthet. Ugyan találmányunk elsődlegesen műsorszóró televízió rendszerben alkalmazható, eredményesen használható vezetékes hálózatokban is multimédia internetes alkalmazásokhoz, zárt láncú televízió rendszerekben, és így tovább.

A "digitális televízió rendszer" leírásunkban bármilyen műholdas, földi sugárzású, kábeles vagy egyéb rendszert magában foglal.

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

1. ábra egy digitális televízió rendszer általános felépítési vázlata, a

2. ábrán az 1. ábra szerinti digitális televízió rendszerben létrehozott feltételes hozzáférési rendszer felépítése látható, a

3. ábra egy programozható csipkártya és egy dekóder között továbbított adatok találmány szerinti eljárással történő kódolására mutat példát.

4. ábrán a 3. ábra szerinti eljárásban használt dekóderben egy eseménykulcs létrehozását vázoltuk fel, és az

5. ábra a 4. ábra szerinti dekóderben használt programozható csipkártyában egy eseménykulcs előállításának lépései követhetők nyomon.

Egy digitális televízió rendszerben egy dekóder, valamint egy hordozható biztonsági modul között továbbított adatok kódolására használható. A megoldás könnyebb megértése érdekében előbb néhány mondattal felvázoljuk egy ismert digitális televízió rendszer felépítését és működését.

Az 1. ábrán a találmány szerinti 1 digitális televízió műsorszóró és vételi rendszer vázlatát tüntettük fel az áttekintés elősegítésére. Az 1 digitális televízió műsorszóró és vételi rendszer hagyományosan felépített 2 digitális televízió rendszert foglal magában, amely az ismert MPEG-2 tömörítő rendszert használja tömörített digitális jelek kibocsátásához. Egy kicsit részletesebben, a 3 MPEG-2 tömörítő, amely egy műsorszóró központban helyezkedik el, digitális adatáramot kap (amely rendszerint video jel adatáram). A 3 MPEG-2 tömörítő 5 vonalon keresztül 4 multiplexer és bitsorkódolóhoz van csatlakoztatva. A 4 multiplexer és bitsorkódoló számos további bemenőjelet kap, ezekből egy vagy több szállító jeláramot állít össze, és a tömörített digitális jelet a műsorszóró központban lévő 6 adóberendezéshez továbbítja egy további 7 vonalon keresztül, amely természetesen számos módon megvalósítható, beleértve a szokásos távközlési vezetékes kapcsolatokat is.

A 6 adóberendezés egy földi állomástól műholdra irányuló 8 adatátviteli kapcsolat segítségével elektromágneses jeleket továbbít 9 transzponderhez, amely azt elektronikusan feldolgozza, és műholdról a földi állomás felé irányuló 10 adatátviteli kapcsolaton át földi 11 vevőhöz továbbítja, mely 11 vevő általában egy végfelhasználó tulajdonában álló, vagy általa bérelt parabola antenna. A 11 vevővel fogadott jelek szintén a végfelhasználó tulajdonában álló vagy általa bérelt integrált 12 vevő és dekódoló berendezésbe kerülnek,

amely a tömörített MPEG-2 jelet olyan televízió jellé alakítja vissza, amely minden további nélkül használható 13 televízió készülékben.

A 4 multiplexer és bitsorkódolóhoz és a 12 vevő és dekódoló berendezéshez egy 20 feltételes hozzáférési rendszer kapcsolódik, amely részben a műsorszóró központban, részben a 12 vevő és dekódoló berendezésben van kialakítva. Ez a 20 feltételes hozzáférési rendszer lehetővé teszi a felhasználó 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 vevő és dekódoló berendezésbe, és a kettő együttes használatával a végfelhasználó vagy előfizetéses módon, vagy fizetős módon (pontosabban "fizess és nézd" módon) műsorok által megtestesülő eseményeket vásárolhat.

Az ugyancsak a 4 multiplexer és bitsorkódolóhoz és a 12 vevő és dekódoló berendezéshez kapcsolódó 17 interaktív rendszer szintén egyrészt a műsorszóró központban, másrészt a 12 vevő és dekódoló berendezésben van kialakítva, és lehetővé teszi a végfelhasználó számára, hogy számos alkalmazással egy modemes 16 válaszcsatornán keresztül interaktív módon álljon kapcsolatban.

Most részletesebben is ismertetjük a 20 feltételes hozzáférési rendszert. A 2. ábrának megfelelően a 20 feltételes hozzáférési rendszer első áttekintésben tartalmaz egy 21 előfizető azonosító rendszert. A 21 előfizető azonosító rendszer kapcsolatban áll egy vagy több 22 előfizető karbantartó rendszerrel, és műsorszóró szolgáltatónként egy előfizető karbantartó rendszerrel, a megfelelő 23 TCP-IP kapcsolaton keresztül (bár vagylagosan használhatóak egyéb kapcsolat típusok is). Vagylagosan az egyik előfizető karbantartó rendszer megosztható két műsorszóró szolgáltató között, vagy egy szolgáltató használhat két előfizető karbantartó rendszert is, és így tovább.

"Anya" 25 csipkártyát használó 24 kódoló egységek alakját öltő első kódoló egységek csatlakoznak az előfizető azonosító rendszerhez a 26 kapcsolattal. Anya 28 csipkártyát alkalmazó, szintén 27 kódoló egységek formáját öltő második kódoló egységek csatlakoznak a 4 multiplexerhez a 29 kapcsolat révén. A 12 vevő és dekódoló berendezés hordozható biztonsági modult kap, például "gyermek" 30 csipkártya formájában. Ez közvetlenül a 21 előfizető azonosító rendszerhez csatlakozik a 31 kommunikációs szerveren keresztül a mo-

demes 16 válaszcsatornán keresztül. Kérésre az előfizető azonosító rendszer küldi el a gyermek 30 csipkártyának többek között az előfizetői jogokat is.

A programozható csipkártyák tartalmazzák egy vagy több kereskedelmi operátor titkos adatait. Az anya 25 csipkártya különböző üzeneteket kódol, és a gyermek 30 csipkártyák dekódolják az üzeneteket, már amennyiben ehhez jogosultságuk van.

A 24 és 27 első és második kódoló egységek mindegyike tartalmaz egy keretet, egy EEPROM-on tárolt szoftverrel bíró elektronikus üzenet kibocsátó kártyát, legfeljebb húsz elektronikus kártyát, és egy 25 ill. 28 csipkártyát minden egyes elektronikus kártyához, egy 28 kártyát a jogosultság vezérlő üzenetek kódolására és egy 25 kártyát a jogosultság kezelő üzenetek kódolására.

A digitális televíziós rendszer 20 feltételes hozzáférési rendszerét most részletesebben is ismertetjük a 2 televíziós rendszer és a 20 feltételes hozzáférési rendszer különböző alkotóelemeire való hivatkozással.

Amint az 1. és a 2. ábrán látható, a műsorközvetítő központban a digitális audio és videó jelet először is tömörítik (vagy csökkentik a bitrátáját) a 3 MPEG-2 tömörítő felhasználásával. A tömörített jelet ezt követően elküldik a 4 multiplexerre és bitsorkódolóra az 5 kapcsolaton át, más adatokkal, így például más tömörített t adatokkal való multiplexelés céljából.

A bitsorkódoló egy ellenőrző szót állít elő, amelyet a bitsorkódolási folyamat során használnak, és amely bekerül a multiplexerben levő MPEG-2 adatáramba. Az ellenőrző szó generálása belsőleg történik, és az ellenőrző szó teszi lehetővé azt, hogy a végfelhasználó 12 vevő és dekódoló berendezése bitsordekódolni tudja a műsort.

A műsor kereskedelmi forgalmazási módjára utaló hozzáférési kritériumokat is hozzáadják a MPEG-2 adatáramhoz. A műsor több "előfizetői" módozat valamelyikében, és/vagy több megtekintés esetén történő fizetési módozatban vagy eseményben ("fizess és nézd") kerülhet kereskedelmi forgalomba. Az előfizetői módban a végfelhasználó egy vagy több kereskedelmi ajánlatra vagy "csokorra" fizet elő, miáltal jogot szerez a csokorba tartozó valamennyi csatorna nézésére. Az előnyös kiviteli alakban akár 960 kereskedelmi ajánlat közül is választhatunk egy csatorna-csokron belül.

A "fizess és nézd" módban a végfelhasználó kívánsága szerint egyes eseményeket vásárolhat meg. Ez történhet az esemény előzetes lefoglalásával ("előfoglalási mód"). Az előnyös

kiviteli formában minden felhasználó előfizető is egyben, akár előfizetői, akár "fizess és nézd" módban működik, de természetesen a "fizess és nézd" nézőknek nem kell feltétlenül előfizetőknek is lenniük.

Az ellenőrző szót és a hozzáférési feltételeket egyaránt felhasználjuk a jogosultság ellenőrző üzenet felépítésére. Ez egy olyan üzenet, amelyet egy kódolt programra vonatkozóan küldenek el; az üzenet tartalmazza az ellenőrző szót (amely lehetővé teszi a műsor dekódolását) és a közvetített műsor hozzáférési kritériumait. Az ellenőrző szót és a hozzáférési kritériumokat a 27 második kódoló egységnek továbbítjuk a 29 kapcsolaton keresztül. Ebben az egységben generálódik, kódolódik és továbbítódik a 4 multiplexerre és bitsorkódolóra egy jogosultság vezérlő üzenet. A műsor közvetítése során az ellenőrző szó tipikus esetben pár másodpercenként változik, és ezért a jogosultság vezérlő üzeneteket is rendszeresen el kell küldeni, hogy dekódolni lehessen a változó ellenőrző szót. Redundancia okokból minden egyes jogosultság vezérlő üzenet tipikusan két ellenőrző szót tartalmaz; az aktuális ellenőrző szót, és a következő ellenőrző szót.

Minden egyes, egy műsorszóró szolgáltató által egy adatáramban sugárzott szolgáltatás több egymástól elkülönülő alkotóelemet tartalmaz; például egy televíziós műsor tartalmaz egy audio komponenst, egy alcím komponenst és így tovább. Egy szolgálat minden ilyen komponensét külön-külön bitsokódolják, majd kódoljuk az ezt követő, a 9 transzponderre történő közvetítés céljából. A szolgáltató minden egyes bitsorkódolt komponenséhez külön jogosultság vezérlő üzenetre van szükség. Vagylagosan előfordulhat az is, hogy egyazon szolgáltatás minden bitsorkódolt komponenséhez ugyanaz a jogosultság vezérlő üzenet szükséges. Többszörös jogosultság vezérlő üzenetek generálására is sor kerül olyankor, amikor többszörös feltételes hozzáférés vezérlő rendszerek ellenőrzik az egyazon közvetített műsorhoz való hozzáférést.

A jogosultság kezelő üzenet egy bizonyos végfelhasználónak (előfizetőnek) vagy végfelhasználók egy csoportjának szóló üzenet. Minden egyes csoport egy bizonyos számú végfelhasználót tartalmazhat. A csoportba szerveződés a sávszélesség optimalizálását szolgálja; vagyis, egy bizonyos csoport elérésével nagy számú végfelhasználót lehet megszólítani.

Különböző konkrét jogosultság kezelő üzenettípusokat lehet használni. Vannak egyéni, egyes előfizetőknek szóló jogosultság kezelő üzenetek, amelyeket tipikusan a "fizess és nézd" szolgáltatásokhoz használnak; ezek tartalmaznak egy csoport-azonosítót és megadják az előfizető pozícióját az adott csoporton belül.

A csoport előfizetői jogosultság kezelő üzenetek mondjuk 256 egyéni felhasználóból álló csoportoknak szólnak, és tipikusan bizonyos előfizetői szolgáltatások lebonyolítására használják fel őket. Az ilyen jogosultság kezelő üzenet rendelkezik egy csoportazonosítóval és az előfizetői csoport bittérképével.

A közönség jogosultság kezelő üzenetek az egész közönségnek szólnak, és például egy bizonyos operátor használhatja őket bizonyos ingyenes szolgáltatások biztosítására. A "közönség" az egyforma feltételes hozzáférés-azonosítóval ellátott programozható csipkártya tulajdonos előfizetők összessége. Végül pedig az "egyedi" jogosultság kezelő üzenet a programozható csipkártya egyedi azonosítójának szól.

Jogosultság kezelő üzenetek generálhatók például a különböző operátorok által az operátor által a fentiekben vázoltak szerint közvetített műsorokhoz kapcsolódó hozzáférési jogok szabályozása céljából. Generálhat jogosultság kezelő üzeneteket a feltételes hozzáférést szabályozó rendszergazda is, a feltételes hozzáférési rendszer bizonyos aspektusainak általános konfigurálása céljából.

A "jogosultság kezelő üzenet" kifejezést gyakran használjuk a dekóder, valamint a rendszer többi eleme között továbbított meghatározott konfigurációs típusú üzenetek leírására, és például leírásunk későbbi részében arra használjuk, hogy a dekódertől egy programozható csipkártyához küldött meghatározott üzenetet azonosítsunk a segítségével.

A 22 előfizető karbantartó rendszer (előfizető karbantartó rendszer) egy 32 adatbázist tartalmaz, amely többek között kezeli az összes végfelhasználói adatállományt, a kereskedelmi ajánlatokat, előfizetéseket, "fizess és nézd" adatokat és a végfelhasználó fogyasztására és engedélyeire vonatkozó adatokat. Az előfizető karbantartó rendszer fizikailag elkülönülhet az előfizető azonosító rendszertől.

Minden egyes 22 előfizető karbantartó rendszer üzeneteket küld a 21 előfizető azonosító rendszernek a megfelelő 23 kapcsolaton keresztül, amelyek a végfelhasználónak továbbítandó jogosultság kezelő üzenetek módosítását vagy létrehozását implikálják.

A 22 előfizető karbantartó rendszer közvetít továbbá olyan üzeneteket is a 21 előfizető azonosító rendszernek, amelyek nem implikálják jogosultság kezelő üzenetek módosítását vagy létrehozását, hanem csak a végfelhasználó státuszát változtatják meg (a végfelhasználónak termékek megrendelése esetén adott engedélyek vagy a végfelhasználónak felszámítandó díj vonatkozásában).

A 21 előfizető azonosító rendszer üzeneteket küld a 22 előfizető azonosító rendszernek (tipikus esetben visszavonási vagy számlázási információkat kérve), vagyis nyilvánvaló, hogy a kettőjük közötti kommunikáció kétirányú.

A 22 előfizető karbantartó rendszer által generált üzenetek a 23 kapcsolaton át jutnak el a 21 előfizető azonosító rendszerhez (előfizető azonosító rendszerhez), amely erre a 21 előfizető karbantartó rendszer által generált üzenetek fogadását nyugtázó üzeneteket generál, és ezeket a nyugtázó üzenetek továbbítja a 22 előfizető karbantartó rendszernek.

Áttekintve, a 22 előfizető azonosító rendszer tartalmaz egy előfizetői lánc területet az előfizetők módozati jogainak a megadására és automatikus havi meghosszabbítására, egy "fizess és nézd" láncot a "fizess és nézd" eseményekhez való jog megadására és egy jogosultság kezelő üzenet bejuttatót az előfizetői és a "fizess és nézd" láncok területén generált jogosultság kezelő üzenetek továbbítására a 4 multiplexerhez és bitsorkódolóhoz, és ezáltal a MPEG adatáram jogosultság kezelő üzenetekkel való feltöltésére. Ha szükség van egyéb jogok megadására is, így például "fizess adatállományonként" (pay per file) jogéra számítógépes szoftver-fájlok letöltésére a felhasználó személyi számítógépére, akkor erre is megvannak a megfelelő hasonló területek.

A 21 előfizető azonosító rendszer egyik feladata a különböző kereskedelmi forgalmazási módozatoknak (előfoglalási mód, impulzus mód) megfelelően előfizetői módban, kereskedelmi ajánlatként vagy "fizess és nézd" eseményként kínált televíziós műsorokhoz való hozzáférési jogok kezelése. A 21 előfizető azonosító rendszer a megfelelő jogok és a 22 előfizető karbantartó rendszertől kapott információk alapján generálja az előfizető jogosultság kezelő üzeneteit.

A jogosultság kezelő üzeneteket elküldik a 24 kódoló egységnek kódolásra a kezelési és megfejtési kódok szerint. A 24 kódoló egység kitölti a jogosultság kezelő üzenet aláírását, és a jogosultság kezelő üzenetet visszaküldi a 21 előfizető azonosító rendszeren található üzenet generátornak, ahol hozzátesznek egy élőfejet. A jogosultság kezelő üzeneteket teljes jogosultság kezelő üzenetként továbbítják az üzenet kibocsátóra. Az üzenet generátor határozza meg a közvetítés időpontjának kezdetét és végét és a jogosultság kezelő üzenet kibocsátás gyakoriságát, és ezeket megfelelő utasításként továbbítja a jogosultság kezelő üzenetekkel együtt az üzenet kibocsátónak. Az üzenet generátor csak egyszer generál egy bizonyos jogosultság kezelő üzenetet - a jogosultság kezelő üzenetek ciklikus közvetítését az üzenet kibocsátó végzi.

Jogosultság kezelő üzenet generálásakor az üzenet generátor egyedi azonosítót rendel a jogosultság kezelő üzenethez. Amikor az üzenet generátor továbbítja a jogosultság kezelő üzenetet az üzenet kibocsátónak, egyszersmind a jogosultság kezelő üzenet azonosítóját is továbbítja. Ez lehetővé teszi egy bizonyos jogosultság kezelő üzenet azonosítását mind az üzenet generátorban, mind az üzenet kibocsátóban.

A 4 multiplexer fogadja a 21 előfizető azonosító rendszerről érkező, kódolt jogosultság kezelő üzeneteket tartalmazó elektromos jeleket, a 27 második kódoló egységről érkező kódolt jogosultság vezérlő üzeneteket és a 3 kompresszorról érkező tömörített műsorokat. A 4 multiplexer bitsorkódolja a műsorokat, és a bitsorkódolt műsort, a kódolt jogosultság kezelő üzeneteket és a kódolt jogosultság vezérlő üzeneteket elküldi a műsorszóró központ 6 adójába a 7 kapcsolaton keresztül. A 6 adó elektromágneses jeleket továbbít a műholdas 9 transzponderre a 8 adatátviteli kapcsolaton keresztül.

A 9 transzponder veszi és feldolgozza a 6 adó által továbbított elektromágneses jeleket, és továbbítja azokaz a 11 földi vevőállomásnak, amely általában a végfelhasználó tulajdonát képező vagy általa bérelt parabola antenna tányérját jelenti, a 10 adatátviteli kapcsolaton keresztül. A 11 vevő által vett jeleket továbbítják egy 12 integrált vevő és dekódoló berendezésre, amely a végfelhasználó tulajdonában van, vagy amelyet az bérel, és amely össze van kapcsolva a végfelhasználó 13 televízió-készülékével. A 12 vevő és dekódoló berendezés demultiplexeli a jeleket, miáltal bitsorkódolt műsorokhoz jut, kódolt jogosultság kezelő üzenetekkel és kódolt jogosultság vezérlő üzenetekkel.

Ha a műsor nincs bitsorkódolva, vagyis ha nem továbbítottak jogosultság vezérlő üzenetet a MPEG-2 áramban, a 12 vevő és dekódoló berendezés kibontja az adatokat, és átalakítja a jelet videó-jellé, a 13 televízió-készülékre való leadás céljából.

Ha a műsor bitsorkódolva van, a 12 vevő és dekódoló berendezés kivonja a MPEG-2 áramból a megfelelő jogosultság vezérlő üzenetet, és az továbbítja azt a végfelhasználó gyermek 30 csipkártyájának. Ez a 12 vevő és dekódoló berendezés dobozában foglal helyet. A gyermek 30 csipkártya szabályozza azt, hogy a végfelhasználónak jogában áll-e a jogosultság vezérlő üzenet dekódolása, és hozzáférhet-e a műsorhoz. Ha nem, a negatív válasz továbbítódik a 12 vevő és dekódoló berendezésre, jelezve, hogy a műsor nem bitsordekódolható. Ha a végfelhasználó rendelkezik a megfelelő jogokkal, sor kerül a jogosultság vezérlő üzenet dekódolására és az ellenőrző szó kivonására.

Ezt követően a 30 programozható csipkártya az ellenőrző szót közli a 12 vevő és dekódoló berendezéssel, amely a programot a kapott ellenőrző szó segítségével bitsor dekódolja. A legtöbb hagyományos felépítésű rendszerben az ellenőrző szó nyílt, kódolatlan formában kerül továbbításra a programozható csipkártya és a dekóder közötti interfészen keresztül, amely a bejelentésünk bevezető részében leírt biztonsági problémákhoz vezet. A 12 vevő és dekódoló berendezéssel történő bitsor dekódolását követően az MPEG-2 jeláram video jellé alakul át, amely a 13 televízió készülékhez kerül, és azon megtekinthető.

A fent leírt rendszerben az MPEG adatok bitsor dekódolását a 12 vevő és dekódoló berendezésben hajtjuk végre, annak az ellenőrző információnak a felhasználásával, amelyet a 30 programozható csipkártya közöl a 12 vevő és dekódoló berendezéssel. Más rendszerekben a bitsor dekódolást végrehajtó áramkört egy a 12 dekódertől különválasztható feltételes hozzáférési modulként is megvalósíthatjuk, amelyet általában a 12 dekóder megfelelő fészkébe helyezhető PCMCIA kártyaként vagy PC kártyaként alakítanak ki.

Ez a feltételes hozzáférési modul saját maga is rendelkezik egy olyan belső fészekkel, amelybe egy 30 programozható csipkártya dugható. Ezekben a rendszerekben az ellenőrző szó adatok dekódolása a 30 programozható csipkártyában történik, amely ezeket az adatokat átadja a feltételes hozzáférési modulnak, amely ennek segítségével a bitsor kódolt MPEG adatáramot bitsor dekódolja, hogy a 12 vevő és dekódoló berendezést dekomprimálás és azt követő megjelenítés céljából egy kódolatlan MPEG árammal láthassa el.

Az ilyen típusú rendszer esetében az érzékeny adatokat a 30 programozható csipkártya és a feltételes hozzáférési modul, és/vagy a feltételes hozzáférési modul és a 12 vevő és dekódoló berendezés között kell átadni (ellenőrző szó adatok, illetve bitsordekódolt MPEG adatok), és bármelyik interfésznél felléphetnek a már korábban jelzett biztonsági problémák.

A 3. ábrára áttérve egy találmány szerinti eljárási foganatosítási módot mutatunk be, amellyel a 30 programozható csipkártya, valamint a 12 vevő és dekódoló berendezés között továbbításra kerülő ellenőrző szó adatokat tudjuk kódolni, a találmány egyik legegyszerűbb megvalósítási formájában. Természetesen az ebből levezethető és megismerhető elvek alkalmazhatók egy programozható csipkártya és egy feltételes hozzáférési modul közötti ellenőrző szó adatok kódolására, vagy egy feltételes hozzáférési modul és egy dekóder között audiovizuális MPEG adatok kódolására, vagy két hasonló eszköz között bármilyen típusú adat kódolására.

Találmányunk értelmében a 12 dekóder nemfelejtő tárában, például Flash memóriájában egy kulcspár készletet tárolunk. Minden egyes kulcspár egy kódolatlan formában megjelenő kulcsnak, valamint egy kódolt változatú kulcsnak felel meg. Mint majd látható, a kulcs kódolt változatát adott esetben egy jogosultság kezelő üzenetben továbbítjuk a 12 dekóderbe helyezett 30 programozható csipkártyához.

Így a 12 dekóderben az alábbi módon tárolunk el egy jogosultság kezelő üzenet - kulcspár készletet:

n	jogosultság kezelő üzenet (19 oktet)	kulcs (8 oktet)
1	jogosultság kezelő üzenet (1)	kulcs (1)
2	jogosultság kezelő üzenet (2)	kulcs (2)
3	jogosultság kezelő üzenet (3)	kulcs (3)
.	.	.
.	.	.
.	.	.
.	.	.
16	jogosultság kezelő üzenet (16)	kulcs (16)

A jogosultság kezelő üzenetben eltárolt kulcs kódolt értékét a 12 dekóderen kívül számítjuk ki, a 12 dekóderben nem található kódoló algoritmus segítségével. A bemutatott esetben a kulcs(1), kulcs(2) kulcsértékek valamilyen szimmetrikus kódoló algoritmussal, például a DES algoritmussal használt szimmetrikus kulcsoknak felelnek meg.

A kódolt DES kulcsértékek előállításához használt és az eltárolt jogosultság kezelő üzenetekben lévő kódoló algoritmus egy szimmetrikus kódoló algoritmus is lehet. Növelt biztonság céljából a DES algoritmustól eltérő megfelelő szimmetrikus algoritmust is használhatunk a kódolt értékek előállításához, bár más kiviteli alakok esetében DES algoritmust is használhatunk a kulcsértékek kódolásánál.

A kulcs kódolt értékén túl egy jogosultság kezelő üzenet az üzenethez tartozó és bármely más aláírás előállító eljárással létrehozott aláírás értéket is tartalmazhat. Például egy üzenetet egy tördelő függvényben, például MD5 függvényben is feldolgozhatunk, majd a tördelő értéket valamilyen nyilvános kulcs - privát kulcs algoritmus, például az RSA algoritmus privát kulcsával kódolhatjuk. Az aláírás ellenőrzését vagy hitelesítését ezt követően a vétel során hajthatjuk végre, amihez ismét egy MD5 algoritmust, valamint a nyilvános

kulcs-privát kulcs pár megfelelő nyilvános kulcsát használjuk fel.

A jogosultság kezelő üzenet ezen túlmenően (az ISO 7816-3 nemzetközi szabvány által meghatározott módon) szabványos programozható csipkártya élőfej elemet is tartalmaz, amelynek segítségével az üzenetet olyan formátummá tudjuk alakítani, amelyet egy 30 programozható csipkártya olvasni képes. Egy nyolc bájtos kulccsal társított jogosultság kezelő üzenet így jellemző módon az alábbi felépítésű lesz:

élőfej	5 bájt
kódolt kulcs	10 bájt
aláírás	9 bájt

A bemutatott foganatosítási mód esetében a 12 dekóder memóriájában tizenhat kulcs-üzenet pár készletet helyezünk el. Ettől eltérő kiviteli alakok ennél több vagy kevesebb kulcs-üzenet párt is használhatnak, és a találmány eredményesen megvalósítható egyetlen kulcs-üzenet pár felhasználásával is. Miközben az sem kizárt, hogy az összes 12 dekóder ugyanazokat a kulcs-üzenet párokat tartalmazza, előnyösnek tartjuk biztonsági okokból, hogy minden egyes 12 dekóder egyedi kulcs-üzenet pár készletet tartalmazzon. Egy ilyen megvalósítás esetében egy rendszergazda a 12 dekóder gyártója számára ezernyi vagy még annál is több kulcs-üzenet pár készletet bocsáthat rendelkezésre, és ilyen esetben a dekóder gyártója véletlenszerűen választja ki az egyes 12 dekóderek elkészítése és testre szabása során a 12 dekóderbe telepített 16 párt.

A biztonság megnövelés érdekében minden egyes használat során a 12 dekóderben lévő más és más kulcs-üzenet pár alkészletet használunk. Egy ilyen használatot úgy definiálhatunk, mint a 12 dekóder bekapcsolása és kikapcsolása közötti időtartamot, vagy például a 12 dekóderrel végrehajtott két csatornaváltás közötti időszakot, és így tovább.

A 3. ábrán látható, hogy a 12 dekóderben lévő 40 véletlenszám generátor az adott használat során használandó nyolc kulcs-üzenet párt választ ki a 12 dekóderben eltárolt 16 kulcs-üzenet pár közül. A kiválasztott nyolc pár 41 jogosultság kezelő üzeneteit átadjuk a 30 programozható csipkártyának, amely azokat hitelesíti és 42 lépésben dekódolja, majd 43 lépésben előállítja a megfelelő eseménykulcsot. Ugyanezt a kulcs előállító műveletet a 12 dekóderben is elvégezzük a 43 lépésben, amelynek során a kulcs-üzenet párok megfelelő kulcsértékeit használjuk fel úgy, hogy ugyanazt az eseménykulcs értéket kapjuk.

A 12 dekóderen belüli eseménykulcs előállítást a 4. ábra segítségével részletesebben is is-

mertetjük.

Egy minden 12 dekóder számára állandó 44 bázis eseménykulcs értéket 45 lépésben a 40 véletlenszám generátor által kiválasztott alkészlet első 46 kulcsával kódolunk. Az ennek során kapott értéket 47 lépésben az alkészlet második 48 kulcsával kódoljuk, és ezt az eljárást mindaddig ismételjük, amíg az utolsó 49 lépésben az alkészlet utolsó 50 kulcsával a kapott értéket úgy kódoljuk, hogy megkapjuk 51 végső eseménykulcs értéket.

A 44 bázis eseménykulcs érték az összes 12 dekóderben és 30 programozható csipkártyában jelen lévő univerzális érték lehet, vagy egy meghatározott 12 dekóder – 30 programozható csipkártya párhoz tartozó érték, vagy akár egy olyan érték lehet, amelyet a 12 dekóder minden egyes bekapcsolását követően hozunk létre a 12 dekóderben, majd adunk át a 30 programozható csipkártyának.

A bemutatott esetben az eseménykulcsot úgy állítjuk elő, hogy a DES algoritmus segítségével, és az alkészlet kiválasztott 46, 48, 50 stb. kulcsaival a 44 bázis eseménykulcs értéket ismétlődően kódoljuk. DES algoritmus esetén az a sorrend, amelyben a 46, 48, 50 stb. kulcsokat alkalmazzuk, lényeges, és figyelembe kell vennünk ahhoz, hogy minden alkalommal elő tudjuk ugyanazt a kulcsot állítani.

Azonban amíg az eseménykulcs önmaga egy olyan számérték, amelyet egy DES kulcsként használunk fel a későbbiekben leírt dekódolási eljárásban, ennek az eseménykulcs értéknek az előállításához alkalmazott lépéseknek nem kell a DES kódolási lépéseknek megfelelniük. Ehelyett a 40 véletlenszám generátor által kiválasztott kulcs alkészletet bármilyen módon összekombinálhatjuk, hogy egy használható és alkalmas 51 végső eseménykulcs értéket kapjunk. Például a 46, 48, 50 kulcsokat egyszerű számtani műveletek sorozataként is előállíthatjuk. A mindenkori választott módszertől függően arra sincs feltétlenül szükség, hogy az eseménykulcs előállításánál alkalmazott lépések sorrendjét figyelembe vegyük annak érdekében, hogy ugyanazt a kulcsot elő tudjuk állítani.

Nézzük az 5. ábrát, az azon feltüntetett információ elősegíti annak a megértését, hogy a 30 programozható csipkártya által használt eseménykulcs előállításához milyen 42 és 43 lépéseket kell megvalósítanunk.

Ha a 30 programozható csipkártyát behelyezzük a 12 dekóderbe, akkor az utóbbi a kiválasztott kulcsértékekkel egyező jogosultság kezelő üzenet alkészletet ad át a 30 programozható csipkártyának. Az egyes jogosultság kezelő üzenetek hitelesítését a hozzá tartozó

aláírás érték segítségével végezzük, például a fent már említett MD5/RSA típusú eljárás segítségével. Az egyszerűség kedvéért ezt a lépést az 5. ábráról elhagytuk.

Az első 60 jogosultság kezelő üzenetet 61 lépésben dekódoljuk, amihez a 30 programozható csipkártyán biztonságos és ki nem olvasható módon tárolt 59 szállítási kulcsot használunk. Mint korábban említettük, a 60 jogosultság kezelő üzenet 61 lépésében használt algoritmus biztonsági okokból egy olyan megfelelő biztonsági algoritmus lehet, amelyet kizárólag a 12 dekóderben, és a 30 programozható csipkártya személyre szabása során használt kulcs-üzenet pár előállításáért felelős rendszergazda ismer.

Az 59 szállítási kulcs a rendszerben használt összes 30 programozható csipkártya számára azonos kulcsérték, vagy minden egyes 30 programozható csipkártya számára egy-egy más kulcsérték lehet. Egy egyedi 59 szállítási kulcsérték használatához az szükséges, hogy 12 dekóderben tárolt kulcs-üzenet táblázatot ugyanazzal a kulccsal hozzuk létre, mint amelyet a 30 programozható csipkártyában alkalmaztunk úgy, hogy a 12 dekóder és a 30 programozható csipkártya megváltoztathatatlan és visszafordíthatatlan módon egymáshoz tartozzon. A gyakorlatban azonban ez a variáció nem előnyös.

Az 59 szállítási kulcs felhasználásával 62 lépésben hasonló műveletet hajtunk végre a következő 63 jogosultság kezelő üzenet vonatkozásában, és ezt folytatjuk mindaddig, amíg el nem jutunk az utolsó 64 lépésig, amelyben az 59 szállítási kulcs segítségével az utolsó 65 jogosultság kezelő üzenetet dekódoljuk.

A bemutatott kiviteli alak esetében az egyes 60, 63, 65 jogosultság kezelő üzenetek kódolása olyan 46, 48, 50 kulcsokat eredményez, amelyek azonosak a 12 dekóderben jelen lévő kulcs-üzenet táblázatban társított 46, 48, 50 kulcsokkal, és amelyeket a korábban leírt módon az eseménykulcs előállításához használtunk. Ezért az említett 46, 48, 50 kulcsokat azonos hivatkozási jellel jelöltük, mint ahogy egy-egy ezek szerint egymással megegyező 43 lépést tüntettünk fel a 3. ábrán mind a 30 programozható csipkártyánál, mind a 12 dekódernél.

A 44 bázis esemény kulcsot ezt követően 45 lépésben az első 46 kulccsal kódoljuk, ennek eredményét 47 lépésben a második 48 kulccsal újra kódoljuk, és így tovább, egészen addig, amíg az utolsó 49 lépésben az utolsó 50 kulccsal létre nem hozzuk az 51 végső eseménykulcsot.

Mind a 12 dekóder, mind a 30 programozható csipkártya immár rendelkezik ugyanazzal az

eseménykulccsal, amelyet ezt követően a két eszköz közötti bármilyen irányú adatforgalom során mind kódolásra, mind dekódolásra használhatunk.

Ha visszanézünk a 3. ábrára, látható, hogy a 30 programozható csipkártya az MPEG audiovizuális vagy egyéb adatok társított szegmensének bitsor dekódolásához szükséges ellenőrző szót tartalmazó kódolt jogosultság vezérlő üzenetet kap.

A 30 programozható csipkártya ezt a 70 jogosultság vezérlő üzenetet 71 lépésben dekódolja, hogy a művelet eredményeképpen megkapja azt az ellenőrző szó értéket, amelyet aztán 72 lépésben használunk fel.

Mellesleg megjegyezzük, hogy a 70 jogosultság vezérlő üzenetek kódolásához használt algoritmus előnyösen megegyezhet azzal a biztonságos algoritmussal, amelyet a 30 programozható csipkártyától a fent leírtak szerint kapott jogosultság kezelő üzenetek dekódolásához is használunk.

A dekódolt ellenőrző szót ezt követően 72 lépésben az eseménykulcs segítségével újra kódoljuk, és az újrakódolt ellenőrző szó értéket a 3. ábrán látható módon továbbítjuk a 30 programozható csipkártya és a 12 dekóder közötti interfészen. Ezt a kódolt ellenőrző szó értéket a 12 dekóderben aztán 73 lépésben dekódoljuk, amihez a 12 dekóderben tárolt eseménykulcs értéket használjuk fel, és ennek eredményeképpen megkapjuk a kódolatlan 74 ellenőrző szó értéket.

Mivel az eseménykulcs szimmetrikus, hasonlóan felhasználhatjuk a 12 dekódertől a 30 programozható csipkártya felé küldött adatok kódolásánál is. Ezen túlmenően a 30 programozható csipkártyától a 12 dekóderhez küldött adatok a sima ellenőrző szó adatokon túl egyéb adatok is lehetnek.

Min már jeleztük, a bemutatott elvet használhatjuk egy olyan 12 dekódert tartalmazó rendszer összes interfésze vonatkozásában, ahol egy kivehető feltételes hozzáférési modul található (12 dekóder-feltételes hozzáférési modul interfész, feltételes hozzáférési modul-30 programozható csipkártya interfész stb.). Hasonlóképpen az itt bemutatott elveket alkalmazhatjuk az egyéb eszközbe, például egy 13 televízió készülékbe vagy videómagnetofonba helyezett hordozható modulra (akár feltételes hozzáférési modul, akár programozható csipkártya) is.

Gyakorlatilag egy kódolt kommunikációs csatorna létrehozására szolgáló eljárást bármilyen eszközpár esetén használhatunk, ahol biztonságos adatkommunikációra van szükség.

Különösen előnyös a bemutatott megoldás alkalmazása egy olyan házi hálózat esetén, ahol több szórakoztató elektronikai és egyéb készülék (ezek között televízió, videó, személyi számítógép, dekóder, stb.) egy kommunikációs útvonalon adatokat, például audióvizuális adatot vagy számítógépes fájlokat továbbít. Ez az útvonal lehet rádiófrekvenciás kapcsolat, infravörös összeköttetés, dedikált busz, a villamos hálózatra ráültetett jeltovábbítás, és így tovább. Például szükség lehet arra, hogy egy ellenőrző szót ilyen más adatokban valamilyen kódolt formában továbbítsunk egy dekóder és egy televízió között, vagy egy mester dekóder és egy szolga dekóder között, ugyanazon a háztartáson belül.

Az olvasó számára nyilvánvalóak és kézzel foghatóak más olyan rendszerek is, ahol szükséges vagy kívánatos lehet biztonságos kommunikációs kapcsolat létrehozása.

Szabadalmi igénypontok

1. Eljárás egy első eszköz és egy második eszköz között továbbított adat kódolására, ***azzal jellemezve,*** hogy az első eszköz memóriájában legalább egy előre kiszámított kulcspárt eltárolunk, ahol a legalább egy kulcspárba egy eseménykulcsot, valamint egy szállítási kulcs felhasználásával előállított szállítási kulcs kódolt verzióját veszünk, majd az eseménykulcs kódolt verzióját a második eszközhöz továbbítjuk, amelyben az eseménykulcs kódolt verzióját annak memóriájában tárolt ekvivalens szállítási kulcs felhasználásával dekódoljuk, úgy, hogy a legalább a második eszköztől az első eszközhöz továbbított adatokat az egyes eszközökben lévő eseménykulccsal tudjuk kódolni és dekódolni.

2. Az 1. igénypont szerinti eljárás, ***azzal jellemezve,*** hogy az első eszköz memóriájában több kulcspárt tárolunk és az első eszközzel legalább egy eseménykulcsot kiválasztunk és feldolgozunk, hogy egy meghatározott eseménykulcsot állítsunk elő, és a legalább egy eseménykulcs kódolt, hozzátartozó változatát a második eszközhöz továbbítjuk, hogy azzal dekódoljuk és feldolgozzuk, hogy előállítsuk a meghatározott eseménykulcsot.

3. A 2. igénypont szerinti eljárás, ***azzal jellemezve,*** hogy több eltárolt eseménykulcsból álló alkészletet választunk ki az első eszközzel a meghatározott eseménykulcs létrehozására, és az eseménykulcs alkészlet hozzátartozó kódolt változatait továbbítjuk a második eszközhöz dekódolás és feldolgozás céljára.

4. A 2. vagy 3. igénypont szerinti eljárás, ***azzal jellemezve,*** hogy a meghatározott eseménykulcs előállításához használt eseménykulcsok kombinációjának a sorrendjét az első

eszköztől a második eszközhöz továbbítjuk.

5. A 4. igénypont szerinti eljárás, ***azzal jellemezve,*** hogy az első eszköz számára és a második eszköz számára egyaránt ismert bázis eseménykulcs értéket (44) ismétlődően kódolunk mindkét eszközben, meghatározott sorrendű eseménykulcsokkal, a kódolás sorrendjére érzékeny kódoló algoritmus alkalmazásával.

6. Az 1-5. igénypontok bármelyike szerinti eljárás, ***azzal jellemezve,*** hogy a legalább egy előre kiszámított kulcspárt még az első eszközben történő eltárolását megelőzően egy nagyobb előre számított kulcspár készletből választjuk ki.

7. Az 1-6. igénypontok bármelyike szerinti eljárás, ***azzal jellemezve,*** hogy a második eszközhöz továbbított eseménykulcs kódolt változata a második eszközzel olvasható aláírás értéket is tartalmaz, hogy az eseménykulcs kódolt változatának hitelességét ellenőrizhessük.

8. Az 1-7. igénypontok bármelyike szerinti eljárás, ***azzal jellemezve,*** hogy egy esménykulcs kódolásához és dekódolásához használt algoritmusként és szállítási kulcsként egy szimmetrikus algoritmust és ahhoz tartozó szimmetrikus kulcsot használunk.

9. Az 1-8. igénypontok bármelyike szerinti eljárás, ***azzal jellemezve,*** hogy az első eszköz és a második eszköz között továbbított adat kódolásához és dekódolásához az eseménykulccsal használt kódoló algoritmusként szimmetrikus algoritmust használunk.

10. Az 1-9. igénypontok bármelyike szerinti eljárás, ***azzal jellemezve,*** hogy első eszközként dekódert (12) használunk.

11. Az 1-10. igénypontok bármelyike szerinti eljárás, ***azzal jellemezve,*** hogy második eszközként hordozható biztonsági modult használunk.

12. A 11. igénypont szerinti eljárás, ***azzal jellemezve***, hogy hordozható biztonsági modulként programozható csipkártya (30) és feltételes hozzáférési modul egyikét alkalmazzuk.

13. Az 1-9. igénypontok bármelyike szerinti eljárás, ***azzal jellemezve***, hogy első eszközként egy feltételes hozzáférési modult, második eszközként pedig egy programozható csipkártyát (30) használunk.

14. A 10-13. igénypontok bármelyike szerinti eljárás, ***azzal jellemezve***, hogy az egy eseménykulccsal kódolt és dekódolt adataként ellenőrző szó adatot továbbítunk.

15. A 10-13. igénypontok bármelyike szerinti eljárás, ***azzal jellemezve***, hogy egy ese-

ménykulccsal kódolt és dekódolt adatként bitsordekódolt sugárzott adatot továbbítunk.

16. Az 1-9. igénypontok bármelyike szerinti eljárás, ***azzal jellemezve***, hogy első eszközként és második eszközként egy első dekódert (12) és egy második dekódert (12) használunk.

17. Az 1-9. igénypontok bármelyike szerinti eljárás, ***azzal jellemezve***, hogy házi hálózatban első eszközként és második eszközként egy kommunikációs útvonalon adatok továbbítására alkalmas első és második szórakoztató elektronikai készüléket használunk.

18. Eszköz az 1-17. igénypontok bármelyike szerinti eljárásban történő használatra, ***azzal jellemezve***, hogy első eszközként legalább egy előre kiszámolt kulcspárt tároló memóriával rendelkezik, ahol a legalább egy előre számított kulcspár egy eseménykulcs, valamint az eseménykulcs kódolt változata.

19. Eszköz az 1-17. igénypontok bármelyike szerinti eljárásban történő használatra, ***azzal jellemezve***, hogy második eszközként az első eszköz memóriájában tárolt kódolt eseménykulcs érték dekódolásához szükséges kulcsot és algoritmust tároló memóriával van ellátva.

20. A 18. vagy 19. igénypont szerinti eszköz, ***azzal jellemezve***, hogy az első eszköz egy dekóder (12), a második eszköz pedig hordozható biztonsági modul.

21. Rendszer egy első eszköz és egy második eszköz közötti biztonságos adattovábbításra, ***azzal jellemezve***, hogy az első eszköz memóriájában legalább egy, egy eseménykulcsot, valamint egy szállítási kulcs felhasználásával előállított szállítási kulcs kódolt verzióját tartalmazó előre kiszámított kulcspárt eltároló, az eseménykulcs kódolt verzióját a második eszközhöz továbbító, és az eseménykulcs kódolt verzióját annak memóriájában tárolt ekvivalens szállítási kulcs felhasználásával, a legalább a második eszköztől az első eszközhöz továbbított adatokat az egyes eszközökben lévő eseménykulccsal kódoló és dekódoló eszközzel rendelkezik.

22. A 21. igénypont szerinti rendszer, ***azzal jellemezve,*** hogy az első eszköz memóriájában több kulcspárt tároló, az első eszközzel legalább egy eseménykulcsot kiválasztó és egy meghatározott eseménykulcs előállításához feldolgozó, és a legalább egy eseménykulcs kódolt, hozzátartozó változatát a meghatározott eseménykulcs előállításához dekódolás és feldolgozás céljából a második eszközhöz továbbító eszközzel rendelkezik.

23. A 21. vagy 22. igénypont szerinti rendszer, ***azzal jellemezve***, hogy a második eszköz-

höz továbbított eseménykulcs kódolt változata annak hitelességnek az ellenőrzéséhez egy, a második eszközzel olvasható aláírás értéket is tartalmaz.

24. A 21-23. igénypontok bármelyike szerinti rendszer, ***azzal jellemezve***, hogy egy eseménykulcs kódolásához és dekódolásához használt algoritmusként és szállítási kulcsként egy szimmetrikus algoritmust és ahhoz tartozó szimmetrikus kulcsot foglal magában.

25. A 21-24. igénypontok bármelyike szerinti rendszer, ***azzal jellemezve***, hogy az első eszköz és a második eszköz között továbbított adat kódolásához és dekódolásához az eseménykulccsal használt kódoló algoritmusként szimmetrikus algoritmust foglal magában.

26. A 21-25. igénypontok bármelyike szerinti rendszer, ***azzal jellemezve,*** hogy első eszközként dekódert (12) tartalmaz.

27. A 21-26. igénypontok bármelyike szerinti rendszer, ***azzal jellemezve,*** hogy második eszközként hordozható biztonsági modult tartalmaz.

28. A 27. igénypont szerinti rendszer, ***azzal jellemezve***, hogy hordozható biztonsági modulként programozható csipkártya (30) és feltételes hozzáférési modul egyikét tartalmazza.

29. A 21-25. igénypontok bármelyike szerinti rendszer, ***azzal jellemezve***, hogy első eszközként egy feltételes hozzáférési modult, második eszközként pedig egy programozható csipkártyát (30) foglal magában.

30. A 21-25. igénypontok bármelyike szerinti rendszer, ***azzal jellemezve***, hogy első eszközként és második eszközként egy első dekódert (12) és egy második dekódert (12) foglal magában.

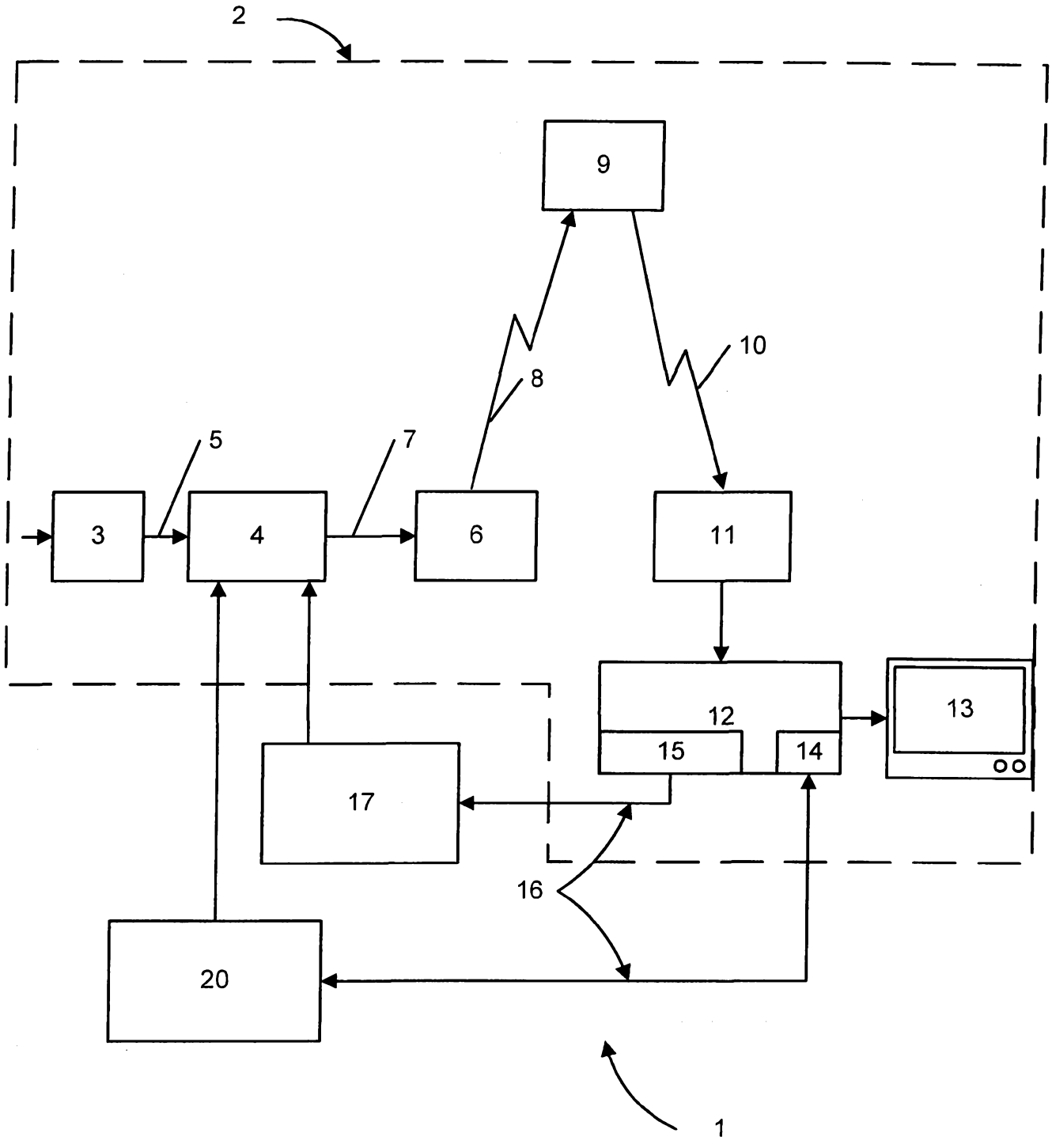
31. A 21-25. igénypontok bármelyike szerinti rendszer, ***azzal jellemezve***, hogy házi hálózatban első eszközként és második eszközként egy kommunikációs útvonalon adatok továbbítására alkalmas első és második szórakoztató elektronikai készüléket foglal magában.

A meghatalmazott:

DANUBIA

Szabadalmi és Védjegy Iroda Kft.

Dr. Antalffy-Zsíros András



1. ÁBRA