72.179/mk

Kivonat

Eljárás és berendezés információ rögzítésére és lejátszására

A találmány szerinti eljárás során

Egy fa-struktúrájú kulcs kiosztási rendszerben mester kulcs és közeg kulcs megújított adatait küldjük el egy kulcs megújítási blokkal (KRB - key renewal block) együtt. A KRB olyan, hogy egy fa struktúra által, annak leveleiként tartalmazott eszközök mindegyike rendelkezik egy levél kulccsal és korlátozással rendelkező csomópont kulccsal. Egy meghatározott KRB-t generálhatunk egy meghatározott csomópont által azonosított csoport számára, és kioszthatjuk a csoportnak egy olyan eszköz korlátozására, amely számára a kulcsot megújíthatjuk. A csoporthoz nem tartozó egyetlen eszköz sem tudja dekódolni a kulcsot, ami által a kulcs kiosztás biztonságosságát biztosíthatjuk. Speciálisan egy olyan rendszerben, amely generálásirányított mester kulcsot használ, egy KRB-vel megújított mester kulcsot oszthatunk ki ~~1. ábrán~~.

A találmány részét képezi továbbá az eljárást megvalósító berendezés.

(—)

Telefon: 34-24-920. Telex: 34-24-323

72.179/MK

Eljárás és berendezés információ rögzítésére és lejátszására

A jelen találmány általánosságban információ rögzítővel, információ lejátszóval, információ rögzítési eljárással, információ lejátszási eljárással, információ hordozóeszközzel és program szolgáltató közeggel kapcsolatos. Szűkebb értelemben pedig olyan információ rögzítővel, információ lejátszóval, információ rögzítési eljárással, információ lejátszási eljárással, információ hordozóeszközzel és program szolgáltató közeggel kapcsolatos, amelyben fa-struktúrájú hierarchikus kulcs kiosztási eljárást használunk valamely üzenet méretének csökkentésére, ami által minimalizáljuk az adat kiosztás terhét akkor, amikor egy kulcsot, például egy mester kulcsot, közeg kulcsot vagy hasonlót megújítunk. Még szűkebb értelemben a jelen találmány olyan információ rögzítővel, információ lejátszóval, információ rögzítési eljárással, információ lejátszási eljárással, információ hordozóeszközzel és program szolgáltató közeggel kapcsolatos, amelyben olyan kulcs kiosztási eljárást használunk egy szükséges kulcs, például egy mester kulcs vagy közeg kulcs kiosztására tartalom adatnak a hordozóeszközön vagy kommunikációs vonalon keresztül a hordozóeszközre való rögzítéséhez vagy az onnan való lejátszásához, amelyben n számú rögzítő/lejátszó mindegyikét egy fa egyes levelein rendezzük el, és minden egyes rögzítő/lejátszó az így kiosztott mester kulcsot vagy közeg kulcsot használja a tartalom adat rög-

zítésére vagy lejátszására.

A digitális jel feldolgozási technológia javulása és fejlődése következtében a digitális rögzítők és hordozóeszközök uralkodnak. Egy ilyen digitális rögzítővel és hordozóeszközzel például egy kép vagy egy hang ismételten rögzíthető és lejátszható a minőségének bárminemű romlása nélkül. Mivel a digitális adat több alkalommal is ismételten másolható a kép és hang minőség romlása nélkül, az olyan hordozóeszközök, amelyekre a digitális adat illegálisan van rögzítve, a piacra kerülésükkel változatos tartalmak, például zene, mozgókép stb. szerzői jogának tulajdonosai (copyrighters) vagy a tartalmak legális terjesztői elesnek olyan haszontól, amely befolyna hozzájuk, ha az ilyen illegális másolás nem lenne lehetséges. A digitális adatok ilyen illegális másolásának megakadályozására változatos illegális másolás-megakadályozó rendszereket (illegal copy-preventing systems) vezettek be a digitális rögzítőkben és hordozóeszközökön.

Példaként a fenti illegális másolás-megakadályozó rendszerekre, az MD (mini disc, mini lemez) meghajtóban (az MD védjegy) SCMS-t (Serial Copy Management System, sorozatos másolás kezelési rendszer) alkalmazunk. Az SCMS olyan, hogy az adat lejátszó oldalon az audió adatot egy SCMS jellel együtt teszzük kimenetre egy digitális interfésztől (DIF - digital interface), míg az adat rögzítő oldalon az adat lejátszó oldaltól származó audió adat rögzítését az adat lejátszó oldalról származó SCMS jel alapján vezérlik, ezáltal megakadályozva az audió adat illegális másolását.

Még szűkebb értelemben a fenti SCMS jel azt jelenti, hogy egy audió adat „szabadon másolható” („copy-free”) adat, amely

több alkalommal is szabadon másolható, „egyszer másolható” („copy-once-allowed”) adat, amely másolása csak egy alkalommal engedélyezett, vagy „nem másolható” („copy-prohibited”) adat, amely másolása tilos. Az adat rögzítő oldalon egy a DIF-től származó audió adat fogadásakor az audió adattal együtt átvitt SCMS jelet észlelünk. Ha az SCMS jel azt jelenti, hogy az audió adat egy „szabadon másolható” adat, akkor az audió adatot az SCMS jellel együtt rögzítjük a mini lemezre. Ha az SCMS jel azt jelenti, hogy az audió adat egy „egyszer másolható” adat, akkor az audió adatot „nem másolható” adattá alakítjuk át, és az SCMS jelet rögzítjük az audió adattal együtt a mini lemezre. Végül, ha az SCMS jel azt jelzi, hogy az audió adat egy „nem másolható” adat, akkor az audió adatot nem rögzítjük a mini lemezre. Az SCMS jellel való vezérlés alatt megakadályozzuk a szerzői jog által védett (copyrighted) audió adat illegális másolását a mini lemez meghajtó egységben.

Az SMSC viszont csak akkor érvényes, amikor maga az adat rögzítő úgy van konstruálva, hogy az adat lejátszó oldalról származó audió adat rögzítését az SCMS jel alapján vezérli. Ezért meglehetősen nehéz az SCMS számára egy olyan mini lemez meghajtó támogatása, amelyet nem úgy konstruáltak, hogy SCMS vezérlést végezzen. Az SCMS alkalmazásához egy DVD lejátszó például egy tartalom-összekeverő (content scrambling) rendszert alkalmaz a szerzői jog által védett adatok illegális másolásának megelőzésére.

A tartalom-összezavaró rendszer olyan, hogy kódolt videó adatot, audió adatot és ehhez hasonlókat rögzítünk egy DVD-ROM-on (ROM - read-only memory, csak olvasható memória), és a kódolt adat dekódolásához használandó dekódolási kulcsot adnak

ki minden egyes engedéllyel rendelkező DVD lejátszóhoz. Az engedélyt olyan DVD lejátszóknak adják ki, amelyeket valamely előre meghatározott működési szabállyal összhangban lévő módon terveztek meg, például illegális másolás ellen stb. Ezért a kiadott dekódolási kulcs használatával egy engedéllyel rendelkező DVD lejátszó dekódolni tudja a DVD-ROM-ban rögzített kódolt adatot, ezáltal lejátszhatja a videó és audïó adatokat a DVD-ROM-ról.

Másrészről, egy engedéllyel nem rendelkező DVD lejátszó nem tud dekódolni egy DVD-ROM-ban rögzített kódolt adatot, mert nincsen dekódolási kulcsa a kódolt adathoz. Röviden, a tartalom-összekeverő rendszer megakadályozza az engedélyezési feltételeket nem teljesítő DVD lejátszókat abban, hogy rögzített digitális adatokkal rendelkező DVD-ROM-okat játsszanak le, az illegális másolás megakadályozása érdekében.

A DVD-ROM-ban alkalmazott tartalom-összezavaró rendszert viszont egy hordozóeszközre irányítjuk, ahova a felhasználó nem írhat adatot (a továbbiakban erre „ROM közegként" fogunk hivatkozni az alkalmas helyeken), viszont nem irányítjuk olyan hordozóeszközre, ahova a felhasználó adatot írhat (a továbbiakban erre „RAM közegként" fogunk hivatkozni az alkalmas helyeken).

Más szóval, egy ROM közegben rögzített teljes kódolt adat átmásolása egy RAM közegre az adatnak egy úgynevezett kalóz kiadását (pirated edition) hozza létre, amely lejátszható egy engedéllyel rendelkező DVD lejátszó által.

A fenti probléma megoldására a jelen találmány bejelentője előterjesztett egy eljárást (amint azt a JP 224461 sz. közzétételi irat (1999) (JP 25310 sz. szabadalmi leírás (1998)

leírja), amelyben minden egyes hordozóeszközt azonosító információt (erre a továbbiakban „közeg ID információként" (medium ID) hivatkozunk) más adatokkal együtt rögzítünk egy hordozóeszközön, így a hordozóeszközön lévő közeg ID információhoz csak akkor engedélyezünk hozzáférést, ha a hordozóeszközt lejátszani szándékozó lejátszó engedéllyel rendelkezik a közeg ID információhoz.

A fenti eljárás a hordozóeszközön az adatokat egy privát kulccsal (mester kulccsal) kódolja, amihez a közeg ID információ engedélyezésén keresztül juthat hozzá, ily módon bármely, engedéllyel nem rendelkező lejátszó nem képes jelentéssel bíró adatot megszerezni még akkor sem, ha képes a kódolt adat olvasására. Megjegyezzük, hogy egy a közeg ID információhoz engedéllyel rendelkező lejátszó működése korlátozva van illegális másolás ellen.

Egy engedéllyel nem rendelkező lejátszó nem férhet hozzá a közeg ID (ID - identification, azonosító) információhoz. A közeg ID információ egyedi minden egyes hordozóeszköz számára. Még ha egy engedéllyel nem rendelkező lejátszó át is tudná másolni egy ilyen hordozóeszközön rögzített összes kódolt adatot egy új hordozóeszközre, az új hordozóeszközön ily módon rögzített adatot akkor sem tudná az engedéllyel nem rendelkező lejátszó helyesen dekódolni, úgy, mint egy engedéllyel rendelkező lejátszó. Ily módon lényegében lehetséges az adatok illegális másolásának megakadályozása.

Itt meg kell jegyeznünk azt, hogy a fenti hagyományos rendszerben egy engedéllyel rendelkező eszközben tárolt valamely mester kulcs általában közös az ugyanabban a rendszer által tartalmazott összes eszköz számára. Egy rendszerben lévő

eszközök valamely sokasága számára közös mester kulcsot azért tároljuk, hogy megengedjük az eszközök egyikének a rendszerben lévő bármely másik eszköz által rögzített adattal rendelkező hordozóeszköz lejátszását (az eszközök közötti együttműködés biztosításához).

Viszont ha egy támadó sikeres támadást hajt végre a rendszerben lévő valamely eszköz ellen és kibontja (extracts) a mester kulcsot, akkor a rögzített kódolt adat a teljes rendszerben dekódolható, és a teljes rendszer összeomlik. A fentiek elkerülése végett, ha kiderül, hogy az eszköz valamely támadása felfedte a mester kulcsot, akkor a mester kulcsot meg kell újítanunk egy új kulcsra, és az új mester kulcsot ki kell adnunk a rendszer által tartalmazott összes eszköznek, kivéve a megtámadottat. Ezt az intézkedést a legegyszerűbben úgy valósíthatjuk meg, hogy az eszközök mindegyikének egy egyedi kulcsot (eszköz kulcsot) adunk, az új mester kulcsot kódoljuk az egyes eszköz kulcsokkal egy megfelelő érték biztosításához, és továbbítjuk az értékeket az egyes eszközöknek egy hordozóeszközön keresztül. Ez viszont hozzáadódik a továbbítandó üzenet méretéhez, a cél eszközök számával arányos mértékben.

Ennek megfelelően a jelen találmány egyik célja, hogy kiküszöbölje az eddig használatos megközelítés fent említett hátrányosságait egy olyan rendszer biztosítása által, amelyben a fa-struktúrájú kulcs kiosztási eljárást használjuk egy üzenet méretének a csökkentésére, ezáltal minimalizálva egy új vagy megújított kulcs, például egy mester kulcs, közeg kulcs vagy hasonlók kiosztásának terhét. Vagyis a jelen találmány tárgya olyan információ rögzítő, információ lejátszó, információ rögzítési eljárás, információ lejátszási eljárás, informá-

ció hordozóeszköz és program szolgáltató közeg biztosítása, amelyben olyan kulcs kiosztási eljárást használunk egy szükséges kulcs, például egy mester kulcs vagy közeg kulcs kiosztására adat tartalomnak hordozóeszközön vagy kommunikációs vonalon keresztül a hordozóeszközre való rögzítésére vagy az onnan való lejátszására, amelyben valamely n számú rögzítő/lejátszó mindegyikét egy fa leveleinek valamelyikén rendezzük el és minden egyes rögzítő/lejátszó az így kiosztott mester kulcsot vagy közeg kulcsot használja a tartalom adat rögzítésére vagy lejátszására.

A jelen találmány első aspektusa szerint biztosíthatunk egy információ rögzítő berendezést információnak egy hordozóeszközre való rögzítésére, amely berendezés magában foglal kriptográfiai (titkosítási) eszközt, amely rendelkezik egy olyan hierarchikus fa struktúra által tartalmazott csomópontok mindegyike számára egyedi csomópont kulccsal, amely magában foglalja különböző információ rögzítők valamely sokaságát a fa struktúra egyes leveleiként, valamint rendelkezik levél kulccsal, ami egyedi az információ rögzítők mindegyike számára, továbbá kódolja a hordozóeszközön eltárolandó adatot; a kriptográfiai eszköz az információ rögzítőbe beépített kódolási kulcs generáló adat alapján kódolási kulcsot generál a hordozóeszközön eltárolandó adat kódolására; és a kódolási kulcs generáló adat olyan adat, amelyet megújíthatunk a csomópont kulcs vagy a levél kulcs legalább egyikével.

A fenti információ rögzítőben a jelen találmány szerint a kódolási kulcs generáló adat egy mester kulcs, amely közös az információ rögzítők sokasága számára.

A jelen találmány szerint továbbá a fenti információ rögzítőben a kódolási kulcs generáló adat egy közeg kulcs, amely egyedi egy meghatározott hordozóeszköz számára.

A jelen találmány szerint ezen kívül a fenti információ rögzítőben a csomópont kulcsot megújíthatjuk, és amikor egy csomópont kulcsot megújítunk, kiosztunk egy olyan levélnél lévő információ rögzítő számára, ahol a kódolási kulcs generáló adatot meg kell újítanunk egy kulcs megújítási blokkot (KRB - key renewal block), amelyet a megújítási csomópont kulcsnak a fa struktúra valamely alacsonyabb szintjén lévő csomópont kulcs vagy levél kulcs legalább egyikével való kódolásából származtatunk, és a kriptográfiai eszköz az információ rögzítőben fogad egy megújítási adatot a megújított csomópont kulccsal kódolt kódolási kulcs generáló adathoz, kódolja a kulcs megújítási blokkot a megújított csomópont kulcs megszerzéséhez, és kiszámít egy megújítási adatot a kódolási kulcs generáló adat számára az így megszerzett megújított csomópont kulcs alapján.

A jelen találmány szerint továbbá a fenti információ rögzítőben a kulcs megújítási blokkot egy hordozóeszközön tároljuk, és a kriptográfiai eszköz a hordozóeszközről olvasott kulcs megújítási blokkot kódolja.

A jelen találmány szerint ezen kívül a fenti információ rögzítőben a kódolási kulcs generáló adat rendelkezik egy generálási számmal vele korrelációban lévő megújítási információként, és a kriptográfiai eszköz eltárolja a rögzítő tagba rögzítési generálási számként annak a kódolási kulcs generáló adatnak egy generálási számát, amelyet egy kódolt adatnak a hordozóeszközön való eltárolásakor használtunk.

A jelen találmány szerint továbbá a fenti információ rögzítőben a következő kódoló eljárásokat szelektív módon hajtjuk végre attól függően, hogy egy lejátszó korlátozás (player restriction) be van-e állítva vagy sem: amikor a lejátszó korlátozás nincs beállítva, első kódolási kulcsot generálunk a hordozóeszközön eltárolandó adat számára első kódolási kulcs generáló adat alapján a hordozóeszközön eltárolandó adatnak az első kódolási kulccsal való kódolására, és az első kódolási kulcs generáló adatot eltároljuk a hordozóeszközön; vagy amikor a lejátszó korlátozás be van állítva, második kódolási kulcsot generálunk a hordozóeszközön eltárolandó adat számára az információ rögzítőbe beépített második kódolási kulcs generáló adat alapján a hordozóeszközön eltárolandó adatnak a második kódolási kulccsal való kódolására.

A jelen találmány szerint továbbá fenti információ rögzítőben, amikor a lejátszó korlátozás nincs beállítva, a kriptográfiai eszköz egy cím-egyértelmű kulcsot generál az információ rögzítőben tárolt olyan mester kulcsból, amely generálását irányítjuk, egy lemez ID-ből (disc ID), ami egy egyedi azonosító egy hordozóeszköz számára, egy cím kulcsból, ami egyedi a hordozóeszközre rögzítendő adat számára és eszköz ID-ből (device ID), ami egy azonosító az információ rögzítő számára, majd generálja az első kódolási kulcsot a cím-egyértelmű kulcsból, vagy amikor a lejátszó korlátozás be van állítva, a kriptográfiai eszköz egy cím-egyértelmű kulcsot generál az információ rögzítőben tárolt generálás-irányított (generation-managed) mester kulcsból, lemez ID-ből, ami egy egyedi azonosító a hordozóeszköz számára, cím kulcsból, ami egyedi a hordozóeszközre rögzítendő adat számára, és az eszköz-egyértelmű

kulcsból, ami egyedi az információ rögzítő számára, majd generálja a második kódolási kulcsot a cím-egyértelmű kulcsból.

A jelen találmány szerint a fenti információ rögzítő magában foglal továbbá szállítási folyam feldolgozó eszközt érkezési időbélyegnek (ATS - arrival time stamp) egy szállítási folyam által tartalmazott diszkrét szállítási csomagok mindegyikéhez való hozzáfűzéséhez, a kriptográfiai eszköz egy blokk kulcsot generál kódolási kulcsként egynél több olyan csomagot magában foglaló blokk adat számára, amelyek mindegyikéhez hozzáfűztük az érkezési időbélyeget, és a blokk kulcsot kódolási kulcsként generáljuk a hordozóeszközön eltárolandó adat kódolásakor olyan adat alapján, amely magában foglalja a kódolási kulcs generáló adatot és egy blokk magot, ami további egyedi információ az érkezési időbélyeget magában foglaló blokk adat számára.

A jelen találmány szerint továbbá a fenti információ rögzítőben a kriptográfiai eszköz a hordozóeszközön eltárolandó adatot DES algoritmus szerint kódolja.

A jelen találmány szerint a fenti információ rögzítőben biztosítunk továbbá egy interfész eszközt egy hordozóeszközre rögzítendő információ fogadására és egy adatban lévő szállítási folyam által tartalmazott csomagok mindegyikéhez hozzáfűzött másolás vezérlési információ azonosítására annak eldöntésére a másolás vezérlési információ alapján, hogy a hordozóeszközre való rögzítés lehetséges-e vagy sem.

A jelen találmány szerint a fenti információ rögzítőben biztosítunk ezen kívül egy interfész eszközt egy hordozóeszközre rögzítendő információ fogadására és 2-bites EMI (encryption mode indicator, kódolási mód jelző) másolás vezér-

lési információként való azonosítására annak eldöntésére az EMI alapján, hogy a hordozóeszközre való rögzítés lehetséges-e vagy sem.

A jelen találmány második aspektusa szerint biztosíthatunk egy információ lejátszó berendezést információnak egy hordozóeszközről való lejátszására, amely berendezés magában foglal kriptográfiai eszközt, amely rendelkezik egy olyan hierarchikus fa struktúra által tartalmazott csomópontok mindegyike számára egyedi csomópont kulccsal, amely magában foglalja különböző információ rögzítők valamely sokaságát a fa struktúra egyes leveleiként, valamint rendelkezik levél kulccsal, ami egyedi az információ rögzítők mindegyike számára, továbbá dekódolja a hordozóeszközön tárolt adatot; a kriptográfiai eszköz az információ rögzítőbe beépített dekódolási kulcs generáló adat alapján dekódolási kulcsot generál a hordozóeszközön tárolt adat dekódolására; és a dekódolási kulcs generáló adat olyan adat, amely megújítható a csomópont kulcs vagy a levél kulcs legalább egyikével.

A jelen találmány szerint a fenti információ lejátszóban a dekódolási kulcs generáló adat egy mester kulcs, amely közös az információ rögzítők sokasága számára.

A jelen találmány szerint továbbá a fenti információ lejátszóban a dekódolási kulcs generáló adat egy közeg kulcs, amely egyedi egy meghatározott hordozóeszköz számára.

A jelen találmány szerint ezen kívül a fenti információ lejátszóban a csomópont kulcsot megújíthatjuk, és amikor egy csomópont kulcsot megújítunk, kiosztunk egy olyan levélnél lévő információ lejátszó számára, ahol a kódolási kulcs generáló adatot meg kell újítanunk egy kulcs megújítási blokkot, ame-

lyet a megújítási csomópont kulcsnak a fa struktúra valamely alacsonyabb szintjén lévő csomópont kulcs vagy levél kulcs legalább egyikével való kódolásából származtatunk, és a kriptográfiai eszköz az információ rögzítőben egy megújítási adatot fogad a megújított csomópont kulccsal kódolt dekódolási kulcs generáló adathoz, kódolja a kulcs megújítási blokkot a megújított csomópont kulcs megszerzéséhez, és kiszámít egy megújítási adatot a dekódolási kulcs generáló adat számára az így megszerzett megújított csomópont kulcs alapján.

A jelen találmány szerint továbbá a fenti információ lejátszóban a kulcs megújítási blokkot egy hordozóeszközön tároljuk, és a kriptográfiai eszköz a hordozóeszközről olvasott kulcs megújítási blokkot kódolja.

A jelen találmány szerint ezen kívül a fenti információ lejátszóban a dekódolási kulcs generáló adat rendelkezik egy generálási számmal vele korrelációban lévő megújítási információként, és a kriptográfiai eszköz a hordozóeszközről beolvasott kódolt adat dekódolásakor a hordozóeszközről beolvassa a kódolt adat kódolásakor használt kódolási kulcs generáló adat egy generálási számát, és az így beolvasott generálási számnak megfelelő dekódolási kulcs generáló adatból dekódolási kulcsot.

A jelen találmány szerint továbbá a fenti információ lejátszóban a következő dekódoló eljárásokat szelektív módon hajtjuk végre attól függően, hogy be van-e állítva egy lejátszó korlátozás vagy sem: amikor a lejátszó korlátozás nincs beállítva, első dekódolási kulcsot generálunk a hordozóeszközön tárolt kódolt adat számára a hordozóeszközön tárolt valamely első dekódolási kulcs generáló adat alapján, a kódolt

adatot az első dekódolási kulccsal dekódoljuk; vagy amikor a lejátszó korlátozás be van állítva, második dekódolási kulcsot generálunk a hordozóeszközön tárolt kódolt adat számára az információ rögzítőbe beépített második kódolási kulcs generáló adat alapján, és a kódolt adatot a második dekódolási kulccsal dekódoljuk.

A jelen találmány szerint továbbá fenti információ lejátszóban, amikor a lejátszó korlátozás nincs beállítva, a kriptográfiai eszköz megszerez egy az információ rögzítőben tárolt generálás-irányított mester kulcsot és megszerez egy hordozóeszköztől egy lemez ID-t, ami egy egyedi azonosító egy hordozóeszköz számára, egy cím kulcsot, ami egyedi a dekódolandó adat számára és eszköz ID-t, ami egy azonosító azon információ rögzítő számára, amely a kódolt adatot rögzítette, és egy cím-egyértelmű kulcsot generál a mester kulcsból, lemez ID-ből, cím kulcsból, és eszköz kulcsból, és az első dekódolási kulcsot generálja a cím-egyértelmű kulcsból, vagy amikor a lejátszó korlátozás be van állítva, a kriptográfiai eszköz megszerez egy az információ rögzítőben tárolt generálás-irányított mester kulcsot, valamint egy eszköz-egyértelmű kulcsot, amely egyedi az információ rögzítő számára és abban is tároljuk, továbbá megszerez valamely hordozóeszköztől egy lemez ID-t, ami egy egyedi azonosító a hordozóeszköz számára és egy cím kulcsot, ami egyedi a dekódolandó adat számára, majd egy cím-egyértelmű kulcsot generál a mester kulcsból, lemez ID-ből, cím kulcsból és eszköz-egyértelmű kulcsból, és a második dekódolási kulcsot a cím-egyértelmű kulcsból generáljuk.

A jelen találmány szerint a fenti információ lejátszó magában foglal továbbá egy szállítási folyam feldolgozó eszközt

az adat kimenetre tételének vezérlésére a kriptográfiai eszköz által dekódolt blokk adat által tartalmazott szállítási csomagok valamely sokaságának mindegyikéhez hozzáfűzött érkezési időbélyeg alapján, a kriptográfiai eszköz generál egy blokk kulcsot dekódolási kulcsként egynél több olyan csomagot magában foglaló blokk adat számára, amelyek mindegyikéhez hozzáfűztük az érkezési időbélyeget, és generáljuk a blokk kulcsot dekódolási kulcsként a hordozóeszközön tárolt kódolt adat dekódolásakor olyan adat alapján, amely magában foglalja a dekódolási kulcs generáló adatot és egy blokk magot, ami további egyedi információ az érkezési időbélyeget magában foglaló blokk adat számára.

A jelen találmány szerint továbbá a fenti információ lejátszóban a kriptográfiai eszköz a hordozóeszközön tárolt kódolt adatot DES algoritmus szerint dekódolja.

A jelen találmány szerint a fenti információ lejátszóban biztosítunk továbbá egy interfész eszközt egy hordozóeszközre rögzítendő információ fogadására és egy adatban lévő szállítási folyam által tartalmazott csomagok mindegyikéhez hozzáfűzött másolás vezérlési információ azonosítására annak eldöntésére a másolás vezérlési információ alapján, hogy a hordozóeszközről való lejátszás lehetséges-e vagy sem.

A jelen találmány szerint a fenti információ lejátszóban biztosítunk továbbá egy interfész eszközt egy hordozóeszközre rögzítendő információ fogadására és 2-bites EMI azonosítására másolás vezérlési információként annak eldöntésére az EMI alapján, hogy a hordozóeszközről való lejátszás lehetséges-e vagy sem.

A jelen találmány harmadik aspektusa szerint biztosíthatunk egy információ rögzítési eljárást információnak egy hordozóeszközre való rögzítésére, amely eljárás magában foglalja a következő lépéseket: megújítunk kódolási kulcs generáló adatot egy kódolási kulcs generálására hordozóeszközön eltárolandó adat kódolásához legalább vagy egy csomópont kulccsal, ami egyedi egy olyan hierarchikus fa-struktúra által tartalmazott csomópontok mindegyike számára, amely különböző információ rögzítők valamely sokaságát foglalja magában a fa struktúra egyes leveleiként, vagy egy levél kulccsal, ami egyedi az információ rögzítők mindegyike számára; valamint egy kódolási kulcsot generálunk a kódolási kulcs generáló adat alapján a hordozóeszközön eltárolandó adat kódolásához.

A jelen találmány szerint a fenti információ rögzítési eljárásban a kódolási kulcs generáló adat egy mester kulcs, ami közös az információ rögzítők sokasága számára.

A jelen találmány szerint továbbá a fenti információ rögzítési eljárásban a kódolási kulcs generáló adat egy közeg kulcs, ami egyedi egy meghatározott hordozóeszköz számára.

A jelen találmány szerint ezen kívül a fenti információ rögzítési eljárásban a csomópont kulcsot megújíthatjuk, és amikor egy csomópont kulcsot megújítunk, kiosztunk egy olyan levélnél lévő információ rögzítő számára, ahol a kódolási kulcs generáló adatot meg kell újítanunk egy kulcs megújítási blokkot, amelyet a megújítási csomópont kulcsnak a fa struktúra valamely alacsonyabb szintjén lévő csomópont kulcs vagy levél kulcs legalább egyikével való kódolásából származtatunk, és a megújítási lépés magában foglalja a következő lépéseket: megszerezzük a megújított csomópont kulcsot a kulcs megújítási

blokk kódolása által; valamint kiszámítunk egy megújítási adatot a kódolási kulcs generáló adat számára az így megkapott megújított csomópont kulcs alapján.

A jelen találmány szerint továbbá a fenti információ rögzítési eljárásban a kódolási kulcs generáló adat rendelkezik egy generálási számmal vele korrelációban lévő megújítási információként, és a kriptográfiai lépés magában foglalja továbbá azt a lépést, hogy amikor kódolt adatot tárolunk el a hordozóeszközön, eltároljuk a használt kódolási kulcs generáló adat valamely generálási számát a hordozóeszközön egy rögzítési generálási számként.

A jelen találmány szerint továbbá a fenti információ rögzítési eljárásban a kriptográfiai lépés magában foglalja a következő két eljárást, amelyek egyikét szelektív módon hajtjuk végre attól függően, hogy egy lejátszó korlátozás be van-e állítva vagy sem: amikor a lejátszó korlátozás nincs beállítva, egy első kódolási kulcsot generálunk a hordozóeszközön eltárolandó adat számára egy első kódolási kulcs generáló adat alapján, a hordozóeszközön eltárolandó adatot az első kódolási kulccsal kódoljuk, és az első kódolási kulcs generáló adatot eltároljuk a hordozóeszközön; és amikor a lejátszó korlátozás be van állítva, egy második kódolási kulcsot generálunk a hordozóeszközön tárolandó adat számára az információ rögzítőbe beépített valamely második kódolási kulcs generáló adat alapján, és a hordozóeszközön eltárolandó adatot a második kódolási kulccsal kódoljuk.

A jelen találmány szerint továbbá a fenti információ rögzítési eljárásban a kriptográfiai lépés magában foglalja a következő két eljárást: amikor a lejátszó korlátozás nincs beál-

lítva, a kriptográfiai eszköz egy cím-egyértelmű kulcsot generál az információ rögzítőben tárolt valamely generálás-irányított mester kulcsból, egy lemez ID-ből, ami egy egyedi azonosító egy hordozóeszköz számára, egy cím kulcsból, ami egyedi a hordozóeszközre rögzítendő adat számára, és egy eszköz ID-ből, ami egy azonosító az információ rögzítő számára, majd generálja az első kódolási kulcsot a cím-egyértelmű kulcsból; és amikor a lejátszó korlátozás be van állítva, a kriptográfiai eszköz egy cím-egyértelmű kulcsot generál az információ rögzítőben tárolt generálás-irányított mester kulcsból, lemez ID-ből, ami egy egyedi azonosító a hordozóeszköz számára, cím kulcsból, ami egyedi a hordozóeszközre rögzítendő adat számára, és az eszköz-egyértelmű kulcsból, ami egyedi az információ rögzítő számára, majd generálja a második kódolási kulcsot a cím-egyértelmű kulcsból.

A jelen találmány szerint a fenti információ rögzítési eljárás magában foglal továbbá egy szállítási folyam feldolgozó lépést, ahol egy érkezési időbélyeget fűzünk hozzá egy szállítási folyam által tartalmazott diszkrét szállítási csomagok mindegyikéhez, a kriptográfiai lépésben generálunk egy blokk kulcsot kódolási kulcsként egynél több olyan csomagot magában foglaló blokk adat számára, amelyek mindegyikéhez hozzáfűztük az érkezési időbélyeget, és a blokk kulcsot kódolási kulcsként generáljuk a hordozóeszközön eltárolandó adat kódolásakor olyan adat alapján, amely magában foglalja a kódolási kulcs generáló adatot és egy blokk magot, ami további egyedi információ az érkezési időbélyeget magában foglaló blokk adat számára.

A jelen találmány szerint továbbá a fenti információ rögzítési eljárásban a kriptográfiai lépésben a hordozóeszközön eltárolandó adatot DES algoritmus szerint kódoljuk.

A jelen találmány szerint a fenti információ rögzítési eljárásban egy adatban lévő szállítási folyam által tartalmazott csomagok mindegyikéhez hozzáfűzött másolás vezérlési információt azonosítunk annak eldöntésére a másolás vezérlési információ alapján, hogy a hordozóeszközre való rögzítés lehetséges-e vagy sem.

A jelen találmány szerint a fenti információ rögzítési eljárásban 2-bites EMI-t azonosítunk másolás vezérlési információként annak eldöntésére az EMI alapján, hogy a hordozóeszközre való rögzítés lehetséges-e vagy sem.

A jelen találmány negyedik aspektusa szerint biztosíthatunk egy információ lejátszási eljárást információnak egy hordozóeszközről való lejátszására, amely eljárás magában foglalja a következő lépéseket: megújítunk dekódolási kulcs generáló adatot egy dekódolási kulcs generálására hordozóeszközön tárolt kódolt adat dekódolásához legalább vagy egy csomópont kulccsal, ami egyedi egy olyan hierarchikus fa-struktúra által tartalmazott csomópontok mindegyike számára, amely különböző információ lejátszók valamely sokaságát foglalja magában a fa struktúra egyes leveleiként, vagy egy levél kulccsal, ami egyedi az információ lejátszók mindegyike számára; valamint egy dekódolási kulcsot generálunk a megújítási lépésben megújított dekódolási kulcs generáló adatból a hordozóeszközön tárolt adat dekódolásához.

A jelen találmány szerint a fenti információ lejátszási eljárásban a dekódolási kulcs generáló adat egy mester kulcs, ami közös az információ rögzítők sokasága számára.

A jelen találmány szerint továbbá a fenti információ lejátszási eljárásban a dekódolási kulcs generáló adat egy közeg kulcs, ami egyedi egy meghatározott hordozóeszköz számára.

A jelen találmány szerint ezen kívül a fenti információ lejátszási eljárásban a csomópont kulcsot megújíthatjuk, és amikor egy csomópont kulcsot megújítunk, kiosztunk egy olyan levélnél lévő információ lejátszó számára, ahol a kódolási kulcs generáló adatot meg kell újítanunk egy kulcs megújítási blokkot, amelyet a megújítási csomópont kulcsnak a fa struktúra valamely alacsonyabb szintjén lévő csomópont kulcs vagy levél kulcs legalább egyikével való kódolásból származtatunk, és a kriptográfiai lépés magában foglalja a következő lépéseket: kódoljuk a kulcs megújítási blokkot a megújított csomópont kulcs megszerzéséhez; valamint kiszámítunk egy megújítási adatot a dekódolási kulcs generáló adat számára az így megszerzett megújított csomópont kulcs alapján.

A jelen találmány szerint továbbá a fenti információ lejátszási eljárásban a dekódolási kulcs generáló adat rendelkezik egy generálási számmal vele korrelációban lévő megújítási információként, és a kriptográfiai lépésben, amikor a hordozóeszközről származó kódolt adatot dekódolunk, beolvassuk a hordozóeszközből a kódolt adat kódolásakor használt kódolási kulcs generáló adat valamely generálási számát egy dekódolási kulcs generálására az így beolvasott generálási számnak megfelelő dekódolási kulcs generáló adatból.

A jelen találmány szerint továbbá a fenti információ lejátszási eljárásban a kriptográfiai lépés magában foglalja a következő két eljárást, amelyek egyikét szelektív módon hajtjuk végre attól függően, hogy egy lejátszó korlátozás be van-e állítva vagy sem: amikor a lejátszó korlátozás nincs beállítva, egy első dekódolási kulcsot generálunk a hordozóeszközön tárolt kódolt adat számára a hordozóeszközön tárolt egy első dekódolási kulcs generáló adat alapján, a kódolt adatot az első dekódolási kulccsal dekódoljuk, vagy amikor a lejátszó korlátozás be van állítva, egy második dekódolási kulcsot generálunk a hordozóeszközön tárolt kódolt adat számára az információ rögzítőbe beépített valamely második kódolási kulcs generáló adat alapján, és a kódolt adatot a második dekódolási kulccsal dekódoljuk.

A jelen találmány szerint továbbá a fenti információ lejátszási eljárásban a kriptográfiai lépés magában foglalja a következő két eljárást: amikor a lejátszó korlátozás nincs beállítva, megszerzünk az információ rögzítőben tárolt valamely generálás-irányított mester kulcsot, és megszerzünk még egy hordozóeszköztől egy lemez ID-t, ami egy egyedi azonosító egy hordozóeszköz számára, egy cím kulcsot, ami egyedi a dekódolandó adat számára, és egy eszköz ID-t, ami egy azonosító azon információ rögzítő számára, amelyen a kódolt adatot rögzítettük, és egy cím-egyértelmű kulcsot generálunk a mester kulcsból, lemez ID-ből, cím kulcsból és eszköz kulcsból, valamint generáljuk az első dekódolási kulcsot a cím-egyértelmű kulcsból; és amikor a lejátszó korlátozás be van állítva, megszerzünk az információ rögzítőben tárolt valamely generálás-irányított mester kulcsot és egy eszköz-egyértelmű kulcsot,

amely egyedi az információ rögzítő számára és abban is tároljuk, továbbá megszerzünk egy hordozóeszköztől egy lemez ID-t, ami egy egyedi azonosító a hordozóeszköz számára, és egy cím kulcsot, ami egyedi a dekódolandó adat számára, majd cím-egyértelmű kulcsot generálunk a mester kulcsból, lemez ID-ből, cím kulcsból és eszköz-egyértelmű kulcsból; és az így generált cím-egyértelmű kulcsból generáljuk a második dekódolási kulcsot.

A jelen találmány szerint a fenti információ lejátszási eljárásban a lejátszó magában foglal egy szállítási folyam feldolgozó eszközt adat kimenetre tétel vezérlésére a dekódolt blokk által tartalmazott szállítási csomagok mindegyikéhez hozzáfűzött érkezési időbélyeg alapján; és a kriptográfiai lépésben generálunk egy blokk kulcsot dekódolási kulcsként egynél több olyan csomagot magában foglaló blokk adat számára, amelyek mindegyikéhez hozzáfűztük az érkezési időbélyeget, és a blokk kulcsot dekódolási kulcsként generáljuk a hordozóeszközön tárolt kódolt adat dekódolásakor olyan adat alapján, amely magában foglalja a dekódolási kulcs generáló adatot és egy blokk magot, ami további egyedi információ az érkezési időbélyeget magában foglaló blokk adat számára.

A jelen találmány szerint továbbá a fenti információ lejátszási eljárásban a kriptográfiai eszköz a hordozóeszközön tárolt kódolt adatot DES algoritmus szerint dekódolja.

A jelen találmány szerint továbbá a fenti információ lejátszási eljárásban egy adatban lévő szállítási folyam által tartalmazott csomagok mindegyikéhez hozzáfűzött másolás vezérlési információt azonosítunk annak eldöntésére a másolás ve-

zérlési információ alapján, hogy a hordozóeszközről való lejátszás lehetséges-e vagy sem.

A jelen találmány szerint továbbá a fenti információ lejátszási eljárásban 2-bites EMI-t azonosítunk másolás vezérlési információként annak eldöntésére az EMI alapján, hogy a hordozóeszközről való lejátszás lehetséges-e vagy sem.

A jelen találmány ötödik aspektusa szerint biztosíthatunk egy információ rögzítésére képes információ hordozóeszközt, amelyben egy olyan kulcs megújítási blokkot tárolunk, amelyet egy megújított csomópont kulcs kódolásából származtatunk legalább vagy egy csomópont kulccsal, ami egyedi egy olyan hierarchikus fa struktúra által tartalmazott csomópontok mindegyike számára, amely különböző információ rögzítők sokaságát foglalja magában a fa struktúra egyes leveleiként, vagy egy levél kulccsal, ami egyedi az információ rögzítők mindegyike számára.

A jelen találmány szerint továbbá a fenti információ hordozóeszköz magában foglal egy kódolási kulcs generálásához használt kódolási kulcs generáló adatnak a megújított csomópont kulccsal való kódolásából származtatott adatot az információ rögzítőben a hordozóeszközön eltárolandó adat kódolásához.

A jelen találmány szerint továbbá a fenti információ hordozóeszköz magában foglal egy dekódolási kulcs generálásához használt dekódolási kulcs generáló adatnak a megújított csomópont kulccsal való dekódolásából származtatott adatot az információ lejátszóban a hordozóeszközön tárolt kódolt adat dekódolásához.

A jelen találmány szerint továbbá a fenti információ hordozóeszközön generálási információt tárolunk a kódolási vagy dekódolási kulcs generáló adatról.

A jelen találmány hatodik aspektusa szerint biztosíthatunk egy hordozóeszköz létrehozó berendezést egy információ hordozóeszköz létrehozására, amely berendezés magában foglal: memóriát egy olyan kulcs megújítási blokk tárolására, amelyet egy megújított csomópont kulcs kódolásából származtatunk legalább vagy egy csomópont kulccsal, ami egyedi egy olyan hierarchikus fa struktúra által tartalmazott csomópontok mindegyike számára, amely különböző információ rögzítők valamely sokaságát foglalja magában a fa struktúra egyes leveleiként, vagy egy levél kulccsal, ami egyedi az információ rögzítők mindegyike számára; valamint egy vezérlési egységet a memóriában tárolt kulcs megújítási blokknak a hordozóeszközre való írásának a vezérlésére.

A fenti hordozóeszköz létrehozó berendezésben továbbá a memória tárolja ezen kívül legalább egy hordozóeszköz azonosító és kódolt kódolási kulcs generáló adat vagy kódolt dekódolási kulcs generáló adat bármelyikét, és a vezérlési egység vezérli legalább a hordozóeszköz azonosító és kódolt kódolási kulcs generáló adat vagy kódolt dekódolási kulcs generáló adat bármelyikének a hordozóeszközre való írását.

A fenti hordozóeszköz létrehozó berendezésben továbbá a memória tárol ezen kívül generálási információt a kódolási kulcs generáló adatról vagy a dekódolási kulcs generáló adatról, és a vezérlési egység vezérli a generálási információnak a hordozóeszközre való írását.

A jelen találmány hetedik aspektusa szerint biztosíthatunk egy hordozóeszköz létrehozási eljárást, amely magában foglalja a következő lépéseket: egy memóriába eltárolunk egy olyan kulcs megújítási blokkot, amelyet egy megújított csomópont kulcs kódolásából származtatunk legalább vagy egy csomópont kulccsal, ami egyedi egy olyan hierarchikus fa struktúra által tartalmazott csomópontok mindegyike számára, amely különböző információ rögzítők valamely sokaságát foglalja magában a fa struktúra egyes leveleiként, vagy egy levél kulccsal, ami egyedi az információ rögzítők mindegyike számára; és a memóriában tárolt kulcs megújítási blokkot a hordozóeszközre írjuk.

A fenti hordozóeszköz létrehozási eljárásban továbbá a memóriába eltároljuk ezen kívül legalább egy hordozóeszköz azonosító és kódolt kódolási kulcs generáló adat vagy kódolt dekódolási kulcs generáló adat bármelyikét, és a hordozóeszközre írjuk legalább a hordozóeszköz azonosító és kódolt kódolási kulcs generáló adat vagy kódolt dekódolási kulcs generáló adat bármelyikét.

A fenti hordozóeszköz létrehozási eljárásban továbbá a memóriába eltárolunk generálási információt a kódolási kulcs generáló adatról vagy a dekódolási kulcs generáló adatról, és vezéreljük a generálási információnak a hordozóeszközre való írását.

A jelen találmány nyolcadik aspektusa szerint biztosíthatunk egy program szolgáltató közeget egy számítógépes program szolgáltatására, amely alatt információ feldolgozást folytatunk információnak egy hordozóeszközre való rögzítéséhez egy számítógépes rendszerben, amely számítógépes program magában

foglalja a következő lépéseket: megújítunk kódolási kulcs generáló adatot egy kódolási kulcs generálására valamely hordozóeszközön eltárolandó adat kódolásához legalább vagy egy csomópont kulccsal, ami egyedi egy olyan hierarchikus fa struktúra által tartalmazott csomópontok mindegyike számára, amely különböző információ rögzítők valamely sokaságát foglalja magában a fa struktúra egyes leveleiként, vagy egy levél kulccsal, ami egyedi az információ rögzítők mindegyike számára; valamint egy kódolási kulcsot generálunk a kódolási kulcs generáló adat alapján a hordozóeszközön eltárolandó adat kódolására.

A jelen találmány kilencedik aspektusa szerint biztosíthatunk egy program szolgáltató közeget egy számítógépes program szolgáltatására, amely alatt egy hordozóeszközön tárolt információt lejátszunk egy számítógépes rendszerben, amely számítógépes program magában foglalja a következő lépéseket: megújítunk dekódolási kulcs generáló adatot, amiből egy dekódolási kulcsot generálunk a hordozóeszközön tárolt kódolt adat dekódolásához legalább vagy egy csomópont kulccsal, ami egyedi egy olyan hierarchikus fa struktúra által tartalmazott csomópontok mindegyike számára, amely különböző információ lejátszók valamely sokaságát foglalja magában a fa struktúra egyes leveleiként, vagy egy levél kulccsal, ami egyedi az információ lejátszók mindegyike számára; valamint generáljuk a dekódolási kulcsot a megújítási lépésben megújított dekódolási kulcs generáló adatból a hordozóeszközön tárolt adat dekódolására.

A jelen találmány szerint a fa-struktúrájú hierarchikus kulcs kiosztási eljárást használjuk egy kiosztandó üzenetnek a kulcs megújításához szükséges méretének csökkentésére. Neveze-

tesen, a kulcs kiosztási eljárásban n számú rögzítő/lejátszó mindegyikét egy fa leveleinek egyikén rendezzük el. Az eljárást egy szükséges kulcs, például egy mester kulcs vagy közeg kulcs kiosztására használjuk egy tartalom adatnak egy hordozóeszközre való rögzítéséhez vagy onnan való lejátszásához a hordozóeszközön vagy egy kommunikációs vonalon keresztül, és minden egyes rögzítő/lejátszó az így kiosztott mester kulcsot vagy közeg kulcsot használja a tartalom adat rögzítésére vagy lejátszására.

A jelen találmány egyik módozata szerint egy hordozóeszközre rögzítendő tartalom MPEG2-definiált TS (transport stream, szállítási folyam) csomagok formájú, és minden egyes TS csomagot úgy rögzítünk, hogy hozzáfűzzük az ATS-t, ami abban az időpontban alakul ki, amikor a rögzítő a csomagot fogadja. Az ATS egy 24-32 bites valamelyest véletlenszerű adat. Az ATS az „érkezési időbélyeg" („arrival time stamp") rövidítése. A hordozóeszköz egy blokkja (szektora) valamely X számú olyan TS csomagot rögzít, amelyek mindegyikéhez hozzáfűztünk egy ATS-t. Egy szállítási folyam által tartalmazott blokkok mindegyikében a TS csomagok közül az elsőhöz hozzáfűzött ATS-t használjuk egy blokk kulcs generálására, amelyet a blokkban lévő adat kódolásához használunk.

Ily módon minden egyes blokkban az adatot egy egyedi blokk kulccsal kódolhatjuk anélkül, hogy bármiféle speciális területet kellene biztosítanunk a kulcs tárolásához vagy a fő adaton kívül bármely más adathoz kellene hozzáférnünk a rögzítés vagy lejátszás közben.

Az ATS mellett továbbá másolás vezérlési információt (CCI - copy control information) fűzhetünk hozzá egy rögzítendő TS

csomaghoz, és mind az ATS-t, mind pedig a CCI-t használhatjuk egy blokk kulcs generálására.

Megjegyezzük, hogy a jelen találmány nyolcadik és kilencedik aspektusa szerinti program szolgáltató közegek mindkettője például olyan közeg, amely számítógépes programot szolgáltat számítógép által olvasható formában egy olyan általános célú számítógépes rendszernek, ami képes változatos program kódok végrehajtására. A közeg nem korlátozódik semmiféle speciális formára, és lehet hordozóeszközök bármelyike, például CD, FD, MO stb. és átviteli közegek bármelyike, például egy hálózat.

A fenti program szolgáltató közegek egy szerkezeti vagy működési együttműködést definiálnak egy számítógépes program és közeg között egy előre meghatározott számítógépes program funkcióinak megvalósítására egy számítógépes rendszerben. Más szóval, amikor a számítógépes programot telepítjük egy számítógépes rendszerben a program szolgáltató közegen keresztül, együttműködően fog dolgozni a számítógépes rendszerben, a jelen találmány más aspektusaiban lévőekhez hasonló hatások biztosítása végett.

A jelen találmány ezen tárgyai és más tárgyai, jellemzői és előnyei világosabbá válnak a jelen találmány előnyös kiviteli példáinak következő részletes bemutatása folytán, összekapcsolva a kísérő rajzokkal.

Az 1. ábra egy blokk diagram, amely a jelen találmány szerinti információ rögzítő/lejátszó egy példa konstrukcióját (1) mutatja be.

A 2. ábra egy blokk diagram, amely a jelen találmány szerinti információ rögzítő/lejátszó egy példa konstrukcióját (2) mutatja be.

A 3A és 3B ábrák egy adat rögzítési folyamatban végrehajtott műveletek folyamatát mutatják be a jelen találmány szerinti információ rögzítő/lejátszóban.

A 4A és 4B ábrák egy adat lejátszási folyamatban végrehajtott műveletek folyamatát mutatják be a jelen találmány szerinti információ rögzítő/lejátszóban.

Az 5. ábra a jelen találmány szerinti információ rögzítő/lejátszóban feldolgozott valamely adat formátumot mutatja be.

A 6. ábra egy blokk diagram, amely egy szállítási folyam feldolgozó eszköz konstrukcióját mutatja be a jelen találmány szerinti információ rögzítő/lejátszóban.

A 7A-7C ábrák a jelen találmány szerinti információ rögzítő/lejátszóban feldolgozott valamely szállítási folyamot mutatnak be.

A 8. ábra egy blokk diagram, amely egy szállítási folyam feldolgozó eszköz konstrukcióját mutatja be a jelen találmány szerinti információ rögzítő/lejátszóban.

A 9. ábra egy blokk diagram, amely egy szállítási folyam feldolgozó eszköz konstrukcióját mutatja be a jelen találmány szerinti információ rögzítő/lejátszóban.

A 10. ábra a jelen találmány szerinti információ rögzítő/lejátszóban feldolgozott blokk adathoz további információnak egy példáját mutatja be.

A 11. ábra egy fa-struktúra diagram, amely kulcsok, például egy mester kulcs, közeg kulcs stb. kódolását mutatja be a jelen találmány szerinti információ rögzítő/lejátszó számára.

A 12A és 12B ábrák a kulcsok, például a mester kulcs, közeg kulcs stb. kiosztásánál használt kulcs megújítási blokk példáit mutatják be a jelen találmány szerinti információ rögzítő/lejátszó számára.

A 13. ábra kulcs kiosztás és dekódolás példáit mutatja be ebben a sorrendben a kulcs megújítási blokk használatával, a mester kulcs esetén a jelen találmány szerinti információ rögzítő/lejátszóban.

A 14. ábra a dekódoláskor végrehajtott műveletek egy folyamatát mutatja be a kulcs megújítási blokk használatával a mester kulcs esetén a jelen találmány szerinti információ rögzítő/lejátszóban.

A 15. ábra a mester kulcs generálás összehasonlításkor végrehajtott műveletek egy folyamatát mutatja be a tartalom rögzítéskor a jelen találmány szerinti információ rögzítő/lejátszóban.

A 16. ábra egy blokk diagram (1), amely bemutatja a kódolást az adat rögzítéshez a jelen találmány szerinti információ rögzítő/lejátszóban egy olyan rendszerben, amelyben beállítható egy lejátszó korlátozás.

A 17. ábra egy blokk diagram (2), amely bemutatja a kódolást az adat rögzítéshez a jelen találmány szerinti információ rögzítő/lejátszóban egy olyan rendszerben, amelyben beállítható egy lejátszó korlátozás.

A 18. ábra az adat rögzítésnél végrehajtott műveletek egy folyamatát mutatja be a jelen találmány szerinti információ

rögzítő/lejátszóban egy olyan rendszerben, amelyben beállítható a lejátszó korlátozás.

A 19. ábra egy lemez-egyértelmű kulcs generálásának egy példáját mutatja be a jelen találmány szerinti információ rögzítő/lejátszóban.

A 20. ábra egy cím-egyértelmű kulcs generálásánál végrehajtott műveletek egy folyamatát mutatja be a jelen találmány szerinti információ rögzítő/lejátszóban egy olyan rendszerben, amelyben beállítható a lejátszó korlátozás.

A 21. ábra egy cím-egyértelmű kulcs generálásának egy példáját mutatja be adat rögzítéshez a jelen találmány szerinti információ rögzítő/lejátszóban egy olyan rendszerben, amelyben beállítható a lejátszó korlátozás.

A 22. ábra bemutatja, hogy hogyan generáljuk a blokk kulcsot a jelen találmány szerinti információ rögzítő/lejátszóban.

A 23. ábra egy blokk diagram, amely bemutatja a dekódolást az adat lejátszáshoz a jelen találmány szerinti információ rögzítő/lejátszóban egy olyan rendszerben, amelyben beállítható a lejátszó korlátozás.

A 24. ábra bemutatja az adat lejátszásnál végrehajtott műveletek egy folyamatát a jelen találmány szerinti információ rögzítő/lejátszóban egy olyan rendszerben, amelyben beállítható a lejátszó korlátozás.

A 25. ábra egy folyamatábra, amely bemutatja részletesen annak eldöntését adat lejátszásnál, hogy lejátszható-e adat vagy sem a jelen találmány szerinti információ rögzítő/lejátszóban egy olyan rendszerben, amelyben beállítható a lejátszó korlátozás.

A 26. ábra bemutatja egy cím-egyértelmű kulcs generálásánál végrehajtott műveletek egy folyamatát adat lejátszáshoz a jelen találmány szerinti információ rögzítő/lejátszóban egy olyan rendszerben, amelyben beállítható a lejátszó korlátozás.

A 27. ábra példákat mutat kulcs kiosztásra és dekódolásra a kulcs megújítási blokk használatával a közeg kulcs esetén a jelen találmány szerinti információ rögzítő/lejátszóban.

A 28. ábra a dekódolásnál végrehajtott műveletek egy folyamatát mutatja be a kulcs megújítási blokk használatával a közeg kulcs esetén a jelen találmány szerinti információ rögzítő/lejátszóban.

A 29. ábra a tartalom rögzítésnél végrehajtott műveletek egy folyamatát mutatja be a közeg kulcs használatával a jelen találmány szerinti információ rögzítő/lejátszóban.

A 30. ábra egy blokk diagram (1), amely bemutatja a kódolást adat rögzítéshez a közeg kulcs használatával a jelen találmány szerinti információ rögzítő/lejátszóban egy olyan rendszerben, amelyben beállítható a lejátszó korlátozás.

A 31. ábra egy blokk diagram (2), amely bemutatja a kódolást adat rögzítéshez a közeg kulcs használatával a jelen találmány szerinti információ rögzítő/lejátszóban egy olyan rendszerben, amelyben beállítható a lejátszó korlátozás.

A 32. ábra az adat rögzítésnél végrehajtott műveletek egy folyamatát mutatja be a közeg kulcs használatával a jelen találmány szerinti információ rögzítő/lejátszóban egy olyan rendszerben, amelyben beállítható a lejátszó korlátozást.

A 33. ábra egy blokk diagram, amely bemutatja a kódolást adat lejátszáshoz a közeg kulcs használatával a jelen talál-

mány szerinti információ rögzítő/lejátszóban egy olyan rendszerben, amelyben beállítható a lejátszó korlátozás.

A 34. ábra az adat lejátszásnál végrehajtott műveletek egy folyamatát mutatja be a közeg kulcs használatával a jelen találmány szerinti információ rögzítő/lejátszóban egy olyan rendszerben, amelyben beállítható a lejátszó korlátozás.

A 35. ábra egy folyamatábra, amely részletesen bemutatja annak eldöntését adat lejátszásnál a közeg kulcs használatával, hogy lejátszható-e adat vagy sem a jelen találmány szerinti információ rögzítő/lejátszóban egy olyan rendszerben, amelyben beállítható a lejátszó korlátozás.

A 36. ábra egy blokk diagram, amely bemutatja a jelen találmány szerinti információ rögzítő/lejátszó azon konstrukcióját, amelyben egy KRB-t kívülről fogadunk egy kommunikációs eszközön vagy hasonlón keresztül, és eltároljuk egy hordozóeszközön.

A 37. ábra egy blokk diagram, amely bemutat egy a jelen találmány szerinti információ rögzítő/lejátszóban követett eljárást KRB fogadására kívülről egy kommunikációs eszközön vagy hasonlón keresztül, és annak eltárolására egy hordozóeszközön.

A 38. ábra KRB-nek kívülről a kommunikációs eszközön vagy hasonlón keresztül való fogadásánál és annak egy hordozóeszközre való eltárolásánál végrehajtott műveletek egy folyamatát mutatja be a jelen találmány szerinti információ rögzítő/lejátszóban.

A 39. ábra bemutatja a jelen találmány szerinti információ rögzítő/lejátszóban követett eljárást KRB fogadásához kívülről a kommunikációs eszközön vagy hasonlón keresztül és annak egy hordozóeszközön való eltárolásához.

A 40A és 40B ábrák másolás vezérléshez végrehajtott műveletek folyamatait mutatják be az adat rögzítésnél a jelen találmány szerinti információ rögzítő/lejátszóban.

A 41A és 41B ábrák másolás vezérléshez végrehajtott műveletek folyamatait mutatják be az adat lejátszásnál a jelen találmány szerinti információ rögzítő/lejátszóban.

A 42. ábra egy adat feldolgozó rendszer blokk diagramja adatnak szoftver általi feldolgozására az információ rögzítő/lejátszóban.

A 43. ábra egy blokk diagram, amely egy berendezés konstrukcióját mutatja be egy olyan információ hordozóeszköz létrehozásához, amelyet a jelen találmány szerinti információ rögzítő/lejátszóban használunk.

A 44. ábra a jelen találmány szerinti információ rögzítő/lejátszóban használt információ hordozóeszköz létrehozásánál végrehajtott műveletek egy folyamatát mutatja be.

A 45. ábra a jelen találmány szerinti információ rögzítő/lejátszóban használt kulcs megújítási blokk egy példa formátumát mutatja be.

A 46A-46C ábrák egy címkét mutatnak be a jelen találmány szerinti információ rögzítő/lejátszóban használt kulcs megújítási blokkhoz.

Az 1. ábrán sematikusan ábrázoljuk egy blokk diagram formájában a jelen találmány szerinti információ rögzítő/lejátszó egy kiviteli példáját. A rögzítő/lejátszót általánosan a „100" hivatkozási jellel jelöljük. Amint azt bemutatjuk, a 100 rögzítő/lejátszó magában foglal egy 120 bemenet/kimenet interfészt (I/F), 130 MPEG (Moving Picture Experts Group) kodeket (codec), 141 A/D átalakító és D/A átalakító kombinációt magá-

ban foglaló 140 bemenet/kimenet I/F-et, 150 kriptográfiai egységet, 160 ROM-ot, 170 CPU-t (central processing unit, központi feldolgozó egység), 180 memóriát, 190 meghajtót egy 195 hordozóeszközhöz, és egy 300 szállítási folyam feldolgozó eszközt (TS feldolgozót). A komponenseket egy 110 sín által csatlakoztatjuk egymáshoz.

A 120 bemenet/kimenet I/F digitális jeleket fogad, amelyet kívülről biztosított változatos tartalmak, például kép, hang, program vagy hasonlók egyike foglal magában, és kimenetre teszi őket a 110 sínre és kívülre is. A 130 MPEG kodek a 110 sínen keresztül biztosított MPEG-kódolt adat MPEG dekódolását végzi el, és kimenetre teszi az MPEG-dekódolt adatot a 140 bemenet/kimenet I/F-hez, míg a 140 bemenet/kimenet I/F-ről biztosított digitális jelek MPEG kódolását végzi el, és kimenetre teszi az adatot a 110 sínre. A 140 bemenet/kimenet I/F a 141 A/D átalakító és D/A átalakító kombinációt alkalmazza. A 140 bemenet/kimenet I/F analóg jeleket fogad tartalomként kívülről, elvégzi az adat A/D (analógról digitálisra való) átalakítását, és az így megkapott digitális jeleket kimenetre teszi a 130 MPEG kodekhez, míg a 130 MPEG kodektől származó digitális jelek D/A (digitálisról analógra való) átalakítását végzi el, és az így megkapott analóg jeleket kimenetre teszi kívülre.

A 150 kriptográfiai egység például egy egychipes LSI (one-chip LSI, LSI - large scale integrated cicuit, nagymértékben integrált áramkör). Ez a 110 sínen keresztül biztosított valamely tartalomban lévő digitális jeleket kódolja vagy dekódolja, és az adatot kimenetre teszi a 110 sínre. Megjegyezzük, hogy a 150 kriptográfiai egység nem korlátozódik egy

egychipes LSI-re, lehet viszont szoftver vagy hardver változatos típusainak valamely kombinációja. Egy szoftver-típusú kriptográfiai egységet a későbbiekben részletesen bemutatunk.

A 160 ROM-ban tárolunk egy levél kulcsot, ami egy egyedi eszköz kulcs például minden egyes rögzítő/lejátszó, vagy rögzítő/lejátszók valamely sokaságának egy csoportja számára, valamint egy csomópont kulcsot, ami egy egyedi eszköz kulcs a rögzítő/lejátszók sokasága vagy csoportok egy sokasága számára. A 170 CPU a 180 memóriában tárolt programot hajt végre a 130 MPEG kodek, 150 kriptográfiai egység stb. vezérlésére. A 180 memória például egy megmaradó memória, amely tárol például a 170 CPU által végrehajtandó programot és a 170 CPU működéséhez szükséges adatokat. A 190 meghajtó meghajtja a 195 hordozóeszközt, amely képes digitális adat rögzítésére, digitális adatnak a 195 hordozóeszközről való olvasásához és kimenetre teszi az adatot a 110 sínre, míg a 110 sínen keresztül biztosított digitális adatot a 195 hordozóeszközhöz biztosítja az utóbbira való rögzítéséhez. Megjegyezzük, hogy a 100 rögzítő/lejátszót konstruálhatjuk oly módon, hogy a 160 ROM tárolja a programot, míg a 180 memória tárolja az eszköz kulcsokat.

A 195 hordozóeszköz egy olyan közeg, amely képes digitális adat tárolására, például valamilyen optikai lemez, ami magában foglal DVD-t, CD-t és hasonlókat, egy magneto- optikai lemez, egy mágneslemez, egy mágnesszalag, vagy valamilyen félvezető memória, amely magában foglal RAM-ot és hasonlókat. Ebben a kiviteli példában a 195 hordozóeszköz eltávolíthatóan telepíthető a 190 meghajtóban. Megjegyezzük viszont, hogy a 195 hordozóeszközt beépíthetjük a 100 rögzítő/lejátszóba.

A 300 szállítási folyam feldolgozó eszköz (TS feldolgozó) egy előre meghatározott programnak (tartalomnak) megfelelő szállítási csomagokat bontja ki például egy olyan szállítási folyamból, amely abban multiplexelt TV programok (tartalmak) egy sokaságával rendelkezik, majd minden egyes csomaggal együtt eltárol a 195 hordozóeszközön információt a kibontott szállítási folyam megjelenésének időpontjáról, továbbá vezérli egy szállítási folyam megjelenésének időpontját a 195 hordozóeszközről való olvasáshoz. A 300 TS feldolgozót a későbbiekben fogjuk részletesebben leírni a 6. ábrával és az azt követő rajzokkal kapcsolatban.

Egy szállítási folyam esetén beállítunk egy ATS-t a szállítási folyamban lévő szállítási csomagok mindegyikének megjelenési idejeként. A megjelenés idejét a kódolás közben határozzuk meg, elkerülendő egy T-STD (transport stream system target decoder, szállítási folyam rendszer cél dekóder) hibázását, ami egy az MPEG-2 Systems-ben definiált virtuális dekóder, és egy szállítási folyam olvasása közben a megjelenés időpontját az egyes szállítási csomagokhoz hozzáfűzött ATS-sel vezéreljük. A 300 TS feldolgozó a fenti vezérlés-fajtákat hajtja végre. Például, szállítási csomagoknak a hordozóeszközre való rögzítésekor a szállítási csomagokat oly módon elrendezett forrás csomagokként rögzítjük, ahol az egymást követő csomagok között nincsen helykihagyás, és minden egyes csomag megjelenésének időpontját változatlanul tartjuk meg, ami lehetővé teszi az egyes szállítási csomagok kimeneti időzítésének vezérlését a hordozóeszközről való olvasás közben. A 300 TS feldolgozó ATS-t fűz hozzájuk, amely azt az időpontot jelzi,

amikor az egyes szállítási csomagokat fogadtuk, amikor adatot rögzítünk a 195 hordozóeszközre, például egy DVD-re.

A jelen találmány szerinti 100 rögzítő/lejátszóban valamely tartalmat, amely olyan szállítási folyamot foglal magában, amelyben az ATS-t hozzáfűztük az egyes szállítási csomagokhoz, a 150 kriptográfiai egység által kódoljuk, és az így kódolt tartalmat a 195 hordozóeszközön tároljuk el. A 150 kriptográfiai egység továbbá dekódol egy a 195 hordozóeszközön tárolt kódolt tartalmat. Ezt a kódolást és dekódolást tovább tárgyaljuk a későbbiekben.

Megjegyezzük, hogy az 1. ábrán a 150 kriptográfiai egységet és a 300 TS feldolgozót különálló blokkokként mutatjuk az ábrázolás és a magyarázat kényelme érdekében, de ezek a funkciók egyesíthetőek egy egychipes LSI-ben, vagy megvalósíthatóak szoftver vagy hardver részek valamely kombinációja által.

Az 1. ábrán bemutatott konstrukción kívül a jelen találmány szerinti rögzítő/lejátszó konstruálható úgy is, hogy ahogyan a 2. ábrán. A 2. ábrán bemutatott rögzítő/lejátszót általánosan a „200" hivatkozási jellel jelöljük. A 200 rögzítő/lejátszóban egy 195 hordozóeszköz eltávolíthatóan telepíthető egy 210 hordozóeszköz interfészen (I/F) meghajtó egységként. Adatoknak a 195 hordozóeszközre való írása és az onnan való olvasása lehetséges továbbá akkor is, amikor azt egy másik rögzítő/lejátszóban használjuk.

A 3. és 4. ábrákra hivatkozva, adatoknak az 1. vagy 2. ábrán bemutatott rögzítő/lejátszóban lévő hordozóeszközre való írásánál és adatoknak a hordozóeszközről való olvasásánál végrehajtott műveletek folyamatait mutatjuk be. Digitális jeleknek kívülről származó tartalomként a 195 hordozóeszközre való

rögzítéséhez a műveleteket a 3A ábrán lévő folyamatábrán bemutatott módon hajtjuk végre. Nevezetesen, amikor digitális jeleket tartalomként (digitális tartalomként) biztosítunk a 120 bemenet/kimenet I/F-hez egy IEEE 1394 (IEEE - Institute of Electrical and Electronic Engineers) soros sínen vagy hasonlón keresztül, a 120 bemenet/kimenet I/F fogadja a digitális tartalmat, és kimenetre teszi az adatot a 300 TS feldolgozóhoz a 110 sínen keresztül az S301 lépésben.

Az S302 lépésben a 300 TS feldolgozó blokk adatot generál, amelyben egy ATS-t fűzünk hozzá minden egyes szállítási csomaghoz egy szállítási folyamban, és kimenetre teszi az adatot a 150 kriptográfiai egységhez a 110 sínen keresztül.

Az S303 lépésben a 150 kriptográfiai egység kódolja a fogadott digitális tartalmat, és kimenetre teszi a kódolt tartalmat a 190 meghajtóhoz vagy a 210 hordozóeszköz I/F-hez a 110 sínen keresztül. Az S304 lépésben a kódolt digitális tartalmat rögzítjük a 195 hordozóeszközre a 190 meghajtón vagy a 210 hordozóeszköz I/F-en keresztül. Itt a rögzítő/lejátszó kilép a rögzítési eljárásból. A 150 kriptográfiai egység általi kódolást tovább tárgyaljuk a későbbiekben.

Emlékeztetnünk kell arra, hogy az eszközök között az IEEE 1394 soros sínen keresztül átvitt digitális tartalom védelmére szabványként az öt vállalat létrehozta az „5CDTCP (Five Company Digital Transmission Content Protection)" (amelyre a továbbiakban „DTCP"-ként hivatkozunk) protokollt, amely öt vállalat magában foglalja a Sony Corporationt, amely a jelen találmány Benyújtója. Ez előírja, hogy abban az esetben, amikor nem egy valamilyen „szabadon másolható" digitális tartalmat továbbítunk, a továbbító és a fogadó oldalaknak kölcsönö-

sen hitelesíteniük kell az átvitel előtt, hogy a másolás vezérlési információt képesek helyesen kezelni, majd ezután a digitális tartalmat kódolni kell a továbbító oldalon annak átviteléhez, és a kódolt digitális tartalmat (kódolt tartalmat) dekódolni kell a fogadó oldalnál.

Eszerint a DTCP szabvány szerinti adat átvitelnél és fogadásnál a 210 bemenet/kimenet I/F az adat fogadó oldalon fogadja a kódolt tartalmat az IEEE 1394 soros sínen keresztül, dekódolja a kódolt tartalmat a DTCP szabvánnyal összhangban, és ezután kimenetre teszi az adatot sima, vagy kódolatlan tartalomként a 150 kriptográfiai egységhez (az S301 lépésben).

Valamely digitális tartalom DTCP-alapú kódolásához egy idő-változó kulcsot (time-varying key) kell generálnunk. A kódoláshoz használt kódolási kulcsot magában foglaló kódolt digitális tartalmat továbbítjuk az IEEE 1394 soros sínen a fogadó oldalhoz, és a fogadó oldal dekódolja a kódolt digitális tartalmat a tartalom által tartalmazott kulccsal.

Még pontosabban a DTCP szabvány azt írja elő, hogy digitális tartalom kódolásához a kódolt tartalom magában foglalja a kulcs egy kezdeti értékét és egy jelzőt (flag), amely a kulcs megváltozásának egy időpontját jelzi. A fogadó oldalon a kódolt tartalom által tartalmazott kulcs kezdeti értéke megváltozik a kódolt tartalom által tartalmazott jelző által jelzett időzítéssel, ily módon generálva a kódoláshoz használt valamely kulcsot, és a kódolt tartalmat az így generált kulccsal dekódoljuk. Nevezetesen, figyelembe vehetjük, hogy a kódolt tartalom magában foglal egy kulcsot, amelyet annak dekódolásához használunk, és ily módon ez a megfontolás igaz lesz a következő leírásban is. A DTCP szabvány szerint, egy infor-

mációs jellegű verzió elérhető például egy a http://www.dtcp.com URL (uniform resource locator) által azonosított Web oldalról.

A következőben külső analóg jeleknek a 195 hordozóeszközre tartalomként való írását mutatjuk be a 3B ábrán lévő folyamatábrára való hivatkozással. Amikor a 140 bemenet/kimenet I/F analóg jeleket fogad tartalomként (analóg tartalom) az S321 lépésben, az S322 lépésre halad, ahol a 141 A/D átalakító és D/A átalakító kombináció az analóg tartalom A/D átalakítását végzi el digitális jeleknek tartalomként (digitális tartalomként) való biztosítására.

A digitális tartalmat a 130 MPEG kodekhez biztosítjuk, amely a digitális tartalom MPEG kódolását hajtja végre, nevezetesen a digitális tartalom kódolását MPEG tömörítés által az S323 lépésben, és a kódolt tartalmat a 150 kriptográfiai egységhez biztosítja a 110 sínen keresztül.

Az ezt követő S324, S325 és S326 lépésekben a 3A ábrán lévő S302 és S303 lépésekhez hasonló műveleteket hajtunk végre. Vagyis a 300 TS feldolgozó ATS-t fűz minden egyes szállítási csomaghoz, a 150 kriptográfiai egység kódolja a tartalmat, és az így megkapott kódolt tartalmat a 195 hordozóeszközre rögzítjük. Itt a rögzítő/lejátszó kilép a rögzítési eljárásból.

A következőben a tartalomnak a 195 hordozóeszközről való lejátszásához és kívülre digitális vagy analóg tartalomként való kimenetre tételéhez végrehajtott műveletek egy folyamatát mutatjuk be a 4. ábrán lévő folyamatábrára való hivatkozással. Ezt úgy végezzük el, mint a 4A ábrán lévő folyamatábrán. Először az S401 lépésben egy kódolt tartalmat olvasunk be a 195

hordozóeszközről a 190 meghajtó vagy a 210 hordozóeszköz I/F által, és kimenetre tesszük a 150 kriptográfiai egységhez a 110 sínen keresztül.

Az S402 lépésben a 150 kriptográfiai egység dekódolja a 190 meghajtótól vagy a 210 hordozóeszköz I/F-től biztosított kódolt tartalmat, és kimenetre teszi a dekódolt adatot a 300 TS feldolgozóhoz a 110 sínen keresztül.

Az S403 lépésben a 300 TS feldolgozó meghatározza a kimenet időzítését a szállítási folyam által tartalmazott szállítási csomagok mindegyikéhez hozzáfűzött ATS alapján az ATS-nek megfelelő vezérlés elvégzéséhez, és az adatot a 120 bemenet/kimenet I/F-hez biztosítja a 110 sínen keresztül. Megjegyezzük, hogy a 300 TS feldolgozó feldolgozási műveleteit és a digitális tartalom dekódolását a 150 kriptográfiai egységben tovább tárgyaljuk majd a későbbiekben.

Megjegyezzük továbbá, hogy amikor a digitális tartalmat az IEEE 1394 soros sínen keresztül tesszük kimenetre, a 120 bemenet/kimenet I/F egy kölcsönös hitelesítést hajt végre egy ellenkező oldali eszközzel, amint azt megelőzően említettük, a DTCP szabvánnyal összhangban az S404 lépésben, és ezután kódolja a digitális tartalmat az átvitelhez.

Valamely tartalomnak a 195 hordozóeszközről való olvasásához és analóg tartalomként való kimenetre tételéhez kívülre a lejátszási műveleteket oly módon hajtjuk végre, mint a 4B ábrán mutatott folyamatábrán.

Nevezetesen, a 4A ábrán lévő S401, S402 és S403 lépésekben lévőekhez hasonló műveleteket hajtunk végre az ezt követő SS421, S422 és S423 lépésekben. Ezáltal a 150 kriptográfiai

egységtől biztosított dekódolt digitális tartalmat a 130 MPEG kodekhez biztosítjuk a 110 sínen keresztül.

Az S424 lépésben a 130 MPEG kodek a digitális tartalom MPEG dekódolását hajtja végre, nevezetesen kitömöríti a digitális adatot, és az adatot a 140 bemenet/kimenet I/F-hez biztosítja. Az S425 lépésben a 140 bemenet/kimenet I/F az S424 lépésben a 130 MPEG kodekben MPEG dekódolásnak alávetett digitális tartalom D/A átalakítását hajtja végre a 141 A/D átalakító és D/A átalakító kombináció által. Ezután a 140 bemenet/kimenet I/F az S426 lépésre halad, ahol az analóg tartalmat kimenetre teszi kívülre. Itt a rögzítő/lejátszó kilép a lejátszási eljárásból.

A következőben a jelen találmány szerinti hordozóeszközre írt vagy onnan olvasott adat formátumát mutatjuk be az 5. ábrára való hivatkozással. A minimális egységet, amelyben a jelen találmány szerinti hordozóeszközről adatot olvasunk vagy arra írunk, „blokknak" nevezzük. Egy blokk 192*X bájt, (például X=32) mérettel rendelkezik.

A jelen találmány szerint egy ATS-t fűzünk minden egyes MPEG2-definiált (188 bájtos) TS csomaghoz egy 192 bájtos adat biztosítására, és X számú ilyen adatot tekintünk egy blokknak. Az ATS egy 24-32 bites adat, amely egy érkezési időpontot jelöl. Az ATS az „érkezési időbélyeg" („arrival time stamp") rövidítése, amint azt megelőzően leírtuk. Az ATS egy véletlenszerű adat, amely az egyes csomagok egy érkezési idejének felel meg. A hordozóeszköz egy blokkja (szektora) X számú olyan TS csomagot rögzít, amelyek mindegyikéhez egy ATS-t fűztünk hozzá. A jelen találmány szerint egy szállítási folyam által tartalmazott egyes blokkokban lévő TS csomagok közül az első-

höz hozzáfűzött valamely ATS-t használjuk egy blokk kulcs generálására, amelyet a blokkban (szektorban) lévő adat kódolására használunk.

Az egyes blokkok számára egy egyedi kulcsot generálunk egy kódolási blokk kulcsnak a véletlenszerű ATS alapján való generálása által. Az így generált blokk-egyértelmű kulcsot használjuk az egyes blokkok kódolására. Továbbá egy blokk kulcsnak az ATS alapján való generálása által szükségtelenné válik egy terület biztosítása a hordozóeszközön a kódolási kulcs tárolásához minden egyes blokk esetében, és lehetségessé válik a fő adat terület hatékony használata a hordozóeszközön. Ezen kívül adat lejátszás közben nem szükséges más adathoz hozzáférni a fő adat területen lévőeken kívül, ami egy hatékonyabb adat rögzítést vagy lejátszást biztosít.

Megjegyezzük, hogy az 5. ábrán bemutatott valamely blokk mag az ATS-t magában foglaló további információ. A blokk mag magában foglalhat ezen kívül másolás vezérlési információt az ATS mellett. Ebben az esetben az ATS-t és a CCI-t használjuk egy blokk kulcs generálására.

Megjegyezzük továbbá, hogy a jelen találmány szerint a hordozóeszközön, például egy DVD-ben tárolt valamely tartalomban lévő adatok túlnyomó része kódolt. Amint azt az 5. ábra alján mutatjuk, egy blokk vezető részletében lévő m bájtot (például m=8 vagy 16 bájtot) sima, vagy kódolatlan, nevezetesen nem kódolt adatként rögzítjük, míg a fennmaradó adatot (m+1-edik és az azt követőket) kódoljuk, mert a kódolt adat hosszúság korlátozott, mivel a kódolást 8-bájtos egységekben végezzük el. Megjegyezzük, hogy ha a kódolást elvégezhetjük például 1-bájtos egységekben 8-bájtos egységek helyett, a

blokk mag kivételével az összes adatot kódolhatjuk a blokk vezető részletében beállított négy bájttal (m=4).

A következőkben az ATS funkcióját írjuk le részletesen. Amint azt megelőzően leírtuk, az ATS egy érkezési időbélyeg, amelyet egy bemeneti szállítási folyam által tartalmazott szállítási csomagok mindegyikéhez hozzáfűztünk a TS csomag megjelenése egy időzítésének megőrzéséhez.

Vagyis amikor egy szállítási folyamban multiplexelt TV programok (tartalmak) valamely sokaságából bontunk ki egyet vagy néhányat, a kibontott szállítási folyam által tartalmazott szállítási csomagok például szabálytalan időintervallumokban jelennek meg (lásd 7A ábra). Egy időzítés, amelyben a valamely szállítási folyamban lévő egyes szállítási csomagok megjelennek, fontos a szállítási folyam számára, és a megjelenés időzítését a kódolás közben határozzuk meg, elkerülendő a T-STD (transport stream system target decoder), ami egy MPEG-2 Systems-ben (ISO/IEC 13818 - 1) definiált virtuális dekóder, bármely hibázását.

A szállítási folyam lejátszása közben a megjelenés időzítését az egyes szállítási csomagokhoz hozzáfűzött ATS alapján vezéreljük. Ezért a szállítási csomagoknak a hordozóeszközre való rögzítésekor a szállítási csomag bemeneti időzítését meg kell őriznünk. Amikor szállítási csomagokat rögzítünk egy hordozóeszközre, például egy DVD-re, minden egyes olyan szállítási csomaghoz, amely a hordozóeszközre rögzítendő hozzáfűzünk egy ATS-t, ami a szállítási csomag bemeneti időzítését jelzi.

A 6. ábra egy blokk diagram, amely a 300 TS feldolgozóban végrehajtott műveleteket mutatja be akkor, amikor egy digitális interfészen keresztül biztosított valamely szállítási fo-

lyamot egy hordozóeszközre, például egy DVD-re rögzítünk. Amint azt bemutatjuk, a szállítási folyamot digitális adatként, például digitális adás jelekként biztosítjuk egy 600 terminältól a 300 TS feldolgozóhoz. Amint azt az 1. vagy 2. ábrákon mutatjuk, a szállítási folyamot a 600 terminältól a 120 bemenet/kimenet I/F-en, vagy a 140 bemenet/kimenet I/F-en és a 130 MPEG kodeken keresztül biztosítjuk.

A szállítási folyamot egy 602 bit folyam tagolóhoz (parser) biztosítjuk, amely észlel egy PCR (program clock reference, program órajel referencia) csomagot a bemeneti szállítási folyamban. A PCR csomag egy olyan csomag, amelyben az MPEG-2 Systems-ben definiált PCR-t kódoljuk. A PCR csomagok 100 msec-nál kisebb időintervallumokban vannak kódolva. A PCR egy olyan időpontot ábrázol, amikor egy szállítási csomag a fogadó oldalra érkezik, 27 MHz-es pontossággal.

Ezután egy 27 MHz-es 603 PLL a rögzítő/lejátszó egy 27 MHz-es órajelét hozzáigazítja a szállítási folyam PCR-éhez. Egy 604 időbélyeg generálási áramkör egy időbélyeget generál 27 MHz-es órajelek számlálása alapján. Egy 605 blokk mag hozzáfűző áramkör a szállítási csomaghoz ATS-ként hozzáfűz egy időbélyeget, amely azt az időpontot jelzi, amikor a szállítási csomag első bájtját bemenetre tettük a 606 simító pufferbe (smoothing buffer).

A hozzáfűzött ATS-sel rendelkező szállítási csomagot kimenetre tesszük egy 607 terminältól a 606 simító pufferen keresztül a 150 kriptográfiai egységhez, ahol, amint azt később leírjuk, majd dekódoljuk, és azután rögzítjük a 195 hordozóeszközre az (1. ábrán lévő) 190 meghajtón és a (2. ábrán lévő) 210 hordozóeszköz I/F-en keresztül.

A 7. ábra bemutatja, példaként, egy bemeneti szállítási folyamnak a hordozóeszközre való rögzítéséhez végrehajtott műveleteket. A 7A ábra egy bizonyos program (tartalom) által tartalmazott szállítási csomagok bemenetét mutatja be. A 7A ábrán a vízszintes tengely egy idő bázis (time base), amely a szállítási folyam egy idejét jelzi. Ebben a kiviteli példában a bemeneti szállítási folyamban lévő szállítási csomagok szabálytalan időközönként jelennek meg, mint azt a 7A ábrán mutatjuk.

A 7B ábra a 605 blokk mag hozzáfűző áramkör egy kimenetét mutatja be. Ez a 605 blokk mag hozzáfűző áramkör a szállítási csomaghoz hozzáfűz egy ATS-t magában foglaló blokk magot, amely ATS egy szállítási folyamban lévő szállítási csomagok mindegyikének az érkezési idejét jelzi, majd kimenetre tesz egy forrás csomagot. A 7C ábra a hordozóeszközön rögzített forrás csomagokat mutat be. A forrás csomagokat a hordozóeszközre úgy rögzítjük, hogy nincsen helykihagyás az egymást követő csomagok között, amint azt a 7C ábrán mutatjuk. A forrás csomagok ilyen, köztes helykihagyás nélküli elrendezésének köszönhetően a hordozóeszközön lévő rögzítési terület hatékonyan használható.

A 8. ábra a 300 TS feldolgozó egy blokk diagramja, amely egy adat feldolgozó eljárást mutat be egy szállítási folyamnak a 195 hordozóeszközről való beolvasására. Egy szállítási csomagot, amelyet egy kriptográfiai egységben dekódoltunk (amit a későbbiekben fogunk tárgyalni) és amelyhez hozzáfűztünk egy ATS-t, biztosítunk egy 800 terminálról egy 801 blokk mag szétválasztási áramkörhöz, ahol az ATS-t és a szállítási csomagot elkülönítjük egymástól. Biztosítunk egy 804 időzítés generálá-

si áramkört egy időpont kiszámítására a lejátszó egy 27 MHz-es 805 órajelének számlálása alapján.

Megjegyezzük, hogy az első ATS-t mint kezdeti értéket állítjuk be a 804 időzítés generálási áramkörben. Biztosítunk továbbá egy 803 összehasonlítót az ATS összehasonlítására a 804 időzítés generálási áramkörből biztosított valamely aktuális idővel. Biztosítunk ezen kívül egy 802 kimenet vezérlési áramkört a szállítási csomagnak a 130 MPEG kodekhez vagy a digitális 120 bemenet/kimenet I/F-hez való kimenetre tételére akkor, amikor egy a 804 időzítés generálási áramkör által generált időzítés egyenlővé válik az ATS-sel.

A 9. ábra bemutatja bemeneti AV jelek MPEG kódolását a 100 rögzítő/lejátszó 130 MPEG kodekében és a szállítási folyam kódolását a 300 TS feldolgozóban. Nevezetesen a 9. ábra mind az 1. vagy 2. ábrán lévő 130 MPEG kodekben, mind pedig a 300 TS feldolgozóban végrehajtott műveletek egy blokk diagramja. A videó jeleket egy 901 terminálától biztosítjuk egy 902 MPEG videó kódolóhoz.

A 902 MPEG videó kódoló a bemeneti videó jeleket egy MPEG videó folyammá kódolja, és kimenetre teszi az adatot egy 903 videó folyam pufferhez. A 902 MPEG videó kódoló kimenetre tesz ezen kívül hozzáférési egység információt az MPEG videó folyamról egy 908 multiplexelő ütemezőhöz (multiplexing scheduler). A videó folyam „hozzáférési egysége" magában foglalja minden egyes kép egy típusát, kódolt bit mennyiségét és dekódolási időbélyegét. A „kép típus" információ egy I/ P/ B képről, és a „dekódolási időbélyeg" az MPEG-2 Systems-ben definiált információ.

Audió jeleket egy 904 terminálтól biztosítunk egy 905 MPEG audió kódolóhoz. A 905 MPEG audió kódoló egy MPEG audió folyammá kódolja a bemeneti audió jeleket, és kimenetre teszi az adatot egy 906 pufferhez. A 905 MPEG audió kódoló kimenetre tesz ezen kívül hozzáférési egység információt az MPEG audió folyamról a 908 multiplexelő ütemezőhöz. Az audió folyam „hozzáférési egysége" egy audió keret, és a hozzáférési egység információ magában foglalja az egyes audió keretek kódolt bit mennyiségét és dekódolási időbélyegét.

A 908 multiplexelő ütemezőhöz biztosítjuk mind a videó, mind pedig az audió hozzáférési információt, és az vezérli a videó és audió folyamok kódolását a hozzáférési egység információ alapján. A 908 multiplexelő ütemező alkalmaz egy órajelet egy referencia idő generálására 27MHz-es pontossággal, és így meghatározza a csomag kódolás vezérlési információt a szállítási csomag számára a T-STD szerint, ami az MPEG-2-ben definiált virtuális dekódoló modell. A csomag kódolás vezérlési információ magában foglalja egy csomagosítandó folyam típusát és hosszúságát.

Abban az esetben, ha a csomag kódolás vezérlési információ videó csomag, egy 976 kapcsolót annak egy a oldalára állítjuk a csomag kódolás vezérlési információ által kijelölt szállítmány adathosszúságú (payload data length) videó adatnak a 903 videó folyam pufferből való olvasására, és az adatnak egy 909 szállítási csomag kódolóhoz való biztosítására.

Abban az esetben, ha a csomag kódolás vezérlési információ audió csomag, a 976 kapcsolót annak egy b oldalára állítjuk egy kijelölt szállítmány adat hosszúságú audió adatnak a

906 audió folyam pufferből való olvasására és az adatnak a 909 szállítási csomag kódolóhoz való biztosítására.

Abban az esetben, ha a csomag kódolás vezérlési információ PCR csomag, a 909 szállítási csomag kódoló a 908 multiplexelő ütemezőtől biztosított PCR-t szerez meg, és kimenetre teszi a PCR csomagot kívülre annak jelzésére, hogy a csomag kódolás vezérlési információ nem kódol majd csomagokat, nem biztosítunk semmit sem a 909 szállítási csomag kódolóhoz.

Annak a jelzéséhez, hogy a csomag kódolás vezérlési információ nem fog csomagokat kódolni, a 909 szállítási csomag kódoló nem tesz kimenetre egyetlen csomagot sem. Más esetben generálunk szállítási csomagokat a csomag kódolás vezérlési információ alapján, és ezeket kimenetre tesszük. Ezért a 909 szállítási csomag kódoló megszakításokkal tesz kimenetre szállítási csomagokat. Biztosítunk ezen kívül egy 910 érkezési időbélyeg kiszámítót egy olyan időpontot jelző ATS kiszámítására, amikor egy szállítási csomag első bájtja a fogadó oldalhoz érkezik, a 908 multiplexelő ütemezőtől biztosított PCR alapján.

Mivel a 908 multiplexelő ütemezőtől biztosított PCR azt az időpontot jelzi, amelynél az MPEG-2-ben definiált valamely szállítási csomag tizedik bájtja a fogadó oldalra érkezik, azért egy ATS értéke egy olyan időpont, amelynél valamely bájt 10 bájttal van a PCR által jelzett idő előtt.

Egy 911 blokk mag hozzáfűző áramkör egy ATS-t fűz hozzá a 909 szállítási csomag kódolótól kimenetre tett minden egyes csomaghoz. A 911 blokk mag hozzáfűző áramkörtől kimenetre tett valamely ATS-hozzáfűzött szállítási csomagot a 150 kriptográfiai egységhez biztosítjuk egy 912 simító pufferen keresztül,

ahol majd kódoljuk, amint azt a későbbiekben tovább tárgyaljuk, és azután a 195 hordozóeszközön eltároljuk.

A 195 hordozóeszközön való tároláshoz az ATS-hozzáfűzött szállítási csomagokat úgy rendezzük el, hogy nincs közöttük helykihagyás, amint azt a 7C ábrán mutatjuk, és ezután eltároljuk őket a 195 hordozóeszközön, mielőtt kódolásnak vetnénk alá őket a 150 kriptográfiai egységben. Még ha a szállítási csomagokat úgy is rendezzük el, hogy nincs közöttük helykihagyás, az egyes csomagokhoz hozzáfűzött ATS-re való hivatkozás lehetővé teszi, hogy vezéreljük a szállítási csomagoknak a fogadó oldalhoz való biztosításának idejét.

Megjegyezzük, hogy az ATS méretét nem rögzítjük 32-biteskent, az egy 24-31 bites tartományba eshet. Minél nagyobb az ATS hosszúsága, annál hosszabb az ATS idő számláló működési ciklusa. Például abban az esetben, amikor az ATS számláló egy bináris számláló, amely ATS számlálási pontossága 27 MHz, egy 24 bit hosszúságú ATS körülbelül 0,6 másodperc múlva fog megjelenni. Ez az időintervallum elég hosszú egy szokásos szállítási folyam számára, mert egy szállítási folyam csomag intervallumát az MPEG-2 maximum 0,1 másodpercnek definiálja. Ennek ellenére az ATS bit hosszúsága lehet 24 bitnél több egy elégséges ráhagyás biztosítása érdekében.

Az ATS bit hosszúságának a fentiek szerinti változtatása által a blokk mag, lévén további adat egy blokk adathoz, konfigurálható néhány típusban. A 10. ábrán a blokk mag példa konfigurációit mutatjuk be. A 10. ábrán mutatott 1. példa egy 32 bit hosszúságú ATS-t használó blokk mag. A 10. ábrán lévő 2. példa egy 30-bites ATS-t és 2-bites másolás vezérlési információt használó blokk mag. A másolás vezérlési információ

azon adat másolásának vezérelt állapotát jelzi, amelyhez a CCI-t hozzáfűztük. Az SCMS és a CGMS (copy generation management system, másolás generálás irányítási rendszer) a legismertebb másolás vezérlési információk. Ezek a másolás vezérlési információk jelzik, hogy az az adat, amelyhez hozzáfűztük a másolás vezérlési információt korlátlanul másolható (szabadon másolható), az adat másolását csak egyetlen generáláshoz engedélyezzük (one-generation-copy-allowed, egy generálásig másolható) vagy megtiltjuk az adat másolását (nem másolható).

A 10. ábrán mutatott 3. példa egy 24-bites ATS-t, 2-bites CCI-t és 6-bites más információt használó blokk mag. A más információt változatos fajtájú információk közül választhatjuk ki, ilyen például egy Macrovision ki/be működését jelző információ, ami egy másolás vezérlési mechanizmus analóg videó adathoz, amikor a blokk mag adatot valamely analóg formában tesszük kimenetre.

Az 1. vagy 2. ábrán bemutatott rögzítő/lejátszó kioszt a rendszer által tartalmazott minden egyes másik rögzítő/lejátszónak egy mester kulcsot, amely adatnak a hordozóeszközre való rögzítéséhez vagy adatnak a hordozóeszközről való lejátszásához szükséges, amint azt a következőkben leírjuk. A 11. ábra a kulcs kiosztást mutatja be a rögzítő/lejátszóban, egy fa-struktúrájú rögzítési rendszerben. A 11. ábra alján mutatott számok 0-tól 15-ig különálló rögzítő/lejátszókat jelölnek. Vagyis a 11. ábrán a fa struktúra minden egyes levele az egyes rögzítő/lejátszóknak felel meg (amelyekre a következőkben „eszközként" fogunk hivatkozni az alkalmas helyeken).

A létrehozás közben (vagyis szállításkor) 0-tól 15-ig minden egyes eszközben tárolunk egy csomópont kulcsot, amelyet egy csomóponthoz rendelünk hozzá a saját levelétől egy gyökérhez, valamint egy levél kulcsot minden egyes levélhez egy előre meghatározott kezdeti fában. A 11. ábrán a következő legalacsonyabb részletben „K0000"-tól „K1111"-ig rendeljük hozzá a levél kulcsokat a 0-15. eszközökhöz, ebben a sorrendben, és a legmagasabb csomópontnál lévő „KR"-től a legalsó csomópontoknál lévő „K1111"-ig vannak a csomópont kulcsok.

A 11. ábrán mutatott fa struktúrában például a 0. eszköz egy K0000 levél kulcsot, valamint a K000, K00, K0 és KR csomópont kulcsokat birtokolja. Az 5. eszköz egy K0101 levél kulcsot, valamint a K010, K01, K0 és KR csomópont kulcsokat birtokolja. A 15. eszköz egy K1111 levél kulcsot, valamint a K111, K11, K1 és KR csomópont kulcsokat birtokolja. Megjegyezzük, hogy a 11. ábrán mutatott fa csak 16 eszközt foglal magában 0-tól 15-ig 4 szinten elhelyezve, és a fa vízszintes szimmetriában jól kiegyensúlyozott, de tartalmazhat több benne elhelyezett eszközt is, és a szintek száma a fa részeiként változhat.

A 11. ábrán bemutatott fa struktúra által tartalmazott rögzítő/lejátszók (eszközök) a rögzítő/lejátszók változatos típusait foglalhatják magukban, amelyek változatos hordozóeszközöket, például DVD-t, CD-t, MD-t, memória lapot (memory stick) (védjegy) stb. használhatnak. Továbbá változatos alkalmazás szolgáltatások létezhetnek egymás mellett a fa struktúrában. A 11. ábrán bemutatott kulcs kiosztási rendszert alkalmazzuk, miközben az ilyen különböző eszközök és alkalmazások egymás mellett létezhetnek.

Abban a rendszerben, amelyben az ilyen eszközök és alkalmazások léteznek egymás mellett, a fa egy részletét, amelyet a 11. ábrán egy szaggatott vonallal körberajzolva mutatunk és a 0., 1., 2. és 3. eszközöket foglalja magában, egy csoportként állítjuk be, amelyben az eszközök ugyanazt a hordozóeszközt használják. Például a körberajzolt csoport által tartalmazott eszközök mindegyike egy tartalom szolgáltatótól küldött kódolt közös tartalmat vagy egy közös mester kulcsot fogad, vagy egy kódolt tartalom-díj fizetési (content-fee payment) adatot tesz kimenetre a szolgáltatóhoz vagy egy díjintéző hivatalhoz (settlement institution). A tartalom szolgáltató, intéző hivatal vagy egy intézet az egyes eszközökkel való kommunikáláshoz kollektív módon küld adatot a bekarikázott részlethez a 11. ábrán, vagyis egy csoportként a 0., 1., 2. és 3. eszközökhöz. A 11. ábrán bemutatott fában egynél több ilyen csomópont létezik.

Megjegyezzük, hogy a csomópont kulcs és a levél kulcs kollektív módon kezelhető egy bizonyos kulcs kezelési központ által vagy az egyes csoportok által, beleértve a szolgáltatót, intéző hivatalt stb. is, amelyek változatos adat kommunikációt folytatnak az egyes csoportokkal. Ha ezeket a csomópont és levél kulcsokat például felfedik, azokat a kulcs kezelési központ, szolgáltató, intéző hivatal stb. megújítja.

A 11. ábrán mutatott fa struktúrában az egy csoport által tartalmazott négy, 0., 1., 2. és 3. eszköz K00, K0 és KR közös kulcsokat birtokolnak csomópont kulcsokként. A csomópont kulcsok ezen közös használatának köszönhetően például egy közös mester kulcs szolgáltatható csak a 0., 1., 2. és 3. eszközöknek. Például magának a közösen birtokolt K00 csomópont kulcs-

nak mester kulcsként való beállítása által csak a 0., 1., 2. és 3. eszközök számára lehetséges egy közös mester kulcs beállítása bármely más új kulcs fogadása nélkül. Ezen kívül a 0., 1., 2. és 3. eszközökhöz egy olyan Enc(K00, Kmaster) értéknek egy hálózaton keresztüli vagy egy hordozóeszközön tároltként való kiosztása által, amely értéket egy új Kmaster mester kulcsnak a K00 csomópont kulccsal való kódolásával kapunk meg, csak a 0., 1., 2. és 3. eszközök elemezhetik ki az Enc(K00, Kmaster) értéket az eszközök mindegyike által birtokolt közös K00 csomópont kulccsal a Kmaster mester kulcs megszerzéséhez. Megjegyezzük, hogy az Enc(Ka, Kb) egy olyan adat, amelyet Kb-nak Ka-val való kódolásából származtatunk.

Ha valamely t időpontban kiderült, hogy például a 3. eszköz által birtokolt K0011, K001, K00, K0 és KR kulcsokat támadók (hacker) elemezték és felfedték, szükségessé válik a 3. eszköznek a lekapcsolása a rendszerről annak érdekében, hogy azután megvédjük egy rendszer (a 0., 1., 2. és 3. eszközöket tartalmazó csoport) irányába és az onnan átvitt adatokat. Evégett a K001, K00, K0 és KR csomópont kulcsokat le kell cserélnünk új K(t)001, K(t)00, K(t)0 és K(t)R kulcsokra ebben a sorrendben, és az új kulcsokat át kell adnunk a 0., 1. és 2. eszközöknek. Megjegyezzük, hogy a K(t)aaa egy megújított változata egy Kaaa kulcsnak egy t generálásban.

A következőkben a megújított kulcs kiosztását írjuk le. Egy kulcsot azáltal újítunk meg, hogy egy kulcs megújítási blokknak nevezett blokk adatokból álló táblázatot, amint azt a 12A ábrán mutatjuk, biztosítunk a 0., 1. és 2. eszközök mindegyikéhez egy hálózaton keresztül, vagy azt egy hordozóeszközön tároljuk.

Amint az a 12A ábrán látható, a kulcs megújítási blokkot egy blokk adatként alakítjuk ki, amely egy olyan adat struktúrával rendelkezik, amit csak egy olyan eszköz újíthat meg, amelynek szüksége van valamely csomópont kulcs megújítására. A 12A ábrán bemutatott példa egy blokk adat, amelyet a t generálás valamely megújított csomópont kulcsának a 11. ábrán bemutatott fa struktúra által tartalmazott 0., 1. és 2. eszközökhöz való kiosztása érdekében alakítottunk ki. Amint az a 11. ábráról leolvasható, a 0. és 1. eszközöknek a K(t)00, K(t)0 és K(t)R megújított csomópont kulcsokra van szükségük, míg a 2. eszköznek a K(t)001, K(t)00, K(t)0 és K(t)R megújított csomópont kulcsokra van szüksége.

Amint az a 12A ábrán látható, a KRB kódolási kulcsok valamely sokaságát foglalja magában. A legalsó kódolási kulcs az Enc(K0010, K(t)001). Ez egy K(t)001 megújított csomópont kulcs, amit a 2. eszköz egy K0010 levél kulcsával kódoltunk. A 2. eszköz dekódolni tudja ezt a kódolási kulcsot a saját levél kulcsával a K(t)001 megszerzéséhez. Ezen kívül a 2. eszköz dekódolni tud egy Enc(K(t)001, K(t)00) kódolási kulcsot is a következő legalsó szinten a dekódolás által megszerzett K(t)001-gyel, ezáltal megszerez egy K(t)001 megújított csomópont kulcsot. Ezután a 2. eszköz dekódol egy Enc(K(t)00, K(t)0) kódolási kulcsot a következő legfelső szinten a 12A ábrán egy K(t)0 megújított csomópont kulcs megszerzéséhez és dekódolja az Enc(K(t)0, K(t)R) kódolási kulcsot a legfelső szinten a 12A ábrán egy K(t)R megújított csomópont kulcs megszerzéséhez. Másrészről, a 0. és 1. eszközök esetében egy K000 csomópont kulcsot nem kell megújítanunk, viszont a K(t)00, K(t)0 és K(t)R csomópont kulcsok megújítandóak. A 0. és 1. eszközök de-

kódolnak egy Enc(K000, K(t)00) kódolási kulcsot egy harmadik legfelső szinten a 12A ábrán egy K(t)00 megújított csomópont kulcs megszerzéséhez. Ezt követően a 0. és 1. eszközök dekódolnak egy Enc(K(t)00, K(t)0) kódolási kulcsot a második legfelső szinten a 12A ábrán egy K(t)0 megújított csomópont kulcs megszerzéséhez, és dekódolnak egy Enc(K(t)0, K(t)R) kódolási kulcsot a legfelső szinten a 12A ábrán egy K(t)R megújított csomópont kulcs megszerzéséhez. Ily módon a 0., 1. és 2. eszközök megszerezhetik a K(t)00, K(t)0 és K(t)R megújított csomópont kulcsokat. Megjegyezzük, hogy a 12A ábrán lévő „Index" egy csomópont kulcs vagy levél kulcs egy abszolút címét mutatja, amelyet dekódolási kulcsként használunk.

A 11. ábrán mutatott fa struktúra legfelső szintjén lévő K0 és KR csomópont kulcsokat nem kell megújítanunk. Abban az esetben, amikor csak a K00 csomópont kulcsot kell megújítanunk, a 12B ábrán lévő kulcs megújítási blokk használata lehetővé teszi a K(t)00 megújított csomópont kulcs kiosztását a 0., 1. és 2. eszközöknek.

A 12B ábrán bemutatott KRB használható például egy új mester kulcs kiosztására egy meghatározott csoportban való közös használatra. Szűkebb értelemben, a 11. ábrán a szaggatott vonallal körülvett csoportban a 0., 1., 2. és 3. eszközök egy bizonyos hordozóeszközt használnak, és szükségük van egy új, közös K(t)master mester kulcsra. Ekkor a 0., 1., 2. és 3. eszközök számára közös K00 csomópont kulcs megújításából származtatott valamely K(t)00 csomópont kulcsot használunk az új közös K(t)master mester kulcs kódolásából származtatott Enc(K(t), K(t)master) adatnak a 12B ábrán bemutatott KRB-vel együtt való kiosztására. Ezzel a kiosztással kioszthatunk

olyan adatot, amely egy másik csoport által tartalmazott eszközben, például a 4. eszközben, nem dekódolható.

Vagyis a 0., 1. és 2. eszközök megszerezhetik a K(t)master mester kulcsot egy t időpontban azáltal, hogy a KRB feldolgozásával megszerzett K(t)00-val dekódolják a kódolt adatot.

A 13. ábra bemutatja az eljárást egy K(t)master mester kulcs megszerzéséhez a t időpontban a 0. eszköz által, amely már megszerzett egy Enc(K(t)00, K(t)master) adatot, amit egy új közös K(t)master mester kulcsnak a K(t)00-val való kódolásából és a 12B ábrán mutatott KRB-ből származtatunk.

Amint azt a 13. ábrán mutatjuk, a 0. eszköz egy K(t)00 csomópont kulcsot generál a KRB-nek a fentihez hasonló feldolgozása által a KRB-ből egy t időpontban (generálás, amelyben a KRB-t eltároltuk) és egy önmagában előre eltárolt K000 csomópont kulcs által. Továbbá a 0. eszköz dekódolja a K(t)master megújított mester kulcsot a dekódolt megújított K(t)00 csomópont kulccsal, kódolja azt a saját K0000 levél kulcsával későbbi használatra, majd eltárolja. Megjegyezzük, hogy abban az esetben, amikor a 0. eszköz biztonságosan el tudja tárolni a K(t)master megújított mester kulcsot, nem szükséges annak a K0000 levél kulccsal való kódolása.

A megújított mester kulcs megszerzését leírjuk a 14. ábrán bemutatott folyamatábrára való hivatkozással is. Itt feltesszük, hogy a rögzítő/lejátszónak kiadtuk a K(C)master legutolsó mester kulcsot a szállítás időpontjában, és biztonságosan eltárolta azt a saját memóriájában (pontosabban a saját levél kulcsával kódoltan).

Amikor a hordozóeszköz, amelyben eltároltuk a K(n)master megújított mester kulcsot és a KRB-t, a rögzítő/lejátszóban van beállítva, az utóbbi beolvassa először az S1401 lépésben a K(n)master mester kulcs n generálási számát (generation number) (amelyre a továbbiakban „Generálás #n elő-rögzítési generálási információként" fogunk hivatkozni (pre-recording generation information Generation #n)) a hordozóeszközből. A hordozóeszközön előre eltároltuk egy K(n)master mester kulcs n generálási számát. Ezután a rögzítő/lejátszó kiolvassa a C kódolt mester kulcsot a saját memóriájából. Az S1402 lépésben összehasonlítja a saját kódolt mester kulcsának a c generálási számát és a Generálás#n elő-rögzítési generálási információ által jelzett n generálást (generation n) annak eldöntésére, hogy melyik a fiatalabb vagy idősebb, a c vagy az n generálás.

Ha rögzítő/lejátszó az S1402 lépésben olyan döntést hozott, hogy a Generálás #n elő-rögzítési generálási információ által jelzett n generálás nem fiatalabb, mint a saját memóriájában tárolt C kódolt mester kulcs c generálása, vagyis, ha a memóriában tárolt C kódolt mester kulcs c generálása ugyanaz vagy idősebb, mint a Generálás #n elő-rögzítési generálási információ által jelzett n generálás, akkor a rögzítő/lejátszó átugorja az S1403-S1408 lépéseket, és kilép a mester kulcs megújítási eljárásból. Ebben az esetben, mivel a rögzítő/lejátszó memóriájában tárolt K(C)master mester kulcs (kódolt C mester kulcs) megújítása nem szükséges, azért a megújítást nem végezzük el.

Másrészről, ha a rögzítő/lejátszó az S1402 lépésben olyan döntést hozott, hogy a Generálás #n elő-rögzítési generálási információ által jelzett n generálás fiatalabb, mint a memóri-

ában tárolt C kódolt mester kulcs c generálása, vagyis, ha a memóriában tárolt C kódolt mester kulcs c generálása idősebb, mint a Generálás #n elő-rögzítési generálási információ által jelzett n generálás, akkor a rögzítő/lejátszó az S1403 lépésre halad, ahol majd beolvas egy kulcs megújítási blokkot a hordozóeszközről.

Az S1404 lépésben a rögzítő/lejátszó kiszámít a 00 csomópont számára egy a Generálás #n elő-rögzítési generálási információ által jelölt időpontban (a 13. ábrán a t időpontban) egy K(t)00 kulcsot az S1403 lépésben beolvasott KRB-ből, levél kulcsból (K0000 a 11. ábrán lévő 0. eszköz esetén) és csomópont kulcsokból (K000, K00, ... a 11. ábrán lévő 0. eszköz esetén), amelyeket a memóriájában tárol.

Az S1405 lépésben megvizsgáljuk, hogy a K(t)00-t az S1404 lépésben szereztük-e meg. Ha nem, az azt jelenti, hogy a rögzítő/lejátszót abban az időpontban eltávolítottuk a csoportból a fa-struktúrában, és ezért a rögzítő/lejátszó átugorja az S1406-S1408 lépéseket, és kilép a mester kulcs megújítási eljárásból.

Ha megszereztük K(t)00-t, a rögzítő/lejátszó az S1406 lépésre halad, ahol beolvas majd egy értéket, amit a mester kulcsnak a t időpontban az Enc(K(t)00, K(t)master) kulccsal való kódolásából származtatunk, nevezetesen a hordozóeszközről beolvasott K(t)00-t. Az S1407 lépésben a rögzítő/lejátszó kiszámítja a K(t)master-t a K(t)00-val kódolt érték dekódolása által.

Az S1408 lépésben a rögzítő/lejátszó kódolja a K(t)master-t a saját levél kulcsával (K0000 a 11. ábrán lévő

0. eszköz esetében), és eltárolja a memóriába. Itt a rögzítő/lejátszó kilép a mester kulcs megújítási eljárásból.

Emlékeztetnünk kell itt arra, hogy a mester kulcsot a 0 időponttól (generálástól) emelkedő sorrendben használjuk, de a rendszerben lévő eszközök mindegyike előnyösen képes megszerezni egy idősebb generálású mester kulcsot egy új generálású mester kulcsból való kiszámítása által. Vagyis a rögzítő/lejátszónak birtokolnia kell egy f egyirányú függvényt (one-way function), és egy mester kulcsot úgy kell generálnia egy vizsgált generálásban, hogy alkalmazza a saját mester kulcsát az f egyirányú függvényhez valahányszor a mester kulcs generálása és egy szükséges mester kulcs generálása közötti különbségnek megfelelően.

Még szűkebb értelemben, például abban az esetben, amikor a rögzítő/lejátszóban tárolt MK mester kulcs generálása i+1, miközben valamely adat lejátszásához szükséges MK mester kulcs (amit az adat rögzítésénél használtunk) generálása i-1, a rögzítő/lejátszó egy K(i-1)master mester kulcsot generál oly módon, hogy az f egyirányú függvényt kétszer használja és kiszámítja f(f(K(i+1)master))-t.

Abban az esetben továbbá, amikor a rögzítő/lejátszóban tárolt mester kulcs generálása i+1, miközben a szükséges mester kulcs generálása i-2, a rögzítő/lejátszó egy K(i-2)master mester kulcsot generál oly módon, hogy az f egyirányú függvényt kétszer használja és kiszámítja f(f(f(K(i+1)master)))-t.

Az egyirányú függvény lehet például egy hasító (hash) függvény. Speciálisan, a hasító függvény lehet például MD5 (message digest 5), SHA - 1 (secure hash algorithm - 1) vagy hasonló. Egy kulcs kibocsátó intézetnek meg kell határoznia

azokat a K(0)master, K(1)master, K(2)master, ..., K(n)master mester kulcsokat, amelyekkel egy az aktuális generálásnál idősebb generálást elő-generálhatunk ezeknek az egyirányú függvényeknek a használatával. Vagyis legelőször az N generálás egy K(N)master mester kulcsát be kell állítanunk és az egyirányú függvényt egyszer a K(N)master mester kulcsra kell alkalmaznunk, ezáltal generálva a megelőző generálások K(N-1)master, K(N-2)master, ..., K(1)master, K(0)master mester kulcsait, egyiket a másik után. A mester kulcsokat egymás után kell használnunk, kezdve a legkorábbi generálás K(0)master mester kulcsával. Megjegyezzük, hogy feltesszük azt, hogy az aktuális generálásnál idősebb generálás mester kulcsának a generálásához használt egyirányú függvényt beállítottuk az összes rögzítő/lejátszóban.

Az egyirányú függvényként továbbá használhatjuk például a nyilvános kulcsú kriptográfiát. ebben az esetben a kulcs kibocsátó intézetnek birtokolnia kell egy privát kulcsot, amely a nyilvános kulcsú kriptográfián alapul, és a lejátszók mindegyike számára ki kell bocsátania egy nyilvános kulcsot, amely megfelel a privát kulcsnak. A kulcs kibocsátó intézetnek be kell állítania egy 0-adik generálású K(0)master mester kulcsot, és a K(0)master-rel kezdődő mester kulcsokat kell használnia. Vagyis amikor a kulcs kibocsátó intézetnek szüksége van egy olyan K(i)master mester kulcsra, amely fiatalabb, mint az első generálású mester kulcs, a K(i)master-t egy generálással megelőző valamely K(i-1)master mester kulcsot alakít át a K(i)master mester kulcs generálására annak használatához. Ily módon a kulcs kibocsátó intézetnek nem kell elő-generálnia egy N-edik generálású mester kulcsot az egyirányú függvény haszná-

latával. Az ilyen módú kulcs generálással elméletileg lehetséges egy mester kulcs generálása az összes generálás fölött. Megjegyezzük, hogy ha a rögzítő/lejátszó rendelkezik mester kulccsal egy generáláshoz, képes lesz a mester kulcs átalakítására a nyilvános kulccsal mester kulcsok megszerzésére olyan generálásokhoz, amelyek idősebbek, mint az a bizonyos generálás.

A következőkben a rögzítő/lejátszó műveleteit írjuk le valamely tartalomnak a saját hordozóeszközére való rögzítéséhez, a 15. ábrán bemutatott folyamatábrára való hivatkozással.

A tartalom adatot valamely generálás egy mester kulcsával kódoljuk és kiosztjuk a tartalom szolgáltatótól a rögzítő/lejátszók mindegyikéhez egy hálózaton vagy egy hordozóeszközön keresztül.

Először az S1501 lépésben rögzítő/lejátszó beolvassa a Generálás #n elő-rögzítési generálási információt a hordozóeszközről. Megszerzi a saját memóriájában tárolt C kódolt mester kulcs c generálását. Az S1502 lépésben a rögzítő/lejátszó elvégez egy összehasonlítást a C kódolt mester kulcs c generálása és a G#n elő-rögzítési generálási információ által jelzett n generálás között annak eldöntésére, hogy melyik fiatalabb vagy idősebb, a c vagy az n generálás.

Ha az S1502 lépésben a döntés eredménye az, hogy a memóriában tárolt C kódolt mester kulcs c generálása nem fiatalabb, mint a Generálás#n elő-rögzítési generálási információ által jelzett n generálás, nevezetesen, ha a memóriában tárolt C kódolt mester kulcs c generálása idősebb, mint a Generálás#n elő-rögzítési generálási információ által jelzett n generálás,

akkor a rögzítő/lejátszó átugorja az S1503 lépést, vagyis kilép az eljárásból anélkül, hogy rögzítenénk a tartalom adatot.

Másrészről, ha az S1502 lépésben a döntés eredmény az, hogy a rögzítő/lejátszó memóriájában tárolt C kódolt mester kulcs c generálása fiatalabb, mint a Generálás#n elő-rögzítési generálási információ által jelzett n generálás, nevezetesen, ha memóriában tárolt C kódolt mester kulcs c generálása ugyanaz, vagy fiatalabb, mint a Generálás#n elő-rögzítési generálási információ által jelzett n generálás, akkor a rögzítő/lejátszó az S1503 lépésre halad, ahol a tartalom adatot rögzíti.

A következőkben egy eljárást írunk le valamely adat tartalomnak a generálás-irányított mester kulccsal való kódolásához és az adatnak a hordozóeszközön való eltárolásához a rögzítő/lejátszóban. Megjegyezzük, hogy egy blokk kulcsot egy generálás-irányított mester kulcsot magában foglaló adat alapján generálunk, és valamely adat tartalmat, amelyet egy szállítási folyamból alkotunk, amint azt megelőzően leírtuk, a blokk kulccsal kódolunk és egy hordozóeszközön tárolunk el, amint azt alább leírjuk. Ezen kívül két példát fogunk tekinteni: az egyik olyan, hogy egy rögzítő/lejátszó által egy hordozóeszközre rögzített adatot lejátszhatunk egy másik lejátszóban; a másik pedig olyan, hogy az ilyen adatot nem játszhatjuk le egy másik lejátszóban.

A leírást a 16. és 17. ábrákon lévő blokk diagramokra és a 18. ábrán bemutatott folyamatábrára való hivatkozással végezzük el. Itt feltesszük, hogy a hordozóeszköz például egy optikai lemez. Ebben a kiviteli példában, megakadályozandó az adatnak bitenkénti másolását a hordozóeszközön, a hordozóesz-

köz számára egyedi azonosítási információként egy lemez ID-vel befolyásolunk egy kulcsot az adat kódolásához.

Először a 16. és 17. ábrákon lévő blokk diagramokra hivatkozva a 150 kriptográfiai egység általi adat kódolást körvonalazzuk.

Egy 1600 rögzítő/lejátszó beolvas a saját 180 memóriájában (lásd 1. és 2. ábrák) tárolt 1601 mester kulcsot, egy 1631 eszköz ID-t eszköz azonosítóként, valamint egy 1632 eszköz-egyértelmű kulcsot. Az 1601 mester kulcs egy engedéllyel rendelkező rögzítő/lejátszóban tárolt privát kulcs. Ez generálásirányított, amint azt az előzőekben leírtuk, és rendelkezik egy vele korrelációban lévő generálási számmal. A mester kulcs egy olyan kulcs, amely közös rögzítő/lejátszók valamely sokasága számára, nevezetesen például a 11. ábrán bemutatott szaggatott vonalú kör által közrezárt eszközök számára. Az eszköz ID egy azonosító az 1600 rögzítő/lejátszó számára. Ez egy olyan azonosító, például egy sorozat szám, amelyet előre eltárolunk a rögzítő/lejátszóban. Az eszköz ID lehet nyílt. Az eszköz-egyértelmű kulcs egy privát kulcs, amely egyedi az 1600 rögzítő/lejátszó számára. Úgy állítjuk be előre, hogy rögzítő/lejátszónként változzon. Ezeket a kulcsokat az 1600 rögzítő/lejátszó memóriájában tároljuk.

Az 1600 rögzítő/lejátszó ellenőrzi, hogy az 1603 lemez ID-t mint azonosítási információt rögzítettük-e már az 1620 hordozóeszközre, ami például egy optikai lemez. Ha az 1603 lemez ID-t megtaláltuk ott rögzítve, akkor az 1600 rögzítő/lejátszó beolvassa azt (mint a 16. ábrán). Ha nem, az 1600 rögzítő/lejátszó generál egy 1701 lemez ID-t véletlenszerűen vagy például a 150 kriptográfiai egység általi valamely előre

meghatározott véletlenszám-generálási eljárással, majd azt az optikai lemezre rögzíti (mint a 17. ábrán). Egyetlen lemez számára csak egyetlen 1603 lemez ID-nek kell elérhetőnek lennie. Tehát eltárolhatjuk azt a lemez valamely bevezető területén vagy hasonlón.

Ezután az 1600 rögzítő/lejátszó egy lemez-egyértelmű kulcsot generál a mester kulcsból és a lemez ID-ből (amint azt az „1602" hivatkozási jelnél jelöljük). Amint azt a 19. ábrán mutatjuk, a lemez-egyértelmű kulcsot a következő két eljárás valamelyikével generáljuk. Nevezetesen, az eljárások egyikében (1. példa) a mester kulcsot és a lemez ID-t egy blokk kódolási függvényt használó hasító függvénybe helyezzük el (placed in), és az elhelyezés valamely eredményét használjuk. A másik eljárásban (2. példa) adatot, amelyet a mester kulcs és lemez ID bitenkénti kombinációjából származtatunk, helyezünk el az FIPS 180 - 1-ben definiált valamely SHA - 1 hasító függvényben egy 160-bites kimenet biztosítására, és a 160-bites kimenetből csak egy szükséges hosszúságú adatot használunk.

Ezután minden egyes rekordhoz egy egyedi cím kulcsot generálunk (amelyet „1604" hivatkozási jelként jelölünk) véletlenszerűen, vagy a 150 kriptográfiai egységben (lásd 1. vagy 2. ábra) egy előre meghatározott véletlenszám-generálással, és az 1620 lemezre rögzítjük.

Továbbá beállítunk egy jelzőt (amelyet az „1633" hivatkozási jelnél jelölünk), nevezetesen egy 1633 lejátszó korlátozás jelzőt, amely jelzi, hogy a cím (adat) egy olyan adat, amelyet csak olyan rögzítő/lejátszóban játszhatunk le, amelyben azt rögzítettük (lejátszó korlátozás be van állítva), vagy egy olyan adat, amelyet bármely más rögzítő/lejátszóban is le-

játszhatunk (lejátszó korlátozás nincs beállítva), és rögzítjük azt (amint azt az „1635" hivatkozási jelnél jelöljük) egy 1620 lemezre. Ezen kívül az 1600 rögzítő/lejátszó kiveszi az eszköz ID-t eszköz azonosítási információként (amint azt az „1631" hivatkozási jelnél jelöljük) és az 1620 lemezre rögzíti (amint azt az „1634" hivatkozási jelnél jelöljük).

Ezen felül az 1600 rögzítő/lejátszó megszerzi az általa használt mester kulcs generálási számát, nevezetesen a saját memóriájában tárolt mester kulcs generálási számát (Generálás#n rögzítési generálási számát, amint azt az „1650" hivatkozási jelnél jelöljük), és eltárolja azt az 1620 hordozóeszközön (lemezen) egy 1651 rögzítési generálási számként.

A lemezben biztosítunk egy adat kezelési fájlt, amelyben arról tárolunk információt, hogy az adatból milyen címet alakítunk ki, és hogy honnan származik az adat, valamint amely tárolhat egy 1605 cím kulcsot, 1635 lejátszó korlátozás jelzőt, 1634 eszköz ID-t és egy 1651 mester kulcs generálási számot (G#n rögzítési generálási számot).

Megjegyezzük, hogy az 1620 hordozóeszközön előre eltárolunk egy elő-rögzítési generálási számot, és csak olyan tartalmat játszhatunk le, amelyet az elő-generálási számnál fiatalabb vagy vele megegyező generálású mester kulccsal kódoltunk, és amelyet az 1620 hordozóeszközön eltároltunk. Ezt a rendszert tovább tárgyaljuk a későbbiekben az adat lejátszás leírásánál.

Ezután egy cím-egyértelmű kulcsot generálunk vagy a lemez-egyértelmű kulcs, cím kulcs és eszköz ID valamely kombinációjából, vagy pedig a lemez-egyértelmű kulcs, cím kulcs és eszköz-egyértelmű kulcs valamely kombinációjából.

Nevezetesen abban az esetben, amikor a lejátszó korlátozás nincs beállítva, a cím-egyértelmű kulcsot a lemez-egyértelmű kulcsból, cím kulcsból és eszköz ID-ből generáljuk. Abban az esetben viszont, amikor a lejátszó korlátozás be van állítva, a cím-egyértelmű kulcsot a lemez-egyértelmű kulcsból, cím kulcsból és eszköz-egyértelmű kulcsból generáljuk.

Még szűkebb értelemben, a cím-egyértelmű kulcsot oly módon generáljuk, mint vagy az 1. példában, vagy a 2. példában a 21. ábrán. Az 1. példában egy cím kulcsot, lemez-egyértelmű kulcsot és vagy egy eszköz ID-t (amikor a lejátszó korlátozás nincs beállítva), vagy egy eszköz-egyértelmű kulcsot (amikor a lejátszó korlátozás be van állítva) helyezünk egy blokk kódoláson alapuló hasító függvénybe, és az elhelyezés valamely eredményét használjuk cím-egyértelmű kulcsként. A 2. példában egy mester kulcs, lemez ID és vagy egy eszköz ID (amikor a lejátszó korlátozás nincs beállítva), vagy pedig egy eszköz-egyértelmű kulcs (amikor a lejátszó korlátozás be van állítva) bitenkénti kombinációja által generált adatot helyezünk el az FIPS 180 - 1-ben definiált valamely SHA - 1 hasító függvényben, és az elhelyezés által eredményezett 160-bites kimenet egy szükséges adat hosszúságát használjuk cím-egyértelmű kulcsként.

A fentiekben egy lemez-egyértelmű kulcsot generálunk egy mester kulcsból és lemez ID-ből, és ezután egy cím-egyértelmű kulcsot generálunk a lemez-egyértelmű kulcsból, cím kulcsból és eszköz ID-ből vagy a cím kulcsból és az eszköz-egyértelmű kulcsból. Megjegyezzük viszont, hogy a cím-egyértelmű kulcsot generálhatjuk közvetlenül a mester kulcsból, lemez ID-ből, cím kulcsból és eszköz ID-ből vagy eszköz-egyértelmű kulcsból a

lemez-egyértelmű kulcs használata nélkül, illetve a cím-egyértelmű kulccsal ekvivalens kulcsot generálhatunk a mester kulcsból, lemez ID-ből és egy eszköz ID-ből (amikor a lejátszó korlátozás nincs beállítva) vagy egy eszköz-egyértelmű kulcsból (amikor a lejátszó korlátozás be van állítva) a cím kulcs használata nélkül.

Emlékeztetnünk kell arra, hogy abban az esetben, amikor például a fenti 5CDTCP szabványban definiált átviteli formátumok egyikét használjuk, az adatot néhány esetben MPEG-2 TS csomagokként visszük át. Például amikor egy műholdas adást (satellite broadcast) fogadó beállított tető doboz (STB - set top box) az adást egy rögzítőnek továbbítja az 5CDTCP átviteli formátum használata nélkül, az STB-nek előnyösen az IEEE 1394 soros adat sínen is a műholdas sugárzás átviteli útvonalon továbbított MPEG-2 TS csomagokat kell továbbítania, mivel nem követeljük meg az adat konverziót.

Az 1600 rögzítő/lejátszó a rögzítendő tartalom adatot TS csomagok formájában fogadja, és az előzőekben említett 300 TS feldolgozó minden egyes TS csomaghoz hozzáfűz egy ATS-t, ami az az időpont, amikor a TS csomagot fogadtuk. Megjegyezzük, hogy csakúgy, mint a fentiekben, a blokk adathoz hozzáfűzött valamely blokk mag állhat egy ATS, másolás vezérlési információ és más információ valamely kombinációjából.

A blokk adat egy blokkjának (az 5. ábra felső részletében mutatjuk) a kialakításához egymás mellé rendezünk el X számú (például X=32) olyan TS csomagot, amelyek mindegyikéhez hozzáfűztünk egy ATS-t. Amint azt a 16. és 17. ábrák alsó részleteiben mutatjuk, a kódoláshoz biztosított blokk adat vezető részletében lévő első négy bájtot elkülönítjük (egy 1608 kivá-

lasztóban (selector)) egy 32-bites ATS-t magában foglaló blokk mag kimenetre tételére. A blokk magból és a megelőzően generált cím-egyértelmű kulcsból egy blokk kulcsot generálunk (amit az „1607" hivatkozási jelnél jelölünk), ami egy kódolási kulcs a blokkban lévő adat számára.

A 22. ábra példát mutat a blokk kulcs generálásra. A 22. ábra két példát mutat egy 64-bites blokk kulcs generálására egy 32-bites blokk magból és egy 64-bites cím-egyértelmű kulcsból.

A 22. ábra felső felében bemutatott 1. példában egy olyan kódolási függvényt használunk, amely kulcs hosszúsága 64 bit, és a bemenet illetve a kimenet 64-bites, ebben a sorrendben. Ehhez a kódolási függvényhez egy cím-egyértelmű kulcsot veszünk kulcsként, egy blokk mag és egy 32-bites konstans valamely kombinációját helyezzük el a kódolási függvényben, és az elhelyezés egy eredményét vesszük blokk kulcsnak.

A 2. példa az FIPS 180 - 1-ben definiált SHA - 1 hasító függvényt használ. Egy cím-egyértelmű kulcs és blokk mag valamely kombinációját helyezzük el az SHA - 1 hasító függvényben, és egy 160-bites kimenetet 64-bitesre csökkentünk (redukálunk), például csak az alsó 64 bit használata által. A 64 bitet használjuk blokk kulcsként.

A fentiekben a blokk kulcs generálás azon példáit mutattuk be, amelyekben generáltuk a lemez-egyértelmű kulcsot, cím-egyértelmű kulcsot és blokk kulcsot. Ennek ellenére a blokk kulcsot generálhatjuk egy mester kulcsból, lemez ID-ből, cím kulcsból, blokk magból az egyes blokkokhoz és vagy egy eszköz ID-ből (amikor a lejátszó korlátozás nincs beállítva), vagy egy eszköz-egyértelmű kulcsból (amikor a lejátszó korlátozás

be van állítva) anélkül, hogy generálnánk a lemez-egyértelmű kulcsot és cím kulcsot.

Az így generált blokk kulcsot használjuk a blokk adat kódolására. Amint azt a 16. és 17. ábrák alsó részletein mutatjuk, egy blokk magot tartalmazó blokk adat vezető részletében lévő első m bájtot (például m=8) elkülönítjük (az 1608 kiválasztóban) nem kódolandóként, és a bájtokat az (m+1)-ediktől az utolsóig kódoljuk (amint azt az „1609" hivatkozási jelnél jelöljük). Megjegyezzük, hogy a nem kódolandó m bájt magában foglalja az első négy bájtot blokk magként. A blokk adatnak az 1608 kiválasztóban kiválasztott (m+1)-edik és az azt követő bájtjait kódoljuk (amint azt az „1609" hivatkozási jelnél jelöljük) a 150 kriptográfiai egységben előre beállított valamely kódolási algoritmus szerint. A kódolási algoritmus lehet például az FIPS 46 - 2-ben definiált DES (Data Encrypting Standard - adat kódolási szabvány).

Amikor a kódolási algoritmusban használt blokk hosszúság (bemeneti/kimeneti adat méret) 8 bájt, mint a DES-ben, az (m+1)-edik és az azt követő bájtokat magában foglaló teljes blokk adat töredék nélkül kódolható például azáltal, hogy X-et 32-nek, és m-et a 8 valamely többszörösének vesszük.

Nevezetesen abban az esetben, amikor X számú TS csomagot tárolunk egyetlen blokkban, a kódolási algoritmus bemeneti/kimeneti adat mérete L bájt és n egy tetszőleges természetes szám, az X, m és L meghatározása oly módon, hogy 192*X=m+n*L szükségtelenné teszi bármely töredék feldolgozását.

A blokk adat kódolt (m+1)-edik és azt követő bájtjait kombinálhatjuk a blokk adat kódolatlan első m bájtjával egy

1610 kiválasztó által, és 1612 kódolt tartalomként tároljuk el az 1620 hordozóeszközön.

A fenti műveletekkel a tartalmat blokkonként kódoljuk egy generálás-irányított mester kulcsot és ATS-t magában foglaló blokk magból generált valamely blokk kulccsal, és eltároljuk azt a hordozóeszközön.

Csakúgy, mint a fentiekben, mivel tartalom adatot egy generálás-irányított mester kulccsal kódoljuk és egy hordozóeszközön tároljuk el, azért az adat csak akkor dekódolható, illetve a hordozóeszköz csak akkor játszható le bármely másik rögzítő/lejátszóban, amikor a másik rögzítő/lejátszó generálása legalább ugyanaz, mint azé a rögzítő/lejátszóé, amely a tartalom adatot a hordozóeszközre rögzítette, vagy fiatalabb, mint a tartalom adat rögzítésekor használt mester kulcs generálása.

Amikor a lejátszó korlátozás nincs beállítva, blokk kulcsot egy eszköz ID alapján generálunk. Amikor viszont a lejátszó korlátozás be van állítva, a blokk kulcsot egy eszközegyértelmű kulcs alapján generáljuk. Amikor a lejátszó korlátozás be van állítva, ezeket a kódolt adatokat csak abban a rögzítő/lejátszóban játszhatjuk le, amely az adatokat rögzítette.

Szűkebb értelemben, amikor a lejátszó korlátozás nincs beállítva, egy blokk kulcsot, ami egy blokk adatok kódolására használt kulcs, egy eszköz ID-t magában foglaló adatból generálunk, és az eszköz ID-t eltároljuk a hordozóeszközön. Ezért a hordozóeszközön lévő tartalmat lejátszani szándékozó valamely lejátszó megszerezheti a hordozóeszközből az ott beállított eszköz ID-t, és így generálni tud egy hasonló blokk kul-

csot. Ily módon a blokk adat dekódolható. Abban az esetben viszont, amikor a lejátszó korlátozás be van állítva, egy blokk kulcsot, ami egy blokk adatok kódolására használt kulcs, egy eszköz-egyértelmű kulcsot magában foglaló adatból generálunk. Mivel ez az eszköz-egyértelmű kulcs egy olyan privát kulcs, amely eszközönként változik, azért azt a másik eszköz nem tudja megszerezni. Abban az esetben, amikor blokk adatot valamely hordozóeszközön való tároláshoz kódolunk, az adat írást nem végezzük el egy olyan hordozóeszközre, amelyben az eszköz-egyértelmű kulcsot tároljuk. Ezért, mivel ugyanazt az eszköz-egyértelmű kulcsot még akkor sem szerezhetjük meg, ha a másik lejátszóban beállított valamely hordozóeszközön tárolunk is kódolt blokk adatot, azért a blokk adat dekódolásához egyetlen dekódolási kulcsot sem generálhatunk, és így a blokk adat nem dekódolható lejátszáshoz. Megjegyezzük, hogy a lejátszási műveleteket a későbbiekben tovább tárgyaljuk.

A következőkben, a 18. ábrára való hivatkozással, a 300 TS feldolgozóban ATS-hozzáfűzésnél végrehajtott műveletek egy folyamát, és a 150 kriptográfiai egység általi kódolásnál végrehajtott műveletek egy folyamatát mutatjuk be, adat rögzítésnél. A 18. ábrán lévő S1801 lépésben a rögzítő/lejátszó beolvas egy mester kulcsot, egy eszköz ID-t, ami a rögzítő/lejátszót azonosítja és egy eszköz-egyértelmű kulcsot, amit a saját 180 memóriájában tárol.

Az S1802 lépésben a rögzítő/lejátszó ellenőrzi, hogy a lemez ID-t mint azonosítási információt rögzítette-e már a hordozóeszközön. Ha megtalálta rögzítve, akkor a rögzítő/lejátszó az S1803 lépésben beolvassa a lemez ID-t. Ha nem, akkor a rögzítő/lejátszó generál egy lemez ID-t véletlenszerű-

en, vagy egy előre meghatározott eljárás által, és rögzíti azt a lemezen az S1804 lépésben. Ezután az S1805 lépésben a rögzítő/lejátszó egy lemez-egyértelmű kulcsot generál a mester kulcsból és lemez ID-ből. Egy lemez-egyértelmű kulcsot az FIPS 180 - 1-ben definiált SHA - 1 függvény használata által, vagy egy, például a fenti blokk kódolási függvényen alapuló hasító függvény által generálunk.

A rögzítő/lejátszó az S1806 lépésre halad, ahol kibont egy cím kulcsot, ami egyedi minden egyes rekord számára, lejátszó korlátozás jelzőt, eszköz ID-t azonosítási információként az eszköz számára és a mester kulcs generálási számát, és a lemezre rögzíti őket. Ezután az S1807 lépésben a rögzítő/lejátszó egy cím-egyértelmű kulcsot generál a lemez-egyértelmű kulcsból, cím kulcsból és vagy egy eszköz ID-ből (amikor a lejátszó korlátozás nincs beállítva), vagy egy eszköz-egyértelmű kulcsból (amikor a lejátszó korlátozás be van állítva).

A 20. ábra egy cím-egyértelmű kulcs generálásánál végrehajtott műveletek folyamatát mutatja be részletesen. Az S2001 lépésben a 150 kriptográfiai egység eldönti, hogy a lejátszó korlátozás be van-e állítva vagy sem a rögzítő/lejátszó felhasználója által bevitt utasítás adatok alapján, vagy a tartalomhoz hozzáfűzött használat-korlátozó információ alapján.

Ha az S2001 lépésben „NEM" döntés született, nevezetesen ha a lejátszó korlátozás nincs beállítva, akkor a rögzítő/lejátszó az S2002 lépésre halad, ahol cím-egyértelmű kulcsot generál egy lemez-egyértelmű kulcsból, cím kulcsból és eszköz ID-ből.

Ha az S2001 lépésben „IGEN" döntés született, nevezetesen ha a lejátszó korlátozás be van állítva, akkor a rögzítő/lejátszó az S2003 lépésre halad, ahol egy cím-egyértelmű kulcsot generál egy lemez-egyértelmű kulcsból, cím kulcsból és eszköz-egyértelmű kulcsból az SHA - 1 hasító függvény vagy egy blokk kódolási függvényen alapuló hasító függvény használata által.

Az S1808 lépésben a rögzítő/lejátszó rögzítendő tartalom adat kódolandó adatait fogadja TS csomagok formájában. Az S1809 lépésben a 300 TS feldolgozó minden egyes TS csomaghoz ATS-t fűz hozzá, ami egy olyan időpontot jelző információ, amikor a csomagot fogadtuk. Alternatívaként a 300 TS feldolgozó minden egyes TS csomaghoz CCI másolás vezérlési információ, ATS és más információ valamely kombinációját fűzi hozzá. Ezután az S1810 lépésben a rögzítő/lejátszó egymás után fogad olyan TS csomagokat, amelyek mindegyikéhez hozzáfűztünk ATS-t, és eldönti, hogy egyetlen blokkot alkotó X számú (például X=32) TS csomagot vagy az utolsó csomagot jelző azonosítási adatot fogadott. Amikor a fenti feltételek bármelyike teljesül, a rögzítő/lejátszó az S1811 lépésre halad, ahol egymás mellé rendezi az X számú TS csomagot, illetve a TS csomagokat egészen az utolsóig, adatok egyetlen blokkjának kialakításához.

Ezután az S1812 lépésben a 150 kriptográfiai egység egy blokk kulcsot generál, ami egy kulcs a fenti blokkban lévő adat kódolására való használatához a blokk adat vezető részletében lévő 32 bitből (ATS-t magában foglaló blokk magból) és az S1807 lépésben generált cím-egyértelmű kulcsból.

Az S1813 lépésben az S1811 lépésben kialakított blokk adatot kódoljuk a blokk kulccsal. Amint azt megelőzően leírtuk, a blokk adatban az (m+1)-ediktől az utolsóig kódolásnak vetjük alá a bájtokat. A kódolási algoritmus például az FIPS 46 - 2-ben definiált DES.

Az S1814 lépésben a kódolt blokk adatot rögzítjük egy hordozóeszközre. Az S1815 lépésben eldöntjük, hogy az összes adatot rögzítettük-e a hordozóeszközre vagy sem. Amikor az összes adatot rögzítettük, a rögzítő/lejátszó kilép a rögzítési eljárásból. Ha nem, a rögzítő/lejátszó visszamegy az S1808 lépéshez, ahol feldolgozza a fennmaradó adatokat.

A következőkben a 23. ábrán lévő blokk diagramra és a 24 - 26. ábrákon lévő folyamatábrákra való hivatkozással leírjuk az előzőekben leírtak szerint egy hordozóeszközre rögzített kódolt tartalom dekódolásánál, vagy lejátszásánál, végrehajtott műveleteket.

Dekódolásnál és lejátszásnál végrehajtott műveletek egy folyamatát mutatjuk be a 23. ábrán lévő blokk diagramra és a 24. ábrán lévő folyamatábrára való hivatkozással. A 24. ábrán lévő S2401 lépésben a 2300 rögzítő/lejátszó kiolvas egy 2302 lemez ID-t és elő-rögzítési generálási számot egy 2320 lemezből, valamint egy 2301 mester kulcsot, 2331 eszköz ID-t eszköz azonosítóként és 2332 eszköz-egyértelmű kulcsot a saját memóriájából. Amint az világos a rögzítésnek az előzőekben történt leírásából, a lemez ID egy olyan lemez-egyértelmű azonosító, amelyet megelőzően rögzítettünk a lemezre, vagy amelyet a rögzítő/lejátszóban generáltunk és a lemezre rögzítettünk.

A 2360 elő-rögzítési generálási szám a lemezben előre eltárolt generálási információ, amely egyedi a lemez, mint hor-

dozóeszköz számára. Az elő-rögzítési generálási számot összehasonlítjuk annak a mester kulcsnak a generálási számával, amellyel az adatot rögzítettük, nevezetesen egy 2350 rögzítési generálási számmal annak eldöntésére, hogy az adat lejátszható-e. A 2301 mester kulcs egy engedéllyel rendelkező rögzítő/lejátszóban tárolt privát kulcs, és amely generálását irányítjuk. Az eszköz ID egy egyedi azonosító a rögzítő/lejátszó számára, és az eszköz-egyértelmű kulcs egy privát kulcs, amely egyedi a rögzítő/lejátszó számára.

Az S2402 lépésben a 2300 rögzítő/lejátszó beolvas egy cím kulcsot a lemezről olvasandó adathoz, valamint egy eszköz ID-t egy olyan rögzítő/lejátszóhoz, amely az adatot rögzítette, egy az adathoz megfelelően beállított lejátszó korlátozás jelzőt és az adat rögzítésekor használt mester kulcs generálási számát (Generálás#n), azaz a 2350 rögzítési generálási számot. Ezután az S2403 lépésben a rögzítő/lejátszó eldönti, hogy az olvasandó adat lejátszható-e. A 25. ábrán részletesen bemutatjuk az ehhez a döntéshez végrehajtott műveletek folyamatát.

A 25. ábrán lévő S2501 lépésben a rögzítő/lejátszó eldönti, hogy melyik a fiatalabb vagy idősebb, az S2401 lépésben beolvasott elő-rögzítési generálási szám vagy az S2402 lépésben beolvasott rögzítési generálási szám. Abban az esetben, amikor a döntés eredmény az, hogy a rögzítési generálási szám által jelzett generálás nem fiatalabb, mint az elő-rögzítési generálási szám által jelzett generálás, vagyis ha adat rögzítési generálási információ által jelzett generálás idősebb, mint az elő-rögzítési generálási információ által jelzett generálás, akkor a rögzítő/lejátszó olyan döntést hoz, hogy az adat nem játszható le, majd átugorja az S2404-S2409 lépéseket

és kilép az eljárásból anélkül, hogy lejátszaná az adatot. Tehát abban az esetben, amikor a hordozóeszközön rögzített tartalmat egy olyan mester kulccsal kódoltuk, amely generálása idősebb, mint az, amit az elő-rögzítési generálási információ jelez, az adat lejátszását nem engedjük meg, és nem hajtunk végre lejátszást.

Más szóval, a fenti eljárás olyan döntést hoz, hogy az adatot egy olyan rögzítő kódolta egy idősebb-generálású mester kulccsal és rögzítette a hordozóeszközre, amelynek nem adtunk ki legújabb-generálású kulcsot, mert kiderült annak nem legális (illegális) mivolta, és megtiltjuk bármely olyan hordozóeszköz lejátszását, amelyre egy ilyen illegális rögzítő rögzített adatot. Ily módon lehetséges egy illegális rögzítő használatának a kiküszöbölése.

Ha viszont az S2501 lépésben a döntés eredménye az, hogy a rögzítési generálási szám által jelzett generálás fiatalabb, mint az elő-rögzítési generálási szám által jelzett generálás, nevezetesen abban az esetben, amikor a rögzítési generálási szám által jelzett generálás ugyanaz, vagy fiatalabb, mint az elő-rögzítési generálási szám által jelzett generálás, és ezért a hordozóeszközre rögzített tartalmat egy olyan mester kulccsal kódoltuk, amely generálása fiatalabb, mint az elő-rögzítési generálási szám által jelzett generálás, akkor a rögzítő/lejátszó az S2502 lépésre halad, ahol megszerzi a generálási információt a saját memóriájában tárolt valamely C kódolt mester kulcsról, és egy összehasonlítást végez el a kódolt mester kulcs generálása és a kódolt generálási információ által jelzett generálás között annak eldöntésére, hogy a generálások közül melyik a fiatalabb vagy idősebb a másiknál.

Ha az S2502 lépésben a döntés eredménye az, hogy a memóriában tárolt C mester kulcs generálása nem fiatalabb, mint a rögzítési generálási információ által jelzett generálás, nevezetesen ha a memóriában tárolt C mester kulcs generálása idősebb, mint a rögzítési generálási információ által jelzett generálás, akkor a rögzítő/lejátszó olyan döntést hoz, hogy a tartalom nem játszható le, akkor átugorja az S2404-S2409 lépéseket, és kilép az eljárásból anélkül, hogy lejátszaná a tartalmat.

Ha az S2502 lépésben a döntés eredménye az, hogy a memóriában tárolt C mester kulcs generálása fiatalabb, mint a rögzítési generálási információ által jelzett generálás, vagyis ha a C mester kulcs generálása ugyanaz, vagy fiatalabb, mint a rögzítési generálási információ által jelzett generálás, akkor a rögzítő/lejátszó az S2503 lépésre halad, ahol ellenőrzi, hogy az adat, amit olvasni fog lejátszó-korlátozott módban van-e rögzítve.

Az S2503 lépésben a rögzítő/lejátszó eldönti, hogy a beolvasott lejátszó korlátozás jelző által jelzett lejátszó korlátozás információ az-e, hogy a „Lejátszó korlátozás be van állítva". Ha a „lejátszó korlátozást" beállítva találta, a rögzítő/lejátszó az S2504 lépésre halad, ahol eldönti, hogy „A hordozóeszközről olvasott eszköz ID egybeesik-e magának a lejátszónak egy eszköz ID-jével". Abban az esetben, amikor „egybeesést" talált, a rögzítő/lejátszó eldönti, hogy a szóban forgó adat lejátszható-e. Továbbá, ha az S2503 lépésben a döntés eredménye az, hogy a „Lejátszó korlátozás nincs beállítva", akkor a rögzítő/lejátszó eldönti, hogy az adat lejátszható-e. Ha a beolvasott lejátszó korlátozás jelző által jelzett

lejátszó korlátozás információ az, hogy „A lejátszó korlátozás be van állítva" és „A hordozóeszközről beolvasott eszköz ID nem esik egybe magának a lejátszónak egy eszköz ID-jével", akkor a rögzítő/lejátszó olyan döntést hoz, hogy az adat nem játszható le.

Ha a döntés eredménye az, hogy az adat lejátszható, a rögzítő/lejátszó az S2404 lépésre halad, ahol egy lemez-egyértelmű kulcsot generál egy lemez ID-ből és egy mester kulcsból (amit a „2303" hivatkozási jelnél jelölünk), amint azt alább bemutatjuk. A mester kulcs és lemez ID bitenkénti kombinációja által generált adatot például az FIPS 180 - 1-ben definiált SHA - 1 hasító függvénybe helyezzük el és az elhelyezés eredményeként kapott 160-bites kimenet csak egy szükséges adat hosszúságát használjuk lemez-egyértelmű kulcsként. Alternatívaként a mester kulcsot és lemez ID-t egy blokk kódolási függvényt használó hasító függvénybe helyezzük el, és az elhelyezés egy eredményét használjuk a lemez-egyértelmű kulcsként. Az itt használt mester kulcs az, amelyet a hordozóeszközből olvastunk be az S2402 lépésben, és amely generálását az adat rögzítési generálási száma jelzi. Ha a rögzítő/lejátszó rendelkezik egy olyan mester kulccsal, amely generálása fiatalabb, mint a mester kulcs generálása, akkor a fent tárgyalt eljárások bármelyike által generálhat egy olyan generálású mester kulcsot, amelyet a rögzítési generálási szám jelez, és az így generált mester kulccsal tovább generálhat egy lemez-egyértelmű kulcsot.

Ezután az S2405 lépésben a rögzítő/lejátszó egy cím-egyértelmű kulcsot generál, amint azt a következőkben alább leírjuk a 26. ábrára való hivatkozással. Az S2601 lépésben a

150 kriptográfiai egység eldönti, hogy a lejátszó korlátozás be van-e állítva vagy sem, a lemezről beolvasott lejátszó korlátozás jelző alapján.

A rögzítő/lejátszó beolvas egy 2334 eszköz ID-t egy olyan rögzítő/lejátszóhoz, amelyre az adatot rögzítettük és egy 2335 lejátszó korlátozás jelzőt, amelyet az adatnak megfelelően állítottunk be. Ha az így beolvasott 2335 lejátszó korlátozás jelző által jelzett lejátszó korlátozás információ az, hogy a „Lejátszó korlátozás be van állítva" és „A hordozóeszközről beolvasott 2334 eszköz ID egybeesik magának a lejátszónak egy 2331 eszköz ID-jével", vagy ha a beolvasott 2333 lejátszó korlátozás jelző által jelzett lejátszó korlátozás információ az, hogy a „Lejátszó korlátozás nincs beállítva", akkor az adat lejátszható. Ha a 2333 lejátszó korlátozás jelző által jelzett lejátszó korlátozás információ az, hogy a „Lejátszó korlátozás be van állítva" és „A hordozóeszközről beolvasott 2334 eszköz ID nem esik egybe magának a lejátszónak egy 2331 eszköz ID-jével", akkor az adat nem játszható le.

Az ok, amiért nem tudjuk lejátszani az adatot az, hogy nem tudunk blokk kulcsot generálni az adat dekódolásához, mivel az adatot egy olyan rögzítő/lejátszóhoz tartozó eszköz-egyértelmű kulcsból generált blokk kulccsal kódoltuk, amelybe az adatot rögzítettük, és az adatot rögzítő rögzítő/lejátszótól különböző rögzítő/lejátszók nem ugyanazzal az eszköz-egyértelmű kulccsal rendelkeznek.

Abban az esetben, amikor az adat lejátszható, egy cím-egyértelmű kulcsot generálunk a lemez-egyértelmű kulcs, cím kulcs és eszköz ID valamely kombinációjából vagy a lemez-

egyértelmű kulcs, cím kulcs és eszköz-egyértelmű kulcs valamely kombinációjából.

Vagyis amikor a lejátszó korlátozás nincs beállítva, a cím-egyértelmű kulcsot a lemez-egyértelmű kulcsból, cím kulcsból, eszköz ID-ből és cím-egyértelmű kulcsból generáljuk. Amikor a lejátszó korlátozás be van állítva, a cím-egyértelmű kulcsot a lemez-egyértelmű kulcsból, cím kulcsból és magának a lejátszónak egy eszköz-egyértelmű kulcsából generáljuk. A cím-egyértelmű kulcs generálásához az SHA - 1 hasító függvényt vagy egy blokk kódolási függvényen alapuló hasító függvényt használhatunk.

A leírást a 26. ábrán bemutatott folyamatábrára való hivatkozással folytatjuk. Ha az S2601 lépésben a döntés eredménye „NEM", nevezetesen ha a lejátszó korlátozás nincs beállítva, akkor a rögzítő/lejátszó az S2602 lépésre halad, ahol egy cím-egyértelmű kulcsot generál a lemez-egyértelmű kulcsból, cím kulcsból és eszköz ID-ből.

Ha az S2601 lépésben a döntés eredménye „IGEN", nevezetesen ha a lejátszó korlátozás be van állítva, akkor a rögzítő/lejátszó az S2603 lépésre halad, ahol egy cím-egyértelmű kulcsot generál a lemez-egyértelmű kulcsból, cím kulcsból és az eszköz-egyértelmű kulcsából az SHA - 1 hasító függvény vagy a blokk kódolási függvényen alapuló hasító függvény használatával.

A fentiekben a lemez-egyértelmű kulcsot a mester kulcsból és lemez ID-ből generáljuk, és a cím-egyértelmű kulcsot a lemez-egyértelmű kulcs, cím kulcs és eszköz ID valamely kombinációjából vagy a cím kulcs és eszköz-egyértelmű kulcs valamely kombinációjából generáljuk. Ennek ellenére a cím-egyértelmű

kulcsot generálhatjuk közvetlenül a mester kulcsból, lemez ID-ből, cím kulcsból és eszköz ID-ből vagy eszköz-egyértelmű kulcsból bármiféle eszköz-egyértelmű kulcs használata nélkül, illetve egy cím-egyértelmű kulccsal ekvivalens kulcsot generálhatunk a mester kulcsból, lemez ID-ből és eszköz ID-ből, (amikor a lejátszó korlátozás nincs beállítva) vagy eszköz-egyértelmű kulcsból (amikor a lejátszó korlátozás be van állítva) bármiféle cím kulcs használata nélkül.

Ezután az S2406 lépésben a rögzítő/lejátszó egyre fiatalabb blokk adatokat olvas be egy 2312 kódolt tartalomból a lemezről, az S2407 lépésben elkülönít a blokk adat vezető részletében egy blokk magot alkotó négy bájtot egy 2310 kiválasztóban, és egy blokk kulcsot generál a blokk magból és az S2405 lépésben generált cím-egyértelmű kulcsból.

A blokk kulcsot generálhatjuk úgy is, amint azt az előzőekben leírtuk a 22. ábrára hivatkozva. Vagyis egy 64-bites blokk kulcsot generálhatunk egy 32-bites blokk magból és 64-bites cím-egyértelmű kulcsból.

A fentiekben a lemez-egyértelmű kulcs, cím-egyértelmű kulcs és blokk kulcs generálásának példáit írjuk le. Megjegyezzük viszont, hogy minden egyes blokk esetén generálhatunk egy blokk kulcsot egy mester kulcsból, lemez ID-ből, cím kulcsból, blokk magból és egy eszköz ID-ből (amikor a lejátszó korlátozás nincs beállítva) vagy egy eszköz-egyértelmű kulcsból (amikor a lejátszó korlátozás be van állítva) anélkül, hogy bármiféle lemez-egyértelmű kulcsot és cím-egyértelmű kulcsot kellene generálnunk.

Az S2408 lépésben a kódolt blokk adatot dekódoljuk az így generált blokk kulccsal (amint azt a „2309" hivatkozási jelnél

jelöljük), és kimenetre tesszük dekódolt adatként egy 2308 kiválasztón keresztül. Megjegyezzük, hogy a dekódolt adat magában foglal a szállítási folyamban lévő minden egyes szállítási csomaghoz hozzáfűzött ATS-t, és a folyamot az ATS alapján dolgozzuk fel a megelőzően említett 300 TS feldolgozóban. Ezután az adatot használhatjuk például egy kép megjelenítésére vagy zene lejátszására.

Ily módon a blokk egységekben kódolt és a hordozóeszközön tárolt tartalmat dekódolhatjuk lejátszáshoz az ATS-t magában foglaló blokk magból generált blokk kulccsal, blokk egységekben. A rögzítő/lejátszó dekódolja a kódolt blokk adatot a blokk kulccsal, és az S2409 lépésben eldönti, hogy az összes adat beolvasásra került-e. Ha az összes adatot beolvasta, a rögzítő/lejátszó kilép az eljárásból. Ha nem, a rögzítő/lejátszó visszamegy az S2406 lépésre, ahol beolvassa a fennmaradó adatokat.

A megelőzően említett kiviteli példában a kulcs megújítási blokkot használjuk egy mester kulcs átvitelére minden egyes rögzítő/lejátszóhoz, és ezt a mester kulcsot használjuk adatnak egy rögzítő/lejátszóra való rögzítéséhez vagy az onnan való lejátszásához.

A mester kulcs érvényes a generálásában az adat minden rögzítése esetében. Egy rögzítő/lejátszó, amely megszerezte valamely generálásnak a mester kulcsát dekódolni tudja a rögzített adatokat abban a generálásban és korábbi generálásban abban a rendszerben, amelyikhez a rögzítő/lejátszó tartozik. Viszont a mester kulcs azon természete miatt, hogy a teljes rendszerben érvényes, a mester kulcsnak egy támadó általi sikeres felfedése a teljes rendszert hátrányosan befolyásolja.

A hordozóeszköz kulcs megújítási blokkját használó valamely továbbítandó kulcsként használhatunk viszont egy közeg kulcsot, amely csak a hordozóeszközön érvényes, valamely a teljes rendszerben érvényes mester kulcs helyett. Az alábbiakban leírjuk közeg kulcs használatát mester kulcs helyett (második kiviteli példa). Megjegyezzük viszont, hogy a második kiviteli példának csak az előzőekben említett első kiviteli példától való eltéréseit írjuk le.

A 13. ábrához hasonlóan, a 27. ábra azt mutatja be, hogy hogyan használja a 0. eszköz a hordozóeszközön tárolt KRB-t valamely t időpontban, az ott előre eltárolt K0000 levél kulcsot valamint a K000 és K00 csomópont kulcsokat egy K(t)00 megújított csomópont kulcs generálására, és hogyan szerez meg egy K(t)media új közeg kulcsot a K(t)00 megújított csomópont kulcs alapján. A K(t)media közeg kulcsot adatoknak a hordozóeszközre való rögzítésüknél és az onnan való lejátszásuknál használjuk.

Megjegyezzük, hogy a 27. ábrán mutatott Generálás#n előrögzítési generálási szám nem nélkülözhetetlen, viszont opcióként beállítjuk, mert a közeg kulcs, ellentétben a mester kulccsal, nem ismeri a generálás, „fiatalabb" vagy „idősebb" fogalmakat.

Például amikor egy hordozóeszközt teszünk be az egyes rögzítő/lejátszókba adat rögzítéshez vagy lejátszáshoz, a rögzítő/lejátszó kiszámít egy K(t)media közeg kulcsot a hordozóeszköz számára, és ezt használja a hordozóeszközhöz való későbbi hozzáférésekhez, amint azt a 28. ábrán lévő folyamatábra mutatja.

A 28. ábrán a KRB beolvasás az S2801 lépésben és a KRB feldolgozás az S2802 lépésben hasonlóak a 14. ábrán az S1403 és S1404 lépésekben lévőekhez.

Az S2803 lépésben a rögzítő/lejátszó beolvassa a hordozóeszközről a K(t)media közeg kulcsnak a K(t)00 csomópont kulcscsal való kódolásából származtatott Enc(K(t)00, K(t)media) kódolt adatot, és az S2804 lépésben dekódolja az adatot egy közeg kulcs megszerzéséhez. Ha a rögzítő/lejátszót kizárjuk vagy eltávolítjuk a 11. ábrán bemutatott fa struktúrában lévő csoportból, nem lesz képes egyetlen közeg kulcs megszerzésére sem, és így adatnak a hordozóeszközre való rögzítésére vagy az onnan való lejátszására sem.

A következőkben adatnak a hordozóeszközre való rögzítését írjuk le. Viszont, mivel a mester kulccsal ellentétben a közeg kulcs nem ismer olyan fogalmakat, mint „generálás", „idősebb" vagy „fiatalabb", azt, hogy az adatot rögzíthetjük-e nem ellenőrizzük az elő-rögzítési generálási információ és a magában a rögzítő/lejátszóban tárolt mester kulcs közötti generálásbeli összehasonlítás által, mint a 15. ábrán, ellenben, ha a fenti feldolgozásban megszereztünk egy közeg kulcsot, akkor olyan döntést hozunk, hogy az adatot rögzíthetjük, amint azt a 29. ábrán mutatott folyamatábrán bemutatjuk. Amint azt a 29. ábrán mutatjuk, az S2901 lépésben eldöntjük, hogy megszereztünk-e egy közeg kulcsot, és csak amikor megszereztünk egy közeg kulcsot, akkor rögzítünk egy tartalmat az S2902 lépésben.

Az alábbiakban a 30. és 31. ábrákon lévő blokk diagramokra és a 32. ábrán lévő folyamatábrára való hivatkozással azt írjuk le, hogy hogyan rögzítünk egy tartalom adatot.

Csakúgy, mint az első kiviteli példában, a hordozóeszköz ebben a második kiviteli példában is egy optikai lemez. Továbbá a második kiviteli példára is igaz az, hogy egy hordozóeszközről származó adat bitenkénti másolásának megakadályozására a lemez ID-vel, mint a hordozóeszköz számára egyedi azonosítási információval befolyásolunk egy kulcsot az adat kódolásához.

A 30. és 31. ábrák hasonlóak az első kiviteli példához tartozó 16. és 17. ábrákhoz kivéve azt, hogy egy közeg kulcsot használunk a mester kulcs helyett és egy mester kulcs generálását jelző bármely Generálás#n rögzítési generálási számot nem használjuk. A 30. és 31. ábrák közti különbség hasonló a 16. és 17. ábrák között lévőhöz, és egy lemez ID írásával kapcsolatos. Nevezetesen nem rögzítünk egyetlen lemez ID-t sem a 30. ábrán bemutatott adat rögzítésben, míg a 31. ábrán bemutatott adat rögzítésben rögzítünk egy lemez ID-t.

A 32. ábra egy olyan adat rögzítést mutat be ebben a kiviteli példában, amelyben egy közeg kulcsot használunk. Nevezetesen a 32. ábrán lévő blokk diagram megfelel a 18. ábrán bemutatott első kiviteli példához tartozó folyamatábrának. Főként a 32. ábrán lévő műveleteknek az első kiviteli példában végrehajtott műveletektől való eltéréseit írjuk le.

A 32. ábrán az S3201 lépésben egy 3000 rögzítő/lejátszó beolvas egy a saját memóriájában tárolt eszköz ID-t és eszközegyértelmű kulcsot, valamint egy K(t)media közeg kulcsot, amelyet kiszámítottunk és ideiglenesen eltároltunk a 28. ábrán lévő S2804 lépésben.

Az S3202 lépésben a 3000 rögzítő/lejátszó ellenőrzi, hogy eltároltunk-e már egy lemez ID-t egy 3020 hordozóeszközön

(optikai lemezben). Ha a lemez ID-t már eltároltuk, a 3000 rögzítő/lejátszó beolvassa a lemez ID-t az S3203 lépésben (mint a 30. ábrán). Ha a lemez ID-t nem tároltuk, a 3000 rögzítő/lejátszó generál egy lemez ID-t véletlenszerűen, vagy egy előre meghatározott eljárás által, és az S3204 lépésben a lemezre rögzíti. Egyetlen lemez számára csak egyetlen lemez ID-nek kell elérhetőnek lennie. Így a lemez ID-t a lemez valamely bevezető területén vagy hasonlón tárolhatjuk el. Bármely esetben a 3000 rögzítő/lejátszó az S3205 lépésre halad.

Az S3205 lépésben a 3000 rögzítő/lejátszó az S3201 lépésben beolvasott közeg kulcsot és lemez ID-t használja egy lemez-egyértelmű kulcs generálására. A lemez-egyértelmű kulcsot közeg kulcsnak egy mester kulcs helyetti használatával ugyanolyan módon generálhatjuk, mint az első kiviteli példában.

Ezután a 3000 rögzítő/lejátszó az S3206 lépésre halad, ahol generál minden egyes rekord számára egy egyedi cím kulcsot véletlenszerűen, vagy egy előre meghatározott eljárás által, és rögzíti azt a lemezre. Ugyanakkor, a 3000 rögzítő/lejátszó a lemezre rögzít egy lejátszó korlátozás jelzőt azt jelző információként, hogy a cím (adat) csak egy olyan eszközben játszható-e le, amelyben azt rögzítettük (amikor a lejátszó korlátozás be van állítva), vagy lejátszható bármely másik eszközben (amikor a lejátszó korlátozás nincs beállítva), valamint rögzít egy eszköz ID-t, amelyet a 3000 rögzítő/lejátszó birtokol.

A lemezben biztosítunk egy adat kezelési fájlt, amelyben információt tárolunk arról, hogy az adatból milyen címet alakítunk ki és hogy honnan származik az adat, és amely tárolhat

továbbá egy cím kulcsot, lejátszó korlátozás jelzőt és egy eszköz ID-t.

Az S3207-S3215 lépésekben végrehajtott műveletek hasonlóak a 18. ábrán lévő S1807-S1815 lépésekben végrehajtottakhoz, ezért ezeket nem tárgyaljuk részletesebben.

Megjegyezzük, hogy az előzőekben leírtuk, hogy a lemez-egyértelmű kulcsot a közeg kulcsból és lemez ID-ből generáljuk, és a cím-egyértelmű kulcsot a lemez-egyértelmű kulcsból, cím kulcsból és eszköz ID-ből, vagy a cím kulcsból és eszköz-egyértelmű kulcsból generáljuk, de a cím-egyértelmű kulcsot generálhatjuk közvetlenül a közeg kulcsból, lemez ID-ből, cím kulcsból és eszköz ID-ből vagy eszköz-egyértelmű kulcsból is anélkül, hogy használnunk kellene az eszköz-egyértelmű kulcsot, valamint a cím-egyértelmű kulccsal ekvivalens kulcsot generálhatunk a közeg kulcsból, lemez ID-ből és az eszköz ID-ből (amikor a lejátszó korlátozás nincs beállítva) vagy eszköz-egyértelmű kulcsból (amikor a lejátszó korlátozás be van állítva) a cím kulcs használata nélkül.

A közeg kulcsot a fentiek szerint használhatjuk adatnak a hordozóeszközre való rögzítésére.

A következőkben a 33. ábrán lévő blokk diagramra és a 34. ábrán lévő folyamatábrára való hivatkozással a fentiek szerint rögzített adat lejátszását írjuk le.

A 33. ábra hasonló az első kiviteli példához tartozó 23. ábrához, kivéve, hogy egy közeg kulcsot használunk a mester kulcs helyett, és ezért a generálás# rögzítési generálási számot figyelmen kívül hagyjuk.

A 34. ábrán lévő S3401 lépésben egy 3400 rögzítő/lejátszó beolvas egy lemez ID-t egy 3420 lemezről, ami egy hordozóesz-

köz, valamint kiolvas a saját memóriájából egy eszköz ID-t, ami saját maga számára egyedi, eszköz-egyértelmű kulcsot, amely egy saját maga számára egyedi kulcs és egy közeg kulcsot, amelyet a 28. ábrán lévő S2804 lépésben kiszámítottunk és ideiglenesen eltároltunk.

Megjegyezzük, hogy ha a 3400 rögzítő/lejátszó nem tud megszerezni egyetlen közeg kulcsot sem, még azután sem, ha végrehajtja a 28. ábrán lévő műveleteket a beléhelyezett hordozóeszközzel, akkor kilép az eljárásból anélkül, hogy megpróbálkozna bármiféle adat lejátszással.

Ezután az S3402 lépésben a 3400 rögzítő/lejátszó beolvas egy cím kulcsot a lemezről beolvasandó adathoz, eszköz ID-t az adatot rögzítő valamely eszközhöz és egy lejátszó korlátozás jelzőt az adathoz.

Ezután az S3403 lépésben a 3400 rögzítő/lejátszó eldönti, hogy az adat lejátszható-e. Az S3403 lépésben végrehajtott műveletet a 35. ábrán mutatjuk be részletesen.

Az S3501 lépésben a 3400 rögzítő/lejátszó eldönti, hogy meg tudna-e szerezni egy közeg kulcsot. Ha nem tudna megszerezni egyetlen közeg kulcsot sem, akkor az adat nem játszható le. Ha meg tudna szerezni egy közeg kulcsot, akkor a 3400 rögzítő/lejátszó az S3502 lépésre halad. Az S3502 és az S3503 lépésekben lévő műveletek hasonlóak a 25. ábrán lévő S2503 és S2504 lépésekben lévő műveletekhez. Amikor a lejátszó korlátozás jelző azt jelenti, hogy a „Lejátszó korlátozás be van állítva", továbbá ha a hordozóeszközből az S3503 lépésben beolvasott, az adatot beolvasó eszközhöz tartozó eszköz kulcs, valamint a memóriából az S3401 lépésben kiolvasott, a 3400 rögzítő/lejátszóhoz tartozó eszköz ID együttesen azt jelentik,

hogy „Az adatot rögzítő eszköz nem a lejátszó", a 3400 rögzítő/lejátszó olyan döntést hoz, hogy „Az adat nem játszható le", átugorja az S3404-S3409 lépéseket, és kilép az eljárásból anélkül, hogy lejátszaná az adatot. A fentitől különböző bármely más esetben a 3400 rögzítő/lejátszó olyan döntést hoz, hogy „Az adat lejátszható", és az S3404 lépésre halad.

Az S3404-S3409 lépésekben végrehajtott műveletek hasonlóak a 24. ábrán az S2404-S2409 lépésekben lévő műveletekhez, ezért azokat nem írjuk le részletesebben.

Megjegyezzük, hogy a megelőzőekben azt írtuk le, hogy a lemez-egyértelmű kulcsot a közeg kulcsból és lemez ID-ből generáljuk, és a cím-egyértelmű kulcsot a lemez-egyértelmű kulcsból, cím kulcsból és eszköz ID-ből, vagy a cím kulcsból és eszköz-egyértelmű kulcsból generáljuk, de a cím-egyértelmű kulcsot generálhatjuk közvetlenül a közeg kulcsból, lemez ID-ből, cím kulcsból és eszköz ID-ből vagy eszköz-egyértelmű kulcsból is anélkül, hogy használnunk kellene az eszköz-egyértelmű kulcsot, valamint egy a cím-egyértelmű kulccsal ekvivalens kulcsot generálhatunk a közeg kulcsból, lemez ID-ből és eszköz ID-ből (amikor a lejátszó korlátozás nincs beállítva) vagy eszköz-egyértelmű kulcsból (amikor a lejátszó korlátozás be van állítva) a cím kulcs használata nélkül.

Adatot a hordozóeszközre vagy onnan a fentiek szerint rögzíthetünk illetve játszhatunk le.

Emlékeztetnünk kell arra, hogy a fentiekben bemutatott és leírt példában a KRB-t előre eltároljuk a hordozóeszközön, de egy 3600 rögzítő/lejátszó egy olyan KRB-t, amelyet bármely más eszköztől a 120 vagy 140 bemenet/kimenet I/F-en, egy 3601 modemen vagy hasonlón keresztül fogadott egy hordozóeszközre

rögzíthet az adatnak a kezdeti rögzítésekor vagy minden egyes alkalommal, amikor adatot rögzít a hordozóeszközre, amint azt a 36. ábrán mutatjuk.

Vagyis, például az első kiviteli példában a rögzítő/lejátszót alkalmazhatjuk oly módon, hogy megszerezzen egy KRB-t és egy csomópont kulcsokkal kódolt mester kulcsot a 120 vagy 140 bemenet/kimenet I/F-en, 3601 modemen vagy hasonlón keresztül, és eltárolja azokat előre a saját 180 memóriájába, amint azt a 37. ábrán mutatjuk, és ezután feldolgozza az adatot egy tartalom adatnak egy hordozóeszközre való rögzítésekor, mint a 38. ábrán bemutatott folyamatábrán.

A leírást a 38. ábrán lévő folyamatábrára való hivatkozással folytatjuk. Az S3801 lépésben a rögzítő/lejátszó ellenőrzi, hogy rögzítettünk-e már KRB-t egy olyan hordozóeszközre, amelyre adatot szándékozik rögzíteni. Ha talál a hordozóeszközön már rögzített KRB-t, akkor a rögzítő/lejátszó átugorja az S3802 lépést és kilép az eljárásból (az adat rögzítési eljárásra halad). Ha az ellenőrzés eredménye az, hogy a hordozóeszközre még nem rögzítettünk egyetlen KRB-t sem, a rögzítő/lejátszó az S3902 lépésre halad, ahol rögzíti a saját 180 memóriájában tárolt KRB-t és kódolt mester kulcsot a hordozóeszközre, ahogyan azt a 39. ábrán mutatjuk. Miután a rögzítést elvégezte, a rögzítő/lejátszó a tartalom adat rögzítésére halad.

A fenti eljárás nem korlátozódik adatnak a mester kulccsal való rögzítésére, viszont alkalmazható adatnak a közeg kulccsal való rögzítésére, például úgy, mint a második kiviteli példában.

Valamely tartalom szerzői jog birtokosának nyeresége védelméhez egy engedéllyel rendelkező eszköznek vezérelnie kell a tartalom másolását.

Más szóval, valamely tartalomnak egy hordozóeszközre való rögzítéséhez szükséges azt ellenőriznünk, hogy a tartalom másolható-e vagy sem, és csak olyan adatot rögzítünk, amely másolható. Ezen kívül valamely tartalomnak egy hordozóeszközről való lejátszása és az adat kimenetre tétele esetén meg kell akadályoznunk a tartalomnak az ezt követő illegális másolását.

Egy ilyen tartalom rögzítéséhez vagy lejátszásához az 1. vagy 2. ábrán mutatott rögzítő/lejátszónak a tartalom másolásának vezérlése közbeni műveleteit írjuk le a következőkben a 40. és 41. ábrákon bemutatott folyamatábrákra való hivatkozással.

Először digitális jelekből álló valamely külső tartalomnak egy hordozóeszközre való rögzítéséhez a rögzítési műveleteket oly módon hajtjuk végre, amint azt a 40A ábrán lévő folyamatábrán mutatjuk. A 40A ábrán lévő műveleteket az alábbiakban példaként az 1. ábrán bemutatott 100 rögzítő/lejátszóval kapcsolatosan írjuk le. a 120 bemenet/kimenet I/F egy digitális jelekből álló tartalmat (digitális tartalmat) fogad az IEEE 1394 soros sínen vagy hasonlón keresztül az S4001 lépésben, és a rögzítő/lejátszó az S4002 lépésre halad.

Az S4002 lépésben a 120 bemenet/kimenet I/F eldönti, hogy a biztosított digitális tartalom másolható-e vagy sem. Vagyis amikor a 120 bemenet/kimenet I/F által fogadott tartalom nem volt kódolva (például a 120 bemenet/kimenet I/F-hez sima, vagy kódolatlan, tartalmat biztosítunk a megelőzően említett DTCP

szabvány alkalmazása nélkül), olyan döntést hozunk, hogy a tartalom másolható.

Tegyük fel itt, hogy a 100 rögzítő/lejátszó egy olyan eszköz, amely megfelel a DTCP szabványnak, és az adatokat a DTCP szabvány szerint rögzíti. A DTCP szabvány 2-bites EMI-t definiál másolás vezérlési információként. Amikor az EMI a „00B" (B jelzi, hogy az azt megelőző érték egy bináris szám), az azt jelenti, hogy a tartalmat szabadon másolhatjuk (szabadon másolható). Amikor az EMI a „01B", az azt jelenti, hogy a tartalmat nem másolhatjuk többször, mint egy előre meghatározott korlát (no-more-copies, nincs több másolás). Továbbá amikor az EMI az „10B", az azt jelenti, hogy a tartalom egyszer másolható (egy generálásig másolható). Végül, amikor az EMI az „11B", az azt jelenti, hogy a tartalmat tilos másolni (copy-never, sosem másolható).

A 100 rögzítő/lejátszó 120 bemenet/kimenet I/F-jéhez biztosított jelek magukban foglalnak EMI-t. Amikor az EMI azt jelenti, hogy „szabadon másolható" vagy „egy generálásig másolható", akkor olyan döntést hozunk, hogy a tartalmat másolhatjuk. Viszont ha az EMI azt jelenti, hogy „többé nem másolható" vagy „sosem másolható", akkor olyan döntést hozunk, hogy a tartalmat nem másolhatjuk.

Ha az S4002 lépésben a döntés eredménye az, hogy a tartalmat nem másolhatjuk, akkor a 100 rögzítő/lejátszó átugorja az S4003-S4005 lépéseket és kilép a rögzítési eljárásból. Tehát ebben az esetben a tartalmat nem fogjuk a 195 hordozóeszközre másolni.

Ha az S4002 lépésben a döntés eredménye az, hogy a tartalmat másolhatjuk, a 100 rögzítő/lejátszó az S4003 lépésre

halad. Ezt követően az S4003-S4005 lépésekben a 100 rögzítő/lejátszó a 3A ábrán lévő S302, S303 és S304 lépésekben végrehajtottakhoz hasonló műveleteket hajt végre. Vagyis a 300 TS feldolgozó egy szállítási folyamban lévő minden egyes szállítási csomaghoz ATS-t fűz hozzá, a 150 kriptográfiai egység kódolja az adatot, végül a 150 kriptográfiai egységtől származó kódolt adatot a 195 hordozóeszközre rögzítjük. Itt a rögzítő/lejátszó kilép a rögzítési eljárásból.

Megjegyezzük, hogy a 120 bemenet/kimenet I/F-hez biztosított digitális jelek magukban foglalnak EMI-t. Abban az esetben, amikor digitális tartalmat rögzítünk, az EMI-t, vagy az EMI-hez hasonló valamely másolás vezérlési állapotot jelző információt (például a DTCP-ben definiált beágyazott CCI-t vagy hasonlót) a digitális tartalommal együtt rögzítjük.

Általában az „egy generálásig másolható" tartalmat jelentő információt átalakítjuk „többé nem másolható" tartalmat jelentő információvá és rögzítjük egy előre meghatározott korlátnál több másolás megtiltására.

A jelen találmány szerinti rögzítő/lejátszó a TS csomagokhoz hozzáfűzve rögzíti a másolás vezérlési információt, például EMI-t, beágyazott CCI-t stb. Vagyis, mint a 10. ábrán lévő 2. és 3. példákban, minden egyes TS csomaghoz hozzáfűzünk 32 bitet, amely magában foglal 24 - 30-bites ATS-t és másolás vezérlési információt, amint azt az 5. ábrán mutatjuk.

Analóg jelekből álló valamely külső tartalomnak egy hordozóeszközre való rögzítéséhez egy olyan rögzítési eljárást hajtunk végre, mint amilyet a 40B ábrán lévő folyamatábrán mutatunk. A 40B ábrán bemutatott rögzítési eljárást írjuk le az alábbiakban. Egy analóg jelekből álló tartalmat (analóg tar-

talmat) biztosítunk a 140 bemenet/kimenet I/F-hez az S4011 lépésben. Ezután a rögzítő/lejátszó az S4012 lépésre halad, ahol eldönti, hogy a fogadott analóg tartalom másolható-e vagy sem.

Az S4012 lépésben a döntést az alapján hozzuk meg, hogy a 140 bemenet/kimenet I/F által fogadott jelek magukban foglalnak-e egy Macrovision jelet és CGMS-A (copy generation management system - analog, másolás generálási irányítási rendszer - analóg) jelet vagy sem. Amikor egy VHS videó kazettta szalagra rögzítjük, a Macrovision jel egy zaj lesz. Amikor a 140 bemenet/kimenet I/F által fogadott jelek magukban foglalják ezt a Macrovision jelet, azt a döntést hozzuk, hogy az analóg tartalom nem másolható.

A CGMS-A jel egy digitális jelek másolás vezérlésénél használt CGMS jel, és analóg jelek másolás vezérlésére alkalmazzuk. Ez jelzi, hogy egy tartalom szabadon másolható vagy egyszer illetve nem másolható (szabadon másolható, egy generálásig másolható, vagy sosem másolható).

Ezért ha a 140 bemenet/kimenet I/F által fogadott jel magában foglalja a CGMS-A jelet és az azt jelenti, hogy „szabadon másolható" vagy „egy generálásig másolható", akkor azt a döntést hozzuk, hogy az analóg tartalom másolható. Amikor a CGMS-A jel azt jelenti, hogy „sosem másolható", akkor azt a döntést hozzuk, hogy az analóg tartalom nem másolható.

Ezen kívül abban az esetben, amikor a 140 bemenet/kimenet I/F által fogadott jelek nem foglalják magukban sem a Macrovision jelet, sem pedig a CGMS-A jelet, akkor azt a döntést hozzuk, hogy az analóg tartalom nem másolható.

Ha az S4012 lépésben a döntés eredménye az, hogy az analóg tartalom nem másolható, a 100 rögzítő/lejátszó átugorja az

S4013-S4017 lépéseket, és kilép a rögzítési eljárásból. Ebben az esetben ezért a tartalmat nem rögzítjük a 195 hordozóeszközre.

Továbbá, ha az S4012 lépésben a döntés eredménye az, hogy az analóg tartalom másolható, akkor a rögzítő/lejátszó az S4013 lépésre halad. Ezt követően az S4013-S4017 lépésekben a 3B ábrán bemutatott S322-S326 lépésekben lévő műveletekhez hasonlóakat hajtunk végre, ami által a tartalmat digitális tartalommá alakítjuk át, és azután MPEG-kódolásnak, TS feldolgozásnak és kódolásnak vetjük alá a hordozóeszközre való rögzítéshez. Itt a rögzítő/lejátszó kilép a rögzítési eljárásból.

Megjegyezzük, hogy amikor a 140 bemenet/kimenet I/F által fogadott analóg jelek magukban foglalják a CGMS-A jelet, akkor az analóg tartalomnak a hordozóeszközre való rögzítésekor a CGMS-A jelet is rögzítjük a hordozóeszközre. Nevezetesen a CGMS-A jelet a 10. ábrán bemutatott CCI vagy más információ helyett rögzítjük. Általában az „egy generálásig másolható" jelentésű információt „többé nem másolható" információvá alakítjuk át a rögzítéshez, egy előre meghatározott korlátnál több másolás tiltására. Viszont ilyen információ-átalakítást nem hajtunk végre feltéve, hogy a rendszerhez kialakítottunk egy olyan szabályt, hogy az „egy generálásig másolható" másolás vezérlési információt nem alakítjuk át „többé nem másolható" információvá a rögzítéshez, hanem „többé nem másolható" információnak vesszük.

A következőkben a tartalmat beolvassuk a hordozóeszközről, és digitális tartalomként kimenetre tesszük kívülre, amint azt a 41A ábrán lévő folyamatábrán mutatjuk. A 41A ábrán bemutatott műveleteket írjuk le. Először az S4101, S4102 és

S4103 lépésekben a 4A ábrán bemutatott S401, S402 és S403 lépésekben lévő műveletekhez hasonlóakat hajtunk végre, ami által a hordozóeszközről beolvasott kódolt tartalmat dekódoljuk a 150 kriptográfiai egység által, és TS feldolgozásnak vetjük alá. Miután a digitális tartalmat alávetettük ezeknek a folyamatoknak, azt a 120 bemenet/kimenet I/F-hez biztosítjuk a 110 sínen keresztül.

Az S4104 lépésben a 120 bemenet/kimenet I/F eldönti, hogy a hozzá biztosított digitális tartalom később másolható-e vagy sem. Nevezetesen abban az esetben, amikor a 120 bemenet/kimenet I/F-hez biztosított digitális tartalom nem foglal magában EMI-t vagy valamely az EMI-hez hasonló, másolás vezérlési állapotot jelző információt (másolás vezérlési információt), akkor olyan döntést hoz, hogy a tartalom később másolható.

Továbbá abban az esetben, amikor a 120 bemenet/kimenet I/F-hez biztosított digitális tartalom magában foglal például EMI-t, nevezetesen abban az esetben, amikor az adat rögzítés közben egy EMI-t rögzítettünk a DTCP szabvánnyal összhangban, és ha az EMI (a rögzített EMI) azt jelenti, hogy „szabadon másolható", akkor olyan döntést hozunk, hogy a digitális tartalom később másolható. Ezen kívül, amikor az EMI azt jelenti, hogy „többé nem másolható", akkor olyan döntést hozunk, hogy a tartalom később nem másolható.

Emlékeztetnünk kell arra, hogy általában a rögzített EMI nem azt jelenti, hogy „egy generálásig másolható" és „sosem másolható", mert egy „egy generálásig másolható" jelentésű EMI-t az adat rögzítés közben „többé nem másolható" jelentésűvé alakítjuk át, és egy „sosem másolható" jelentésű EMI-vel

rendelkező digitális tartalmat nem rögzítünk a hordozóeszközre. Viszont az EMI átalakítását nem hajtjuk végre feltéve, hogy a rendszer számára definiáltunk egy olyan szabályt, hogy az „egy generálásig másolható" másolás vezérlési információt nem alakítjuk át „többé nem másolható" információvá a rögzítéshez, hanem „többé nem másolható" információnak vesszük.

Ha az S4104 lépésben a döntés eredménye az, hogy a tartalom később másolható, akkor a 120 bemenet/kimenet I/F az S4105 lépésre halad, ahol kimenetre teszi a digitális tartalmat kívülre és kilép a lejátszási eljárásból.

Ezen kívül, ha az S4104 lépésben a döntés eredménye az, hogy a tartalom később nem másolható, akkor a 120 bemenet/kimenet I/F az S4106 lépésre halad, ahol kimenetre teszi a digitális tartalmat a DTCP vagy hasonló szerint egy olyan formában, amely nem másolható, és kilép a lejátszási eljárásból.

Más szóval, abban az esetben, amikor a rögzített EMI azt jelenti, hogy „többé nem másolható", mint a fentiekben (vagy a rendszer számára definiáltunk egy olyan szabályt, hogy például az „egy generálásig másolható" másolás vezérlési információt nem alakítjuk át „többé nem másolható" információvá a rögzítéshez, hanem „többé nem másolható" információnak vesszük, és az ezen feltétel mellett rögzített EMI „egy generálásig másolható" jelentésű), akkor megtiltjuk a tartalom további másolását.

Ily módon a 120 bemenet/kimenet I/F kölcsönös hitelesítést hajt végre egy ellenkező oldali eszközzel a DTCP szabvány szerint. Ha az ellenkező oldali eszköz legális (itt egy olyan eszköz, amely megfelel a DTCP szabványnak), akkor a 120 beme-

net/kimenet I/F kódolja a digitális tartalmat, és kimenetre teszi az adatot kívülre.

Ezután a tartalomnak a hordozóeszközről való lejátszásához és az adatnak analóg tartalomként való kimenetre tételéhez a lejátszást oly módon végezzük el, amint azt a 41B ábrán lévő folyamatábrán mutatjuk. A lejátszáshoz végrehajtott műveleteket a 41B ábrára való hivatkozással írjuk le. Az S4111-S4115 lépésekben a 4B ábrán bemutatott S421-S425 lépésekben lévőekhez hasonló műveleteket végzünk el. Vagyis egy kódolt tartalmat beolvasunk, majd alávetjük dekódolásnak, TS feldolgozásnak, MPEG dekódolásnak és D/A átalakításnak. A 140 bemenet/kimenet I/F egy ily módon biztosított analóg tartalmat fogad.

Az S4116 lépésben a 140 bemenet/kimenet I/F eldönti, hogy egy hozzá biztosított tartalom később másolható-e vagy sem. Nevezetesen abban az esetben, amikor nem talál a rögzített tartalommal együtt rögzített másolás vezérlési információt, olyan döntést hoz, hogy a tartalom később másolható.

Abban az esetben, amikor EMI-t vagy másolás vezérlési információt rögzítettünk a tartalom rögzítés közben például a DTCP szabvánnyal összhangban, és ha az EMI vagy másolás vezérlési információ azt jelenti, hogy „szabadon másolható”, akkor olyan döntést hoz, hogy a tartalom később másolható.

Ezen kívül abban az esetben, amikor az EMI vagy másolás vezérlési információ azt jelenti, hogy „többé nem másolható”, illetve abban az esetben, amikor a rendszer számára definiáltunk egy olyan szabályt, hogy például az „egy generálásig másolható” másolás vezérlési információt nem alakítjuk át „többé nem másolható” információvá, hanem „többé nem másolható” in-

formációnak vesszük, és ha az ezen feltétel mellett rögzített EMI vagy másolás vezérlési információ azt jelenti, hogy „egy generálásig másolható", akkor olyan döntést hozunk, hogy a tartalom később nem másolható.

Továbbá abban az esetben, amikor a 140 bemenet/kimenet I/F-hez biztosított valamely analóg tartalom magában foglal egy CGMS-A jelet, nevezetesen abban az esetben, amikor a CGMS-A jelet a tartalommal együtt rögzítettük az adat rögzítés közben, és ha a CGMS-A jel azt jelenti, hogy „szabadon másolható", akkor olyan döntést hozunk, hogy az analóg tartalom később másolható. Ezen kívül, amikor a CGMS-A jel azt jelenti, hogy „sosem másolható", akkor olyan döntést hozunk, hogy az analóg jel később nem másolható.

Ha az S4116 lépésben a döntés eredménye az, hogy a tartalom később másolható, akkor a 140 bemenet/kimenet I/F az S4117 lépésre halad, ahol kimenetre teszi a hozzá biztosított analóg jeleket úgy, ahogy vannak, és kilép a lejátszási eljárásból.

Ezen kívül, ha az S4116 lépésben a döntés eredménye az, hogy az analóg tartalom később nem másolható, akkor a 140 bemenet/kimenet I/F az S4118 lépésre halad, ahol kimenetre teszi az analóg tartalmat egy olyan formában, hogy a tartalom nem másolható, és kilép a lejátszási eljárásból.

Nevezetesen abban az esetben, amikor a másolás vezérlési információ, például a rögzített EMI azt jelenti, hogy „többé nem másolható", mint a fentiekben (alternatívaként abban az esetben, amikor a rendszer számára definiáltunk egy olyan szabályt, hogy például az „egy generálásig másolható" másolás vezérlési információt nem alakítjuk át „többé nem másolható" információvá, hanem „többé nem másolható" információnak vesszük,

és ha az ezen feltétel mellett rögzített másolás vezérlési információ, például az EMI azt jelenti, hogy „egy generálásig másolható"), akkor megtiltjuk a tartalom további másolását.

Ily módon a 140 bemenet/kimenet I/F egy jelet és egy „sosem másolható" jelentésű CGMS-A jelet fűz hozzá az analóg tartalomhoz, és kimenetre teszi az analóg tartalmat kívülre. Ezen kívül abban az esetben, amikor a rögzített CGMS-A jel például azt jelenti, hogy „sosem másolható", megtiltjuk a tartalom további másolását. Így a 140 bemenet/kimenet I/F a CGMS-A jelet „sosem másolható" jelentésűre módosítja, és kimenetre teszi az analóg tartalommal együtt kívülre.

Csakúgy, mint a fentiekben, valamely tartalom másolásának rögzítés/lejátszás közbeni vezérlése által lehetséges a tartalom megóvása valamely a tartalom számára megengedett tartományon túl való másolásától (illegális másolástól).

Megjegyezzük, hogy a műveleteknek az előzőekben említett sorozatát végrehajthatjuk hardver vagy egy szoftver által. Nevezetesen a 150 kriptográfiai egységet kialakíthatjuk egy kódolási/dekódolási LSI-ből, továbbá a 150 kriptográfiai egység általi kriptográfiát, nevezetesen a kódolást/dekódolást is elvégezhetjük egy általános célú számítógép vagy egy egychipes mikroszámítógép által, amelyek egy megfelelő programot hajtanak végre. Hasonlóan, a 300 TS feldolgozó műveleteit is végrehajthatjuk egy szoftver által. A TS feldolgozáshoz a műveletek sorozatának egy szoftver általi végrehajtásához valamely, a szoftvert magában foglaló programot telepítünk egy általános célú számítógépre, egychipes mikroszámítógépre vagy hasonlóra. A 42. ábra egy példát mutat egy olyan számítógép egyik kivite-

li példájának konstrukciójára, amelyben a műveletek sorozatához a programot telepítettük.

A programot előre rögzíthetjük a számítógépben hordozóeszközként alkalmazott valamely 4205 merevlemezen és 4203 ROM-ban. Alternatívaként a programot tárolhatjuk ideiglenesen vagy véglegesen egy 4210 eltávolítható hordozóeszközön, például egy floppy lemezen, CD-ROM-on (compact disc read-only memory), MO (magneto-optikai) lemezen, DVD-n (digital versatile disc), mágnes lemezen, félvezető memóriában vagy hasonlóban. Egy ilyen 4210 eltávolítható hordozóeszközt biztosíthatunk egy úgynevezett csomag szoftverként (package software).

Emlékeztetnünk kell arra, hogy a programot telepíthetjük a fentiekben említett 4210 eltávolítható hordozóeszközről egy számítógépre, vagy másképpen, átvihetjük egy letöltési oldalról (download site) a számítógépre egy rádió kommunikációs hálózat által egy digitális adás műholdon keresztül, illetve átvihetjük a számítógépre egy kábelen egy hálózaton, például LAN-on (local area network, lokális területi hálózat), Interneten vagy hasonlón keresztül, majd a számítógép fogadja az ily módon átvitt programot egy 4208 kommunikációs egysége által, és telepíti azt a beépített 4205 merevlemezre.

A számítógép, amint azt mutatjuk, alkalmaz egy 4202 CPU-t. A 4202 CPU-t összekapcsoljuk egy 4211 bemenet/kimenet interfésszel egy 4201 sínen keresztül. Amikor a 4202 CPU-hoz biztosítunk a felhasználó által működtetett valamely 4207 bemeneti egységről, például egy billentyűzetről, egérről vagy hasonlóról egy utasítást, a 4211 bemenet/kimenet interfészen keresztül, akkor a számítógép végrehajtja a valamely 4203 ROM-ban tárolt programot.

Alternatívaként a 4202 CPU betölt egy 4204 RAM-ba (random access memory, közvetlen hozzáférésű memória) végrehajtásra egy programot, amelyet a 4205 merevlemezen tárolunk, egy programot, amelyet egy műholdról vagy hálózatról viszünk át, a 4208 kommunikációs egység által fogadunk és a 4205 merevlemezre telepítünk, vagy egy programot, amelyet egy 4209 meghajtóba helyezett 4210 eltávolítható hordozóeszközről olvasunk és a 4205 merevlemezre telepítünk.

Ily módon a 4202 CPU a megelőzően említett folyamatábrák szerinti műveleteket vagy a megelőzően említett blokk diagramok szerinti műveleteket hajtja végre. A 4202 CPU ezeknek a műveleteknek az eredményeit egy 4206 kimeneti egységről, például egy LCD-ről (liquid crystal display, folyadékkristály kijelző) vagy egy hangszóróról (speaker) kimenetre teszi, vagy továbbítja őket a 4208 kommunikációs egységtől, vagy rögzíti őket a 4205 merevlemezre, a 4211 bemenet/kimenet interfészen keresztül, ha szükséges.

Megjegyezzük, hogy a műveleteket és folyamatokat, amelyek egy olyan programot írnak le, amely a számítógép számára változatos műveletek végrehajtását teszi lehetővé, nem lehet mindig olyan időrendben végrehajtani, mint a folyamatábrákon, lehetnek közöttük olyanok is, amelyeket párhuzamosan vagy egyedileg hajtunk végre (például párhuzamos folyamatok vagy objektumok általi folyamatok).

A program lehet olyan, amelyet egyetlen számítógép hajthat végre, vagy olyan, amelyet decentralizált módon számítógépek sokasága hajthat végre. Továbbá a program lehet olyan, hogy amelyet átvihetünk egy távoli számítógépre a végrehajtáshoz.

A fentiekben a jelen találmányt egy olyan példa vonatkozásában írtuk le, amelyben egy egychipes kódolási/dekódolási LSI által alkotott kriptográfiai blokk kódol és dekódol egy tartalmat. Megjegyezzük viszont, hogy a tartalom kódolási/dekódolási blokk lehet egyetlen szoftver modul is, amelyet például az 1. és 2. ábrákon mutatott 170 CPU hajt végre. Hasonlóképpen a 300 TS feldolgozó műveletei is elvégezhetőek egyetlen szoftver modul által, amelyet a 170 CPU hajt végre.

A jelen találmány biztosít továbbá egy információ hordozóeszköz létrehozó berendezést és eljárást a jelen találmány szerinti, fent említett információ hordozóeszköz létrehozásához. Az alábbiakban a berendezést és eljárást írjuk le.

A 43. ábra körvonalazza a lemez gyártási berendezést, amelyet egy hordozóeszköz gyártásához használunk, és amely a hordozóeszközre rögzít egy lemez ID-t, kulcs megújítási blokkot és egy kódolt mester kulcsot vagy közeg kulcsot.

A 43. ábrán bemutatott lemez gyártási berendezés rögzít egy lemez ID-t, kulcs megújítási blokkot és egy kódolt mester kulcsot vagy közeg kulcsot egy olyan hordozóeszközre, amelyet már összeállítottunk egy összeállítási folyamatban (nem mutatjuk), és a hordozóeszközre rögzíti továbbá a mester kulcs egy Generálás#n elő-rögzítési generálási számát, ha szükséges.

Egy 4300 lemez gyártási berendezés magában foglal egy 4302 memóriát, amelyben előre eltároltunk egy lemez ID-t, kulcs megújítási blokkot és kódolt mester kulcsot vagy közeg kulcsot, illetve bármely más memória eszközt, egy 4303 hordozóeszköz I/F-et, ami a valamely 4350 hordozóeszközre való írást és onnan való olvasást hajtja végre, egy 4304 bemenet/kimenet I/F-et, ami egy interfész más eszközökhöz, egy

4301 vezérlőt, amely vezérli a fenti komponenseket, továbbá egy 4305 sínt, amely összekapcsolja a fenti komponenseket egymással.

A 43. ábrán mutatott példában a 4302 memóriát és a 4303 hordozóeszköz I/F-et beépítettük a 4300 lemez gyártási berendezésbe. Ennek ellenére a 4302 memória és a 4303 hordozóeszköz I/F lehetnek külső eszközök a 4300 lemez gyártási berendezéshez való csatlakozáshoz.

A lemez ID-t, kulcs megújítási blokkot, kódolt mester kulcsot vagy közeg kulcsot és a Generálás#n elő-rögzítési generálási számot például egy kulcs kibocsátó központ bocsátja ki, és ezeket a beépített vagy külső memóriában előre eltároljuk.

A 4302 memóriában tárolt lemez ID-t, kulcs megújítási blokkot és kódolt mester kulcsot vagy közeg kulcsot rögzítjük a hordozóeszközre a 4303 hordozóeszköz I/F-en keresztül a 4301 vezérlő vezérlése alatt. Megjegyezzük, hogy a Generálás#n elő-rögzítési generálási számot a hordozóeszközre rögzítjük, ha szükséges.

Ezen kívül a 4302 memóriában tárolt lemez ID, kulcs megújítási blokk, kódolt mester kulcs vagy közeg kulcs, illetve a Generálás#n elő-rögzítési generálási szám lehetnek azok, amelyeket, amint azt a fentiekben említettük, a 4302 memóriában előre eltároltunk, csakúgy, mint másokat is, amelyeket a kulcs kibocsátó központ küldött például a 4304 bemenet/kimenet I/F-en keresztül.

A 44. ábra a jelen találmány szerinti hordozóeszköz létrehozási eljárásnál végrehajtott műveletek egy folyamatát mutatja be a hordozóeszköz létrehozására és egy lemez ID-nek,

kulcs megújítási blokknak, kódolt mester kulcsnak vagy közeg kulcsnak és egy Generálás#n elő-rögzítési generálási számnak a hordozóeszközre való rögzítésére.

A hordozóeszköz létrehozási eljárásban először a 44. ábrán lévő S4401 lépésben összeállítunk egy hordozóeszközt, például egy DVD-t, CD-t vagy hasonlót egy jól ismert összeállítási folyamatban (nem mutatjuk).

Ezután az S4402 lépésben a 43. ábrán bemutatott rögzítő/lejátszó rögzít a fent leírtak szerint létrehozott hordozóeszközre egy lemez ID-t, kulcs megújítási blokkot és kódolt mester kulcsot vagy közeg kulcsot. Ezen kívül a rögzítő/lejátszó, ha szükséges, rögzít a hordozóeszközre egy Generálás#n elő-rögzítési generálási számot.

A fenti lemez gyártási folyamat befejezése után a gyárból elszállítjuk a hordozóeszközt, amelyre rögzítettünk egy lemez ID-t, kulcs megújítási blokkot és egy kódolt mester kulcsot vagy közeg kulcsot. Ezen kívül, miután szükség szerint rögzítettünk egy Generálás#n elő-rögzítési generálási számot, a hordozóeszközt elszállítjuk a gyárból.

A 45. ábra a kulcs megújítási blokk egy példa formátumát mutatja be. A formátumban a 4501 „Verzió" azonosítja a kulcs megújítási blokk verzióját. A 4502 „Mélység" jelzi egy olyan eszközhöz tartozó kulcs megújítási blokk hierarchikus fája szintjeinek a számát, amelyhez a hordozóeszközt rendeljük. A 4503 „Adat mutató" jelzi a kulcs megújítási blokkban valamely adat rész pozícióját, és a 4504 „Címke mutató" jelzi valamely címke rész pozícióját. A 4505 „Aláírás mutató" jelzi valamely aláírás pozícióját. A 4506 „Adat részben" tároljuk például a

megújítandó csomópont kulcsok kódolásából származtatott adatokat.

A 4507 „Címke rész" egy olyan címke, amely az adat részben tárolt kódolt csomópont kulcsok és levél kulcsok geometriáját jelzi. A címke hozzáfűzési szabályt a 46. ábrára való hivatkozással írjuk le, amely egy példát mutat a megelőzően a 12A ábrára való hivatkozással leírt kulcs megújítási blokk elküldésére. Az aktuális adat az, amelyiket a 46. ábrán a jobb oldali táblázatban mutatunk. Az aktuális kódolási kulcs által tartalmazott valamely legfelső csomópont címét vesszük legfelső csomópont címként. Ebben az esetben, mivel a legfelső csomópont cím egy gyökér kulcs K(t)R megújítási kulcsát tartalmazza, azért ez „KR" lesz.

Amint azt a 46. ábrán mutatjuk, a kódolási kulcsban a legfelső szinten lévő Enc(K(t)0, K(t)R) adat a mutatott hierarchikus fában az ábra baloldali részletén helyezkedik el. Az Enc(K(t)0, K(t)R) adat mellett az Enc(K(t)00, K(t)0) adat van a megelőző adat egy baloldali legalsó pozíciójában. Amikor ott nincs adat, a címkét „0"-ra állítjuk. Amikor ott van adat, a címkét „1"-re állítjuk. A címkét a következőképpen állítjuk össze: {bal(L)címke, jobb(R)címke}. Mivel létezik adat az Enc(K(t)0, K(t)R) legfelső adattól balra, a címke Lcímke=0 lesz. Az Enc(K(t)0, K(t)R) adattól jobbra nincs adat, ezért a címke Rcímke=1 lesz. A címkéket az összes adat számára beállítjuk ily módon, amelyek adat sort és címke sort alkotnak, amint azt a 46C ábrán mutatjuk. A fában lévő csomópontokat előnyösen „szélességi bejárás" („width first") vagy „mélységi bejárás" („depth first") eljárással dolgozzuk fel. A „szélességi bejárás" eljárásban először az azonos szinten lévő

csomópontokat dolgozzuk fel, a szint irányában. A „mélységi bejárás" eljárásban a mélység irányában dolgozzuk fel először a csomópontokat.

A KRB formátumot ismét a 45. ábrára való hivatkozással tárgyaljuk tovább. A formátumban az „Aláírás" egy elektronikus aláírás, amelyet az a kulcs kibocsátó központ, tartalom szolgáltató, intéző hivatal vagy hasonló készített, amely a kulcs megújítási blokkot kibocsátotta. Egy KRB-t fogadó eszköz aláírás ellenőrzés által megerősíti, hogy a fogadott KRB olyan, amelyet egy legális kulcs megújítási blokk kibocsátó fél számára bocsátottak ki.

Az ezt megelőzőekben a jelen találmányt részletesen leírtuk annak meghatározott kiviteli példáinak tekintetében. Látható viszont, hogy egy a tárgykörben járatos személy módosíthatja vagy megváltoztathatja a jelen találmányt anélkül, hogy eltérne annak lényegétől és tárgykörétől. Vagyis a jelen találmány kiviteli példáit csak példaként írtuk le, és a jelen találmány nem korlátozódik ezekre a kiviteli példákra. A jelen találmány lényegére a későbbiekben definiált igénypontok hivatkoznak.

Amint azt az előzőekben leírtuk, mivel a fa-struktúrájú kulcs kiosztási rendszer egy mester kulcs vagy közeg kulcs megújított adatának mindegyikét egy kulcs megújítási blokkal együtt továbbítja, azért a jelen találmány szerinti információ rögzítő/lejátszó képes arra, hogy csak egy olyan eszköznek továbbítson vagy osszon ki dekódolható kulcsokat, amelyben a kulcsokat meg kell újítanunk, és így a kiosztandó üzenetet csökkenthetjük. Továbbá csökkentett üzenet mérettel oszthatunk ki egy olyan kulcsot, amely a fa struktúra által definiált

eszközöknek csak egy meghatározott csoportja által dekódolható, és amely nem dekódolható a csoporthoz nem tartozó egyetlen másik eszköz által sem, ily módon biztosíthatjuk a kulcs kiosztás vagy továbbítás biztonságát.

Ezen kívül a jelen találmány szerint az egyes rögzítő/lejátszókhoz a fa-struktúrájú kulcs kiosztási rendszer által továbbítandó valamely kulcs kehet egy mester kulcs, amely közösen használható egy a fa struktúra által tartalmazott valamely meghatározott csoport által definiált rendszerben, vagy lehet egy közeg kulcs, amely egyedi az egyes hordozóeszközök számára. Azáltal, hogy egy olyan KRB-t generálunk, amely egyedi az egyes rögzítő/lejátszók vagy hordozóeszközök számára, majd azt eljuttatjuk hozzájuk egy hálózaton vagy közegen keresztül, lehetségessé válik a kulcs egyszerű és biztonságos megújítása.

Ily módon a jelen találmány szerint lehetséges egy olyan információ rögzítő/lejátszó rendszer felépítése, amelyben megakadályozhatjuk a szerzői jog által védett adatoknak, például filmnek, zenének vagy hasonlónak az illegális (a szerzői jog tulajdonosának akaratával ellenkező) másolását.

Egy olyan, generálás-irányított mester kulcsot használó rendszer elrendezésével, amelyben egy új generálású, KRB-megújított mester kulcsot kioszthatunk, lehetséges egy egyedi kulcs blokk generálása egy olyan eszköz irányában, amely képes megújítani egy a KRB-vel együtt kiosztott és kódolt megújított mester kulcsot. Ezért a jelen találmány szerint lehetséges egy olyan kódolt mester kulcs generálása, amely csak egy olyan eszköz által dekódolható, amelynek szüksége van a mester kulcs megújítására, és lehetséges a kulcs biztonságos megújítása

anélkül, hogy minden egyes eszközzel végre kellene hajtanunk a hagyományos hitelesítést.

Továbbá a jelen találmány szerinti információ rögzítő/lejátszóban és információ rögzítési/lejátszási eljárásban az adatnak egy hordozóeszközre való tárolásához nem csak egy generálás-irányított mester kulccsal vagy közeg kulccsal való kódolást hajtunk végre, hanem a beállítható lejátszó korlátozással való kódolást is. Ennek a rendszernek köszönhetően adatot úgy rögzítünk egy hordozóeszközre, hogy egy eszköz-egyértelmű kulccsal befolyásoljuk azt a kódolási kulcsot, amellyel az adatot kódoltuk, amikor a lejátszó korlátozás be van állítva (az adat egy korlátozással rendelkező lejátszóban játszható le). Abban az esetben, amikor a lejátszó korlátozás nincs beállítva, egy eszköz ID-vel befolyásoljuk azt a kódolási kulcsot, amellyel az adatot kódoltuk, ezáltal kódoljuk a hordozóeszközre rögzítendő adatot. Továbbá, mivel a hordozóeszközre rögzítünk eszköz azonosítási információt az adatot rögzítő eszközről, valamint információt, amely azt jelzi, hogy melyiket használtuk az adat rögzítéséhez, a lejátszó korlátozási módot vagy a lejátszó nem-korlátozási módot (lejátszó korlátozás jelzőt), azért csak egy olyan eszköz dekódolhatja az adatot akkor, amikor a lejátszó korlátozás be van állítva, amely ismeri az eszköz-egyértelmű kulcsot és amely az adatot rögzítette. Amikor a lejátszó korlátozás nincs beállítva, bármelyik eszköz dekódolhatja az adatot egy eszköz azonosítási információval (eszköz ID-vel) ahhoz az eszközhöz, amely az adatot rögzítette.

Ezen kívül a jelen találmány szerinti információ rögzítő/lejátszó berendezés és eljárás egy kódolási blokk kulcsot

generálnak blokk adatokhoz egy ATS alapján, amely annak az időpontnak megfelelő véletlenszerű adat, amikor az egyes csomagok megérkeznek. Ezért lehetséges egy olyan egyedi kulcs generálása, amely blokkonként változik, lehetséges továbbá különböző kódolási kulcs használata minden egyes blokkhoz és így a védelem javítása az adat kriptoanalízis (titkosítás-elemzés) ellen. Továbbá azáltal, hogy egy blokk kulcsot az ATS alapján generálunk, a hordozóeszközön nem kell biztosítanunk területet minden egyes blokk kódolási kulcsának tárolására, és ily módon a fő adat területet hatékonyabban használhatjuk. Ezen kívül még az adat rögzítés vagy lejátszás közben nem kell a fő adattól különböző adatokhoz hozzáférnünk, és ezért az adat rögzítést vagy lejátszást nagyobb hatékonysággal végezhetjük el.

Szabadalmi igénypontok

1. Berendezés információ rögzítésére hordozóeszközön, **azzal jellemezve,** hogy a berendezés magában foglal:

kriptográfiai eszközt, amely rendelkezik olyan hierarchikus fa struktúra által tartalmazott csomópontok mindegyike számára egyedi csomópont kulccsal, amely magában foglalja különböző információ rögzítők sokaságát a fa struktúra egyes leveleiként, valamint levél kulccsal, ami egyedi az információ rögzítők mindegyike számára, továbbá amely kódolja a hordozóeszközön eltárolandó adatot;

a kriptográfiai eszköz kódolási kulcsot generál az információ rögzítőbe beépített kódolási kulcs generáló adat alapján a hordozóeszközön eltárolandó adat kódolására; és

a kódolási kulcs generáló adat olyan adat, amelyet megújíthatunk a csomópont kulcs vagy levél kulcs legalább egyikével.

2. Az 1. igénypont szerinti berendezés, **azzal jellemezve,** hogy a kódolási kulcs generáló adat mester kulcs, amely közös az információ rögzítők sokasága számára.

3. Az 1. igénypont szerinti berendezés, **azzal jellemezve,** hogy a kódolási kulcs generáló adat közeg kulcs, amely egyedi meghatározott hordozóeszköz számára.

4. Az 1. igénypont szerinti berendezés, **azzal jellemezve,** hogy:

a csomópont kulcsot megújíthatjuk;

amikor csomópont kulcsot megújítunk, kiosztunk olyan levélnél lévő információ rögzítő számára, ahol a kódolási kulcs generáló adatot meg kell újítanunk kulcs megújítási blokkot, amelyet a megújítási csomópont kulcsnak a fa struktúra alacsonyabb szintjén lévő csomópont kulcs vagy levél kulcs legalább egyikével való kódolásából származtatunk; és

a kriptográfiai eszköz az információ rögzítőben megújítási adatot fogad a megújított csomópont kulccsal kódolt kódolási kulcs generáló adathoz, kódolja a kulcs megújítási blokkot a megújított csomópont kulcs megszerzéséhez, majd kiszámít megújítási adatot a kódolási kulcs generáló adat számára az így megszerzett megújított csomópont kulcs alapján.

5. A 4. igénypont szerinti berendezés, **azzal jellemezve,** hogy:

a kulcs megújítási blokkot hordozóeszközön tároljuk; és

a kriptográfiai eszköz kódolja a hordozóeszközről beolvasott kulcs megújítási blokkot.

6. Az 1. igénypont szerinti berendezés, **azzal jellemezve,** hogy:

a kódolási kulcs generáló adat rendelkezik generálási számmal vele korrelációban lévő megújítási információként; és

a kriptográfiai eszköz eltárolja a rögzítő tagba rögzítési generálási számként annak a kódolási kulcs generáló adatnak generálási számát, amelyet kódolt adatnak a hordozóeszközre való tárolásakor használtunk.

7. Az 1. igénypont szerinti berendezés, **azzal jellemezve,** hogy a következő kódoló eljárásokat szelektív módon hajtjuk végre attól függően, hogy lejátszó korlátozás be van-e állítva vagy sem:

amikor a lejátszó korlátozás nincs beállítva, első kódolási kulcsot generálunk a hordozóeszközön eltárolandó adat számára első kódolási kulcs generáló adat alapján a hordozóeszközön eltárolandó adatnak az első kódolási kulccsal való kódolásához, és az első kódolási kulcs generáló adatot eltároljuk a hordozóeszközön; és

amikor a lejátszó korlátozás be van állítva, második kódolási kulcsot generálunk a hordozóeszközön eltárolandó adat számára az információ rögzítőbe beépített második kódolási kulcs generáló adat alapján a hordozóeszközön eltárolandó adatnak a második kódolási kulccsal való kódolásához.

8. A 7. igénypont szerinti berendezés, **azzal jellemezve,** hogy a kriptográfiai eszköz a következőt hajtja végre attól függően, hogy a lejátszó korlátozás be van állítva vagy sem:

amikor a lejátszó korlátozás nincs beállítva, a kriptográfiai eszköz cím-egyértelmű kulcsot generál az információ rögzítőben tárolt azon mester kulcsból, amely generálását irányítjuk, lemez ID-ből, ami egyedi azonosító hordozóeszköz számára, cím kulcsból, ami egyedi a hordozóeszközre rögzítendő adat számára és eszköz ID-ből, ami azonosító az információ rögzítő számára az első kódolási kulcsnak a cím-egyértelmű kulcsból való generálására; és

amikor a lejátszó korlátozás be van beállítva, a kriptográfiai eszköz cím-egyértelmű kulcsot generál az információ

rögzítőben tárolt generálás-irányított mester kulcsból, lemez ID-ből, ami egyedi azonosító a hordozóeszköz számára, cím kulcsból, ami egyedi a hordozóeszközre rögzítendő adat számára és az eszköz-egyértelmű kulcsból, ami egyedi az információ rögzítő számára a második kódolási kulcsnak a cím-egyértelmű kulcsból való generálására.

9. Az 1. igénypont szerinti berendezés, **azzal jellemezve,** hogy magában foglal továbbá szállítási folyam feldolgozó eszközt szállítási folyam által tartalmazott diszkrét szállítási csomagok mindegyikéhez érkezési időbélyeg hozzáfűzéséhez;

a kriptográfiai eszköz blokk kulcsot generál kódolási kulcsként egynél több olyan csomagot magában foglaló blokk adat számára, amelyek mindegyikéhez hozzáfűztük az érkezési időbélyeget; és

a kriptográfiai eszköz blokk kulcsot generál kódolási kulcsként a hordozóeszközön eltárolandó adat kódolásakor olyan adat alapján, amely magában foglalja a kódolási kulcs generáló adatot és blokk magot, ami további egyedi információ az érkezési időbélyeget magában foglaló blokk adat számára.

10. Az 1. igénypont szerinti berendezés, **azzal jellemezve,** hogy a kriptográfiai eszköz a hordozóeszközön eltárolandó adatot DES algoritmus szerint kódolja.

11. Az 1. igénypont szerinti berendezés, **azzal jellemezve,** hogy:

biztosítunk interfész eszközt hordozóeszközre rögzítendő információ fogadására; és

az interfész eszköz szállítási folyam által tartalmazott csomagok mindegyikéhez hozzáfűzött másolás vezérlési információt azonosít annak eldöntésére a másolás vezérlési információ alapján, hogy a hordozóeszközre való rögzítés lehetséges-e vagy sem.

12. Az 1. igénypont szerinti berendezés, **azzal jellemezve**, hogy:

biztosítunk interfész eszközt hordozóeszközre rögzítendő információ fogadására; és

az interfész eszköz 2-bites EMI-t azonosít másolás vezérlési információként annak eldöntésére az EMI alapján, hogy a hordozóeszközre való rögzítés lehetséges-e vagy sem.

13. Berendezés információ lejátszására hordozóeszközről, **azzal jellemezve**, hogy a berendezés rendelkezik olyan hierarchikus fa struktúra által tartalmazott csomópontok mindegyike számára egyedi csomópont kulccsal, amely magában foglalja különböző információ rögzítők sokaságát a fa struktúra egyes leveleiként, valamint levél kulccsal, ami egyedi az információ rögzítők mindegyike számára, továbbá magában foglal kriptográfiai eszközt a hordozóeszközön tárolt kódolt adat dekódolására;

a kriptográfiai eszköz dekódolási kulcsot generál az információ rögzítőbe beépített dekódolási kulcs generáló adat alapján a hordozóeszközön tárolt kódolt adat dekódolására; és

a dekódolási kulcs generáló adat olyan adat, amelyet megújíthatunk a csomópont kulcs vagy levél kulcs legalább egyikével.

14. A 13. igénypont szerinti berendezés, **azzal jellemezve**, hogy a dekódolási kulcs generáló adat mester kulcs, amely közös az információ rögzítők sokasága számára.

15. A 13. igénypont szerinti berendezés, **azzal jellemezve**, hogy a dekódolási kulcs generáló adat közeg kulcs, amely egyedi meghatározott hordozóeszköz számára.

16. A 13. igénypont szerinti berendezés, **azzal jellemezve**, hogy:

a csomópont kulcsot megújíthatjuk;

amikor csomópont kulcsot megújítunk, kiosztunk olyan levélnél lévő információ lejátszó számára, ahol a kódolási kulcs generáló adatot meg kell újítanunk kulcs megújítási blokkot, amelyet a megújítási csomópont kulcsnak a fa struktúra alacsonyabb szintjén lévő csomópont kulcs vagy levél kulcs legalább egyikével való kódolásából származtatunk; és

a kriptográfiai eszköz az információ rögzítőben megújítási adatot fogad a megújított csomópont kulccsal kódolt dekódolási kulcs generáló adathoz, kódolja a kulcs megújítási blokkot a megújított csomópont kulcs megszerzéséhez, majd kiszámít megújítási adatot a dekódolási kulcs generáló adat számára az így megszerzett megújított csomópont kulcs alapján.

17. A 16. igénypont szerinti berendezés, **azzal jellemezve**, hogy:

a kulcs megújítási blokkot hordozóeszközön tároljuk; és

a kriptográfiai eszköz kódolja a hordozóeszközről beolvasott kulcs megújítási blokkot.

18. A 13. igénypont szerinti berendezés, **azzal jellemezve**, hogy:

a dekódolási kulcs generáló adat rendelkezik generálási számmal vele korrelációban lévő megújítási információként; és

a kriptográfiai eszköz a hordozóeszközről beolvasott kódolt adat dekódolásakor a hordozóeszközről beolvassa a kódolt adat kódolásakor használt kódolási kulcs generáló adat generálási számát, és az így beolvasott generálási számnak megfelelő dekódolási kulcs generáló adatból dekódolási kulcsot generál.

19. A 13. igénypont szerinti berendezés, **azzal jellemezve**, hogy a következő dekódoló eljárásokat szelektív módon hajtjuk végre attól függően, hogy lejátszó korlátozás be van-e állítva vagy sem:

amikor a lejátszó korlátozás nincs beállítva, első dekódolási kulcsot generálunk a hordozóeszközön tárolt kódolt adat számára a hordozóeszközön tárolt első dekódolási kulcs generáló adat alapján a kódolt adatnak az első dekódolási kulccsal való dekódolásához; és

amikor a lejátszó korlátozás be van állítva, második dekódolási kulcsot generálunk a hordozóeszközön tárolt kódolt adat számára az információ rögzítőbe beépített második kódolási kulcs generáló adat alapján a kódolt adatnak a második dekódolási kulccsal való dekódolásához.

20. A 19. igénypont szerinti berendezés, **azzal jellemezve**, hogy a kriptográfiai eszköz a következőt hajtja végre attól függően, hogy a lejátszó korlátozás be van állítva vagy sem:

amikor a lejátszó korlátozás nincs beállítva, a kriptográfiai eszköz megszerez az információ rögzítőben tárolt generálás-irányított mester kulcsot, valamint megszerez hordozóeszközből lemez ID-t, ami egyedi azonosító hordozóeszköz számára, cím kulcsot, ami egyedi a dekódolandó adat számára és eszköz ID-t, ami azonosító azon információ rögzítő számára, amely a kódolt adatot rögzítette cím-egyértelmű kulcs generálására a mester kulcsból, lemez ID-ből, cím kulcsból és eszköz kulcsból és az első dekódolási kulcsnak a cím-egyértelmű kulcsból való generálására; és

amikor a lejátszó korlátozás be van beállítva, a kriptográfiai eszköz megszerez az információ rögzítőben tárolt generálás-irányított mester kulcsot és eszköz-egyértelmű kulcsot, amely egyedi az információ rögzítő számára és abban is tároljuk, valamint megszerez hordozóeszközből lemez ID-t, ami egyedi azonosító a hordozóeszköz számára és cím kulcsot, ami egyedi a dekódolandó adat számára cím-egyértelmű kulcs generálására a mester kulcsból, lemez ID-ből, cím kulcsból és eszköz-egyértelmű kulcsból és a második dekódolási kulcsnak a cím-egyértelmű kulcsból való generálására.

21. A 13. igénypont szerinti berendezés, **azzal jellemezve**, hogy magában foglal továbbá szállítási folyam feldolgozó eszközt adat kimenetre tételének vezérlésére a kriptográfiai eszköz által dekódolt blokk adat által tartalmazott szállítási

csomagok sokaságának mindegyikéhez hozzáfűzött érkezési időbélyeg alapján;

a kriptográfiai eszköz blokk kulcsot generál dekódolási kulcsként egynél több olyan csomagot magában foglaló blokk adat számára, amelyek mindegyikéhez hozzáfűztük az érkezési időbélyeget; és

a blokk kulcsot dekódolási kulcsként generáljuk a hordozóeszközön tárolt kódolt adat dekódolásakor olyan adat alapján, amely magában foglalja a dekódolási kulcs generáló adatot és blokk magot, ami további egyedi információ az érkezési időbélyeget magában foglaló blokk adat számára.

22. A 13. igénypont szerinti berendezés, **azzal jellemezve**, hogy a kriptográfiai eszköz a hordozóeszközön tárolt kódolt adatot DES algoritmus szerint dekódolja.

23. A 13. igénypont szerinti berendezés, **azzal jellemezve**, hogy biztosítunk továbbá interfész eszközt hordozóeszközre rögzítendő információ fogadására; és

az interfész eszköz adatban lévő szállítási folyam által tartalmazott csomagok mindegyikéhez hozzáfűzött másolás vezérlési információt azonosít annak eldöntésére a másolás vezérlési információ alapján, hogy a hordozóeszközről való lejátszás lehetséges-e vagy sem.

24. A 13. igénypont szerinti berendezés, **azzal jellemezve**, hogy biztosítunk továbbá interfész eszközt hordozóeszközre rögzítendő információ fogadására; és

az interfész eszköz 2-bites EMI-t azonosít másolás vezérlési információként annak eldöntésére az EMI alapján, hogy a hordozóeszközről való lejátszás lehetséges-e vagy sem.

25. Információ rögzítési eljárás információnak hordozóeszközre való rögzítésére, **azzal jellemezve**, hogy az eljárás magában foglalja a következő lépéseket:

megújítunk kódolási kulcs generáló adatot kódolási kulcs generálására hordozóeszközön eltárolandó adat kódolásához legalább vagy csomópont kulccsal, ami egyedi olyan hierarchikus fa struktúra által tartalmazott csomópontok mindegyike számára, amely magában foglalja különböző információ rögzítők sokaságát a fa struktúra egyes leveleiként, vagy levél kulccsal, ami egyedi az információ rögzítők mindegyike számára; és

kódolási kulcsot generálunk a kódolási kulcs generáló adat alapján a hordozóeszközön eltárolandó adat kódolásához.

26. A 25. igénypont szerinti eljárás, **azzal jellemezve**, hogy a kódolási kulcs generáló adat mester kulcs, ami közös az információ rögzítők sokasága számára.

27. A 25. igénypont szerinti eljárás, **azzal jellemezve**, hogy a kódolási kulcs generáló adat közeg kulcs, ami egyedi meghatározott hordozóeszköz számára.

28. A 25. igénypont szerinti eljárás, **azzal jellemezve**, hogy:

a csomópont kulcsot megújíthatjuk;

amikor csomópont kulcsot megújítunk, kiosztunk olyan levélnél lévő információ rögzítő számára, ahol a kódolási kulcs generáló adatot meg kell újítanunk kulcs megújítási blokkot, amelyet a megújítási csomópont kulcsnak a fa struktúra alacsonyabb szintjén lévő csomópont kulcs vagy levél kulcs legalább egyikével való kódolásából származtatunk; és

a megújítási lépés magában foglalja a következő lépéseket:

megszerezzük a megújított csomópont kulcsot a kulcs megújítási blokk kódolása által; és

kiszámítunk megújítási adatot a kódolási kulcs generáló adat számára az így megszerzett megújított csomópont kulcs alapján.

29. A 25. igénypont szerinti eljárás, **azzal jellemezve,** hogy:

a kódolási kulcs generáló adat rendelkezik generálási számmal vele korrelációban lévő megújítási információként; és

a kriptográfiai lépés magában foglalja továbbá azt a lépést, hogy amikor kódolt adatot tárolunk el a hordozóeszközön, eltároljuk a használt kódolási kulcs generáló adat generálási számát a hordozóeszközön rögzítési generálási számként.

30. A 25. igénypont szerinti eljárás, **azzal jellemezve,** hogy a kriptográfiai lépés magában foglalja a következő két eljárást, amelyek egyikét szelektív módon hajtjuk végre attól függően, hogy lejátszó korlátozás be van-e állítva vagy sem:

amikor a lejátszó korlátozás nincs beállítva, első kódolási kulcsot generálunk a hordozóeszközön eltárolandó adat

számára első kódolási kulcs generáló adat alapján, a hordozóeszközön eltárolandó adatot kódoljuk az első kódolási kulccsal, és az első kódolási kulcs generáló adatot eltároljuk a hordozóeszközön; és

amikor a lejátszó korlátozás be van beállítva, második kódolási kulcsot generálunk a hordozóeszközön eltárolandó adat számára az információ rögzítőbe beépített második kódolási kulcs generáló adat alapján, és a hordozóeszközön eltárolandó adatot kódoljuk a második kódolási kulccsal.

31. A 30. igénypont szerinti eljárás, **azzal jellemezve**, hogy a kriptográfiai eszköz a következőt hajtja végre attól függően, hogy a lejátszó korlátozás be van-e állítva vagy sem:

amikor a lejátszó korlátozás nincs beállítva, a kriptográfiai eszköz cím-egyértelmű kulcsot generál az információ rögzítőben tárolt generálás-irányított mester kulcsból, lemez ID-ből, ami egyedi azonosító hordozóeszköz számára, cím kulcsból, ami egyedi a hordozóeszközre rögzítendő adat számára és eszköz ID-ből, ami azonosító az információ rögzítő számára, és generálja az első kódolási kulcsot a cím-egyértelmű kulcsból; és

amikor a lejátszó korlátozás be van beállítva, a kriptográfiai eszköz cím-egyértelmű kulcsot generál az információ rögzítőben tárolt generálás-irányított mester kulcsból, lemez ID-ből, ami egyedi azonosító a hordozóeszköz számára, cím kulcsból, ami egyedi a hordozóeszközre rögzítendő adat számára és az eszköz-egyértelmű kulcsból, ami egyedi az információ rögzítő számára, és generálja a második kódolási kulcsot a cím-egyértelmű kulcsból.

32. A 25. igénypont szerinti eljárás, **azzal jellemezve,** hogy az eljárás magában foglal továbbá szállítási folyam feldolgozási lépést, amelyben szállítási folyam által tartalmazott diszkrét szállítási csomagok mindegyikéhez hozzáfűzünk érkezési időbélyeget; továbbá a kriptográfiai lépésben:

blokk kulcsot generálunk kódolási kulcsként egynél több olyan csomagot magában foglaló blokk adat számára, amelyek mindegyikéhez hozzáfűztük az érkezési időbélyeget; és

generáljuk a blokk kulcsot kódolási kulcsként a hordozóeszközön eltárolandó adat kódolásakor olyan adat alapján, amely magában foglalja a kódolási kulcs generáló adatot és blokk magot, ami további egyedi információ az érkezési időbélyeget magában foglaló blokk adat számára.

33. A 25. igénypont szerinti eljárás, **azzal jellemezve,** hogy a kriptográfiai lépésben a hordozóeszközön eltárolandó adatot DES algoritmus szerint kódoljuk.

34. A 25. igénypont szerinti eljárás, **azzal jellemezve,** hogy adatban lévő szállítási folyam által tartalmazott csomagok mindegyikéhez hozzáfűzött másolás vezérlési információt azonosítunk annak eldöntésére a másolás vezérlési információ alapján, hogy a hordozóeszközre való rögzítés lehetséges-e vagy sem.

35. A 25. igénypont szerinti eljárás, **azzal jellemezve,** hogy 2-bites EMI-t azonosítunk másolás vezérlési információ-

ként annak eldöntésére az EMI alapján, hogy a hordozóeszközre való rögzítés lehetséges-e vagy sem.

36. Információ lejátszási eljárás információnak hordozóeszközről való lejátszására, **azzal jellemezve**, hogy az eljárás magában foglalja a következő lépéseket:

megújítunk dekódolási kulcs generáló adatot, amelyből dekódolási kulcsot generálunk hordozóeszközön tárolt kódolt adat dekódolásához legalább vagy csomópont kulccsal, ami egyedi olyan hierarchikus fa struktúra által tartalmazott csomópontok mindegyike számára, amely magában foglalja különböző információ lejátszók sokaságát a fa struktúra egyes leveleiként, vagy levél kulccsal, ami egyedi az információ lejátszók mindegyike számára; és

generáljuk a dekódolási kulcsot a megújítási lépésben megújított dekódolási kulcs generáló adatból a hordozóeszközön tárolt adat dekódolásához.

37. A 36. igénypont szerinti eljárás, **azzal jellemezve**, hogy a dekódolási kulcs generáló adat mester kulcs, amely közös az információ rögzítők sokasága számára.

38. A 36. igénypont szerinti eljárás, **azzal jellemezve**, hogy a dekódolási kulcs generáló adat közeg kulcs, amely egyedi meghatározott hordozóeszköz számára.

39. A 36. igénypont szerinti eljárás, **azzal jellemezve**, hogy:

a csomópont kulcsot megújíthatjuk;

amikor csomópont kulcsot megújítunk, kiosztunk olyan levélnél lévő információ lejátszó számára, ahol a kódolási kulcs generáló adatot meg kell újítanunk kulcs megújítási blokkot, amelyet a megújítási csomópont kulcsnak a fa struktúra alacsonyabb szintjén lévő csomópont kulcs vagy levél kulcs legalább egyikével való kódolásából származtatunk; és

a kriptográfiai lépés magában foglalja a következő lépéseket:

kódoljuk a kulcs megújítási blokkot a megújított csomópont kulcs megszerzéséhez; és

kiszámítunk megújítási adatot a dekódolási kulcs generáló adat számára az így megszerzett megújított csomópont kulcs alapján.

40. A 36. igénypont szerinti eljárás, **azzal jellemezve**, hogy:

a dekódolási kulcs generáló adat rendelkezik generálási számmal vele korrelációban lévő megújítási információként; és

a kriptográfiai lépésben, amikor a hordozóeszközből származó kódolt adatot dekódolunk, beolvassuk a hordozóeszközről a kódolt adat kódolásakor használt kódolási kulcs generáló adat generálási számát dekódolási kulcs generálására az így beolvasott generálási számnak megfelelő dekódolási kulcs generáló adatból.

41. A 36. igénypont szerinti eljárás, **azzal jellemezve**, hogy a kriptográfiai lépés magában foglalja a következő két eljárást, amelyek egyikét szelektív módon hajtjuk végre attól függően, hogy lejátszó korlátozás be van-e állítva vagy sem:

amikor a lejátszó korlátozás nincs beállítva, első dekódolási kulcsot generálunk a hordozóeszközön tárolt kódolt adat számára a hordozóeszközön tárolt első dekódolási kulcs generáló adat alapján, és a kódolt adatot dekódoljuk az első dekódolási kulccsal; és

amikor a lejátszó korlátozás be van beállítva, második dekódolási kulcsot generálunk a hordozóeszközön tárolt kódolt adat számára az információ rögzítőbe beépített második kódolási kulcs generáló adat alapján, és a kódolt adatot dekódoljuk a második dekódolási kulccsal.

42. A 41. igénypont szerinti eljárás, **azzal jellemezve**, hogy a kriptográfiai lépés magában foglalja a következő két eljárást:

amikor a lejátszó korlátozás nincs beállítva, megszerzünk az információ rögzítőben tárolt generálás-irányított mester kulcsot, és megszerzünk ezen kívül hordozóeszközből lemez ID-t, ami egyedi azonosító hordozóeszköz számára, cím kulcsot, ami egyedi dekódolandó adat számára és eszköz ID-t, ami azonosító azon információ rögzítő számára, amely a kódolt adatot rögzítette cím-egyértelmű kulcs generálására a mester kulcsból, lemez ID-ből, cím kulcsból és eszköz kulcsból és az első dekódolási kulcsnak a cím-egyértelmű kulcsból való generálására; és

amikor a lejátszó korlátozás be van beállítva, megszerzünk az információ rögzítőben tárolt generálás-irányított mester kulcsot és eszköz-egyértelmű kulcsot, amely egyedi az információ rögzítő számára és abban is tároljuk, és megszerzünk ezen kívül hordozóeszközből lemez ID-t, ami egyedi azonosító a

hordozóeszköz számára és cím kulcsot, ami egyedi a dekódolandó adat számára cím-egyértelmű kulcs generálására a mester kulcsból, lemez ID-ből, cím kulcsból és eszköz-egyértelmű kulcsból; és a második dekódolási kulcsot generáljuk az így generált cím-egyértelmű kulcsból.

43. A 36. igénypont szerinti eljárás, **azzal jellemezve**, hogy:

a lejátszó magában foglal szállítási folyam feldolgozó eszközt adat kimenetre tétel vezérlésére a dekódolt blokk által tartalmazott szállítási csomagok sokaságának mindegyikéhez hozzáfűzött érkezési időbélyeg alapján; továbbá a kriptográfiai lépésben:

blokk kulcsot generálunk dekódolási kulcsként egynél több olyan csomagot magában foglaló blokk adat számára, amelyek mindegyikéhez hozzáfűztük az érkezési időbélyeget; és

generáljuk a blokk kulcsot dekódolási kulcsként a hordozóeszközön tárolt kódolt adat dekódolásakor olyan adat alapján, amely magában foglalja a dekódolási kulcs generáló adatot és blokk magot, ami további egyedi információ az érkezési időbélyeget magában foglaló blokk adat számára.

44. A 36. igénypont szerinti eljárás, **azzal jellemezve**, hogy a hordozóeszközön tárolt kódolt adatot DES algoritmus szerint dekódoljuk.

45. A 36. igénypont szerinti eljárás, **azzal jellemezve**, hogy adatban lévő szállítási folyam által tartalmazott csomagok mindegyikéhez hozzáfűzött másolás vezérlési információt

azonosítunk annak eldöntésére a másolás vezérlési információ alapján, hogy a hordozóeszközről való lejátszás lehetséges-e vagy sem.

46. A 36. igénypont szerinti eljárás, **azzal jellemezve,** hogy 2-bites EMI-t azonosítunk másolás vezérlési információként annak eldöntésére az EMI alapján, hogy a hordozóeszközről való lejátszás lehetséges-e vagy sem.

47. Információ hordozóeszköz, amely képes információ rögzítésére, **azzal jellemezve,** hogy tárolunk benne kulcs megújítási blokkot, amelyet megújított csomópont kulcs kódolásából származtatunk legalább vagy csomópont kulccsal, ami egyedi olyan hierarchikus fa struktúra által tartalmazott csomópontok mindegyike számára, amely különböző információ rögzítők sokaságát foglalja magában a fa struktúra egyes leveleiként, vagy levél kulccsal, ami egyedi az információ rögzítők mindegyike számára.

48. A 47. igénypont szerinti hordozóeszköz, **azzal jellemezve,** hogy magában foglal kódolási kulcs generálásához használt kódolási kulcs generáló adatnak a megújított csomópont kulccsal való kódolásából származtatott adatot az információ rögzítőben hordozóeszközön eltárolandó adat kódolásához.

49. A 47. igénypont szerinti hordozóeszköz, **azzal jellemezve,** hogy magában foglal dekódolási kulcs generálásához használt dekódolási kulcs generáló adatnak a megújított csomópont kulccsal való dekódolásából származtatott adatot az in-

formáció lejátszóban a hordozóeszközön tárolt kódolt adat dekódolásához.

50. A 47. igénypont szerinti hordozóeszköz, **azzal jellemezve,** hogy generálási információt tárolunk rajta a kódolási vagy dekódolási kulcs generáló adatról.

51. Berendezés információ hordozóeszköz létrehozására, **azzal jellemezve,** hogy a berendezés magában foglal:

memóriát olyan kulcs megújítási blokk tárolására, amelyet megújított csomópont kulcs kódolásából származtatunk legalább vagy csomópont kulccsal, ami egyedi olyan hierarchikus fa struktúra által tartalmazott csomópontok mindegyike számára, amely különböző információ rögzítők sokaságát foglalja magában a fa struktúra egyes leveleiként, vagy levél kulccsal, ami egyedi az információ rögzítők mindegyike számára; és

vezérlési egységet a memóriában tárolt kulcs megújítási blokknak a hordozóeszközre való írásának a vezérlésére.

52. Az 51. igénypont szerinti berendezés, **azzal jellemezve,** hogy:

a memória tárolja ezen kívül legalább hordozóeszköz azonosító és kódolt kódolási kulcs generáló adat vagy kódolt dekódolási kulcs generáló adat bármelyikét; és

a vezérlési egység vezérli legalább a hordozóeszköz azonosító és kódolt kódolási kulcs generáló adat vagy kódolt dekódolási kulcs generáló adat bármelyikének a hordozóeszközre való írását.

53. Az 51. igénypont szerinti berendezés, **azzal jellemezve**, hogy a memória tárol ezen kívül generálási információt a kódolási kulcs generáló adatról és a dekódolási kulcs generáló adatról; és

a vezérlési egység vezérli a generálási információnak a hordozóeszközre való írását.

54. Eljárás hordozóeszköz létrehozására, **azzal jellemezve**, hogy magában foglalja a következő lépéseket:

memóriába eltárolunk olyan kulcs megújítási blokkot, amelyet megújított csomópont kulcs kódolásából származtatunk legalább vagy csomópont kulccsal, ami egyedi olyan hierarchikus fa struktúra által tartalmazott csomópontok mindegyike számára, amely különböző információ rögzítők sokaságát foglalja magában a fa struktúra egyes leveleiként, vagy levél kulccsal, ami egyedi az információ rögzítők mindegyike számára; és

a memóriában tárolt kulcs megújítási blokkot a hordozóeszközre írjuk.

55. Az 54. igénypont szerinti eljárás, **azzal jellemezve**, hogy:

a memóriába eltároljuk ezen kívül legalább hordozóeszköz azonosító és kódolt kódolási kulcs generáló adat vagy kódolt dekódolási kulcs generáló adat bármelyikét; és

a hordozóeszközre írjuk legalább a hordozóeszköz azonosító és kódolt kódolási kulcs generáló adat vagy kódolt dekódolási kulcs generáló adat bármelyikét.

56. Az 54. igénypont szerinti eljárás, **azzal jellemezve,** hogy:

a memóriába eltárolunk generálási információt a kódolási kulcs generáló adatról vagy dekódolási kulcs generáló adatról; és

vezéreljük a generálási információnak a hordozóeszközre való írását.

57. Program szolgáltató közeg számítógépes program szolgáltatására, amely alatt információ feldolgozást folytatunk információnak hordozóeszközre való rögzítéséhez számítógépes rendszerben, **azzal jellemezve,** hogy a számítógépes program magában foglalja a következő lépéseket:

megújítunk kódolási kulcs generáló adatot kódolási kulcs generálására hordozóeszközön eltárolandó adat kódolásához legalább vagy csomópont kulccsal, ami egyedi olyan hierarchikus fa struktúra által tartalmazott csomópontok mindegyike számára, amely különböző információ rögzítők sokaságát foglalja magában a fa struktúra egyes leveleiként, vagy levél kulccsal, ami egyedi az információ rögzítők mindegyike számára; és

kódolási kulcsot generálunk a kódolási kulcs generáló adat alapján a hordozóeszközön eltárolandó adat kódolására.

58. Program szolgáltató közeg számítógépes program szolgáltatására, amely alatt hordozóeszközön tárolt információt lejátszunk számítógépes rendszerben, **azzal jellemezve,** hogy a számítógépes program magában foglalja a következő lépéseket:

megújítunk dekódolási kulcs generáló adatot, amiből dekódolási kulcsot generálunk hordozóeszközön tárolt kódolt adat

dekódolásához legalább vagy csomópont kulccsal, ami egyedi olyan hierarchikus fa struktúra által tartalmazott csomópontok mindegyike számára, amely különböző információ lejátszók sokaságát foglalja magában a fa struktúra egyes leveleiként, vagy levél kulccsal, ami egyedi az információ lejátszók mindegyike számára; és

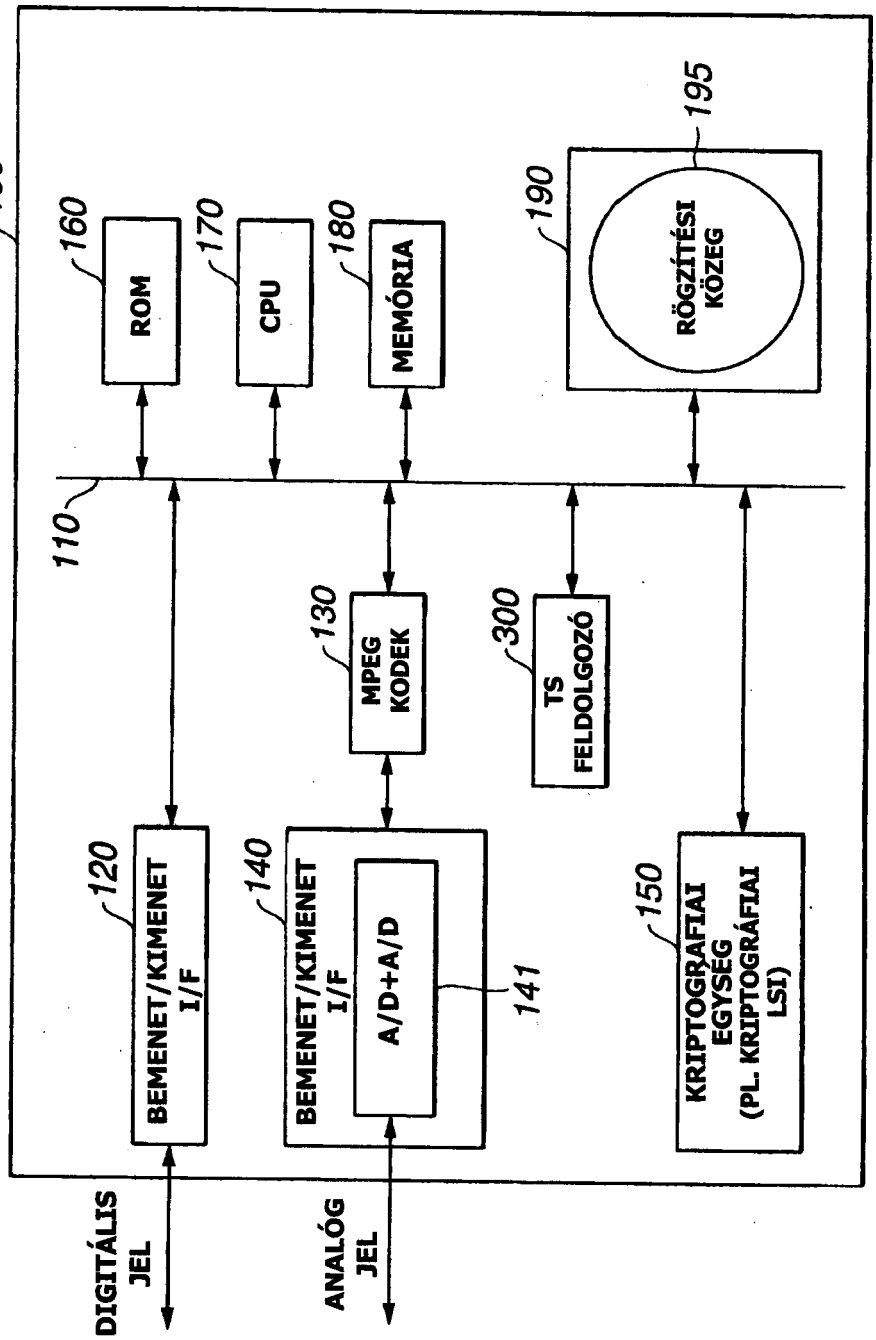
generáljuk a dekódolási kulcsot a megújítási lépésben megújított dekódolási kulcs generáló adatból a hordozóeszközön tárolt adat dekódolására.

A meghatalmazott:

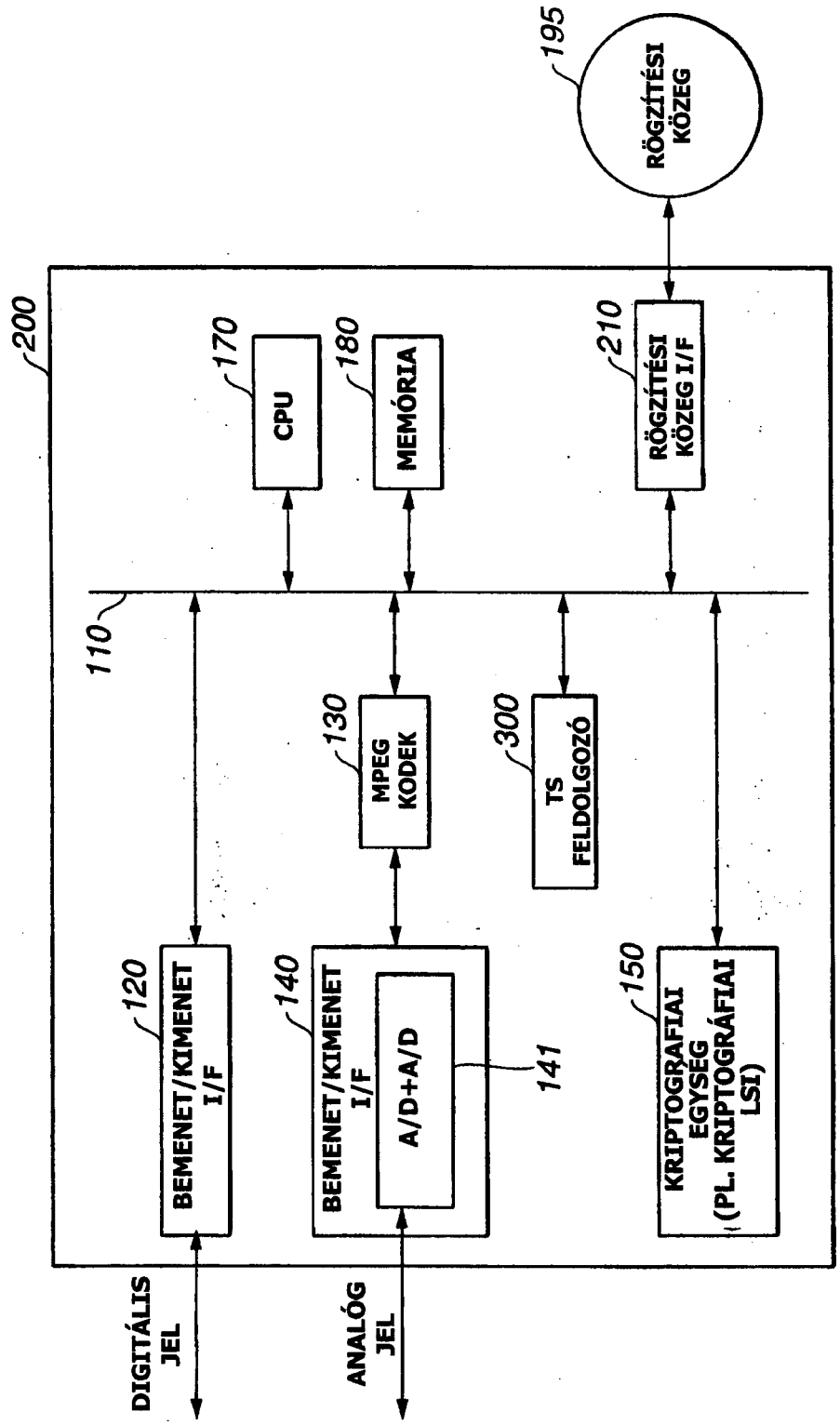
43 rajz, 46 ábra

P0202148

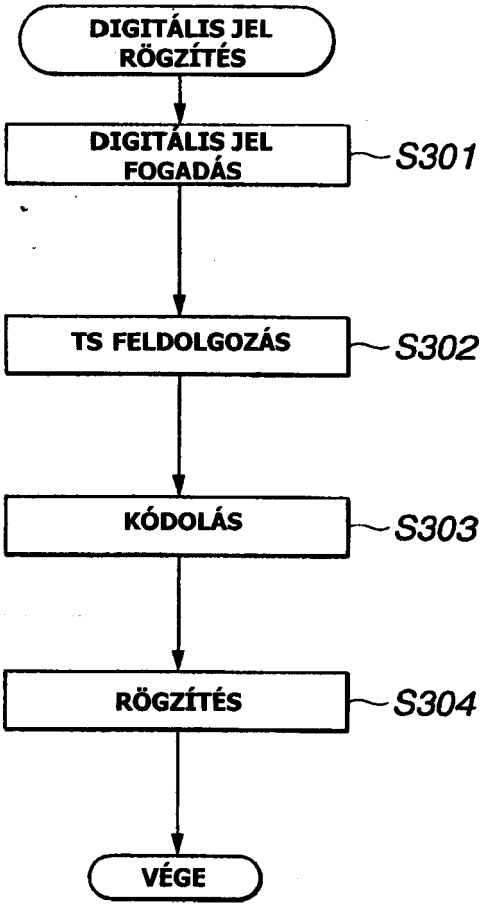
KÖZZÉTÉTELI PÉLDÁNY (A1)



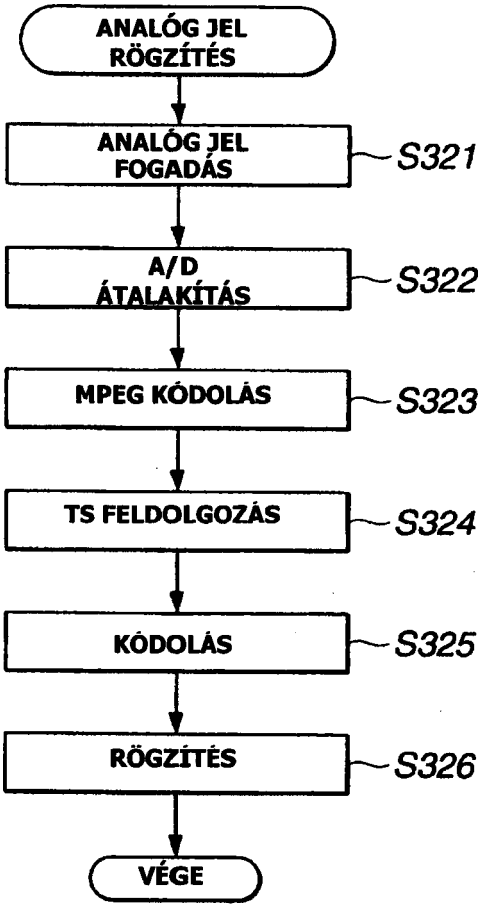
1. ÁBRA



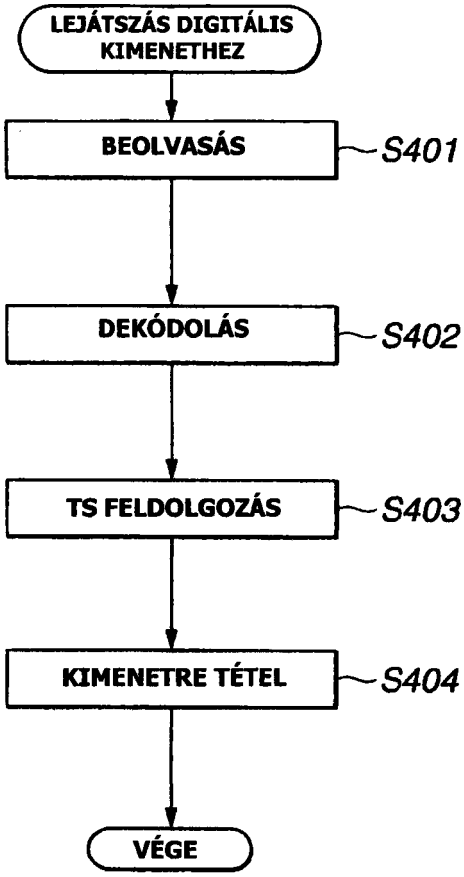
2. ÁBRA



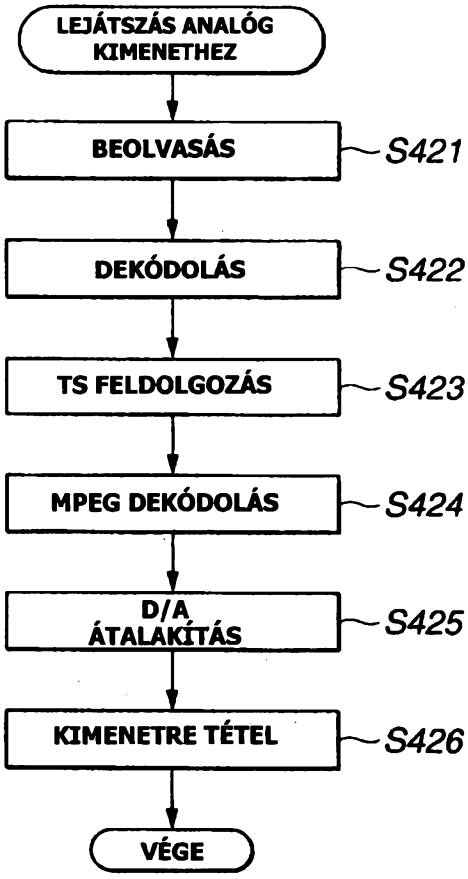
3A ÁBRA



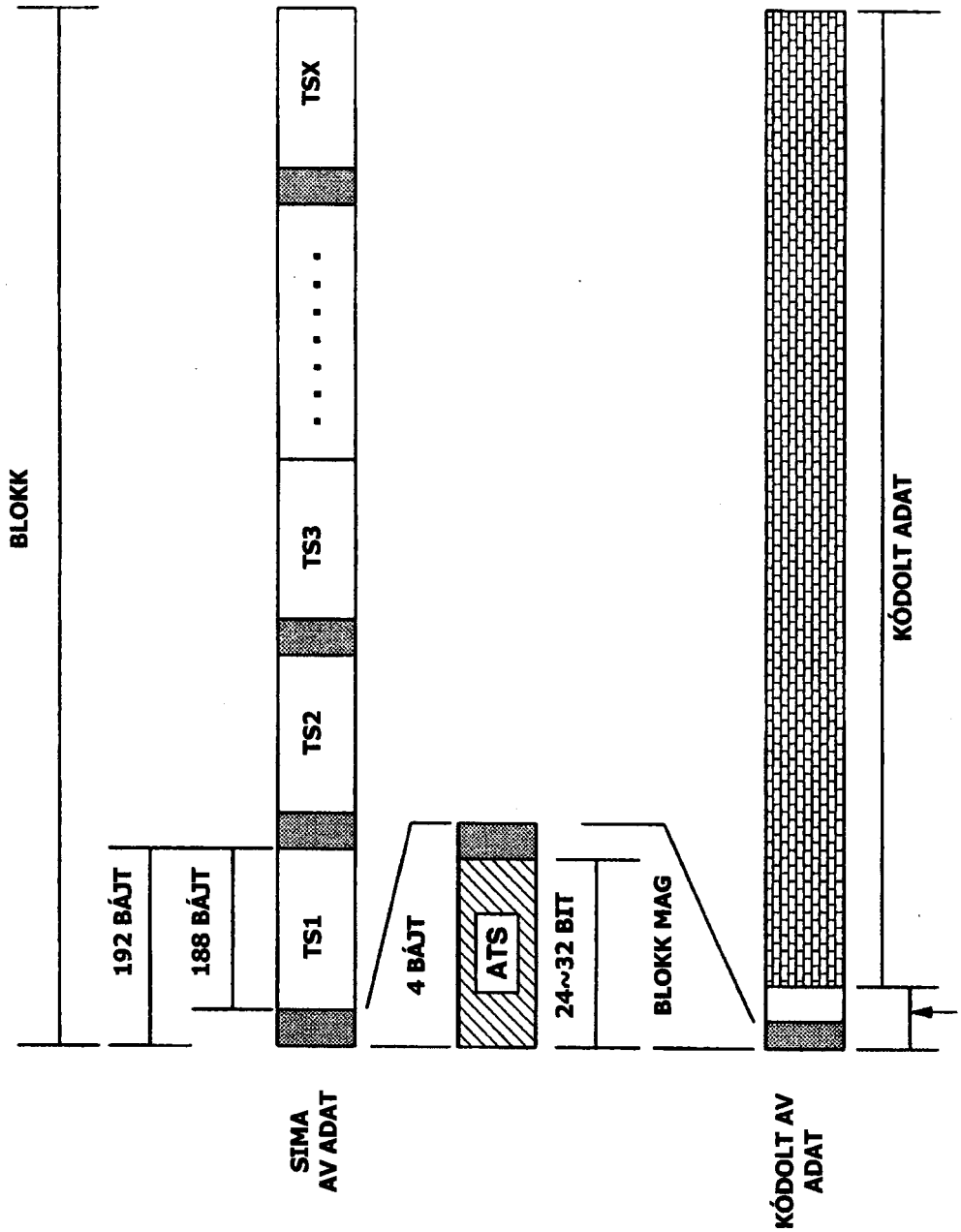
3B ÁBRA



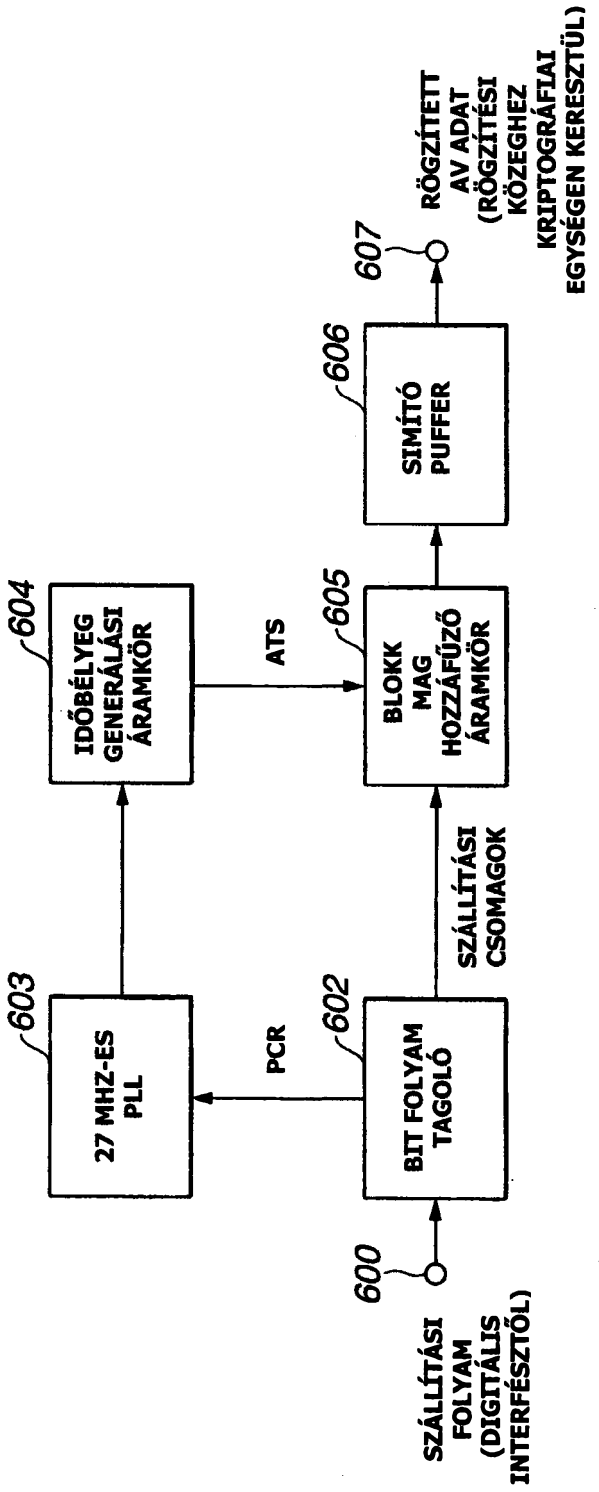
4A ÁBRA



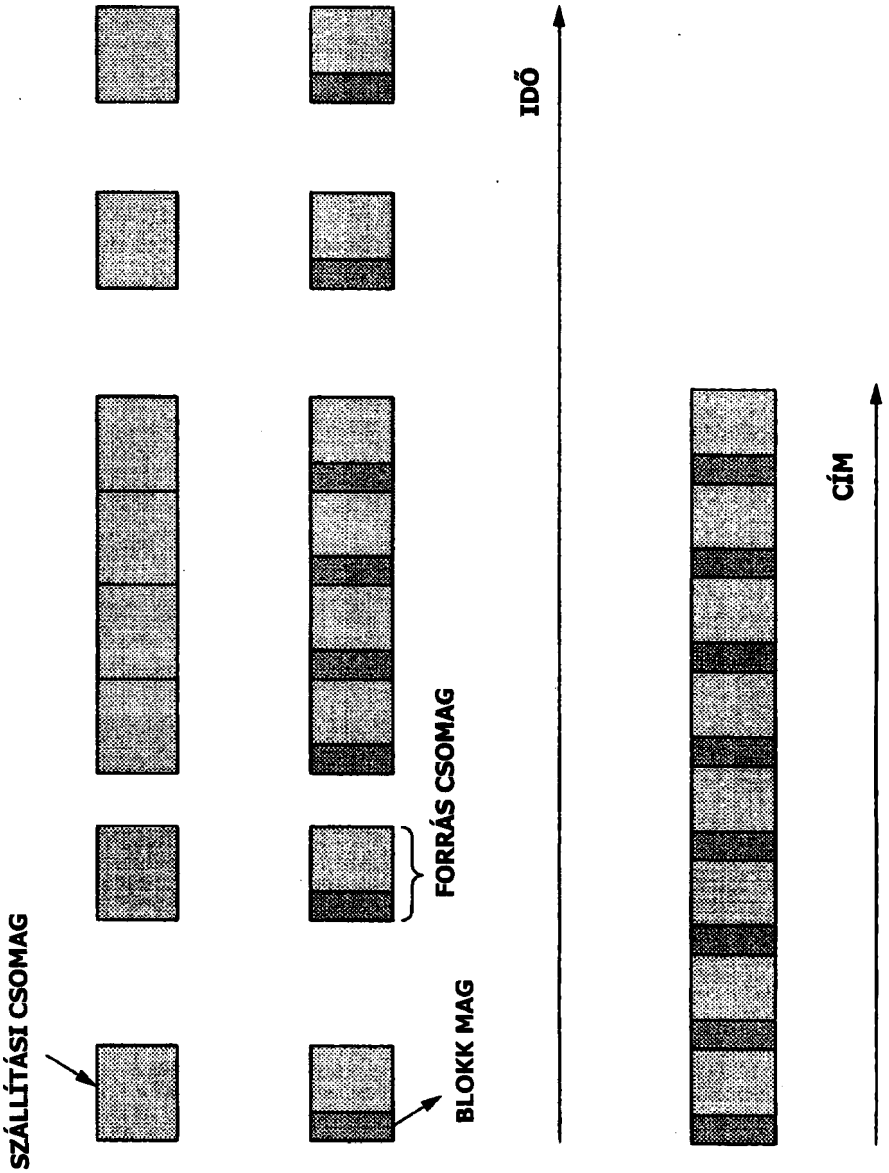
4B ÁBRA



5. ÁBRA



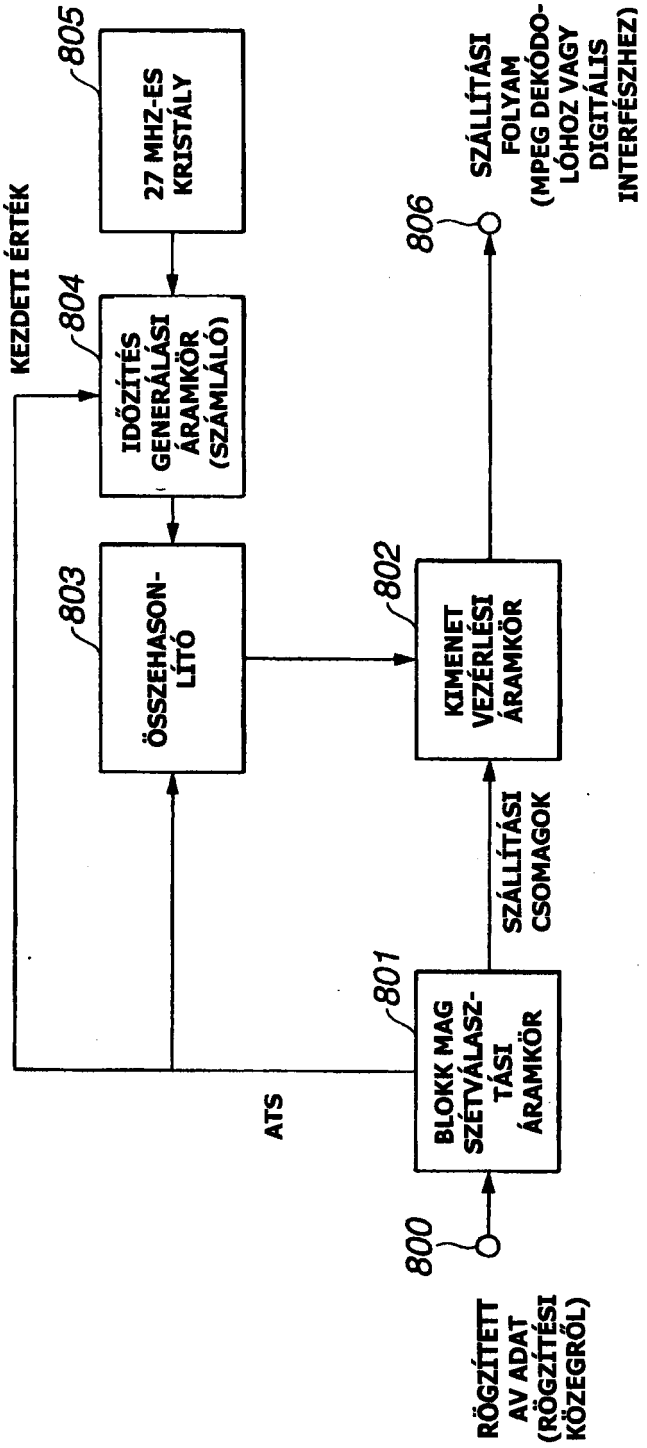
6. ÁBRA



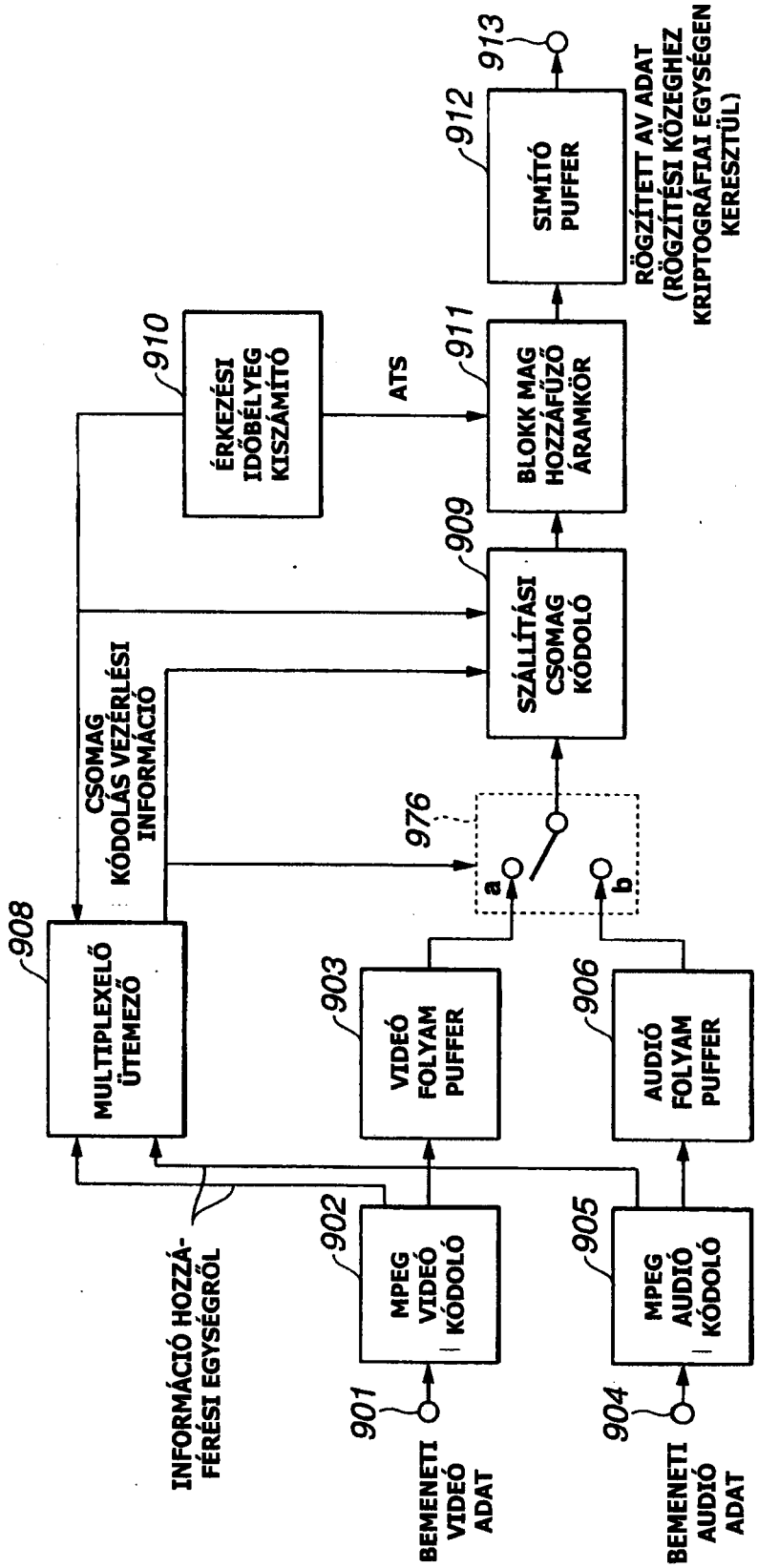
7A ÁBRA
BEMENETI SZÁLLÍTÁSI FOLYAM

7B ÁBRA
BLOKK MAG HOZZÁFŰZŐ ÁRAMKÖR KIMENETE

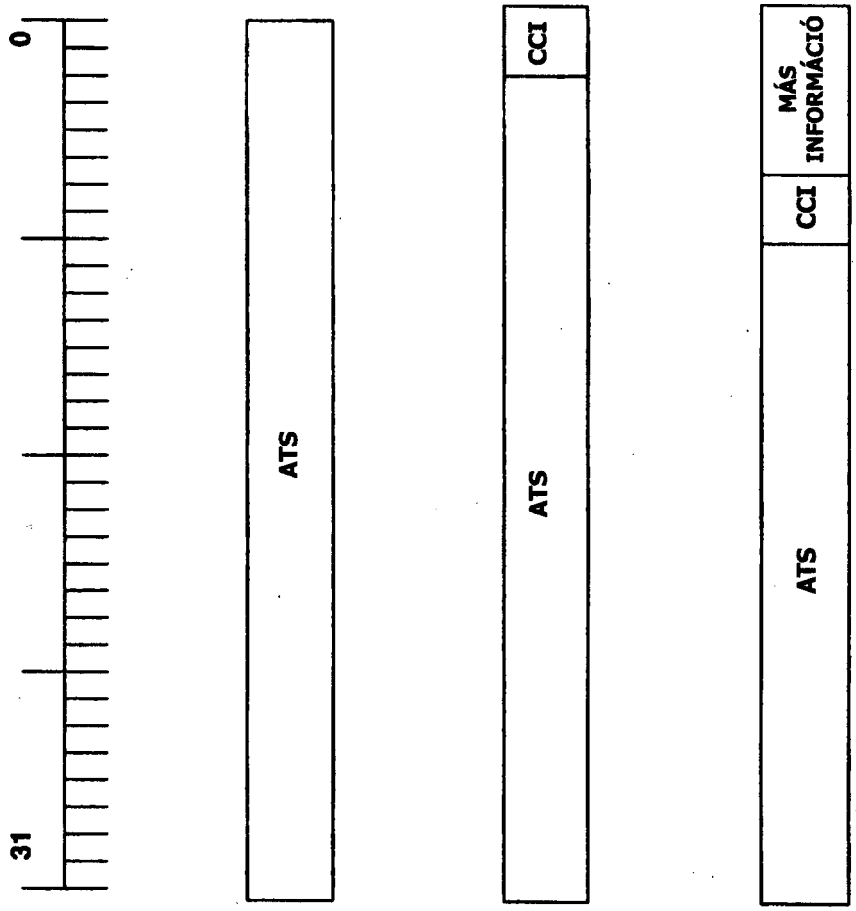
7C ÁBRA
AV ADAT RÖGZÍTÉSI KÖZEGEN



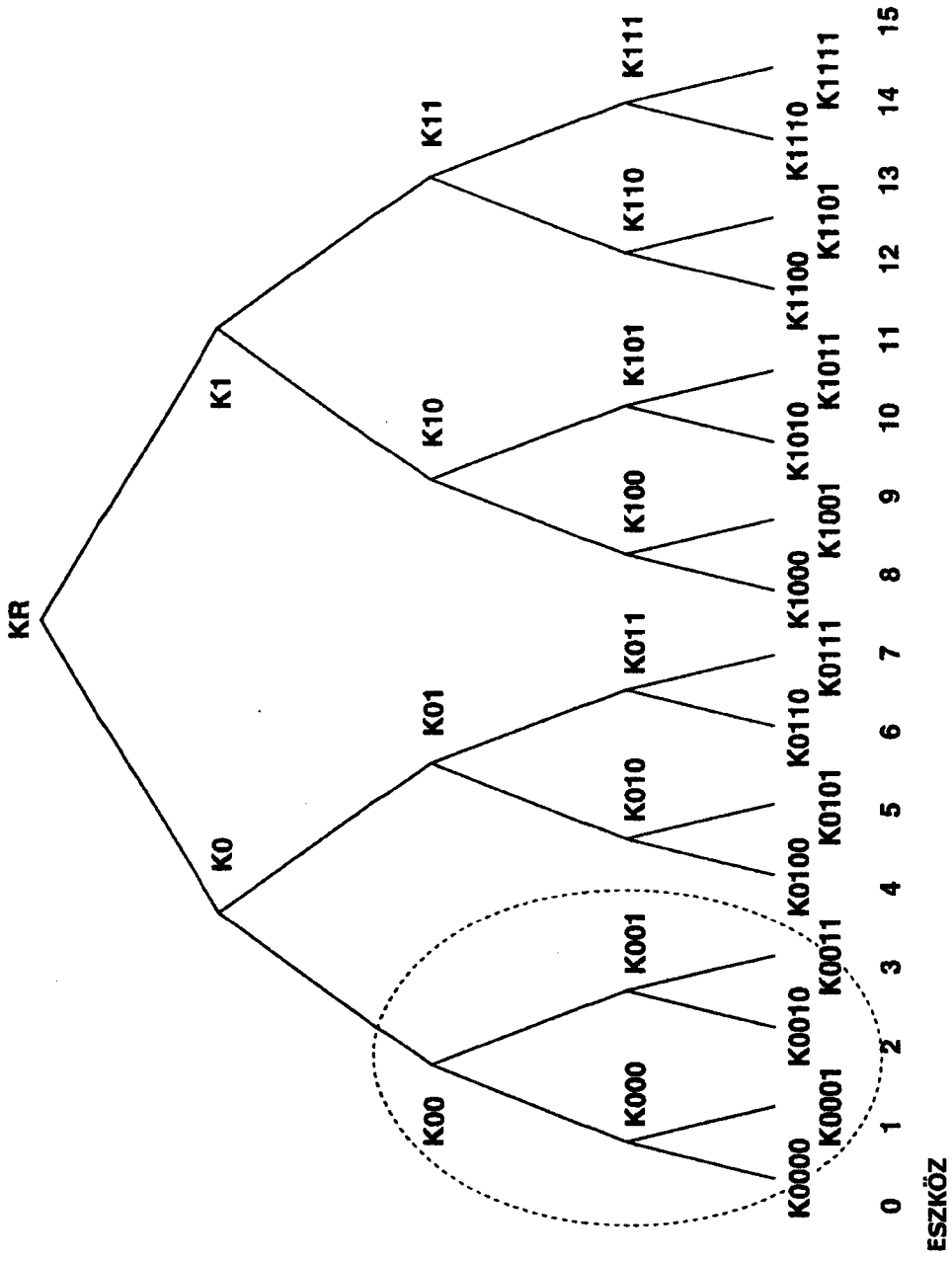
8. ÁBRA



9. ÁBRA



10. ÁBRA



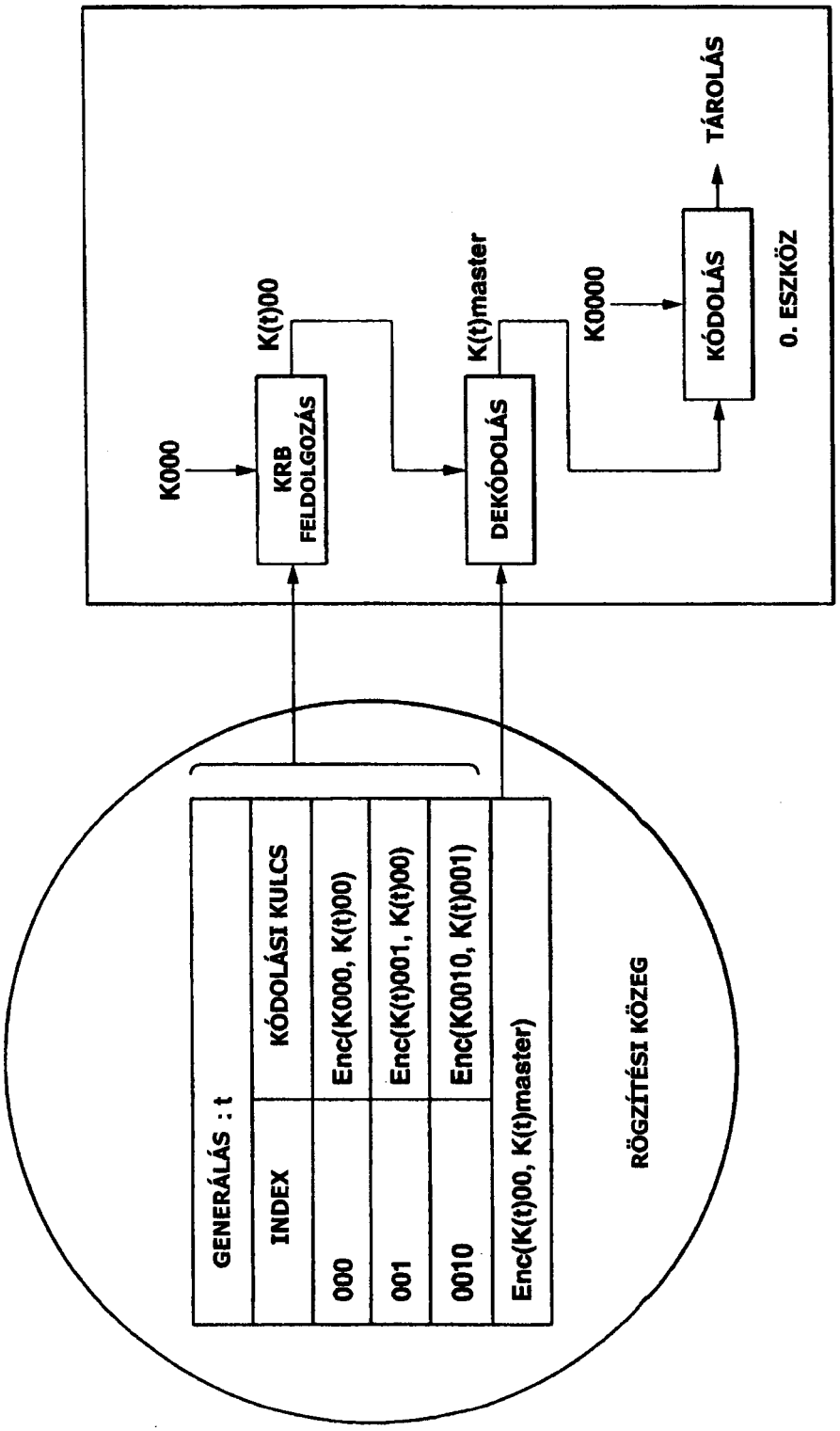
11. ÁBRA

GENERÁLÁS : t	
INDEX	KÓDOLÁSI KULCS
0	Enc(K(t)0, K(t)R)
00	Enc(K(t)00, K(t)0)
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

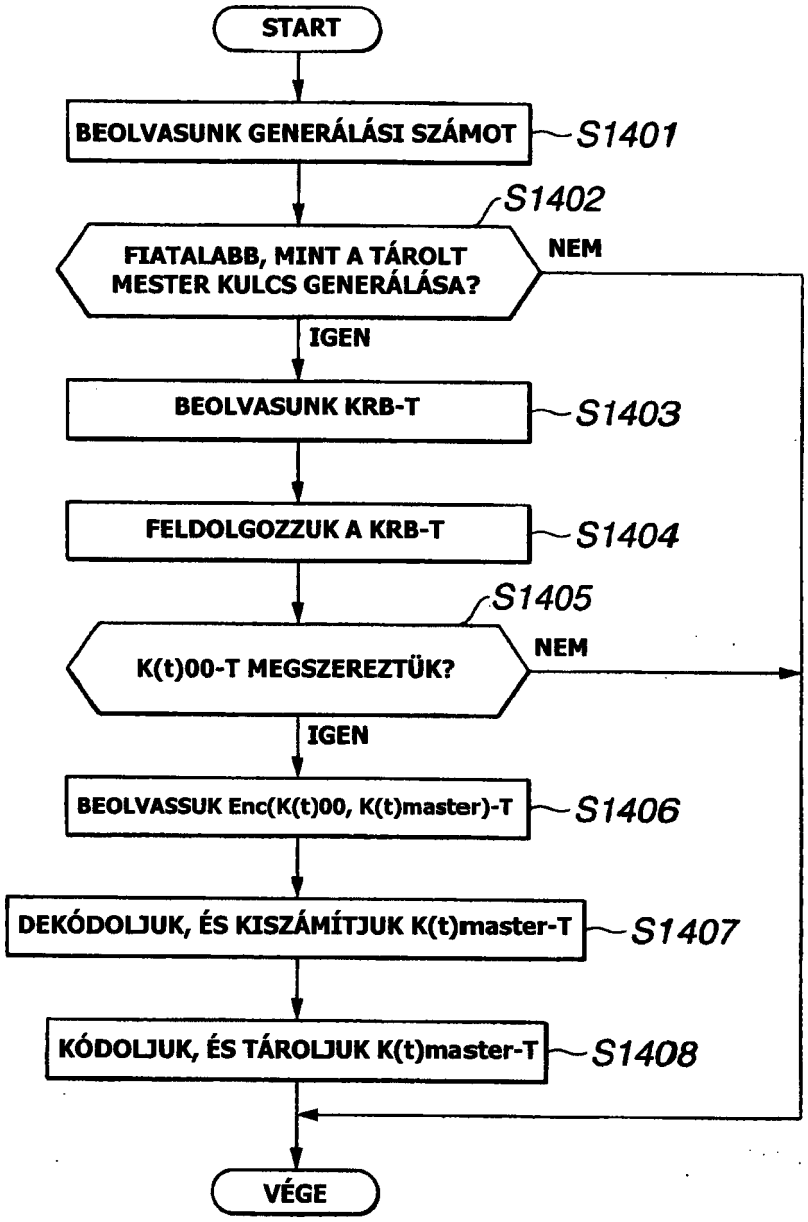
12A ÁBRA

GENERÁLÁS : t	
INDEX	KÓDOLÁSI KULCS
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

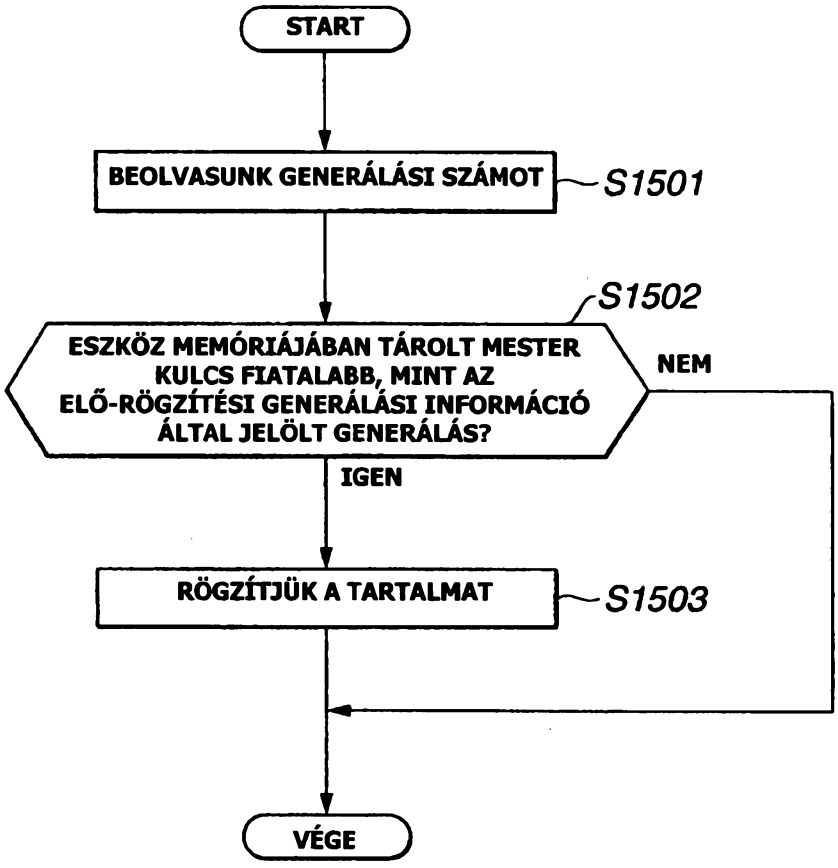
12B ÁBRA



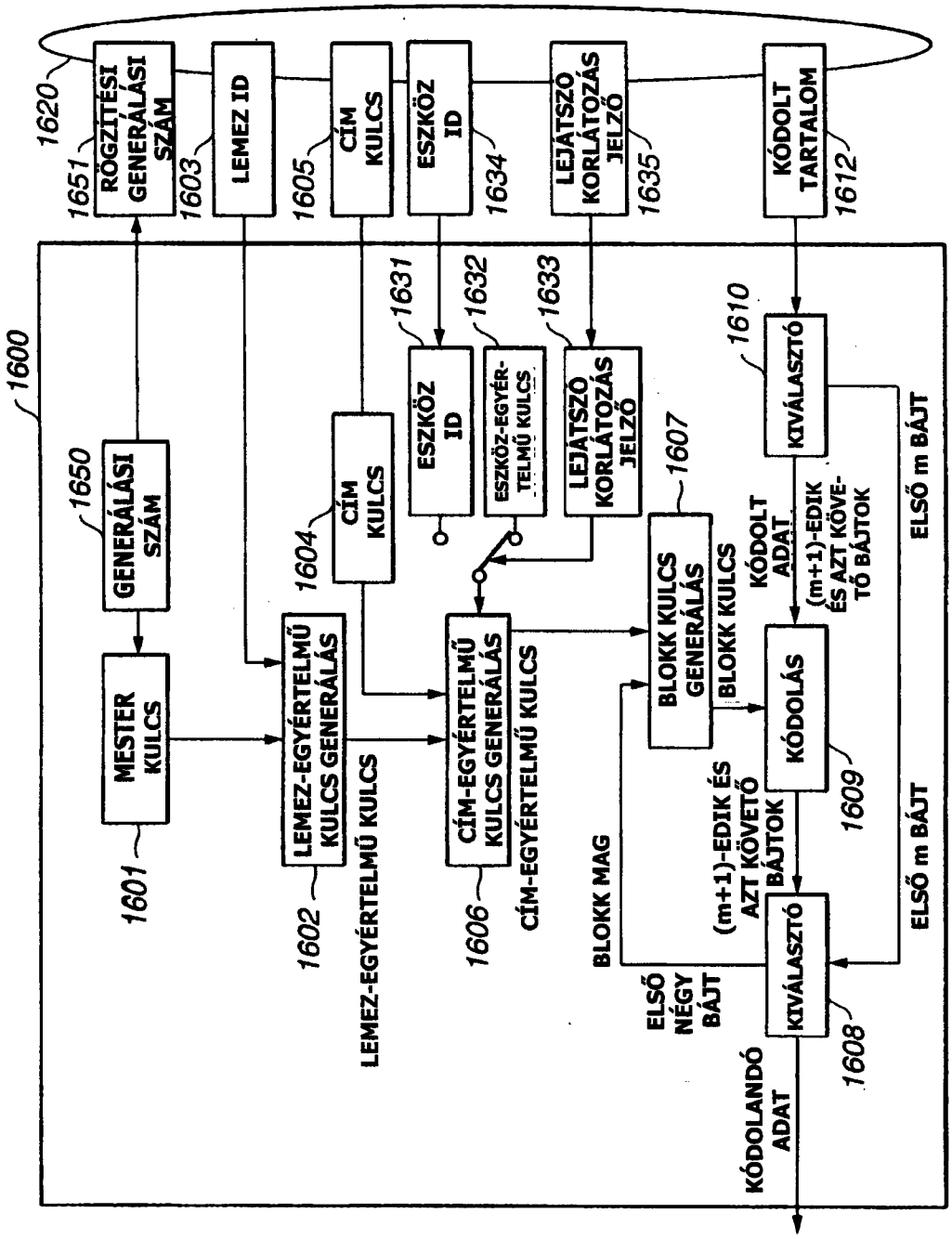
13. ÁBRA



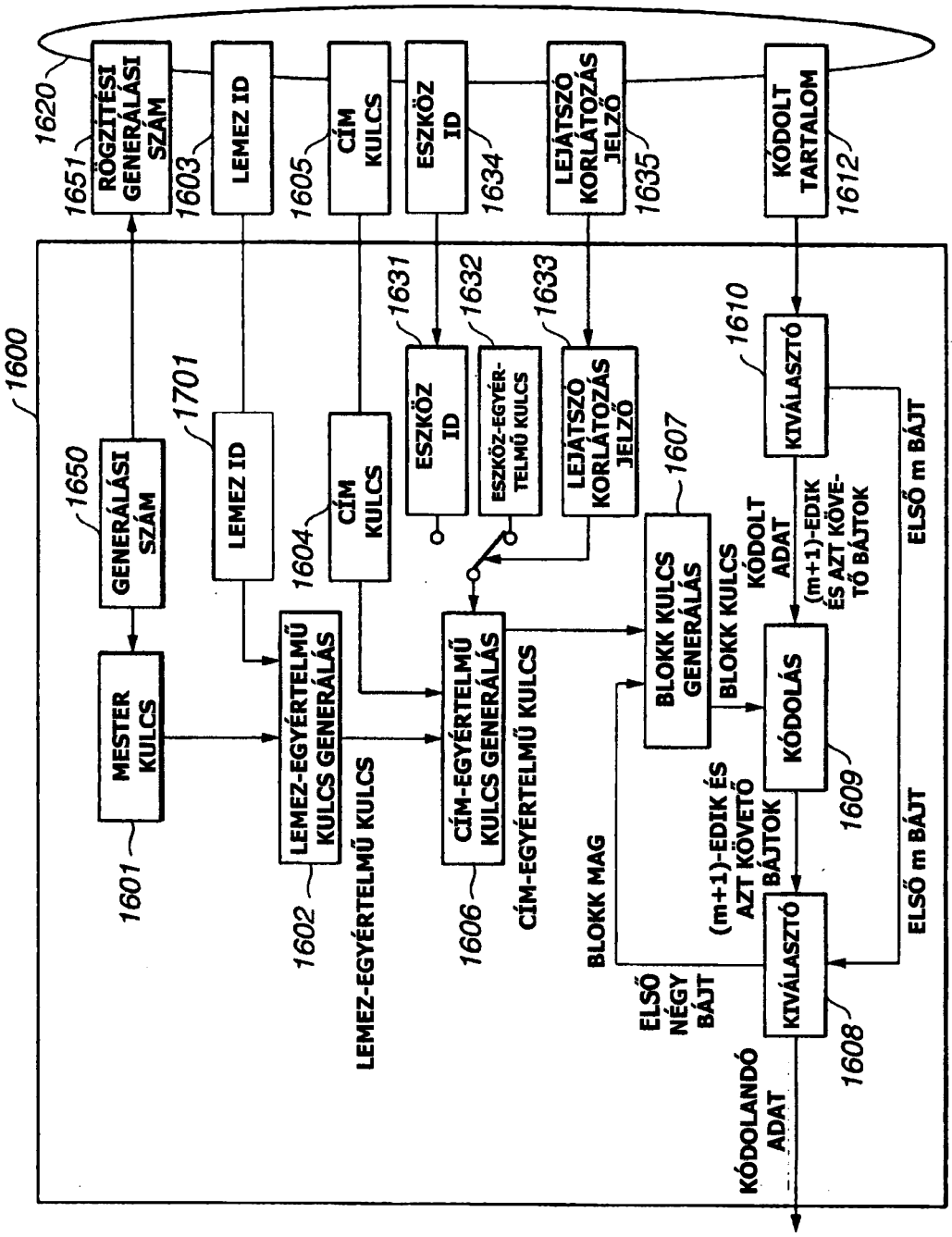
14. ÁBRA



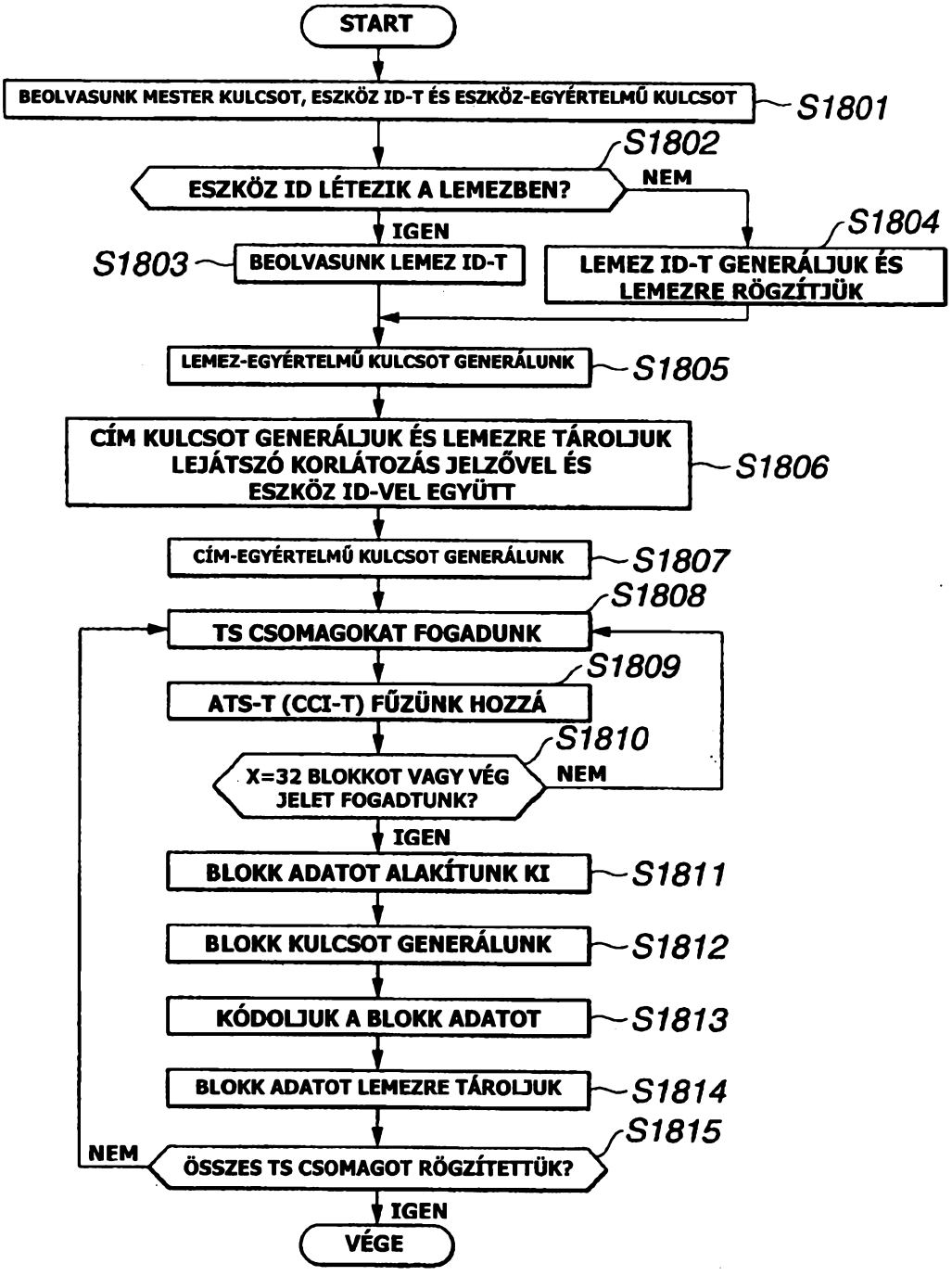
15. ÁBRA



16. ÁBRA



17. ÁBRA



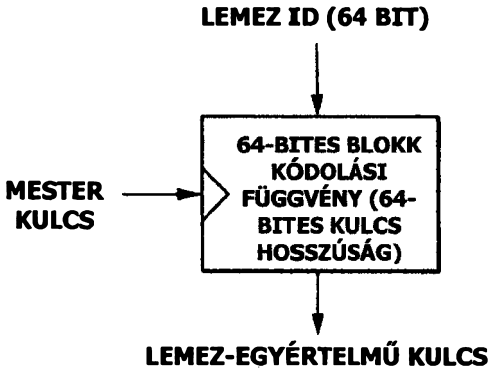
18. ÁBRA

1. PÉLDA

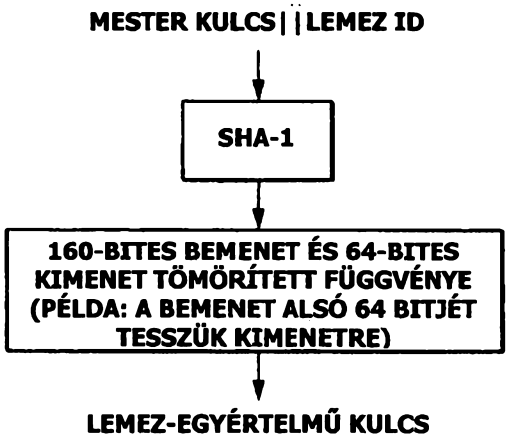
PÉLDA ESZKÖZ-EGYÉRTELMŰ KULCS GENERÁLÁSÁRA

BEMENETEK:
MESTER KULCS (64 BIT)
LEMEZ ID (64 BIT)

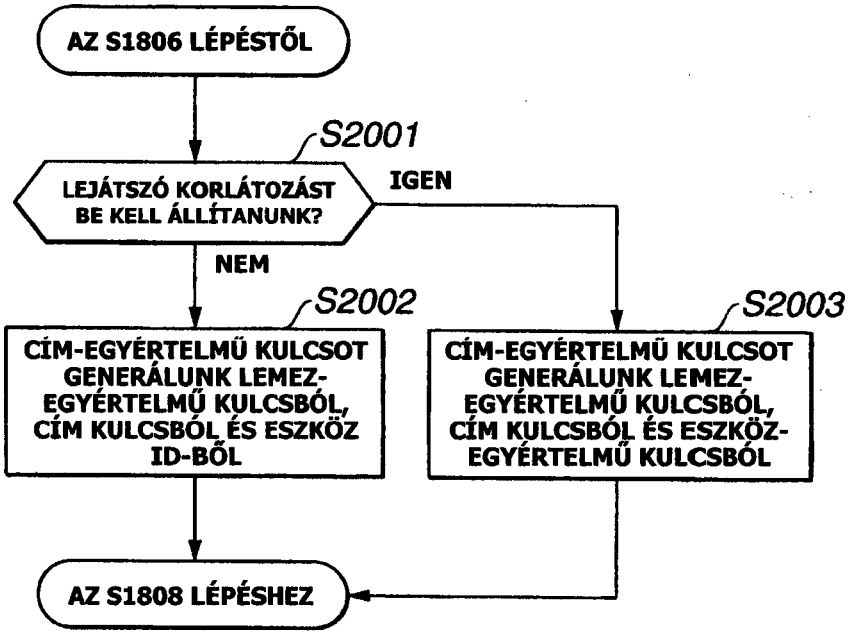
KIMENETEK:
LEMEZ-EGYÉRTELMŰ KULCS (64 BIT)



2. PÉLDA



19. ÁBRA



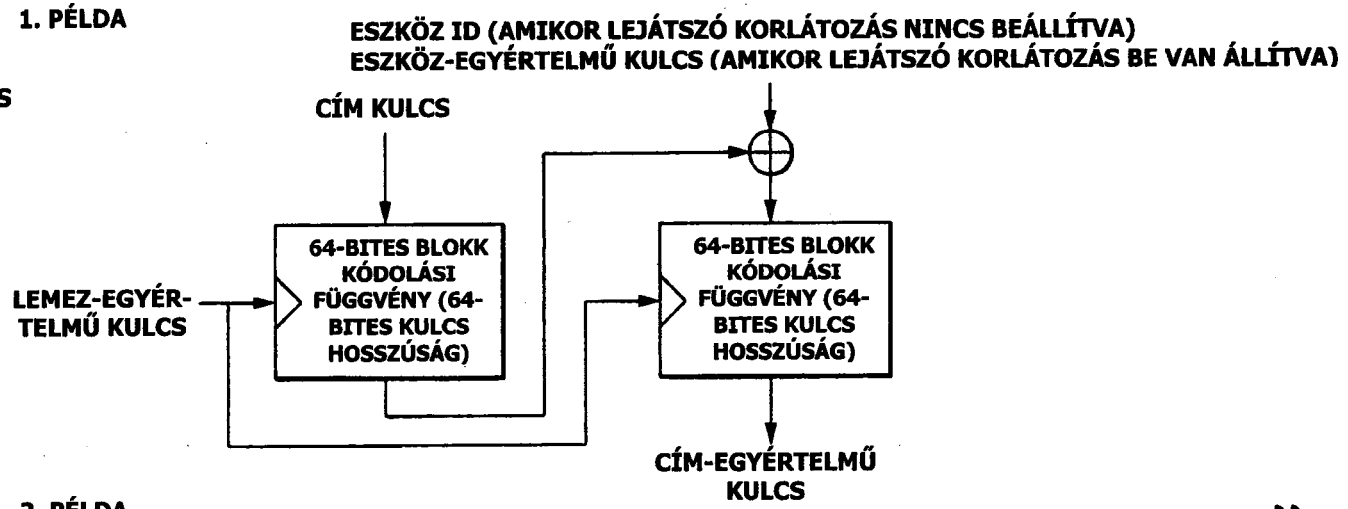
20. ÁBRA

PÉLDA CÍM-EGYÉRTELMŰ KULCS GENERÁLÁSÁRA

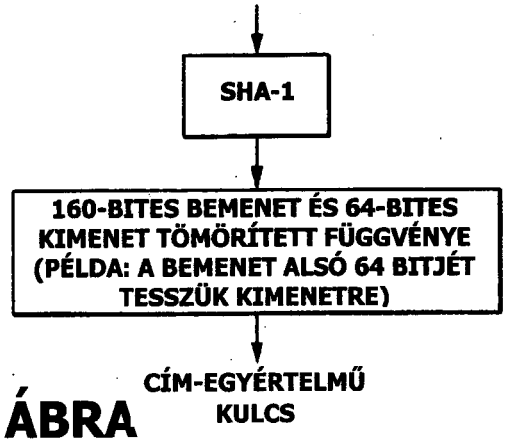
BEMENETEK:
LEMEZ-EGYÉRTELMŰ KULCS (64 BIT)
CÍM KULCS (64 BIT)
LEMEZ ID (64 BIT) VAGY ESZKÖZ-EGYÉRTELMŰ KULCS (64 BIT)

KIMENETEK:
CÍM-EGYÉRTELMŰ KULCS (64 BIT)

1. PÉLDA



2. PÉLDA



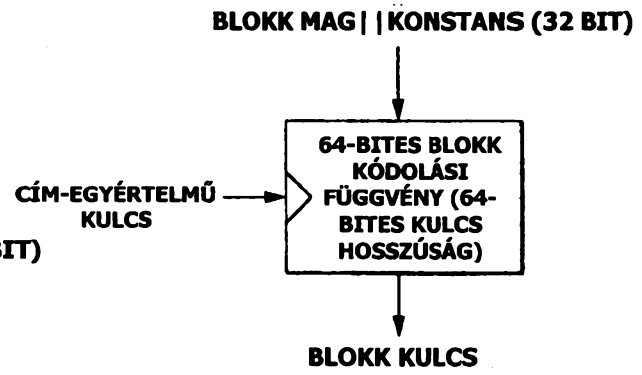
21. ÁBRA

1. PÉLDA

PÉLDA BLOKK KULCS GENERÁLÁSRA

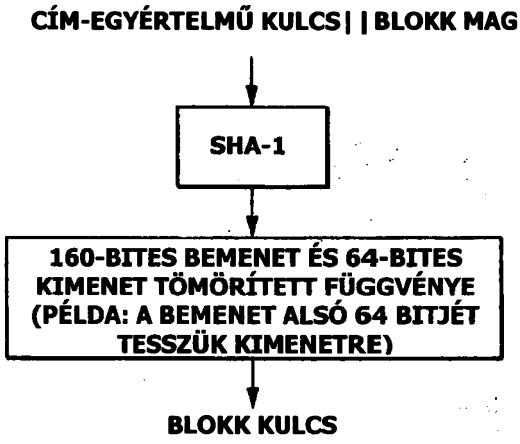
BEMENETEK:

BLOKK MAG (32 BIT)
CÍM-EGYÉRTELMŰ KULCS (64 BIT)

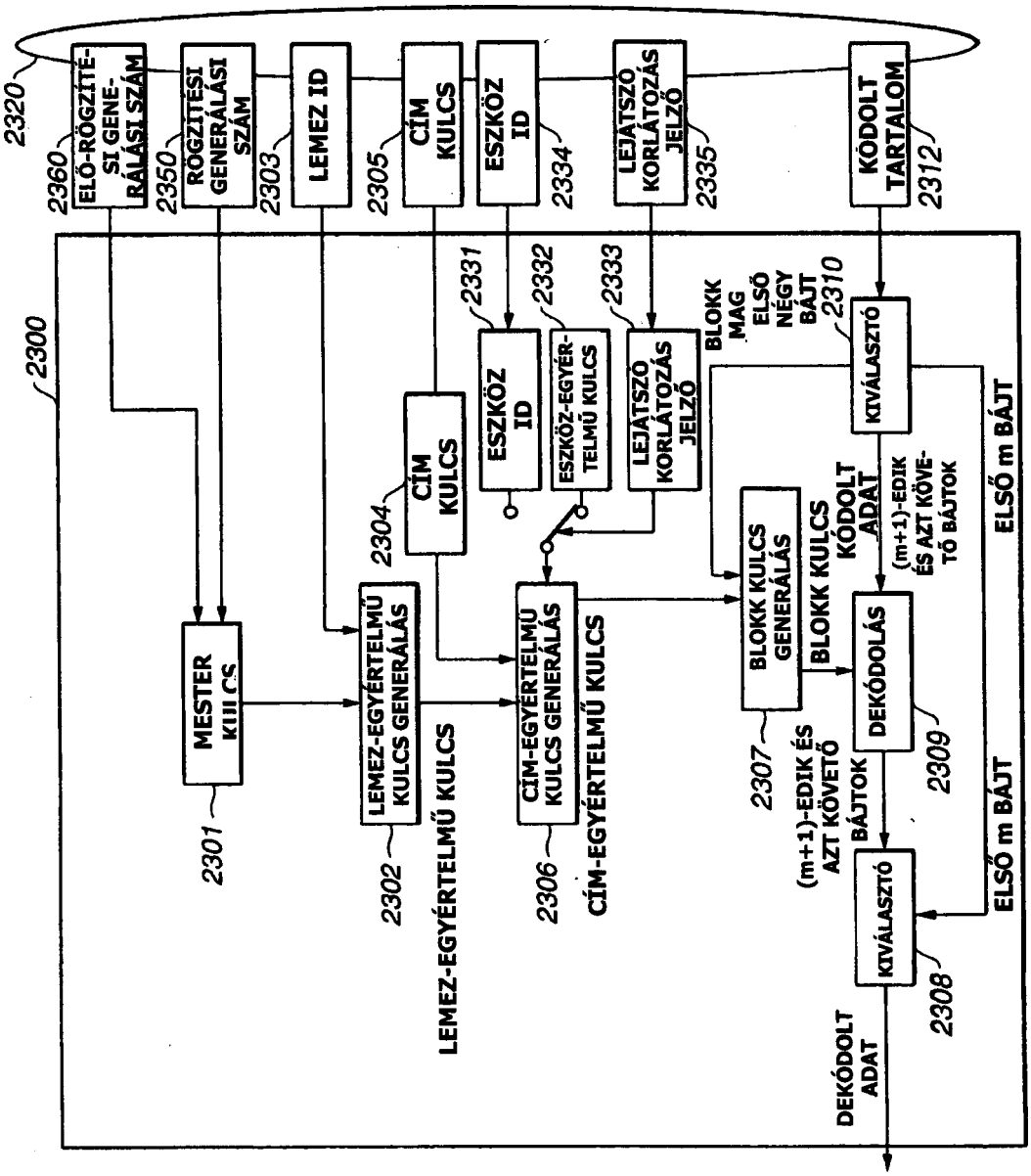


2. PÉLDA

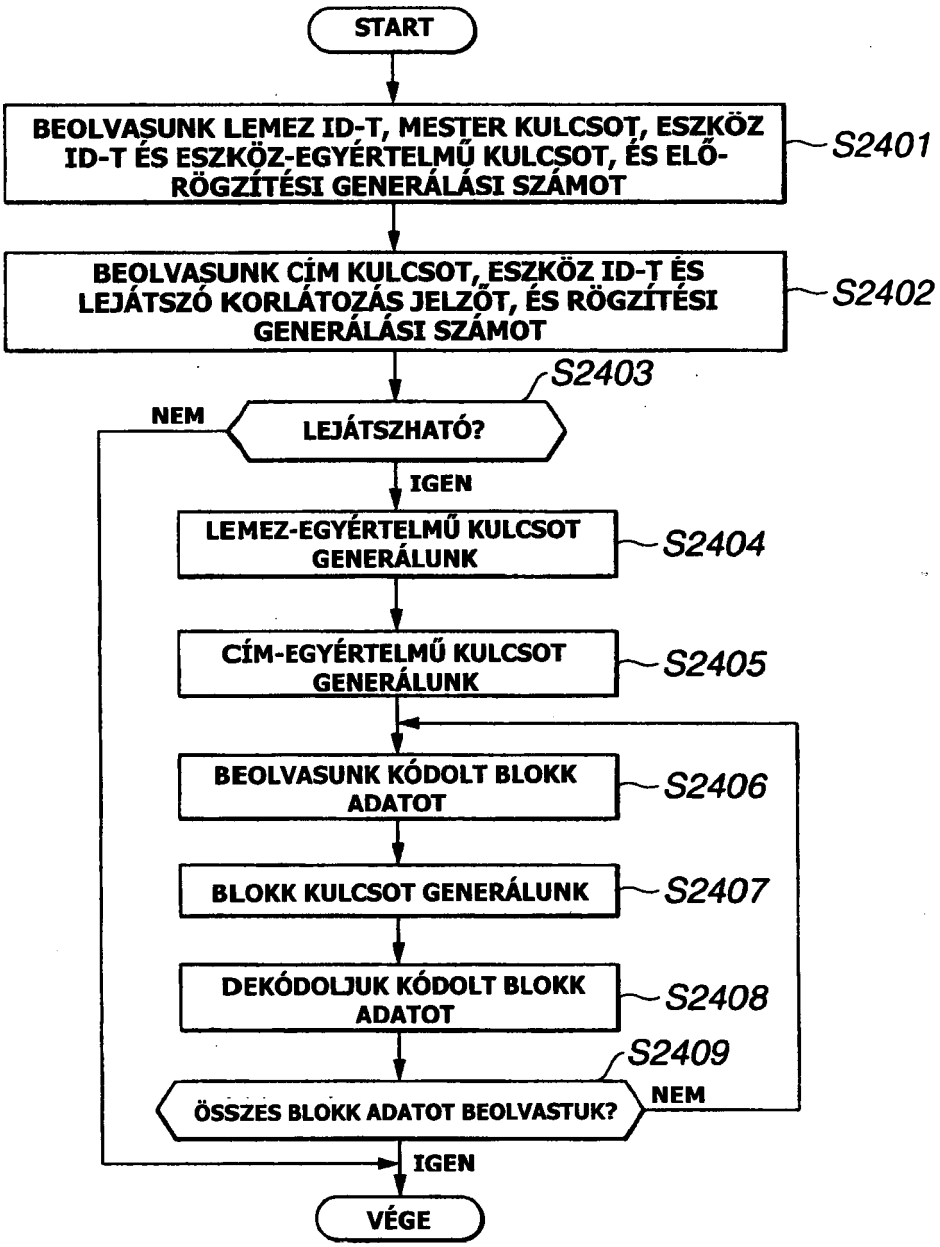
KIMENETEK:
BLOKK KULCS (64 BIT)



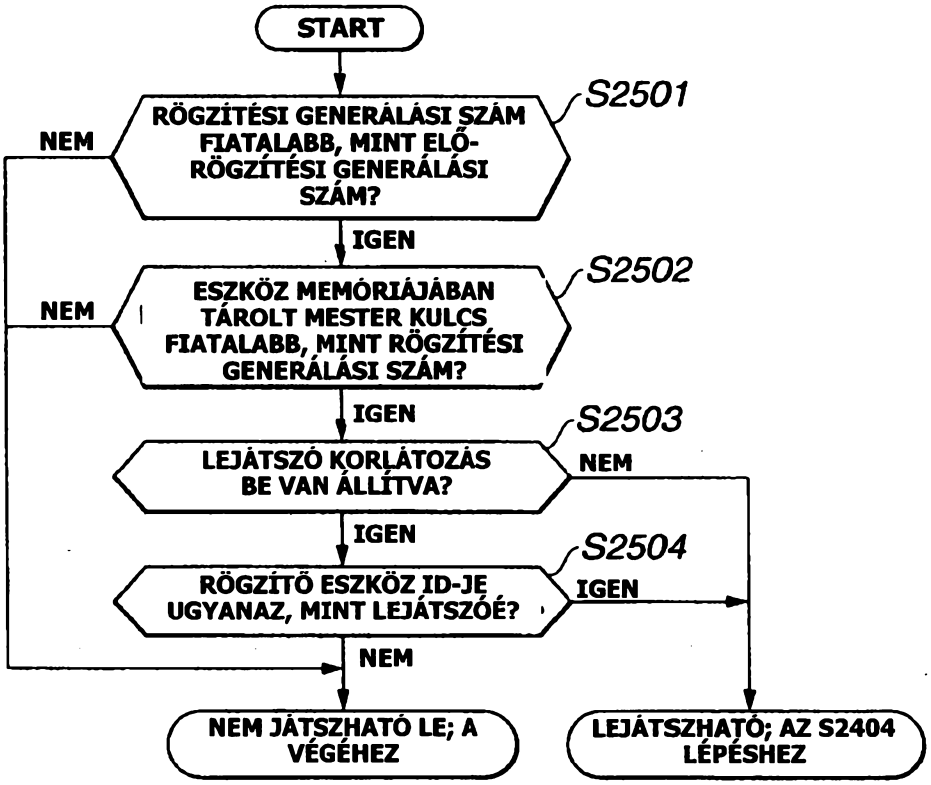
22. ÁBRA



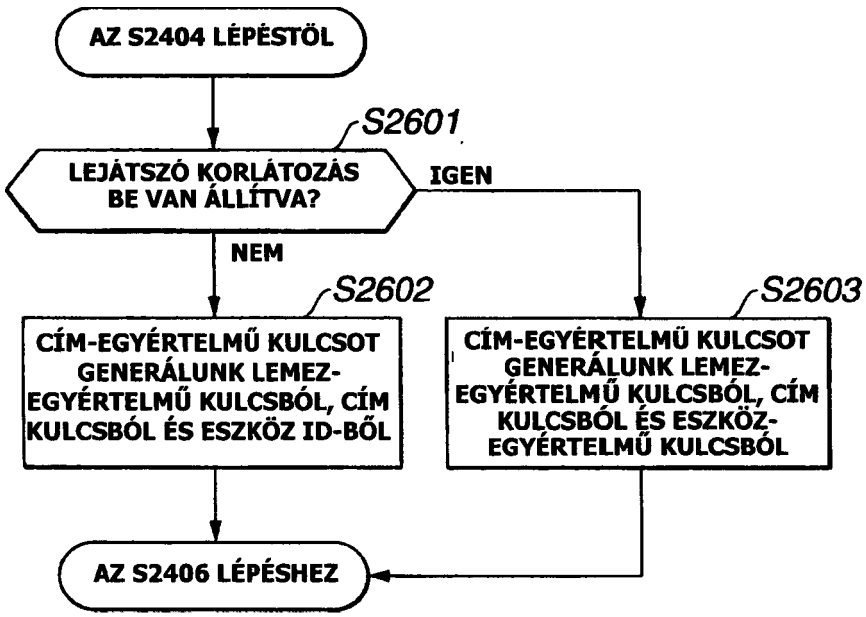
23. ÁBRA



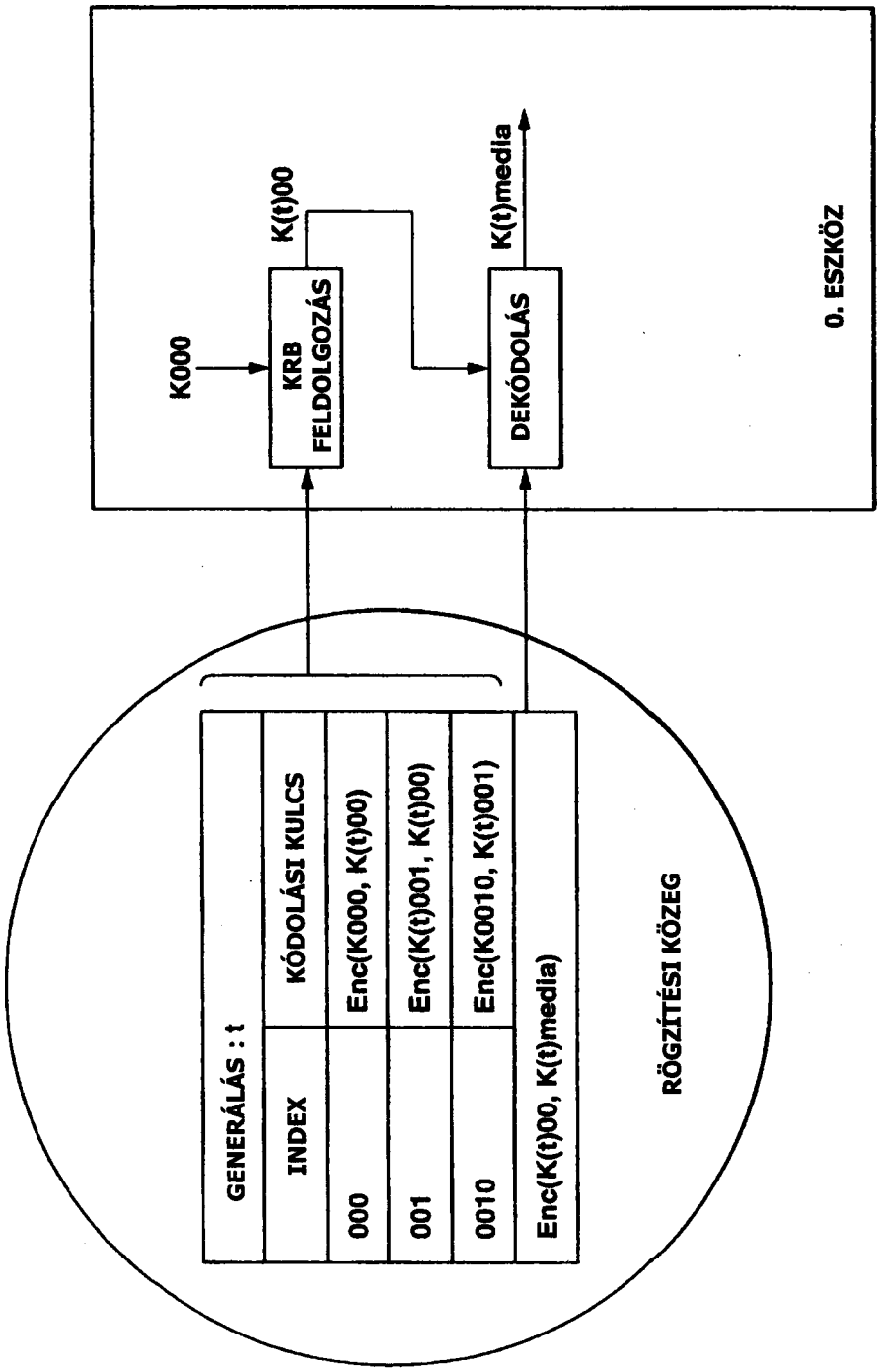
24. ÁBRA



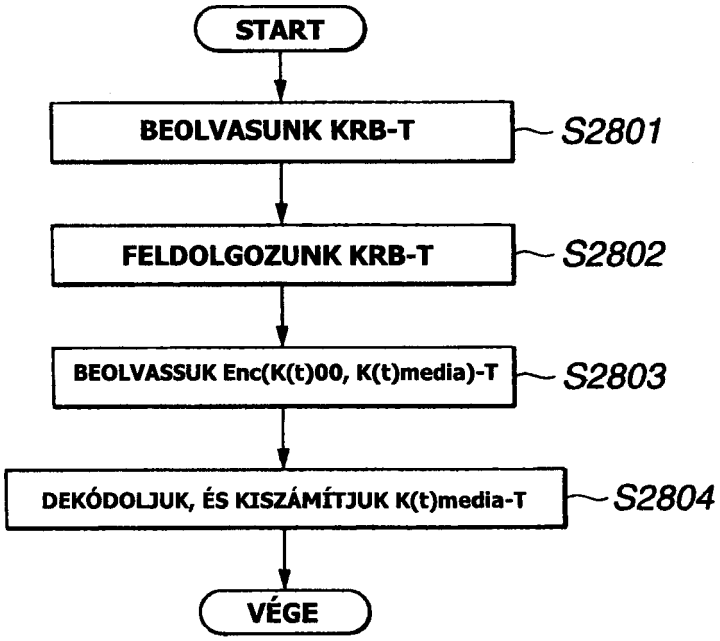
25. ÁBRA



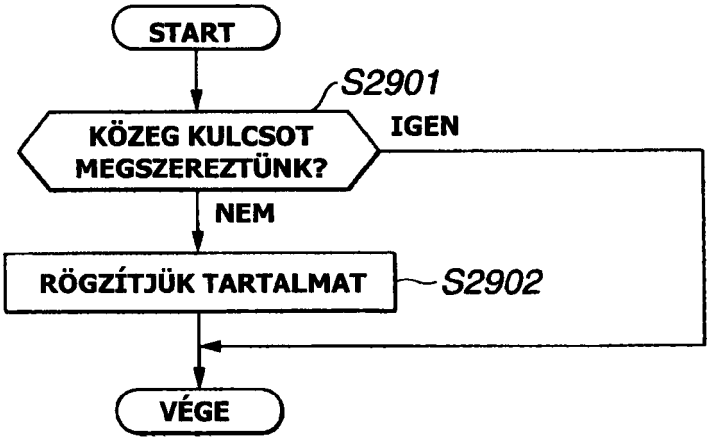
26. ÁBRA



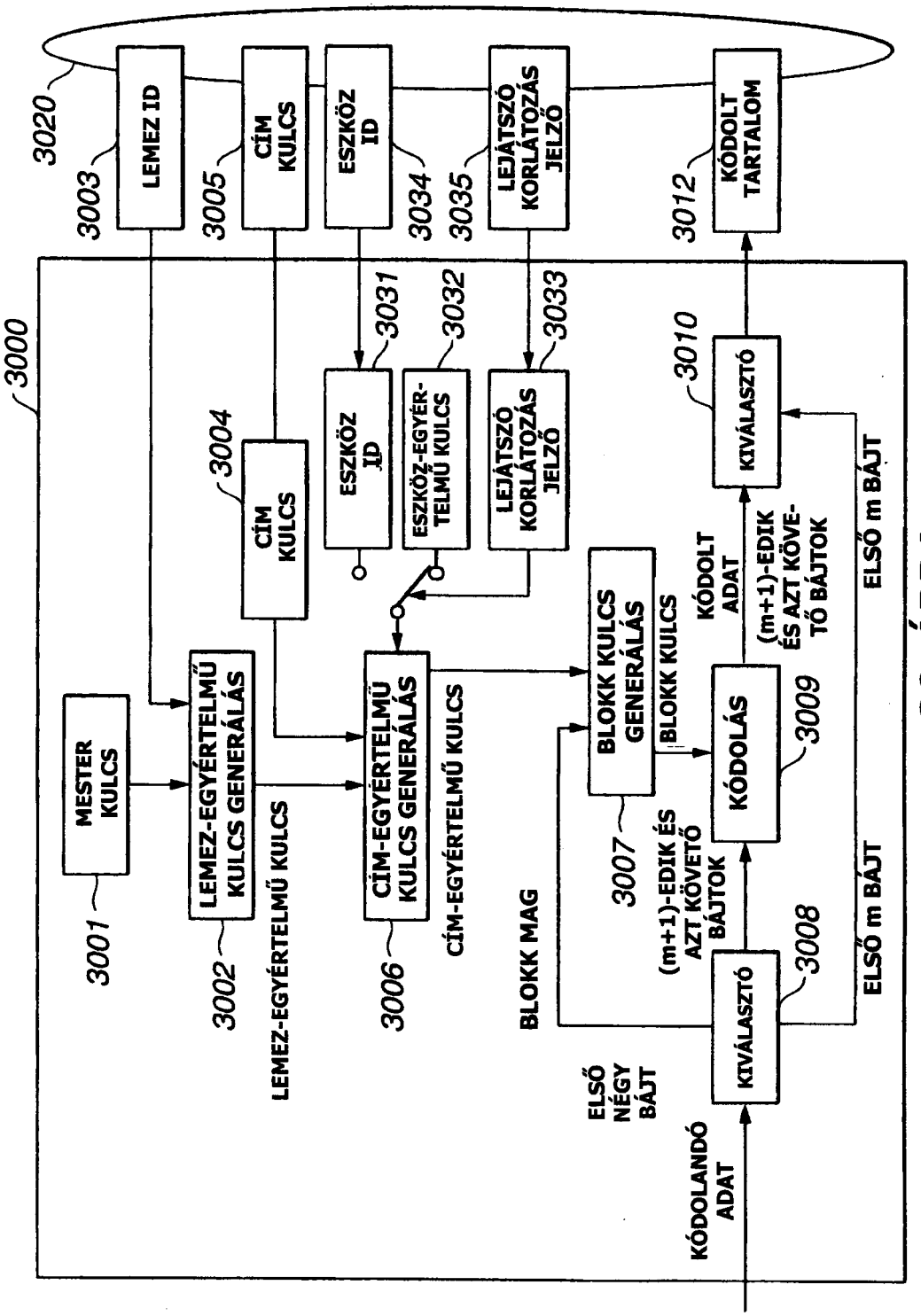
27. ÁBRA



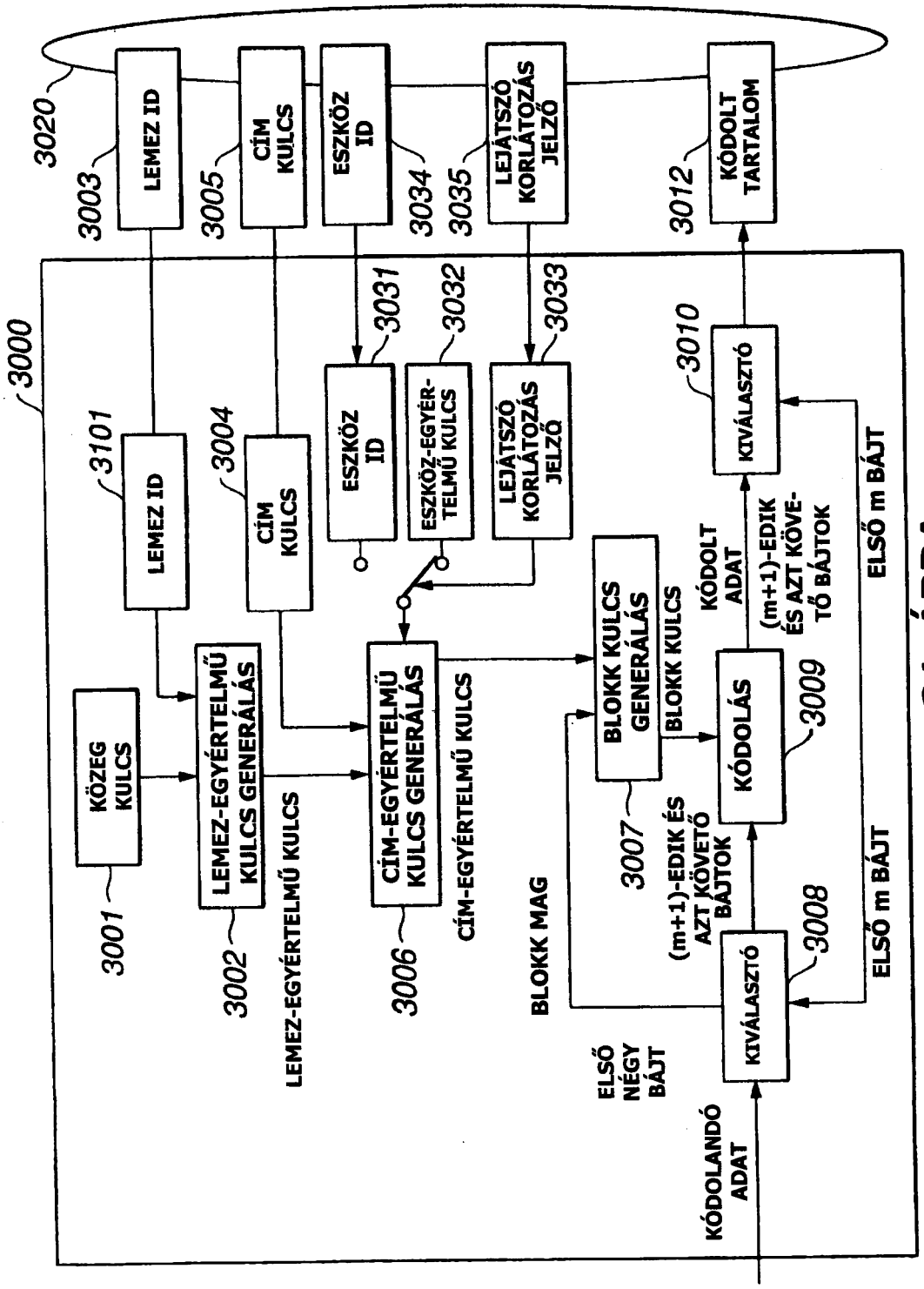
28. ÁBRA



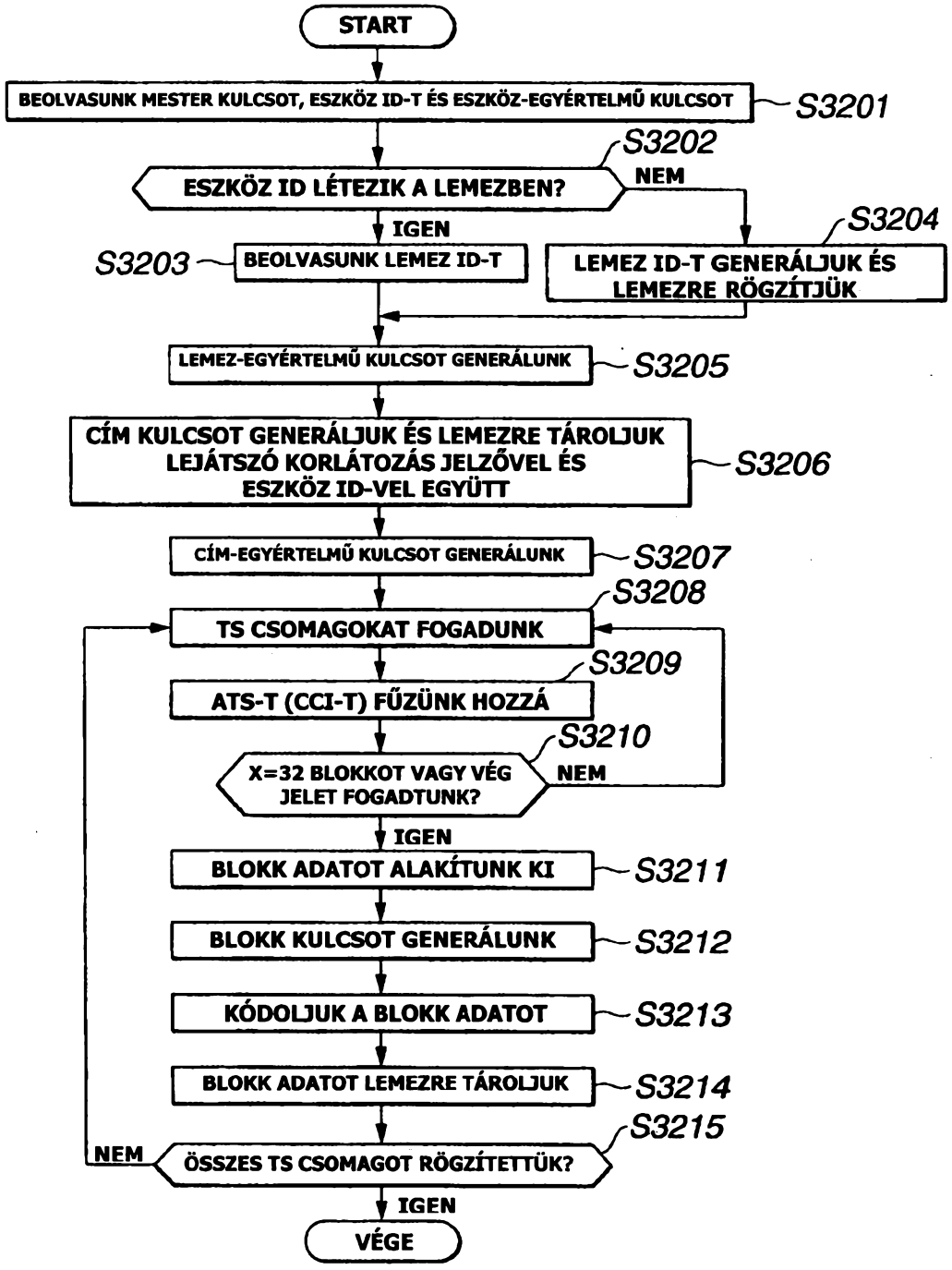
29. ÁBRA



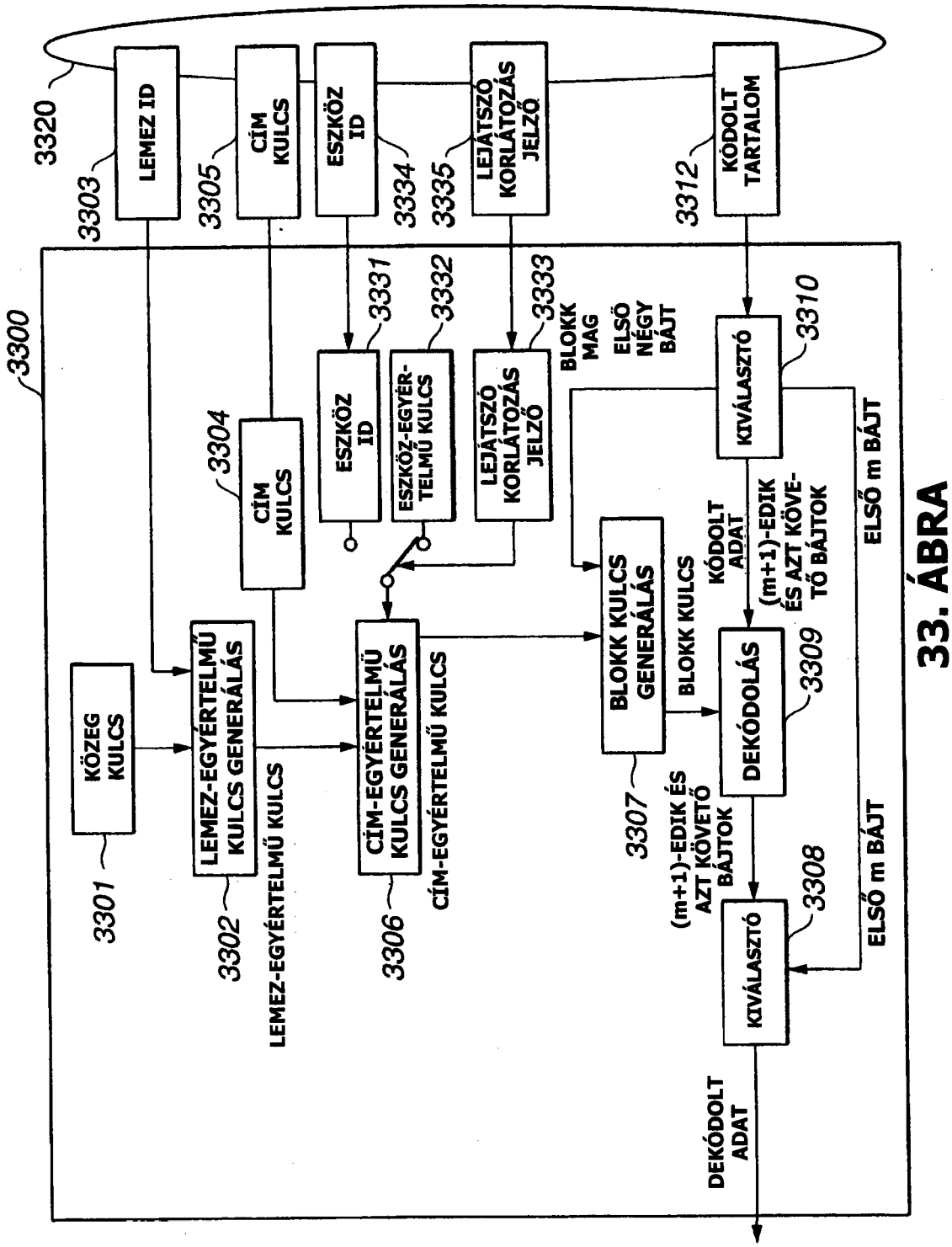
30. ÁBRA



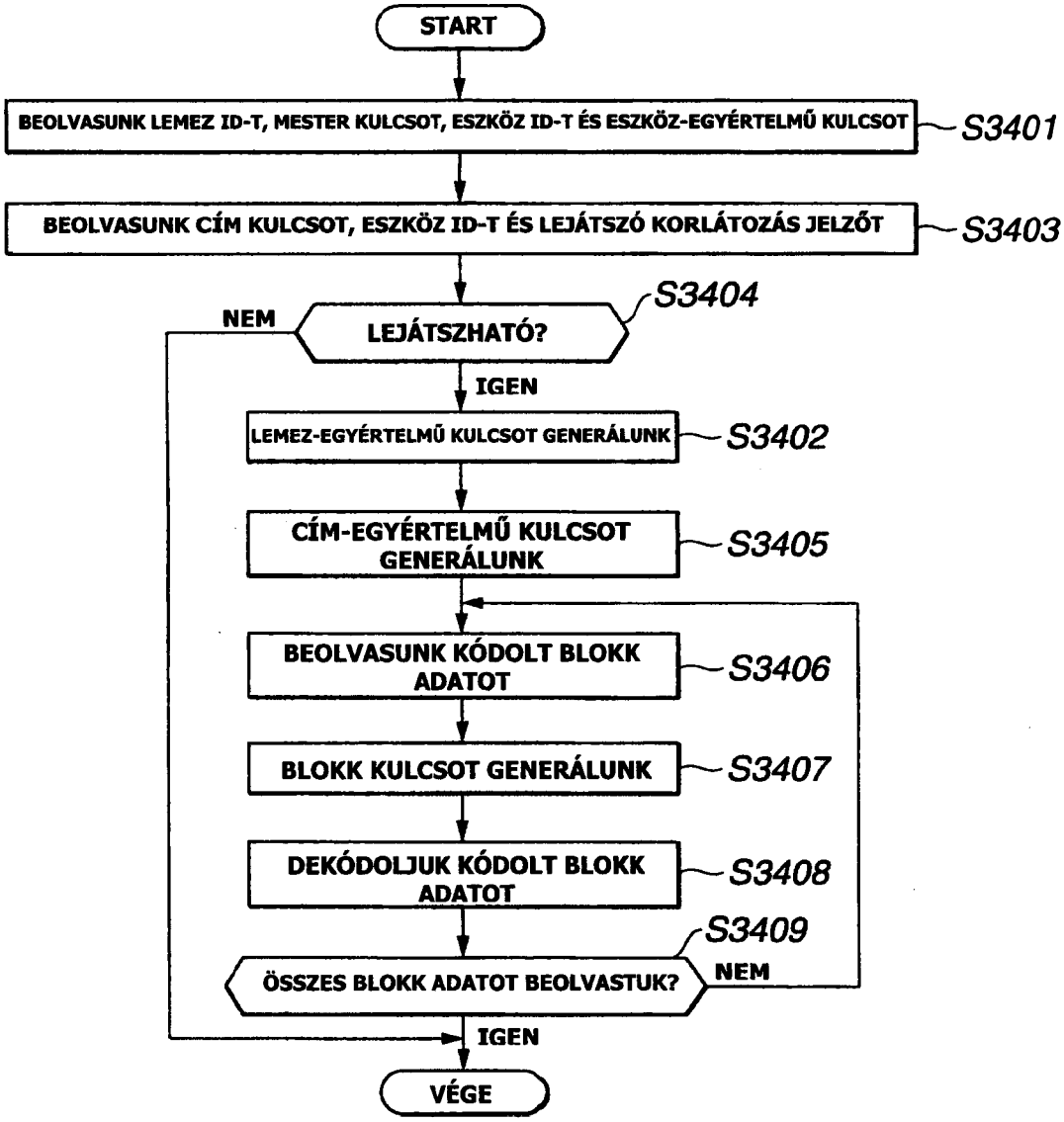
31. ÁBRA



32. ÁBRA

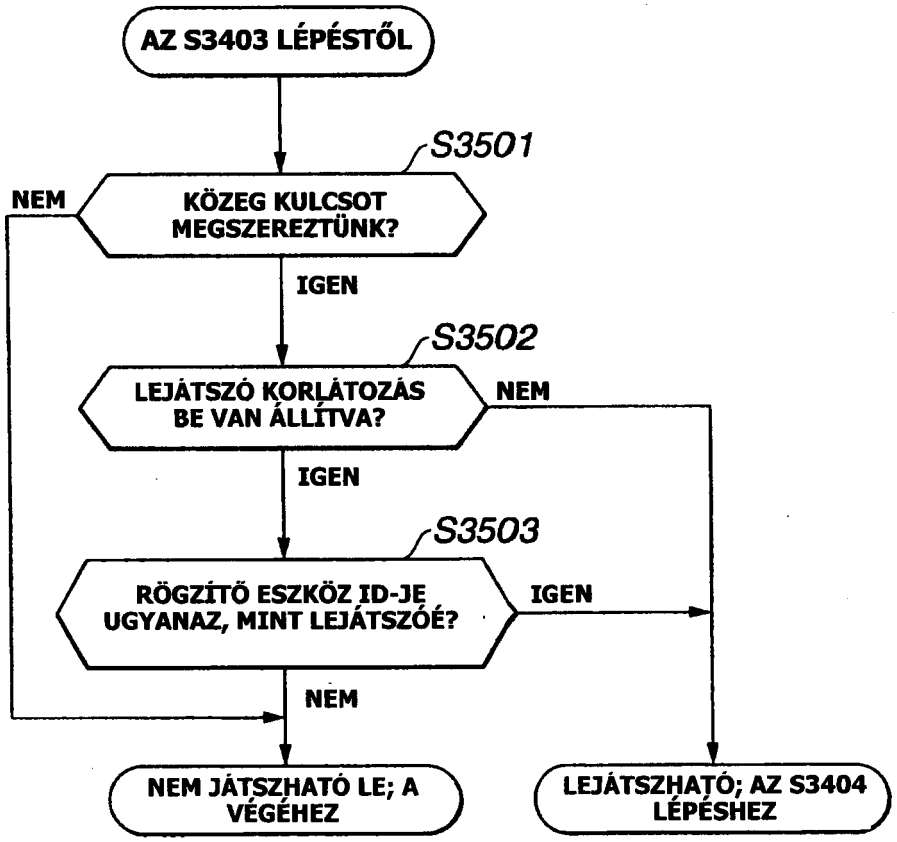


33. ÁBRA



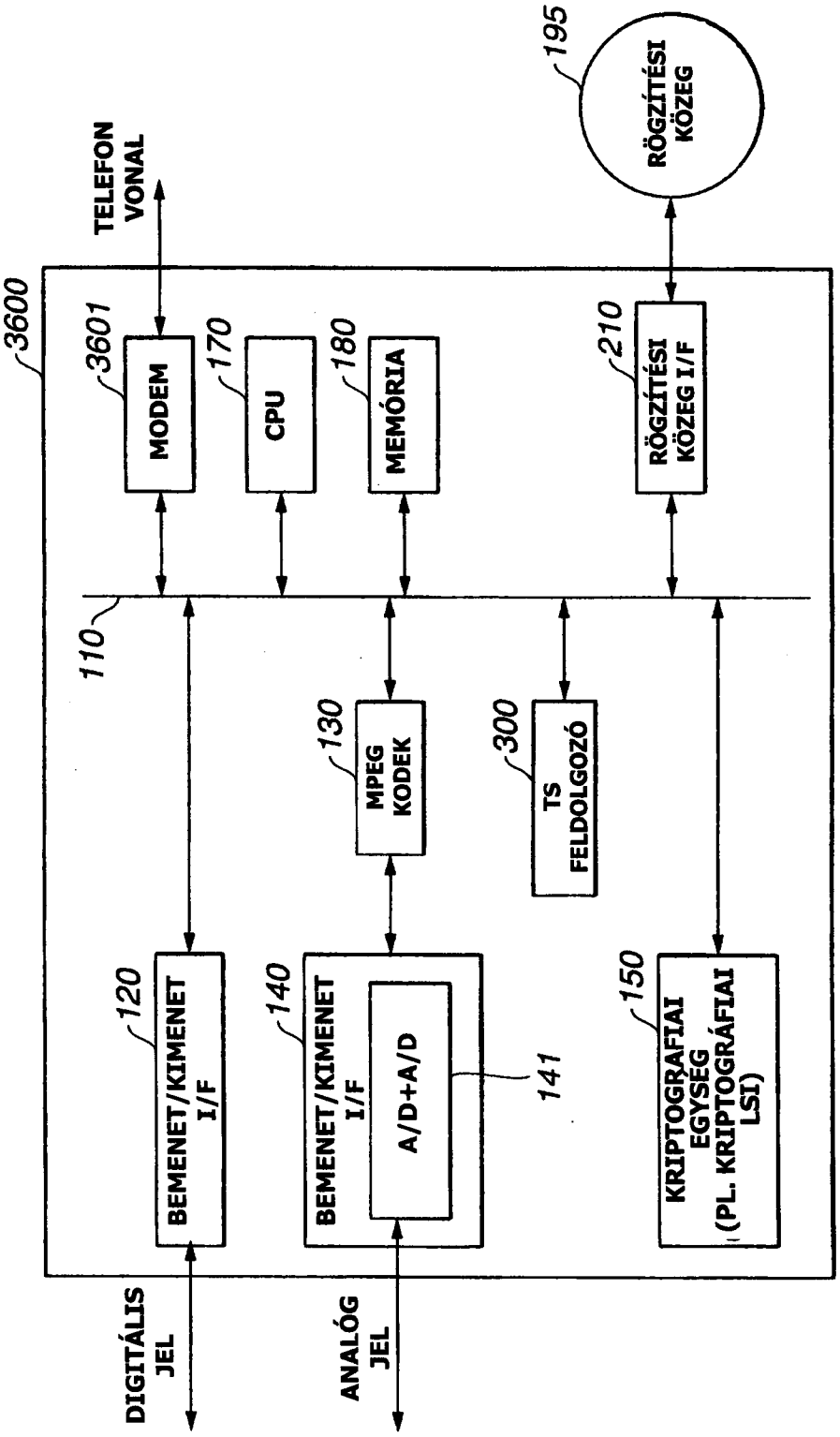
34. ÁBRA

KÖZZÉTÉTELI
PÉLDÁNY

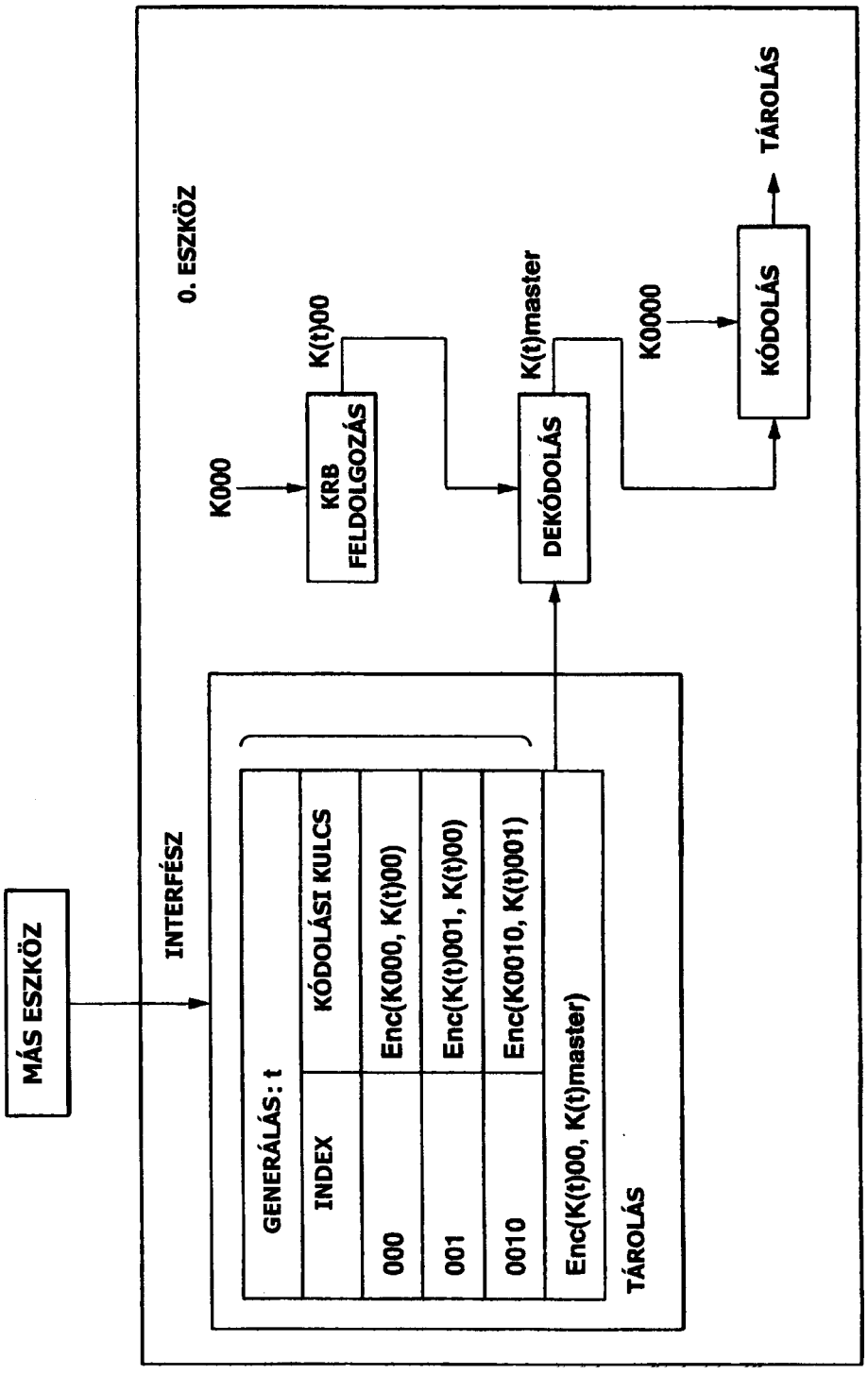


35. ÁBRA

KÖZZÉTÉTELI PÉLDÁNY

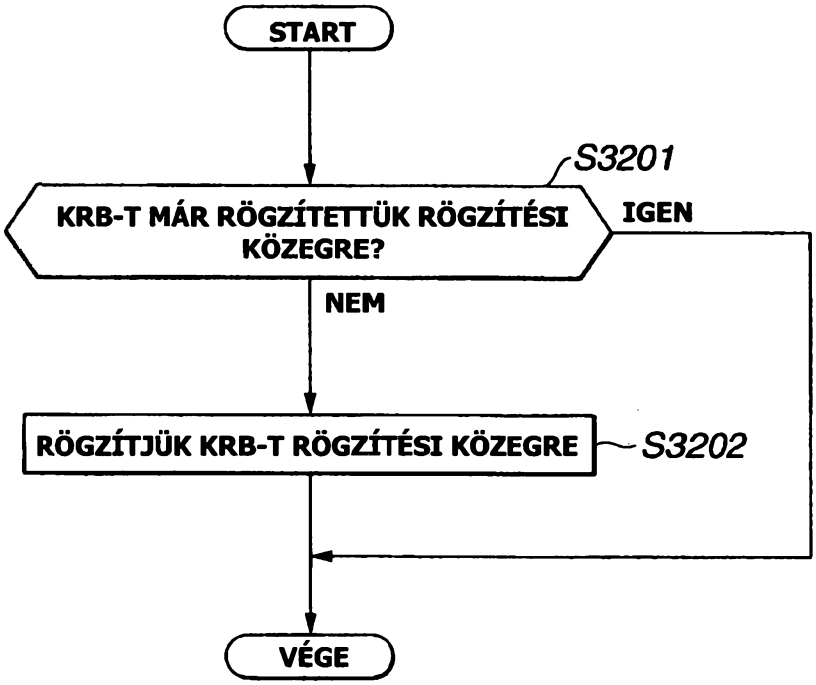


36. ÁBRA

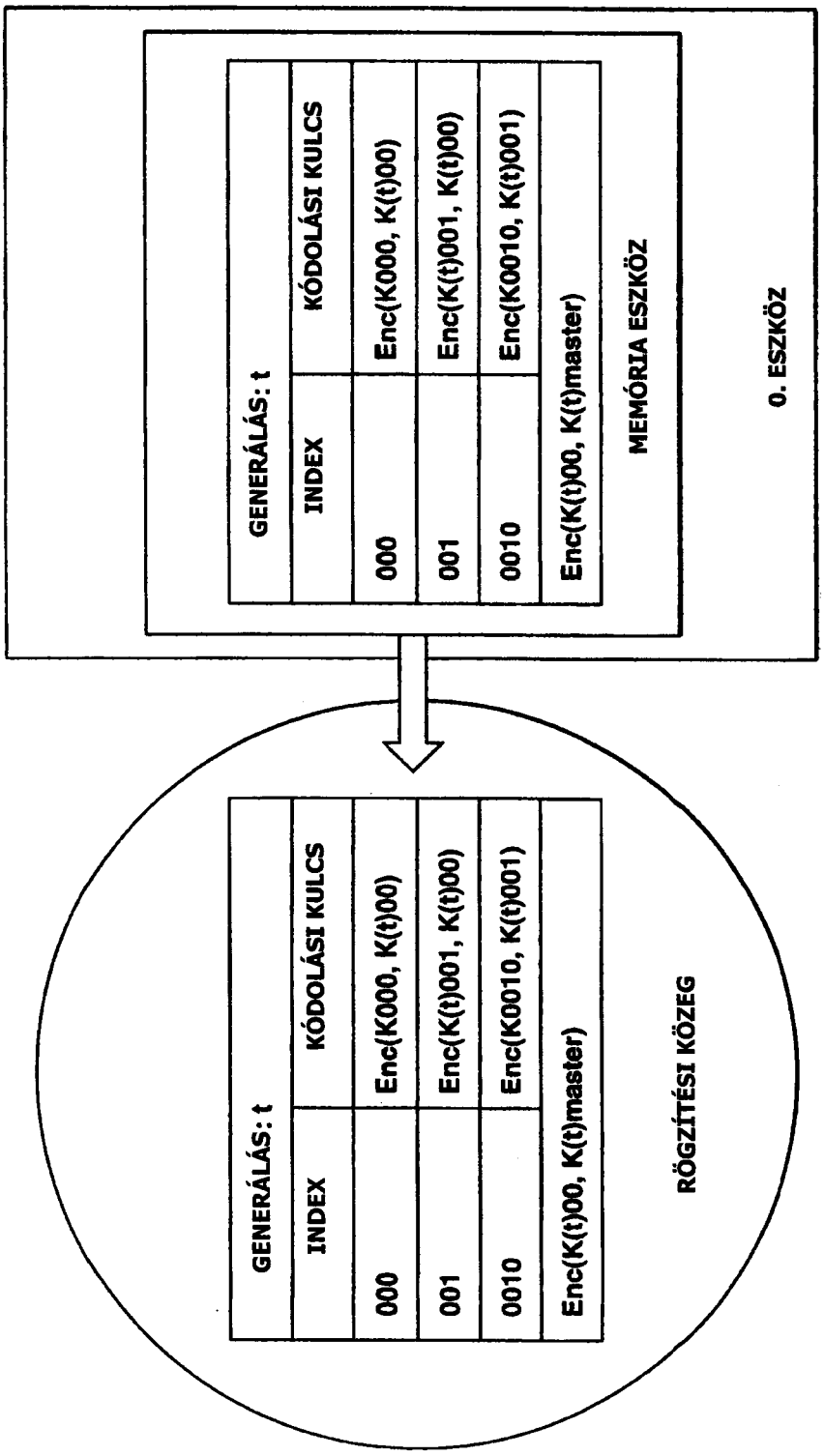


13. ÁBRA

KÖZZÉTÉTELI
PÉLDÁNY

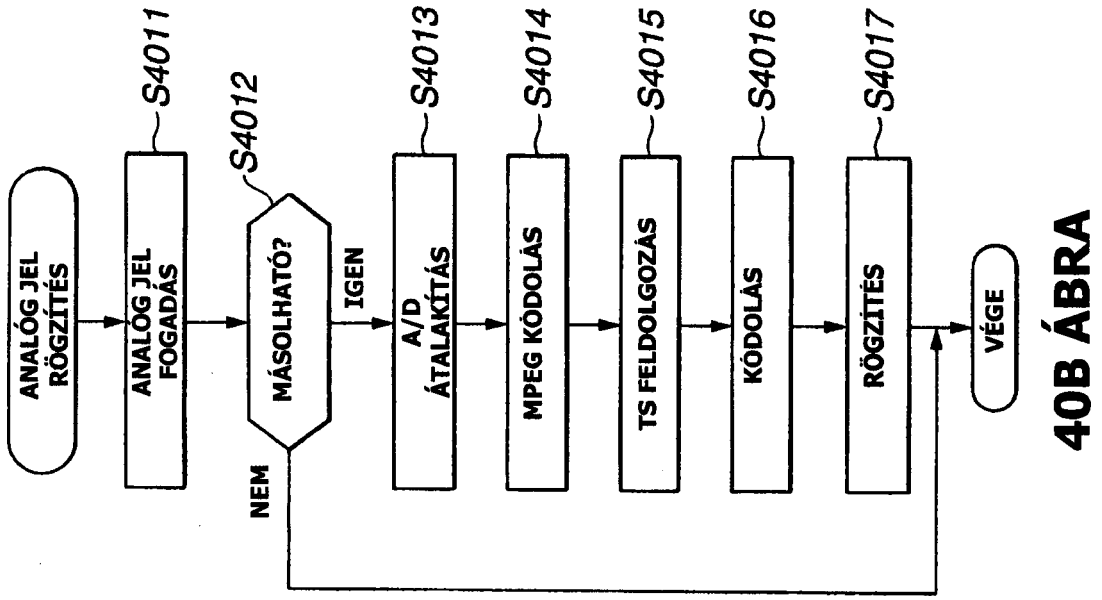


38. ÁBRA

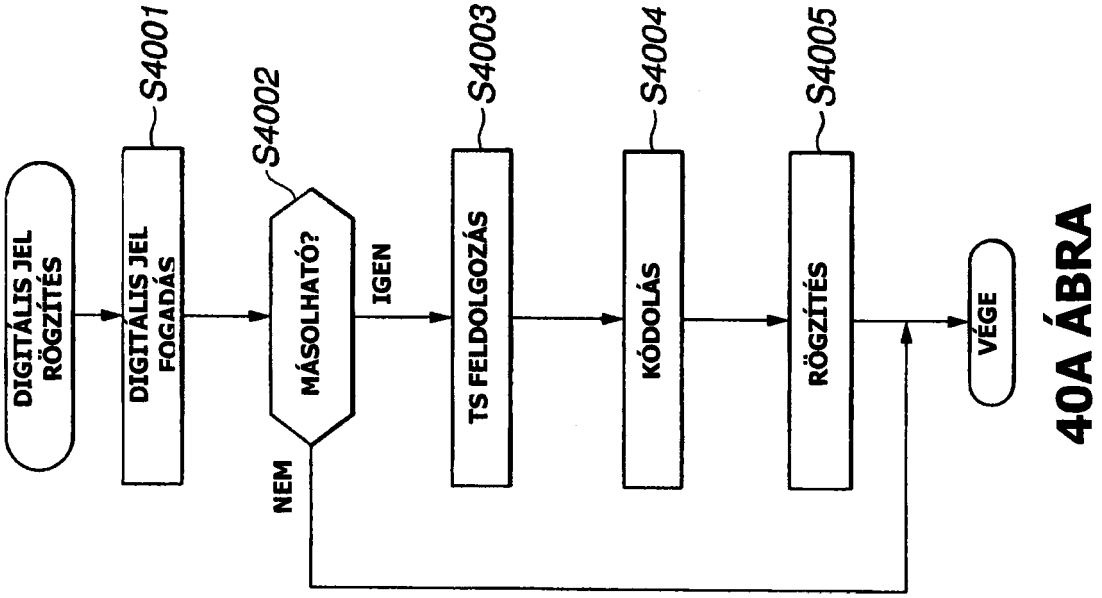


39. ÁBRA

KÖZZÉTÉTELI PÉLDÁNY

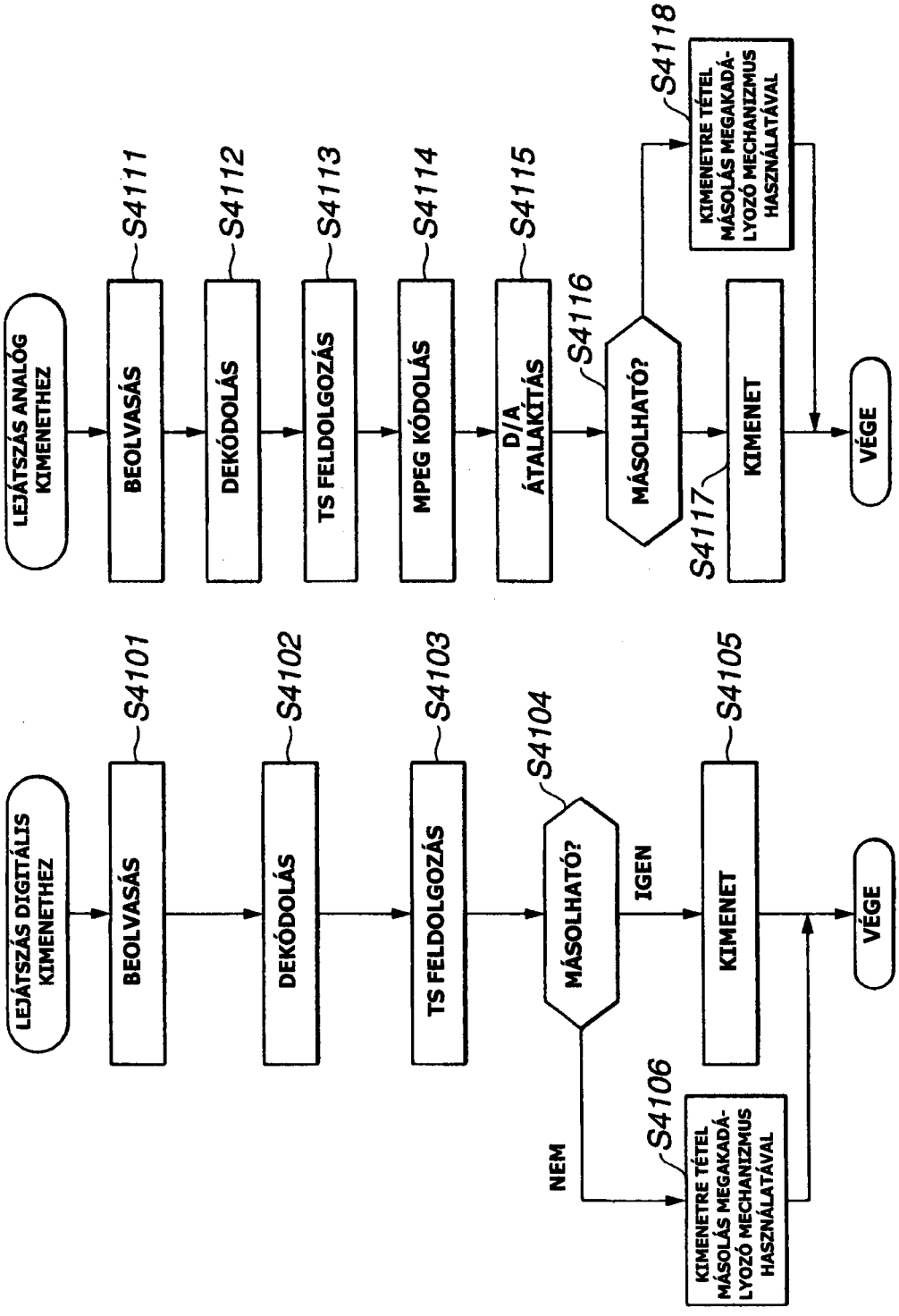


40B ÁBRA



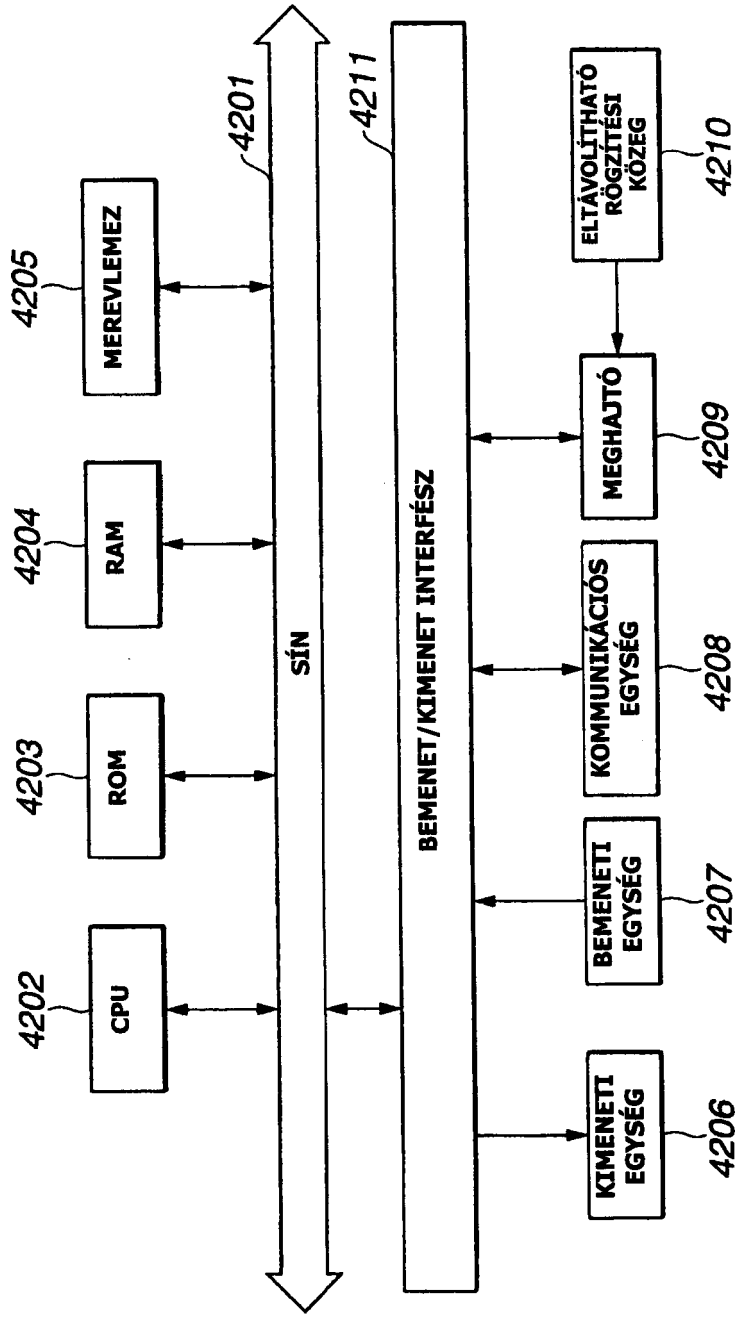
40A ÁBRA

KÖZZÉTÉTELI PÉLDÁNY



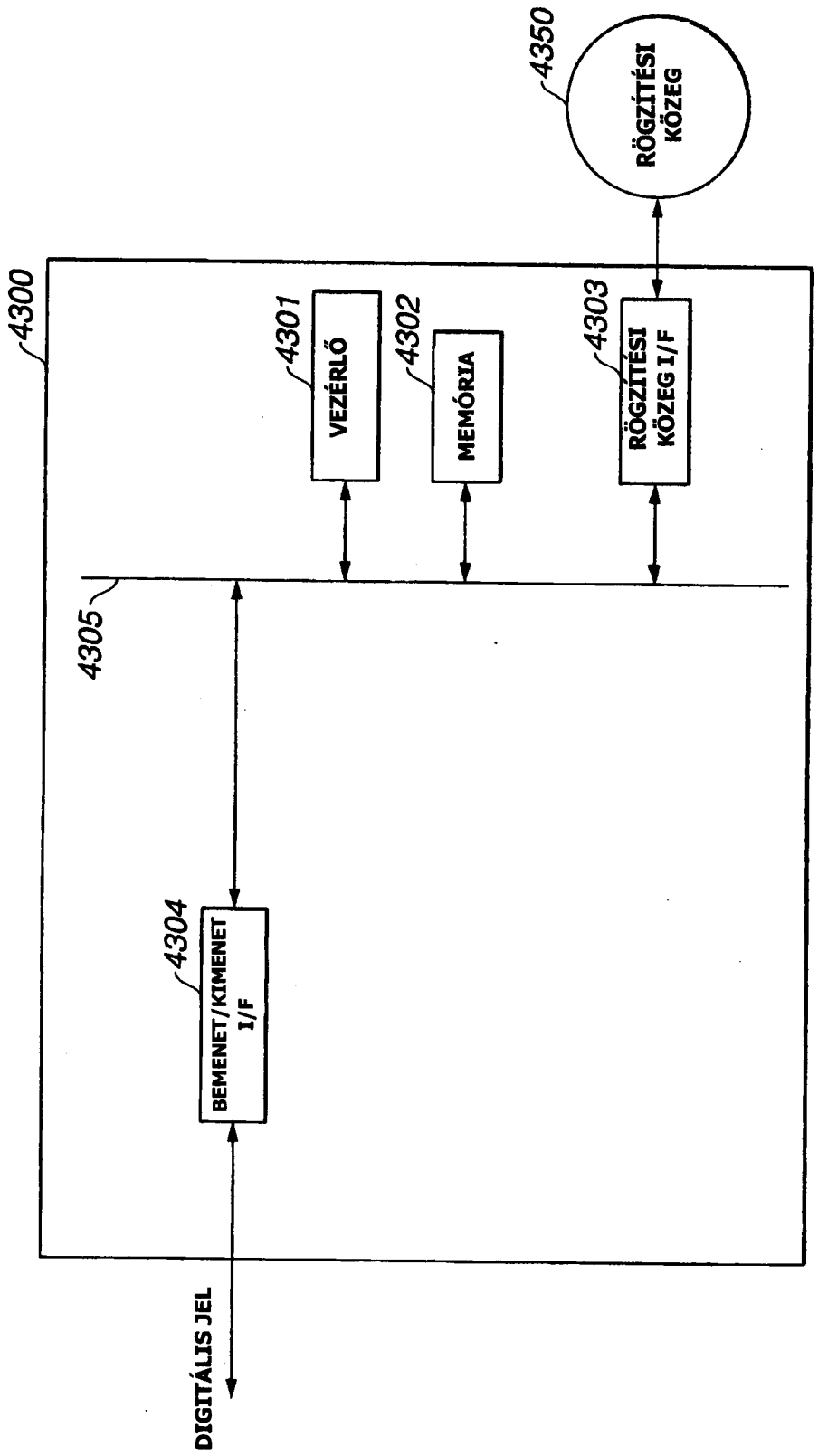
41A ÁBRA

41B ÁBRA



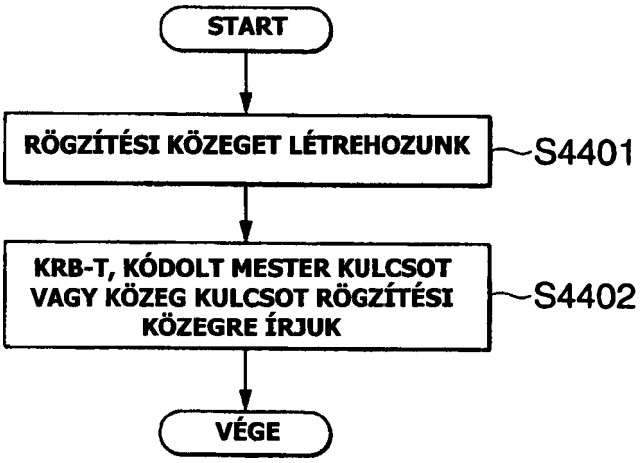
42. ÁBRA

KÖZZÉTÉTELI PÉLDÁNY

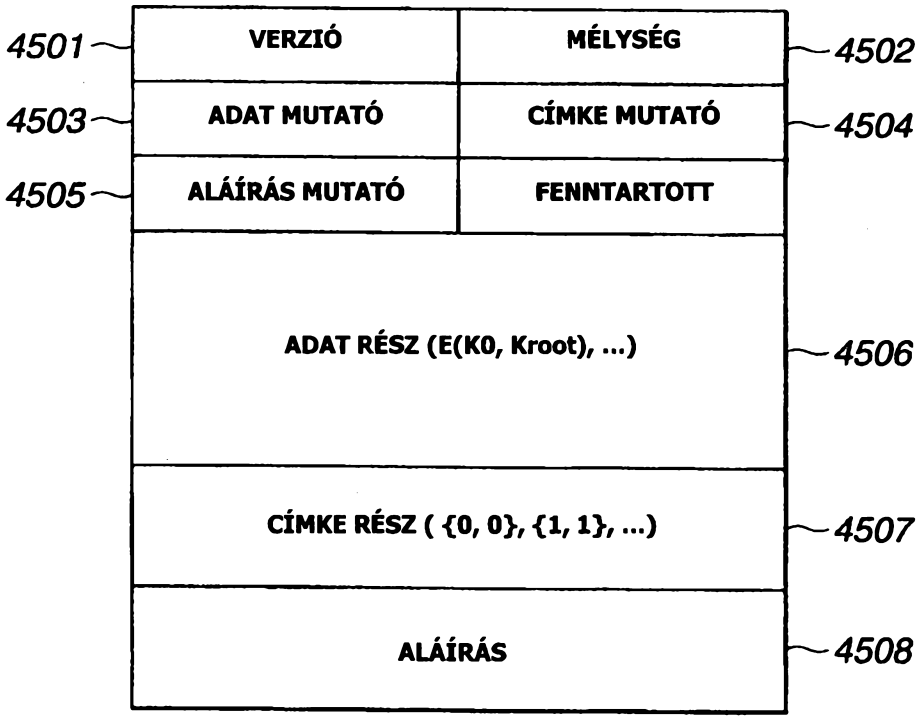


43. ÁBRA

KÖZZÉTÉTELI PÉLDÁNY



44. ÁBRA



45. ÁBRA

KÖZZÉTÉTELI
PÉLDÁNY