PŘIHLÁŠKA VYNÁLEZU

zveřejněná podle § 31 zákona č. 527/1990 Sb.

(21) Číslo dokumentu:
2001 - 2824

(13) Druh dokumentu: **A3**

(51) Int. Cl.[7]:
H 04 N 7/16

(19) ČESKÁ REPUBLIKA

ÚŘAD PRŮMYSLOVÉHO VLASTNICTVÍ

(22) Přihlášeno: **04.02.2000**

(32) Datum podání prioritní přihlášky: **04.02.1999**

(31) Číslo prioritní přihlášky: **1999/99400261**

(33) Země priority: **EP**

(40) Datum zveřejnění přihlášky vynálezu: **13.02.2002**
(Věstník č. 2/2002)

(86) PCT číslo: **PCT/IB00/00163**

(87) PCT číslo zveřejnění: **WO00/46994**

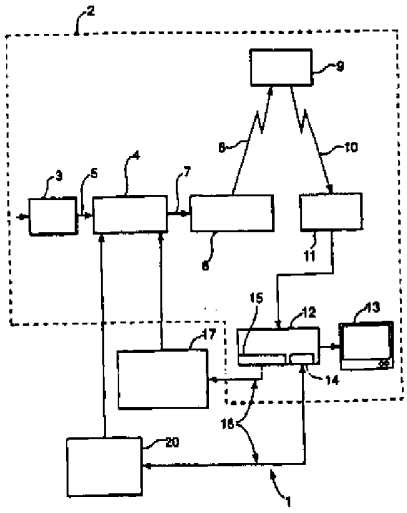
(71) Přihlašovatel:
CANAL+ SOCIETE ANONYME, Paris, FR;

(72) Původce:
Maillard Michel, Maintenon, FR;

(74) Zástupce:
Korejzová Zdeňka JUDr., Spálená 29, Praha 1, 11000;

(54) Název přihlášky vynálezu:

Způsob kódování dat a systém pro zajištění bezpečné komunikace dat



(57) Anotace:

Způsob a zařízení pro kódování dat mezi prvním zařízením (12) a druhým zařízením (30), ve kterém je jedna nebo více předem vypočítaných dvojic (41) klíčů uloženo v paměti prvního zařízení (12), přičemž každá dvojice (41) klíčů zahrnuje relační klíč a kódovanou verzi tohoto relačního klíče. Kódovaná verze se předává do druhého zařízení (30), které dekóduje relační klíč a ten potom používá pro kódování dat komunikovaných z druhého zařízení (30) do prvního zařízení (12) a/nebo obráceně. Vynález je obzvláště využitelný v digitálním televizním systému, ve kterém data, zejména data řídícího slova, mají být komunikována v kódované formě mezi dekodérem a přidruženým přenosným bezpečnostním modulem.

CZ 2001 - 2824 A3

Způsob kódování dat a systém pro zajištění bezpečné komunikace dat

Oblast techniky

Předkládaný vynález se týká způsobu a zařízení pro kódování zpráv mezi dvěma zařízeními, například dekodérem a přenosným bezpečnostním modulem v digitálním televizním systému.

Dosavadní stav techniky

Vysílání kódovaných (šifrovaných) dat je velmi dobře známé zejména v oblasti placených televizních systémů, kde kódované audiovizuální informace jsou obvykle přenášeny prostřednictvím satelitu k množství účastníků či předplatitelů, přičemž každý účastník má v držení dekodér, který je schopen dekódovat vysílaný program pro následné sledování.

V typickém systému jsou kódovaná či šifrovaná data vysílána společně s řídícím slovem pro dekódování těchto dat, přičemž řídící slovo samotné je kódováno nebo šifrováno prostřednictvím tak zvaného exploatačního klíče a je vysíláno v této kódované formě. Kódovaná (šifrovaná) data a šifrované (kódované) řídící slovo jsou potom přijímána dekodérem majícím přístup k ekvivalentu exploatačního klíče, uloženému na přenosném bezpečnostním modulu, jako je inteligentní karta vložená do dekodéru. Kódované řídící slovo je potom dekódováno na inteligentní kartě a následně komunikováno do dekodéru pro použití při dekódování (dešifrování) vysílaných dat.

Za účelem zlepšení bezpečnosti systému je řídící slovo měněno obvykle každých deset sekund, nebo podobně. To vylučuje situaci se statickým nebo pomalu se měnícím řídícím slovem, kde takové řídící slovo se může stát veřejně známým. Za takových okolností by potom bylo relativně jednoduché pro podvodného uživatele dodat toto známé řídící slovo do dekódovací jednotky na jeho dekodéru za účelem dekódování vysílání.

Nicméně přes toto bezpečnostní opatření vznikl v nedávných letech problém s tím, že tok řídících slov. vysílaných během přenosu, se stává známým prostřednictvím monitorování dat, komunikovaných v propojovacím rozhraní mezi inteligentní kartou a dekodérem. Tyto informace mohou být využity jakýmkoliv neautorizovaným uživatelem, který zaznamenal ještě kódovaný přenos na videorekordér. Pokud je film přehráván ve stejném okamžiku, jako je tok řídících slov dodáván do dekodéru, stává se možnou vizualizace (dekódování) přenosu. Tento problém byl navíc dále zvýrazněn s nástupem internetu, přičemž nyní lze běžně nalézt jakýkoliv počet internetových míst, která uvádějí seznam toku řídících slov, vysílaných během daných přenosů.

Evropská patentová přihláška PCT WO 97/3530 (Digco) se potýká s tímto problémem navržením řešení, ve kterém tok řídících slov, předávaný přes propojovací rozhraní mezi inteligentní kartou a dekodérem, je sám šifrován či kódován relačním klíčem. Relační klíč je generován náhodně dekodérem a je šifrován (kódován) s druhým klíčem, drženým v dekodéru a odpovídajícím veřejnému klíči, používanému s kódovacím algoritmem privátního a veřejného klíče. Přidružená inteligentní karta má v držení potřebný privátní klíč pro

dekódování relačního klíče, který je potom použit inteligentní kartou pro kódování toku řídících slov, vysílaného z inteligentní karty do dekodéru.

Jak by mělo být zcela zřejmé, použití lokálně generovaného relačního klíče pro kódování toku řídících slov znamená, že tento kódovaný tok potom nemůže být přiváděn do dalšího dekodéru pro použití při dekódování (dešifrování) dat, protože každý dekodér bude mít v držení odlišný relační klíč pro použití při dekódování toku řídících slov, vysílaného z inteligentní karty.

Ačkoliv toto řešení poskytuje vyšší úroveň zabezpečení než běžné systémy, je nicméně přesto s tímto systémem spojeno množství nevýhod.

Zjevně je použití algoritmu veřejného a privátního klíče skutečně obligatorní v takovémto systému, protože není z bezpečnostních důvodů žádoucí ukládat jak symetrický klíč tak i přidružený algoritmus v dekodéru vzhledem ke snadnosti s jakou tyto informace mohou být z paměti dekodéru získány. Tento problém nevzniká v případě veřejného klíče, protože držení tohoto klíče neumožňuje dekódování zpráv kódovaných s privátním klíčem.

Jedním cílem předkládaného vynálezu je vytvoření adaptabilnější alternativy ke shora uvedenému známému systému. Vynález ale není omezen pouze na oblast zabezpečení dekodéru a, jak bude podrobněji popsáno níže, může být aplikován na množství dalších situací, ve kterých je požadována bezpečná komunikace dat.

Podstata vynálezu

První aspekt předkládaného vynálezu navrhuje způsob kódování dat komunikovaných mezi prvním a druhým zařízením, ve kterém se alespoň jedna předem vypočítaná dvojice klíčů uloží v paměti prvního zařízení, přičemž tato alespoň jedna dvojice klíčů zahrnuje relační klíč a kódovanou verzi tohoto relačního klíče, připravenou s použitím transportního klíče, přičemž kódovaná verze relačního klíče se následně komunikuje do druhého zařízení, které dekóduje tuto kódovanou verzi s použitím ekvivalentu transportního klíče, uloženého v jeho paměti, takže data, komunikovaná z alespoň druhého zařízení do prvního zařízení, mohu být potom v příslušných zařízeních kódována a dekódována prostřednictvím relačního klíče.

Výhodné provedení předkládaného vynálezu navrhuje způsob kódování dat komunikovaných mezi prvním a druhým zařízením charakterizovaný tím, že jedna nebo více předem vypočítaných dvojic klíčů se uloží v paměti prvního zařízení, přičemž tato jedna nebo každá dvojice klíčů zahrnuje relační klíč a kódovanou verzi tohoto relačního klíče, připravenou s použitím transportního klíče, přičemž kódovaná hodnota relačního klíče se následně komunikuje do druhého zařízení, které dekóduje tuto hodnotu s použitím ekvivalentu transportního klíče, uloženého v jeho paměti, takže data, komunikovaná z alespoň druhého zařízení do prvního zařízení, mohu být potom v příslušných zařízeních kódována a dekódována prostřednictvím relačního klíče.

Oproti výše popisovanému systému podle patentového spisu PCT WO 97/3530 (Digco) vylučuje použití předem vypočítané, uložené dvojice hodnot nutnost muset zajistit

kódovací algoritmus uvnitř prvního zařízení (kterým je například dekodér) pro dekódování vnitřně generovaného relačního klíče. V důsledku toho algoritmu, zvolený pro kódování relačního klíče, nemusí být omezen na algoritmus veřejného a privátního klíče, ale může odpovídat algoritmu symetrického typu, pokud je to žádoucí. Jak by ale mělo být zcela zřejmé, předkládaný vynález nicméně přesto může být také realizován s použitím algoritmů veřejného a privátního klíče pro kódování relačního klíče, jak ostatně bude podrobněji diskutováno níže.

Výhodně se v paměti prvního zařízení uloží množství dvojic klíčů, přičemž první zařízení vybírá a zpracovává jeden nebo více relačních klíčů pro generování definitivního relačního klíče a komunikuje přidruženou kódovanou hodnotu nebo hodnoty do druhého zařízení pro dekódování a zpracování druhým zařízením pro generování definitivního relačního klíče.

Vytvoření množství dvojic klíčů uvnitř prvního zařízení umožňuje prvnímu zařízení volit a definovat různé definitivní relační klíče pro každou komunikační relaci. V jednom provedení vynálezu se prvním zařízením zvolí či vybere podskupina z množství uložených relačních klíčů pro generování definitivního relačního klíče, přičemž přidružené kódované hodnoty podskupiny těchto relačních klíčů se komunikují do druhého zařízení pro dekódování a zpracování.

V závislosti na typu použité operace může být výsledný definitivní relační klíč závislý na pořadí kombinace zvolených relačních klíčů. V takovém provedení se tyto informace o pořadí komunikují do druhého zařízení pro

umožnění druhému zařízení správně generovat definitivní relační klíč s použitím přidružených kódovaných hodnot.

Například úvodní hodnota relačního klíče, známá jak prvnímu tak i druhému zařízení, může být opakovaně kódována v obou zařízeních prostřednictvím seřazené sekvence relačních klíčů s využitím kódovacího algoritmu citlivého na pořadí kódování, jako je DES symetrický algoritmus.

Samozřejmě že tam, kde první zařízení využívá zvolenou podskupinu klíčů pro generování definitivního relačního klíče, nemusí být potřebné rovněž použít na pořadí závislý algoritmus pro generování proměnného definitivního relačního klíče a klíče mohou být kombinovány, například, s použitím jednoduché aritmetické operace.

V jednom výhodném provedení vynálezu může být jedna nebo více předem vypočítaných hodnot dvojic klíčů zvoleno z větší skupiny předem vypočítaných hodnot klíčů před uložením do prvního zařízení. Například, operátor nebo správce systému může komunikovat velké množství předem vypočítaných dvojic klíčů výrobci prvního zařízení, přičemž výrobce zařízení potom zvolí náhodně dvojice klíčů pro uložení do daného zařízení.

Tímto způsobem hodnoty dvojice nebo dvojic klíčů, uložené v prvním zařízení, budou unikátní pro toto zařízení, nebo alespoň kvazi-unikátní, což zvyšuje úroveň zabezpečení systému. Navíc entita, odpovědná za výrobu zařízení, nemusí mít v držení algoritmus nebo klíče použité pro přípravu hodnot kódovaných relačních klíčů, ale může jí být jednoduše dodána tabulka dvojic klíčů.

Výhodně kódovaná hodnota nebo hodnoty klíčů, komunikované do druhého zařízení, rovněž obsahují hodnotu podpisu, která může být čtena druhým zařízením pro ověření pravosti komunikované hodnoty.

Taková hodnota podpisu může být generována a ověřována podle běžného podpisového systému, například s použitím kombinace přepočítacích algoritmů a algoritmů veřejného a privátního klíče, jako je MD5 a RSA, přičemž podpis je připojen k hodnotám dvojic klíčů, uloženým v prvním zařízení.

Výhodně může být hodnota podpisu rovněž předem vypočítána v okamžiku výpočtu kódované hodnoty klíče a potom uložena v prvním zařízení.

Ve zvláště výhodném provedení vynálezu algoritmus a transportní klíč, použité pro kódování a dekódování relačního kliče nebo klíčů, odpovídají symetrickému algoritmu a přidruženému symetrickému klíči. Použití symetrického algoritmu umožňuje zvýšení doby zpracování, potřebné pro druhé zařízení, aby dekódovalo relační klíč, ve srovnání s operací využívající algoritmus veřejného a privátního kliče.

Ačkoliv jedna z výhod předkládaného vynálezu spočívá v adaptabilitě předkládaného systému pro použití symetrického algoritmu, mělo by být zcela zřejmé, že to není obligatorní. Například v alternativním provedení vynálezu relační klíč nebo klíče mohu být kódovány veřejným klíčem přes uložením do prvního zařízení a dekódovány ekvivalentním privátním klíčem uvnitř druhého zařízení.

Výhodně dále kódovací algoritmus, použitý s relačním klíčem pro kódování a dekódování dat komunikovaných mezi

prvním a druhým zařízením (nebo obráceně), odpovídá symetrickému algoritmu. Volba použitého algoritmu může záviset na systémových požadavcích, jako je nutnost mít dvousměrnou komunikaci mezi zařízeními.

Vhodné symetrické algoritmy mohou zahrnovat DES algoritmy nebo dokonce vhodný autorizovaný algoritmus. Vhodné algoritmy veřejného a privátního klíče mohou zahrnovat RAS algoritmy nebo další podobné algoritmy.

Jak bylo zmiňováno výše, předkládaný vynález je zejména využitelný v oblasti digitální televize, přičemž v jednom výhodném provedení první zařízení odpovídá dekodéru a druhé zařízení odpovídá přenosnému bezpečnostnímu modulu (nebo obráceně).

Přenosný bezpečnostní modul může výhodně zahrnovat inteligentní kartu. Pokud je tomu tak, mohou data, kódovaná s relačním klíčem, odpovídat jednoduchým informacím řídícího slova, použitým dekodérem pro dekódování přenášených dat.

Stejný princip může být rovněž aplikován na případ, ve kterém je dekódovací jednotka v dekodéru realizována jako odnímatelný modul podmíněného přístupu nebo CAM, přičemž přenášená data jsou dekódována v tomto modulu podmíněného přístupu a komunikována do dekodéru.

V takovém provedení tedy první zařízení může odpovídat dekodéru a druhé zařízení může odpovídat odnímatelnému modulu podmíněného přístupu. Pokud je tomu tak, budou data, kódovaná s relačním klíčem, obvykle odpovídat datům, dekódovaným modulem podmíněného přístupu, to jest například vlastnímu přenášenému programu.

V realizaci s modulem podmíněného přístupu může inteligentní karta rovněž tvořit součást systému, přičemž tato karta se vkládá do modulu podmíněného přístupu pro dekódování řídícího slovo, které se potom předává do modulu podmíněného přístupu pro umožnění dekódování přenášeného programu. Pokud je tomu tak, první zařízení potom může odpovídat modulu podmíněného přístupu, druhé zařízení může odpovídat inteligentní kartě a data, kódovaná s relačním klíčem, mohou odpovídat datům řídícího slova.

V oblasti digitální televize může být předkládaný vynález rovněž aplikován na komunikaci dat mezi dekodérem a dalšími zařízeními, jako je televize nebo videorekordér. Například v jednom výhodném provedení první zařízení odpovídá prvnímu dekodéru a druhé zařízení odpovídá druhému dekodéru.

V domácnostech, majícím v držení první a druhé dekodér, se často objevuje množství problémů spojených s udržováním komunikace mezi prvním nebo "nadřazeným" dekodérem a druhým "podřízeným" dekodérem. Použití bezpečné kódované linky pro komunikování audiovizuálních dat, dat řídícího slova, nebo dokonce dat, týkajících se aktuálních účastnických (předplatitelských) práv a exploatačních klíčů, se může v této souvislosti jevit užitečným.

V ještě další realizaci může být předkládaný vynález aplikován pro domácí síťový systém, kde první a druhé zařízení odpovídá prvnímu a druhému elektronickému zařízení spotřebitele, upraveným pro přenos dat přes komunikační linku (například rádiovou, PLC, infračervenou, a podobně).

Shora uvedená provedení byla popsána ve spojení se způsobem kódování dat. Z hlediska dalšího aspektu může být

předkládaný vynález stejně tak aplikován na první a druhé zařízení, upravená pro provádění takovéhoto způsobu.

Další aspekt předkládaného vynálezu navrhuje systém pro zajištění bezpečné komunikace dat mezi prvním a druhým zařízením, přičemž první zařízení zahrnuje paměť pro uložení alespoň jedné předem vypočítané dvojice klíčů, zahrnující relační klíč a kódovanou verzi relačního klíče, připravenou s použitím transportního klíče, a komunikační prostředek, jako je komunikační linka, pro komunikování kódované verze relačního klíče do uvedeného druhého zařízení, přičemž druhé zařízení zahrnuje paměť pro uložení ekvivalentu transportního klíče, dekódovací prostředek, jako je procesor, pro dekódování uvedené kódované verze relačního klíče s použitím uvedeného ekvivalentu transportního klíče, a prostředek, jako je procesor, pro kódování dat, která mají být komunikována do uvedeného prvního zařízení, s použitím relačního klíče.

Znaky popsané výše, týkající se aspektů způsobu podle předkládaného vynálezu, mohou být rovněž aplikovány na aspekty zařízení nebo systému, a obráceně.

Výše použité termíny "přenosný bezpečnostní modul", "inteligentní karta" a "modul podmíněného přístupu" mohou být interpretovány v jejich nejširším smyslu a označují tedy jakoukoliv přenosnou kartu na bázi mikroprocesoru a/nebo paměti, která je schopná provádět popisované funkce.

Pro podání určitých příkladů takových zařízení lze uvést, že inteligentní karta může odpovídat kartovému zařízení zkonstruovanému v souladu se známými mezinárodními standardy ISO 7816-1, 7816-2 a 7816-3, zatímco modul podmíněného přístupu může být realizován jako PCMCIA nebo PC

karta odpovídající standardům navrženým skupinu PCMCIA. Další fyzické tvary a podoby jsou ale samozřejmě možné.

Termíny "kódovaný" a "šifrovaný" a "řídící slovo" a "klíč" mohou být použity v různých částech textu zcela zaměnitelně pro účely jasnějšího popisu. Mělo by být ale zcela zřejmé, že neexistuje zásadní rozdíl mezi "šifrovanými daty" a "kódovanými daty" nebo mezi "řídícím slovem" a "klíčem".

Podobně pokud obligatorně z hlediska kontextu není uvedeno nebo specifikováno jinak, není kladeno žádné omezení na kterýkoliv ze symetrický algoritmů nebo algoritmů veřejného a privátního klíče pro daný proces kódování a/nebo dekódování. Stejným způsobem, ačkoliv odpovídající klíče, použité při kódování a dekódování informací, mohou být označovány stejném jménem (například "transportní klíč", "relační klíč"), mělo by být zcela zřejmé, že to číselně nemusí být shodné klíče, pokud splňují příslušné funkce. Například odpovídající veřejné a privátní klíče, použité pro kódování a dekódování dat, budou obvykle mít číselně odlišné hodnoty.

Termín "přijímač/dekodér" nebo "dekodér" používaný v tomto popisu může zahrnovat přijímač pro přijímání buď kódovaných nebo nekódovaných signálů, například televizních a/nebo rádiových signálů, které mohou být přenášeny nebo vysílány nějakým dalším vhodným prostředkem. Provedení takovýchto dekodérů mohou rovněž zahrnovat dekodér integrální s přijímačem pro dekódování přijímaných signálů, například, v "nastavovací řídící skříni (STB)", nebo takový dekodér, který funguje v kombinaci s fyzicky samostatným přijímačem, nebo takový dekodér, který zahrnuje přídavné funkce, jako je

webový prohlížeč, a je integrovaný s dalšími zařízeními, jako je videorekordér nebo televize.

Zde použitý termín "digitální vysílací systém" zahrnuje jakýkoliv vysílací systém pro vysílání nebo přenos, například, primárně audiovizuálních nebo multimediálních digitálních dat. Ačkoliv je předkládaný vynález zejména využitelný pro přenosový (vzduchem) digitální televizní systém, může být tento vynález rovněž použitelný pro pevnou telekomunikační síť pro multimediální internetovské aplikace, pro uzavřený televizní okruh a podobně.

Zde použitý termín "digitální televizní systém" zahrnuje, například, jakékoliv satelitní, pozemní, kabelové a další systémy.

V následujícím popisu bude čistě prostřednictvím příkladů podrobněji popsáno množství provedení předkládaného vynálezu ve spojení s odkazy na připojené výkresy.

Přehled obrázků na výkresech

Obr.1 znázorňuje prostřednictvím přehledu celkovou architekturu digitálního televizního systému;

Obr.2 znázorňuje architekturu systému podmíněného přístupu podle obr. 1;

Obr.3 ilustruje způsob kódování dat mezi inteligentní kartou a dekodérem podle provedení předkládaného vynálezu;

Obr.4 ilustruje generování relačního klíče v dekodéru pracujícím podle provedení ilustrovaného na obr. 3;

Obr.5 ilustruje kroky při přípravě relačního klíče v inteligentní kartě propojení s dekodérem podle obr. 4.

Příklady provedení vynálezu

Předkládaný vynález popisuje způsob kódování dat, zejména, ale ne výhradně, použitelný pro kódování dat na propojovacím rozhraní mezi přenosným bezpečnostním modulem a dekodérem v digitálním televizním systému. Prostřednictvím přehledu bude nyní popsána architektura známého digitálního televizního systému.

Digitální televizní systém

Přehled digitálního televizního systému 1 je znázorněn na obr. 1, přičemž tento systém zahrnuje přenosový systém 2, který využívá MPEG-2 kompresní systém pro vysílání komprimovaných digitálních signálů. Přesněji MPEG-2 komprimátor 3 ve vysílacím centru přijímá tok digitálního signálu (obvykle tok audio nebo video signálů). Komprimátor 3 je spojen s multiplexorem a kodérem 4 prostřednictvím spojení 5. Multiplexor 4 přijímá množství dalších vstupních signálů, sestavuje jeden nebo více transportních toků a vysílá komprimované digitální signály do vysílače 6 vysílacího centra přes spojení 7, které samozřejmě může být představováno velkým množstvím různých forem včetně telekomunikačních linek.

Vysílač 6 vysílá elektromagnetické signály přes vzestupné spojení 8 směrem k satelitnímu odpovídači 9, kde jsou tyto signály elektronicky zpracovány a vysílány přes teoretické sestupné spojení 10 do pozemního přijímače 11,

běžně ve formě parabolické antény vlastněné nebo pronajímané koncovým uživatelem. Signály přijímané přijímačem 11 jsou vysílány do integrovaného přijímače/dekodéru 12 vlastněného nebo pronajímaného koncovým uživatelem a spojeného s televizním zařízením 13 koncového uživatele. Přijímač/dekodér 12 dekóduje komprimovaný MPEG-2 signál na televizní signál pro televizní zařízení 13.

Systém 20 podmíněného přístupu je spojen s multiplexorem 4 a přijímačem/dekodérem 12 a je umístěn částečně ve vysílacím centru a částečně v dekodéru. Tento systém umožňuje koncovému uživateli přístup k digitálním televizním vysíláním (přenosům) od jednoho nebo více dodavatelů (poskytovatelů) vysílání. Přenosný bezpečnostní modul v podobě inteligentní karty, schopné dekódování zpráv týkajících se přenášených programů nebo dat, může být vložena do přijímače/dekodéru 12.

S multiplexorem 4 a přijímačem/dekodérem 12 je rovněž spojen interaktivní systém 17, který je opět umístěn částečně ve vysílacím centru a částečně v dekodéru a který umožňuje koncovému uživateli interagovat s různými aplikacemi přes modemový zpětný kanál 16.

Nyní bude podrobněji popsán systém 20 podmíněného přístupu. Jak je znázorněno na obr. 2, systém 20 podmíněného přístupu v přehledu zahrnuje účastnický autorizační systém (SAS) 21. SAS 21 je spojen s jedním nebo s více účastnickými řídícími systémy (SMS) 22, přičemž jeden SMS 22 je pro každého poskytovatele vysílání, například prostřednictvím příslušného TCP-IP spojení 23 (ačkoliv jiné typy spojení by alternativně také mohly být použity). Alternativně by jeden SMS 22 mohl být sdílen mezi dvěma poskytovateli vysílání,

nebo by jeden poskytovatel vysílání mohl používat dva SMS 22 a podobně.

První kódovací jednotky ve formě šifrovacích jednotek 24, využívajících "mateřské" inteligentní karty 25, jsou spojené se SAS 21 spojením 26. Druhé kódovací jednotky opět ve formě šifrovacích jednotek 27, využívajících mateřské inteligentní karty 28, jsou spojené s multiplexorem 4 spojením 29. Přijímač/dekodér 12 přijímá přenosný bezpečnostní modul, například ve formě "dceřinné" inteligentní karty 30. Přijímač/dekodér 12 je spojen přímo se SAS 21 prostřednictvím komunikačních obslužných kanálů (serverů) 31 přes modemový zpětný kanál 16. SAS 21 vysílá, kromě jiných informací, přihlašovací práva do dceřiné inteligentní karty 30 podle požadavků.

Inteligentní karty obsahují tajné informace jednoho nebo více komerčních operátorů. "Mateřská" inteligentní karta kóduje různé typy zpráv a "dceřiné" inteligentní karty dekódují tyto zprávy, pokud k tomu mají oprávnění.

První a druhé šifrovací jednotky 24 a 27 zahrnují rám, elektronickou VME kartu se softwarem uloženým na EEPROM, až 20 elektronických karet a jednu inteligentní kartu 25 respektive 28 na každou elektronickou kartu, jednu (karta 28) pro kódování zpráv ECM a jednu (karta 25) pro kódování zpráv EMM.

Činnost systému 20 podmíněného přístupu v digitálním televizním systému bude nyní podrobněji popsána ve vztahu k různým komponentům přenosového systému 2 a systému 20 podmíněného přístupu.

Multiplexor a kodér

Jak je patrné ze znázornění na obr. 1 a obr. 2, je ve vysílacím centru digitální audio nebo video signál nejprve komprimován (nebo je mu snížena bitová rychlost) s použitím MPEG-2 komprimátoru 3. Tento komprimovaný signál je potom vysílán do multiplexoru a kodéru 4 přes spojení 5, aby byl multiplexován s dalšími daty, jako jsou další komprimovaná data.

Kodér vytváří řídicí slovo použité v kódovacím procesu a obsažené v toku MPEG-2 v multiplexoru. Řídicí slovo je vytvářeno vnitřně a umožňuje integrovanému přijímači/dekodéru 12 koncového uživatele dekódovat program.

Přístupová kritéria, která indikují způsob komercionalizace programu, jsou rovněž přidávána do toku MPEG-2. Program může být komercionalizován kterýmkoliv jedním z množství "předplatitelských" módů a/nebo jedním z množství módů nebo událostí "placených za shlédnutí" (PPV). V předplaceném módu koncový uživatel předplácí (účastní se) jednu nebo více komerčních nabídek, nebo "souborů", což mu poskytuje práva sledovat každý kanál uvnitř těchto souborů. Ve výhodném provedení může být ze souboru kanálů zvoleno až 960 komerčních nabídek.

V módu platby za shlédnutí je koncový uživatel vybaven možností kupovat události podle přání. To může být dosaženo buď předobjednáním události předem ("objednávkový mód"), nebo nákupem události, jakmile je vysílána ("impulzní mód"). Ve výhodném provedení jsou všichni uživatelé předplatitelé, ať již sledují nebo ne v předplatitelském nebo

PPV módu, samozřejmě že ale PPV diváci nemusejí být nezbytně předplatiteli.

Opravňovací řídící zprávy ECM

Jak řídící slovo tak i přístupová kritéria jsou použita pro sestavení opravňovací řídící zprávy (ECM). Tato zpráva je vysílaná ve spojení s kódovaným programem; přičemž tato zpráva obsahuje řídící slovo (které umožňuje dekódování programu) a přístupová kritéria vysílaného programu. Přístupová kritéria a řídící slovo jsou vysílány do druhé šifrovací jednotky 27 přes spojení 29. V této jednotce je zpráva ECM vytvářena, kódována a vysílána na multiplexor a kodér 4. Během přenosového vysílání se řídící slovo obvykle mění každých několik sekund a tak jsou zprávy ECM rovněž periodicky vysílány pro umožnění dekódování měnícího se řídícího slova. Pro účely redundance každá zpráva ECM obvykle obsahuje dvě řídící slova, současné řídící slovo a následující řídící slovo.

Každá služba přenášená poskytovatelem vysílání v datovém toku zahrnuje množství oddělených komponentů; například televizní program obsahuje video komponent, audio komponent, titulkovací komponent a podobně. Každý z těchto komponentů služby je individuálně kódován a šifrován pro následující přenos do odpovídače 9. Ve spojení s každým kódovaným komponentem služby je vyžadována samostatná zpráva ECM. Alternativně jedna zpráva ECM může být vyžadována pro všechny z kódovaných komponentů služby. Více zpráv ECM může být rovněž generováno v případě, kdy více systémů podmíněného přístupu řídí přístup do stejného vysílaného programu.

Opravňovací ovládací zprávy EMM

EMM je zpráva přidělená pouze jednotlivému koncovému uživateli (účastníkovi), nebo skupině koncových účastníků, (na rozdíl od zprávy ECM, která je přidělena pouze jednomu kódovanému programu nebo sadě kódovaných programů, pokud jsou součástí stejné komerční nabídky). Každá skupina může obsahovat daný počet koncových uživatelů. Tato organizace do skupin má za cíl optimalizovat využití šířky pásma; to znamená, že přístup k jedné skupině může umožnit dosažení většího počtu koncových uživatelů.

Různé specifické typy zprávy EMM mohou být používány. Jednotlivé zprávy EMM jsou přiděleny jednotlivým účastníkům a jsou obvykle používány při zajišťování služeb placených za shlédnutí; přičemž tyto zprávy obsahující identifikátor skupiny a pozici účastníka v této skupině.

Skupinové účastnické zprávy EMM jsou přiděleny skupinám, řekněme o 256 jednotlivých účastnících, a jsou obvykle použity při spravování určitých účastnických služeb. Tato zpráva EMM má identifikátor skupiny a bitovou mapu skupiny účastníků.

Publikové zprávy EMM jsou přiděleny celým publikům a mohly by například být použity určitým operátorem pro zajištění určitých volných služeb. "Publikum" je celek účastníků majících inteligentní karty, které nesou identifikátor stejného systému podmíněného přístupu (CA ID). Nakonec "unikátní" zpráva EMM je určena pro unikátní identifikátor inteligentní karty.

Zprávy EMM mohou být generovány různými operátory pro řízení přístupu k právům sdruženým s programy vysílanými

operátory, jak bylo uvedeno výše. Zprávy EMM mohou být rovněž generovány řídícím programem systému podmíněného přístupu pro konfiguraci aspektů systému podmíněného přístupu obecně.

Termín zpráva EMM je rovněž často používán pro popis typu zpráv se specifickým uspořádáním, které jsou komunikovány mezi dekodérem a dalšími prvky systému a, například, bude dále použit v této přihlášce vynálezu pro označení specifické zprávy předávané z dekodéru do inteligentní karty.

Účastnický řídící systém (SMS)

Účastnický řídící systém (SMS) 22 zahrnuje databázi 32, která spravuje, kromě jiného, všechny soubory koncových uživatelů, komerční nabídky (jako jsou tarify a reklamy), předplacení, detaily PPV, a data týkající se spotřeby koncových uživatelů a autorizace. SMS 22 může být fyzicky vzdálený od SAS 21.

Každý SMS 22 vysílá zprávy do SAS 21 přes odpovídající spojení 23, které zahrnují modifikace nebo vytváření opravňovacích řídících (ovládacích) zpráv (EMM), určených k vysílání ke koncovým uživatelům.

SMS 22 rovněž vysílá zprávy do SAS 21, které nezahrnují jakékoliv modifikace nebo vytváření zpráv EMM, ale zahrnují pouze změnu stavu koncového uživatele (týkající se autorizace přidělené koncovému uživateli při objednávání produktů nebo hodnoty, jaká bude koncovému uživateli účtována).

SAS 21 vysílá zprávy (obvykle vyžadující informace, jako jsou zpětné informace nebo účtovací informace) do SMS

22, takže by mělo být zcela zřejmé, že komunikace mezi těmito systémy je dvoucestná.

Účastnický autorizační systém (SAS)

Zprávy vytvářené SMS 22 jsou předávány přes spojení 23 do účastnického autorizačního systému (SAS) 21, který dále vytváří zprávy potvrzující příjem zpráv vytvořených SMS 22 a předává tato potvrzení do SMS 22.

V přehledu SAS zahrnuje oblast předplatitelského řetězce pro poskytování práv pro předplacený mód a pro obnovování práv automaticky každý měsíc, oblast řetězce plateb za shlédnutí pro poskytování práv pro PPV události, a zaváděč zpráv EMM pro předávání zpráv EMM, vytvářených oblastmi předplatitelského řetězce a řetězce PPV, do multiplexoru a kodéru 4 a tudíž pro plnění toku MPEG zprávami EMM. Pokud mají být udělena další práva, jako jsou práva při platbách za soubor (PPF) v případě stahování počítačového softwaru do osobního počítače uživatele, jsou rovněž vytvořeny další podobné oblasti.

Jednou funkcí SAS 21 je spravovat přístupová práva k televizním programům, dostupným jako komerční nabídky v předplatitelském módu nebo prodávaným jako PPV události podle různých módů komercionalizace (například objednávkový mód, impulzní mód). SAS 21 podle těchto práv a podle informace, přijaté ze SMS 22, vytváří zprávy EMM pro účastníka.

Zprávy EMM jsou předávány do šifrovací jednotky (CU) 24 pro šifrování vzhledem k řízení a exploatačním klíčům. CU dokončuje podpis na zprávě EMM a předává zprávu EMM zpět do generátoru zpráv (MG) v SAS 21, kde je přidáno záhlaví.

Zprávy EMM jsou předávány do vysílače zpráv (ME) jako úplné zprávy EMM. Generátor zpráv určuje čas začátku a konce vysílání a rychlost vysílání zpráv EMM a předává tyto parametry jako vhodné směrnice společně se zprávami EMM do vysílače zpráv. MG vytváří danou EMM pouze jednou, to znamená, že je to ME, který provádí cyklické vysílání zpráv EMM.

Při vytváření zprávy EMM generátor MG přiřazuje zprávě EMM unikátní identifikátor ID. Když MG předává zprávu EMM do ME, předává rovněž tento ID zprávy EMM. To umožňuje identifikaci určité zprávy EMM jak v generátoru MG tak i ve vysílači ME.

Vysílání programů

Multiplexor 4 přijímá elektrické signály zahrnující kódované zprávy EMM ze SAS 21, kódované zprávy ECM z druhé šifrovací jednotky 27 a komprimované programy z komprimátoru 3. Multiplexor 4 kóduje programy a vysílá kódované programy, kódované zprávy EMM a kódované zprávy ECM do vysílače 6 vysílacího centra přes spojení 7. Vysílač 6 vysílá elektromagnetické signály směrem k satelitnímu odpovídači 9 přes vzestupné spojení 8.

Přijímání programů

Satelitní odpovídač 9 přijímá a zpracovává elektromagnetické signály vysílané vysílačem 6 a vysílá tyto signály k pozemnímu přijímači 11, obvykle ve formě parabolické antény vlastněné nebo pronajaté koncovým uživatelem, přes sestupné spojení 10. Signály přijímané

pozemním přijímačem 11 jsou vysílány do integrovaného přijímače/dekodéru 12 vlastněného nebo pronajatého koncovým uživatelem a spojeného s televizním zařízením 13 koncového uživatele. Přijímač/dekodér 12 demultiplexuje signály, aby získal kódované programy s šifrovanými zprávami EMM a s šifrovanými zprávami ECM.

Pokud program není kódován, to znamená, že žádná zpráva ECM nebyla vysílána s MPEG-2 tokem, přijímač/dekodér 12 dekomprimuje data a mění signál na video signál pro vysílání do televizního zařízení 13.

Pokud program je kódován, přijímač/dekodér 12 vybírá odpovídající zprávu ECM z toku MPEG-2 a předává tuto zprávu ECM "dceřiné" inteligentní kartě 30 koncového uživatele. Ta je zasunuta do štěrbiny (slotu) v pouzdru přijímače/dekodéru 12. Dceřiná inteligentní karta 30 řídí, zda koncový uživatel má právo dekódovat zprávu ECM a právo přístupu k programu. Pokud koncový uživatel má příslušná práva, je zpráva ECM dekódována uvnitř inteligentní karty a je vyjmuto řídící slovo.

Potom inteligentní karta komunikuje řídící slovo do dekodéru 12, který pak dekóduje program s použitím tohoto řídícího slova. V nejběžnějších systémech je řídící slovo komunikováno přes propojovací rozhraní inteligentní karty v čisté nebo nekódované formě, což vede na problémy se zabezpečením, jak bylo popisováno v úvodu předkládané přihlášky vynálezu. Po dekódování dekodérem je MPEG-2 tok dekomprimován a převeden na video signál pro následné vysílání do televizního zařízení 13.

Ve výše popsaném systému se dekódování MPEG dat provádí uvnitř dekodéru s použitím informací řídícího slova, komunikovaných do dekodéru z inteligentní karty. V jiných systémech mohou být dekódovací obvody realizovány v odnímatelném modulu podmíněného přístupu nebo CAM, běžně provedeném ve formě PCMCIA nebo PC karty zasunutelné do zdířky v dekodéru.

CAM modul může sám dále obsahovat štěrbinu (slot) pro přijetí inteligentní karty. V takových systémech se data řídícího slova dekódují v inteligentní kartě a komunikují do CAM modulu, který potom dekóduje kódovaný MPEG datový tok pro dodání do dekodéru čistého MPEG toku pro dekomprimování a následné zobrazení.

V tomto typu systému mohou být citlivá data předávána mezi inteligentní kartou a CAM (data řídícího slova) a/nebo CAM a dekodérem (dekódovaná MPEG data) a problémy se zabezpečením mohou vznikat v kterémkoliv z těchto propojovacích rozhraní.

Kódování data na propojovacím rozhraní

Ve spojení s odkazy na obr. 3 bude nyní popsán způsob kódování dat při aplikaci na data řídícího slova, komunikovaná mezi inteligentní kartou a dekodérem v jednom z nejjednodušších provedení předkládaného vynálezu. Stejné principy ale mohou být aplikovány na kódování dat řídícího slova mezi inteligentní kartou a CAM, audiovizuálních MPEG dat mezi CAM a dekodérem, nebo dokonce jakýkoliv typ dat mezi dvěma takovými zařízeními.

Podle předkládaného vynálezu je skupina dvojic klíčů uložena v energeticky nezávislé (trvalé) paměti dekodéru, jako je například FLASH paměť. Každá dvojice klíčů odpovídá hodnotě klíče v čisté podobě a kódované verzi klíče. Jak bude popsáno, kódovaná verze klíče bude eventuálně komunikována v EMM zprávě vysílané do inteligentní karty zasunuté do dekodéru.

Uvnitř dekodéru je tudíž uložena sada dvojic EMM zpráv a klíčů, a to následovně:

n	EMM (19 oktetů)	Klíč (8 oktetů)
1	EMM(1)	Klíč(1)
2	EMM(2)	Klíč(2)
3	EMM(3)	Klíč(3)
.	...	...
.	...	...
.	...	...
16	EMM(16)	Klíč(16)

Kódovaná hodnota klíče, uložená v EMM, je vypočítána vně dekodéru s použitím kódovacího algoritmu, který není přítomen v dekodéru. V předkládaném příkladu hodnoty klíčů Klíč(1), Klíč(2), a tak dále, odpovídají symetrickým klíčům pro použití se symetrickým kódovacím algoritmem, jako je DES.

Kódovací algoritmus, použitý pro přípravu DES kódovaných hodnot klíčů, obsažených s uloženými EMM zprávami, může rovněž odpovídat symetrickému kódovacímu algoritmu. Pro

zvýšené zabezpečení bude pro přípravu kódovaných hodnot použit autorizovaný symetrický algoritmus (PSA), odlišný od DES, ačkoliv v jiném provedení může být DES rovněž použit pro kódování hodnot klíčů.

Vedle kódované hodnoty přidruženého klíče může zpráva EMM rovněž obsahovat hodnotu podpisu, sdruženou se zprávou a připravenou prostřednictvím jakéhokoliv běžného postupu pro vytvoření podpisu. Například může být zpráva podrobena přepočítací funkci, jako je MD5, následované kódováním přepočítací hodnotou prostřednictvím privátního klíče algoritmu privátního a veřejného klíče, jako je RSA. Ověření podpisu se potom může provádět v okamžiku přijetí s použitím algoritmu MD5 a odpovídajícího veřejného klíče dvojice privátního a veřejného klíče.

Zpráva EMM bude navíc obsahovat standardní prvek záhlaví inteligentní karty (jak je definován mezinárodním standardem ISO 7816-3) pro uvedení zprávy do formátu potřebného pro umožnění jejího čtení prostřednictvím inteligentní karty. Zpráva EMM, sdružená s 8 bytovým klíčem, tudíž bude obvykle mít následující strukturu:

Záhlaví	5 bytů
Kódovaný klíč	10 bytů
Podpis	9 bytů

V prezentovaném provedení je do paměti dekodéru zadána skupina 16 dvojic klíčů a zpráv. Alternativní provedení jsou samozřejmě rovněž možná a využívají více či méně dvojic klíčů a zpráv, přičemž předkládaný vynález může

být dokonce realizován s použitím pouze jedné dvojice klíče a zprávy. Ačkoliv může být předpokládáno takové provedení, že všechny dekodéry jsou vybaveny stejnými dvojicemi klíčů a zpráv, je z bezpečnostních důvodů výhodné, aby každý měl unikátní skupinu dvojic klíčů a zpráv. Při realizaci tohoto provedení vynálezu může operátor dodat výrobci dekodéru skupinu deseti tisíc nebo více dvojic klíčů a zpráv, přičemž výrobce dekodéru provede náhodný výběr 16 dvojic během individualizace každého dekodéru.

Za účelem zvýšení zabezpečení bude během každé relace použita odlišná podskupina z dvojic zpráv a klíčů, uložených v dekodéru. Relace může být definována například tak, že odpovídá každému zapnutí a vypnutí dekodéru, nebo každé změně kanálu na dekodéru.

Jak je patrné na obr. 3, generátor 40 náhodných čísel uvnitř dekodéru volí 8 z 16 dvojic zpráv a klíčů pro použití v dané relaci. 8 zvolených EMM zpráv 41 z dvojic je potom komunikováno do inteligentní karty 30, aby byly ověřeny, dekódovány a zpracovány, jak je znázorněno krokem 42 dekódování 42 a krokem 43 zpracování zprávy či vytvoření klíče, pro získání vhodného relačního klíče (viz níže). Stejná operace generování klíče se provede uvnitř dekodéru v kroku 43 vytvoření klíče s použitím odpovídajících hodnot klíčů z dvojic tak, aby se získala stejná hodnota relačního klíče.

Generování relačního klíče uvnitř dekodéru bude nyní podrobněji popsáno ve spojení s odkazy na obr. 4.

Základní hodnota 44 relačního klíče KeyS Initial je konstantně pro všechny dekodéry kódována v kroku 45 kódování

prostřednictvím prvního klíče 46 z podskupiny zvolené generátorem 40 náhodných čísel. Výsledná hodnota je potom kódována v kroku 47 kódování s použitím druhého klíče 48 z relační podskupiny a tato činnost se opakuje až do provedení poslední operace kódování v kroku 49 kódování s posledním klíčem 50 z podskupiny tak, aby se získala finální hodnota 51 relačního klíče.

Počáteční hodnota relačního klíče KeyS Initial může být univerzální hodnotou, přítomnou ve všech dekodérech a inteligentních kartách, hodnotou, spojenou se specifickou dvojicí dekodéru a inteligentní karty, nebo dokonce hodnotou, generovanou na začátku každé relace v dekodéru a potom komunikovanou do inteligentní karty.

Ve výše uvedeném příkladu se relační klíč připraví prostřednictvím sekvence opakovaných operací na hodnotě KeyS Initial s použitím DES algoritmu s zvolených klíčů 46, 48, 50, a tak dále. V případě DES algoritmu je důležité pořadí, ve kterém jsou klíče použity, a musí být respektováno pro vytvoření pokaždé stejného klíče.

Zatímco ale relační klíč S je sám numerickou (číselnou) hodnotou, která bude použita jako DES klíč v následné kódovací operaci (viz níže), kroky použité pro generování této hodnoty klíče nemusí odpovídat krokům DES kódování. Namísto toho může být podskupina klíčů, zvolených generátorem náhodných čísel, kombinována dohromady jakýmkoliv množstvím způsobů pro vytvoření vhodné hodnoty relačního klíče KeyS Final. Například mohou být klíče kombinovány s použitím sekvence jednoduchých aritmetických operací. V závislosti na zvoleném postupu nemusí být nezbytné, aby

pořadí kroků při přípravě hodnoty KeyS bylo respektováno v pořadí pro opětovné generování stejného klíče.

Nyní budou ve spojení s odkazy na obr. 5 popsány operace 42 a 43 dekódování a zpracování, prováděné v inteligentní kartě 30 pro generování relačního klíče používaného inteligentní kartou.

Po vložení inteligentní karty do dekodéru je do této inteligentní karty vyslána podskupina EMM zpráv odpovídající zvoleným hodnotám klíčů. Nejprve se provede ověření každé EMM zprávy ve spojení s připojenou hodnotou podpisu a s použitím například procesu typu MD5/RSA, jak bylo popisováno výše. Pro jednoduchost byl tento krok z obr. 5 vypuštěn.

První EMM zpráva 60 je potom dekódována v kroku 61 dekódování s použitím transportního klíče 59 zaneseného bezpečným a neodečitatelným způsobem uvnitř inteligentní karty. Jak bylo zmiňováno výše, z bezpečnostních důvodů může algoritmus, použitý při dekódování v kroku 61 dekódování EMM zprávy, odpovídat autorizovanému bezpečnému algoritmu PSA, známému pouze operátorovi odpovědnému za přípravu dvojic zpráv a klíčů, použitých v dekodéru, a za individualizaci inteligentní karty.

Transportní klíč 59 KeyT může být hodnotou klíče, společnou pro všechny inteligentní karty v systému nebo unikátní pro jednu takovou kartu. Použití unikátní hodnoty klíče KeyT vyžaduje, aby tabulka zpráv a klíčů, uložená v dekodéru, byla připravena se stejným klíčem jako v inteligentní kartě, takže dekodér a inteligentní karta budou nevratně spolu spojeny. V praxi takové provedení ale nemusí být žádoucí.

Podobná dekódovací operace s použitím transportního klíče 59 se potom provede v kroku 62 dekódování na další EMM zprávě 63 v sérii a tak dále, dokud není provedena poslední operace dekódování v posledním kroku 64 dekódování na finální EMM zprávě 65.

V prezentovaném provedení kódování každé z EMM zpráv 60, 63, 65 vytváří klíče 46, 48, 50, shodné s klíči sdruženými v tabulce zpráv a klíčů, přítomné v dekodéru, a použitými pro generování relačního klíče, jak bylo popisováno výše. Z tohoto důvodu byly použity stejné vztahové značky pro tyto klíče a pro operaci 42 vytváření klíče, rovněž prováděnou v dekodéru. Podobně je v inteligentní kartě rovněž uložena stejná základní hodnota 44 relačního klíče.

Úvodní nebo základní hodnota 44 relačního klíče KeyS je potom kódována v kroku 45 kódování prostřednictvím prvního klíče 46, přičemž výsledek je opět kódován v kroku 47 kódování prostřednictvím druhého klíče 48 a tak dále, dokud se neprovede poslední krok 49 kódování s použitím posledního klíče 50 v sérii tak, aby se získala finální hodnota 51 relačního klíče.

Jak dekodér tak i inteligentní karta nyní mají v držení stejný relační klíč KeyS, který potom může být použit při kódování a dekódování dat předávaných v kterémkoliv směru mezi těmito dvěma zařízeními.

Opět ve spojení s odkazy na obr. 3 je patrné, že inteligentní karta 30 přijímá kódovanou ECM zprávu 70, obsahující řídící slovo potřebné pro dekódování přidruženého segmentu MPEG audiovizuálních nebo jiných dat. Inteligentní

karta dekóduje zprávu ECM v kroku 71 dekódování pro získání hodnoty CW řídícího slova.

V předcházejícím popisu bylo poznamenáno, že algoritmus, použitý pro kódování ECM zpráv pro uživatele, může výhodně odpovídat autorizovanému bezpečnému algoritmu, použitému pro dekódování EMM zpráv přijímaných z inteligentní karty, jak bylo popisováno výše.

Dekódované řídící slovo je potom opětovně kódováno v kroku 72 kódování s použitím relačního klíče KeyS a kódovaná hodnota řídícího slova f(CW) je vysílána přes propojovací rozhraní mezi dekodérem a inteligentní kartou, jak je znázorněno. Kódovaná hodnota f(CW) je potom dekódována v kroku 73 dekódování s použitím relačního klíče KeyS, obsaženého v dekodéru, a čistá hodnota CW řídícího slova je získána v kroku 74.

Protože relační klíč je symetrický, může být stejně tak použit při kódování dat vysílaných z dekodéru do inteligentní karty. Navíc data, vysílaná z inteligentní karty do dekodéru, mohou být daty jinými než jednoduchými daty řídícího slova.

Jak bylo zmiňováno výše, stejný princip může být aplikován na všech propojovacích rozhraních v systému zahrnujícím dekodér, do kterého je vložen odpojitelný CAM modul (propojovací rozhraní mezi dekodérem a CAM, propojovací rozhraní mezi CAM a inteligentní kartou, a podobně). Podobně může být také stejný princip aplikován v případě přenosného modulu (buď modul typu CAM nebo inteligentní karta), vloženého do jiných zařízení, jako je televize nebo videorekordér.

Ve skutečnosti shora popsaný způsob nastavení kódovaného komunikačního kanálu může být aplikován na jakoukoliv dvojici zařízení, u kterých je požadována bezpečná datová komunikace. Zejména přitom může být stejný princip aplikován v domácích síťových systémech, kde je množství zařízení spotřebitele (televize, video, PC, dekodér, a podobně) přenáší data, jako jsou audiovizuální data nebo počítačové soubory, přes komunikační linku. Takovou linkou může být RF (rádiová) linka, infračervená linka, přidělená sběrnice, spojení výkonovým kabelem, a podobně. Například může být žádoucí vysílat řídicí slovo v jiných datech v kódované formě mezi dekodérem a televizí nebo mezi nadřízeným dekodérem a podřízeným dekodérem ve stejné domácnosti.

Další příklady systémů tohoto typu, u kterých by bylo žádoucí vytvořit bezpečnou komunikační linku, jsou znalému čtenáři zcela zřejmé.

Zastupuje :

PATENTOVÉ NÁROKY

1. Způsob kódování dat komunikovaných mezi prvním a druhým zařízením, **vyznačující se tím, že** se alespoň jedna předem vypočítaná dvojice klíčů uloží v paměti prvního zařízení, přičemž tato alespoň jedna dvojice klíčů zahrnuje relační klíč a kódovanou verzi tohoto relačního klíče, připravenou s použitím transportního klíče, přičemž kódovaná verze relačního klíče se následně komunikuje do druhého zařízení, které dekóduje tuto kódovanou verzi s použitím ekvivalentu transportního klíče, uloženého v jeho paměti, takže data, komunikovaná z alespoň druhého zařízení do prvního zařízení, mohu být potom v příslušných zařízeních kódována a dekódována prostřednictvím relačního klíče.

2. Způsob podle nároku 1, **vyznačující se tím, že** v paměti prvního zařízení se uloží množství dvojic klíčů, přičemž první zařízení vybírá a zpracovává alespoň jeden relační klíč pro generování definitivního relačního klíče a komunikuje přidruženou kódovanou hodnotu uvedeného alespoň jednoho relačního klíče do druhého zařízení pro dekódování a zpracování druhým zařízením pro generování definitivního relačního klíče.

3. Způsob podle nároku 2, **vyznačující se tím, že** se prvním zařízením vybere podskupina z množství uložených relačních klíčů pro generování definitivního relačního klíče, přičemž přidružené kódované verze podskupiny těchto relačních klíčů se komunikují do druhého zařízení pro dekódování a zpracování.

4. Způsob podle nároku 2 nebo 3, **vyznačující se tím, že** z prvního do druhého zařízení se komunikuje pořadí kombinace

množství relačních klíčů použitých pro generování definitivního relačního klíče.

5. Způsob podle nároku 4, **vyznačující se tím, že** úvodní hodnota relačního klíče, známá jak prvnímu tak i druhému zařízení, se opakovaně kóduje v obou zařízeních prostřednictvím seřazené sekvence relačních klíčů s použitím kódovacího algoritmu citlivého na pořadí kódování.

6. Způsob podle kteréhokoliv z předcházejících nároků, **vyznačující se tím, že** uvedená alespoň jedna předem vypočítaná dvojice klíčů se vybere z větší skupiny předem vypočítaných dvojic klíčů před uložením do prvního zařízení.

7. Způsob podle kteréhokoliv z předcházejících nároků, **vyznačující se tím, že** kódovaná verze relačního klíče, komunikovaná do druhého zařízení, rovněž obsahuje hodnotu podpisu, čitelnou druhým zařízením, pro ověření pravosti kódované verze relačního klíče.

8. Způsob podle kteréhokoliv z předcházejících nároků, **vyznačující se tím, že** algoritmus a transportní klíč, použité pro kódování a dekódování relačního klíče, odpovídají symetrickému algoritmu a přidruženému symetrickému klíči.

9. Způsob podle kteréhokoliv z předcházejících nároků, **vyznačující se tím, že** kódovací algoritmus, použitý s relačním klíčem pro kódování a dekódování dat komunikovaných mezi prvním a druhým zařízením, odpovídá symetrickému algoritmu.

10. Způsob podle kteréhokoliv z předcházejících nároků, **vyznačující se tím, že** prvním zařízením je dekodér.

11. Způsob podle kteréhokoliv z předcházejících nároků, **vyznačující se tím, že** druhým zařízením je přenosný bezpečnostní modul.

12. Způsob podle nároku 11, **vyznačující se tím, že** přenosný bezpečnostní modul odpovídá jednomu prvku ze skupiny zahrnující inteligentní kartu a modul podmíněného přístupu.

13. Způsob podle kteréhokoliv z nároků 1 až 9, **vyznačující se tím, že** první zařízení odpovídá modulu podmíněného přístupu a druhé zařízení odpovídá inteligentní kartě.

14. Způsob podle kteréhokoliv z nároků 10 až 13, **vyznačující se tím, že** data, kódovaná a dekódovaná s relačním klíčem, odpovídají datům řídícího slova.

15. Způsob podle kteréhokoliv z nároků 10 až 13, **vyznačující se tím, že** data, kódovaná a dekódovaná s relačním klíčem, odpovídají datům dekódovaného přenosu.

16. Způsob podle kteréhokoliv z nároků 1 až 9, **vyznačující se tím, že** první a druhé zařízení odpovídají prvnímu a druhému dekodéru.

17. Způsob podle kteréhokoliv z nároků 1 až 9, **vyznačující se tím, že** se aplikuje na domácí síťový systém, přičemž první a druhé zařízení odpovídají prvnímu a druhému elektronickému zařízení spotřebitele, upraveným pro přenos dat přes komunikační linku.

18. První zařízení upravené pro použití ve způsobu definovaném podle kteréhokoliv z nároků 1 až 17, **vyznačující se tím, že** zahrnuje paměť, ve které je uložena alespoň jedna předem vypočítaná dvojice klíčů, přičemž tato alespoň jedna

předem vypočítaná dvojice klíčů zahrnuje relační klíč a kódovanou verzi tohoto relačního klíče.

19. První zařízení upravené pro použití ve způsobu definovaném podle kteréhokoliv z nároků 1 až 17 a s prvním zařízením definovaným podle nároku 18, **vyznačující se tím, že** zahrnuje paměť, ve které je uložen klíč a algoritmus, které jsou potřebné pro dekódování kódované verze relačního klíče, uložené v paměti prvního zařízení.

20. První a druhé zařízení podle nároků 18 a 19, **vyznačující se tím, že** první zařízení odpovídá dekodéru a druhé zařízení přenosnému bezpečnostnímu modulu.

21. Systém pro zajištění bezpečné komunikace dat mezi prvním a druhým zařízením, **vyznačující se tím, že** první zařízení zahrnuje paměť pro uložení alespoň jedné předem vypočítané dvojice klíčů, zahrnující relační klíč a kódovanou verzi relačního klíče, připravenou s použitím transportního klíče, a komunikační prostředek pro komunikování kódované verze relačního klíče do uvedeného druhého zařízení, přičemž druhé zařízení zahrnuje paměť pro uložení ekvivalentu transportního klíče, dekódovací prostředek pro dekódování uvedené kódované verze relačního klíče s použitím uvedeného ekvivalentu transportního klíče, a prostředek pro kódování dat, která mají být komunikována do uvedeného prvního zařízení, s použitím relačního klíče.

22. Systém podle nároku 21, **vyznačující se tím, že** paměť prvního zařízení je upravena pro uložení množství dvojic klíčů, přičemž první zařízení zahrnuje prostředek pro výběr a zpracování alespoň jednoho relačního klíče pro generování definitivního relačního klíče a uvedený komunikační

prostředek je upraven pro komunikování přidružené kódované hodnoty uvedeného alespoň jednoho relačního klíče do druhého zařízení, přičemž druhé zařízení zahrnuje prostředek pro zpracování uvedeného alespoň jednoho relačního klíče pro generování definitivního relačního klíče.

23. Systém podle nároku podle nároku 21 nebo 22, **vyznačující se tím, že** kódovaná verze relačního klíče obsahuje hodnotu podpisu, čitelnou druhým zařízením, pro ověření pravosti kódované verze relačního klíče.

24. Systém podle kteréhokoliv z nároků 21 až 23, **vyznačující se tím, že** algoritmus a transportní klíč, použité pro kódování a dekódování relačního klíče, odpovídají symetrickému algoritmu a přidruženému symetrickému klíči.

25. Systém podle kteréhokoliv z nároků 21 až 24, **vyznačující se tím, že** kódovací algoritmus, použitý s relačním klíčem pro kódování a dekódování dat komunikovaných mezi prvním a druhým zařízením, odpovídá symetrickému algoritmu.

26. Systém podle kteréhokoliv z nároků 21 až 25, **vyznačující se tím, že** prvním zařízením je dekodér.

27. Systém podle kteréhokoliv z nároků 21 až 26, **vyznačující se tím, že** druhým zařízením je přenosný bezpečnostní modul.

28. Systém podle nároku 27, **vyznačující se tím, že** přenosný bezpečnostní modul odpovídá jednomu prvku ze skupiny zahrnující inteligentní kartu a modul podmíněného přístupu.

29. Systém podle kteréhokoliv z nároků 21 až 25, **vyznačující se tím, že** první zařízení odpovídá modulu podmíněného přístupu a druhé zařízení odpovídá inteligentní kartě.

30. Systém podle kteréhokoliv z nároků 21 až 25, **vyznačující se tím, že** první a druhé zařízení odpovídají prvnímu a druhému dekodéru.

31. Systém podle kteréhokoliv z nároků 21 až 25, **vyznačující se tím, že** se aplikuje na domácí síťový systém, přičemž první a druhé zařízení odpovídají prvnímu a druhému elektronickému zařízení spotřebitele, upraveným pro přenos dat přes komunikační linku.

32. Způsob kódování dat, komunikovaných mezi prvním a druhým zařízením, v podstatě podle zde uvedeného popisu.

33. Systém pro zajištění bezpečné komunikace dat mezi prvním a druhým zařízením v podstatě podle zde uvedeného popisu.

Zastupuje :

FIG. 1

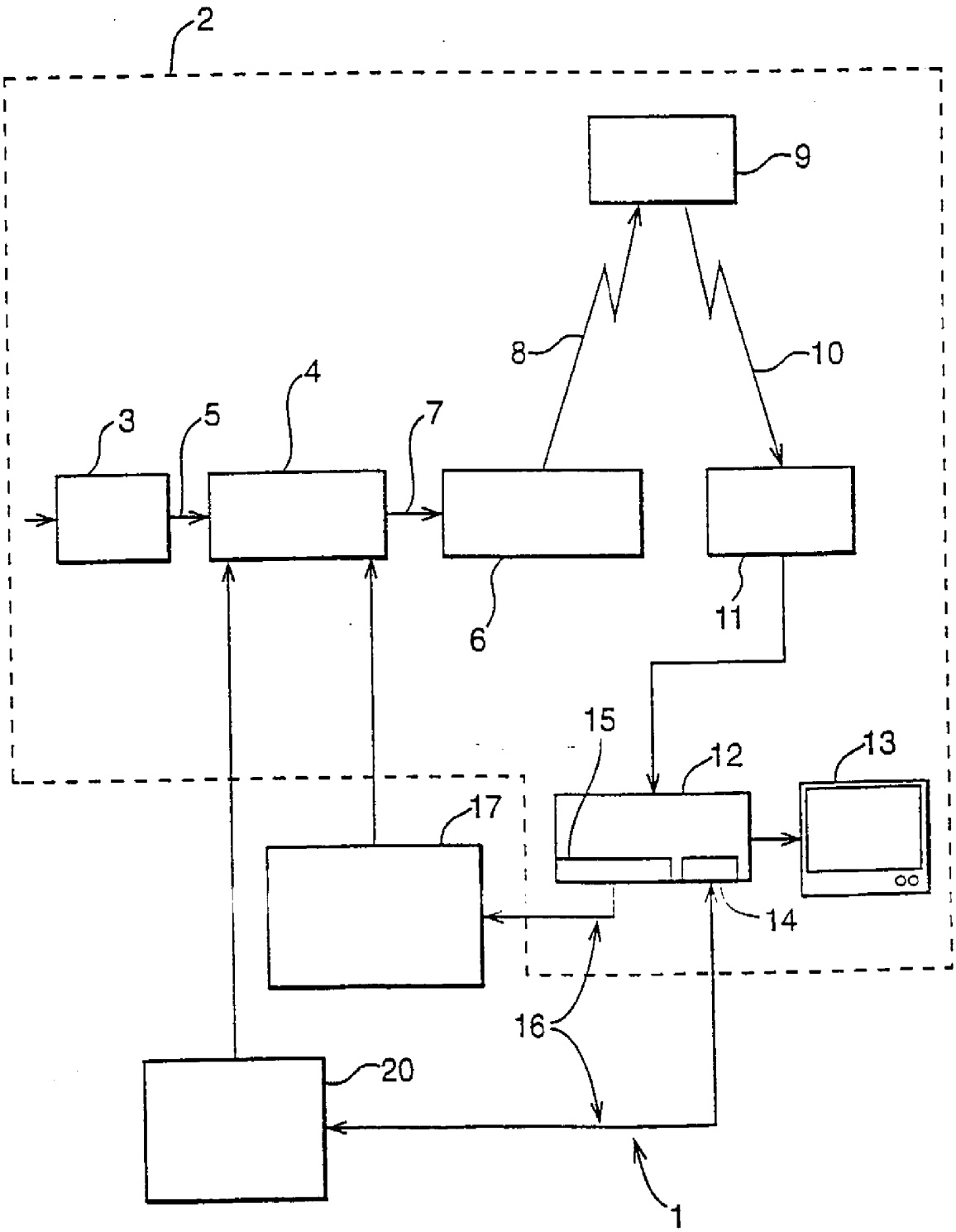


FIG. 2

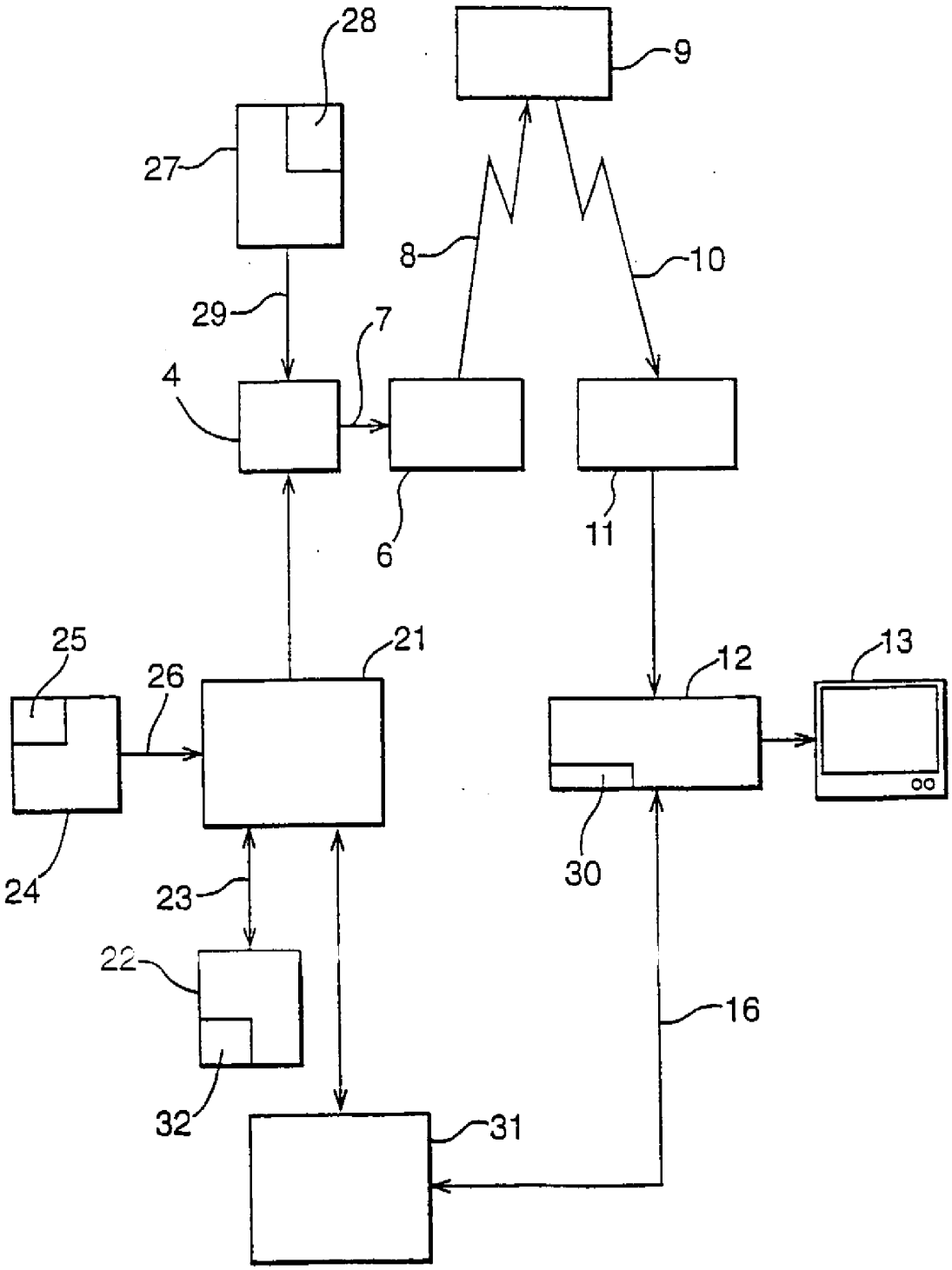
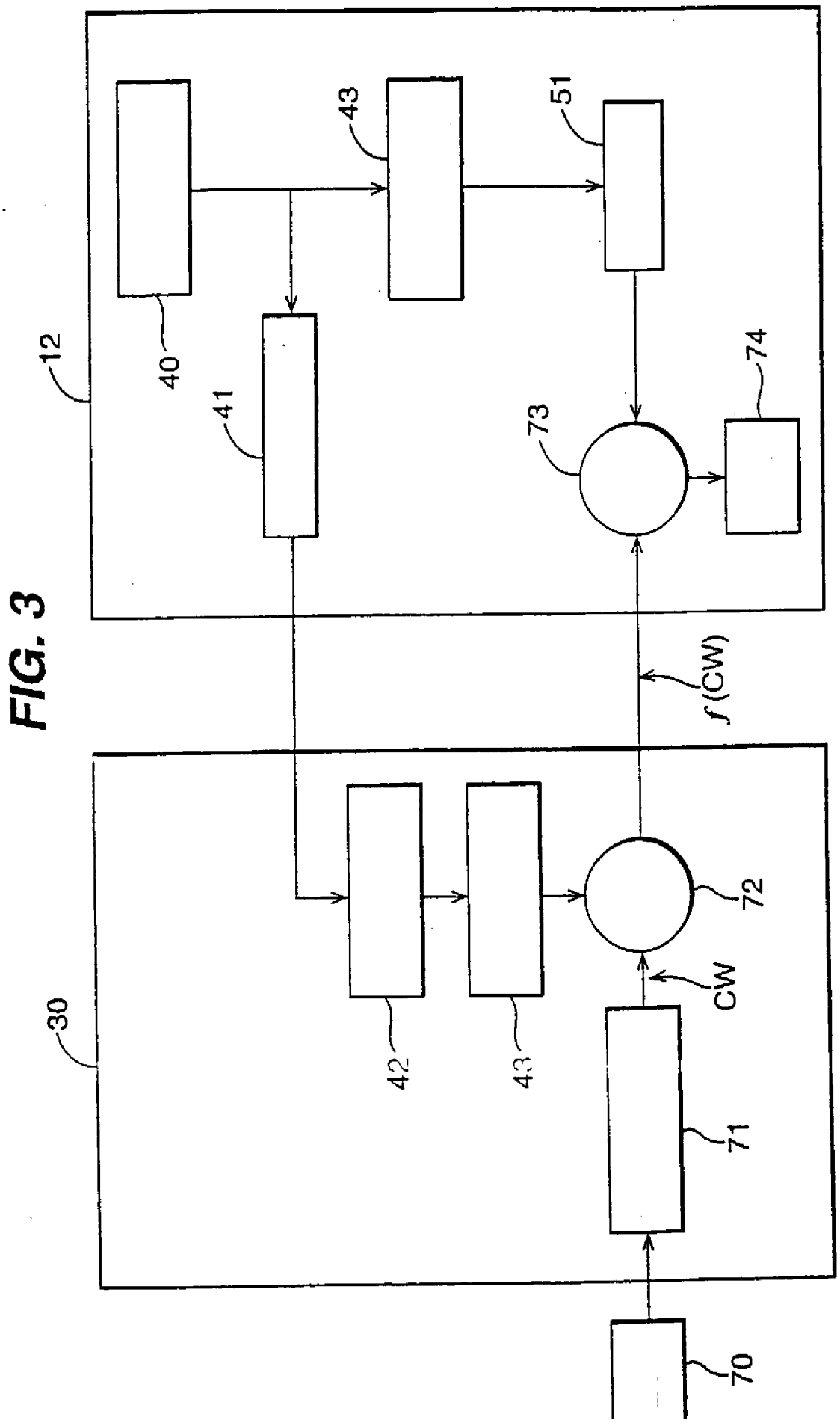


FIG. 3



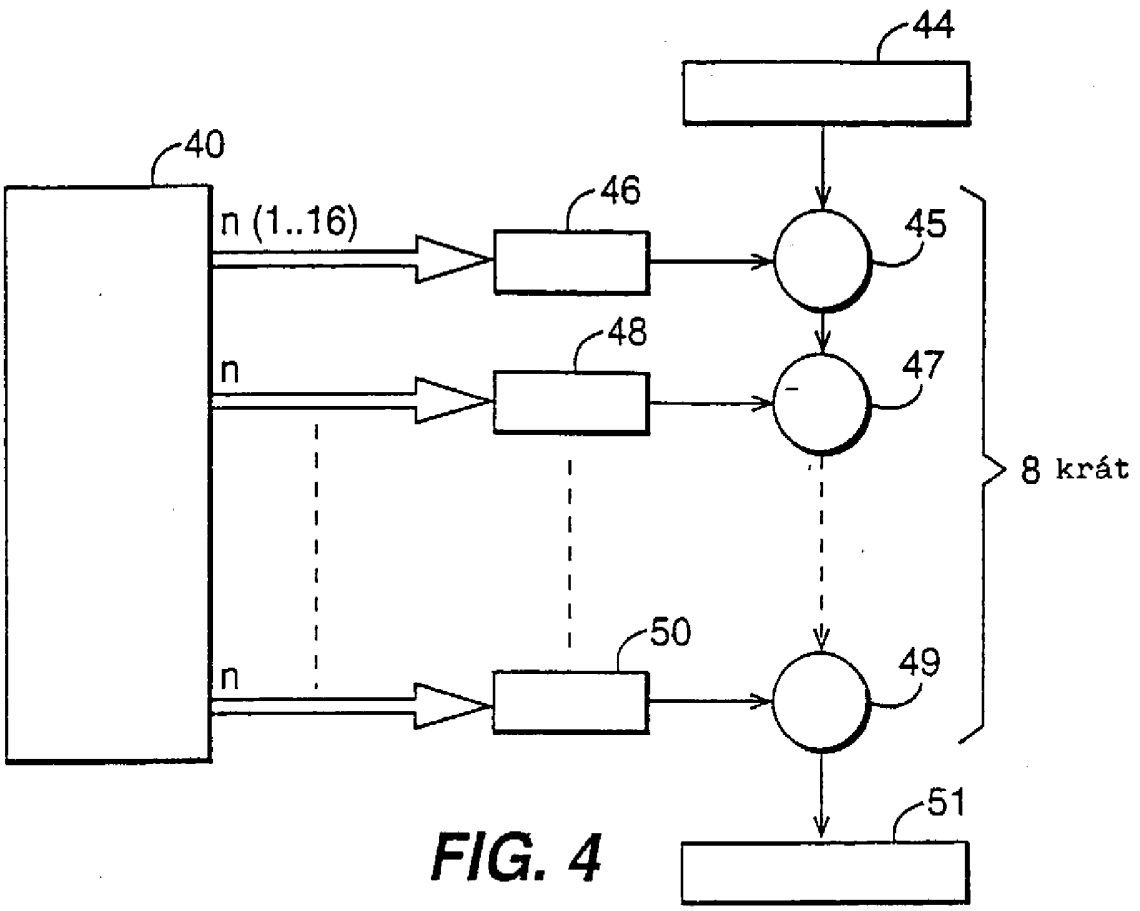

44
40
n (1..16)
46
45
48
n
47
8 krát
50
n
49
51

FIG. 4

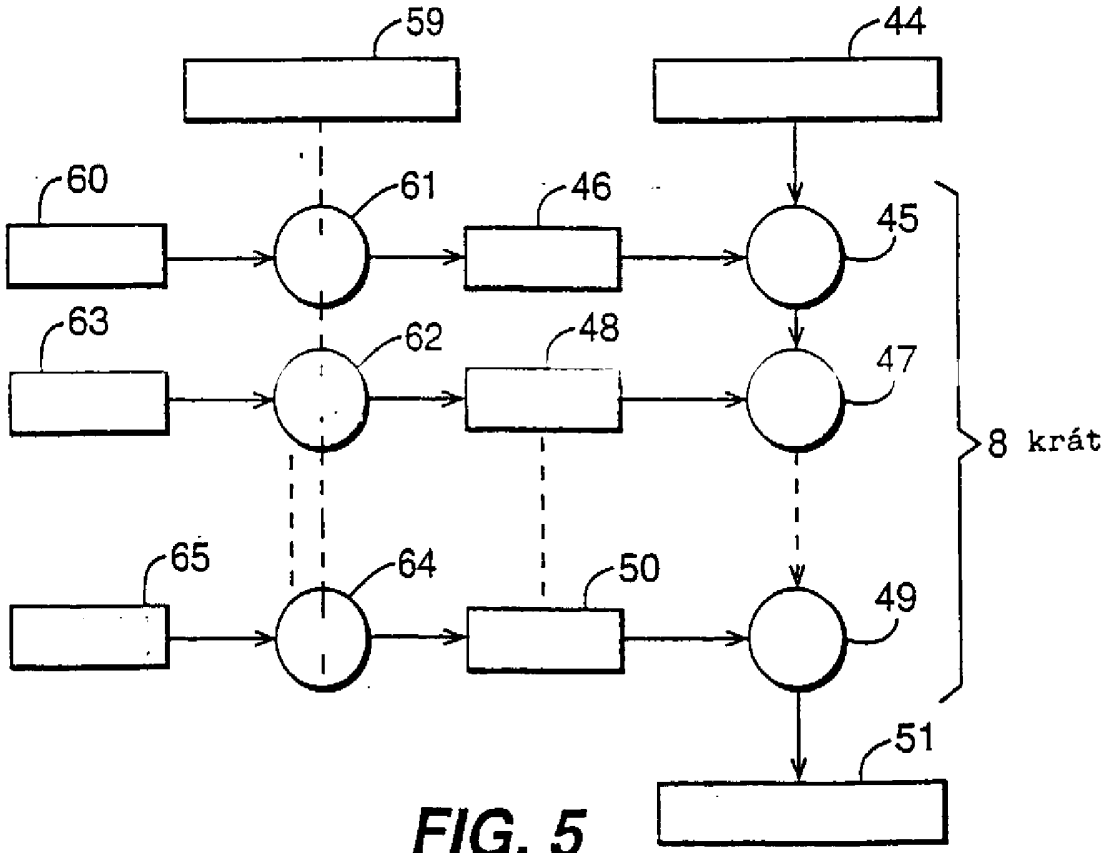

59
44
60
61
46
45
63
62
48
47
8 krát
65
64
50
49
51

FIG. 5