(19) **Bundesrepublik Deutschland**
Deutsches Patent- und Markenamt

(10) **DE 600 11 405 T2** 2005.06.16

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 163 798 B1**
(21) Deutsches Aktenzeichen: **600 11 405.8**
(86) PCT-Aktenzeichen: **PCT/US00/05111**
(96) Europäisches Aktenzeichen: **00 913 651.6**
(87) PCT-Veröffentlichungs-Nr.: **WO 00/59222**
(86) PCT-Anmeldetag: **29.02.2000**
(87) Veröffentlichungstag der PCT-Anmeldung: **05.10.2000**
(97) Erstveröffentlichung durch das EPA: **19.12.2001**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **09.06.2004**
(47) Veröffentlichungstag im Patentblatt: **16.06.2005**

(51) Int Cl.[7]: **H04N 7/16**
H04L 9/08

(30) Unionspriorität:

126805 P	**30.03.1999**	**US**
497393	**03.02.2000**	**US**

(84) Benannte Vertragsstaaten:
AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LI, LU, MC, NL, PT, SE

(73) Patentinhaber:
Sony Electronics Inc., Park Ridge, N.J., US

(72) Erfinder:
CANDELORE, L., Brant, Escondido, US

(74) Vertreter:
Mitscherlich & Partner, Patent- und Rechtsanwälte, 80331 München

(54) Bezeichnung: **VERAHREN UND GERÄT ZUR SICHERUNG VON STEUERUNGSWORTEN**

Beschreibung

HINTERGRUND DER ERFINDUNG

1. Gebiet der Erfindung

[0001] Die vorliegende Erfindung betrifft digitale Einrichtungen. Insbesondere betrifft die vorliegende Erfindung ein Gerät und Verfahren zum Entwürfeln digitalen Inhalts in digitalen Einrichtungen.

2. Genereller Hintergrund

[0002] Analoge Kommunikationssysteme machen schnell ihren digitalen Gegenstücken Platz. Gegenwärtig ist geplant, dass digitales Fernsehen im Jahr 2002 allen Konsumenten national zur Verfügung steht und im Jahr 2006 vollständig im Dienst ist. Hochauflösende Fernsehsendungen bzw. HDTV-Fernsehsendungen (high definition television (HDTV) broadcasts) haben in den meisten Hauptstädten auf begrenzter Basis schon begonnen. Ähnlich hat das explosive Wachstum des Internets und des World Wilde Web in einem korrelativen Wachstum bei der Zunahme herunterladbarer audiovisueller Dateien, beispielsweise MP3-formatierter Audiodateien, sowie anderen Inhalts resultiert.

[0003] Gleichzeitig mit und zum Teil aufgrund dieser schnellen Bewegung zum digitalen Kommunikationensystem hat es signifikante Fortschritte bei digitalen Aufzeichnungseinrichtungen gegeben. DVD-Rekorder (DVD steht für digital versatile disk (mehrseitige Digitalplatte)), digitale VHS-Videokassettenrekorder (digital VHS video cassette recorders (D-VHS VCR)), CD-ROM-Rekorder (beispielsweise CD-R und CD-RW), MP3-Aufzeichnungseinrichtungen und hart- bzw. festplattenbasierte Aufzeichnungseinheiten sind aber nur repräsentativ für die digitalen Aufzeichnungseinrichtungen, die fähig sind, Hochqualitäts- bzw. Qualitätsaufzeichnungen und Kopien davon zu erzeugen, ohne die Generationsverschlechterung (d.h. zunehmende Verschlechterung zwischen sukzessiven Kopien), die bei den analogen Gegenstücken bekannt sind, zu erzeugen. Die Kombination aus einer Bewegung zu digitalen Kommunikationssystemen und digitalen Aufzeichnungseinrichtungen bringen Inhaltanbieter bzw. -provider wie beispielsweise die Film- bzw. Bewegtbild- und Musikindustrie in Sorge, die das unautorisierte und unkontrollierte Kopieren von urheberrechtlich oder anderweitig geschütztem Material zu verhindern wünschen.

[0004] Als Antwort darauf gibt es eine Bewegung, Dienstprovider, beispielsweise terrestrische Rundfunk-, Kabel- und Direkt-Rundstrahlsatellit- bzw. DBS-Gesellschaften (DBS steht für dirct broadcast satellite (Direkt-Rundstrahlsatellit)) und Gesellschaften mit Internetstellen (Internet sites), welche herunterladbaren Inhalt bereitstellen, aufzufordern, Schutzschemata einzuführen. Zwei solche Kopierschutzsysteme sind von der 5C-Gruppe der DHSG (= Data Hiding Sub Group (Datenverdeckungs-Subgruppe)) (5C umfasst Vertreter von Sony, Hitachi, Toshiba, Matsushita und Intel) und der DTDG (= Data Transmission Discussion Group (Datenübertragungs-Diskussionsgruppe)), die Industriekomitee-Subgruppen der CPTWG (= Copy Protection Technical Working Group (kopierschutztechnische Arbeitsgruppe)) sind, vorgeschlagen worden. Die CPTWG repräsentiert die Inhaltprovider, Computer- und Konsumelektronikprodukt-Hersteller.

[0005] Der DTDG-DTCP-Vorschlag (DTCP = Digital Transmission Copy Protection (Digitalübertragungskopierschutz)) ist auf den Schutz von kopiergeschütztem digitalen Inhalt gerichtet, der zwischen digitalen Einrichtungen, die über ein digitales Übertragungsmedium wie beispielsweise einen IEEE 1394-Seriellbus verbunden sind, übertragen wird. Einrichtungsbasiert verwendet der Vorschlag Symmetrischschlüssel-Verschlüsselungstechniken zum Codieren von Komponenten einer konformen Einrichtung. Dies berücksichtigt die Authentisierung jeder digitalen Einrichtung vor der Übertragung des digitalen Inhalts, um zu bestimmen, ob die Einrichtung konform ist. Der digitale Inhalt wird vor der Übertragung selbst codiert, so dass ein unautorisiertes Kopieren des Inhalts in einer Kopie, die ein unverständliches Format aufweist, resultiert.

[0006] Ein Verfahren zum Codieren des Inhalts ist von der DHSG vorgeschlagen worden und basiert auf Wasserzeichentechniken. Obgleich der Hauptfokus des DHSG-Vorschlags bei einem Kopierschutz digitalen Film- und Videoinhalts, insbesondere als auf DVD-Systeme angewendet, gewesen ist, wird erwartet, dass er zum Kopierschutz jeden digitalen Inhalts, der über digitale Rundsendungen und Netzwerke elektronisch verbreitet wird, anwendbar ist. Die Wasserzeichentechniken, die für den Benutzer unsichtbar sind, erlauben, dass der hereinkommende Inhalt in einer Weise markiert wird, die es extrem schwierig macht, präzise zu erkennen, wie der Inhalt codiert wurde, und folglich extrem schwierig, das Wasserzeichen ohne Beschädigung des Inhalts zu entfernen oder zu ändern. Die DHSG hat drei primäre Fälle von Detektion und Steuerung bestimmt, die eine solche Technik bzw. Technologie erfüllen sollte: Wiedergabe-, Aufzeichnungs- und Generationskopiersteue-

rung. Es wird erwartet, dass die Wasserzeichentechnologie dem Inhaltprovider erlaubt, wenigstens zu spezifizieren, ob der Inhalt ein „Copy never (Niekopieren)"-, „Copy once (Einmalkopieren)"- oder „Copy free (Freikopieren)"-Inhalt ist. „Copy never" wird zum Markieren digitalen Inhalts verwendet, um anzuzeigen, dass nicht erlaubt ist, den Inhalt zu kopieren, während „Copy free" anzeigt, dass der Inhalt frei kopiert werden kann und er mit zusätzlicher Information markiert werden kann. Dies ist verschieden von Material, das nie markiert wird. Schließlich wird „Copy once" verwendet, um anzuzeigen, dass erlaubt ist, den digitalen Inhalt nur einmal zu kopieren. Wenn eine Kopie gemacht wird, werden der originale „Copy once"-Inhalt und der neu kopierte Inhalt neu markiert mit „no more copy (keine Kopie mehr)". Natürlich können andere Typen von Kopierverwaltungs- bzw. Kopiermanagementbefehlen das Spielen oder die Wiedergabe solchen digitalen Inhalts begrenzen, beispielsweise auf eine spezifische Zeitperiode, Dauer oder Zahl von Spielen oder Vorführungen.

[0007] Infolgedessen erstreckt sich auch heute die Funktionalität digitaler Einrichtungen wie beispielsweise Set-top-Boxen (Set-top-Box = Digitalempfänger (Konverter und Decodierer in einem Gerät), Satellitenempfänger, multimediales Zusatzgerät, Aufsatzgerät) digitale Fernseher, digitaler Audiospieler und ähnliche solche digitalen Einrichtungen über ihre historische Rolle des bedingten Zugriffs (conditional access (CA)), d.h. lediglich Entwürfeln eines Inhalts zu einem CA-klaren Format zum Realzeitanschauen und/oder -hören, hinaus und enthält nun Beschränkungen und Bedingungen bei der Aufzeichnung und Wiedergabe solchen digitalen Inhalts. Beispielsweise kann gegenwärtig ein Kopieren verwürfelten Inhalts für eine nachfolgende Entwürfelung und Sehen oder Hören mit der geeigneten Dienst/Inhalt-Providerautorisation oder den der digitalen Einrichtung bereitgestellten Schlüssel erlaubt werden.

[0008] Traditionelle Bedingtzugriffssysteme für Pay-TV (Bezahlfernsehen) entstanden aus Simplex- bzw. Einweg-Rundfunksystemen, bei denen ein Rückkanal nicht verfügbar war. Einem Verschlüsselungsprozessor, beispielsweise eine Chipkarte (smart card), in einer Bedingtzugriffseinheit, beispielsweise eine Set-top-Box, wird generell Information und Funktionalität eingegeben, um einen Zugriff zu Programmen automatisch zu garantieren.

[0009] Beispielsweise empfängt eine Chipkarte mit einer Pay-TV-Zugriffssteueranwendung typisch EMMs, die gewisse Dienstbetitelungen bzw. -berechtigungen bzw. -benutzungsberechtigungen garantieren. Typischerweise werden Dienste- oder Gruppenschlüssel zur gleichen Zeit abgegeben, und wenn der Set-top-Box erlaubt ist, IPPV-Programme anzusehen, kann die Kredit- und Kostengrenze-Information ebensogut übertragen werden.

[0010] Beim Abstimmen auf ein Programm empfängt die Chipkarte ECMs, die beschreiben, welche Betitelungen bzw. Berechtigungen die Chipkarte benötigt, um einen Zugriff zur Show zu garantieren. Hacker können versuchen, sowohl EMMs als auch ECMs zu manipulieren, um Programme ohne Bezahlung der erforderlichen Teilnehmergebühren sehen. Nicht nur werden die EMMs und ECMs manipuliert, sondern die Hardware wird ebenso attackiert. Diese Kombination aus Software- und Hardware-Attacken werden benutzt, um zu bewirken, dass die Chipkarte verwürfelte Programme ohne Autorisation vom Anbieter bzw. Provider der Programme entschlüsselt.

[0011] Einmal aufgefangen bzw. in Felder unterteilt ist es schwer, die Funktionalität der Chipkarten zu ändern. Mechanismen zum Herunterladen eines neuen Codes zu Chipkarten sind empfänglich für Attacken von Hackern, die versuchen können, die gleichen Mechanismen zum Laden eines Pirat- bzw. Raubcodes in die Chipkarte zu verwenden, um Programme zu stehlen. Ein „sicherer" Weg, das Zugriffssteuersystem zu verbessern ist, existierende Chipkarten vom Feld zu nehmen und neue bereitzustellen. Dies kann jedoch teuer und logistisch schwierig sein.

[0012] WO 86/07224 offenbart ein Verfahren und Gerät zum Verwürfeln und Entwürfeln von Fernsehsignalen. Ein Fernsehsignal wird verwürfelt und mit einem verschlüsselten Sessionsschlüssel (Sitzungsschlüssel) und einem verschlüsselten Entwürfelungscode übertragen. Der Entwürfelungscode ist unter Verwendung des Sessionsschlüssels verschlüsselt, und der Sessionsschlüssel ist entsprechend einem Verteiler- bzw. Verteilungsschlüssel, der einem Empfänger bekannt ist, verschlüsselt. Der Empfänger ist angeordnet zum Wiedergewinnen des Fernsehsignals durch Entschlüsselung des Sessionsschlüssels unter Verwendung des Verteilungsschlüssels und Entschlüsselung des Entwürfelungscodes unter Verwendung des Sessionsschlüssels und Entwürfelung der Fernsehsignale unter Verwendung des Entwürfelungscodes.

[0013] WO 97/38530 offenbart eine Anordnung zur Entschlüsselung von Fernsehsignalen, die eine Bedingtzugriffseinrichtung und eine Chipkarte aufweist. Die Bedingtzugriffseinrichtung erzeugt einen Zufallsschlüssel und überträgt den Zufallsschlüssel zur Chipkarte in einer verschlüsselten Form. Der Zufallsschlüssel ist unter

Verwendung eines öffentlichen Schlüssels, der von der Chipkarte unter Verwendung eines korrespondierenden geheimen Schlüssels verschlüsselt ist, verschlüsselt, um den Zufallsschlüssel, der nachfolgend zum Verschlüsseln/Entschlüsseln von Meldungen zwischen der Chipkarte und der Bedingtzugriffseinrichtung verwendet wird, zu erhalten.

[0014] US 5 485 577 offenbart ein Sicherheitsgerät für Informationsverarbeitungssysteme, in welchem authentisierte Zugriffsrechte zunehmend abgegeben werden, um auf Steuerprozessoren zuzugreifen.

[0015] Die UK Patentanmeldung GB 22 41 096 A offenbart einen Empfänger zur Dechiffrierung verwürfelter Videosignale, der eine Steuereinheit, einen Videoprozessor und eine Dateneingabeschaltung aufweist. Die Steuereinheit umfasst eine Speichereinrichtung. Die Speichereinrichtung weist Dechiffrierungsalgorithmen und einen darin vorgespeicherten eindeutigen bzw. einzigen M-Chiffreschlüssel auf. Die Steuereinheit empfängt den M-Chiffreschlüssel und dechiffriert eine chiffrierte Meldung, die einen V-Chiffreschlüssel enthält, mit dem das Videosignal verwürfelt worden ist. Der V-Chiffreschlüssel wird dann dem Videoprozessor zur Entschlüsselung der verwürfelten Videosignale zugeführt.

ZUSAMMENFASSUNG

[0016] Verschiedene Aspekte und Merkmale bzw. Eigenschaften der vorliegenden Erfindung sind in den beigefügten Ansprüchen definiert.

[0017] Gemäß einer Ausführungsform ist ein Verfahren zur Sicherung von Steuerungswörtern bereitgestellt. Das Verfahren umfasst Empfangen verwürfelten digitalen Inhalts in einer integrierten Entwürflerschaltung bzw. Entwürflerintegriertschaltung. Das Verfahren umfasst außerdem Empfangen eines verschlüsselten Steuerungswortes (encrypted control word) in der Entwürflerintegriertschaltung, Entschlüsseln des verschlüsselten Steuerungswortes unter Verwendung eines in einer Registerschaltung der Entwürflerintegriertschaltung gespeicherten Schlüssels und Entwürfeln des verwürfelten digitalen Inhalts in der Entwürflerintegriertschaltung unter Verwendung des entschlüsselten Steuerungsworts.

KURZE BESCHREIBUNG DER ZEICHNUNGEN

[0018] Die vorliegende Erfindung ist mittels eines Beispiels und nicht mittels einer Einschränkung in den Figuren der beigefügten Zeichnungen dargestellt, in denen gleiche Bezugszeichen ähnliche Elemente bezeichnen, und in denen:

[0019] Fig. 1 ein Blockschaltbild eines exemplarischen Unterhaltungssystems ist, das eine Ausführungsform einer digitalen Einrichtung enthält;

[0020] Fig. 2 eine Ausführungsform einer Bedingtzugriffseinheit (conditional access unit) mit einer Chipkarte ist;

[0021] Fig. 3 eine Ausführungsform eines Verfahrens zur sicheren Übertragung von Steuerungswörtern von einer Chipkarte zu einer Bedingtzugriffseinheit ist;

[0022] Fig. 4 und Fig. 5 Ausführungsformen eines Verfahrens zur Verschlüsselung und Entschlüsselung von Daten sind;

[0023] Fig. 6 ein Blockschaltbild einer Ausführungsform der Entwürflerintegriertschaltung ist;

[0024] Fig. 7 eine Ausführungsform eines Empfangsstellen- bzw. Kopfstellenservers, einer Netzwerkverbindung und eines Decodierers ist;

[0025] Fig. 8 eine andere Ausführungsform eines Decodierers ist;

[0026] Fig. 9 Ausführungsformen von Diensten zeigen, die an einen Decodierer oder eine Bedingtzugriffseinheit abgegeben werden können; und

[0027] Fig. 10 eine Ausführungsform eines Verfahrens zur Anforderung und zum Empfang von Steuerungswörtern oder Dienstschlüsseln zeigt.

DETAILLIERTE BESCHREIBUNG

[0028] Fig. 1 ist ein Blockschaltbild eines Unterhaltungssystems **100**, das eine Ausführungsform eines Kopierverwaltungs- bzw. Kopiermanagementsystems der vorliegenden Erfindung umfasst. Das Unterhaltungssystem **100** umfasst eine digitale Einrichtung **110** zum Empfang eines Programmdaten von einem oder mehreren Dienstprovidern enthaltenden Bitstroms. Solche Dienst- oder Inhaltprovider können terrestrische Rundfunk-Programmanbieter bzw. -provider, Kabeloperatoren, DBS-Gesellschaften (DBS = direct broadcast satellite (Direkt-Rundstrahlsatellit)), Inhalt zum Herunterladen über das Internet bereitstellende Gesellschaften oder jeden ähnlichen solchen Inhalt- und/oder Dienstprovider umfassen. Die Programmdaten können Systeminformation, Betitelungs- bzw. Berechtigungs- bzw. Benutzungsberechtigungs-Steuermeldungen, Betitelungs- bzw. Berechtigungs- bzw. Benutzungsberechtigungs-Managementmeldungen, Inhalt und andere Daten enthalten, die jeweils kurz beschrieben werden. Systeminformation kann Information über Programmnamen, Rundfunkzeit, Quelle und ein Verfahren zur Wiedergewinnung und Decodierung sowie Kopiermanagementbefehle, die digitalen Empfängern und anderen Einrichtungen Information, die steuert, wie und wann Programmdaten rückgespielt, rückübertragen und/oder aufgezeichnet werden können, bereitstellen. Diese Kopierverwaltungs- bzw. Kopiermanagementbefehle können auch zusammen mit Betitelungs- bzw. Berechtigungssteuermeldungen (entitlement control messages (ECM)), die von der Bedingtzugriffseinheit zum Regulieren eines Zugriffs einen besonderen Kanal oder Dienstes generell verwendet werden, übertragen werden. Betitelungs- bzw. Berechtigungsmanagementmeldungen (entitlement management messages (EMM)) können zum Abgeben von Privilegien an den digitalen Empfänger **111** wie beispielsweise Rechte, Zugriffsparameter und Entwürfelungsschlüssel verwendet werden. Wie bekannt ist ein Entschlüsselungsschlüssel generell ein Code, der zum Wiederherstellen verwürfelter Daten erforderlich ist und eine Funktion der garantierten Rechte sein kann. Schließlich kann ein Inhalt im Programmdatenstrom Audio- und Videodaten, die in einem verwürfelten oder klaren Format sein können, enthalten.

[0029] Die digitale Einrichtung **110** umfasst einen digitalen Empfänger **111**, der den hereinkommenden Bitstrom verarbeitet, daraus die Programmdaten extrahiert und die Programmdaten in einem sichtbaren Format bereitstellt. Die digitale Einrichtung **110** kann über ein Übertragungsmedium **120** an andere Komponenten des Unterhaltungssystems **100** gekoppelt sein. Das Übertragungsmedium **120** arbeitet so, dass es Steuerinformation und Programmdaten enthaltende Daten zwischen der digitalen Einrichtung **110** und anderen Komponenten im Unterhaltungssystem **100** überträgt.

[0030] Das Unterhaltungssystem **100** kann ein an das Übertragungsmedium **120** gekoppeltes Audiosystem **130** enthalten. Ein digitaler VCR **140** wie beispielsweise ein D-VHS VCR kann durch das Übertragungsmedium **120** ebenfalls an die digitale Einrichtung **110** und andere Komponenten des Unterhaltungssystems **100** gekoppelt sein.

[0031] Eine Hartplatten- bzw. Festplatten-Aufzeichnungseinheit **150** kann über das Übertragungsmedium **120** auch an die digitale Einrichtung **110** und andere Komponenten gekoppelt sein. Eine Anzeige **160** kann eine hochauflösende Fernsehanzeige (high definition television display), einen Monitor oder eine andere zur Verarbeitung digitaler Videosignale fähige Einrichtung aufweisen. Schließlich kann eine Steuereinheit **170** an das Übertragungsmedium **120** gekoppelt sein. Die Steuereinheit **170** kann zum Koordinieren und Steuern des Betriebs bzw. der Operation einiger oder jeder der Komponenten auf dem Unterhaltungssystem **100** verwendet sein.

[0032] Der Inhalt eines digitalen Programms kann in verwürfelter Form übertragen werden. Damit eine Bedingtzugriffseinheit den verwürfelten Inhalt zurückgewinnen und eine Person den Inhalt in klarer Form sehen kann, muss die Einheit die dem verwürfelten Inhalt zugeordneten notwendigen Zugriffserfordernisse aufweisen. Ein Zugriffserfordernis enthält eine Meldung, welche die Merkmale beschreibt, die Bedingtzugriffseinheit haben muss, um den verwürfelten Inhalt zu decodieren. Beispielsweise kann zum Sehen des Inhalts ein gewisser Schlüssel notwendig sein. Alternativ dazu kann ein einem gegebenen Inhaltprovider zugeordnetes Dienstkennzeichen erforderlich sein. Technische Erfordernisse wie beispielsweise ein besonderes Entwürfelungsverfahren können auch notwendig und als ein Teil der Zugriffserfordernisse enthalten sein. Die einem besonderen Programm zugeordneten Zugriffserfordernisse können zusammen mit dem Programm zu einer Bedingtzugriffseinheit übertragen werden.

[0033] Wenn ein verwürfeltes Programm von einer Bedingtzugriffseinheit empfangen wird, werden die Zugriffserfordernisse für das Programm mit den Betitelungen bzw. Berechtigungen verglichen, welche die Bedingtzugriffseinheit tatsächlich hat. Damit die Bedingtzugriffseinheit den verwürfelten Inhalt in klarer Form anzeigen kann, müssen die Zugriffserfordernisse für das Programm mit den Betitelungen bzw. Berechtigungen

der Bedingtzugriffseinheit übereinstimmen bzw. zu diesen passen. Die Betitelungen bzw. Berechtigungen können festlegen bzw. spezifizieren, dass die Bedingtzugriffseinheit betitelt bzw. berechtigt ist, den Inhalt von einem gegebenen Dienstprovider wie beispielsweise HBO zu sehen. Die Betitelungen bzw. Berechtigungen können auch einen oder mehrere zum Entwürfeln des Inhalts notwendige Schlüssel enthalten. Die Betitelungen bzw. Berechtigungen können auch die Zeitperioden definieren, für welche die Bedingtzugriffseinheit Programme entwürfeln kann. Die Zugriffserfordernisse und Betitelungen bzw. Berechtigungen bilden auf diese Weise einen Teil des Zugriffssteuersystems zum Bestimmen, ob ein Decodierer autorisiert ist, ein besonderes Programm zu sehen.

[0034] Die Zugriffserfordernisse und Berechtigungen können Konsumenten mit einer Vielfalt von Wahlen zum Bezahlen für den Inhalt und gewinnen eines Zugriffs auf den verwürfelten Inhalt bereitstellen. Diese Wahlen können Bezahlen-pro-Spiel bzw. Pay per play (PPP), Videoabrufdienst bzw. Bezahlen-pro-Sehen bzw. Pay per view (PPV), Impuls-Bezahlen-pro-Sehen bzw. Impulse pay per view (IPPV), zeitbasiertes Historisches bzw. Altes bzw. Time based historical, Bezahlen-pro-Zeit bzw. Pay per time (PPT), Rückkauf-von Niekopiefilmen, bzw. Repurchase of copy never movies, persönliches Verwürfeln bzw. Personal scrambling und regionales Pay per view bzw. Regional pay per view umfassen. Impulse pay per view ist ein Merkmal, das einen Kauf von Bezahlen-pro-Sehen-Filmen bzw. Pay per view movies durch Kredit, der vorher in die Set-top-Box heruntergeladen worden ist, erlaubt. Kaufaufzeichnungen können gespeichert und durch Telefon zu einem Rechnungserstellungszentrum weitergeleitet werden. Time based historical erlaubt einen Zugriff auf einen Inhalt, der während einer vergangenen Zeitperiode wie beispielsweise März bis Dezember 1997 geliefert wurde. Die Zugriffserfordernisse und Berechtigungen können Kunden auch verschiedene Optionen zum Speichern des verwürfelten Inhalts bereitstellen.

[0035] Die Zugriffserfordernisse können an die Bedingtzugriffseinheit unter Verwendung von Paket-Identifizierern (packet identifiers (PIDs)) abgegeben werden. Jeder PID kann die einem gegebenen Dienst oder Merkmal zugeordneten Zugriffserfordernisse enthalten. Der an eine Bedingtzugriffseinheit abgegebene Inhalt kann eine große Zahl an PIDs enthalten und dadurch spezielle Einnahmemerkmale, technische Merkmal oder andere spezielle Merkmale ermöglichen, die lokal auszuführen sind.

[0036] Vor Empfang des Inhalts kann dem Kunden eine Zahl Wahlen zur Gewinnung eines Zugriffs auf den Inhalt, der in Begriff ist, auf Media gespeichert zu werden, gegeben sein. Der Kunde kann aufgefordert werden, das Recht auf den Zugriff und das Sehen des Inhalts zu kaufen. Wenn deshalb der Kunde den Inhalt für eine spätere Wiedergewinnung und ein späteres Sehen aufzeichnen will, müssen die Zugriffserfordernisse, die der Kunde kaufte, mit dem Inhalt gespeichert sein.

[0037] Es gibt verschiedene Typen von Sicherheitsarchitekturen für Bedingtzugriffseinheiten: 1) eingebettete, 2) gespaltene bzw. gesplittete Sicherheit und 3) externe Sicherheit. Bei eingebetteter Sicherheit werden die Inhaltentwürfelung und das Schlüsselmanagement insgesamt in der Bedingtzugriffseinheit, beispielsweise einer Set-top-Box, ausgeführt. Bei gesplitteter Sicherheit wird die Entwürfelung in der Set-top-Box ausgeführt, jedoch wird das Schlüsselmanagement außerhalb der Set-top-Box durch Verwendung eines Verschlüsselungsrozessors wie beispielsweise einer Chipkarte ausgeführt. Bei externer Sicherheit werden sowohl die Inhaltentwürfelung als auch das Schlüsselmanagement extern, beispielsweise mit den NRSS-A- und NRSS-B-Bedingtzugriffsspezifikationen (NRSS-A and NRSS-B conditional access specifications), ausgeführt. Die Kabelindustrie hat durch den bzw. „Open Cable(Offen-Kabel)"-Prozesess eine modifizierte Version von NRSS-B, die als „Point-of-Deployment(Punkt-des-Einsatzes)"-Modul (POD-Modul) bezeichnet wird. Das POD-Modul hat den gleichen Formfaktor wie NRSS-B. Es enthält Funktionalität zum Senden und Empfangen von Meldungen auf dem „Out-of-Band"-Kanal („Außerband"-Kanal). Der externe Sicherheitstyp kann auch gesplittet sein, beispielsweise durch Verwendung einer PCMCIA-Formfaktorkarte, die Inhalt entwürfelt, und einer Chipkarte, die das Schlüsselmanagement ausführt.

[0038] Außerdem kann auf den CA-entwürfelten Transportstrom ein Kopierschutz angewendet sein. Kopiergeschützter Inhalt wird über das CA-Modul (NRSS-A-, NRSS-B- oder POD-)Schnittstelle und den Hauptcomputer bzw. Host neu verwürfelt. Das CA-Element und der Host müssen dem zum neuen Verschlüsseln dieses Inhalts verwendeten Schlüssel zustimmen. Bei einer Ausführungsform sind auf jeder Seite der Schnittstelle verschiedenen Parameter sicher geteilt, mit dem Resultat, dass von jedem Teilnehmer der gleiche Kopierschutzschlüssel abgeleitet wird. Das CA-Modul kann alternativ dazu seinen eigenen Schlüssel ableiten und den Kopierschutzschlüssel mit dem eindeutigen bzw. einzigen Schlüssel der Entwürflerintegriertschaltung im Host verschlüsseln. Das CA-Modul kann diesen einzigen Schlüssel der Entwürflerintegriertschaltung durch eine EMM oder ein anderes Verfahren, beispielsweise Fabrikladeprozedur, empfangen.

[0039] Wie in Fig. 2 zu sehen ist, weist eine das Kopiermanagementsystem der vorliegenden Erfindung aufweisende Ausführungsform des digitalen Empfängers **111** eine Chipkartenschnittstelle **420** auf. Obgleich die Chipkartenschnittstelle **420** in den digitalen Empfänger **111** eingebaut sein kann, wird erwartet, dass der digitale Empfänger einen Erweiterungsschlitz, beispielsweise einen PCMCIA-Schlitz oder Universaldienstebus- bzw. Universal-Services-Bus-Schlitz (USB-Schlitz) zur Aufnahme einer Karte oder Einrichtung, welche die Schnittstelle **420** enthält, aufweist. Der digitale Empfänger **111** dieser Ausführungsform weist eine CPU **430** und eine Entwürflerintegriertschaltung **440** auf.

[0040] Die Chipkartenschnittstelle **420** nimmt eine Chipkarte auf, die verschlüsselte Steuerungswörter zum Entwürfeln verschlüsselten Programminhalts enthält. Die Chipkarte **410** kann die Steuerungswörter in verschlüsselter Form zur Chipkartenschnittstelle **420** übertragen. Wenn der Inhalt unter Verwendung von Steuerungswörtern zusätzlich zu Schlüsseln original verschlüsselt wurde, kann die Chipkarte **410** einen der Einheit **401** eindeutigen bzw. einzigen Verschlüsselungssteuerschlüssel verwenden, um die Steuerungswörter zu verschlüsseln. Die Bedingtzugriffseinheit **401** entschlüsselt die Steuerungswörter und verwendet die klaren Steuerungswörter zum Entwürfeln des Programminhalts.

[0041] So zeigt Fig. 2 eine Ausführungsform der gesplitteten Sicherheitsarchitektur und externen Architektur. Bei der gesplitteten Sicherheitsarchitektur ist die Bedingtzugriffseinheit **401** eine Set-top-Box oder anderer Typ einer digitalen Einrichtung, beispielsweise die in Fig. 1 gezeigte Einrichtung **110**. Bei der externen Architektur ist die Bedingtzugriffseinheit eine NRSS-B-Bedingtzugriffseinheit. Ein externer Verschlüsselungsprozessor **410**, beispielsweise eine ISO 7816-Chipkarte, empfängt Steuerungswörter (control words (CWs)), die zum Entwürfeln eines Programms benötigt werden. Die Chipkarte **410** verschlüsselt die CWs im Verschlüsselungsblock **414** mit Schlüsseln, die für die Transportentwürflerintegriertschaltung (Intergriertschaltung = integrated circuit (IC)) **440** eindeutig bzw. einzig sind.

[0042] Die Chipkarte **410** gibt die verschlüsselten CWs an die Set-top-CPU **430** durch die Schnittstelle **420** ab. Die Transportentwürfler-IC (descrambler IC) **440** in der Set Top Box **401** entschlüsselt die CWs unter Verwendung der eindeutigen bzw. einzigen Entwürfeer-IC-Schlüssel (unique descrambler IC keys) die im Register **450** gespeichert sind. Der Entschlüsselungsblock **460** schreibt dann die entschlüsselten CWs alternierend in UNGERADE- und GERADE-Schlüsselregister (ODD and EVEN key registers) des im Transportentwürflerchip **440** lokalisierten Entwürflers **470**. Der Entwürfler **470** wendet dann die UNGERADE/GERADE-CWs (ODD/EVEN-CWs) auf den verwürfelten Inhalt **480** zur rechten Zeit an und gibt den entwürfelten Programminhalt **490** aus.

[0043] So ist die Übertragung des Steuerungsworts von der Chipkarte zur Set-top-Box sicher, da das Steuerungswort in verschlüsselter Form übertragen wird. Das Steuerungswort bleibt in der Set-top-Box sicher, da das Steuerungswort von dem nicht sichereren Prozessor **430** nicht entschlüsselt wird. Das Steuerungswort wird nur in der Entwürfler-IC **440** entschlüsselt, die das Steuerungswort tatsächlich verwendet, und deshalb ist das Steuerungswort nie freigelegt und kann von Hackern nicht erhalten werden.

[0044] Außerdem ist der zum Entschlüsseln des Steuerungsworts verwendete Schlüssel als Hardware im Register **450** in der IC **440** gespeichert. Das Register **450** kann nicht gehackt werden, wenn nicht das Silizium getestet und das Register zerstört wird. Es kann ein Versuch gemacht werden, den im Register **450** in der IC **440** erschöpfend auszuloten bzw. versuchen. Wenn jedoch der Schlüssel ausreichend groß ist, werden die Angriffsmittel als hoffnungslos angesehen. Außerdem kann der Schlüssel nur für eine einzelne besondere Einheit **401** gültig sein und kann nicht von anderen Einheiten zum Entschlüsseln von Steuerungswörtern benutzt werden, da die Steuerungswörter von der Chipkarte unter Verwendung eines Schlüssels, der für eine zugeordnete Bedingtzugriffseinheit **401** eindeutig bzw. einzig ist, verschlüsselt sind. Deshalb ist die Übertragung der verschlüsselten Steuerungswörter von der Chipkarte **410** zur Bedingtzugriffseinheit **401** sicher, und die Steuerungswörter sind für Diebstahl durch Hacker nicht zugänglich.

[0045] Der Sicherheitschip **440** führt die gesamte Sicherheitsverarbeitung der Steuerungswörter aus. Dieser Sicherheitschip weist keine CPU, keine Firmware und keine Software auf. Es gibt dort keine komplizierte Schlüsselhierarchie. Ein nicht auf CPU basierter Entwürflerchip empfängt die verschlüsselten Steuerungswörter, wendet einen eindeutigen bzw. einzigen Schlüssel (unique key) auf sie an und entschlüsselt sie. Es sind keine Instruktionen, kein Code, kein Hashing und keine Software in den Entschlüsselungsblock geladen. Die Entschlüsselung wird ganz von einer Hardwareschaltung, die nur eine einzelne Schlüsselfunktion verwendet, ausgeführt.

[0046] Die einzigen Schlüssel können während der Herstellung in das Register **450** programmiert werden.

Beispielsweise weist bei einer Ausführungsform die Entwürfler-IC ein nichtflüchtiges Einzig-Schlüssel-Register **450** auf, das nur einmal beschrieben werden kann. Wenn die Set-top, der TV oder das NRSS-B-Modul **401** hergestellt wird, wird das Einzig-Schlüssel-Register **450** programmiert. Bei dieser Ausführungsform gibt es keinen Weg, um entweder die originalen Schlüssel, die in das Register **450** geladen wurden, zu lesen oder überschreiben. Eine Zuordnung zwischen der Seriennummer der Hosts (**401**) und dem einzigen Schlüssel, der in die Entwürfler-IC dieses Hosts geladen wurde, kann aufgezeichnet werden.

[0047] Wenn die Set-top **401** hergestellt ist und eine Chipkarte **410** installiert ist, kann die Chipkarte **410** den der Einheit **401** zugeordneten einzigen Schlüssel zur Zeit der Paarung empfangen. Von da an ist die Chipkarte mit diesem besonderen Host **401** „gepaart". Wenn später die Chipkarte jemals ersetzt oder zu einem neuen Host bewegt wird, kann die Chipkarte die Entwürfler-IC-Einzig-Schlüssel in einer EMM (Berechtigungs-Management-Meldung)) empfangen. Neue Chipkarten mit den schon in die Karte programmierten Einzig-Schlüsseln können auch an Benutzer abgegeben werden.

[0048] Ein Verfahren zur Übertragung der CWs von der Chipkarte zur Bedingtzugriffseinheit ist in Fig. 3 gezeigt. Ein Steuerungswort wird in der Chipkarte unter Verwendung eines in einer Registerschaltung der Chipkarte gespeicherten Schlüssels beim verschlüsselt, Schritt **40**. Der in der Registerschaltung der Chipkarte gespeicherte Schlüssel ist dem in der Registerschaltung der Entwürflerintegriertschaltung gespeicherten Schlüssel zugeordnet. Das verschlüsselte Steuerungswort wird von der Chipkarte empfangen, Schritt **41**. Dieses Verfahren umfasst Empfangen eines Programmdaten enthaltenden digitalen Bitstroms in einer Entwürflerintegriertschaltung, wobei die Programmdaten Systeminformation und verwürfelten digitalen Inhalt enthalten, Schritt **42**. Das verschlüsselte Steuerungswort wird unter Verwendung eines in der Registerschaltung der Entwürflerintegriertschaltung gespeicherten Schlüssels entschlüsselt, Schritt **44**. Der verwürfelte digitale Inhalt wird in der Entwürflerintegriertschaltung unter Verwendung des entschlüsselten Steuerungsworts entwürfelt, Schritt **45**, und der entwürfelte digitale Inhalt wird ausgegeben, Schritt **46**.

[0049] Ausführungsformen der vom Verschlüsselungsblock **414** und Entschlüsselungsblock **460** ausgeführten Verschlüsselungs- und Entschlüsselungsfunktionen sind in den Fig. 4, Fig. 5 und Fig. 6 gezeigt. Diese Operationen transformieren die CWs auf der Basis der in den Registern **412** und **450** gespeicherten einzige Schlüssel. Ein Verschlüsselungsalgorithmus wie beispielsweise DES, M6 oder DVB-Common Scrambling Algorithm kann verwendet werden. Bei den in den Fig. 4, Fig. 5 und Fig. 6 gezeigten Ausführungsformen ist Triple DES (Dreifach-DES) verwendet. Wie in Fig. 6 gezeigt verwendet die Entwürfler-IC **440** Triple DES zum Entschlüsseln der Steuerungswörter im Entschlüsselungsblock **460**. Die entschlüsselten Steuerungswörter werden dann vom Entwürfler **470** zum Entwürfeln des Programminhalts **480** und Ausgeben klaren Programminhalts **490** verwendet.

[0050] Da jedoch die Verschlüsselung und Entschlüsselung der CWs lokal bei der Set-top-Box sind, ist es möglich, die Entwicklung einer zunehmen robusteren Verschlüsselung in Phase zu bringen. Beispielsweise kann ein einzelner DES (single DES) anfänglich eingesetzt werden, und später können double (doppelte) oder triple (dreifache) DES ohne Konsequenz für schon in Felder unterteilte gepaarte Einheiten von Set-tops und Chipkarten in Phase gebracht werden. Die Schlüssellänge der einzigen Schlüssel kann wenigstens so groß wie die Entwürfelungs-Steuerungswörter sein, um zu helfen, Attacken auf die einzigen Schlüssel durch Hacker zu reduzieren.

[0051] Bei einer in Fig. 7 gezeigten alternativen Ausführungsform kann die Chipkarte durch die Eingabe- bzw. Kopfstelle **710** eines Ein- oder Zweiwegnetzwerks **720** ersetzt sein. Die Kopfstelle hält die Zugriffsrechte für den Decodierer **701** anstelle eines lokalen Krypto-Mikrokontrollers. Die Kopfstelle **710** kann Dienstschlüssel auf der Basis der in der Entwürfler-IC **740** gespeicherten einzigen Schlüssel abgeben. Die verschlüsselten Dienstschlüssel können im Host **701** lokal gespeichert sein, um Übergänge von einem Kanal zu einem anderen zu erleichtern. Die Schlüssel sind in verschlüsselter Form gespeichert und sind in die Entwürfler-IC **740** wie benötigt geladen. Die Schlüssel werden nur in der Entwürfler-IC **740** durch Verwendung der im Register **750** gespeicherten Entwürfler-IC-Einzig-Schlüssel entschlüsselt. Bei einer Ausführungsform sind die Dienstschlüssel als Steuerungswörter zum direkten Entschlüsseln des Inhalts verwendet. Bei einer anderen Ausführungsform sind die Dienstschlüssel zum Entschlüsseln von Steuerungswörtern, die in-band mit dem Inhalt empfangen werden.

[0052] Die Dienstschlüssel können unter Verwendung eines der für die Steuerungswörter in den vorstehend beschriebenen Ausführungsformen der Fig. 2, Fig. 4, Fig. 5 und Fig. 6 verwendeten Algorithmen verschlüsselt und entschlüsselt werden. Der zum Verschlüsseln und Entschlüsseln der Dienstschlüssel verwendete Algorithmus kann von dem zum Verwürfeln und Entwürfeln des Programminhalts verwendeten Algorithmus ver-

schieden sein. Beispielsweise kann M6 in Software in entweder der Chipkarte oder des Kopfstellenschlüsselservers leichter getan werden. Auch kann jeder Dienst-Schlüssel unter Verwendung verschiedener öffentlicher und eigentümlicher Verschlüsselungsalgorithmen verschlüsselt werden. Diese verschiedenen eigentümlichen Algorithmen können als Antiplagiatmaßnahmen zum außer Kraft setzen von Klonhardware betrachtet werden.

[0053] Die Kopfstelle **710** kann Dienstschlüssel an einen Kanal oder einem Rang bzw. eine Netzebene einer Servicebasis in EMMs abgeben. Die Diensteschlüssel sind im Decodierer **401** verschlüsselt lokal gespeichert und werden vom unsicheren Prozessor **730** wie benötigt verwendet, wenn auf verschiedene Kanäle abgestimmt wird. Da die Set-tops im Vergleich mit der Kopfstelle in hohem Volumen in Felder unterteilt sind, kann ein Eliminieren der Verschlüsselungsprozessoren, beispielsweise Chipkarten, von den Set-tops die Kosten der Implementierung eines Pay-TV-Systems in einem Netzwerk stark reduzieren.

[0054] Während diese Ausführungsform in (Nicht-IPPV)-Einwegrundfunk- bzw. Einwegsendenetzwerken arbeitet, funktioniert sie auch in interaktiven Zweiwegnetzwerken, wo die Schlüssel für einen besonderen Dienst, beispielsweise IPPV- oder VOD-Käufe oder einen beliebig anderen Nichtteilnehmerdienst angefordert werden. Der Rückführkanal **721** fordert die Schlüssel an, da die Fähigkeit, einen Zugriff auf einen neuen Dienst zu garantieren von, der Kopfstelle **710** anstelle von einem lokalen Steuerungs-Kryptoprozessor ausgeführt wird.

[0055] Um an der Kopfstelle Überlastungsprobleme zu vermeiden, die durch eine große Zahl gleichzeitiger Impulskäufe von IPPV-Programmen verursacht werden, kann eine Frei-Vorschau-Periode (Free Preview period) bestimmt werden, und IPPB-Programme können vor dem tatsächlichen Sehen vermarktet werden. Bei dieser Ausführungsform können Dienst-Schlüssel für individuelle Shows oder Filme von der Einheit **701** angefordert und der Zeit voraus abgegeben werden. Beispielsweise können interaktive Netzwerke wie beispielsweise ein Kabelsystem, das einen Rückkanal **721**, beispielsweise ein DOCSIS-Modem oder einen Außerband-Sender/Empfänger (Out-of-Band transmitter/receiver), aufweist, können die Anforderung von der Einheit **701** zur Kopfstelle **710** abgeben. Alternativ dazu kann die Set-top-Einheit **701** den laufenden Entschlüsselungsdienstschlüssel für jedes Programm, auf das zugegriffen wird, anfordern.

[0056] Ein Kontroller auf dem Netzwerk-Kopfstellenserver **710** verarbeitet diese Anforderung für Programmschlüssel PRK (Request for Program Key). Die Anforderung kann die Einheitsadresse des Decodierers und zum Identifizieren des zu sehenden Kanals enthalten (von denen alle vom MPEG-System und vom unsicheren Prozessor schon verarbeiteter Programminformation erhalten werden können). Die Anforderung kann, wenn Notwendigkeit besteht, zur Nichtablehnung und Verhinderung einer Abweisung von Dienstattacken, beispielsweise IPPV oder VOD-Anforderungen, verschlüsselt sein.

[0057] Bei Empfang der Meldung sieht der Schlüsselserver **710** beim Decodierer **710** in der Zugriffssteuerungsliste (die alle Betitelungen bzw. Berechtigungen von Einheiten auflistet) nach und verifiziert die Autorisierung des Decodierers. Wenn autorisiert, sendet der Kontroller den Dienstschlüssel (verschlüsselt unter dem in der Entwürfler-IC lokalisierten einzige Schlüssel des Decodierers) zur Einheit. Fig. 8 zeigt eine alternative Ausführungsform des Decodierers **701**, der Dienstschlüssel anfordern und empfangen kann.

[0058] Bei dieser Ausführungsform kann der Dienst-Schlüssel für eine gewisse Zeitperiode gültig sein. Der Decodierer **701** kann den Schlüssel, wenn er zu anderen Diensten surft, speichern, was dem Decodierer erlaubt, mit einem noch gültigen Schlüssel wieder auf den Dienst zuzugreifen, ohne dass er den Schlüssel wieder anfordern muss. Bei dieser Ausführungsform ist der Schlüssel in seiner einheitsspezifisch verschlüsselter Form (wie er vom Schlüsselserver über das Netzwerk kommt) im Speicher **735** des unsicheren Prozessors **730** (der den Decodierer betreibt) gespeichert.

[0059] Durch Verwendung des Speichers und der Verarbeitungsleistung des unsichern Allzweck- bzw. Universalhostprozessors und nicht eines separaten Verschlüsselungsprozessors kann eine große Kostenreduzierung erzielt werden. Nicht nur kann der Verschlüsselungsprozessor eliminiert werden, sondern es gibt auch weniger Zusatz am Teil des Hostprozessors beim Behandeln der Kommunikation zu diesem Verschlüsselungsprozessor.

[0060] Der Dienstschlüssel kann für die Dauer eines Programms gültig sein, oder er kann für eine Zeitperiode, beispielsweise 6 Stunden gültig sein. Die Verwendung eines Schlüssels für eine längere Zeitperiode reduziert die Gesamtzahl von Transaktionen zwischen dem Decodierer **701** und der Kopfstelle **710**, da, wenn der Schlüssel einmal im Decodierer **710** gespeichert ist, er vom Speicher des Decodierers dem Decodierer verfügbar ist. Abhängig von der Dauer des gegenwärtigen bzw. laufenden Dienstschlüssels kann der nächste Schlüssel zusammen mit dem laufenden Schlüssel abgegeben werden. Alternativ dazu kann der Decodierer den

nächsten Dienstschlüssel nach Detektion des Endes der Gültigkeitsepoche des laufenden Dienstschlüssels anfordern. Bei einer Ausführungsform ist der Dienstschlüssel für die Dauer einer Teilnehmerperiode eines Benutzers gültig.

[0061] Der Dienstschlüssel muss richtig identifiziert werden, so dass er auf einem Kanal, auf den abgestimmt ist, angewendet werden kann. Wenn die Set-top-Box **701** auf einen Kanal abstimmt, schlägt sie beim geeigneten verschlüsselten Dienstschlüssel vom Speicher **735** nach und schreibt diesen in das Ungerade/Gerade-MPEG-Schlüsselregister (Odd/Even-MPEG key register) der Entwürfler-IC **740** nach. Wie bei der Ausführungsform der Fig. 2 kann die geheime Einzig-Schlüssel-Information in die IC **740** programmiert werden, wenn der Decodierer **701** hergestellt wird.

[0062] Bei einer Ausführungsform können die Dienstschlüssel 56-Bit-, 112-Bit- oder 168-Bit-Schlüssel aufweisen. Die Tabelle 1 zeigt die Speichererfordernisse für verschiedene Größen von Schlüsseln.

Tabelle 1: Zahl von Bytes zum Speichern unabhängiger Dienstschlüssel

Von Kanälen mit unabhängigen Schlüsseln	Kanal-ID (3 Bytes)	16 Byte-Dreifach-DES-Verschlüsselter-Dienst-Schlüssel	16 Byte-Dreifach-DES-Verschlüsselter-Dienst-Schlüssel	Summe der Bytes
		LAUFEND	NÄCHSTER	
20	60	320	320	700
50	150	800	800	1.750
100	300	1600	1600	3.500
200	600	3200	3200	7.000
400	1200	6400	6400	14.000

[0063] Dienste können à la Carte verkauft oder als ein Bouquet oder Packet verkauft werden. Es kann mehrere Ränge bzw. Netzebenen von Diensten geben. Beispielsweise kann es, wie in Fig. 9 gezeigt, eine Basisnetzebene von Diensten, eine mittlere Netzebene, die mehrere Dienste anbietet, und fortgeschrittene bzw. vorgesetzte Netzebenen, die verschiedene Prämien- bzw. Premiumdienste anbieten, geben. Bei dieser Ausführungsform kann jeder Zuwachsnetzebene von Diensten ein separater Schlüssel gegeben sein.

[0064] Wenn von der obigen Tabelle 1 ein Kunde bei 20 verschiedenen Typen von Dienstnetzebenen teilnehmen würde, würde dies 60 Bytes ID-Speicher, 320 Bytes Speicher der laufend gültigen Dienstschlüssel, 320 Bytes Speicher für die für die nächste Epoche (oder Rechnungserstellungsperiode) gültigen Dienstschlüssel erfordern, für eine Summe von 700 Bytes.

[0065] Typischerweise müssen ECMs die zum Zugriff auf einen Kanal zusammen mit der Kanal- oder Dienst-ID-Information (Channel or Service ID information) und Steuerungs-Wort-(Schlüssel)information benötigten Zugriffsbedingungen bzw. Zugriffs-Bedingungen (Access Condition) transportieren. Bei dieser Ausführungsform können die EMCs vereinfacht sein. Nur die Kanal- oder Dienst-ID-Information und möglicherweise ein Programm-ID (Program ID), wenn es ein IPPV- oder VOD-Programm ist, muss bzw. müssen in der ECM enthalten sein. Dies deswegen, weil keine ECM-Verarbeitung anders als die Identifizierung des geeigneten verschlüsselten Schlüssels vom Speicher und seine Verwendung zum Schreiben und seine Verwendung zum Schreiben desselben in das geeignete Register der Entwürfler-IC ausgeführt werden muss.

[0066] Fig. 10 zeigt eine Ausführungsform eines Verfahrens zur Anforderung und zum Empfang von Dienstschlüsseln. Programminformation wird von der Kopfstelle des Decodierers kontinuierlich gesendet, Schritte **1010** und **1015**. Ein Zuschauer wählt dann einen Kanal zum Zuschauen, Schritt **1020**. Der Decodierer fordert einen Dienstschlüssel von der Kopfstelle an, Schritt **1025**. Die Kopfstelle prüft den Teilnehmerstatus des Decodierers, Schritt **1030**. Wenn der Decodierer Teilnehmer ist, stellt die Kopfstelle den Dienstschlüssel dem Decodierer bereit, Schritt **1055**. Wenn der Decodierer nicht Teilnehmer ist, wird der Zuschauer vom Decodierer aufgefordert, teilzunehmen, Schritt **1035**. Der Zuschauer entscheidet sich zur Teilnahme, Schritt **1040**. Der Decodierer sendet eine Anforderung zum Kauf zur Kopfstelle, Schritt **1045**. Die Kopfstelle sendet einen verschlüsselten Dienstschlüssel zum Decodierer, Schritt **1050**.

[0067] Infolgedessen weist bei dieser Ausführungsform der Decodierer eine Entwürfler-IC mit einem einzigen Schlüssel auf. Dienstschlüssel werden vom Entwürfler-IC-Einzig-Schlüssel verschlüsselt an den Decodierer **701** abgegeben und in verschlüsselter Form im Decodierer gespeichert. Alternativ dazu könnte der Decodierer jedesmal einen Dienstschlüssel anfordern, wenn der Decodierer auf einen Kanal abstimmt, ohne Dienstschlüssel lokal zu speichern. Die vom sicheren Verschlüsselungsprozessor normalerweise gehaltenen Berechtigungen werden von der kontrollierenden bzw. steuernden Autorität, beispielsweise ein Schlüsselserver in der Kopfstelle, gehalten. Der unsichere Prozessor **730** im Decodierer **701** kann eine Meldung empfangen (beispielsweise eine ECM oder EMM), die ihm sagt, was autorisiert ist, zu entwürfeln, so dass er einem Zuschauer Zuschauoptionen richtig anzeigen kann. Der Prozessor **730** kann dann Dienstschlüssel für gewählte Kanäle anfordern. Bei dieser Ausführungsform gibt es keine eingebettete „sichere" Firmware oder Software. Bei Verwendung der oben erwähnten Hardwareverschlüsselungsschaltung wird ein eingebetteter CPU-Kern oder eine eingebettete Firmware, der bzw. die eine Verschlüsselungsfunktion ausführt, nicht benötigt. Dies ermöglicht eine Anzahl von Bedingtzugriffsanwendungen, die zum unsicheren Prozessor heruntergeladen werden können. Der Dienstschlüssel ist einheitsschlüsselverschlüsselt. Er kann ein öffentlicher asymmetrischer Schlüssel oder ein geheimer symmetrischer Schlüssel sein.

[0068] Zusätzliche Vorteile umfassen Pay-TV-Anwendungen ohne Verwendung eines Verschlüsselungsprozessors durch Bereitstellen eines Decodierers, der eine Entwürfler-IC mit in die IC festverdrahteten einzigen Schlüsseln aufweist. Der Decodierer kann einen Dienstschlüssel oder ein Steuerungswort von einem Netzwerkprovider anfordern. Eine Lokal-Zugriffs-Steuerung kann vom unsichere Prozessor ausgeführt werden, da die kritische „sichere" Funktion in der Entwürfler-IC isoliert ist.

[0069] Bei der vorstehenden Beschreibung ist die Erfindung in Bezugnahme auf spezifische exemplarische Ausführungsformen derselben beschrieben. Es ist jedoch evident, dass verschiedene Modifikationen und Änderungen bei ihr ohne Verlassen des wie in den beigefügten Ansprüchen dargelegten Schutzbereichs der vorliegenden Erfindung gemacht werden können. Die Beschreibung und Zeichnungen sind demgemäss in einem illustrativen und nicht in einem restriktiven Sinn zu betrachten.

Patentansprüche

1. Verfahren zum Entwürfeln verwürfelten digitalen Inhalts, aufweisend:
permanentes Speichern eines Schlüssels in einem nichtflüchtigen Register einer Entwürflerintegriertschaltung (**440**,**740**) während der Herstellung,
Empfangen des verwürfelten digitalen Inhalts in der Entwürflerintegriertschaltung (**440**,**740**),
Empfangen eines verschlüsselten Steuerungsworts in der Entwürflerintegriertschaltung (**440**,**740**),
Entschlüsseln des verschlüsselten Steuerungsworts unter Verwendung des im nicht-flüchtigen Register permanent gespeicherten Schlüssels, der in einem nichtflüchtigen Register der Entwürflerintegriertschaltung (**440**, **740**) gespeichert worden ist, und
Entwürfeln des verwürfelten digitalen Inhalts in der Entwürflerintegriertschaltung (**440**,**740**) unter Verwendung des entschlüsselten Steuerungsworts, wobei die Entwürflerintegriertschaltung eine nicht-CPU-, nicht-Firmware- und nicht-Softwarebasierte integrierte Schaltung ist.

2. Verfahren nach Anspruch 1, wobei der Empfang des verwürfelten digitalen Inhalts
Empfangen einer den verwürfelten digitalen Inhalt enthaltenden Fernsehübertragung aufweist.

3. Verfahren nach Anspruch 1, wobei der Empfang des verwürfelten digitalen Inhalts
Herunterladen des verwürfelten digitalen Inhalts vom Internet aufweist

4. Verfahren nach Anspruch 1, wobei die Entschlüsselung des verschlüsselten Steuerungsworts unter Verwendung eines in der Entwürflerintegriertschaltung (**440**, **740**) gespeicherten Schlüssels
Entschlüsseln des Steuerungsworts unter Verwendung von Triple-DES umfasst.

5. Verfahren nach Anspruch 1, wobei der Empfang des verschlüsselten Steuerungsworts in der Entwürflerintegriertschaltung (**440**, **740**)
Empfangen des verschlüsselten Steuerungsworts von einer Chipkarte (**410**) aufweist.

6. Verfahren nach Anspruch 5, außerdem mit
Verschlüsseln des Steuerungsworts in der Chipkarte (**410**) unter Verwendung eines in einer Registerschaltung (**412**) der Chipkarte gespeicherten Schlüssels, wobei
der in der Registerschaltung (**412**) der Chipkarte gespeicherte Schlüssel ein einem in einer Registerschaltung

(**450**) der Entwürflerintegriertschaltung (**440**) gespeicherten Schlüssel zugeordnet ist.

7. Verfahren nach Anspruch 1, wobei der Empfang eines verschlüsselten Steuerungsworts in der Entwürflerintegriertschaltung (**440**,**740**)
Empfangen des verschlüsselten Steuerungsworts von einer durch ein Netz (**720**) mit der Entwürflerintegriertschaltung (**440**,**740**) verbundenen Steuerungsentität (**710**) umfasst.

8. Verfahren nach Anspruch 1, wobei die Steuerungsentität (**710**) von einem Kopfstellenserver, einer Aufwärtsstrecke oder einer Rundfunkstation eine ist.

9. Verfahren nach Anspruch 7, mit
Verschlüsseln eines Steuerungsworts in der Steuerungsentität unter Verwendung eines dem in der Registerschaltung (**750**) der Entwürflerintegriertschaltung (**740**) gespeicherten Schlüssel zugeordneten Schlüssels.

10. Verfahren nach Anspruch 1, wobei der Empfang des verschlüsselten Steuerungsworts in der Entwürflerintegriertschaltung (**440**,**740**) Empfangen des verschlüsselten Steuerungsworts in einem Modul (**401**) aufweist.

11. Verfahren nach Anspruch 10, wobei das Modul (**401**) von einem NRSS-A-Modul, einem NRSS-B-Modul, einem POD-Modul und einem anderen CA-Element eines ist.

12. Gerät zur Entwürfelung verwürfelten digitalen Inhalts, aufweisend:
eine Entwürflerintegriertschaltung, wobei die Entwürflerintegriertschaltung geeignet ist zum
Empfangen (**111**) verwürfelten digitalen Inhalts und
Empfangen (**410**, **420**, **720**, **725**) eines verschlüsselten Steuerungsworts, wobei die Entwürflerintegriertschaltung aufweist:
eine Einrichtung zur Entschlüsselung (**410**, **420**, **720**, **760**) des verschlüsselten Steuerungsworts unter Verwendung eines Schlüssels, der in einem nicht-flüchtigen Register der Entwürflerintegriertschaltung (**440**,**740**) während der Herstellung permanent gespeichert worden ist, und
eine Einrichtung zur Entwürfelung (**470**, **770**) des verwürfelten digitalen Inhalts in der Entwürflerintegriertschaltung unter Verwendung des entschlüsselten Steuerungsworts, wobei die Entwürflerintegriertschaltung eine nicht-CPU-, nicht-Firmware- und nicht-Software-basierte integrierte Schaltung ist.

13. Gerät nach Anspruch 12, aufweisend eine
Einrichtung zum Empfang einer den verwürfelten digitalen Inhalt enthaltenden Fernsehübertragung.

14. Gerät nach Anspruch 12, aufweisend eine
Einrichtung zum Herunterladen des verwürfelten digitalen Inhalts vom Internet.

15. Gerät nach Anspruch 12, wobei die Einrichtung zur Entschlüsselung des einen in der Entwürflerintegriertschaltung (**440**, **740**) gespeicherten verschlüsselten Steuerungsworts Triple-DES verwendet.

16. Gerät nach Anspruch 12, wobei die Entwürflerintegriertschaltung geeignet ist zum Empfang des verschlüsselten Steuerungsworts von einer Chipkarte (**410**).

17. System zur Übertragung digitalen Inhalts, wobei das System aufweist:
eine Einrichtung zur Übertragung des verwürfelten digitalen Inhalts zu einem Gerät zur Enwürfelung des verwürfelten digitalen Inhalts, wobei das Gerät
eine Entwürflerintegriertschaltung aufweist, wobei die integrierte Entwürflerintegriertschaltung geeignet ist zum Empfangen des verwürfelten digitalen Inhalts und zum
Empfangen eines verschlüsselten Steuerungsworts, wobei die Entwürflerintegriertschaltung
eine Einrichtung zur Entschlüsselung (**440**, **460**, **740**, **760**) des verschlüsselten Steuerungsworts unter Verwendung eines Schlüssels, der in einem nicht-flüchtigen Register der Entwürflerintegriertschaltung (**440**, **740**) während der Herstellung permanent gespeichert worden ist, und
eine Einrichtung zur Entwürfelung (**470**, **770**) des verwürfelten digitalen Inhalts in der Entwürflerintegriertschaltung unter Verwendung des verschlüsselten Steuerungsworts, wobei die Entwürflerintegriertschaltung eine nicht-CPU-, nicht-Firmware- und nicht-Software-basierte integrierte Schaltung ist, aufweist.

18. System nach Anspruch 17, aufweisend eine Chipkarte und
eine Einrichtung zur Verschlüsselung (**414**) des Steuerungsworts (CW) in der Chipkarte unter Verwendung ei-

nes in einer Registerschaltung (**412**) der Chipkarte gespeicherten Schlüssels, wobei die Entwürflerintegriertschaltung (**440**, **740**) geeignet ist zum
Empfangen des verschlüsselten Steuerungsworts von der Chipkarte (**410**),
wobei der in der Registerschaltung (**412**) gespeicherte Schlüssel der Chipkarte (**410**) einem in einer Registerschaltung (**412**) der Entwürflerintegriertschaltung (**440**) gespeicherten Schlüssel zugeordnet ist.

19. System nach Anspruch 17, aufweisend
eine Einrichtung zur Übertragung des verschlüsselten Steuerungsworts von einer mit der Entwürflerintegriertschaltung (**740**) verbundenen Steuerungsentität (**710**) über ein Netz (**720**).

20. System nach Anspruch 19, wobei die Steuerungsentität (**710**) von einem Kopfstellenserver, einer Aufwärtsstrecke oder einer Rundfunkstation eine ist.

21. System nach Anspruch 19, wobei die Steuerungsentität (**710**)
eine Einrichtung zur Verschlüsselung eines Steuerungsworts in der Steuerungsentität unter Verwendung eines dem in der Registerschaltung (**750**) der Entwürflerintegriertschaltung (**740**) gespeicherten Schlüssel zugeordneten Schlüssels.

22. System nach Anspruch 20, aufweisend ein Modul (**401**) zur Übertragung des verschlüsselten Steuerungsworts zur Entwürflerintegriertschaltung.

23. System nach Anspruch 22, wobei das Modul (**401**) von einem NRSS-A-Modul, einem NRSS-B-Modul, einem POD-Modul und einem anderen CA-Element eines ist.

Es folgen 9 Blatt Zeichnungen

Anhängende Zeichnungen

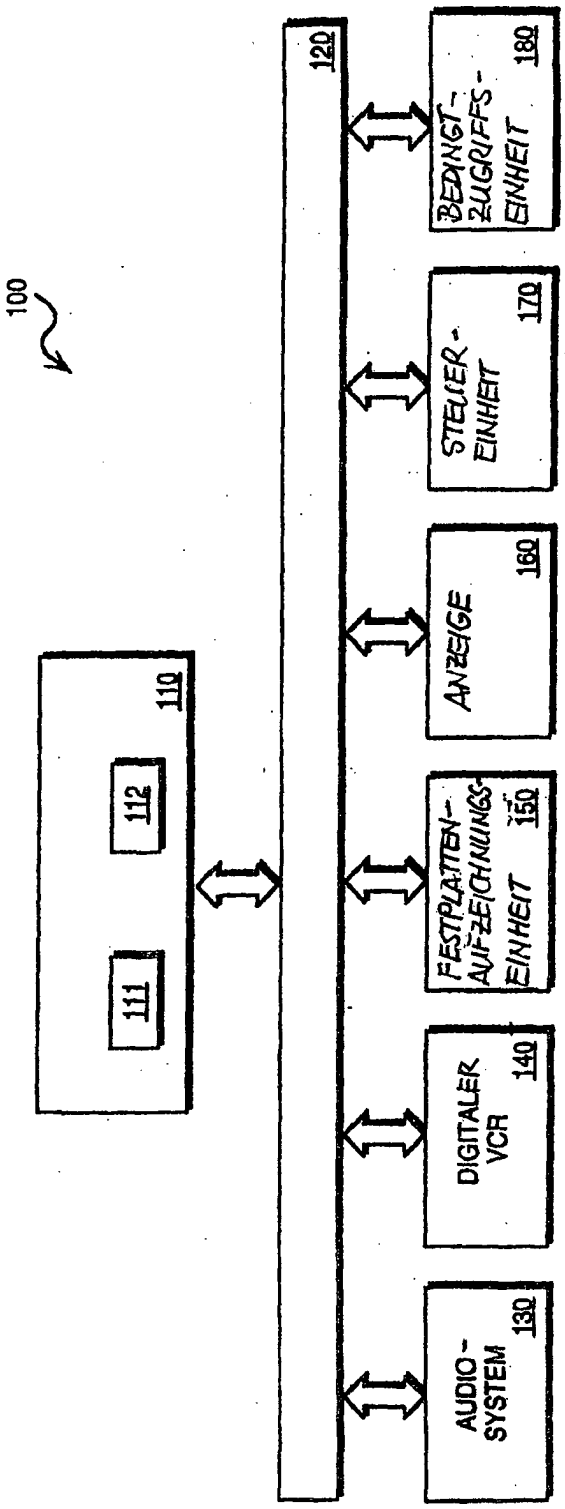

FIG. 1

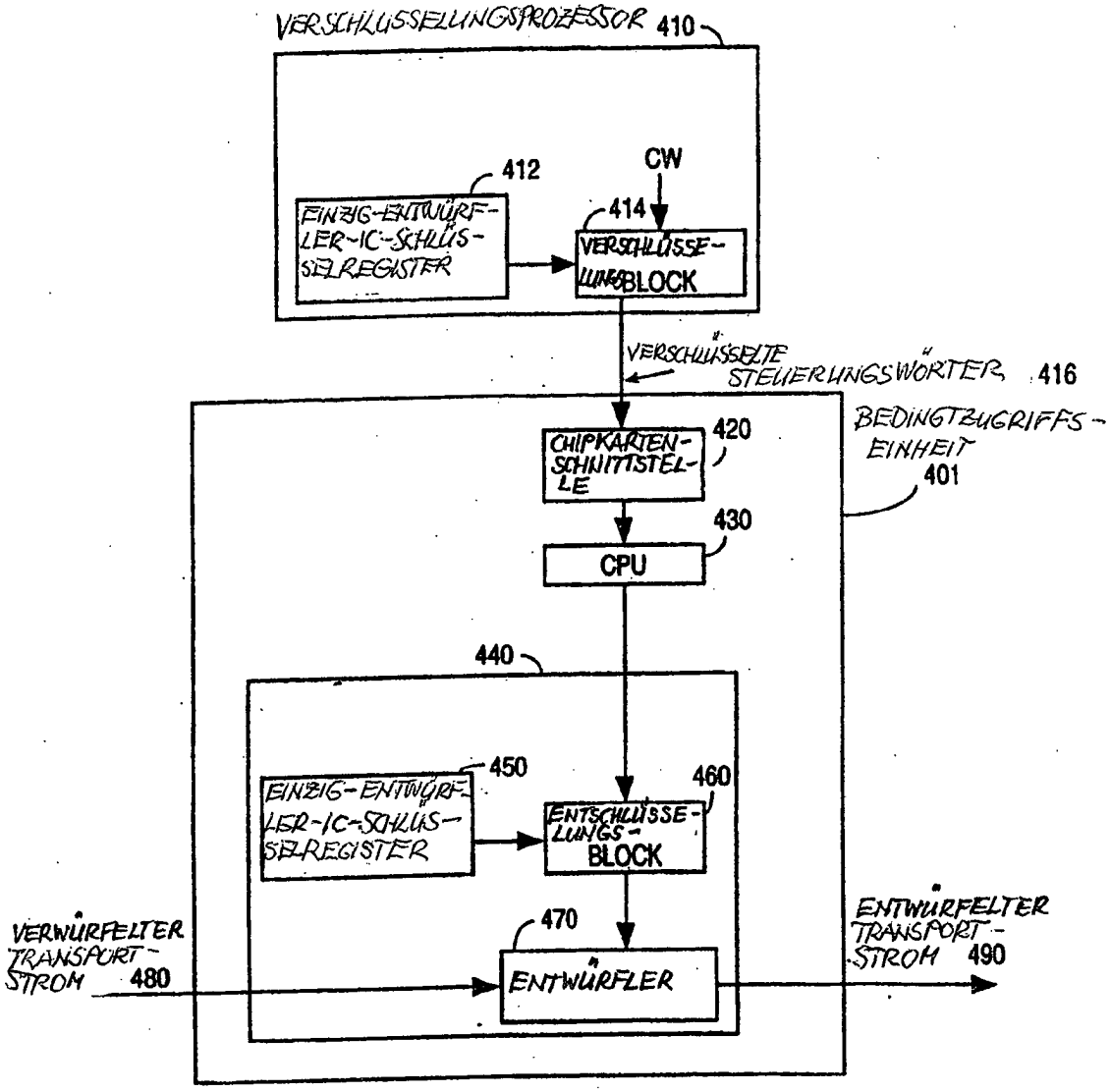
VERSCHLÜSSELUNGSPROZESSOR 410
412
CW
EINZIG-ENTWÜRFLER-IC-SCHLÜSSELREGISTER
414
VERSCHLÜSSELUNGSBLOCK
VERSCHLÜSSELTE STEUERUNGSWÖRTER 416
BEDINGTZUGRIFFS-EINHEIT 401
CHIPKARTEN-SCHNITTSTELLE 420
430
CPU
440
450
460
EINZIG-ENTWÜRFLER-IC-SCHLÜSSELREGISTER
ENTSCHLÜSSELUNGS-BLOCK
470
ENTWÜRFLER
VERWÜRFELTER TRANSPORT-STROM 480
ENTWÜRFELTER TRANSPORT-STROM 490

FIG. 2

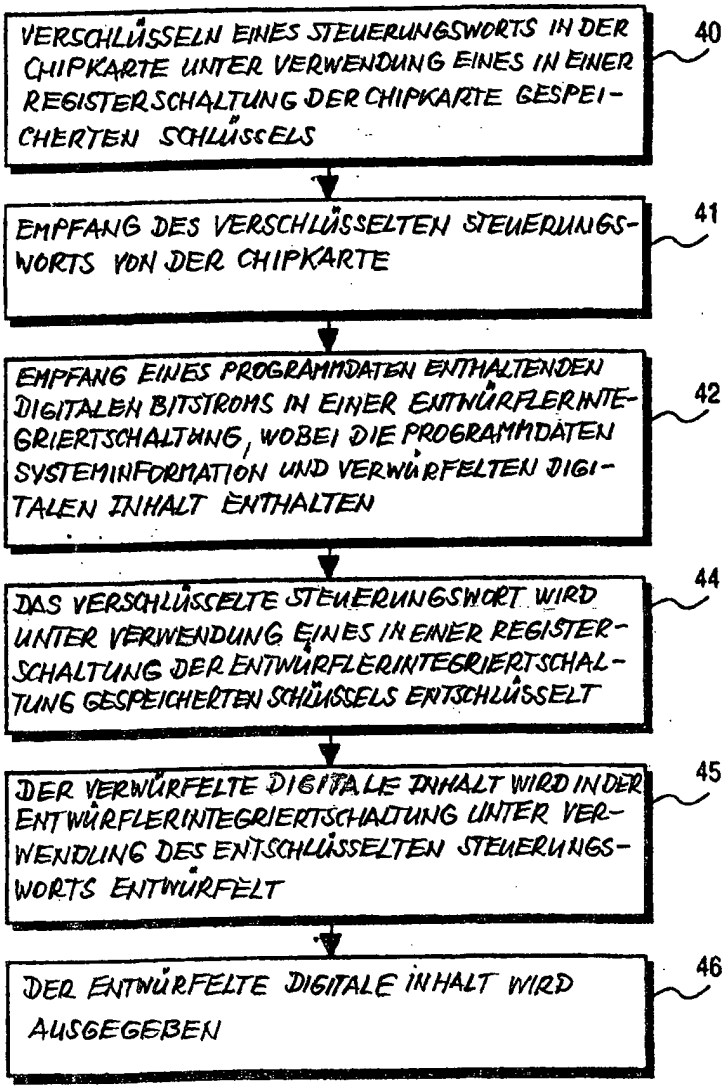
VERSCHLÜSSELN EINES STEUERUNGSWORTS IN DER CHIPKARTE UNTER VERWENDUNG EINES IN EINER REGISTERSCHALTUNG DER CHIPKARTE GESPEICHERTEN SCHLÜSSELS
40
EMPFANG DES VERSCHLÜSSELTEN STEUERUNGSWORTS VON DER CHIPKARTE
41
EMPFANG EINES PROGRAMMDATEN ENTHALTENDEN DIGITALEN BITSTROMS IN EINER ENTWÜRFLERINTEGRIERTSCHALTUNG, WOBEI DIE PROGRAMMDATEN SYSTEMINFORMATION UND VERWÜRFELTEN DIGITALEN INHALT ENTHALTEN
42
DAS VERSCHLÜSSELTE STEUERUNGSWORT WIRD UNTER VERWENDUNG EINES IN EINER REGISTERSCHALTUNG DER ENTWÜRFLERINTEGRIERTSCHALTUNG GESPEICHERTEN SCHLÜSSELS ENTSCHLÜSSELT
44
DER VERWÜRFELTE DIGITALE INHALT WIRD IN DER ENTWÜRFLERINTEGRIERTSCHALTUNG UNTER VERWENDUNG DES ENTSCHLÜSSELTEN STEUERUNGSWORTS ENTWÜRFELT
45
DER ENTWÜRFELTE DIGITALE INHALT WIRD AUSGEGEBEN
46

FIG. 3

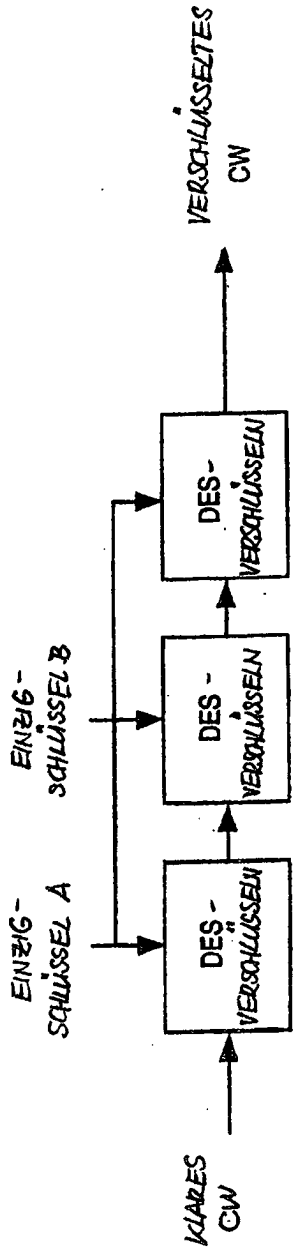
KLARES CW
EINZEL-SCHLÜSSEL A
EINZEL-SCHLÜSSEL B
DES-VERSCHLÜSSELN
DES-VERSCHLÜSSELN
DES-VERSCHLÜSSELN
VERSCHLÜSSELTES CW

FIG. 4

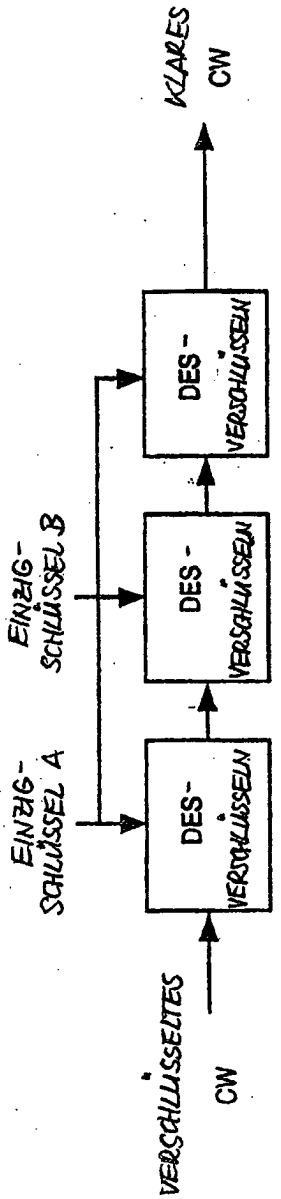
VERSCHLÜSSELTES CW
EINZEL-SCHLÜSSEL A
EINZEL-SCHLÜSSEL B
DES-VERSCHLÜSSELN
DES-VERSCHLÜSSELN
DES-VERSCHLÜSSELN
KLARES CW

FIG. 5

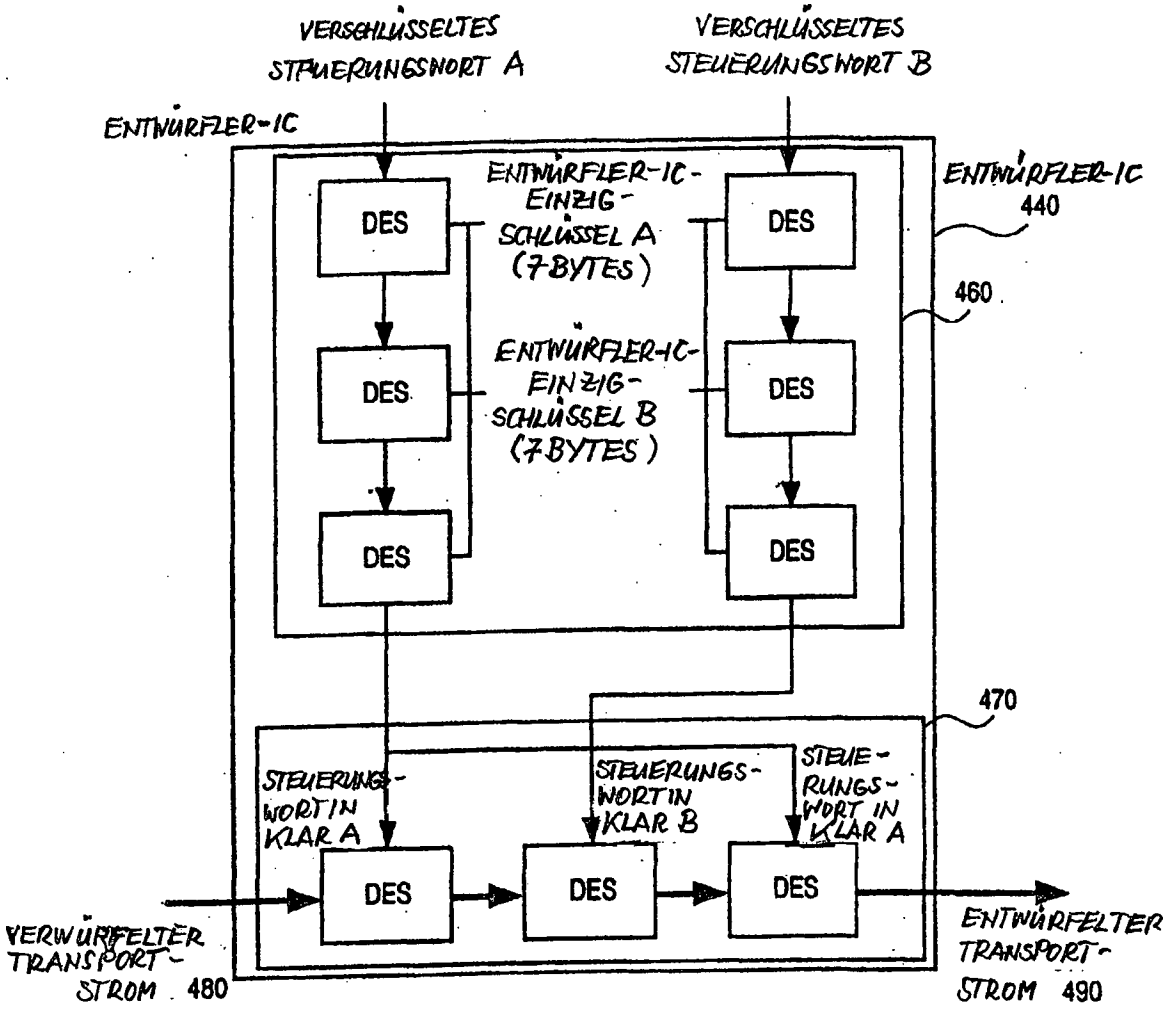
VERSCHLÜSSELTES STEUERUNGSWORT A
VERSCHLÜSSELTES STEUERUNGSWORT B
ENTWÜRFLER-IC
ENTWÜRFLER-IC-EINZIG-SCHLÜSSEL A (7 BYTES)
ENTWÜRFLER-IC-EINZIG-SCHLÜSSEL B (7 BYTES)
ENTWÜRFLER-IC
440
460
470
DES
STEUERUNGSWORT IN KLAR A
STEUERUNGSWORT IN KLAR B
STEUERUNGSWORT IN KLAR A
VERWÜRFELTER TRANSPORTSTROM 480
ENTWÜRFELTER TRANSPORTSTROM 490

FIG. 6

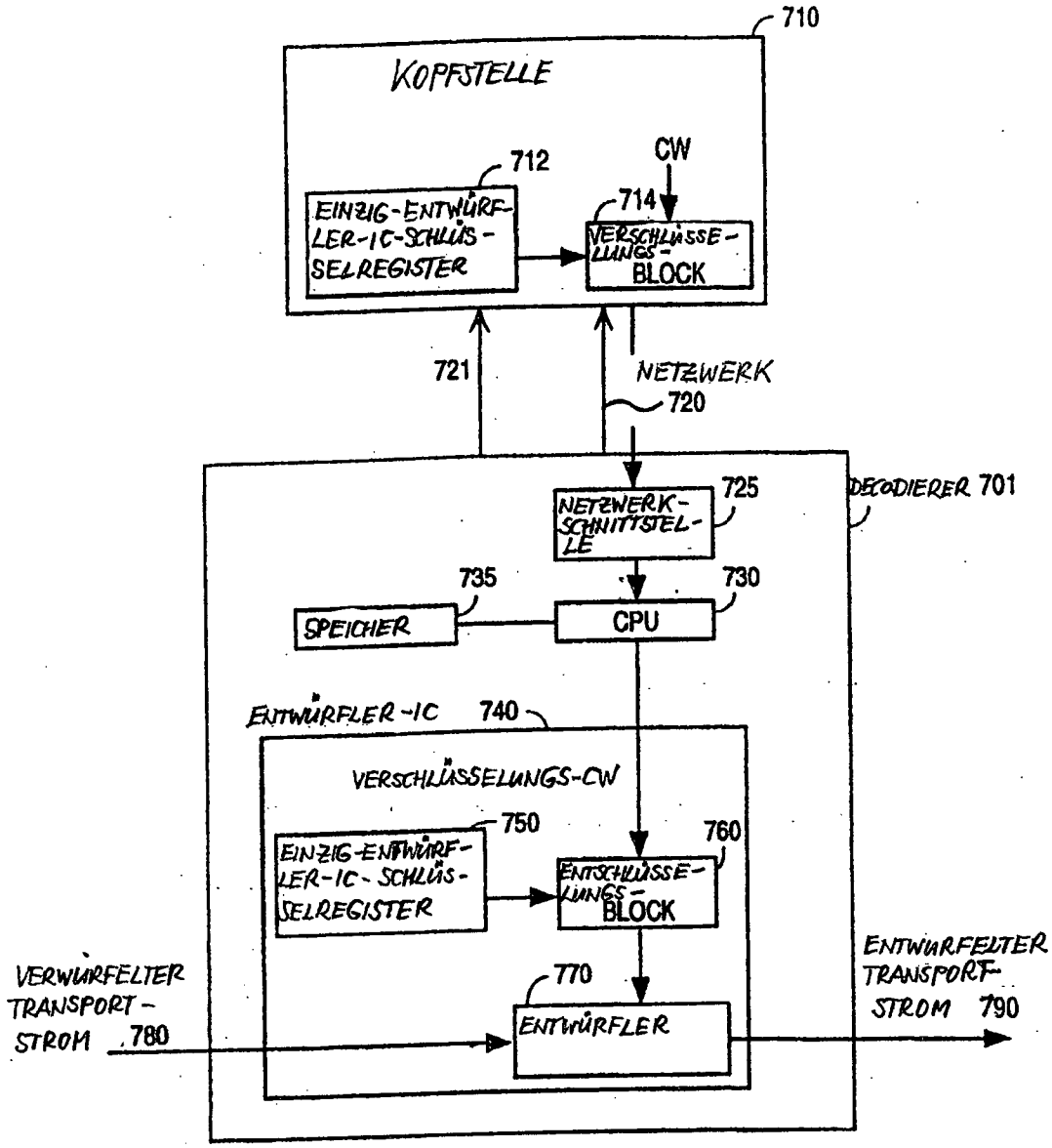
710
KOPFSTELLE
712
CW
714
EINZIG-ENTWÜRFLER-IC-SCHLÜSSELREGISTER
VERSCHLÜSSELUNGS-BLOCK
721
NETZWERK
720
DECODIERER 701
725
NETZWERK-SCHNITTSTELLE
735
730
SPEICHER
CPU
ENTWÜRFLER-IC 740
VERSCHLÜSSELUNGS-CW
750
760
EINZIG-ENTWÜRFLER-IC-SCHLÜSSELREGISTER
ENTSCHLÜSSELUNGS-BLOCK
770
ENTWÜRFLER
VERWÜRFELTER TRANSPORT-STROM 780
ENTWÜRFELTER TRANSPORT-STROM 790

FIG. 7

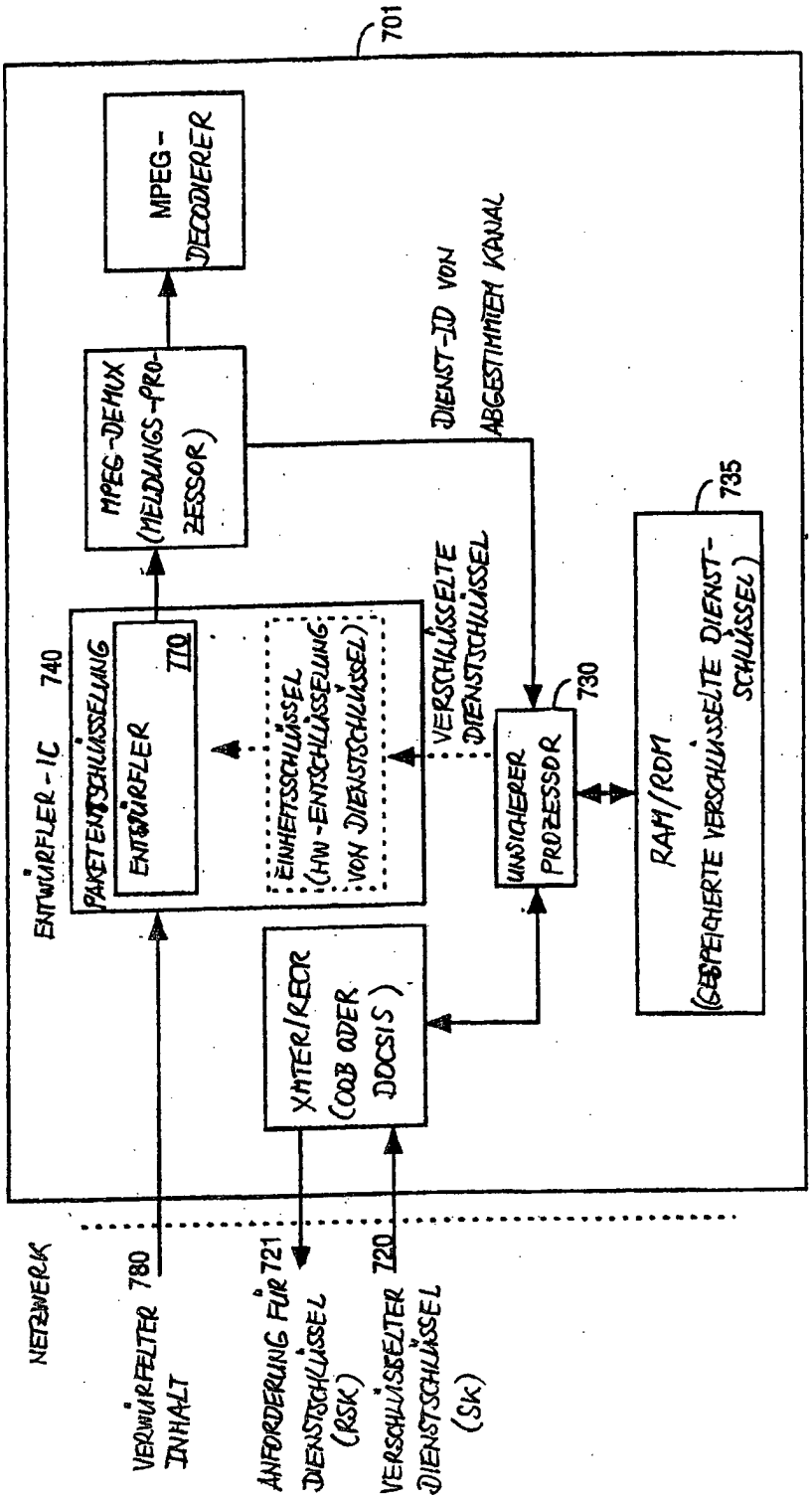
701
MPEG-DECODIERER
MPEG-DEMUX (MELDUNGS-PROZESSOR)
DIENST-ID VON ABGESTIMMTEM KANAL
ENTWÜRFLER-IC 740
PAKETENTSCHLÜSSELUNG
ENTWÜRFLER 770
EINHEITSSCHLÜSSEL (HW-ENTSCHLÜSSELUNG VON DIENSTSCHLÜSSEL)
VERSCHLÜSSELTE DIENSTSCHLÜSSEL
UNSICHERER PROZESSOR 730
RAM/ROM (GESPEICHERTE VERSCHLÜSSELTE DIENSTSCHLÜSSEL) 735
XMTER/RECR (COAB ODER DOCSIS)
NETZWERK
VERWÜRFELTER INHALT 780
ANFORDERUNG FÜR DIENSTSCHLÜSSEL (RSK) 721
VERSCHLÜSSELTER DIENSTSCHLÜSSEL (SK) 720

FIG. 8

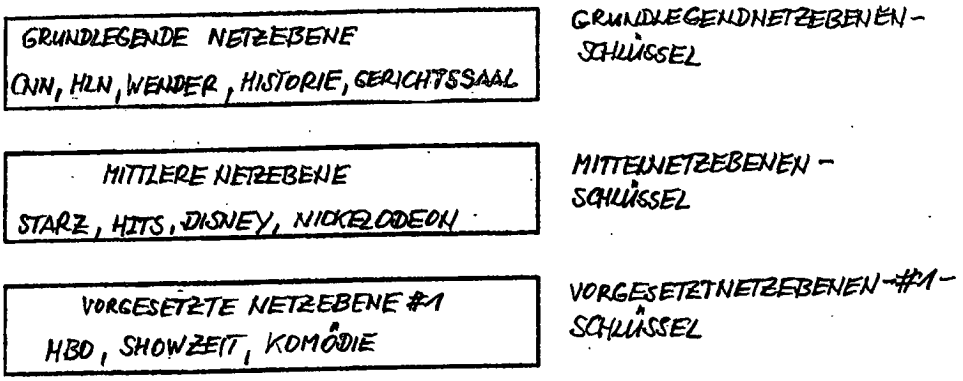
GRUNDLEGENDE NETZEBENE
CNN, HLN, WEATHER, HISTORIE, GERICHTSSAAL
GRUNDLEGENDNETZEBENEN-SCHLÜSSEL
MITTLERE NETZEBENE
STARZ, HITS, DISNEY, NICKELODEON
MITTELNETZEBENEN-SCHLÜSSEL
VORGESETZTE NETZEBENE #1
HBO, SHOWZEIT, KOMÖDIE
VORGESETZTNETZEBENEN-#1-SCHLÜSSEL

FIG. 9

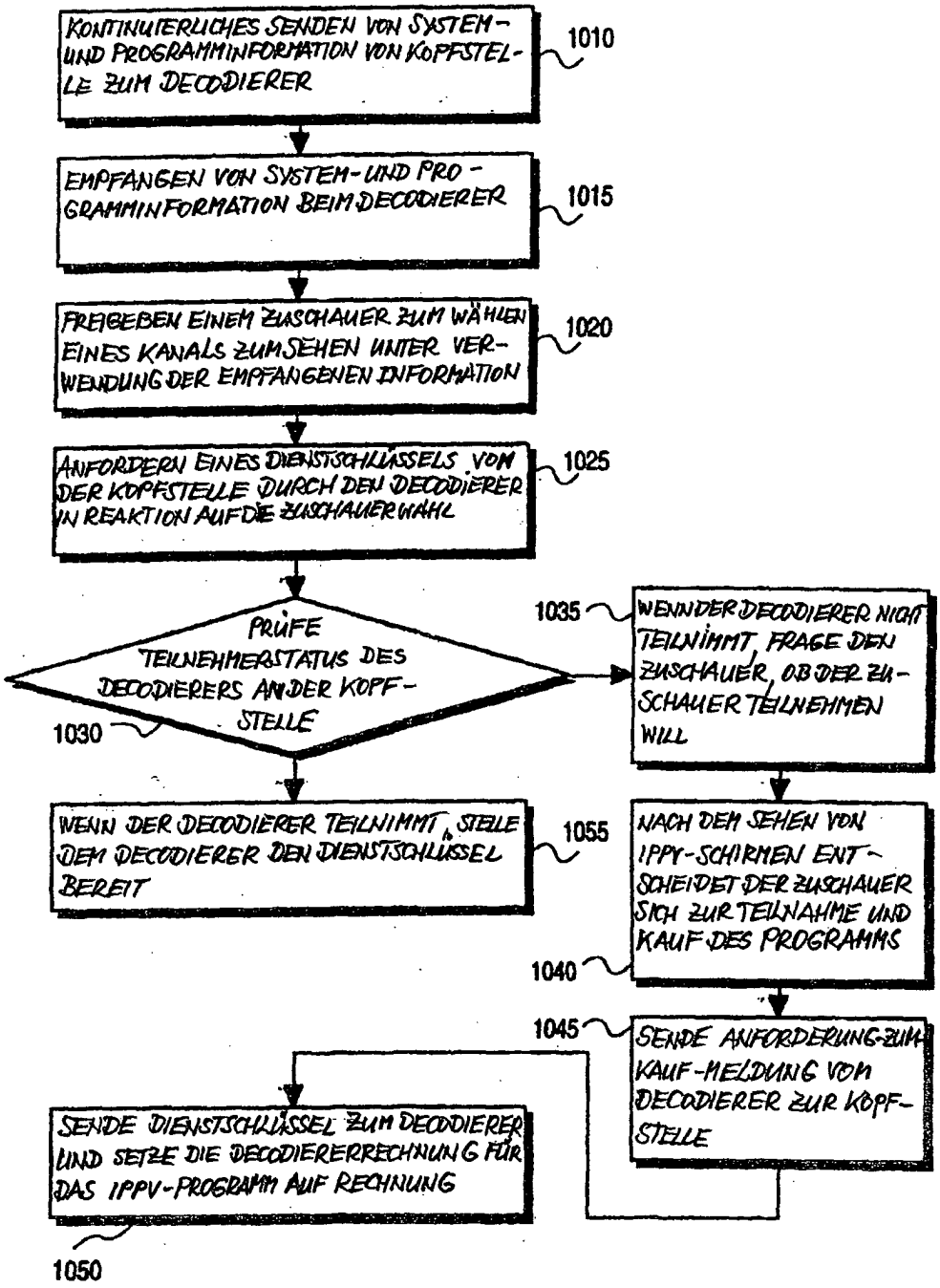
KONTINUIERLICHES SENDEN VON SYSTEM- UND PROGRAMMINFORMATION VON KOPFSTELLE ZUM DECODIERER
1010
EMPFANGEN VON SYSTEM- UND PROGRAMMINFORMATION BEIM DECODIERER
1015
FREIGEBEN EINEM ZUSCHAUER ZUM WÄHLEN EINES KANALS ZUM SEHEN UNTER VERWENDUNG DER EMPFANGENEN INFORMATION
1020
ANFORDERN EINES DIENSTSCHLÜSSELS VOM DER KOPFSTELLE DURCH DEN DECODIERER IN REAKTION AUF DIE ZUSCHAUERWAHL
1025
PRÜFE TEILNEHMERSTATUS DES DECODIERERS AN DER KOPFSTELLE
1030
1035
WENN DER DECODIERER NICHT TEILNIMMT, FRAGE DEN ZUSCHAUER, OB DER ZUSCHAUER TEILNEHMEN WILL
WENN DER DECODIERER TEILNIMMT, STELLE DEM DECODIERER DEN DIENSTSCHLÜSSEL BEREIT
1055
NACH DEM SEHEN VON IPPV-SCHIRMEN ENTSCHEIDET DER ZUSCHAUER SICH ZUR TEILNAHME UND KAUF DES PROGRAMMS
1040
1045
SENDE ANFORDERUNG-ZUM-KAUF-MELDUNG VON DECODIERER ZUR KOPFSTELLE
SENDE DIENSTSCHLÜSSEL ZUM DECODIERER UND SETZE DIE DECODIERERRECHNUNG FÜR DAS IPPV-PROGRAMM AUF RECHNUNG
1050

FIG. 10