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

(10) **DE 60 2004 003 346 T2** 2007.05.31

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 595 399 B1**
(21) Deutsches Aktenzeichen: **60 2004 003 346.4**
(86) PCT-Aktenzeichen: **PCT/EP2004/050060**
(96) Europäisches Aktenzeichen: **04 706 694.9**
(87) PCT-Veröffentlichungs-Nr.: **WO 2004/071087**
(86) PCT-Anmeldetag: **30.01.2004**
(87) Veröffentlichungstag der PCT-Anmeldung: **19.08.2004**
(97) Erstveröffentlichung durch das EPA: **16.11.2005**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **22.11.2006**
(47) Veröffentlichungstag im Patentblatt: **31.05.2007**

(51) Int Cl.[8]: ***H04N 7/16*** (2006.01)
H04N 7/167 (2006.01)

(30) Unionspriorität:
0301243 **04.02.2003** **FR**

(73) Patentinhaber:
NAGRA THOMSON LICENSING, Boulogne-Billancourt, FR

(74) Vertreter:
Diehl & Partner GbR, 80333 München

(84) Benannte Vertragsstaaten:
DE, ES, FR, GB, IT

(72) Erfinder:
DAUVOIS, Jean-Luc, F-75116 Paris, FR

(54) Bezeichnung: **PAY-FERNSEHEN, VERFAHREN ZUM ENTZIEHEN VON RECHTEN IN EINEM SOLCHEN SYSTEM, ASSOZIIERTER DECODER UND CHIPKARTE UND AN EINEN SOLCHEN DECODER ÜBERTRAGENE NACHRICHT**

Beschreibung

TECHNISCHER BEREICH

[0001] Die vorliegende Erfindung betrifft ein Zahl-Fernsehsystem, ein Verfahren zur Rücknahme von Rechten in einem solchen System, einen zugeordneten Decodierer und eine zugeordnete Chipkarte und eine zu einem solchen Decodierer übertragene Nachricht. In solchen Zahl-Fernsehsystemen können zwei sehr bekannte Arten der Vermittlung von audiovisuellen Programmen entweder getrennt oder zusammen existieren.

[0002] Bei einer ersten Art ist die Teilnahme und/oder die Zahlung eine Vorbedingung für den unverschlüsselten Zutritt zu den audiovisuellen Programmen. In diesem Fall muss sich der Teilnehmer einschreiben und periodisch, beispielsweise jeden Monat, eine Teilnahmegebühr bezahlen, um auf die auf einem oder mehreren Kanälen ausgestrahlten audiovisuellen Programmen zuzugreifen.

[0003] Bei einer zweiten Art wird das vorübergehende entwürfelte (in angelsächsischer Terminologie "descrambled") Vorvisualisierungsangebot vor Abonnierung oder Zahlung gemacht. In diesem Fall wird der Teilnehmer beispielsweise durch eine Nachricht auf seinem Bildschirm informiert, dass ihm ein kostenloser und entschlüsselter (d.h. entwürfelter) Zugang zu einem laufenden oder zukünftigen Programm zu Vorvisualisierungszwecken gewährt wird, oder der Teilnehmer verlangt diesen Zugang. Der Teilnehmer kann auf diese Weise vorübergehend während eines relativ kurzen Zeitraums ein Programm auf einem gegebenen Kanal unverschlüsselt visualisieren. Wenn der Teilnehmer das Programm weiter visualisieren möchte, muss er vor Ablauf dieser Frist eine Zahlungstransaktion, beispielsweise über Modem gemäß einem "Pay-Per-View" (Bezahlen, um zu sehen) oder "Impulsive-Pay-Per-View" (Bezahlen, um impulsiv zu sehen) genannten Schema gemäß dem Fachmann bekannten Mechanismen durchführen. Wenn diese Transaktion nicht vor Ablauf der Frist durchgeführt wird, wird der kostenlose und unverschlüsselte Zugang zum Programm unterbrochen und, das Programm erscheint nun auf dem Fernsehschirm des Teilnehmers verwürfelt.

[0004] Die Erfindung ist insbesondere auf die beiden oben genannten Arten anwendbar, wird aber im Besonderen im Rahmen der zweiten Art beschrieben.

[0005] In der vorliegenden Anmeldung bezeichnet der Ausdruck "audiovisuelles Programm" jedes Video- und/oder Audioprogramm.

STAND DER TECHNIK

[0006] Die im Zahl-Fernsehen verwendeten Techniken beruhen auf zwei voneinander unabhängigen Mechanismen: einerseits auf einer Verwürfelung/Verschlüsselung des bzw. der Video- und/oder Audioprogramme, andererseits auf einer Funktion der Zuteilung von kommerziellen Rechten, die als gesicherte Nachrichten zum Entwürfelungsgerät oder zum Decodierer (mit Kontrollzugang) übertragen werden. Die Verwürfelung/Verschlüsselung kann leicht auf einem digitalen Bitfluss angelegt werden. Alle Bits können verwürfelt/verschlüsselt werden, indem beispielsweise eine Chiffrierung in Blöcken verwendet wird. Die Verwürfelung wird für analoge Sendungen verwendet. Bei Verwendung einer solchen Verwürfelung wird das Format des Signals geändert, die Synchronisierungssignale werden unterdrückt und getrennt in einer verschlüsselten Form übertragen. Das Audiosignal kann in ein digitales Signal umgewandelt werden und dann verschlüsselt werden. Das verschlüsselte digitale Audiosignal kann in das Videosignal eingefügt werden.

[0007] Das übertragene audiovisuelle Programm wird verwürfelt oder verschlüsselt, indem Schlüssel verwendet werden, wobei das verwürfelte oder verschlüsselte audiovisuelle Programm nur entwürfelt oder entschlüsselt werden kann, indem Äquivalente dieser Schlüssel, Kontrollwörter (CW) genannt, verwendet werden. Bei einer symmetrischen Verschlüsselungsart sind die Verschlüsselungs-/Verwürfelungsschlüssel gleich den Kontrollwörtern. Bei der asymmetrischen Verschlüsselungsart sind die Verschlüsselungs-/Verwürfelungsschlüssel von den Kontrollwörtern verschieden. Bei jedem gegebenen audiovisuellen Programm ändern sich die Werte des zu den Decodern übertragenen Kontrollworts periodisch mit einer relativ hohen Frequenz von beispielsweise etwa einer Sekunde. Um die Entschlüsselung bei Empfang des audiovisuellen Programms zu gestatten, werden ECM-Nachrichten zur Kontrolle der Zuordnung von Rechten ("Entitlement Control Messages") und EMM-Nachrichten zur Verwaltung der Zuteilung von Rechten ("Entitlement Management Messages") zu den Decodern übertragen.

[0008] Diese beiden Typen von Nachrichten ECM und EMM können über den Decoder zu einer Chipkarte oder jedem beliebigen tragbaren Objekt, wie einer PCMCIA-Karte, einem Chipschlüssel ..., gesendet werden, das insbesondere Funktionen der Entschlüsselung und Speicherung von Benutzerrechten erfüllt. In der vorliegenden Beschreibung bezeichnet der Ausdruck "Karte" jedes tragbare Objekt, das im Zusammenhang mit dem Decoder arbeitet.

[0009] Die ECM-Nachrichten enthalten verschlüsselte Kontrollwörter, wobei die Kontrollwörter dem Decoder gestatten, ein audiovisuelles Programm zu

entwürfeln/entschlüsseln. Die ECM-Nachrichten werden zur Karte übertragen, die die verschlüsselten Kontrollwörter entschlüsselt und diese Kontrollwörter CW zum Decoder sendet. Die Karte führt die Operation der Entschlüsselung der verschlüsselten Kontrollwörter nur aus, wenn der Benutzer autorisiert ist, auf das laufende Fernsehprogramm zuzugreifen. Hierzu speichert die Karte in einer Zone ihres Speichers die dem betreffenden Benutzer zugeteilten Rechte. Wenn ein Benutzer durch Abonnement einer Chipkarte zugeordnet ist, wird die Zugangsautorisierung durch Daten der Zuteilung von Rechten ("entitlement data") angezeigt, die in der Karte gespeichert sind.

[0010] Die EMM-Nachrichten enthalten Informationen, die die Aktualisierung der Daten der Zuteilung von Rechten des Benutzers gestatten, indem beispielsweise die in der Karte gespeicherten Daten geändert werden. Im Fall eines Angebots einer vorübergehenden entwürfelten Vorvisualisierung und gemäß dem Stand der Technik wird eine erste EMM-Nachricht zum Decoder gesendet, um dem Teilnehmer zeitweise die für den Zugang zu einem Programm auf einem gegebenen Kanal erforderlichen Rechte anzubieten. Wenn von dem System zur Verwaltung der Rechte des Operators keine Zahlungstransaktion empfangen wird, wird eine andere EMM-Nachricht gesendet, um eben diese Rechte zurückzunehmen.

[0011] Die ECM- und EMM-Nachrichten haben ein digitales Signaturfeld, das die Unversehrtheit der Nachricht gewährleistet (beispielsweise einen Hash-Code). Dies gestattet es, jede böswillige oder versehentliche Beschädigung der Inhalte der Nachrichten zu erfassen.

[0012] Eine ECM-Nachricht wird mit dem verwürfelten übertragenen Signal gesendet. Sie umfasst drei Felder. Das erste Feld enthält gewisse Zugangsparameter. Diese Parameter definieren die Bedingungen, unter denen der Zugang zu einem Fernsehprogramm gestattet ist. Dieses Feld macht beispielsweise eine elterliche Beurteilung (hierfür wird von dem Decoder ein zusätzlicher Pincode verlangt) und eine geografische Unterdrückung möglich (ein Film kann nicht in allen europäischen Ländern verfügbar sein). Das zweite Feld enthält ein Kontrollwort in verschlüsselter Form. Dieses Feld enthält Informationen zur Kontrolle der Unversehrtheit der Daten der betreffenden ECM-Nachricht.

[0013] Eine EMM-Nachricht umfasst typischerweise vier Felder. Jede EMM-Nachricht beginnt mit einem Adressfeld, um einen individuellen Decoder auszuwählen. Es gibt zwei Adressierarten, die eine für einen individuellen Decoder und die andere für eine Gruppe von Decodern. Das zweite Feld enthält eine Zuteilung von Rechten für einen gegebenen Benutzer. Das dritte Feld enthält einen Auswertungsschlüssel in verschlüsselter Form. Dieses Feld enthält Informationen zur Kontrolle der Unversehrtheit der Daten der betreffenden EMM-Nachricht. Die EMM-Nachrichten können auch verwendet werden, um zum Decoder einen Befehl zu senden. Die Sendung von EMM-Nachrichten ist im Allgemeinen das Ergebnis einer Aktion (Abonnement) oder eines Fehlens einer Aktion (Nichtzahlung im Modus "Bezahlen mit vorübergehender entwürfelter Vorvisualisierung") des Benutzers gegenüber dem Operator. Diese Nachrichten sind im Allgemeinen individuell. Ihr Inhalt wird von einem Decoder (oder der zugeordneten Karte) oder von einer begrenzten Anzahl von Decodern interpretiert, die von diesen besonderen Rechten betroffen sind. Die EMM-Nachrichten werden nicht synchron mit dem Fernsehprogramm, auf das sie anwendbar sind, gesendet. Sie werden zuvor übertragen, um den Zugang zu einem gegebenen Programm einem autorisierten Benutzer zu gestatten. Für die Übertragung dieser EMM-Nachrichten zum Empfänger kann jedes beliebige Netz verwendet werden: Modem, Mail oder Funk.

[0014] Um sicher zu sein, dass eine EMM-Nachricht von dem Benutzer empfangen wurde, um beispielsweise eine Subskription zu erneuern, wird diese mehrere Male gesendet. Die EMM-Nachrichten werden auf diese Weise zyklisch gemäß einer gegebenen Periode für die Sendung organisiert. Die Dauer einer solchen Periode definiert die maximale Zeit, die abzuwarten ist, um eine Zuteilung von Rechten für einen Benutzer zu erhalten, der seinen Decoder während einer langen Zeit abgeschaltet hat.

[0015] In Fig. 1 sind ein Verwürfler **10**, ein Entwürfler **11**, der typischerweise in einen Decoder (nicht dargestellt) integriert ist, eine Chipkarte **12** sowie ECM- und EMM-Nachrichten dargestellt.

[0016] Die Chipkarte **12** speichert insbesondere:
- eine Kartenadresse, die feststehend ist,
- mindestens einen sk-Auswertungsschlüssel, der periodisch durch EMM aktualisiert wird,
- einen Einzelschlüssel Q, der feststehend ist.

[0017] Wie oben erwähnt wurde, enthält eine ECM-Nachricht drei Felder, die jeweils enthalten:
- die Zugangsparameter,
- ein durch einen Auswertungsschlüssel E_{sk} verschlüsseltes Kontrollwort (CW),
- ein Feld zur Kontrolle der Unversehrtheit der Daten (Hash-Code) der betreffenden ECM-Nachricht.

[0018] Eine EMM-Nachricht enthält vier Felder, die jeweils enthalten:
- eine Adresse,
- die Rechte des Benutzers,
- einen verschlüsselten Auswertungsschlüssels sk: $E_Q(sk)$,

– ein Wort zur Kontrolle der Unversehrtheit der Daten (Hash-Code) der betreffenden EMM-Nachricht.

[0019] Die aufeinander folgenden Kontrollwörter CW werden zum Verwürfler **10** und parallel zum Decoder übertragen, um die Verwürfelung und/oder Verschlüsselung bzw. die Entwürfelung und/oder Entschlüsselung der übertragenen Daten zu gestatten.

[0020] Auf diese Weise können die Video- und/oder Audiosignale verwürfelt werden, indem aufeinander folgende Kontrollwörter (CW) verwendet werden. Periodisch (beispielsweise alle 10 Sekunden) wird eine ECM-Nachricht mit dem verwürfelten Signal gesendet. Diese ECM-Nachrichten enthalten die Kontrollwörter, die durch den gegenwärtig gültigen Auswertungsschlüssel sk verschlüsselt sind, der durch EMM-Nachricht übertragen wird, um in dem Decoder oder der Karte (beispielsweise Chipkarte oder PCMCIA-Karte) gespeichert zu werden, die dem mit einem Kartenleser versehenen Decoder zugeordnet ist.

[0021] Die Auswertungsschlüssel sk werden weniger häufig durch EMM-Nachrichten aktualisiert, beispielsweise jeden Monat.

[0022] Die Auswertungsschlüssel sk werden mit einem oder mehreren individuellen Einzelschlüsseln Q verschlüsselt, die in der Chipkarte oder im Decoder sicher gespeichert sind.

[0023] In Zahl-Fernsehsystemen, die nach einer der beiden in der Beschreibungseinleitung beschriebenen Arten arbeitet, kann ein Sicherheitsproblem auftreten. Und zwar findet die Rücknahme der Teilnahmerechte an einem Programm oder die Rücknahme der Teilnehmerrechte gemäß der bekannten Technik durch Zusendung einer EMM-Teilnehmernachricht statt (vom Typ individuelle EMM-Nachricht oder EMM-Einzelnachricht). Ein Pirat (oder "Hacker") kann von einer solchen Arbeitsweise profitieren wollen, um zu verhindern, dass eine solche Rücknahme effektiv wird, nachdem ein Abonnement subskribiert wurde und eine vorübergehende entwürfelte Vorvisualisierung dem Teilnehmer durch Sendung einer EMM-Nachricht der Zuteilung von Rechten angeboten wurde. Der Pirat kann hierfür eine Technik entwickeln, die dazu bestimmt ist, die ECM-Nachrichten von den EMM-Nachrichten zu unterscheiden. Er kann nun durch Filterung EMM-Nachrichten identifizieren und unterdrücken, indem er "Blocker" verwendet. Eine solche Technik besteht beispielsweise in der digitalen Technologie MPEG ("Moving Picture Expert Group") darin, dass die Filterparameter der MPEG-Filter geändert werden, um keine EMM-Nachrichten zu empfangen, nachdem eine EMM-Nachricht von einem Decoder empfangen wurde und die Benutzerrechte von dem Decoder (oder der ihm zugeordneten Karte) über eine EMM-Nachricht empfangen wurden. Der Pirat kann auf diese Weise beispielsweise alle EMM-Nachrichten filtern und ausschließen, nachdem eine Karte autorisiert wurde, ein gegebenes Programm zu entwürfeln, das im vorübergehenden entwürfelten Vorvisualisierungsmodus zugänglich gemacht wurde, und zwar durch vorhergehende Sendung von geeigneten EMM-Nachrichten. Die Unterdrückung von späteren EMM-Nachrichten, nachdem ein Zugang zu einem der Programme autorisiert wurde, verhindert eine Änderung des Autorisierungszustands.

[0024] Die Autorisierungsdaten können nun nicht geändert werden und ein nicht autorisierter Zugang zu allen Programmen, die auf dem Kanal mit vorübergehender entwürfelter Vorschau gesendet werden, wird auf diese Weise während einer Zeit erhalten, die gleich der Dauer der Gültigkeit der Auswertungsschlüssel ist, die in der Karte vor Filterung der EMM-Nachrichten gespeichert wurden.

[0025] Zur Lösung dieses Problems sieht das Patent US 5461675, das ein Zugangskontrollverfahren beschreibt, eine Zeitperiode vor, während der die Chipkarte mindestens eine EMM-Nachricht empfangen muss, die der Karte gewidmet ist oder nicht. Wenn diese Anforderung nicht erfüllt ist, liefert die Chipkarte nicht die richtigen Informationen für die Entwürfelung des audiovisuellen Programms.

[0026] Gegenstand der Erfindung ist es, dieses Problem durch eine andere Lösung, als sie in dem Patent US 5461675 beschrieben wird, zu lösen, wobei gleichzeitig das für die Sendung der Nachrichten erforderliche Durchlassband begrenzt wird.

ZUSAMMENFASSUNG DER ERFINDUNG

[0027] Die vorliegende Erfindung schlägt deshalb ein Verfahren zur Rücknahme von Zugangsrechten zu einem von einem Decodierer empfangenen audiovisuellen Programm vor, umfassend die Schritte:

– der Sendung von zwei Typen von Nachrichten zum Decodierer, wobei erste Nachrichten verschlüsselte Kontrollwörter enthalten, wobei jedes Kontrollwort verwendet wird, um das empfangene audiovisuelle Signal während eines gegebenen Zeitraums zu entwürfeln, und zweite Nachrichten jeweils Informationen der Zuteilung von Rechten des Benutzers umfassen,

– der Entschlüsselung der ersten Nachrichten im Decodierer oder einem ihm zugeordneten tragbaren Objekt, um Kontrollwörter für die Entwürfelung des vom Decoder empfangenen Signals zu erzeugen, wenn der Benutzer berechtigt ist, auf die in diesem enthaltenen Informationen zuzugreifen,

gekennzeichnet durch die Sendung von dritten hybriden Nachrichten, die sich jeweils aus der Kombinati-

on mindestens eines verschlüsselten Kontrollworts, einer Decodiereradresse und einer Information der Rücknahme von Rechten ergeben.

[0028] Die Verwendung von hybriden Nachrichten (E3M) zur Invalidierung der Abonnementrechte oder der abonnierten Rechte gestattet es zu gewährleisten, dass die Rücknahme empfangen wird (da ohne empfangene hybride Nachricht keine Fernsehvisualisierung möglich ist), und schaltet somit den oben behandelten Typ von Systempiraterie aus.

[0029] Das erfindungsgemäße Verfahren gestattet ferner eine Reduzierung der gesendeten Nachrichtenmenge. Es ist nämlich nicht mehr erforderlich, Nachrichten zur Verwaltung der Zuteilung von Rechten (EMM) zu senden, um ein Angebot für einen Teilnehmer zu unterdrücken. Es ist möglich, dies direkt zu tun, indem eine hybride Nachricht E3M verwendet wird. Über die Abonnementangebote selbst hinaus ist es möglich, bei einer Abonnementkündigung Abonnements zu löschen (Schlüssel, Ablaufdatum, Gruppe).

[0030] Vorteilhafterweise wird in einer hybriden Nachricht das Kontrollwort durch einen anderen Auswertungsschlüssel als den Einzelschlüssel verschlüsselt, der zur Verschlüsselung der Decodiereradresse und der Information zur Rücknahme von Rechten verwendet wird. Man kann vorteilhafterweise eine asymmetrische Verschlüsselung verwenden.

[0031] Die Erfindung betrifft ferner ein Zahl-Fernsehsystem umfassend eine Teilnehmerverwaltungseinheit, die die Identifizierungen der Teilnehmer und ihre Rechte in Form einer Datenbasis speichert, eine Einheit zum Chiffrieren von EMM-Nachrichten, ein durch die Teilnehmerverwaltungseinheit gesteuertes Teilnehmerautorisierungssystem, einen MPEG-Kompressor für die audiovisuellen Programme, eine Einheit zum Chiffrieren von ECM-Nachrichten, einen Verwürfler/Multiplexer, mindestens einen einer Chipkarte zugeordneten Decodierer, einen Kommunikationsserver, einen Supervisor und eine Verbindung über Satellit, Erde oder über Kabel zwischen dem Verwürfler/Multiplexer und dem Decodierer, dadurch gekennzeichnet, dass es eine Einheit zum Kombinieren von EMM-Nachrichtenfeldern und von ECM-Nachrichtenfeldern umfasst, die für jeden audiovisuellen Zahl-Programmkanal eine Warteschlange für EMM-Rücknahmenachrichten und einen Multiplexer aufweist, wobei diese Einheit zum Kombinieren von Feldern am Eingang des Verwürflers/Multiplexers angeordnet ist.

[0032] Ferner betrifft die Erfindung einen Chipkarte oder einen Decodierer zur Behandlung von hybriden Nachrichten, die bzw. der Mittel umfasst, um in seinem bzw. ihrem Speicher eingeschriebene Rechte zu löschen und die mit dem gängigen Auswertungsschlüssel verschlüsselten Kontrollwörter zu entschlüsseln, um Kontrollwörter zu erzeugen.

[0033] Die Erfindung betrifft schließlich eine zu mindestens einem Decodierer übertragene Nachricht in einem Zahl-Fernsehsystem, umfassend mindestens:

– ein verschlüsseltes Kontrollwortfeld, wobei ein Kontrollwort dazu bestimmt ist, während eines gegebenen Zeitraums ein von dem Decodierer empfangenes audiovisuelles Signal zu entwürfeln;
– ein Decodiereradressenfeld, und
– ein Feld der Rücknahme von Rechten, die einem oder mehreren Decodierern zugeteilt sind, der bzw. die durch eine Adresse in diesem Adressfeld adressiert ist bzw. sind.

KURZE BESCHREIBUNG DER ZEICHNUNG

[0034] Fig. 1 zeigt ein Codier/Decodiersystem des Stands der Technik, das im Bereich des digitalen Fernsehens arbeitet;

[0035] Fig. 2 zeigt ein allgemeines Architekturschema eines Zahl-Fernsehsystems; und

[0036] Fig. 3 ist ein Blockdiagramm einer Feldkombinationseinheit gemäß der Erfindung, die in einem Multiplexer der Architektur von Fig. 2 enthalten ist.

AUSFÜHRLICHE BESCHREIBUNG VON BESONDEREN AUSFÜHRUNGSFORMEN

[0037] Im erfindungsgemäßen Verfahren wird die Unterdrückung der Zugangsrechte zumindestens einem Kanal, der Programme mit vorübergehender entwürfelter Vorvisualisierung befördert, mit Hilfe einer Nachricht von einem dritten Typ, E3M genannt, vorgenommen, die von den ECM- und EMM-Nachrichten verschieden ist.

[0038] Diese E3M-Nachrichten, die zumindestens zu einem Decodierer in dem Zahl-Fernsehsystem übertragen werden, umfassen mindestens:

– ein Feld für ein verschlüsseltes Kontrollwort,
– ein Decodiereradressfeld, und
– ein Feld der Rücknahme von Rechten, die einem oder mehreren Decodierern zugeteilt sind, die durch eine einzelne Adresse/Adressengruppe im Adressfeld adressiert ist bzw. sind.

[0039] Jede hybride Nachricht umfasst außerdem typischerweise ein ECM-Identifizierungskopffeld, das von einem EMM-Identifizierungskopffeld verschieden ist. Derartige Identifizierungskopffelder gestatten es, bei Empfang die ECM- und die EMM-Nachrichten zu unterscheiden.

[0040] Die Tatsache, dass Zugangsrechte zu einem Kanal, der Programme mit vorübergehender entwürfelter Vorvisualisierung befördert, in einer der

E3M-Nachrichten zurückgenommen werden, die jeweils gleichzeitig ein Kontrollwort und eine Information der Rücknahme von Rechten einschließen, begrenzt die Piraterie, denn der Pirat kann nicht mehr einen "Blocker" benutzen, da er sonst fast augenblicklich keinen Zugang mehr zu dem laufenden Programm hat, da er auf diese Weise jeden Zugang zu den Kontrollwörtern blockiert, die für die Entwürfelung des verwürfelten audiovisuellen Programms verwendet werden.

[0041] Ein Teilnehmer, der auf seinen Wunsch oder auf ein Angebot hin auf ein Programm mit vorübergehender entwürfelter Vorvisualisierung (oder Programm) zu einem gegebenen Zeitpunkt t0 zugreift und es auf ausdrückliche Anforderung oder durch Transaktionsfehler zu einem Zeitpunkt t0 + Δt (wobei Δt ein sehr kurzer Zeitraum sein kann) annulliert hat, um dieses Angebot nicht zu bezahlen, könnte nämlich zuvor einen "EMM-Blocker" auf den folgenden EMM-Nachrichten verwenden, um das gewünschte Angebot kostenlos zu visualisieren (während eines maximalen Zeitraums von EMM-Rückleitungszyklen, denn typischerweise speichert die tragbare Karte zwei Auswertungsschlüssel: den laufenden Schlüssel und den zukünftigen Schlüssel).

[0042] Es ist nicht mehr möglich, einen "E3M-Nachrichtenblocker" zu verwenden, denn eine Blockierung der E3M-Nachrichten liefe darauf hinaus, dass die Visualisierung der verlangten Programme gesperrt wird.

[0043] Die Zurückziehung der kommerziellen Angebote (oder Abonnementkündigung) wird mit Hilfe der E3M-Nachrichten erhalten. Jede E3M-Nachricht ergibt sich aus der Kombination von gewissen Informationen, die von ECM-Nachrichten befördert werden, und gewissen Informationen, die von EMM-Nachrichten befördert werden, und zwar umfasst jede E3M-Nachricht mindestens ein verschlüsseltes Kontrollwort, eine Decodiereradresse und eine Information der Rücknahme von Rechten.

[0044] Wie in Fig. 2 dargestellt, umfasst eine als Beispiel dienende Architektur eines Zahl-Fernsehsystems eine Teilnehmerverwaltungseinheit (SMS) **20**, die in Form einer Datenbasis die Identifizierungen der Teilnehmer und ihre Rechte speichert, eine EMM-Nachrichtenchiffriereinheit **21**, ein durch die SMS-Einheit **20** gesteuertes Teilnehmerautorisierungssystem **22**, einen MPEG-Kompressor der audiovisuellen Programme **23**, eine ECM-Nachrichtenchiffriereinheit **24**, einen Verwürfler/Multiplexer **25**, Decodierer **26**, die jeweiligen Chipkarten **27** ("Smart-Card") zugeordnet sind, einen Kommunikationsserver **30**, der mit einem Teilnehmerautorisierungssystem **22** und mit den Decodern **26** verbunden ist, einen mit dem Verwürfler/Multiplexer **25** verbundenen Supervisor **31** und eine Satelliten-, Erd- oder Kabelverbindung **32** zwischen dem Verwürfler/Multiplexer **25** und den Decodern **26**. Eine ausführliche Beschreibung der Arbeitsweise dieses Typs von System ist beispielsweise in der Patentanmeldung WO 98/43430 zu finden.

[0045] Wie in Fig. 3 dargestellt, umfasst die Einheit der Kombination von EMM-Nachrichtenfeldern und ECM-Nachrichtenfeldern typischerweise für jeden audiovisuellen Zahl-Programmkanal eine Rücknahme-EMM-Warteschleife **40** sowie einen Multiplexer **41**. Diese Felderkombinationseinheit ist typischerweise am Eingang des Verwürflers/Multiplexers **25** von Fig. 2 angeordnet.

[0046] Die Synchronisation der ECM-Nachrichten mit dem verwürfelten Programm ist entscheidend und die ECM-Nachrichten können deshalb in den Warteschleifen nicht verzögert werden.

[0047] Typischerweise wird eine Rücknahme-EMM-Nachricht bei einem gegebenen Kanal, sobald sie erzeugt ist, in der Warteschleife **40** gespeichert. Sobald eine ECM-Nachricht erzeugt ist (typischerweise bei einer Frequenz von etwa einer Sekunde) findet eine Multiplexierung statt, um gewisse Rücknahme-EMM-Nachrichten- und ECM-Nachrichtenfelder zu kombinieren, um eine hybride Nachricht E3M zu erzeugen. Eine solche E3M-Nachricht am Ausgang des Multiplexers **41** umfasst typischerweise:

– ein verschlüsseltes Kontrollwort, das aus einer ECM-Nachricht kommt,
– ein Decoderadressfeld, das aus einer Rücknahme-EMM-Nachricht kommt, und
– ein Feld der Rücknahme von Rechten, die dem Decoder oder der Gesamtheit von Decodern zugeteilt sind, die durch eine Adresse in diesem Adressfeld adressiert ist bzw. sind, die von derselben EMM-Nachricht kommt.

[0048] Die EMM-Nachrichten können nämlich Einzel-, individuelle oder Gruppennachrichten sein.

[0049] Angesichts des Änderungszyklus der ECM-Nachrichten von 2 bis 10 Sekunden ist es möglich, einen Zyklus von 300 bis 1800 verschiedenen Änderungen pro Stunde zu haben.

[0050] Um eine Piraterie seitens eines konkurrierenden Benutzers zu vermeiden, dem die Auswertungsschlüssel bekannt sein könnten (Piraterie, die darin besteht, dass richtig signierte Löschnachrichten gesendet werden), kann man diese Löschung über eine EMM-Nachricht vornehmen, die durch den einmaligen Schlüssel Q des Teilnehmers signiert ist, der in einer (signierten und authentifizierten) ECM-Nachricht, die einen Auswertungsschlüssel verwendet, enthalten ist.

[0051] Die Hauptbeschränkung des erfindungsgemäßen Verfahrens entspricht der Gesamtgröße jeder ECM-Nachricht und auch der Dauer der Verarbeitung der Inhalte dieser ECM-Nachrichten.

[0052] Eine solche Beschränkung ist heute jedoch nicht störend. Die Größe der ECM-Nachrichten kann nämlich 256 Bytes erreichen (ohne einen Verkettungsmodus zu verwenden) und die in den Chipkarten vorhandenen dynamischen RAM-Speicher sind weit ausreichend.

[0053] Außerdem gestatten die Geschwindigkeit der Prozessoren (CPU) und die Verwendung von Kryptoprozessoren, eine geeignete Verarbeitungszeit zu erreichen.

[0054] Um jeden von einem konkurrierenden Benutzer kommenden Systemangriff zu verhindern, verwendet man eine asymmetrische Verschlüsselung: Dieser Benutzer kann nämlich nun keine von den Chipkarten der Teilnehmer akzeptierten EMM- oder ECM-Nachrichten erzeugen wenn er nicht zuvor die asymmetrischen Schlüssel geknackt hat. Man kann auf diese Weise Algorithmen vom Typ RSA oder elliptische Kurven verwenden: Algorithmen des letzteren Typs haben den Vorteil, dass sie im Speicher weniger Platz einnehmen und größere Nutzinhalte von Nachrichten gestatten.

[0055] Es ist zu bemerken, dass die Chipkarte in der Lage ist, drei Typen von Nachrichten zu verarbeiten, und zwar auf herkömmliche Weise:

– Verarbeitung der EMM-Nachrichten, um die Änderungen der Teilnehmerrechte und des Verwertungsschlüssels, den sie in ihrem geschützten Speicher gespeichert hat, zu berücksichtigen,
– Entschlüsselung der verschlüsselten Kontrollwörter der ECM-Nachrichten mit dem laufenden Auswertungsschlüssel, um Kontrollwörter zu erzeugen,

und erfindungsgemäß:

– Verarbeitung der hybriden E3M-Nachrichten, um zuvor zugeteilte Rechte durch Löschung von in ihren Speicher eingeschriebenen Rechten zurückzunehmen, und Entschlüsselung der verschlüsselten Kontrollwörter der E3M-Nachrichten mit dem laufenden Auswertungsschlüssel, um Kontrollwörter zu erzeugen.

[0056] Eine solche Funktion kann auch ganz oder teilweise anstelle der Karte in dem Decoder enthalten sein.

Patentansprüche

1. Verfahren zur Rücknahme von Zugangsrechten zu einem von einem Decodierer (**11**) empfangenen audiovisuellen Programm, umfassend die Schritte:

– der Sendung von zwei Typen von Nachrichten zum Decodierer, wobei erste Nachrichten (ECM) verschlüsselte Kontrollwörter enthalten, wobei jedes Kontrollwort (CW) verwendet wird, um das empfangene audiovisuelle Signal während eines gegebenen Zeitraums zu entwürfeln, und zweite Nachrichten (EMM) jeweils Informationen der Zuteilung von Rechten des Benutzers umfassen,
– der Entschlüsselung der ersten Nachrichten im Decodierer oder einem ihm zugeordneten tragbaren Objekt, um Kontrollwörter (CW) für die Entwürfelung des vom Decodierer (**11**) empfangenen Signals zu erzeugen, wenn der Benutzer berechtigt ist, auf die in diesem enthaltenen Informationen zuzugreifen,
gekennzeichnet durch die Sendung von dritten hybriden Nachrichten (E3M), die sich jeweils aus der Kombination mindestens eines verschlüsselten Kontrollworts, einer Decodiereradresse und einer Information der Rücknahme von Rechten ergeben.

2. Verfahren nach Anspruch 1, bei dem das Kontrollwort (CW) in einer hybriden Nachricht (E3M) durch einen Auswertungsschlüssel verschlüsselt wird, der von dem zum Verschlüsseln der Decodiereradresse und der Information der Rücknahme von Rechten verwendeten gemeinsamen Schlüssel verschieden ist.

3. Verfahren nach Anspruch 1, bei dem man eine asymmetrische Verschlüsselung verwendet.

4. Zahl-Fernsehsystem, umfassend eine Teilnehmerverwaltungseinheit (**20**), die die Identifizierungen der Teilnehmer und ihre Rechte speichert, eine Einheit zum Chiffrieren von EMM-Nachrichten (**21**), ein durch die Teilnehmerverwaltungseinheit (**20**) gesteuertes Teilnehmerautorisierungssystem (**22**), einen MPEG-Kompressor für die audiovisuellen Programme (**23**), eine Einheit zum Chiffrieren von ECM-Nachrichten (**24**), einen Verwürfler/Multiplexer (**25**), mindestens einen einer Chipkarte (**27**) zugeordneten Decodierer (**26**), einen Kommunikationsserver (**30**), einen Supervisor (**31**) und eine Verbindung (**32**) zwischen dem Verwürfler/Multiplexer (**25**) und den Decodierern (**26**), dadurch gekennzeichnet, dass es eine Einheit zum Kombinieren von EMM-Nachrichtenfeldern und von ECM-Nachrichtenfeldern umfasst, die für jeden audiovisuellen Zahl-Programmkanal eine Warteschlange für EMM-Rücknahmenachrichten (**40**) und einen Multiplexer (**41**) aufweist, wobei diese Einheit zum Kombinieren von Feldern am Eingang des Verwürflers/Multiplexers (**25**) angeordnet ist.

5. Chipkarte, dadurch gekennzeichnet, dass sie speziell dafür ausgelegt ist, hybride Nachrichten (E3M) zu verarbeiten, die zu einem Decodierer übertragen werden und sich jeweils aus der Kombination mindestens eines verschlüsselten Kontrollworts, einer Decodiereradresse und einer Information der

Rücknahme von Rechten ergeben, wobei die Chipkarte zu diesem Zweck Mittel zum Löschen der in ihren Speicher eingeschriebenen Rechte und zum Entschlüsseln der mit einem gängigen Auswertungsschlüssel verschlüsselten Kontrollwörter umfasst, um Kontrollwörter zu erzeugen.

6. Decodierer, dadurch gekennzeichnet, dass er speziell dafür ausgelegt ist, hybride Nachrichten (E3M) zu verarbeiten, die ihm übertragen werden und sich jeweils aus der Kombination mindestens eines verschlüsselten Kontrollworts, einer Decodiereradresse und einer Information der Rücknahme von Rechten ergeben, wobei der Decodierer zu diesem Zweck Mittel umfasst, um in seinen Speicher eingeschriebene Rechte zu löschen und die mit einem gängigen Auswertungsschlüssel verschlüsselten Kontrollwörter zu entschlüsseln, um Kontrollwörter zu erzeugen.

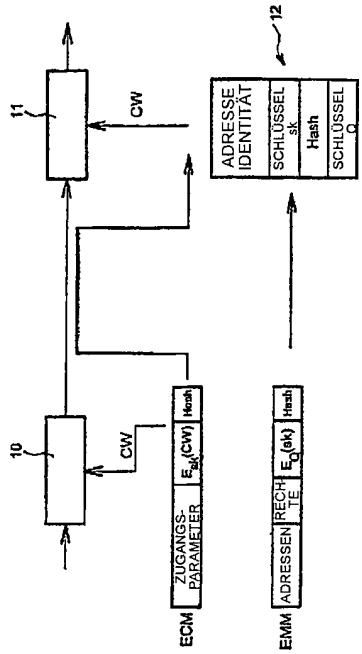
7. Zu mindestens einem Decodierer übertragene Nachricht in einem Zahl-Fernsehsystem, umfassend mindestens:
– ein verschlüsseltes Kontrollwortfeld, wobei ein Kontrollwort dazu bestimmt ist, während eines gegebenen Zeitraums ein von dem Decodierer empfangenes audiovisuelles Signal zu entwürfeln;
– ein Decodiereradressenfeld, und
– ein Feld der Rücknahme von Rechten, die einem oder mehreren Decodierern zugeteilt sind, der bzw. die durch eine Adresse in diesem Adressfeld adressiert ist bzw. sind.

8. Verfahren zur Rücknahme von Zugangsrechten zu einem von einem Decodierer (**11**) empfangenen audiovisuellen Programm, umfassend die Schritte:
– des Empfangs von zwei Typen von Nachrichten in dem Decodierer, wobei erste Nachrichten (ECM) verschlüsselte Kontrollwörter enthalten, wobei jedes Kontrollwort (CW) verwendet wird, um während eines gegebenen Zeitraums das empfangene audiovisuelle Signal zu entwürfeln, und zweite Nachrichten (EMM) jeweils Informationen der Zuteilung von Rechten des Benutzers umfassen,
der Entschlüsselung der ersten Nachrichten in dem Decodierer oder einem ihm zugeordneten tragbaren Objekt, um Kontrollwörter (CW) für die Entwürfelung des von dem Decodierer (**11**) empfangenen audiovisuellen Signals zu erzeugen, wenn der Benutzer autorisiert ist, auf die in diesem enthaltenen Informationen zuzugreifen,
gekennzeichnet durch den Empfang von dritten hybriden Nachrichten (E3M), die sich jeweils aus der Kombination mindestens eines verschlüsselten Kontrollworts, einer Decodiereradresse und einer Information der Rücknahme von Rechten ergeben.

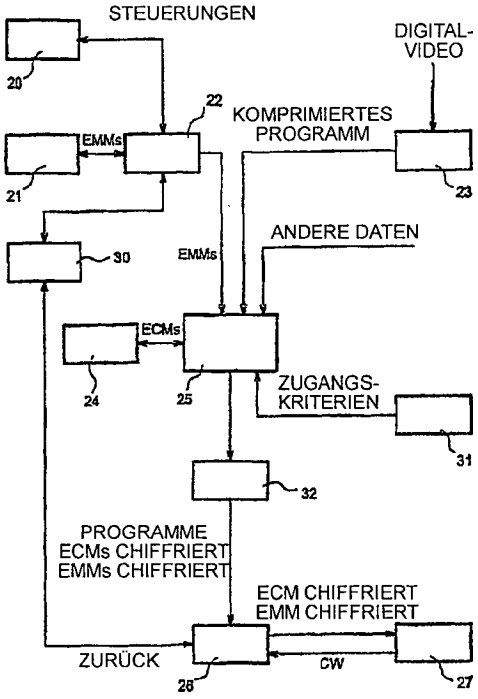
Es folgen 3 Blatt Zeichnungen

Anhängende Zeichnungen

[Fig. 001]



[Fig. 002]


STEUERUNGEN
DIGITAL-
VIDEO
20
22
KOMPRIMIERTES
PROGRAMM
EMMs
21
23
ANDERE DATEN
30
EMMs
ECMs
24
25
ZUGANGS-
KRITERIEN
31
32
PROGRAMME
ECMs CHIFFRIERT
EMMs CHIFFRIERT
ECM CHIFFRIERT
EMM CHIFFRIERT
ZURÜCK
CW
26
27

[Fig. 003]