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

(10) **DE 698 28 071 T2** 2005.11.24

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 018 265 B1**
(21) Deutsches Aktenzeichen: **698 28 071.7**
(86) PCT-Aktenzeichen: **PCT/IB98/01511**
(96) Europäisches Aktenzeichen: **98 942 975.8**
(87) PCT-Veröffentlichungs-Nr.: **WO 99/016244**
(86) PCT-Anmeldetag: **22.09.1998**
(87) Veröffentlichungstag der PCT-Anmeldung: **01.04.1999**
(97) Erstveröffentlichung durch das EPA: **12.07.2000**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **08.12.2004**
(47) Veröffentlichungstag im Patentblatt: **24.11.2005**

(51) Int Cl.[7]: **H04N 5/913**

(30) Unionspriorität:
97402238 25.09.1997 EP

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

(73) Patentinhaber:
Thomson Licensing S.A., Boulogne-Billancourt, FR

(72) Erfinder:
MAILLARD, Michel, F-78120 Rambouillet, FR

(74) Vertreter:
Roßmanith, M., Dipl.-Phys. Dr.rer.nat., Pat.-Anw., 30457 Hannover

(54) Bezeichnung: **VERFAHREN UND VORRICHTUNG ZUR AUFNAHME CHIFFRIERTER DIGITALER DATEN**

Anmerkung: Innerhalb von neun Monaten nach der Bekanntmachung des Hinweises auf die Erteilung des europäischen Patents kann jedermann beim Europäischen Patentamt gegen das erteilte europäische Patent Einspruch einlegen. Der Einspruch ist schriftlich einzureichen und zu begründen. Er gilt erst als eingelegt, wenn die Einspruchsgebühr entrichtet worden ist (Art. 99 (1) Europäisches Patentübereinkommen).

Die Übersetzung ist gemäß Artikel II § 3 Abs. 1 IntPatÜG 1991 vom Patentinhaber eingereicht worden. Sie wurde vom Deutschen Patent- und Markenamt inhaltlich nicht geprüft.

Beschreibung

[0001] Die vorliegende Erfindung betrifft ein Verfahren und eine Vorrichtung zur Aufzeichnung verwürfelter digitaler Daten, zum Beispiel Fernsehsendungen.

[0002] Die Übertragung von verschlüsselten Daten ist bekannt auf dem Gebiet der Gebührenfernsehsysteme, wo verwürfelte audiovisuelle Informationen im allgemeinen durch einen Satelliten zu einer Anzahl von Abonnenten gesendet werden, wobei jeder Abonnent einen Decoder oder Empfänger/Decoder besitzt, der die übertragenen Programme für eine darauffolgende Betrachtung entwürfeln kann.

[0003] In einem typischen System werden verwürfelte digitale Daten zusammen mit einem Steuerwort übertragen zur Entwürfelung der digitalen Daten, wobei das Steuerwort selbst durch einen ersten Schlüssel verschlüsselt ist und in verschlüsselter Form übertragen wird, die verwürfelten digitalen Daten und der verschlüsselte Code werden durch einen Decoder empfangen, der ein Äquivalent des ersten Schlüssels besitzt, der für die Entschlüsselung des verwürfelten Codeworts und danach zur Entwürfelung der übertragenen Daten benötigt wird. Der Decoder leitet die digitalen Daten in ihrer noch verwürfelten Form zu einem digitalen Aufzeichnungsgerät. Ein Abonnent, der dafür gezahlt hat, empfängt auf einer monatlichen Basis den Schlüssel, der zur Entschlüsselung des verschlüsselten Steuerworts benutzt wird, um so die Betrachtung eines bestimmten Programms zu ermöglichen.

[0004] Mit der Einführung der digitalen Technologie wurde die Qualität der übertragenen Daten um ein Vielfaches erhöht. Ein besonderes Problem bei der Qualität der digitalen Daten liegt in ihrer einfachen Wiedergabe. Wo ein entwürfeltes Programm über eine analoge Strecke (z. B. die "Peritel" Strecke) übertragen wird zur Betrachtung und Aufzeichnung durch einen üblichen VCR, bleibt die Qualität nicht größer als diejenige mit einer üblichen analogen Kassettenaufzeichnung. Die Gefahr, dass eine Aufzeichnung als ein Masterband benutzt wird, um Raubkopien herzustellen, ist somit nicht größer als mit einer üblichen, in einem Geschäft gekauften analogen Kassette.

[0005] Im Gegensatz dazu wird jedes entwürfelte digitale Signal über eine direkte digitale Strecke zu einem der neuen Geräte zur Bildung einer digitalen Aufzeichnung (zum Beispiel ein DVHS Recorder) dieselbe Qualität haben wie das ursprünglich übertragene Programm und kann somit häufig ohne jede Verschlechterung der Bild- oder Tonqualität wiedergegeben werden. Es besteht daher eine nennenswerte Gefahr, dass die entwürfelten Daten als eine Masteraufzeichnung benutzt werden zur Herstellung von Raubkopien, entweder weiter digitalen Kopien oder auch einfache analoge VHS-Kopien.

[0006] Die französische Patentanmeldung 95 03859 (Veröffentlichungsnummer FR-A-2 732 537) zeigt einen Weg zur Lösung dieses Problems durch ein System, in dem die entwürfelten digitalen Daten niemals auf einem digitalen Aufzeichnungsträger aufgezeichnet werden können. Stattdessen bewirkt der in dieser Anmeldung beschriebene Decoder eine Aufzeichnung der Daten in ihrer verwürfelten Form auf dem Aufzeichnungsträger, zusammen mit dem Steuerwort, dass für die Entwürfelung der Daten durch einen anderen Schlüssel benötigt wird. Dieser neue Schlüssel ist nur dem Empfänger/Decoder bekannt und ersetzt den ersten Schlüssel, der für die Bildung des Codeworts für die Betrachtung des Programms benötigt wird.

[0007] Der Vorteil eines derartigen Systems besteht darin, dass die Daten niemals in einer "klaren" Form gespeichert werden und ohne Besitz des in dem Empfänger/Decoder gespeicherten neuen Schlüssels nicht betrachtet werden können. Das System besitzt den Vorteil, dass, da der erste Schlüssel sich auf einer monatlichen Basis ändert, die Anwendung eines konstanten Schlüssels zur Entschlüsselung des auf dem digitalen Band aufgezeichneten Steuerworts bedeutet, dass der Empfänger/Decoder noch in der Lage ist, das auf dem Band aufgezeichnete Steuerwort selbst nach dem Ende eines Abonnementsmonats zu entschlüsseln.

[0008] Der Nachteil des in dieser Patentanmeldung vorgeschlagenen Systems besteht darin, dass die Aufzeichnung nur in Verbindung mit einem besonderen Empfänger/Decoder betrachtet werden kann. Wenn dieser Decoder ausfällt oder ersetzt wird, kann die Aufzeichnung nicht mehr wiedergegeben werden. Ebenso ist es nicht möglich, die Aufzeichnung direkt in einem digitalen Recorder wiederzugeben, ohne den Empfänger/Decoder in dem System anzuschließen, und ein Betrachter muss daher sein Abonnement in der Gebührenfernsehanstalt aufrechterhalten, um den Decoder so zu halten, dass er bereits übertragene Filme ansehen kann.

[0009] Es ist eine Aufgabe der vorliegenden Erfindung, die Probleme bei dieser Lösung zu lösen, dennoch eine sichere Aufzeichnung von digitalen Daten zu bilden, die zur Erzeugung von Raubkopien der übertragenen Daten nicht ohne weiteres benutzt werden kann.

[0010] Die vorliegende Erfindung ist in den beigefügten Ansprüchen angegeben.

[0011] Auf diese Weise löst die vorliegende Erfindung die Probleme des Standes der Technik, da die darauffolgende Neu-Wiedergabe der aufgezeichneten Daten unabhängig wird von der Identität des De-

coders. Bei der Wiedergabe der Aufzeichnung werden die Informationen durch einen in den Aufzeichnungsmitteln gespeicherten zweiten Schlüssel entschlüsselt.

[0012] Der Ersatz des Decoders macht die in Frage stehende Aufzeichnung nicht ungültig, solange der neue Decoder einen Behälter zur Aufnahme der den zweiten Schlüssel enthaltenen Aufzeichnungseinheitt hat. Bei Anwendung eines geeigneten Lesers kann der digitale Recorder selbst den zweiten Schlüssel lesen und die Wiedergabe der Informationen ermöglichen, ohne dass der Decoder benötigt wird. Anders als der Decoder, der ein relativ komplexes Teil der Anlage ist, der leicht ausfallen kann, kann das tragbare Aufzeichnungsgerät in einer einfachen, robusten Form ausgeführt werden.

[0013] Die Informationen, die durch den zweiten Schlüssel neu-verschlüsselt werden und auf dem digitalen Aufzeichnungsträger gespeichert sind, können in einfacher Weise den audiovisuellen Informationen entsprechen. Jedoch entsprechen in einer bevorzugten Ausführungsform die digitalen Informationen einem Steuerwort für die Entwürfelung der verwürfelten digitalen Daten. Dabei werden die verwürfelten digitalen Daten zusammen mit dem Steuerwort übertragen, wie es durch den ersten Schlüssel verschlüsselt ist, das Steuerwort wird danach durch den äquivalenten ersten Schlüssel entschlüsselt und durch den zweiten Schlüssel neu verschlüsselt, und das neu verschlüsselte Steuerwort und die verwürfelten Daten werden auf dem digitalen Aufzeichnungsträger aufgezeichnet.

[0014] In einer besonders bevorzugten Ausführungsform ist das tragbare Speichergerät eine Smart Card, die in einem Smart Card Leser in dem Decoder und/oder dem digitalen Recorder empfangen werden kann. In dieser Anmeldung dient der Ausdruck "Smart Card" zur Bezeichnung jeder konventionellen, auf einem Chip beruhende Karteneinheit, die zum Beispiel einen Mikroprozessor oder EEPROM Speicher für die Speicherung des zweiten Schlüsselalgorithmus besitzt. Der Ausdruck soll auch bedeuten Chipeinheiten mit anderen räumlichen Formen, zum Beispiel tastenförmige Geräte wie sie in Fernsehdecodersystemen häufig benutzt werden.

[0015] In einer Ausführungsform enthält die Smart Card auch das Äquivalent des ersten Schlüssels, der zur Entschlüsselung des Steuerworts für die anfängliche Entwürfelung der Daten dient, zum Beispiel zur Betrachtung in dem Fall eines Fernsehsendesystems. In einem derartigen Fall bildet die Smart Card einen Teil des Gebührenfernsehsystems und kann ebenfalls einen persönlichen Schlüssel enthalten, der dem Sender bekannt ist und dem Sender ermöglicht, selektiv zu identifizieren, welche Abonnenten am Ende des Monats einen aktualisierten ersten Schlüssel empfangen.

[0016] In einer alternativen Ausführungsform wird der zweite Schlüssel auf einer Smart Card gespeichert, die sich von derjenigen unterscheidet, die zur Speicherung des ersten Schlüssels dient. In einer derartigen Ausführungsform wird das Lesen der auf dem digitalen Träger gespeicherten Informationen vollständig getrennt von dem Abonnentensystem und, nachdem ein Abonnent sich aus dem System zurückgezogen und seine Abonnentenkarte abgegeben hat, kann er weiterhin vorher aufgezeichnete Filme betrachten, die von dem digitalen Recorder/Spieler zum Lesen der zugehörigen Smart Card geliefert werden.

[0017] In einem derartigen System können eine einzige Smart Card und ein zweiter Schlüssel zur Erzeugung des neu-verschlüsselten Codeworts für mehrere Aufzeichnungen dienen. Auf diese Weise kann eine einzige "Bibliothekskarte" zur Entschlüsselung einer beliebigen Anzahl von Aufzeichnungen dienen.

[0018] Bei der Erfindung enthält die Smart Card auch eine Anzahl von Krediteinheiten zur Ermittlung, wie oft die Aufzeichnung wiedergegeben werden kann, wobei die Zahl der Einheiten mit jeder darauffolgenden teilweisen oder vollständigen Wiedergabe der Aufzeichnung dekrementiert wird. Diese Krediteinheiten können zum Beispiel in einer Nachricht zusammen mit dem übertragenen ersten Schlüssel herunter geladen werden.

[0019] In einer Ausführungsform gehören die Krediteinheiten zu einem bestimmten Segment der Aufzeichnung, so dass bei der Wiedergabe eines Abschnitts der Aufzeichnung zum Beispiel die ersten oder letzten Viertelstunden der Aufzeichnung die Krediteinheiten für diese Abschnitte dekrementieren. Alternativ bilden die Krediteinheiten einen einzigen Typ und werden mit der Wiedergabe jedes Abschnitts der Aufzeichnung dekrementiert.

[0020] Wie oben erläutert, ist die vorliegende Erfindung besonders anwendbar bei dem Fall, wo der zweite Schlüsselalgorithmus auf einer Smart Card mit dem Aufzeichnungsträger gespeichert wird. Jedoch wird in einer alternativen Ausführungsform der tragbare Träger durch die Aufzeichnung selbst gebildet, und der zweite Schlüssel wird in einer integrierten Schaltung gespeichert, die in das Gehäuse des digitalen Aufzeichnungsträgers eingebettet ist.

[0021] Eine derartige Lösung wurde bereits erwogen, zum Beispiel in dem Fall von DVHS-Kassetten, wo ein Satz von Metallkontakten auf einer Außenfläche des Kassettengehäuses vorgesehen ist. Die Kontakte führen zu einer elektronischen Schaltung, wie einer integrierten Schaltung oder einem Chip, innerhalb des Gehäuses. Diese Kontakte können mit

einem entsprechenden Satz von Kontakten in dem Aufnahmefach des Recorders zusammenwirken, um eine Kommunikation zwischen der integrierten Schaltung und dem Videorecorder zu ermöglichen.

[0022] In derartigen Systemen wird die Sicherheit nach wie vor gewährleistet, trotz der Tatsache, dass der Schlüssel mit der Aufzeichnung übertragen wird, da der Schlüssel aus dem eingebetteten Chip nicht leicht zu kopieren ist. Die oben beschriebenen Varianten hinsichtlich der Smart Card-Ausführungsformen sind ebenso auf Systeme anwendbar, in denen der Träger durch das Recordergehäuse bestimmt ist.

[0023] Die vorliegende Erfindung ist besonders anwendbar auf ein Verfahren, in dem die verwürfelten Daten in einer Fernsehsendung verwürfelte audiovisuelle Daten übertragen.

[0024] Die vorliegende Erfindung wurde oben anhand eines Verfahrens beschrieben, ist jedoch ebenso auf eine Kombination eines Decoders und eine Smart Card ; und auf eine Smart Card anwendbar.

[0025] Die Ausdrücke "verwürfelt" und "verschlüsselt" und "Steuerwort" und "Schlüssel" wurden hier zum Zwecke der Klarheit der Sprache benutzt. Es sei jedoch bemerkt, dass keine grundsätzliche Unterscheidung gemacht werden muss zwischen "verwürfelte Daten" und "verschlüsselte Daten" oder zwischen einem "Steuerwort" und einem "Schlüssel".

[0026] Auf ähnliche Weise wird davon ausgegangen, wenngleich die Beschreibung auf "Empfänger/Decoder" und "Decoder" gerichtet ist, die vorliegende Erfindung ebenso auf Ausführungsformen anwendbar ist mit einem mit dem Decoder integrierten Empfänger wie einer Decodereinheit, die in Kombination mit einem räumlich getrennten Empfänger arbeitet. Die Erfindung betrifft ebenso Ausführungsformen, in denen der Decoder mit andern Einheiten, wie Fernsehgeräten oder auch digitalen Videorecordern, integriert ist.

[0027] Eine bevorzugte Ausführungsform der Erfindung wird nunmehr an einem Beispiel anhand der beigefügten Figuren beschrieben:

[0028] Fig. 1 zeigt den Gesamtaufbau eines digitalen Fernsehsystems, wie er durch die vorliegende Erfindung angewendet werden kann, um mit einem digitalen Aufzeichnungsgerät zusammen zu arbeiten,

[0029] Fig. 2 zeigt ein System für einen bedingten Zugriff des Fernsehsystems von Fig. 1,

[0030] Fig. 3 zeigt die verschiedenen Werte der Verschlüsselung in dem Fernsehsystem,

[0031] Fig. 4 zeigt die Struktur eines übertragenen digitalen Pakets in dem Fernsehsystem einschließlich audiovisueller, Audio- und Teletext-Daten und einer ECM Nachrichtenkomponente,

[0032] Fig. 5 zeigt eine erste Ausführungsform der Erfindung einschließlich eines digitalen Recordergerätes und einer Smart Card, die einen zweiten Algorithmus zur Verschlüsselung des Codeworts benutzt, das auf einer digitalen Videokassette registriert werden soll,

[0033] Fig. 6 zeigt eine zweite Ausführungsform der Erfindung, in der die Smart Card den ersten und den zweiten Schlüssel zum Betrachten des übertragenen und aufgezeichneten Programms enthält, beziehungsweise zusammen mit den Krediteinheiten zur Ermittlung der Häufigkeit, mit der ein Programm betrachtet werden kann, und

[0034] Fig. 7 zeigt eine dritte Ausführungsform der Erfindung, in der der zweite Schlüssel auf einer in dem Gehäuse der digitalen Videokassette enthaltenen integrierten Schaltung gespeichert wird.

Digitales Fernsehsystem

[0035] Eine Übersicht eines digitalen Fernseh- Sende- und Empfangssystems **1000** für die vorliegende Erfindung ist in Fig. 1 dargestellt. Das System enthält ein weitestgehend bekanntes digitales Fernsehsystem **2000**, das das bekannte MPEG-2 Komprimiersystem benutzt, zur Übertragung von komprimierten digitalen Signalen. Im Einzelnen empfängt der MPEG-2 Komprimierer **2002** in einem Sendezentrum einen digitalen Signalstrom (im allgemeinen einen Strom von Videosignalen). Der Komprimierer **2002** ist über eine Verbindung **2006** mit einem Multiplexer und Verwürfeler **2004** verbunden. Der Multiplexer **2004** empfängt mehrere weitere Eingangsignale, stellt einen oder mehreren Transportströme zusammen und überträgt komprimierte digitale Signale zu einem Sender **2008** des Sendezentrums über eine Strecke **2010**, die natürlich eine weite Vielfalt von Formen, einschließlich Telekomstrecken annehmen kann. Der Sender **2008** sendet elektromagnetische Signale über eine nach oben gerichtete "uplink Strecke" **2012** zu einem Satellitentransponder **2014**, wo sie elektronisch verarbeitet und über die so genannte Abwärtsstrecke **2016** zu dem erdgebundenen Empfänger **2018** übertragen werden, bekannt in der Form einer Schüssel, die der Endverbraucher besitzt oder mietet. Die durch den Empfänger **2018** empfangenen Signale werden zu einem integrierten Empfänger/Decoder **2020** übertragen, den der Endverbraucher besitzt oder mietet, und sind mit dem Fernsehgerät **2022** des Endverbrauchers verbunden. Der Empfänger/Decoder **2020** decodiert das komprimierte MPEG-2-Signal in ein Fernsehsignal für das Fernsehgerät **2022**.

[0036] Ein System **3000** für einen bedingten Zugriff ist mit dem Multiplexer **2004** und dem Empfänger/Decoder **2020** verbunden und liegt teilweise in dem Sendezentrum und teilweise in dem Decoder. Es ermöglicht, dass der Endverbraucher Zugriff hat zu digitalen Fernsehsendungen von einem oder mehreren Sendeanbietern. Eine Smart Card, die Nachrichten für die kommerziellen Angebote entschlüsseln kann (das heißt ein oder mehrere durch den Sendeanbieter verkaufte Fernsehprogramme), kann in den Empfänger/Decoder **2020** eingefügt sein. Durch Anwendung des Decoders **2020** und der Smart Card kann der Endbenutzer Ereignisse in einem Abonnementmodus oder einem Gebührenfernsehmodus kaufen.

[0037] Ein interaktives System **4000**, das ebenfalls mit dem Multiplexer **2004** und dem Empfänger/Decoder **2020** verbunden ist und wieder teilweise in der Sendestation und teilweise in dem Decoder liegt, ermöglicht, dass der Endbenutzer mit verschiedenen Anwendungen über einen Rückkanal **4002** mit einem Modem zusammen arbeiten kann.

System für einen bedingten Zugriff

[0038] In Fig. 2 enthält das System **3000** für einen bedingten Zugriff ein sogenanntes Subscriber Authorization System (SAS) **3002**. Das SAS **3002** ist mit einem oder mehreren Subscriber Management Systems (SMS) **3004**, einem SMS für jeden Sendeanbieter, über eine jeweilige TCP-IP Strecke **3006** verbunden (wenngleich alternativ andere Typen einer Verbindung benutzt werden könnten). Alternativ könnte ein SMS Anteil haben an zwei Sendeanbietern, oder ein Anbieter könnte zwei SMSs benutzen, undsoweiter.

[0039] Erste Verschlüsselungseinheiten in der Form von Chiffrierungseinheiten **3008**, die "Mutter"-Smart Cards **3010** benutzen, sind über die Verbindungsstrecke **3012** mit dem SAS verbunden. Zweite Verschlüsselungseinheiten, wieder in der Form von Chiffrierungseinheiten **3014**, die "Mutter"-Smart Cards **3016** benutzen, sind über eine Strecke **3018** mit dem Multiplexer **2004** verbunden. Der Empfänger/Decoder **2020** empfängt eine "Tochter"-Smart Card **3020**. Er ist direkt mit dem SAS **3002** durch Communications Servers **3022** über den mit einem Modem versehenen Rückkanal **4002** verbunden. Das SAS sendet unter anderen Dingen Abonnementsrechte auf Anforderung zu der "Tochter"-Smart Card.

[0040] Die Smart Cards enthalten die Geheimwerte einer oder mehrerer kommerzieller Operatoren. Die "Mutter"-Smart Card verschlüsselt verschiedene Arten von Nachrichten, und die "Tochter"-Smart Cards entschlüsseln die Nachrichten, wenn sie die Rechte haben, dieses zu tun.

[0041] Die erste und die zweite Chiffrierungseinheit **3008** und **3014** enthalten ein Gestell (rack), eine elektronische VME Card mit einer auf einem EEPROM gespeicherten Software, bis zu 20 elektronische Karten und einer Smart Card **3010** bzw. **3016** für jede elektronische Card, eine (Card **3016**) für die Verschlüsselung der ECMs und eine (Card **3010**) für die Verschlüsselung der EMMS.

[0042] Wie im Folgenden beschrieben wird, sind die sogenannten Entitlement Control Messages verschlüsselte Nachrichten, eingebettet in den Datenstrom eines übertragenen Programms, die das für die Endwürfelung eines Programms benötigte Steuerwort enthalten. Die Berechtigung eines bestimmten Empfänger/Decoders wird gesteuert durch EMMs oder so genannte Entitlement Management Messages, die weniger häufig übertragen werden, zum Beispiel jeden Monat, und die einen berechtigten Empfänger/Decoder mit den zur Decodierung der ECM benötigten Schlüssel versorgen.

[0043] Der Betrieb des Systems **3000** für einen bedingten Zugriff des digitalen Fernsehsystems wird nunmehr im Detail anhand der verschiedenen Bauteile des Fernsehsystems **2000** und des Systems **3000** für den bedingten Zugriff beschrieben.

Multiplexer und Verwürfeler

[0044] In den Fig. 1 und Fig. 2 wird in dem Sendezentrum das digitale Videosignal zunächst komprimiert (oder in der Bitrate reduziert) durch Anwendung des MPEG-2 Komprimierers **2002**. Dieses komprimierte Signal wird dann über die Verbindung **2006** zu dem Multiplexer und Entwürfeler **2004** übertragen, um mit anderen Daten gemultiplext zu werden, wie anderen komprimierten Daten.

[0045] Der Verwürfeler erzeugt ein Steuerwort Ce, das in dem Verwürfelungsvorgang benutzt wird und in dem MPEG-2 Strom in dem Multiplexer **2004** enthalten ist. Das Steuerwort Ce wird intern erzeugt und ermöglicht, dass der integrierte Empfänger/Decoder **2020** des Endverbrauchers das Programm entwürfeln kann. Zugriffskriterien, die anzeigen, wie das Programm kommerzialisiert wird, werden ebenfalls dem MPEG-2 Strom hinzugefügt. Das Programm kann in einer Anzahl von "Abonnements"-Modi und/oder auf einer Anzahl von "Gebührenfernsehen" (PPV = Pay Per View) Modi oder Ereignisse kommerzialisiert werden. In dem Abonnementsmodus abonniert der Endbenutzer einen oder mehrere kommerzielle Angebote von "Bouquets" und erhält dadurch das Recht, jeden Kanal innerhalb dieser Bouquets zu betrachten. In der bevorzugten Ausführungsform können bis zu 960 kommerzielle Angebote aus einem Bouquet von Kanälen ausgewählt werden. In dem Gebührenfernsehmodus erhält der Endbenutzer die Möglichkeit, Ereignisse zu kaufen, wie er wünscht. Das kann erreicht werden entweder durch Vorbu-

chung des Ereignisses im voraus ("Vorbuchungsmodus") oder durch Kauf des Ereignisses, sobald es gesendet wird ("Impulsmodus").

[0046] Das Steuerwort Ce und die Zugriffskriterien dienen zur Bildung einer so genannten Entitlement Control Message (ECM). Dies ist eine Nachricht, die gesendet wird für ein verwürfeltes Programm. Die Nachricht enthält ein Steuerwort (das die Entwürfelung des Programms ermöglicht) und die Zugriffskriterien des Sendeprogramms. Die Zugriffskriterien und das Steuerwort werden über die Verbindung **3018** zu der zweiten Verschlüsselungseinheit **3014** übertragen. In dieser Einheit wird eine ECM erzeugt, verschlüsselt mit einem ersten Schlüssel Cex und übertragen zu dem Multiplexer und Verwürfeler **2004**.

[0047] Jeder Service, der durch einen Sendeanbieter gesendet wird, enthält eine Anzahl von unterschiedlichen Komponenten. Zum Beispiel enthält ein Fernsehprogramm eine Videokomponente V, eine Audiokomponente S, eine Untertitel- oder Teletextkomponente CT undsoweiter (siehe **Fig. 4**). Jede dieser Komponenten eines Service wird individuell für die darauffolgende Sendung zu dem Transponder **2014** verwürfelt und verschlüsselt. Für jede verwürfelte Komponente des Service wird eine getrennte ECM benötigt.

Programmübertragung

[0048] Der Multiplexer **2004** empfängt elektrische Signale mit verschlüsselten EMMs von dem SAS **3002**, verschlüsselte ECMs von der zweiten Verschlüsselungseinheit **3014** und komprimierte Programme von dem Komprimierer **2002**. Der Multiplexer **2004** verwürfelt die Programme und überträgt die verwürfelten Programme, die verschlüsselte EMM (sofern anwesend) und die verschlüsselten ECMs als elektrische Signale zu einem Sender **2008** des Sendezentrums über die Verbindung **2010**. Der Sender **2008** überträgt elektromagnetische Signale über eine nach oben gerichtete Strecke **2012** zu dem Satellitentransponder **2014**.

Programmempfang

[0049] Der Satellitentransponder **2014** empfängt und verarbeitet die durch den Sender **2008** gesendeten elektromagnetischen Signale und überträgt die Signale zu einem erdgebundenen Empfänger **2018**, im allgemeinen in der Form einer Schüssel, die der Endverbraucher besitzt oder gemietet hat, durch eine nach unten gerichtete Strecke **2016**. Die durch den Empfänger **2018** empfangenen Signale werden zu dem integrierten Empfänger/Decoder **2020** übertragen, die der Endbenutzer besitzt oder mietet, und an das Fernsehgerät **2022** des Endbenutzers angeschlossen sind. Der Empfänger/Decoder **2020** demultiplexiert die Signale, um verwürfelte Programme mit verschlüsselten EMMs und verschlüsselten ECMs zu gewinnen.

[0050] Wenn das Programm nicht verwürfelt ist, dekomprimiert der Empfänger/Decoder **2020** die Daten und setzt das Signal in ein Videosignal für die Übertragung zu dem Fernsehgerät **2022** um. Wenn das Programm verwürfelt ist, extrahiert der Empfänger/Decoder **2020** die entsprechende ECM aus dem MPEG-2 Strom und lenkt die ECM zu der "Tochter"-Smart Card **3020** des Endbenutzers. Der Endbenutzer gibt die ECM in Schlitze in einem Gehäuse in dem Empfänger/Decoder **2020** ein. Die Tochter-Smart Card **3020** prüft, ob der Endbenutzer das Recht für die Entschlüsselung der ECM und den Zugriff zu dem Programm hat.

[0051] Wenn der Benutzer nicht die erforderlichen Rechte hat, wird ein negativer Status zu dem Empfänger/Decoder **2020** übertragen, um anzuzeigen, dass das Programm nicht entwürfelt werden kann. Wenn der Endbenutzer die Rechte hat, wird die ECM entschlüsselt und das Steuerwort extrahiert. Der Decoder **2020** wird durch Anwendung dieses Steuerworts das Programm entwürfeln. Der MPEG-2 Strom wird dekomprimiert und in ein Videosignal für die Übertragung zu dem Fernsehgerät **2022** umgesetzt.

[0052] Die Werte der benutzten Verschlüsselung werden detaillierter anhand der folgenden **Fig. 3** beschrieben.

Abonnenten-Verwaltungs-System (SMS)

[0053] Ein Abonnenten-Verwaltugns-System (SMS) **3004** enthält eine Datenbank **3024**, die unter anderem alle Eingaben des Endbenutzers, kommerzielle Angebote (wie Tarife und Werbungen), Abonnements, PPV Details und Daten für den Verbrauch und die Berechtigung beim Endbenutzer verwaltet. Die SMS kann physisch von dem SAS entfernt sein.

[0054] Jede SMS **3004** überträgt Nachrichten zu dem SAS **3002** über eine jeweilige Verbindung **3006**, damit Änderungen oder Bildungen von Entitlement Management Messages (EMMs) zu den Endbenutzern übertragen werden können.

[0055] Das SMS **3004** überträgt außerdem Nachrichten zu dem SAS **3002**, die keine Änderungen oder Bildungen von EMMs beinhalten, sondern nur eine Änderung in einem Endbenutzerzustand zu implizieren (für die dem Endbenutzer gewährte Berechtigung bei der Forderung von Produkten oder zu dem Betrag, mit dem der Endbenutzer belastet wird).

Berechtigungs-Verwaltungs-Nachrichten (EMMs)

[0056] Das EMM ist eine Nachricht speziell für einen einzelnen Endbenutzer (Abonnent) oder eine Gruppe

von Endbenutzern (im Gegensatz zu einem ECM, das einem verwürfelten Programm zugeordnet ist oder ein Satz von verwürfelten Programmen, wenn Teil desselben kommerziellen Angebots). Eine Gruppe kann eine bestimmte Anzahl von Endbenutzern enthalten. Diese Organisation als eine Gruppe dient zur Optimierung der Bandbreite. Das heißt, ein Zugriff zu einer Gruppe kann das Erreichen einer größeren Zahl von Endbenutzern ermöglichen.

[0057] Es werden verschiedene spezielle Typen der EMM für die Umsetzung der vorliegenden Erfindung in die Praxis benutzt. Individuelle EMMs sind für einzelne Abonnenten vorgesehen und werden im allgemeinen benutzt in der Lieferung von Gebührenfernsehdiensten. Diese enthalten den Gruppenidentifizierer und die Lage des Abonnenten in dieser Gruppe. Sogenannte "Gruppen" Abonnements EMMs sind den Gruppen gewidmet von zum Beispiel 256 einzelnen Benutzern, und werden im allgemeinen benutzt in der Verwaltung einiger Abonnementdienste. Diese EMM enthält einen Gruppenidentifizierer und eine Gruppen Bitmap der Abonnenten. EMMs für das Publikum sind dem gesamten Publikum gewidmet und können zum Beispiel von einem Benutzer durch einen bestimmten Operator benutzt werden, um einen gewissen freien Service zu bilden. Ein "Publikum" (Audience) ist die Gesamtheit der Abonnenten mit Smart Cards, die denselben Operator-Identifizierer (OPI) tragen. Schließlich ist eine "einzige" EMM dem einzigen Identifizierer der Smart Card zugeordnet.

Verschlüsselungswerte des Systems

[0058] Anhand der Fig. 3 werden nunmehr die Verschlüsselungswerte in dem Sendesystem beschrieben. Die Stufen der Verschlüsselung für die Sendung der digitalen Daten sind bei **4001** dargestellt, der Übertragungskanal (z. B. eine Satellitenstrecke wie oben beschrieben) bei **4002** und die Stufen der Verschlüsselung beim Empfänger bei **4003**.

[0059] Die digitalen Daten N werden durch ein Steuerwort Ce verwürfelt, bevor es zu einem Multiplexer Mp für die darauf folgende Übertragung gesendet wird. Wie aus Fig. 4 ersichtlich ist, enthalten die übertragenen Daten eine ECM, die unter anderem das Steuerwort Ce enthält, wie es durch einen Verschlüsseler Ch1 verschlüsselt ist, der durch einen ersten Verschlüsselungsschlüssel Cex gesteuert wird. Beim Empfänger/Decoder wird das Signal durch einen Demultiplexer DMp und einen Entwürfeler D geführt, bevor es zur Betrachtung einem Fernsehgerät **2022** zugeführt wird. Eine Entschlüsselungseinheit DCh1, die ebenfalls den Schlüssel Cex besitzt, entschlüsselt die ECM in dem demultiplexierten Signal zur Gewinnung des Steuerworts Ce, das danach zur Entwürfelung des Signals benutzt wird.

[0060] Aus Sicherheitsgründen ändert sich das in die verschlüsselte ECM eingebettete Steuerwort Ce im Mittel ungefähr alle 10 Sekunden. Im Gegensatz dazu ändern sich der Verschlüsselungsschlüssel Cex, der durch den Empfänger zur Decodierung des ECM benutzt wird, etwa jeden Monat mittels einer EMM. Der Verschlüsselungsschlüssel Cex wird durch eine zweite Einheit ChP verschlüsselt, die einen persönlichen Schlüssel Cg benutzt, entsprechend der Identität des Decoders. Wenn der Decoder einer von denjenigen ist, die zum Empfang eines aktualisierten Schlüssels Cex gewählt wurden, entschlüsselt eine Entschlüsselungseinheit DChP in dem Decoder die Nachricht unter Anwendung ihres Schlüssels Cg, um den monatlichen Schlüssel Cex zu gewinnen.

[0061] Die Entschlüsselungseinheiten DChp und DCh1 und die zugehörigen Schlüssel werden auf einer Smart Card gehalten, die dem Abonnenten geliefert wird und in einen Smart Card Leser in dem Decoder eingefügt wird. Die Schlüssel können gemäß einem bekannten symmetrischen Schlüsselalgorithmus, wie einem DES, erzeugt werden. Alternative Ausführungsformen, die öffentliche/private Schlüsselalgorithmen benutzen, sind ebenfalls möglich.

Aufzeichnung von digitalen Daten

[0062] Wie in der Einführung festgestellt, ist es für die entwürfelten digitalen Daten nicht zu empfehlen, dass die entschlüsselten digitalen Daten in Anbetracht der Gefahren aufgezeichnet werden können, die entstehen für die unberechtigte Kopierung und die Raubkopierung. Wie in Fig. 5 gezeigt, bildet die vorliegende Erfindung Mittel zur Lösung dieses Problems.

[0063] Das system enthält eine Smart Card **4004** zur Einfügung in einen Smart Card Schlitz in dem Empfänger/Decoder, zusammen mit einem digitalen Recorder **4005**, z. B. einem DVHS Recorder, einschließlich eines digitalen Aufzeichnungsträgers **4006**, wie einer DVHS Kassette.

[0064] In dieser Ausführungsform wird das empfangene Steuerwort durch die zugehörige Smart Card **3020** entschlüsselt, die in dem Decoder eingefügt wird (siehe Fig. 2). Das decodierte Steuerwort Ce (zusammen mit beliebigen anderen Daten, die eine ECM bilden, wie Zugriffssteuerinformationen usw.) wird dann dem in der Smart Card **4004** eingebetteten Mikroprozessor zugeführt. Durch Anwendung eines zweiten Verschlüsselungsschlüssels C2 und eines zweiten Verschlüsselungsalgorithmus Ch2 erzeugt die Smart Card **4004** eine neue ECM, die in der Figur mit ECM' bezeichnet ist. Diese Berechtigungsnachricht ECM' dient dann zum Ersatz der ECM in dem verwürfelten Datenstrom von dem Demultiplexer DMp, wie bei **4007** gezeigt, und die Kombination der verwürfelten Daten und die Neu-Berechtigungsnach-

richt ECM' werden auf der DVHS Kassette **4006** aufgezeichnet. Die Berechtigungsnachricht ECM' kann in den Datenstrom in einem Schiebesteuerregister R eingefügt werden.

[0065] Durch diese Mittel vermeidet die Erfindung die Aufzeichnung von decodierten audiovisuellen Informationen auf der Kassette. Zum Abspielen der Kassette wird die Karte erneut in den Decoder eingesetzt, der Schlüssel C2 dient zur Decodierung der Berechtigungsnachricht ECM', und das darauffolgend extrahierte Steuerwort Ce dient zur Steuerung des Decoders zur Entwürfelung des Programms für die Betrachtung.

[0066] In dem in Fig. 5 gezeigten System unterscheidet sich die Smart Card **4004** von der in Fig. 2 gezeigten Smart Card **3020** des Fernsehsystems, die die für die Betrachtung des Programms benötigten Verschlüsselungsschlüssel enthält. Jedoch enthält in der in Fig. 6 gezeigten alternativen Ausführungsform die Smart Card **3020** sowohl den ersten als auch den zweiten Verschlüsselungsschlüssel Cex bzw. C2, die für die Betrachtung und die Aufzeichnung des Programms benötigt werden. Wie dargestellt, steuert der Schlüssel Cex die Entschlüsselung der ECM zur Erzeugung des durch den Entwürfeler D benutzten Steuerworts Ce, das danach durch den Schlüssel C2 verschlüsselt wird, um die neue Berechtigungsnachricht ECM' zu bilden.

[0067] Die Algorithmen DCh1 und DCh2 sind aus Platzgründen nicht dargestellt. Die Karte **3020** wird tatsächlich üblicherweise mit dem (nicht dargestellten) persönlichen Schlüssel Cg initialisiert, der die Entschlüsselung der EMMs ermöglicht, um so den in dem Speicher der Karte gespeicherten monatlichen Schlüssel Cex zu gewinnen. Wenngleich die Smart Card in der Form einer im wesentlichen rechteckförmigen Karte dargestellt ist, sind natürlich andere physische Formen wie Schlüsselformen usw. möglich.

[0068] Das mit dem Programm übertragene und durch die Smart Card verwürfelte ECM kann zusätzlich Krediteinheiten U enthalten, die danach in der Card gespeichert werden und die die Häufigkeit steuern, mit der ein aufgezeichneter Film betrachtet werden kann. In der einfachsten Ausführungsform können die Krediteinheiten während der Wiedergabe des aufgezeichneten Films jedes Mal dekrementiert werden, wenn eine ECM' durch den Decoder läuft. Wenn die Anzahl der Kredite auf null dekrementiert ist, und dadurch anzeigt, dass die Aufzeichnung um vorbestimmte Male betrachtet wurde, wird eine Nachricht zu dem Decoder gesendet, um weitere Betrachtungen des Films zu verhindern, wenn die Kreditkarten nicht neu geladen werden (z. B. durch eine in einer EMM gesendete Belastungsanweisung).

[0069] In alternativen Ausführungsformen können die Krediteinheiten alle zehn oder hundert ECM' Nachrichten dekrementiert werden. In weiteren Ausführungen können die Krediteinheiten bestimmten Abschnitten des Films entsprechen (z. B die ersten oder letzten 10 Minuten des Films), derart, dass die Wiedergabe dieser Abschnitte die zu ihnen gehörenden Krediteinheiten dekrementiert. Die Abschnitte können identifiziert werden durch Etikettierung oder Kennzeichnung der ECM' Nachrichten in diesen Abschnitten.

[0070] Eine weitere Ausführungsform der Erfindung ist in Fig. 7 dargestellt. In dieser Ausführungsform wird die Erzeugung der neuen Berechtigungsnachricht ECM' durch eine integrierte Schaltung oder einen Chip **4008** gesteuert, der den zweiten Verschlüsselungsschlüssel C2 besitzt und in das Gehäuse der aufgezeichneten Kassette **4000** eingebettet ist. Die Aufnahme eines Mikroprozessors in dem Gehäuse des Aufzeichnungsträgers ist eine bekannte Lösung und wurde zum Beispiel im Fall von DVHS Kassetten erwogen. In diesem Beispiel kann ein Satz von Metallkontakten auf der Außenfläche des Kassettengehäuses vorgesehen sein, wobei die Kontakte zu einer elektronischen Schaltung führen, wie einer integrierten Schaltung oder einem Chip im Inneren des Gehäuses. Diese Kontakte greifen in einen entsprechenden Kontaktsatz in dem Aufnahmefach des Recorders ein, um die Kommunikation zwischen der integrierten Schaltung und dem Videorecorder zu ermöglichen.

[0071] Wenngleich sie zur Kopierung der aufgezeichneten (und verwürfelten) digitalen Daten dienen, sind die in dem Chip gespeicherte Daten resistent gegenüber einer Kopierung, und bezüglich der vorangehenden Ausführungsformen sind die verwürfelten Daten ohne den Schlüssel C2 nutzlos, der zur Entriegelung der ECM' benötigt wird, um das durch den Entwürfeler benutzte Steuerwort zu gewinnen.

[0072] In allen beschriebenen Ausführungsformen können die Bauteile des Empfänger/Decoders und des digitalen Aufzeichnungsgeräts kombiniert oder ausgetauscht werden, derart, dass der digitale Recorder zum Beispiel einen Smart Card Schlitz zur Aufnahme einer Smart Card besitzt, und/oder die benötigten Bauteile zur Entwürfelung des Programms, wenn das Steuerwort Ce aus der ECM'-Nachricht extrahiert worden ist. Der Decoder und/oder der digitale Recorder können ebenfalls mit anderen Geräten integriert sein, wie zum Beispiel einem Fernsehgerät.

Patentansprüche

1. Verfahren zur Aufzeichnung von digitalen Informationen (Ce), die durch einen ersten Schlüssel (Cex) verschlüsselt sind und durch einen Decoder (**2020**) empfangen werden, mit dem Zugriff zu einem Äquivalent des ersten Schlüssels (Cex), der zur Ent-

schlüsselung der Informationen benötigt wird, **dadurch gekennzeichnet**, dass die entschlüsselten Informationen danach durch einen zweiten Schlüssel (C2) neu-verschlüsselt werden, der in einer Smart Card (**3020**, **4004**) gespeichert ist, die in einem Smart Card-Leser in dem Decoder (**2020**) empfangen wird, und die neu-verschlüsselten Informationen danach auf einem digitalen Aufzeichnungsträger (**4006**) durch einen digitalen Recorder (**4005**) aufgezeichnet werden, und die Smart Card außerdem eine Anzahl von Krediteinheiten (U) enthält, um zu ermitteln, wieviele Male eine Aufzeichnung wiedergegeben werden kann, und die Anzahl der Einheiten mit jeder darauffolgenden teilweisen oder vollständigen Wiedergabe der Aufzeichnung dekrementiert werden.

2. Verfahren nach Anspruch 1, in dem die Krediteinheiten (U) zu einem bestimmten Segment der Aufzeichnung gehören, derart, dass die Wiedergabe eines Abschnitts der Aufzeichnung bestimmte Kredite für diesen Abschnitt dekrementiert.

3. Verfahren nach Anspruch 2, in dem die Krediteinheiten von einem einzigen Typ sind und mit der Wiedergabe eines Abschnitts der Aufzeichnung dekrementiert werden.

4. Verfahren nach einem der Ansprüche 1 bis 3, wobei der zweite Schlüssel in einer integrierten Schaltung gespeichert wird, die in dem Gehäuse des digitalen Aufzeichnungsträgers eingebettet ist.

5. Verfahren nach einem der Ansprüche 1 bis 3, wobei der zweite Schlüssel (C2) auf einer Smart Card für den Aufzeichnungsträger gespeichert wird.

6. Kombination eines Decoders (**2020**) zum Empfang von digitalen Informationen (Ce), die durch einen ersten Schlüssel (Cex) verschlüsselt sind und Zugriff haben zu einem Äquivalent des ersten Schlüssels (Cex), der zur Entschlüsselung der Informationen. benötigt wird und eine Smart Card (**3020**, **4004**), die in einem Smart Card Leser in dem Decoder (**2020**) empfangen wird, dadurch gekennzeichnet, dass die Smart Card (**3020**, **4004**) einen zweiten Schlüssel (C2) für die Anwendung bei der Neu-Verschlüsselung der entschlüsselten Informationen für die darauf folgende Übertragung zu einem digitalen Aufzeichnungsgerät (**4005**) besitzt, zur Aufzeichnung auf einem digitalen Aufzeichnungsmedium (**4006**), und in dem die Smart Card außerdem eine Anzahl von Krediteinheiten (U) enthält, um zu ermitteln, wie viele Male eine Aufzeichnung wiedergegeben werden kann, und dass die Smart Card die Anzahl der Einheiten mit jeder darauffolgenden, teilweisen oder vollständigen Wiedergabe der Aufzeichnung dekrementiert wird.

7. Kombination nach Anspruch 6, in der die Krediteinheiten (U) zu einem bestimmten Segment der Aufzeichnung gehören, derart, dass bei der Wiedergabe eines Abschnitts der Aufzeichnung die Smart Card bestimmte Kredite für diesen Abschnitt dekrementiert.

8. Kombination nach Anspruch 7, in der die Krediteinheiten vom einzigen Typ sind und die Smart Card die Krediteinheiten mit der Wiedergabe eines Bereichs der Aufzeichnung dekrementiert.

9. Smart Card (**3020**, **4004**), die von einem Smart Card-Leser in einem Decoder (**2020**) empfangen wird, wobei die Smart Card digitale Informationen (Ce) von dem Decoder empfängt durch Anwendung eines ersten Schlüssels (Cex) und Zugriff hat zu einem äquivalenten ersten Schlüssel (Cex), der zur Entschlüsselung der Informationen benötigt wird, dadurch gekennzeichnet, dass die Smart Card (**3020**, **4004**) einen zweiten Schlüssel (C2) für die Anwendung bei der Neu-Verschlüsselung der entschlüsselten Informationen für die darauffolgende Übertragung zu einem digitalen Aufzeichnungsträger (**4005**) besitzt, zur Aufzeichnung auf einem digitalen Aufzeichnungsmedium (**4006**), und in dem die Smart Card außerdem eine Anzahl von Krediteinheiten (U) enthält, um zu ermitteln, wie viele Male eine Aufzeichnung wiedergegeben werden kann, wobei die Smart Card die Anzahl der Einheiten mit jeder darauffolgenden, teilweisen oder vollständigen Wiedergabe der Aufzeichnung dekrementiert wird.

Es folgen 6 Blatt Zeichnungen

Anhängende Zeichnungen

Fig.1.

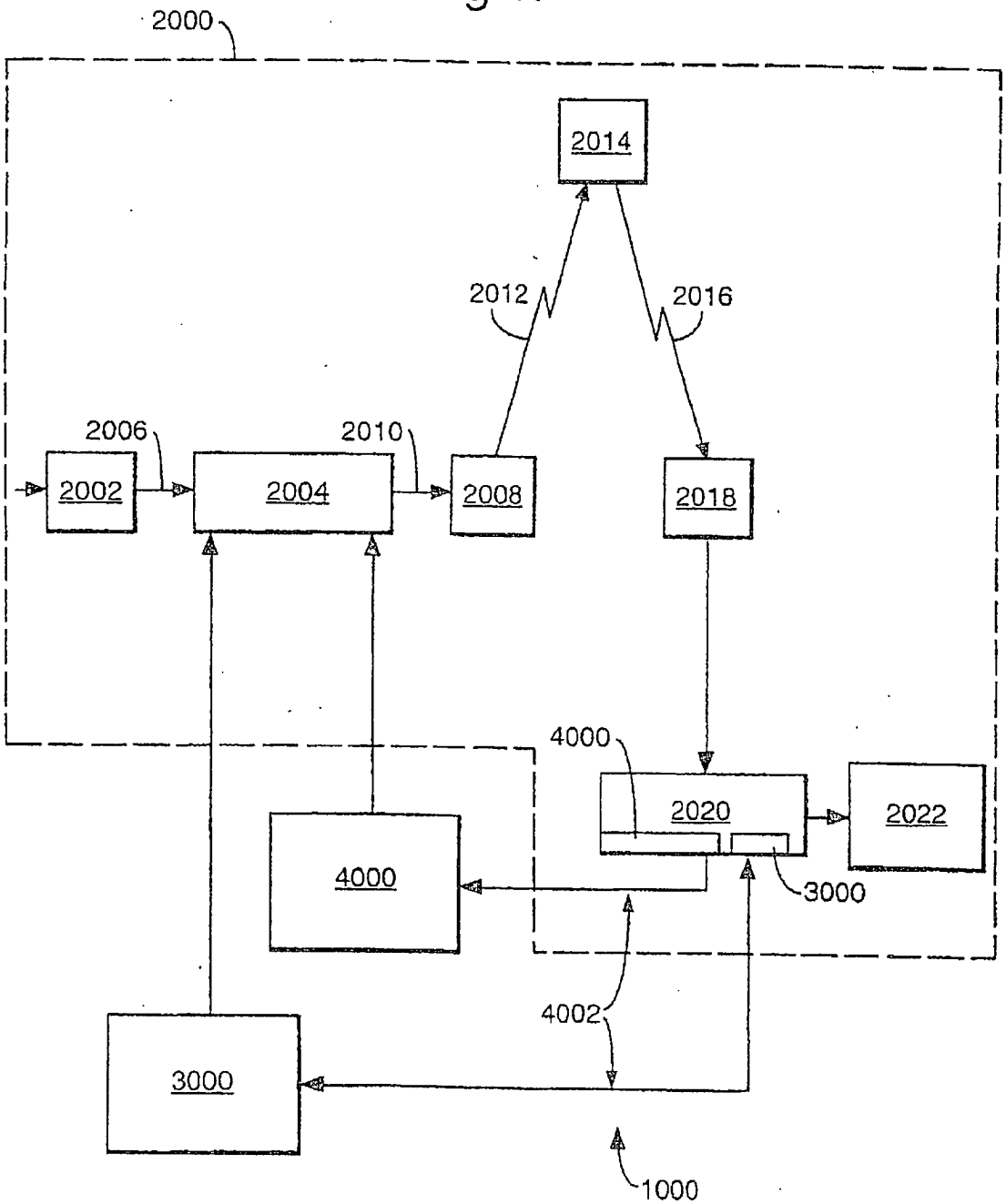

Fig.2.

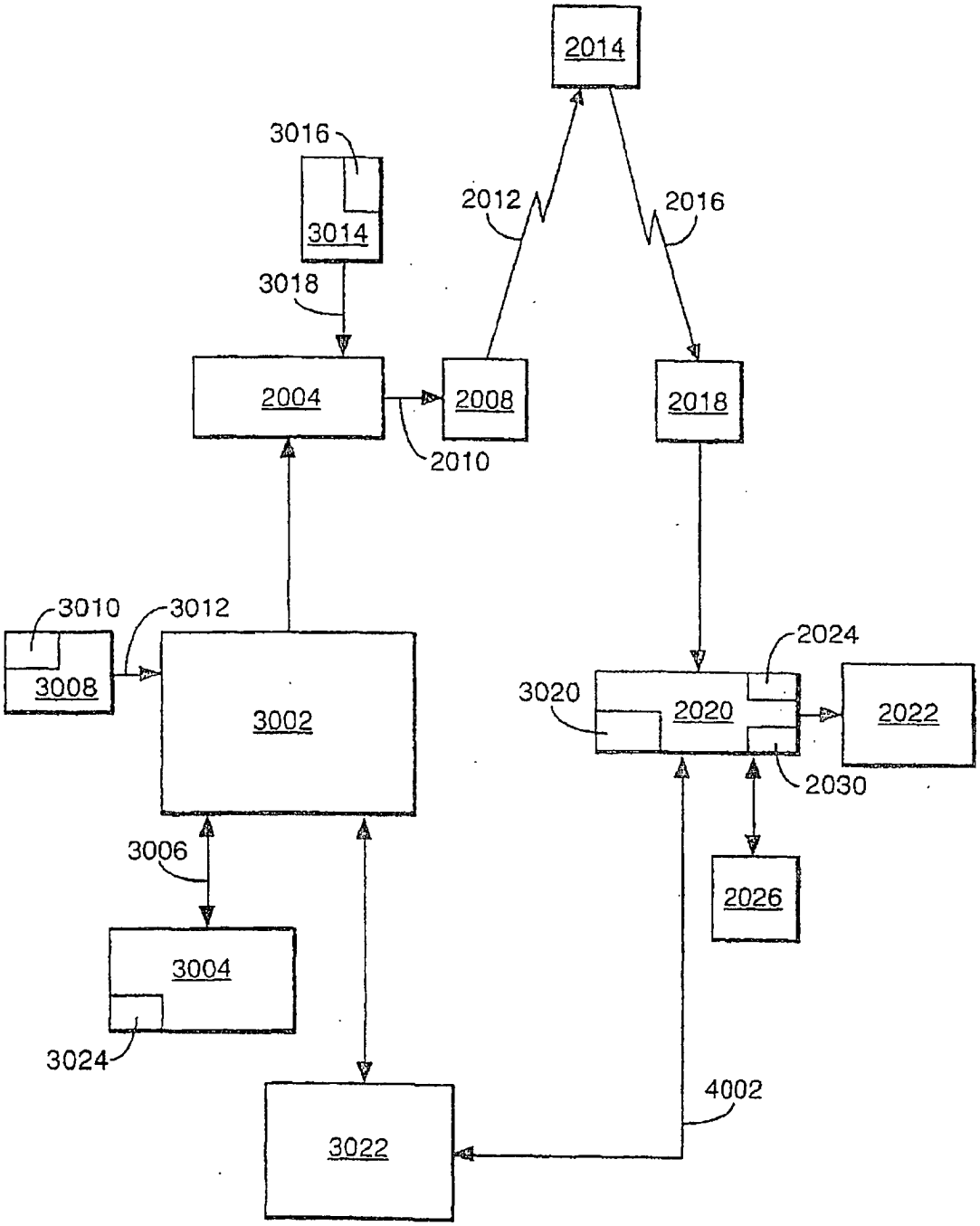
2014
3016
3014
2012
2016
3018
2004
2008
2018
2010
3010
3012
3008
3002
2024
3020
2020
2022
2030
3006
2026
3004
3024
4002
3022

Fig.3.

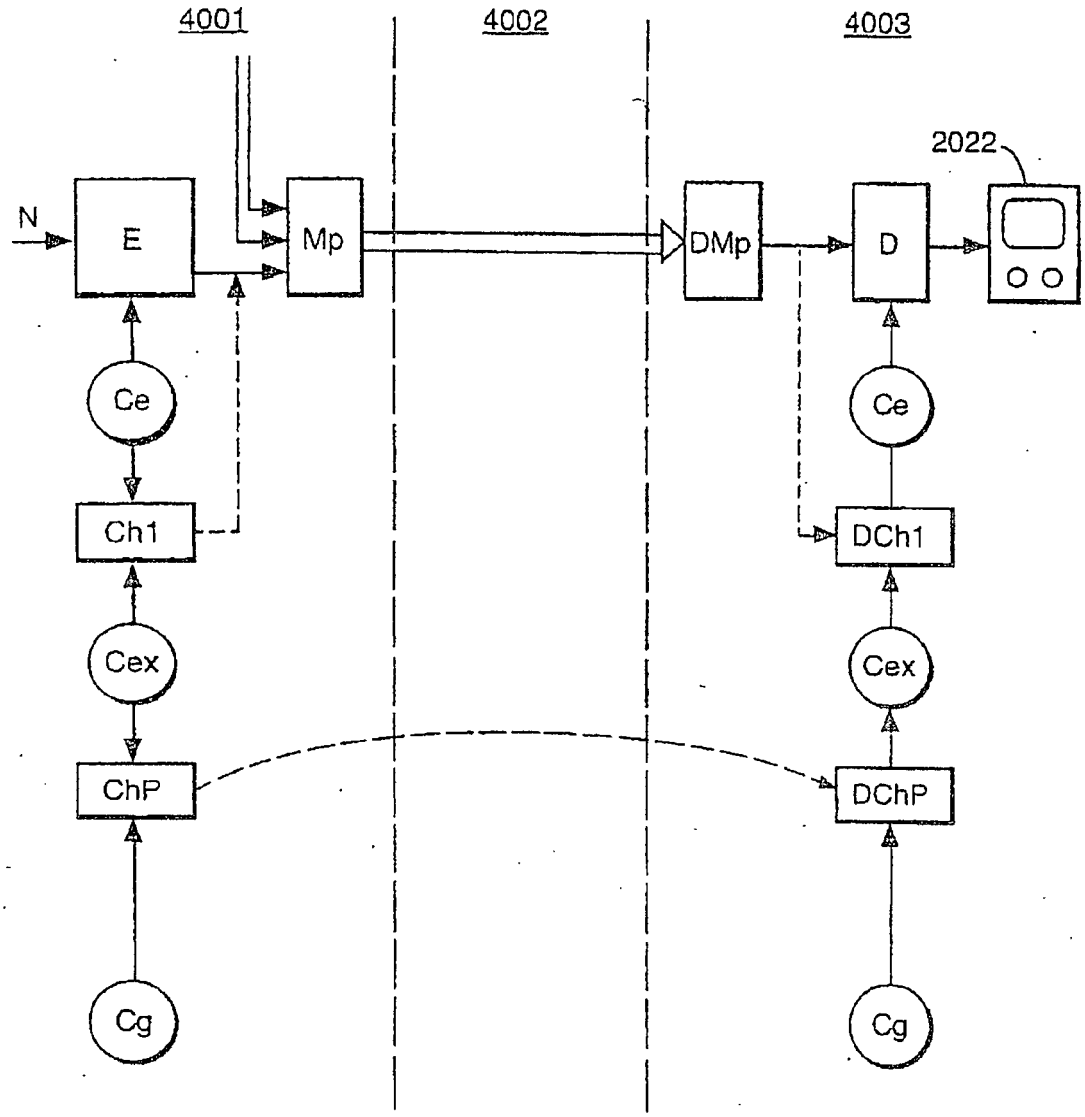
4001
4002
4003
2022
N
E
Mp
DMp
D
Ce
Ch1
Cex
ChP
Cg
Ce
DCh1
Cex
DChP
Cg

Fig.4.

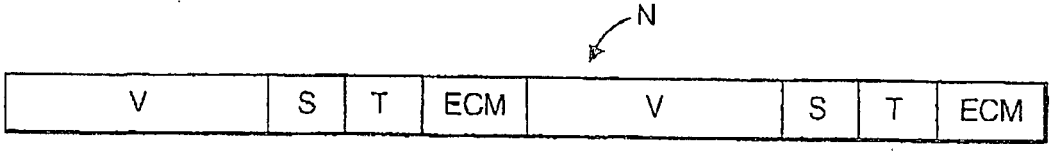
N
V
S
T
ECM
V
S
T
ECM

Fig.5.

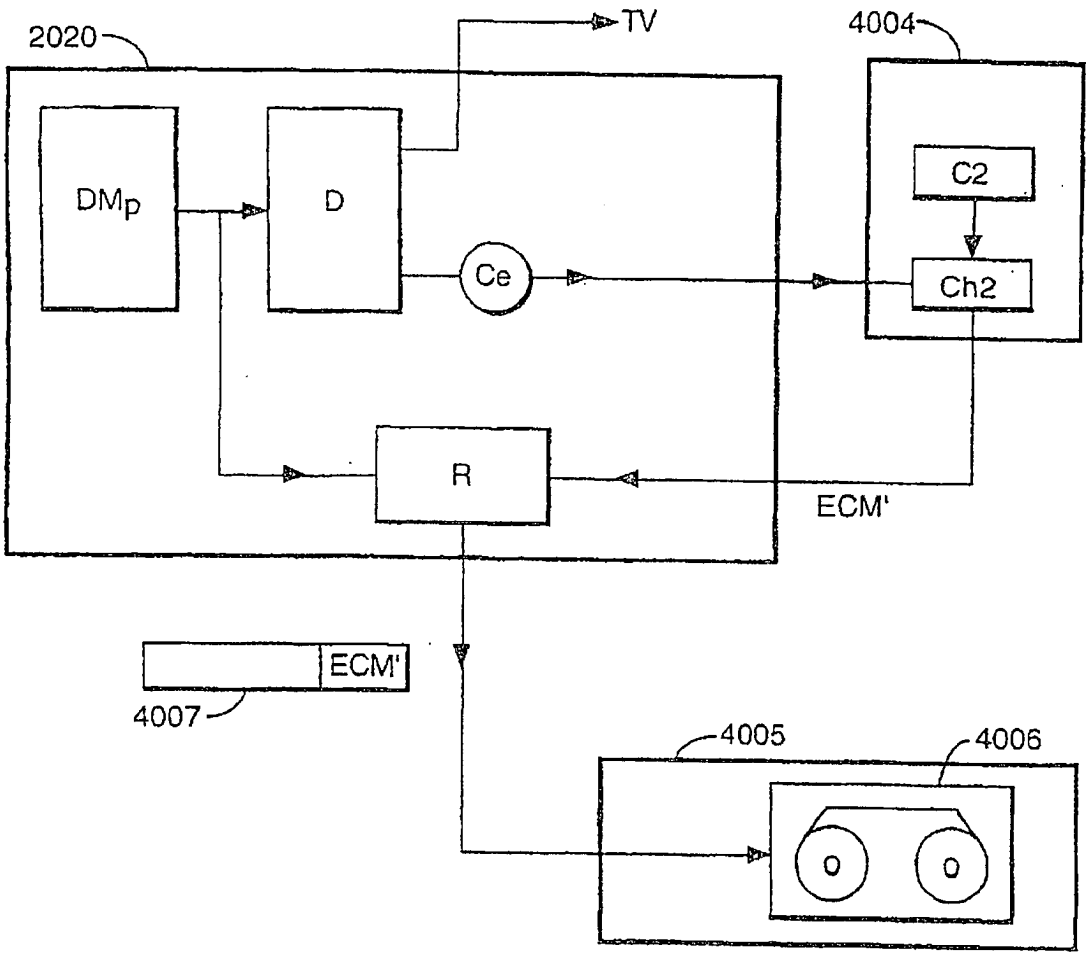

Fig.6.

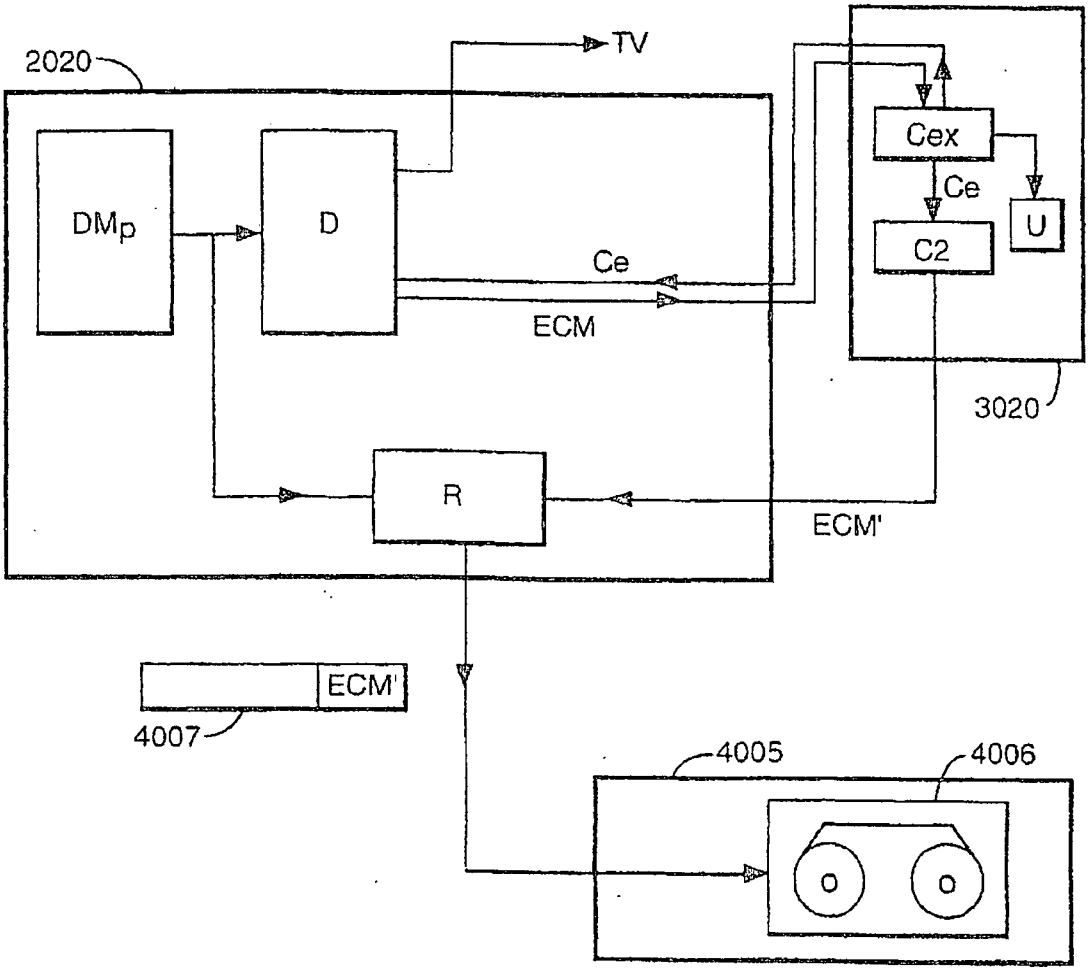

Fig.7.