



(19)
Bundesrepublik Deutschland
Deutsches Patent- und Markenamt

(10) **DE 698 26 099 T2 2005.09.15**

(12)

Übersetzung der europäischen Patentschrift

(97) EP 0 925 686 B1

(51) Int Cl.⁷: **H04N 7/167**

(21) Deutsches Aktenzeichen: **698 26 099.6**

(86) PCT-Aktenzeichen: **PCT/IB98/00986**

(96) Europäisches Aktenzeichen: **98 924 532.9**

(87) PCT-Veröffentlichungs-Nr.: **WO 99/003277**

(86) PCT-Anmeldetag: **25.06.1998**

(87) Veröffentlichungstag

der PCT-Anmeldung: **21.01.1999**

(97) Erstveröffentlichung durch das EPA: **30.06.1999**

(97) Veröffentlichungstag

der Patenterteilung beim EPA: **08.09.2004**

(47) Veröffentlichungstag im Patentblatt: **15.09.2005**

(30) Unionspriorität:

97890135 11.07.1997 EP

(74) Vertreter:

derzeit kein Vertreter bestellt

(73) Patentinhaber:

**Koninklijke Philips Electronics N.V., Eindhoven,
NL**

(84) Benannte Vertragsstaaten:

AT, DE, FR, GB

(72) Erfinder:

PROIDL, Adolf, NL-5656 AA Eindhoven, NL

(54) Bezeichnung: **ANORDNUNG ZUR UNABHÄNGIGEN BEANTRAGUNG EINER ABSPIELBERECHTIGUNG FÜR
EIN REPRODUZIERTES VERSCHLÜSSELTES NACHRICHTENSIGNAL**

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 eingelebt, 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 bezieht sich auf eine Anordnung zum Überprüfen einer Abspielberechtigung für ein reproduziertes verschlüsseltes Informationssignal – das mit Hilfe einer Wiedergabeausrüstung wiedergegeben wird, die dazu vorgesehen ist, mit der Anordnung zusammenzuarbeiten, – und zum Liefern eines verschlüsselten Informationssignals, wenn eine Wiedergabeberechtigung verfügbar ist,

wobei diese Anordnung die nachfolgenden Elemente umfasst:

- Überprüfungsmitte, vorgesehen zum Empfangen eines reproduzierten verschlüsselten Informationssignals und vorgesehen zum Liefern von Schlüsselinformation, geeignet zum einwandfreien Entschlüsseln des reproduzierten verschlüsselten Informationssignals, wenn eine Wiedergabeberechtigung verfügbar ist, und
- Entschlüsselungsmittel, vorgesehen zum Empfangen von Schlüsselinformation und vorgesehen zum Entschlüsseln des reproduzierten verschlüsselten Informationssignals, wenn geeignete Schlüsselinformation verfügbar ist.

[0002] Eine derartige Anordnung der eingangs beschriebenen Art ist beispielsweise aus dem Dokument WO 96/05700 A1 bekannt. Bei der bekannten Anordnung, die durch eine sog. "Set-Top-Box" gebildet wird, ermöglichen die Überprüfungsmitte es, dass Identifikationsinformation in einem reproduzierten verschlüsselten Informationssignal ermittelt werden. Wenn derartige Identifikationsinformation vorhanden ist, wird eine Abspielberechtigung für das reproduzierte verschlüsselte Informationssignal erhalten. Die Identifikationsinformation enthält Schlüsselinformation, die den Entschlüsselungsmitteln zugeführt werden können um das reproduzierte verschlüsselte Informationssignal zu entschlüsseln. Ein reproduziertes verschlüsseltes Informationssignal kann mit Hilfe eines Fernsehgeräts wiedergegeben werden, wobei dieses Gerät mit der bekannten Anordnung verbunden ist.

[0003] Die bekannte Anordnung ist dazu vorgesehen, charakteristische Abspielinformation aufzuzeichnen, welche die Nummer und die Länge von Abspielveranstaltungen eines verschlüsselten Informationssignals im Falle einer Abspielberechtigung charakterisiert. Weiterhin ist mit Hilfe einer Datenverbindung die bekannte Anordnung mit einer Sendestation verbunden, die eine Abspielfrageanordnung bildet. Durch Abfragung der aufgezeichneten charakteristischen Abspielinformation mit Hilfe der bekannten Anordnung kann die Abfrageanordnung ermitteln, wie viele Male und wie lange ein verschlüsseltes Bezahl-Informationssignal von der Abspielanordnung in der bekannten Anordnung entschlüsselt wurde und daraufhin von dem Benutzer der bekannten Anord-

nung verwendet worden ist. Verrechnung für die normalerweise wiederholte Reproduktion der Bezahl-Informationssignale kann auf Basis der charakteristischen Abspielinformation effektuiert werden.

[0004] In Bezug auf die bekannte Anordnung hat es sich aber herausgestellt, dass das Vorhandensein verschlüsselter Identifikationsinformation in dem reproduzierten verschlüsselten Informationssignal, wobei diese Information eine einwandfreie Entschlüsselung eines verschlüsselten Informationssignals erlaubt und notwendig ist für den einwandfreien Betrieb der bekannten Anordnung, von nicht berechtigten Personen benutzt wurde zum herstellen illegaler Kopien, die das Informationssignal enthalten, das bereits entschlüsselt worden ist. Aufzeichnungsträger mit entschlüsselten Informationssignalen wurden verkauft von Personen, die dazu nicht berechtigt waren, was zu einem wesentlichen Schaden für Sendestationen führt.

[0005] Wenn aber die mit der bekannten Anordnung aufgezeichnete charakteristische Abspielinformation mit Hilfe einer Abspielabfrageanordnung abgefragt wird, entsteht das Problem, dass eine Abspielabfrageanordnung zunächst keine Information hat ob es eine bekannte Anordnung gibt und wo diese sich befindet, mit deren Hilfe Bezahl-Informationssignale reproduziert werden, für welche das Einziehen der Gebühren mit Hilfe der Abspielabfrageanordnung effektuiert wird. Dies erschwert das Einziehen von Gebühren für die Reproduktion von Bezahl-Informationssignalen wesentlich.

[0006] Weiterhin ist es nicht möglich, auszuschließen, dass die von der bekannten Anordnung aufgezeichnete charakteristische Abspielinformation durch eine Person geändert wird, die nicht berechtigt ist dies zu machen, was das Einziehen von Gebühren zusätzlich erschwert.

[0007] Weiterhin hat es sich in Bezug auf die bekannte Anordnung herausgestellt, dass, einerseits, das Abfragen der mit Hilfe der bekannten Anordnung aufgezeichneten charakteristischen Abspielinformation zu relativ langen Zeitintervallen zu einer Unwissheit für den Benutzer der bekannten Anordnung über den Betrag der Gebühren führt und, andererseits, das Abfragen der mit Hilfe der bekannten Anordnung aufgezeichneten charakteristischen Abspielinformation zu relativ kurzen Zeitintervallen zu einem relativ großen Aufwand für die Sendestation führt.

[0008] Es ist nun u. a. eine Aufgabe der vorliegenden Erfindung die oben genannten Probleme zu vermeiden und eine verbesserte Anordnung der eingangs beschriebenen Art zu schaffen, mit deren Hilfe einerseits Manipulation bei der Bestimmung der Gebühren für die Reproduktion von Bezahl-Informationssignalen im Wesentlichen ausgeschlossen wird,

aber andererseits eine große Flexibilität und geringe Kosten bei der Bestimmung der Gebühren für eine Sendestation erhalten werden kann. Nach der vorliegenden Erfindung wird diese Aufgabe erfüllt durch eine Anordnung nach dem Oberbegriff des Anspruchs 1 erfüllt, wobei die Anordnung ausgebildet ist mit Abfragemitteln zum automatischen und unabhängigen Beantragen einer Wiedergabeberechtigung, wie in dem kennzeichnenden Teil des Anspruchs 1 beschrieben. So wird auf einfache An und Weise erzielt, dass mit Hilfe der Anordnung nach der vorliegenden Erfindung ein unabhängiger Antrag zur Wiedergabeberechtigung möglich ist, wenn dies erforderlich ist. Bei Empfang von Schlüsselinformation, auf der eine Wiedergabeberechtigung basiert ist, kann ein reproduziertes verschlüsseltes Informationssignal mit Hilfe der Anordnung nach der vorliegenden Erfindung entschlüsselt werden. Manipulation durch eine nicht berechtigte Person ist dann nahezu völlig ausgeschlossen, weil bei Empfang der Wiedergabeberechtigungsbeantragungsinformation charakteristische Bezahlungsinformation ausschließlich in der Wiedergabeberechtigungszuordnungsanordnung erzeugt wird. Weiterhin kann das Auferlegen der Gebühren an den Benutzer der Anordnung nach der vorliegenden Erfindung zu relativ kurzen Zeitintervallen und mit einem besonders geringen Aufwand für die Wiedergabeberechtigungszuordnungsanordnung erfolgen.

[0009] In einer Anordnung nach der vorliegenden Erfindung mit den Kennzeichen, wie in Anspruch 1 definiert, hat es sich als vorteilhaft herausgestellt, wenn außerdem die in Anspruch 2 definierten Maßnahmen getroffen werden. In der Praxis hat es sich bewährt, dass eine derartige Ausführungsform besonders zuverlässig und einfach ist und zu relativ geringen Kosten verwirklicht werden kann.

[0010] In einer Anordnung nach der vorliegenden Erfindung mit den Merkmalen nach Anspruch 2 hat es sich als vorteilhaft erwiesen, wenn die Maßnahmen nach Anspruch 3 getroffen werden. Auf diese Weise wird erreicht, dass Abspielberechtigungsbeantragungsinformation für ein bestimmtes Bezahlinformationssignal der Abspielberechtigungszuordnungsanordnung zugeführt werden kann, die imstande ist, eine Abspielberechtigung für dieses bestimmte Bezahl-Informationssignal zuzuordnen. Weiterhin wird die Schlüsselinformation, die zum Entschlüsseln des reproduzierten verschlüsselten Informationssignals erforderlich ist und die bei Empfang der Abspielberechtigung zu der Anordnung übertragen wird, wird nur in der durch die Freigabeinformation identifizierten Abspielberechtigungszuordnungsanordnung gespeichert.

[0011] In einer Anordnung nach der vorliegenden Erfindung mit den Merkmalen, wie in Anspruch 3 definiert, hat es sich als vorteilhaft erwiesen, wenn die

in Anspruch 4 definierten Maßnahmen getroffen werden. Dies hat den Vorteil, dass verschlüsselte Informationssignale, die von einer Sendestation übertragen und von der Anordnung nach der vorliegenden Erfindung empfangen werden, wobei diese Signale Freigabeinformation enthält, die eine Abspielberechtigungszuordnungsanordnung identifiziert, die freigegeben ist eine Abspielberechtigung zuzuordnen, einer Aufzeichnungs- und Wiedergabebeanordnung zugeführt werden können zum Aufzeichnen des verschlüsselten Informationssignals. Dadurch kann Bestimmung der Gebühren für die Wiedergabe von Bezahl-Informationssignalen von einer Anzahl Sendestationen mit Hilfe nur einer einzigen Abspielberechtigungszuordnungsanordnung effektuiert werden.

[0012] In einer Anordnung nach der vorliegenden Erfindung, Informationsträger den Merkmalen, definiert in Anspruch 3, hat es sich weiterhin als vorteilhaft herausgestellt, wenn außerdem die in Anspruch 5 definierten Maßnahmen getroffen werden. Dies hat den Vorteil, dass die Verbindungsbaufbauinformation einer Anzahl Abspielberechtigungszuordnungsanordnungen gespeichert werden kann und dass auf eine besonders einfache Art und Weise und mit einer sehr geringen Zeitverzögerung über die Datenverbindung Abspielberechtigungsbeantragungsinformation zu einer Abspielberechtigungszuordnungsanordnung geliefert werden kann.

[0013] In einer Anordnung nach der vorliegenden Erfindung mit den Merkmalen, definiert in Anspruch 2 hat es sich als vorteilhaft herausgestellt, wenn außerdem die in Anspruch 6 definierten Maßnahmen getroffen werden. Dies hat den Vorteil, dass auf Basis der Abspielberechtigungsbeantragungsinformation eine Abspielberechtigungszuordnungsanordnung detektieren kann, welches Bezahl-Informationssignal der Benutzer der Anordnung abspielen möchte. Dadurch ist Ermittlung der Gebühren auf eine besonders flexible Weise möglich. Es sei bemerkt, dass die in Anspruch 6 definierten Maßnahmen auch auf vorteilhafte Weise in Anordnungen nach der vorliegenden Erfindung mit den Merkmalen, wie in den Ansprüchen 3, 4 und 5 definiert, angewandt werden können.

[0014] In einer Anordnung nach der vorliegenden Erfindung mit den Merkmalen, definiert in Anspruch 2 hat es sich als vorteilhaft erwiesen, wenn außerdem die in Anspruch 7 definierten Maßnahmen getroffen werden. Dies hat den Vorteil, dass das Vorhandensein oder das Fehlen einer Abspielberechtigung für ein reproduziertes Bezahl-Informationssignal auf eine besonders einfache Art und Weise detektiert werden kann. Es sei bemerkt, dass die in Anspruch 7 definierten Maßnahmen auch auf vorteilhaft Weise in Anordnungen nach der vorliegenden Erfindung mit den Merkmalen, definiert in den Ansprüchen 3, 4, 5

und 6 angewandt werden können.

[0015] In einer Anordnung nach der vorliegenden Erfindung mit den Merkmalen, definiert in Anspruch 2 hat es sich als vorteilhaft herausgestellt, wenn außerdem die in Anspruch 8 definierten Maßnahmen getroffen werden. Durch die Lieferung von Schlüsselinformation bestehend aus erster Schlüsselinformation und zweiter Schlüsselinformation wird mit der Anordnung nach der vorliegenden Erfindung ein besonders hoher Schutzgrad vor Manipulation durch unberechtigte Personen erreicht. Derartige Verschlüsselungssysteme werden beispielsweise während der Übertragung entsprechend der "Digital Video Broadcasting Standard" angewandt. Es sei bemerkt, dass die in Anspruch 8 definierten Maßnahmen auch bei den Anordnungen nach der vorliegenden Erfindung mit den Merkmalen, wie in den Ansprüchen 3, 4, 5, 6 und 7 definiert, angewandt werden können.

[0016] In einer Anordnung nach der vorliegenden Erfindung mit den Merkmalen, definiert in Anspruch 1 hat es sich als vorteilhaft herausgestellt, wenn außerdem die in Anspruch 9 definierten Maßnahmen getroffen werden. Dies hat den Vorteil, dass die Reproduktion eines Bezahl-Informationssignals unterbrochen wird, bis eine Abspielberechtigung von einer Abspielberechtigungszuordnungsanordnung erscheint und der Benutzer der Anordnung folglich nicht einen Teil des Bezahl-Informationssignals während der Reproduktion dieses Signals überspringt. Es sei bemerkt, dass die in Anspruch 8 definierten Maßnahmen auch bei den Anordnungen nach der vorliegenden Erfindung mit den Merkmalen, wie in den Ansprüchen 2, 3, 4, 5, 6, 7 und 8 definiert, angewandt werden können.

[0017] Die oben genannten Aspekte sowie weitere Aspekte der vorliegenden Erfindung dürften auf der nachstehend als Beispiel beschriebenen Ausführungsform hervorgehen und werden auf Basis dieser Ausführungsform näher erläutert.

[0018] Ein Ausführungsbeispiel der Erfindung ist in der Zeichnung dargestellt und wird im vorliegenden Fall näher beschrieben. Es zeigen:

[0019] [Fig. 1](#) eine schematische Darstellung in Form eines Blockschaltbildes einer Anordnung nach der vorliegenden Erfindung, der ein verschlüsseltes Bezahl-Informationssignal zugeführt werden kann und die konstruiert ist zum unabhängigen Beantragen einer Abspielberechtigung für das Informationssignal beim Fehlen einer derartigen Abspielberechtigung.

[0020] [Fig. 1](#) zeigt eine Anordnung 1, bestehend aus einer sog. Set-Top-Box, konstruiert zur Überprüfung einer Abspielberechtigung für ein Bezahl-Informationssignal I, reproduziert mit Hilfe einer Repro-

duktionsanordnung, wobei dieses Informationssignal gegen Bezahlung verfügbar und deswegen verschlüsselt ist. Ein Informationssignal I kann beispielsweise durch einen DVHS-Videorecorder 2 reproduziert werden, der eine Aufzeichnungs- und Wiedergabebeanordnung bildet, oder durch ein DVD-Gerät 3, das eine Reproduktionsanordnung bildet. Wenn es eine Abspielberechtigung gibt, wird die Anordnung 1 einem Fernsehgerät 4 ein entschlüsseltes Informationssignal I liefern. Eine Abspielberechtigung kann gegeben werden durch die Tatsache, dass ein von der Wiedergabebeanordnung reproduziertes Informationssignal nicht verschlüsselt ist. Eine Abspielberechtigung für ein reproduziertes verschlüsseltes Bezahl-Informationssignal I wird gegeben durch das Vorhandensein einer Schlüsselinformation S, geeignet zum erfolgreichen Entschlüsseln des verschlüsselten Informationssignals I. Geeignete Schlüsselinformation S kann in der Anordnung 1 gespeichert sein oder kann von Abspielberechtigungszuordnungsmitteln 5 empfangen werden, die eine oder mehrere Abspielberechtigungszuordnungsanordnungen umfassen, die nachher noch näher erläutert werden.

[0021] Der DVHS-Videorecorder 2 umfasst Eingabemittel 6, die eine Abspieltaste 7 und eine Aufzeichnungstaste 8 umfassen. Durch Betätigung der Abspieltaste 7 kann der DVHS-Recorder 2 in die Abspielmode gebracht werden, in der auf eine allgemein bekannte Art und Weise der DVHS-Recorder 2 digitale Informationssignale I wiedergibt, die auf einem Magnetband 9 entsprechend der DVHS-Norm aufgezeichnet sind. Wiedergegebene Informationssignale I können über eine Operationsverbindung 10 ersten Schnittstellenmitteln 11 zugeführt werden. Die ersten Schnittstellenmittel 11 übertragen dann Informationssignale I und Steuersignale ST über einen allgemein bekannten Datenbus entsprechend der Busnorm IEEE1394. In der Abspielmode wiedergegebene Informationssignale I können von den ersten Schnittstellenmitteln 11 zweiten Schnittstellenmitteln 13 der Anordnung 1 über eine Busverbindung 12 zugeführt werden.

[0022] Das DVD-Gerät 3 umfasst Eingabemittel 14, die eine Abspieltaste 15 aufweisen. Durch Betätigung der Abspieltaste 15 kann das DVD-Gerät 3 in eine Abspielmode gebracht werden, in der auf allgemein bekannte An und Weise das DVD-Gerät 3 digitale Informationssignale I, die entsprechend der DVD-Norm auf einer DVD "Digital Versatile Disc" aufgezeichnet sind, wiedergibt. In der Abspielmode wiedergegebene Informationssignale I können den zweiten Schnittstellenmitteln 13 der Anordnung 1 über eine Operationsverbindung 17, über dritte Schnittstellenmittel 18 des DVD-Geräts 3 und die Busverbindung 12 zugeführt werden.

[0023] Die Anordnung 1 umfasst Überprüfungsmit tel 19 mit einem Informationssignaleingang 20 zum

Empfangen eines wiedergegebenen verschlüsselten Informationssignals I von den zweiten Schnittstellenmitteln **13**. Die Überprüfungsmittel **19** umfassen eine Verarbeitungsstufe **21**, bekannt als ein PIP-Selektor, und eine Schlüsselstufe **22**.

[0024] Ein wiedergegebenes verschlüsseltes Informationssignal I kann von dem Informationssignaleingang **20** der Wiedergabestufe **21** zugeführt werden. Ein wiedergegebenes verschlüsseltes Informationssignal I entsprechend der ISO/IEC 13818-1 Norm wird durch aufeinander folgende Informationssignalblöcke von je 188 Bytes gebildet. Diese Informationssignalblöcke können eine Anzahl Videokanäle und Audiokanäle sowie zusätzliche Information für einen Videokanal oder einen Audiokanal enthalten. Ein wiedergegebenes verschlüsseltes Informationssignal I enthält Freigabeinformation E, die zusätzliche Information bildet. Freigabeinformation E identifiziert eine Abspielberechtigungszuordnungsanordnung der Abspielberechtigungszuordnungsmittel **5**, die freigegeben oder berechtigt sind eine Abspielberechtigung für das Bezahl-Informationssignal I, das die Freigabeinformation E enthält, zuzuordnen.

[0025] Die Verarbeitungsstufe **21** hat einen Steuereingang **23**, über den Kanalsteuerinformation K von Eingangsmitteln **26** der Verarbeitungsstufe **21** zugeführt werden kann, wobei diese Eingangsmittel umfassen eine Vorwärtstaste **24** und eine Abwärtstaste **25**. Durch Betätigung der Vorwärtstaste **24** oder der Abwärtstaste **25** kann ein Videokanal und der in dem wiedergegebenen verschlüsselten Informationssignal I enthaltene Audiokanal selektiert werden. Der selektierte Videokanal, der zugeordnete Audiokanal sowie zusätzliche Information, die zu diesen zwei Kanälen gehört, kann in Form von Informationssignalblöcken von der Verarbeitungsstufe **21** einem Informationssignalausgang **27** der Verarbeitungsstufe **21** zugeführt werden. Freigabeinformation E, die mit dem selektierten Videokanal und dem zugehörigen Audiokanal assoziiert ist, kann einem Freigabeausgang **28** der Verarbeitungsstufe **21** zugeführt werden.

[0026] Wenn ein wiedergegebenes Informationssignal I ein Bezahl-Informationssignal I und deswegen verschlüsselt ist, ist das wiedergegebene Informationssignal I durch Verschlüsselung verschlüsselt – d.h. durch Zeitverschiebung der Informationssignalblöcke. Ein wiedergegebenes verschlüsseltes Informationssignal umfasst eine weitere zusätzliche zweite Schlüsselinformation S2, auch bekannt als ECM-Information in der DVB-Norm. Zweite Schlüsselinformation S2 enthält Information darüber, wie die verschlüsselten – d.h. zeitverschobenen – Informationssignalblöcke zu der richtigen Sequenz wiederhergestellt und folglich wie sie entschlüsselt werden sollen. Eine derartige zweite Schlüsselinformation S2 ist aber auch verschlüsselt und kann nur zusammenge setzte Schlüsselinformation S bilden, geeignet zum

Entschlüsseln eines wiedergegebenen verschlüsselten Informationssignals I im Zusammenhang mit der ersten Schlüsselinformation S1, die als EMM Information in der DVD-Norm bekannt ist und zum Entschlüsseln der zweiten Schlüsselinformation S2 dient. Um einen effektiven Schutz vor unberechtigtem Wiedergeben eines Bezahl-Informationssignals I durch nicht berechtigte Personen, wird die zweite Schlüsselinformation S2 zu kurzen periodischen Zeintervallen geändert. Die erste Schlüsselinformation S1 wird meist zu langen periodischen Intervallen geändert und wird als Zusatzinformation in einem Informationssignal I übertragen.

[0027] Eine Mitgliedskarte **29** kann in die Schlüsselstufe **22** eingesteckt werden, wobei diese Karte durch eine sog. Smart Card gebildet ist und in der durch Bezahlung von Mitgliedsgebühren erste Schlüsselinformation S1 gespeichert werden kann. Wenn durch Bezahlung von Gebühren durch den Inhaber der Mitgliedskarte **29** erlaubt die Mitgliedskarte **29** dem Inhaber der Mitgliedskarte **29** das Bezahl-Informationssignal I zu entschlüsseln und während der nächsten Wochen zu benutzen, wobei die neue erste Schlüsselinformation S1 in der Mitgliedskarte **29** gespeichert wird.

[0028] Von der Verarbeitungsstufe **21** kann zweite Schlüsselinformation S2 der Schlüsselstufe **22** zugeführt werden. Zusammen mit der Mitgliedskarte **29** ist die Schlüsselstufe **22** imstande, die zweite Schlüsselinformation S2 mit Hilfe der in der Mitgliedskarte **29** gespeicherten und einem ersten Schlüsseleingang **30** oder einem zweiten Eingang **31** zugeführten ersten Schlüsselinformation S1 zu Entschlüsseln. Im Falle einer Abspielberechtigung speichert die Mitgliedskarte **29** geeignete erste Schlüsselinformation S1 für die zweite Schlüsselinformation S2 in dem wiedergegebenen verschlüsselten Informationssignal I, wodurch die Schlüsselstufe **22** imstande ist die erste Schlüsselinformation S1 und die zweite Schlüsselinformation S2 gemeinsam zu verarbeiten und zusammenge setzte Schlüsselinformation S geeignet für eine einwandfreie Entschlüsselung des wiedergegebenen verschlüsselten Informationssignals I zu liefern. Dadurch können wiedergegebene verschlüsselte Informationssignale I dem Informationssignaleingang **20** der Überprüfungsmittel **19** zugeführt werden und im Falle einer Abspielberechtigung können die Überprüfungsmittel **19** zusammenge setzte Schlüsselinformation S für die einwandfreie Entschlüsselung des wiedergegebenen verschlüsselten Informationssignals I liefern. Durch die Lieferung zusammenge setzter Schlüsselinformation – gebildet durch die erste Schlüsselinformation S1, gespeichert in der Mitgliedskarte **29**, und durch die zweite Schlüsselinformation S2, anwesend in dem wiedergegebenen verschlüsselten Informationssignal I – wird mit der Anordnung nach der vorliegenden Erfindung ein besonders hoher Schutz vor Manipulation durch eine

unberechtigte Person erzielt.

[0029] Die zusammengesetzte Schlüsselinformation S kann Entschlüsselungsmitteln 32 zugeführt werden, die in dem vorliegenden Fall durch einen sog. Descrambler gebildet sind. Weiterhin kann ein verschlüsseltes Informationssignal I, das an dem Ausgang 27 der Verarbeitungsstufe 21 erscheint, den Entschlüsselungsmitteln 32 zugeführt werden. Entschlüsselung des Informationssignals I, das durch Verschlüsselung von Informationssignalblöcken verschlüsselt worden ist, wird durch Wiederherstellung der richtigen Zeitsequenz – d.h. durch Entschlüsselung – der Informationssignalblöcke des verschlüsselten Informationssignals I effektuiert.

[0030] Wenn das wiedergegebene Informationssignal I ein gebührenfreies und folglich nicht verschlüsseltes Informationssignal I ist, kann das Informationssignal I, das den Entschlüsselungsmitteln 32 zugeführt wird, unmittelbar zu einem Ausgang 33 der Entschlüsselungsmittel 32 befördert werden. Wenn aber ein wiedergegebenes Informationssignal I, verfügbar an dem Informationssignalausgang 27 der Verarbeitungsstufe 21 ein Bezahl-Informationssignal I ist, das infolgedessen verschlüsselt ist, versorgen die Entschlüsselungsmittel 32 eine Entschlüsselung des verschlüsselten Informationssignals I. Es sei bemerkt, dass die Entschlüsselungsmittel 32 – die nur zusammengesetzte Schlüsselinformation S, geeignet für die richtige Entschlüsselung des verschlüsselten Informationssignals I im Falle einer Abspielberechtigung – nur ein verschlüsseltes Informationssignal I an dem Ausgang 33 erzeugen in dem Fall, dass eine Abspielberechtigung verfügbar ist. Wenn aber keine Abspielberechtigung verfügbar ist und die Entschlüsselungsmittel 32 keine zusammengesetzte Schlüsselinformation S, geeignet für die richtige Entschlüsselung des verschlüsselten Informationssignals I empfangen, ist kein verschlüsseltes Informationssignal I sondern eher ein nicht einwandfrei verschlüsseltes und deswegen im Wesentlichen immer noch verschlüsseltes Informationssignal I an dem Ausgang 33 der Entschlüsselungsmittel 32 verfügbar.

[0031] Ein Informationssignal I, verfügbar an dem Ausgang 33 der Entschlüsselungsmittel 32, kann einer Demultiplexerstufe 34, vorgesehen in den Verarbeitungsmitteln 35, zugeführt werden, die in dem vorliegenden Fall auch einen Teil der Abfragemittel zur unabhängigen Beantragung einer Abspielberechtigung. Die Demultiplexerstufe 34 liefert die Videoinformationssignalblöcke entsprechend dem selektierten Videokanal und in dem Informationssignal I vorhanden, zu den ersten Decodermitteln 36 und liefert Audioinformationssignalblöcke entsprechend dem selektierten Audiokanal und in dem Informationssignal I vorhanden, zu zweiten Decodermitteln 37.

[0032] Die ersten Decodermittel 36 werden durch einen MPEG-Decoder gebildet und decodieren die Videoinformationssignalblöcke, die entsprechend einer MPEG-Norm codiert sind. Ein decodiertes digitales Videoinformationssignal kann von den ersten Decodermitteln 36 zu einem Digital-Analog-Wandler 38 zugeführt werden, der ein analoges Videoinformationssignal zu einem Videoausgang 39 der Anordnung 1 liefern kann. Die ersten Decodermittel 36 haben einen Steuerinformationsausgang 40, an dem Steuerinformation SI verfügbar ist, wenn die ersten Decodermittel 36 nicht erfolgreich die Videoinformationssignalblöcke decodiert haben. Dies ist der Fall, wenn durch das Fehlen einer Abspielberechtigung sich ein verschlüsseltes, sondern ein nicht einwandfrei verschlüsseltes und folglich verschlüsseltes Informationssignal erscheint und, dadurch nicht einwandfrei verschlüsselte, d.h. im Wesentlichen verschlüsselte Videoinformationssignalblöcke zu den ersten Decodermitteln 36 zugeführt werden.

[0033] Die zweiten Decodermittel 37 enthalten einen MPEG-Decoder und einen AC-3 Decoder und decodieren die Audiosignalblöcke, die entsprechend einer MPEG-Norm oder der AC-3 Norm codiert worden sind. Ein decodiertes digitales Audioinformationssignal kann von den zweiten Decodermitteln 37 zu einer Digital-Analog-Wandlerstufe 41 geliefert werden, die ein analoges Audioinformationssignal zu einem Audioausgang 42 der Anordnung 1 liefern kann.

[0034] Das Fernsehgerät 4 kann mit dem Videoausgang 39 und dem Audioausgang 42 verbunden sein und ein Informationssignal I wiedergeben.

[0035] Die Anordnung 1 nach der vorliegenden Erfindung umfasst nun Abfragemittel zum unabhängigen Beantragen einer Abspielberechtigung. Diese Anfragemittel umfassen Kommunikationsmittel 43, die beim Fehlen einer Abspielberechtigung für ein reproduziertes verschlüsseltes Informationssignal, das durch das Erscheinen von Steuerinformation SI gekennzeichnet ist, imstande sind, eine Datenverbindung mit wenigstens einer Abspielzuordnungsanordnung der Abspielberechtigungszuordnungsmittel S herzustellen. Dazu kann Steuerinformation an dem Steuerinformationsausgang 40 der ersten Decodermittel 36 einer Steuereinheit 44 der Kommunikationsmittel 43 zugeführt werden. Weiterhin kann Freigabeinformation E, verfügbar an dem Freigabeausgang 28 der Verarbeitungsstufe 21, der Steuereinheit 44 zugeführt werden. Die Kommunikationsmittel 43 umfassen weiterhin Speichermittel 45, die mit der Steuereinheit 44 verbunden sind und Verbindungsaufrbauinformation der Abspielberechtigungszuordnungsanordnungen 5 der Abspielberechtigungszuordnungsmittel speichern, wobei diese Anordnungen durch Freigabeinformation E gekennzeichnet sind. Verbindungsaufrbauinformation kann durch eine Telefon-

nummer einer Abspielberechtigungszuordnungsanordnung, eine bestimmte Adresse in einem Funkübertragungsnetzwerk oder durch einen bestimmten Rückwegkanal eines Kabelsystems gebildet werden, wie dies nachstehend noch näher beschrieben wird.

[0036] Zur Kommunikation mit einer Abspielberechtigungszuordnungsanordnung der Abspielberechtigungszuordnungsmittel 5 umfassen die Kommunikationsmittel 43 eine erste Kommunikationsstufe 46, eine zweite Kommunikationsstufe 47 und eine dritte Kommunikationsstufe 48. In dem vorliegenden Fall ist die erste Kommunikationsstufe 46 durch einen sog. Modem gebildet, der eine Datenverbindung bildet, geformt durch eine Telefonverbindung 49. Zum Aufbauen einer Telefonverbindung 49 hat die erste Kommunikationsstufe 46 einen Eingang 50 zum Empfangen von Verbindungsaufbauinformation in Form einer Telefonnummer einer Gebühreneinnahmeanordnung, die gleichzeitig eine erste Abspielberechtigungszuordnungsanordnung 51 der Abspielberechtigungszuordnungsmittel 5 bildet. Weiterhin kann Verbindungsaufbauinformation in Form einer weiteren Telefonnummer zu dem Eingang 50 der ersten Kommunikationsstufe 46 zugeführt werden, mit deren Hilfe eine weitere Telefonverbindung 52 zwischen der ersten Kommunikationsstufe 4 und einer ersten Funkstation aufgebaut werden kann, die gleichzeitig eine zweite Abspielberechtigungszuordnungsanordnung 53 der Abspielberechtigungszuordnungsmittel 5 bildet. Die erste Sendestration überträgt Fernsehprogramme in Form verschlüsselter oder nicht verschlüsselter Informationssignale I per Satteliten über eine Satellitenverbindung 54. Weiterhin darf die erste Sendestration Abspielberechtigungen für Bezahl-Fernsehprogramme herausgeben, die von der ersten Sendestration übertragen werden, wobei diese Programme in einer Aufzeichnungs- und Wiedergabebeanordnung aufgezeichnet werden und zu einem späteren Zeitpunkt wiedergegeben werden können.

[0037] Verbindungsaufbauinformation in Form einer Adresse in einem Funkübertragungsnetzwerk kann einem Eingang 54 der zweiten Kommunikationsstufe 47 zugeführt werden. Unter Verwendung der Adresse in einem Funkübertragungsnetzwerk baut die zweite Kommunikationsstufe 47 eine Datenverbindung in Form einer Mikrowellenverbindung 56 zwischen der zweiten Kommunikationsstufe 47 und einer zweiten Sendestration auf, die gleichzeitig eine dritte Abspielberechtigungszuordnungsanordnung 57 der Abspielberechtigungszuordnungsmittel 5 bildet. Dazu kann die zweite Kommunikationsstufe 47 einer Mikrowellenantenne 58 Mikrowellensignale liefern. Derartige Mikrowellenverbindungen zwischen einer Sendestration und einer Set-Top-Box sind als "Drahtloskabel"-Funkverbindungen bekannt. Die zweite Sendestration 57 überträgt Fernsehprogramme, die aus verschlüsselten oder nicht verschlüsselten Informationssignalen I bestehen, über die Mikrowellen-

verbindung 56 und darf Abspielberechtigungen für Fernsehprogramme zuordnen, die von der zweiten Sendestration übertragen werden, die in einer Aufzeichnungs- und Wiedergabebeanordnung aufgezeichnet werden und die zu einem späteren Zeitpunkt wiedergegeben werden können.

[0038] Die dritte Kommunikationsstufe 48 baut über ein Kabelfernsehsystem 59 eine Datenverbindung mit einer Kabelfernseheinheit auf, wobei diese Kabelfernseheinheit ebenfalls eine Sendestration sowie eine vierte Abspielberechtigungszuordnungsanordnung 60 der Abspielberechtigungszuordnungsmittel 5 bildet. Dazu empfängt ein Eingang 61 der dritten Kommunikationsstufe 48 Kanalinformation, die den Umkehrkanal für die Übertragung von Information zu der Kabelfernseheinheit kennzeichnet. Die Kabelfernseheinheit ist dazu vorgesehen, Fernsehprogramme zu übertragen, die aus verschlüsselten oder nicht verschlüsselten Informationssignalen I bestehen, und zwar über das Kabelfernsehsystem 59 übertragen werden und darf Abspielberechtigungen für Bezahl-Fernsehprogramme zuordnen, die von der Kabelfernseheinheit übertragen werden, die in einer Aufzeichnungs- und Wiedergabebeanordnung aufgezeichnet werden und die zu einem späteren Zeitpunkt wiedergegeben werden können.

[0039] Alle Verbindungsaufbauinformation – die erste und die zweite Telefonnummer, die Adresse in einem Funkkommunikationsnetzwerk und die Kanalinformation – wird in den Speichermitteln 45 derart gespeichert, dass wenn Freigabeinformation E, die eine der Abspielberechtigungszuordnungsanordnungen 51, 53, 57 und 60 der Freigabeberechtigungszuordnungsmittel 5 kennzeichnet, erscheint, die Steuereinheit 44 dafür sorgt, dass die betreffende Verbindungsaufbauinformation aus den Speichermitteln 45 ausgelesen werden. Die auf diese An und Weise ausgelesene Verbindungsaufbauinformation ermöglicht es, dass eine Datenverbindung von den Kommunikationsmitteln 43, d.h. von der Anordnung 1, zu der Abspielberechtigungszuordnungsanordnung 51, 53, 57 oder 60 aufgebaut wird, identifiziert durch die Freigabeinformation E. Die Steuereinheit 44 liefert aus den Speichermitteln 45 ausgelesene Verbindungsaufbauinformation zu dem Eingang 50 der ersten Kommunikationsstufe 46, oder zu dem Eingang der zweiten Kommunikationsstufe 47, oder aber zu dem Eingang 61 der dritten Kommunikationsstufe 48 in Abhängigkeit von dem Typ der Verbindungsaufbauinformation, die ausgelesen worden ist. Verbindungsaufbauinformation in Form von Telefonnummern wird dann der ersten Kommunikationsstufe 46 zugeführt, Verbindungsaufbauinformation in Form von Adressen in einem Funkkommunikationsnetzwerk wird der zweiten Kommunikationsstufe 47 zugeführt und Verbindungsaufbauinformation in Form von Kanalinformation wird der dritten Kommunikationsstufe 48 geliefert.

[0040] Wenn ein verschlüsseltes Bezahl-Informati onssignal I von einer gekauften vorweg aufgezeichneten DVHS-Kassette mit Hilfe des DVHS-Videorecorders 2 wiedergegeben werden soll und die erste Schlüsselinformation S1, erforderlich zur Entschlüsselung der zweiten Schlüsselinformation S2 in dem Bezahl-Informationssignal I nicht in der Mitgliedskarte der Schlüsselstufe 22 gespeichert ist, gibt es keine Abspielberechtigung. Wenn eine gekaufte oder eine frei verteilte vorweg aufgezeichnete DVHS-Kassette von einer Firma hergestellt worden ist, welche die Gebühreneinnahme zum Abspielen des verschlüsselten Bezahl-Informationssignals I, aufgezeichnet auf der vorweg aufgezeichneten DVHS-Kassette zu einer Gebühreneinnahmeanordnung übertragen hat, die durch die erste Abspielberechtigungsanordnung 51 gebildet ist, enthält das Informationssignal, aufgezeichnet auf dieser DVHS-Kassette Freigabeinformation, welche diese erste Abspielberechtigungsanordnung 51 identifiziert.

[0041] Durch Betätigung der Abspieltaste 7 kann der DVHS-Videorecorder 2 in die Abspielmode gebracht werden zum Wiedergaben des verschlüsselten Bezahl-Informationssignals von der DVHS-Kassette in dem DVHS-Videorecorder. Das wiedergegebene verschlüsselte Informationssignal I kann dem Informationssignaleingang 20 und ggf. über die ersten Schnittstellenmittel 11, die Busverbindung 12 und die zweiten Schnittstellenmittel 13 der Verarbeitungsstufe 21 der Überprüfungsmittel 19 zugeführt werden. Die Freigabeinformation E in dem wiedergegebenen verschlüsselten Informationssignal I wird von der Verarbeitungsstufe 21 detektiert und wird dem Freigabeausgang 28 zugeführt. Auf eine in [Fig. 1](#) nicht dargestellte Art und Weise kann der Benutzer der Anordnung 1 angespornt werden, eine Mitgliedskarte 29 einzugeben, die durch die erste Abspielberechtigungsanordnung 51 zur Verfügung gestellt wird.

[0042] Wenn die Mitgliedskarte 29 nicht die richtige erste Schlüsselinformation S1 enthält und wenn es folglich keine Abspielberechtigung für das von der vorweg aufgezeichneten DVHS-Kassette wiedergegebene verschlüsselte Informationssignal I gibt, können die Entschlüsselungsmittel 32 kein entschlüsseltes Informationssignal I an dem Ausgang 33 erzeugen. Dadurch können die Videoinformationssignalböcke in dem wiedergegebenen verschlüsselten Informationssignal I nicht einwandfrei decodiert werden, wodurch die ersten Decodermittel 36 Steuerinformation SI zu der Steuereinheit 44 liefern. Das von der Verarbeitungsstufe 21 detektierte und an dem Freigabeausgang 28 dieser Stufe verfügbare Freigabeinformationssignal E wird auch der Steuereinheit 44 zugeführt. Die Steuereinheit 44 liest danach die erste Telefonnummer aus den Speichermitteln 45 aus, und zwar zum Aufbauen der Telefonverbindung 49 mit der ersten Abspielberechtigungsanordnungs-

nordnung 51, identifiziert durch die Freigabeinformation E und überträgt diese erste Telefonnummer zu der ersten Kommunikationsstufe 46. Die erste Kommunikationsstufe 46, gebildet durch einen Modem, wählt die erste Telefonnummer der ersten Abspielberechtigungsanordnung 51 und baut auf diese Art und Weise die Telefonverbindung 49 auf. Nach einem erfolgreichen Aufbau der Telefonverbindung 49 kann die Steuereinheit 44 der ersten Abspielberechtigungsanordnung 51 über die erste Kommunikationsstufe 46 und über die erste Telefonverbindung 49 Abspielberechtigungsbeantragungsinformation liefern.

[0043] Mit Hilfe der Abspielberechtigungsbeantragungsinformation überprüft die erste Abspielberechtigungsanordnung 51, die durch die Gebühreneinnahmeanordnung gebildet wird, ob es möglich ist, die Gebühren über die bestehende Mitgliedschaft des Inhabers der Mitgliedskarte 29 mit der ersten Abspielberechtigungsanordnung 51 einzunehmen. Auf Basis der Abspielberechtigungsbeantragungsinformation, die beispielsweise das Aufzeichnungsdatum des wiederzugebenden Informationssignals I umfasst, kann die erste Abspielberechtigungsanordnung 51 erste Schlüsselinformation S1 ermitteln, wobei diese ersten Schlüsselinformation S1 notwendig ist, dies im Zusammenhang mit der zweiten Information S2 in dem Bezahl-Informationssignal I, zum Bilden zusammengesetzter Schlüsselinformation S, geeignet für die richtige Entschlüsselung des wiedergegebenen verschlüsselten Bezahl-Informationssignals I. Wenn es eine Möglichkeit gibt, die Gebühren von dem Inhaber der Mitgliedskarte 29 in der ersten Abspielberechtigungsanordnung 51 einzunehmen und wenn die richtige erste Schlüsselinformation S1 detektiert worden ist, kann die erste Abspielberechtigungsanordnung 51 dadurch eine Abspielberechtigung abgeben, dass die erste Schlüsselinformation S1 zu der Steuereinheit 44 der Kommunikationsstufe 43 über die erste Telefonverbindung 49 und die erste Kommunikationsstufe übertragen wird. Wenn die erste Schlüsselinformation S1 in der Steuereinheit 44 verfügbar ist, kann die Steuereinheit 44 die erste Schlüsselinformation S1 dem ersten Schlüsseleingang 30 der Schlüsselstufe 22 zu führen. Wenn die erste Schlüsselinformation S1 in der Schlüsselstufe 22 erscheint, wird die Schlüsselstufe 22 freigegeben zum Überschreiben der ersten Schlüsselinformation S1, die vorher in der Mitgliedskarte 29 gespeichert war, mit der Schlüsselinformation S1, die an dem Schlüsseleingang 30 empfangen wird. Die Schlüsselstufe 22 liefert zusammengesetzte Schlüsselinformation S, die geeignet ist zum einwandfreien Entschlüsseln des wiedergegebenen Bezahl-Informationssignals I, zu den Entschlüsselungsmitteln 32. Dadurch können die Entschlüsselungsmittel das wiedergegebene verschlüsselte Informationssignal I mit Hilfe der zusammengesetzten Schlüssel-

information S entschlüsseln und die Verarbeitungsmittel **35** können das wiedergegebene Informationsignal I zu einem Videoinformationssignal verarbeiten, das an dem Videoausgang **39** verfügbar ist und zu einem Audioinformationssignal, das an dem Audioausgang **42** verfügbar ist.

[0044] Auf diese Weise ist die Anordnung **1** nach der vorliegenden Erfindung geeignet zum unabhängigen Beantragen einer Abspielberechtigung. Wenn die erste Schlüsselinformation S1, die eine Abspielberechtigung darstellt, empfangen wird, wird der Anordnung **1** die Möglichkeit geboten, ein wiedergegebenes Informationssignal I zu entschlüsseln. Manipulation durch nicht berechtigte Personen wird nahezu völlig ausgeschlossen, weil charakteristische Kaufinformation, welche die Anzahl Abspieldurchführungen von Bezahl-Informationssignalen spezifiziert, bei Empfang von Abspielberechtigungsbeantragungsinformation in der ersten Abspielberechtigungszuordnungsanordnung **51** erzeugt wird und deswegen durch einen Benutzer der Anordnung **1** nicht illegal geändert werden kann. Weiterhin kann das Einnehmen der Gebühren von dem Benutzer der Anordnung **1** nach der vorliegenden Erfindung zu relativ kurzen Zeitintervallen und mit einem besonders geringen Aufwand mit Hilfe der ersten Abspielberechtigungszuordnungsanordnung **51**, d.h. mit der Abspielberechtigungsanordnung erfolgen. Die erste Abspielberechtigungszuordnungsanordnung **51** kann dann das Einnehmen von Gebühren für eine Anzahl vorweg aufgezeichneter DVHS-Kassetten und andere digitale Aufzeichnungsmedien erledigen. Dieser Vorteil der gemeinsamen Einnahme von Gebühren ist insbesondere dadurch erzielbar, dass die Freigabeinformation E in jedem Bezahl-Informationssignal I eine betreffende Abspielberechtigungszuordnungsanordnung identifiziert, die eine Abspielberechtigung zuordnen darf.

[0045] Weiterhin ist es sehr vorteilhaft, dass das Aufbauen der Datenverbindung das Liefern der Abspielberechtigungsbeantragungsinformation und das Erhalten der Abspielberechtigung bis zur richtigen Entschlüsselung des wiedergegebenen verschlüsselten Bezahl-Informationssignals I innerhalb eines sehr kurzen Zeitintervalls effektuiert werden kann, wodurch der Benutzer der Anordnung **1** nach der vorliegenden Erfindung nur sehr kurz zu warten braucht, bevor das Bezahl-Informationssignal abgespielt wird.

[0046] Ein weiterer Vorteil der Gebühreneinnahme ist, dass ein Hersteller vorweg aufgezeichneter Datenträger – wie DVHS-Kassetten, DVDs oder CD-ROMs – Kunden einen vorweg aufgezeichneten Datenträger geben kann und jeweils beim Abspielen des vorweg aufgezeichneten Aufzeichnungsträgers durch Gebühreneinnahme verdienen kann.

[0047] In einem zweiten Beispiel einer Applikation kann ein verschlüsseltes Bezahl-Informationssignal I mit Hilfe des DVD-Geräts **3** von einer DVD **16** wiedergegeben werden. Die Freigabeinformation E in dem wiedergegebenen verschlüsselten Informationssignal I identifiziert die erste Sendestation als eine zweite Abspielberechtigungszuordnungsanordnung **53**, berechtigt, eine Abspielberechtigung zuzuordnen. Beim Fehlen einer Abspielberechtigung, die – wie oben bereits erwähnt – gekennzeichnet ist durch das Auftreten von Steuerinformation S1, sind die Kommunikationsmittel imstande, eine Datenverbindung aufzubauen, die durch die Telefonverbindung **52** gebildet wird, und zwar zu der ersten Sendestation, die durch die Freigabeinformation E identifiziert ist. Die Kommunikationsmittel **43** liefern weiterhin Abspielberechtigungsbeantragungsinformation zu der ersten Sendestation über die Telefonverbindung **52** und empfangen eine Abspielberechtigung für das wiedergegebene verschlüsselte Informationssignal I von der ersten Sendestation über die Telefonverbindung **52**. Nachdem die erste Schlüsselinformation S1, welche die Abspielberechtigung darstellt, empfangen worden ist und nachdem die erste Schlüsselinformation S1 in der Mitgliedskarte **29** gespeichert worden ist, kann das verschlüsselte Bezahl-Informationssignal I auf einwandfreie Art und Weise in den Entschlüsselungsmitteln **32** entschlüsselt werden und kann mit Hilfe des Fernsehgeräts **4** wiedergegeben werden.

[0048] In einem dritten Beispiel einer Applikation identifiziert Freigabeinformation E, die in einem wiedergegebenen verschlüsselten Bezahl-Informationssignal I enthalten ist und die von einer Festplatte eines in der [Fig. 1](#) nicht dargestellten Computers wiedergegeben wird, die zweite Sendestation als die dritte Abspielberechtigungszuordnungsanordnung **57** für das wiedergegebene verschlüsselte Bezahl-Informationssignal I. In dem vorliegenden Fall wird Abspielberechtigungsbeantragungsinformation über die zweite Kommunikationsstufe **47** und die Mikrowellenantenne **58** mit Hilfe der Mikrowellenverbindung **56** von der Steuereinheit **44** zu der zweiten Sendestation übertragen. In dem Fall einer Abspielberechtigung, die von der zweiten Sendestation zugeordnet worden ist, wird diese Berechtigung über die Mikrowellenverbindung **56**, die Mikrowellenantenne **58** und die zweite Kommunikationsstufe **47** zu der Steuereinheit übertragen und wird in der Mitgliedskarte **29** gespeichert, wodurch auf diese Art und Weise eine einwandfreie Entschlüsselung des wiedergegebenen verschlüsselten Informationssignals S1 ermöglicht wird.

[0049] Bei einem weiteren Beispiel einer Applikation identifiziert Freigabeinformation E, die in einem verschlüsselten Bezahl-Informationssignal I enthalten ist, das mit Hilfe eines DVD-Geräts **3** von einer DVD wiedergegeben wird, die Kabelfernseheinheit, d.h.

die vierte Abspielberechtigungszuordnungsanordnung **60**. In dem vorliegenden Fall wird Abspielberechtigungsbeantragungsinformation, die das abzuspielende Bezahl-Informationssignal identifiziert, über das Kabelfernsehsystem **59** über den durch die Kanalinformation identifizierten Rückkehrkanal zu dem Kabelfernsehseinheit übertragen. Die Kabelfernsehseinheit kann erste Schlüsselinformation SI, die eine Abspielberechtigung darstellt, über denselben Kanal oder über einen anderen Kanal des Kabelfernsehsystems **59** zu den Kommunikationsmitteln **43** übertragen.

[0050] Auf diese Weise liefern die Kommunikationsmittel **43** der Anordnung **1** nach der vorliegenden Erfindung Abspielberechtigungsbeantragungsinformation, die das wiedergegebene verschlüsselte Informationssignal I identifiziert und empfangen erste Schlüsselinformation SI, die von der Abspielberechtigungsbeantragungsinformation abhängig ist, von wenigstens einer Abspielberechtigungszuordnungsanordnung. Dies bietet den Vorteil, dass auf Basis der Abspielberechtigungsbeantragungsinformation jede Abspielberechtigungszuordnungsanordnung detektieren kann, welches Bezahl-Informationssignal I von dem Benutzer der Anordnung **1** wiedergegeben werden soll. Auf diese Weise ist es möglich, für einen auf einer vorweg aufgezeichneten DVHS-Videokassette aufgezeichneten besonders beliebten Film mehr Gebühren einzunehmen als für einen weniger beliebten Film. Weiterhin kann der Betrag der Gebühren davon abhängig sein, ob ein abzuspielender Film bereits öfters von dem Inhaber der Mitgliedskarte abgespielt wurde und ein Mengenrabatt gewährt werden kann.

[0051] Die Anordnung **1** umfasst weiterhin Steuermittel **62**, denen die Steuerinformation SI von dem Steuerinformationsausgang **40** der ersten Decodermittel beim Fehlen einer Abspielberechtigung zugeführt werden kann. Die Steuermittel **62** können weiterhin Abspielberechtigungsinformation WB von der Steuereinheit **44** erhalten, wobei diese Information von der Steuereinheit **44** geliefert wird, wenn erste Schlüsselinformation SI, die von einer Abspielberechtigungszuordnungsanordnung geliefert wird, verfügbar ist. Beim Fehlen einer Abspielberechtigung für ein von dem DVHS-Videorecorder **2** wiedergegebenes Bezahl-Informationssignal I, wobei dieses Fehlen durch das Auftreten von Steuerinformation SI gekennzeichnet wird, liefern die Steuermittel **62** über die zweiten Schnittstellenmittel **13** die Busverbindung **12** und die ersten Schnittstellenmittel **11** Pauseinformation zu dem DVHS-Recorder **2** um die Wiedergabe des Bezahl-Informationssignals zu unterbrechen. Weiterhin, wenn es danach eine Abspielberechtigung für das von dem DVHS-Videorecorder **2** wiedergegebene Bezahl-Informationssignal I gibt, wobei dieses Vorhandensein durch das Auftreten von Abspielberechtigungsinformation WB gekennzeichnet ist, liefern die Steuermittel **62** Ende-der-Pause-Information

zu dem DVHS-Recorder **2**, und zwar über die zweiten Schnittstellenmittel **13**, die Busverbindung **12** und die erste Schnittstelle **11** und bringen den DVHS-Recorder **2** in die Abspielmode. Ähnliche Pause-Information und Ende-der-Pause-Information kann jeder beliebigen Wiedergabebeanordnung zugeführt werden, d.h. auch dem DVD-Gerät **3** – der über die Busverbindung **12** mit den zweiten Schnittstellenmitteln **13** verbunden ist und ein verschlüsseltes Informationssignal I liefert.

[0052] Dies bietet den Vorteil, dass die Wiedergabe eines Bezahl-Informationssignals I unterbrochen wird, bis eine Abspielberechtigung von einer Abspielberechtigungszuordnungsanordnung vorhanden ist und der Benutzer der Anordnung **1** folglich keinen Teil des Bezahl-Informationssignals I zu verpassen braucht, wenn dieses wiedergegeben wird.

[0053] Die Anordnung **1** umfasst weiterhin Empfangsmittel **63** zum Empfangen eines verschlüsselten oder nicht verschlüsselten Informationssignals I von einer Anzahl Sendestationen. Dazu empfängt eine Empfangsstufe **64** der Empfangsmittel **63** Informationssignale I von der Kabelfernsehseinheit, d.h. von der vierten Abspielberechtigungszuordnungsanordnung **60** über das Kabelfernsehsystem **59** und von der zweiten Sendestation, d.h. der dritten Abspielberechtigungszuordnungsanordnung **57**, über die Mikrowellenverbindung **56** und die Mikrowellenantenne **58**. Weiterhin empfängt die Tunerstufe **64** Informationssignale ω von einer dritten Sendestation **65** über eine terrestrische Funkverbindung **66** und eine terrestrische Antenne **68**, vorgesehen in einer Antennenstufe **67**. Außerdem kann die Tunerstufe **64** über die Satellitenverbindung **54** und eine Satellitenantenne **69** der Antennenstufe **67** Informationssignale I von der ersten Sendestation **53** empfangen.

[0054] Kanalsteuerinformation K, die von den Eingabemitteln **26** durch Betätigung der Vorwärtstaste **24** oder der Rückwärtstaste **25** erzeugt werden kann, kann der Tunerstufe **64** und dem Steuereingang **23** der Verarbeitungsstufe **21** zugeführt werden. Je nach der Kanalsteuerinformation K wird ein in der Tunerstufe **64** empfangenes Informationssignal I dem Informationssignaleingang **20** der Überprüfungsmittel **19** zugeführt. Ein dem Informationssignaleingang **20** zugeführtes Informationssignal I kann der Verarbeitungsstufe **21** zugeführt werden. In der Verarbeitungsstufe **21** – wie bereits oben erwähnt – werden die Informationssignalblöcke des Videokanals und des zugeordneten Audiokanals, der mit Hilfe der Vorwärtstaste **24** und der Rückwärtstaste **25** selektiert worden sind, sowie die zusätzliche Information, die mit der Information in diesen zwei Kanälen assoziiert ist – insbesondere die entsprechende Freigabeinformation E und die zweite Schlüsselinformation S2 – auf Basis der Kanalsteuerinformation K selektiert. Die selektierte Information kann an dem Informati-

onssignalausgang **27** verfügbar gemacht werden. Ein an dem Informationssignalausgang **27** verfügbare Informationssignal I – wobei dieses Signal ein Bezahl-Informationssignal I sein kann, das folglich verschlüsselt ist und das dann Freigabeinformation E enthält, die eine Abspielberechtigungsanordnung identifiziert, die eine Abspielberechtigung für das verschlüsselte Informationssignal I zuordnen darf – kann den zweiten Schnittstellenmitteln **13** der Anordnung **1** zugeführt werden. Es sei bemerkt, dass es auch möglich ist, eine Anzahl Videokanäle, Audio-kanäle sowie zusätzliche Information zu selektieren, die mit der Information in diesen zwei Kanälen assoziiert ist und all diese Information mit Hilfe des DV-HS-Videorecorders **2** aufzuzeichnen.

[0055] Erste Schlüsselinformation S1 in dem von einer Sendestation empfangenen Informationssignal kann in der Verarbeitungsstufe **21** detektiert werden und kann dem zweiten Schlüsseleingang **31** der Schlüsselstufe **22** zugeführt werden, und zwar zum Speichern der ersten Schlüsselinformation S1 in der Mitgliedskarte **29**.

[0056] Durch Betätigung der Aufzeichnungstaste **8** der Eingabemittel **6** des DVHS-Videorecorders **2**, der eine Aufzeichnungs- und Wiedergabebeanordnung bildet, kann der DVHS-Videorecorder **2** in eine Aufzeichnungsmodus gebracht werden. Wenn die Aufzeichnungsmodus aktiv ist, kann der DVHS-Videorecorder **2** Informationssignale I aufzeichnen, die über die Busverbindung **12** von den zweiten Schnittstellenmitteln **13** den ersten Schnittstellenmitteln **11** zugeführt werden, und zwar über die Arbeitsverbindung **10** auf dem Magnetband **9** einer DVHS-Kassette. Ein Mit Hilfe des DVHS-Videorecorders **2** aufgezeichnetes Bezahl-Informationssignal I kann in einer durch Betätigung der Abspieltaste **7** in einer Wiedergabemode wiedergegeben werden, wie oben bereits erwähnt wurde.

[0057] Dies bietet den Vorteil, dass auch für einen von einer Sendestation übertragenen und auf einer DVHS-Kassette mit Hilfe des DVHS-Videorecorders **2** aufgezeichneten Film die Sendestation Gebühren für jede Wiedergabe des Bezahl-Films einnehmen kann.

[0058] In dieser Hinsicht sei es bemerkt, dass eine Abspielberechtigung für ein von der dritten Sendestation **65** geliefertes Bezahl-Informationssignal I durch die Gebühreneinnahmeanordnung, d.h. die erste Abspielberechtigungsanordnung **51**, die durch die dritte Sendestation **65** Erlaubnis hat, Abspielberechtigungen zuzuordnen, gewährt werden kann.

[0059] Es sei bemerkt, dass alle Abspielberechtigungsanordnungen Speichermittel enthalten, die imstande sind, Information über alle Be-

zahl-Informationssignale I, für welche die betreffende Abspielberechtigungsanordnung eine Abspielberechtigung abgeben darf, zu speichern. Diese Information umfasst insbesondere Identifikationsinformation, die auch in Abspielberechtigungsbeantragungsinformation vorhanden ist und die das wiederzugebende Informationssignal I identifiziert. Weiterhin ist es für die Identifikationsinformation, die jedes Bezahl-Informationssignal identifiziert möglich, assoziierte erste Schlüsselinformation S1 zum Entschlüsseln des verschlüsselten Informationssignals sowie Bezahlinformation zu speichern, die den zu bezahlenden Gebührenbetrag für das betreffende Bezahl-Informationssignal angibt.

[0060] Es sei bemerkt, dass die Speichermittel **45** bereits Verbindungsaubauinformation enthalten, wenn eine Anordnung **1** nach der vorliegenden Erfindung gekauft wird. Weiterhin kann Verbindungsaubauinformation für eine neue Abspielberechtigungsanordnung auf einer assoziierten Mitgliedskarte **29** gespeichert werden, wobei diese Information über eine in [Fig. 1](#) nicht dargestellte Verbindung der Steuereinheit **44** zugeführt werden kann, damit die Verbindungsaubauinformation in den Speichermitteln **55** gespeichert werden kann, wenn die Mitgliedskarte **29** in die Schlüsselstufe **22** eingegeben wird. Weiterhin kann eine neue Abspielberechtigungsanordnung über eine Datenverbindung der Anordnung **1** die entsprechende Verbindungsaubauinformation zuführen, damit die Verbindungsaubauinformation in den Speichermitteln **45** gespeichert werden.

[0061] Es sei bemerkt, dass die Kommunikationsmittel auch eine Datenverbindung mit einem Internet-Netzwerkserver aufbauen können, der aus einer Abspielberechtigungsanordnung besteht.

[0062] Weiterhin sei es bemerkt, dass eine Anordnung nach der vorliegenden Erfindung auch unmittelbar in einem Videorecorder, in einem DVD-Gerät oder aber in einem Fernsehempfänger vorgesehen werden kann.

[0063] In der oben als Beispiel beschriebenen Ausführungsform umfassen die Abfragemittel zum unabhängigen Beantragen einer Abspielberechtigung für ein wiedergegebenes verschlüsseltes Informationssignal im Grunde die Kommunikationsmittel **43** und die Verarbeitungsmittel **35**, von denen die ersten Decodermittel **36** gleichzeitig als Detektionsmittel zum Detektieren eines verschlüsselten und eines nicht verschlüsselten Informationssignals wirksam sind. Es hat sich herausgestellt, dass eine derartige Konstruktion der Abfragemittel in der Praxis besonders vorteilhaft ist. Es sei aber bemerkt, dass auf alternative Weise eine Anordnung nach der vorliegenden Erfindung anders konstruierte Abfragemittel enthalten

kann. Derartige Abfragemittel können beispielsweise Mittel enthalten, in denen die ersten Decodermittel zum Decodieren codierter Videoinformationssignalblöcke nicht gleichzeitig mit den Detektormitteln zum Detektieren verschlüsselter oder nicht verschlüsselter Informationssignale benutzt werden, sondern wobei separate Detektormittel vorgesehen sind, durch die verschlüsselte oder nicht verschlüsselte Informationssignale detektiert werden können. Es ist auch möglich, Abfragemittel mit Kommunikationsmitteln zu versehen, die einen anderen Schaltungsentwurf haben als in der Anordnung nach der vorliegenden Erfindung, die anhand der [Fig. 1](#) beschrieben worden ist.

Patentansprüche

1. Anordnung (1) zum Überprüfen einer Abspielberechtigung für ein reproduziertes verschlüsseltes Informationssignal – das mit Hilfe einer Wiedergabe-anordnung (2, 3) wiedergegeben wird, die dazu vorgesehen ist, mit der Anordnung (1) zusammenzuarbeiten, – und zum Liefern eines verschlüsselten Informationssignals, wenn eine Wiedergabeberechtigung verfügbar ist, wobei diese Anordnung die nachfolgenden Elemente umfasst:

- Überprüfungsmitte (19) vorgesehen zum Empfangen eines reproduzierten verschlüsselten Informationssignals (I) und vorgesehen zum Liefern von Schlüsselinformation (S) geeignet zum einwandfreien Entschlüsseln des reproduzierten verschlüsselten Informationssignals, wenn eine Wiedergabeberechtigung verfügbar ist, und
- Entschlüsselungsmittel (32) vorgesehen zum Empfangen von Schlüsselinformation (S) und vorgesehen zum Entschlüsseln des reproduzierten verschlüsselten Informationssignals (I), wenn geeignete Schlüsselinformation (S) verfügbar ist, **dadurch gekennzeichnet**, dass die Anordnung (1) ausgebildet ist mit Abfragemitteln (35, 43) zum automatischen und unabhängigen Be-antragen einer Wiedergabeberechtigung von einem Wiedergabeberechtigungsanordnungsmittel (5) wenn eine Wiedergabeberechtigung für das genann-te reproduzierte verschlüsselte Informationssignal, das empfangen wird, fehlt.

2. Anordnung (1) nach Anspruch 1, dadurch gekennzeichnet, dass die Abfragemittel (35, 43) Kommunikationsmittel (43) enthalten, die beim Fehlen einer Wiedergabeberechtigung für ein reproduziertes verschlüsseltes Informationssignal eine Datenverbindung (49, 52, 56, 59) zwischen den Kommunikations-mitteln (43) und wenigstens einer Wiedergabebe-rechtigungsanordnungsanordnung (51, 53, 57, 60) aufbauen, und die Kommunikationsmittel (43) über die Datenverbindung (49, 52, 56, 59) Wiedergabeberechtigungsbeantragungsinformation

zu der Wiedergabeberechtigungsanordnung (51, 53, 57, 60) liefern und eine Wiedergabebe-rechtigung für das reproduzierte verschlüsselte Infor-mationssignal von der Wiedergabeberechtigungszuordnungsanordnung

3. Anordnung (1) nach Anspruch 2, dadurch ge-kennzeichnet, dass die Überprüfungsmitte (19) Frei-gabeinformation, die sich in einem wiedergegebenen verschlüsselten Informationssignal befindet und eine Wiedergabeberechtigungsanordnung identifiziert, die eine Wiedergabeberechtigung für das reproduzierte verschlüsselte Informationssignal zuordnen darf, auslesen und diese liefern kann, und die Kommunikationsmittel (43) Wiedergabeberech-tigungsbeantragungsinformation zu der Wiedergabeberechtigungsanordnung (51, 53, 57, 60) liefern, die durch die Freigabeinfor-mation identifiziert worden ist ([Fig. 1](#)).

4. Anordnung (1) nach Anspruch 3, dadurch ge-kennzeichnet, dass Empfangsmittel (63) vorgesehen sind zum Empfangen eines verschlüsselten Informa-tionssignals, das von einer Sendestation (53, 57, 60, 65) geliefert wird, wobei das verschlüsselte Informa-tionssignal Freigabeinformation enthält, die eine Wiedergabeberechtigungsanordnung (51, 53, 57, 60) identifiziert, die eine Wiedergabebe-rechtigung für das verschlüsselte Informationssignal zuordnen darf, und Schnittstellenmittel (13) vorgese-hen sind zum Liefern eines verschlüsselten Informa-tionssignals mit der Freigabeinformation zu einer Aufzeichnungs- und Wiedergabevorrichtung (2) zum Zusammenarbeiten mit den Schnittstellenmitteln (13) zum Aufzeichnen des verschlüsselten Informations-signals. ([Fig. 1](#)).

5. Anordnung (1) nach Anspruch 3, dadurch ge-kennzeichnet, dass die Kommunikationsmittel (43) Speichermitte (45) aufweisen, in denen Verbin-dungsaufbauinformation von der Wiedergabebe-rechtigungsanordnung (51, 53, 57, 60), iden-tifiziert durch Freigabeinformation gespeichert wer-ten kann, und die Kommunikationsmittel (43) beim Fehlen einer Wiedergabeberechtigung für ein repro-duziertes verschlüsseltes Informationssignal mit der betreffenden Freigabeinformation mit Hilfe der Ver-binungsaufbauinformation in den Speichermitte (45) zum Liefern von Wiedergabeberechtigungsbe-antragungsinformation zu der Wiedergabeberech-tigungsanordnung (51, 53, 57, 60) identifi-ziert durch die betreffende Freigabeinformation, und zum Empfangen einer Wiedergabeberechtigung für das wiedergegebene verschlüsselte Informationssignal über die Datenverbindung (49, 52, 56, 59) eine Datenverbindung (49, 52, 56, 59) aufbauen ([Fig. 1](#)).

6. Anordnung (1) nach Anspruch 2, dadurch ge-kennzeichnet, dass die Kommunikationsmittel (43) einer Wiedergabeberechtigungsanordnungsanordnung

nung (51, 53, 57, 60) Wiedergabeberechtigungsbeantragungsinformation liefern, die das reproduzierte verschlüsselte Informationssignal identifiziert, und Schlüsselinformation (S1) von der Wiedergabeberechtigungszuordnungsanordnung (51, 53, 57, 60) empfangen, wobei diese Schlüsselinformation von der Wiedergabeberechtigungsbeantragungsinformation abhängig ist.

7. Anordnung (1) nach Anspruch 2, dadurch gekennzeichnet, dass Verarbeitungsmittel (35) vorgesehen sind zum Decodieren eines wiedergegebenen nicht verschlüsselten Informationssignals, wobei diese Mittel ebenfalls einen Teil der Abfragemittel (35, 43) bilden und die Verarbeitungsmittel (35) den Kommunikationsmitteln (43) Steuerinformation (SI) liefern, wobei diese Steuerinformation kennzeichnend für eine nicht einwandfreie Entschlüsselung eines reproduzierten verschlüsselten Informationssignals, und zwar durch das Fehlen einer Wiedergabeberechtigung ([Fig. 1](#)).

8. Anordnung (1) nach Anspruch 2, dadurch gekennzeichnet, dass die Überprüfungsmittel (19) eine Schlüsselstufe (22) aufweisen, die vorgesehen ist, erste Schlüsselinformation (S1) zu empfangen, empfangen in den Kommunikationsmitteln (43) von einer Wiedergabeberechtigungszuordnungsanordnung (51, 53, 57, 60) und zweite Schlüsselinformation (S2) in dem reproduzierten verschlüsselten Informationssignal zu empfangen, und die Schlüsselstufe (22), wenn eine Wiedergabeberechtigung verfügbar ist, dazu vorgesehen ist, die erste Schlüsselinformation (S1) und die zweite Schlüsselinformation (S2) gemeinsam zu verarbeiten und den Entschlüsselungsmitteln (32) eine zusammengesetzte Schlüsselinformation zu liefern, wobei diese zusammengesetzte Schlüsselinformation für die einwandfreie Entschlüsselung des reproduzierten verschlüsselten Informationssignals geeignet ist ([Fig. 1](#)).

9. Anordnung (1) nach Anspruch 1, dadurch gekennzeichnet, dass Steuermittel (62) vorgesehen sind, die beim Fehlen einer Wiedergabeberechtigung der Wiedergabebeanordnung (2, 3) über Schnittstellenmittel (13) Pauseinformation liefern um die Wiedergabe eines verschlüsselten Informationssignals zu unterbrechen, und die Steuermittel (62), wenn danach eine Wiedergabeberechtigung für das verschlüsselte Informationssignal verfügbar ist, der Wiedergabebeanordnung (2, 3) über die Schnittstellenmittel (13) Ende-der-Pause-Information liefern, damit die Wiedergabe des verschlüsselten Informationssignals fortgesetzt werden kann ([Fig. 1](#)).

Es folgt ein Blatt Zeichnungen

