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

(10) **DE 602 22 012 T2** 2008.05.15

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 449 370 B1**
(21) Deutsches Aktenzeichen: **602 22 012.2**
(86) PCT-Aktenzeichen: **PCT/IB02/03206**
(96) Europäisches Aktenzeichen: **02 755 460.9**
(87) PCT-Veröffentlichungs-Nr.: **WO 2003/017666**
(86) PCT-Anmeldetag: **31.07.2002**
(87) Veröffentlichungstag der PCT-Anmeldung: **27.02.2003**
(97) Erstveröffentlichung durch das EPA: **25.08.2004**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **22.08.2007**
(47) Veröffentlichungstag im Patentblatt: **15.05.2008**

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

(30) Unionspriorität:
932069 **17.08.2001** **US**

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

(73) Patentinhaber:
Koninklijke Philips Electronics N.V., Eindhoven, NL

(72) Erfinder:
FREEMAN, Martin, NL-5656 AA Eindhoven, NL;
LU, Jin, NL-5656 AA Eindhoven, NL

(74) Vertreter:
Volmer, G., Dipl.-Ing., Pat.-Anw., 52066 Aachen

(54) Bezeichnung: **SYSTEM UND VERFAHREN FÜR HYBRIDEN BEDINGTEN ZUGANG FÜR EMPFÄNGER VERSCHLÜSSELTER ÜBERTRAGUNGEN**

Beschreibung

[0001] Die vorliegende Erfindung betrifft die Entschlüsselung verschlüsselter Übertragungen und insbesondere ein System, eine Einrichtung und ein Verfahren zum Bereitstellen hybriden bedingten Zugangs für Empfänger verschlüsselter Übertragungen.

[0002] Anbieter von Kabelfernsehdienst (KFS-Dienst) übertragen ein Signal über ein Kabel an Abonnenten. Das Signal enthält mehrere Kanäle, die innerhalb des Frequenzbereichs des Signals verteilt werden. Typischerweise verschlüsseln die KFS-Dienstanbieter ihre Übertragungssignale, um Nicht-Abonnenten daran zu hindern, die Signale zu nutzen. Damit der Fernseher oder Videorecorder des Abonnenten das Signal nutzen kann, muss ein Mittel zum Empfangen des Signals, Entschlüsseln des Signals und Auswählen eines Kanals bereitgestellt sein. Das bereitgestellte Mittel ist typischerweise eine Einrichtung, die als Set-Top-Box bekannt ist. Zum Empfangen des Signals, das durch den KFS-Dienstanbieter übertragen wird, ist die Set-Top-Box mit einem Kabel verbunden. Ferner ist die Set-Top-Box zum Bereitstellen eines Signals, das anzeigefähig ist, mit dem Fernseher oder Videorecorder des Abonnenten verbunden. Die Set-Top-Box stellt typischerweise eine Navigationsfunktion und eine Sicherungsfunktion bereit. Die Navigationsfunktion dient zum Navigieren in und Auswählen von Kanälen innerhalb des empfangenen Signals. Die Sicherungsfunktion dient zum Entschlüsseln des empfangenen Signals. Die Sicherungsfunktion der Set-Top-Box ist Teil eines Systems für bedingten Zugang (BZ-Systems) zum Ermitteln der Berechtigungen der Set-Top-Box des Abonnenten zu den Diensten, die durch den KFS-Dienstanbieter bereitgestellt werden.

[0003] Gemäß durch die FCC erlassenen Vorschriften muss die Navigationsfunktion von der Sicherungsfunktion getrennt gehalten werden. Dies ist typischerweise durch Set-Top-Boxen erreicht worden, die entweder eine separate permanente Sicherungsfunktion, die in den Set-Top-Boxen eingebettet ist, oder eine separate entfernbare Sicherungsfunktion in Form einer Chipkarte erreicht worden, die an die Set-Top-Box ankoppelt.

[0004] Beim Versehen einer Set-Top-Box nur mit einer eingebetteten Sicherungsfunktion gibt es Nachteile. Die Sicherungsfunktion in der Set-Top-Box ist feststehend. Wenn kritische Merkmale innerhalb des Zugangskontrollsystems geändert werden, wird die Sicherungsfunktion in der Set-Top-Box funktionsunfähig. Beispielsweise mögen Kabel-Dienstanbieter periodisch das verwendete Verschlüsselungsverfahren ändern und mögen ihren Abonnenten unterschiedliche Berechtigungsebenen für gewisse Kanäle anbieten oder von diesen verlangen. Um einer Änderung bei Berechtigung oder Verschlüsselungsverfahren Rechnung zu tragen, ist eine neue Set-Top-Box mit einer unterschiedlichen Sicherungsfunktion erforderlich, um die ursprüngliche zu ersetzen. Außerdem muss jede Set-Top-Box spezialangefertigt werden, wie durch den KFS-Dienstanbieter vorgegeben, womit hohe Herstellungskosten einhergehen.

[0005] Das Versehen der Set-Top-Box mit einer entfernbaren Sicherungsfunktion stellt die Fähigkeit bereit, die Sicherungsfunktion der Set-Top-Box zu ändern, ohne sie ersetzen zu müssen. Außerdem könnte eine Standard-Set-Top-Box für verschiedene KFS-Dienstanbieter verwendet werden, womit die Herstellungskosten gesenkt werden. Jedoch gibt es Nachteile beim Versehen einer Set-Top-Box nur mit einem entfernbaren Modul, das die Sicherungsfunktion bereitstellt. Beim Fehlen oder Abkoppeln eines entfernbaren Moduls übersteuert die Set-Top-Box die Navigierfunktion und ist nicht in der Lage, irgendeine der empfangenen Übertragungen zu entschlüsseln. Ohne das entfernbare Modul ist die Set-Top-Box nur in der Lage, Inhalt zu zeigen, der kein verschlüsselter Inhalt sind, die nicht von hohem Wert sind.

[0006] EP-Anmeldung Nummer 0 585 833 A1 mit dem Titel „Video Signal Decoder System" beschreibt eine Set-Top-Box zum Decodieren von Videosignalen, wobei die Box zwei Sicherungsfunktionsmodule beinhaltet: ein eingebettetes Sicherungsfunktionsmodul und ein austauschbares Chipkarten-Sicherungsfunktionsmodul, das an die Box ankoppelt. Jedoch weist die beschriebene Box eine Reihe von Nachteilen auf. Beim Empfangen eines Signals wird die Entschlüsselung durch eines der Sicherungsfunktionsmodule vorgenommen. Das Sicherungsfunktionsmodul wird durch die Box über ein Versuchs-und-Irrtums-Verfahren ausgewählt. Das eingebettete Sicherungsfunktionsmodul wird als Erstes für die Auswahl geprüft, und die Chipkarte wird als Zweites geprüft. Das Sicherungsfunktionsmodul entweder der eingebetteten Sicherungsfunktion oder der Chipkarten-Sicherungsfunktion, das ausgewählt worden ist, hängt davon ab, welches einen Entschlüsselungsalgorithmus aufweist, der dem Verschlüsselungsalgorithmus des empfangenen Signals entspricht. Somit erfolgt die Auswahl eines Sicherungsfunktionsmoduls zum Vornehmen der Entschlüsselung gemäß dem Signal, das durch die Box empfangen wird, wobei das andere Sicherungsfunktionsmodul deaktiviert ist. Somit stellt die Box kein Standard-Sicherungsfunktionsmodul bereit. Die Box erlaubt keine unterschiedlichen Zugangsebenen auf die empfangene Übertragung.

[0007] US-Patentschrift Nr. 5.742.680 beschreibt eine Set-Top-Box zum Bereitstellen von Entschlüsselung eines empfangenen Signals, wobei das Signal durch einen ausgewählten Sender von mehreren Sendern gesendet wird und die Entschlüsselung

durch eine entsprechende Chipkarte von mehreren Chipkarten-Sicherungsfunktionsmodulen vorgenommen wird. Die Box beinhaltet kein eingebettetes Sicherungsfunktionsmodul. Ohne eine entsprechende Chipkarte für das ausgewählte Signal kann die Set-Top-Box keine Entschlüsselung vornehmen.

[0008] In den oben erwähnten Referenzen kann jedweder Inhaber einer Chipkarte die Chipkarte mit jedweder kompatiblen Set-Top-Box verwenden. Jedoch halten es Anbieter übertragener Signale oft für einen Vorteil für sich, Entschlüsselung ihrer Signale auf die Set-Top-Box zu beschränken, die zum Abonnenten gehört. Außerdem sehen die oben erwähnten Referenzen kein Prüfen der Berechtigung zum Entschlüsseln der übertragenen Signale vor. Auch deaktivieren sie keine Sicherungsfunktionsmodule, die nicht mehr berechtigt sind. Um unberechtigte Entschlüsselung zu verhindern, müssen Anbieter von Signalübertragungen den Verschlüsselungsalgorithmus der übertragenen Signale ändern. Dies würde die Verteilung neuer Chipkarten an alle berechtigten Kunden erfordern.

[0009] EP-Anmeldung 0 570 785 A1 beschreibt ein Verfahren zum Erlauben von Entschlüsselung übertragener Signale an definierten geografischen Ort unter Verwendung von Chipkarten. Jedoch erfordert das obige Verfahren, um dies zu erreichen, die Übertragung von mindestens zwei Datenkanälen, die durch mindestens zwei separate Prozessoren zu empfangen sind.

[0010] Es ist eine Aufgabe der vorliegenden Erfindung, einen Empfänger zum Empfangen und Entschlüsseln verschlüsselter Übertragungen von einer Übertragungsstation bereitzustellen, wobei der Empfänger eine eingebettetes Standard-Sicherungsfunktionsmodul und ein entfernbares Sicherungsfunktionsmodul zum Bereitstellen einer zusätzlichen Zugangsebene auf die Übertragungen aufweist und wobei die Standardbetriebsart ungeachtet der Verfügbarkeit des entfernbaren Sicherungsfunktionsmoduls in Betrieb ist.

[0011] Eine andere Aufgabe der vorliegenden Erfindung ist es, ein System und ein Verfahren zum Bereitstellen von Zugang zu verschlüsselten Übertragungen von einem Übertragungssystem durch einen Empfänger bereitzustellen, wobei dem Empfänger verschiedene Zugriffsebenen auf die Übertragung einschließlich einer Standardebene erlaubt sind.

[0012] Eine weitere Aufgabe der vorliegenden Erfindung ist es, ein System und ein Verfahren zum Bereitstellen von Zugang zu verschlüsselten Übertragungen von einem Übertragungssystem durch einen Empfänger gemäß Berechtigungen eines von dem Benutzer und dem Empfänger zu den Übertragungen bereitzustellen.

[0013] Eine weitere Aufgabe der vorliegenden Erfindung ist es, ein System und Verfahren zum Bereitstellen eines Empfängers und Sicherungsfunktionsmoduls bereitzustellen, die effizient herzustellen und zu verteilen sind, während sie maximalen Service bereitstellen.

[0014] Um die obigen Aufgaben zu lösen, ist ein System und Verfahren, wie in den angehängten Ansprüchen dargelegt, beansprucht worden.

[0015] Die vorliegende Erfindung bezieht eine Übertragungsstation zum Übertragen verschlüsselter Übertragungen an einen Empfänger ein. Die Übertragungsstation umfasst mindestens eine Kopfstelle, die ein erstes Modul für bedingten Zugang zum Verschlüsseln eines ersten Signals und ein zweites Modul für bedingten Zugang zum Verschlüsseln eines zweiten Signals aufweist. Die Kopfstelle umfasst ferner ein Berechtigungsmodul zum Ermitteln, ob ein Empfänger das Recht zum Entschlüsseln des zweiten Signals aufweist. Bei einer positiven Ermittlung durch das Berechtigungsmodul überträgt die Übertragungsstation an den Empfänger einen Berechtigungscode, der es dem Empfänger erlaubt, das zweite Signal zu entschlüsseln.

[0016] Daher besteht Bedarf an einem System, in dem ein Empfänger eine Übertragung, die durch eine Übertragungsstation übertragen wird, empfängt und entschlüsselt, wobei der Empfänger sowohl ein eingebettetes Sicherungsfunktionsmodul als auch ein entfernbares Sicherungsfunktionsmodul aufweist. Es besteht Bedarf daran, dass das eingebettete Sicherungsfunktionsmodul eine Standardbetriebsart bereitstellt, sodass Übertragungen von der Übertragungsstation ungeachtet der Verfügbarkeit des entfernbaren Sicherungsfunktionsmoduls auf einer Standardebene entschlüsselt werden können. Es besteht der Bedarf am Bereitstellen variierender Zugangsebenen zu Übertragungen. Es besteht Bedarf daran, Benutzer, die keine Berechtigungen haben, am Betrachten beschränkter Übertragungen zu hindern, ohne die permanente Deaktivierung vorhandener Sicherungsfunktionsmodule zu erfordern.

[0017] Der Vollständigkeit halber wird auf EP-Anmeldung 0 506 435 und auf EP-Anmeldung 0 752 635 verwiesen.

[0018] EP-Anmeldung 0 506 435 betrifft einen Decodierer zum Descramblen codierter Satellitenübertragungen. Der Decodierer umfasst ein internes Sicherungsmodul und ein austauschbares Sicherungsmodul. Das Programmsignal wird mit einem Schlüssel gescramblet, und dann wird der Schlüssel selbst doppelt verschlüsselt und mit dem gescrambleten Programmsignal gemultiplext. Der Decodierer nimmt eine erste Schlüssel-Entschlüsselung unter Verwendung der zweiten geheimen Seriennummer vor, die

im Decodierer gespeichert ist. Der teilweise entschlüsselte Schlüssel wird dann unter Verwendung der ersten geheimen Seriennummer, die im austauschbaren Sicherungsmodul gespeichert ist, durch das austauschbare Sicherungsmodul weiter entschlüsselt. Dann descramblet der Decodierer das Programm mithilfe des doppelt entschlüsselten Schlüssels. Das austauschbare Sicherungsmodul kann ausgetauscht werden, womit ermöglicht wird, dass das Sicherungssystem auf eine Systemlücke folgend aktualisiert oder geändert wird. Auswählbar durch ein Signal, das vom Codierer übertragen wird, kann jedes der Sicherungsmodule zum aktiven Sicherungsmodul werden, um den Gehalt abschließend zu entschlüsseln. Dementsprechend betrifft dieser Verweis Doppelschicht-Verschlüsselung. Sowohl interne als auch entfernbare Entschlüsselungsmodule (Decodierer und Sicherungsmodul) können separat/individuell oder gemeinsam unter Kontrolle spezieller Adressbits arbeiten, die durch einen Lenkungsmanager bedient werden. Weder lehrt dieser Verweis die Erfindungsmerkmale eines Senders zum Übertragen einer Meldung darüber, dass das entfernbare Modul aktiviert ist, an eine Station außerhalb des Systems und des Empfangens einer Berechtigung, die das Entschlüsseln des zweiten Signals aktiviert, von der Station daraufhin, falls das entfernbare Modul zugelassen ist, noch legt er sie nahe. Das Aktivieren erfolgt im bekannten System durch Benutzereingriff (Anschließen oder Einsetzen des Moduls oder Ändern der Einstellung des Empfängers durch Umlegen eines Schalters.).

[0019] EP-Anmeldung 0 752 635 betrifft ein System und Verfahren, die transparente Integration von Chipkarten-Privatschlüsselbenutzung mit einem vorhandenen Satz von Verschlüsselungsdiensten und Systemanwendungen bereitstellen. Ein Schlüsselspeichermanager verwaltet Benutzerschlüsseldaten und behandelt Anforderungen um Schlüsselbenutzung von den Systemanwendungen. Eine Benutzerinformationsdatei speichert Benutzerdaten einschließlich privater Benutzerschlüssel für Benutzer, die keine Chipkarten besitzen, und einer Angabe jener Benutzer, die Chipkarten besitzen. Ein Satz von Systemanwendungen koppelt über Verschlüsselungsprotokoll-spezifische Anwendungsprogrammierungs-Schnittstellen an den Schlüsselspeichermanager an. Benutzer verbinden sich mit dem System über Endgeräte oder entfernte Computer, die mit Chipkartenlesern ausgerüstet sein können. Bei Benutzern, die Chipkarten besitzen, leitet der Schlüsselspeichermanager Anforderungen um Privatschlüsselbenutzung, wie z.B. Verschlüsselung oder Entschlüsselung mit dem privaten Schlüssel des Benutzers, von den Systemanwendungen an die Chipkarten weiter. Auf diese Art und Weise kann der private Schlüssel des Benutzers nicht durch Darstellung gegenüber dem Computersystem kompromittiert werden. Bei Benutzern ohne Chipkarten leitet der Schlüsselspeichermanager die Anforderung um Privatschlüsselbenutzung zur Behandlung an einen Verschlüsselungsdienst weiter. Der Schlüsselspeichermanager kann nur Anforderungen um Privatschlüsselbenutzung behandeln, wobei die Systemanwendungen die Benutzung öffentlicher Schlüssel direkt identifizieren und behandeln, oder der Schlüsselspeichermanager kann sowohl die Privatschlüsselbenutzung als auch die Benutzung öffentlicher Schlüssel behandeln.

[0020] EP-Anmeldung 0752 635 betrifft das technische Gebiet vernetzter Computer und nicht die Umgebung der Unterhaltungs- und Haushaltselektronik, die in der aktuellen Erfindung angesprochen wird. EP-Anmeldung 0752 635 betrifft das Verfügbarmachen eines privaten Schlüssels für das System auf verschiedene Art und Weise einschließlich Chipkarten und einer Schlüsselspeichermanager-Software-Anwendung. Weder lehrt EP-Anmeldung 0752 635 die Verarbeitung von Videoinhalt noch, dass eine Chipkarte ein eingebettetes Modul übersteuert, noch die Übertragung von Meldungen, um eine Station darüber zu benachrichtigen, dass eine Chipkarte aktiviert ist, noch das Empfangen von Berechtigungscodes daraufhin, noch legt sie diese nahe.

[0021] Die obigen und andere Aufgaben, Merkmale und Vorteile der vorliegenden Erfindung werden im Lichte der folgenden ausführlichen Beschreibung eines Ausführungsbeispiels derselben in Verbindung mit den angehängten Zeichnungen offensichtlicher, wobei:

[0022] Fig. 1 ein Blockschaltbild eines Systems nach Stand der Technik zur Entschlüsselung durch einen Empfänger eines verschlüsselten Signals ist, das durch eine Übertragungsstation eines KFS-Dienstanbieters übertragen wird;

[0023] Fig. 2 ein Blockschaltbild eines zweiten Systems nach Stand der Technik zur Entschlüsselung durch einen Empfänger eines verschlüsselten Signals ist, das durch eine Übertragungsstation eines KFS-Dienstanbieters übertragen wird;

[0024] Fig. 3 ein Blockschaltbild eines Systems zur Entschlüsselung durch einen Empfänger eines verschlüsselten Signals ist, das durch eine Übertragungsstation übertragen wird, gemäß der vorliegenden Erfindung;

[0025] Fig. 4 ein beispielhaftes Flussdiagramm ist, das die Schritte darstellt, die durch einen Empfänger entschlüsselter Übertragungen durchgeführt werden, gemäß der vorliegenden Erfindung; und

[0026] Fig. 5 ein beispielhaftes Flussdiagramm ist, das die Schritte darstellt, die durch einen Sender verschlüsselter Übertragungen durchgeführt werden,

gemäß der vorliegenden Erfindung.

[0027] Übergehend zu den Zeichnungen, in denen über die mehreren Ansichten hinweg ähnliche Bezugszeichen ähnliche oder identische Elemente identifizieren, ist ein System nach Stand der Technik zur Entschlüsselung verschlüsselter Übertragungen, die durch eine Übertragungsstation übertragen werden, in Fig. 1 abgebildet.

[0028] Bezug nehmend auf Fig. 1 beinhaltet das System nach Stand der Technik, gezeigt unter **10**, eine Übertragungsstation, die eine Kopfstelle **12** aufweist, die ein Signal zu einem Empfänger **14** überträgt. Die Übertragungsstation ist typischerweise ein Kabelfernseh-(KFS-)-Dienstanbieter. Der Empfänger **14** ist typischerweise ein Set-Top-Box. Ein Kabel, durch das die Übertragung übertragen wird, verläuft zwischen der Set-Top-Box und dem Übertragungssystem. Die Set-Top-Box steht ferner in Kommunikation mit einem Fernseher oder Videorecorder zum Betrachten der Übertragungen, sobald sie empfangen und entschlüsselt sind. Ein Sicherungssystem, das als System für bedingten Zugang (BZ-System) bekannt ist, ist zum Sichern der Übertragung dagegen bereitgestellt, dass auf sie durch einen Empfänger zugegriffen wird, der keine Berechtigungen aufweist. Das BZ-System des in Fig. 1 gezeigten Systems umfasst BZ-Modul **16** und BZ-Modul **18**. BZ-Modul **16** befindet sich in der Kopfstelle der Übertragungsstation. BZ **16** verschlüsselt Inhalte des Signals zur Übertragung, während BZ **18** das empfangene Signal zum Betrachten entschlüsselt. BZ **18** ist als permanente Komponente innerhalb der Set-Top-Box eingebettet.

[0029] Ein anderes System nach Stand der Technik ist in Fig. 2 abgebildet. Das gezeigte System nach Stand der Technik **20** beinhaltet Kopfstelle **22** und Set-Top-Box **24**. Das BZ-Modul **26** befindet sich in Kopfstelle **22**, und das BZ-Modul **28** befindet sich in Set-Top-Box **24**. BZ-Modul **28** ist eine entfernbare Chipkarte. Das BZ-Modul **28** kann gegen eine unterschiedliche Chipkarte ausgetauscht werden.

[0030] Jetzt Bezug nehmend auf Fig. 3 ist eine Ausführungsform des Systems der vorliegenden Erfindung gezeigt. Das System **50** der vorliegenden Erfindung stellt eine Übertragungsstation bereit, die Kopfstelle **52** und eine Set-Top-Box **54** aufweist. Die Set-Top-Box **54** empfängt über Kabel oder über drahtlose Mittel wie z.B. Funkwellen, die durch eine Satellitenschüsselantenne empfangen werden, eine Übertragung von einer Übertragungsstation **52**. Die Übertragungsstation **52** überträgt zwei Signale. Ein erstes BZ-Modul **56** verschlüsselt das erste Signal. Ein zweites BZ-Modul **58** verschlüsselt das zweite Signal.

[0031] Die Set-Top-Box stellt eine Architektur für hybriden bedingten Zugang bereit, die ein eingebettetes BZ-Modul **60** und ein entfernbares BZ-Modul **62** zum Entschlüsseln der Signale umfasst, die durch die Übertragungsstation übertragen werden. Die Set-Top-Box ist mit einer Standardschnittstelle zum Eingreifen von BZ-Modul **62** darin und Ankoppeln derselben an die Set-Top-Box versehen.

[0032] Während des Betriebs empfängt die Set-Top-Box anfangs die Signale von der Übertragungsstation, die durch BZ-Modul **56** verschlüsselt sind, und entschlüsselt das erste verschlüsselte Signal über das eingebettete BZ-Modul **60**. Zum Entschlüsseln der Übertragung von der Übertragungsstation auch dann, wenn ein entfernbares Modul nicht aktiviert oder nicht verfügbar ist, stellt BZ-Modul **60** eine standardmäßige bedingte Zugangsfähigkeit bereit.

[0033] Beim Aktivieren von BZ-Modul **62** setzt eine Neuinitialisierungseinheit **64** die Set-Top-Box durch Neuinitialisieren der Set-Top-Box zurück, um es BZ-Modul **62** zu erlauben, die empfangene Übertragung zu entschlüsseln, weist die Set-Top-Box **54** an, eine Signaländerungsmeldung zur Übertragungsstation **52** zu übertragen, und stellt die Entschlüsselung des ersten Signals durch BZ-Modul **60** ein. Die Signaländerungsmeldung informiert die Übertragungsstation darüber, dass die Set-Top-Box **54** bereit ist, das zweite Signal zu entschlüsseln.

[0034] Die Kopfstelle von Übertragungsstation **52** ermittelt beim Empfangen der Signaländerungsmeldung, ob die Set-Top-Box berechtigt ist, das zweite Signal zu empfangen, oder nicht. Die Ermittlung erfolgt nach Kriterien, die durch die Manager der Übertragungsstation festgelegt sind, wie z.B., ob die Eigentümer der Set-Top-Box die Abonnementgebühren für den Dienst, der durch die Übertragungsstation bereitgestellt wird, bezahlt haben oder nicht, wie in einer Datenbank aufgezeichnet.

[0035] Bei einer positiven Ermittlung überträgt die Kopfstelle einen Berechtigungscode, der die Set-Top-Box in die Lage versetzt, das zweite Signal zu entschlüsseln. Daraufhin, dass die Set-Top-Box **54** das zweite Signal mit dem Berechtigungscode empfangt, fährt das BZ-Modul **62** fort, das zweite Signal zu entschlüsseln.

[0036] In der Set-Top-Box der bevorzugten Ausführungsform ist das entfernbare BZ-Modul **62** ein Standardmodul, das effiziente Herstellung und Verteilung bereitstellt. Dies ist vorteilhaft zur Behandlung von Aktualisierungen, Sicherheitsänderungen und neuen Produkten.

[0037] Fig. 4 und Fig. 5 sind beispielhafte Flussdiagramme, die die Schritte darstellen, die durch die Set-Top-Box bzw. die Übertragungsstation einer Aus-

führungsform der Erfindung durchgeführt werden. Es versteht sich, dass nach Vorlieben, Konstruktionsentscheidungen usw. Modifikationen implementiert werden könnten.

[0038] Bezug nehmend auf Fig. 4 werden nun die Schritte beschrieben, die durch die Set-Top-Box durchgeführt werden. In Schritt **98** sendet beim Aktivieren der Set-Top-Box **54**, um Übertragungen zu empfangen, die Set-Top-Box **54** eine Meldung zur Übertragungsstation, um die Übertragungsstation darüber zu informieren, dass das BZ-Modul **60** der Set-Top-Box **54** bereit ist, das erste Signal zu entschlüsseln.

[0039] In Schritt **100** empfangt die Set-Top-Box die Übertragungen. In der bevorzugten Ausführungsform wird das erste Signal zusammen mit einem Berechtigungscode für das erste Signal empfangen. Der erste Signalberechtigungscode erlaubt es der Set-Top-Box, das erste Signal zu empfangen. In einer anderen Ausführungsform stellt der Berechtigungscode Schlüsseldaten bereit, um es der Set-Top-Box zu erlauben, das Signal zu entschlüsseln. In noch einer anderen Ausführungsform erlaubt der Berechtigungscode beide obigen Funktionen.

[0040] In Entscheidungsschritt **102** wird ermittelt, ob der erste Signalberechtigungscode empfangen wurde oder nicht. Falls nicht, kann das erste Signal nicht entschlüsselt werden, und die Steuerung geht zu Schritt **103**, um den Benutzer der Set-Top-Box darüber zu informieren, dass er nicht berechtigt ist, jedwede Signale zu betrachten, und dass der Zugang verwehrt wird. Dann kehrt der Prozess zu Schritt **98** zurück.

[0041] Bei Ermittlung, dass der erste Signalberechtigungscode empfangen wurde, geht der Prozess zu Schritt **105** über. In Schritt **105** wird das erste Signal durch BZ-Modul **60** entschlüsselt. In Entscheidungsschritt **110** ermittelt die Set-Top-Box, ob BZ-Modul **62** aktiviert worden ist oder nicht. Während des Betriebs kann das BZ-Modul **62** auf verschiedene Weise aktiviert werden, wie z.B. durch Einsetzen des entfernbaren Moduls oder durch Aktivieren eines Schalters, sobald es eingesetzt ist. Ist BZ-Modul **62** nicht aktiviert, fährt die Set-Top-Box fort, das erste Signal zu empfangen und entschlüsseln, und der Prozess kehrt zu Schritt **110** zu rück. Ist BZ-Modul **62** aktiviert worden, geht der Prozess zu Schritt **115** über.

[0042] In Schritt **115** wird die Set-Top-Box zurückgesetzt. Eine Initialisierungsroutine wird durchgeführt, um es dem BZ-Modul **62** zu erlauben, das empfangene Signal zu entschlüsseln. In Schritt **120** wird die Entschlüsselung des ersten Signals durch BZ-Modul **60** eingestellt. In Schritt **125** überträgt die Set-Top-Box eine Signaländerungsmeldung zur Übertragungsstation, um die Übertragungsstation darüber zu informieren, dass das BZ-Modul **62** ausgewählt worden ist und bereit ist, das zweite Signal zu entschlüsseln. Die Reihenfolge der Durchführung der Schritte **115**–**125** kann gemäß Konstruktionsentscheidung umgeordnet werden.

[0043] In Schritt **130** empfängt die Set-Top-Box, falls zugelassen, von der Übertragungsstation den Berechtigungscode für das zweite Signal. In Entscheidungsschritt **132** wird ermittelt, ob der zweite Signalberechtigungscode für das zweite Signal empfangen wurde oder nicht. Falls nicht, kann das zweite Signal nicht entschlüsselt werden, und der Prozess geht zum Neuinitialisieren der Set-Top-Box, um das erste Signal zu entschlüsseln, und Informieren der Übertragungsstation darüber, dass die Set-Top-Box bereit ist, das erste Signal zu entschlüsseln, zu Schritt **133** über.

[0044] Bei Ermittlung in Schritt **132**, dass der zweite Signalberechtigungscode empfangen wurde, geht der Prozess zu Schritt **135** über. In Schritt **135** entschlüsselt BZ-Modul **62** das zweite Signal. In Schritt **140** erfolgt eine Ermittlung dahin gehend, ob BZ-Modul **62** noch aktiviert ist oder nicht. Die Entschlüsselung des zweiten Signals wird fortgesetzt, bis das BZ-Modul **62** deaktiviert wird. Bei Deaktivierung von BZ-Modul **62** stellt die Set-Top-Box das Entschlüsseln des zweiten Signals ein, und der Prozess geht zur Neuinitialisierung, um das erste Signal zu empfangen und entschlüsseln, zu Schritt **133** über.

[0045] Als Nächstes werden unter Bezug auf Fig. 5 nun die Schritte beschrieben, die durch die Übertragungsstation durchgeführt werden. Während sie fortwährend verschlüsselte erste und zweite Signale überträgt, wartet die Übertragungsstation in Schritt **210** auf den Eingang einer Meldung, dass das BZ-Modul **60** bereit ist, die erste Meldung zu entschlüsseln.

[0046] Bei Eingang der Meldung in Schritt **210** geht der Prozess zu Entscheidungsschritt **215** über. In Schritt **215** ermittelt die Übertragungsstation, ob die Set-Top-Box berechtigt ist, das erste Signal zu entschlüsseln, oder nicht. Falls nicht, kehrt der Prozess zu Schritt **210** zurück. Gemäß Konstruktionsentscheidung kann alternativ eine Routine unter Verwendung verschiedener Schritte durchgeführt werden. Beispielsweise kann die Routine eine Meldung zur Set-Top-Box senden, um den Benutzer darüber zu informieren, dass er nicht berechtigt ist, die Inhalte der Übertragungen zu betrachten, wonach der Prozess zu Schritt **210** zurückkehrt. Auch können die Schritte **210** und **215** zu einem Schritt kombiniert werden, in dem nur Meldungen erkannt werden, die von Set-Top-Boxen empfangen werden, die aktuelle Berechtigungen aufweisen. Falls in Schritt **215** bestätigt wird, dass die Set-Top-Box berechtigt ist, das erste Signal zu entschlüsseln, geht der Prozess mit Schritt

225 weiter.

[0047] In Schritt **225** wird ein erster Signalberechtigungscode zur Set-Top-Box übertragen. Der erste Signalberechtigungscode erlaubt es der Set-Top-Box, das erste Signal zu entschlüsseln. Der erste Signalberechtigungscode ist in einer Ausführungsform eine der Set-Top-Box entsprechende Adresse, die als Präfix der Übertragung des ersten Signals beigefügt ist, um es der Set-Top-Box zu erlauben, das erste Signal zu empfangen. In einer anderen Ausführungsform enthält der erste Signalberechtigungscode einen Schlüssel, der es BZ-Modul **60** erlaubt, einen Entschlüsselungsalgorithmus zu verwenden, der dem Verschlüsselungsalgorithmus entspricht, der durch BZ-Modul **56** verwendet wird. In noch einer anderen Ausführungsform kann das erste Signal durch jedwede Set-Top-Box in Kommunikation mit der Übertragungsstation empfangen und entschlüsselt werden, ohne die Überprüfung der Berechtigung zu erfordern. Bei Abschluss von Schritt **225** geht der Prozess mit Schritt **230** weiter.

[0048] Schritt **230** ist ein Warteschritt, in dem die Übertragungsstation auf Eingang einer Signaländerungsmeldung von der Set-Top-Box wartet, die erklärt, dass das BZ-Modul **60** das erste Signal nicht länger entschlüsseln wird und dass das BZ-Modul **62** bereit ist, das zweite Signal zu entschlüsseln. Bei Eingang einer Signaländerungsmeldung geht der Prozess mit Schritt **235** weiter. In Entscheidungsschritt **235** überprüft die Übertragungsstation, ob die Set-Top-Box berechtigt ist, das zweite Signal zu entschlüsseln. Auf die Überprüfung hin geht der Prozess mit Schritt **240** weiter.

[0049] In Schritt **240** überträgt die Übertragungsstation einen zweiten Signalberechtigungscode zur Set-Top-Box. Der zweite Signalberechtigungscode erlaubt es der Set-Top-Box, das zweite Signal zu entschlüsseln. Der zweite Signalberechtigungscode funktioniert in dem ersten Signalberechtigungscode ähnlicher Art und Weise.

[0050] Falls ermittelt wurde, dass die Set-Top-Box nicht zur Entschlüsselung des zweiten Signals berechtigt ist, kehrt der Prozess zu Schritt **225** zurück. Alternativ kann gemäß Konstruktionsentscheidung eine Routine durchgeführt werden. Beispielsweise kann die Routine einen Schritt zum Senden einer Meldung zur Set-Top-Box aufweisen, um den Benutzer darüber zu informieren, dass er nicht berechtigt ist, die Inhalte des zweiten Signals zu betrachten, und dann kann der Prozess zu Schritt **225** zurückgelenkt werden, um es der Set-Top-Box zu erlauben, das erste Signal zum Betrachten zu entschlüsseln.

[0051] In der in Fig. 4 und Fig. 5 abgebildeten Ausführungsform wird bevorzugt, dass die Set-Top-Box das erste Signal empfängt und entschlüsselt, bevor ihr erlaubt wird, das zweite Signal zu empfangen und zu entschlüsseln. In einer anderen Ausführungsform kann das System und Verfahren modifiziert sein, um es dem Benutzer der Set-Top-Box zu erlauben, anfangs entweder BZ-Modul **60** zur Entschlüsselung des zweiten oder BZ-Modul **62** zur Entschlüsselung des zweiten Signals auszuwählen. In einer möglichen Modifikation überprüft die Übertragungsstation die Berechtigung der Set-Top-Box, Übertragungen von der Übertragungsstation zu entschlüsseln, bevor dem BZ-Modul **62** erlaubt wird, das zweite Signal zu entschlüsseln. Dies begrenzt die Verwendung des entfernbaren BZ-Moduls **62** auf die Verwendung mit Set-Top-Boxen, die Abonnenten mit vollständig geleisteten Zahlungen gehören. In einer anderen Modifikation werden die Berechtigungen individuell für jedes der BZ-Module **60**, **62** überprüft, sodass das entfernbare BZ-Modul **62** ungeachtet der Berechtigungen, die der Set-Top-Box zugeordnet sind, in jedweder kompatiblen Set-Top-Box verwendet werden kann.

[0052] In einer anderen Ausführungsform stellt das BZ-Modul **60** eine Basiszugangsebene bereit, und das BZ-Modul **62** stellt Zusatzzugangsebenen bereit, stellt aber nicht die Basiszugangsebene bereit. Wenn das BZ-Modul **62** aktiviert ist, stellen die BZ-Module **60**, **62** zusammen den vollständigen Bereich an Zugangsebenen bereit. Beispielsweise wird eine Übertragung bereitgestellt, in der ein Transportstrom einen Videostrom und zwei Audioströme beinhaltet. Ein Audiostrom ist in Englisch und der andere Audiostrom ist in Spanisch. BZ-Modul **60** kann nur den englischen Audiostrom entschlüsseln, während BZ-Modul **62** nur den spanischen Audiostrom entschlüsseln kann. Vor dem Einsetzen von BZ-Modul **62** in den Empfänger können Betrachter nur die englische Sprache hören, wobei den Betrachtern ein Standardzugang bereitgestellt wird. Auf das Einsetzen des BZ-Modul **62** in den Empfänger hin können die Betrachter unter beiden Sprachen wählen, wobei den Betrachtern ein Premiumzugang bereitgestellt wird.

[0053] Wie oben nahe gelegt, können, während die Ausführungsformen ein „erstes Signal" und ein „zweites Signal" verwendet haben, diese erste und zweite Pakete repräsentieren, die jedes mehrere Signale umfassen. Beispielsweise kann ein erstes Paket von Signalen Basiskabelkanälen entsprechen, und ein zweites Paket von Signalen kann einem Paket von Premiumkabelkanälen entsprechen. Der Kabelanbieter kann eine Anzahl unterschiedlicher Zweit- oder Premiumpakete verfügbar machen. Jedes derartige Paket würde ein bestimmtes entfernbaren BZ-Modul aufweisen, das die Signale für jenes Paket entschlüsselt.

[0054] Darüber hinaus kann der Empfänger mehr als einen Port zum Aufnehmen einer Anzahl entfern-

barer BZ-Module aufweisen. Jedes derartige entfernbare Modul kann, wie oben beschrieben, ein separates „zweites Signal" empfangen, anders ausgedrückt, ein drittes, viertes usw. Signal. Jedes derartige entfernbare Modul kann einen verschiedenen Entschlüsselungsalgorithmus aufweisen, und das Zulassen der Entschlüsselung kann analog dem oben beschriebenen Verarbeiten und Signalaustausch mit der Übertragungsstation erfolgen. Darüber hinaus kann ein Prioritätsschema zum Aktivieren eines der eingebetteten BZ-Module und der mehreren entfernbaren BZ-Module bei Deaktivieren der anderen festgelegt werden. Beispielsweise können die Ports im Empfänger für die entfernbaren BZ-Module derart konfiguriert sein, dass nur das entfernbare Modul für ein gewisses Kabelpaket darin angeschlossen werden kann. Sind mehrere Module angeschlossen, kann der Premiumkanal oberster Ebene, der durch die Übertragungsstation zugelassen ist, aktiviert sein, während alle anderen deaktiviert sind.

[0055] Es ist vorgesehen, dass, wie durch die Leitung der Übertragungsstation gewünscht, die Ermittlung von Berechtigungsrechten bei Rechten zum Entschlüsseln eines der Signale unterbleibt.

[0056] Die in Fig. 4 und Fig. 5 abgebildete Ermittlung von Berechtigungsrechten ist lediglich beispielhaft, und es könnte ein unterschiedliches Verfahren gemäß den Zielen der Leitung der Übertragungsstation implementiert werden.

[0057] Es ist vorgesehen, dass das BZ-Modul **62** mehrere entfernbare Module umfassen kann, wobei jedes entfernbare Modul eine unterschiedliche Zugangsebene zur Übertragungsstation bereitstellt, und dass das BZ-Modul **60** entfernbar und auswechselbar ist, während trotzdem eine Standardbetriebsart bereitgestellt wird.

[0058] Es ist ferner vorgesehen, dass die Übertragungsstation ein Signal überträgt, wobei die eingebetteten und entfernbaren BZ-Module unterschiedliche Zugangsebenen auf dasselbe Signal bereitstellen. Somit kann beispielsweise das System zum Entschlüsseln verschlüsselter Übertragungen mindestens eines Signals sein. Das System kann einen Empfänger zum Empfangen von Übertragungen des mindestens einen Signals umfassen. Der Empfänger weist ein erstes eingebettetes Modul für bedingten Zugang und ein zweites entfernbares Modul für bedingten Zugang zum Entschlüsseln empfangener Übertragungen auf. Das Aktivieren des zweiten Moduls für bedingten Zugang veranlasst, dass das zweite Modul für bedingten Zugang das erste Modul für bedingten Zugang übersteuert. Das erste eingebettete Modul für bedingten Zugang und das zweite entfernbare Modul für bedingten Zugang können unterschiedliche Entschlüsselungsalgorithmen aufweisen. Dort, wo ein einzelnes Signal empfangen wird, kann das erste Modul für bedingten Zugang des Entschlüsselns nur gewisser Aspekte des Signals fähig sein (wie z.B. einer „Vorschau" einer Premiumsendung), wohingegen der Entschlüsselungsalgorithmus des zweiten entfernbaren Moduls für bedingten Zugang des Entschlüsselns des gesamten Signals fähig sein kann, womit das Betrachten der eigentlichen Premiumsendung erlaubt wird. Wenn das zweite entfernbare Modul für bedingten Zugang aktiviert ist, sieht der Betrachter somit die Premiumsendung.

[0059] Es ist ferner vorgesehen, dass die Übertragungsstation mehr als zwei Signale überträgt, während die Set-Top-Box Übertragungen von mehr als einer Übertragungsstation empfängt.

[0060] Es ist ferner vorgesehen, dass die Übertragungsstation Signale über jedwedes verfügbare Medium überträgt und dass das Signal jedweder Typ von Signal sein kann, für das Verschlüsselung gewünscht wird.

Bezugszeichenliste

Fig. 4

98:	MELDUNG AN ÜBERTRAGUNGSSTATION BZ-MOD. **60** FÜR 1. SIGNAL BEREIT
100:	1.SIGNAL UND 1. SIGNALBERECHTIGUNGS-CODE EMPFANGEN
102:	BERECHTIGUNGS-CODE EMPFANGEN?
103:	BENUTZER INFORMIEREN, DASS ZUGANG VERWEHRT WIRD
105:	1. SIGNAL DURCH BZ-MODUL **60** ENTSCHLÜSSELN
110:	IST BZ-MODUL **62** AKTIVIERT?
115:	EMPFÄNGER ZURÜCKSETZEN, UM BZ-MOD. **62** ENTSCHLÜSSELN DES SIGNALS ZU ERLAUBEN
120:	ENTSCHLÜSSELUNG DES 1. SIGNALS DURCH BZ-MOD. **60** EINSTELLEN
125:	SIGNALÄNDERUNGS-MELDUNG SENDEN
130:	2. SIGNAL UND BERECHTIGUNGSCODE EMPFANGEN

132:	BERECHTIGUNG EMPFANGEN?
133:	NEUINITIALISIEREN ZUR ENTSCHLÜSSELUNG DES 1. SIGNALS
135:	ZWEITES SIGNAL DURCH BZ-MOD. **62** ENTSCHLÜSSELN
140:	BZ-MOD **62** DEAKTIVIERT?
ACTIVATE SET-TOP BOX:	SET-TOP BOX AKTIVIEREN
YES:	JA
NO:	NEIN

Fig. 2

210:	AUF EINGANG DER MELDUNG WARTEN, DASS BZ-MODUL **60** BEREIT IST
215:	SET-TOP BOX BERECHTIGT, 1. SIGNAL ZU ENTSCHLÜSSELN?
225:	1. SIGNALBERECHTIGUNGSCODE ÜBERTRAGEN
230:	AUF EINGANG DER SIGNALÄNDERUNGSMELDUNG WARTEN
235:	SET-TOP BOX BERECHTIGT, 2. SIGNAL ZU ENTSCHLÜSSELN?
240:	2. SIGNALBERECHTIGUNGSCODE ÜBERTRAGEN
TRANSMIT ENCRYPTED 1ST & 2ND SIGNALS:	VERSCHLÜSSELTE 1. UND 2. SIGNALE ÜBERTRAGEN
YES:	JA
NO:	NEIN

Patentansprüche

1. System zum Entschlüsseln verschlüsselter Übertragungen mindestens eines ersten Signals oder eines zweiten Signals, wobei jedes repräsentativ für Videoinhalt von einem Dienstanbieter (**52**) ist, wobei das System einen Empfänger (**54**) mit einem eingebetteten Modul für bedingten Zugang (**60**) zum Entschlüsseln des ersten Signals, ein entfernbares Modul für bedingten Zugang (**62**) und eine Schnittstelle zum Eingreifen in das entfernbare Modul für bedingten Zugang umfasst, wobei das entfernbare Modul für Entschlüsseln des zweiten Signals und Übersteuern des eingebetteten Moduls, wenn das entfernbare Modul aktiviert ist, konfiguriert ist, **dadurch gekennzeichnet**, dass das System ferner einen Sender zum Übertragen (**125**) einer Meldung darüber, dass das entfernbare Modul aktiviert ist, zu einer Station (**52**) außerhalb des Systems umfasst, um daraufhin von der Station eine Berechtigung (**130**) zu empfangen, die das Entschlüsseln des zweiten Signals ermöglicht, falls das entfernbare Modul zugelassen ist.

2. System nach Anspruch 1, wobei das entfernbare Modul durch Eingreifen des entfernbaren Moduls in die Schnittstelle aktiviert wird.

3. System nach Anspruch 1, wobei das entfernbare Modul durch Ändern einer Einstellung des Systems aktiviert wird.

4. System nach Anspruch 1, wobei jedes jeweilige der Module einen jeweiligen Entschlüsselungsalgorithmus verwendet, wobei die jeweiligen Entschlüsselungsalgorithmen sich voneinander unterscheiden.

5. System nach Anspruch 1, untergebracht in einer Set-Top-Box.

6. System nach Anspruch 1, wobei das erste Signal einen Teil des Videoinhalts repräsentiert, der kleiner als der gesamte Videoinhalt ist, und wobei das zweite Signal den gesamten Videoinhalt repräsentiert.

7. Verfahren, das ein System in die Lage versetzt, verschlüsselte Übertragungen mindestens eines ersten Signals oder eines zweiten Signals zu entschlüsseln, wobei jedes repräsentativ für Videoinhalt von einem Dienstanbieter (**50**) ist, wobei das System einen Empfänger (**54**) mit einem eingebetteten Modul für bedingten Zugang (**60**) zum Entschlüsseln des ersten Signals und eine Schnittstelle zum Eingreifen in ein entfernbares Modul für bedingten Zugang (**62**) umfasst, wobei das entfernbare Modul für Entschlüsseln des zweiten Signals und Übersteuern des eingebetteten Moduls konfiguriert ist, dadurch gekennzeichnet, dass das Verfahren Übertragen (**125**) einer Meldung darüber, dass das entfernbare Modul aktiviert ist, zu einer Station (**52**) außerhalb des Systems umfasst, um daraufhin von der Station eine Berechtigung (**130**) zu empfangen, die ermöglicht, das zweite Signal zu entschlüsseln, falls das entfernbare Modul zugelassen ist.

8. Verfahren nach Anspruch 7, wobei das Ermöglichen, zu entschlüsseln, Ermöglichen umfasst, das zweite Signal zu empfangen.

9. Verfahren nach Anspruch 7, umfassend Verschlüsseln des ersten Signals unter Verwendung eines ersten Algorithmus und Verschlüsseln des zweiten Signals unter Verwendung eines zweiten Algorithmus, der vom ersten Algorithmus verschieden ist.

10. Verfahren nach Anspruch 7, wobei das erste Signal einen Teil des Videoinhalts repräsentiert, der kleiner als der gesamte Videoinhalt ist, und wobei

das zweite Signal den gesamten Videoinhalt repräsentiert.

Es folgen 3 Blatt Zeichnungen

Anhängende Zeichnungen

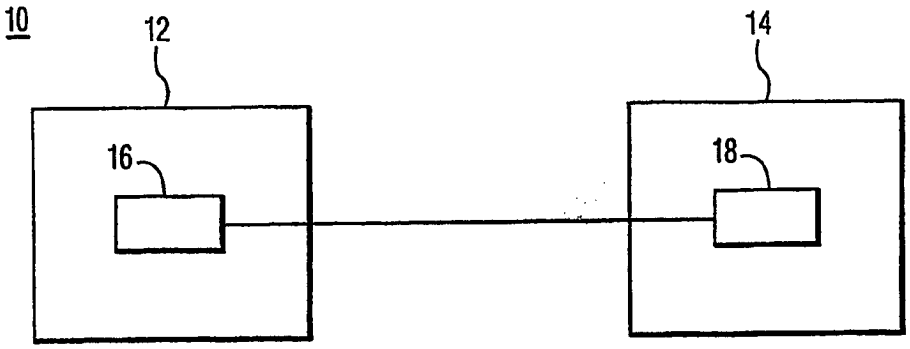

FIG. 1

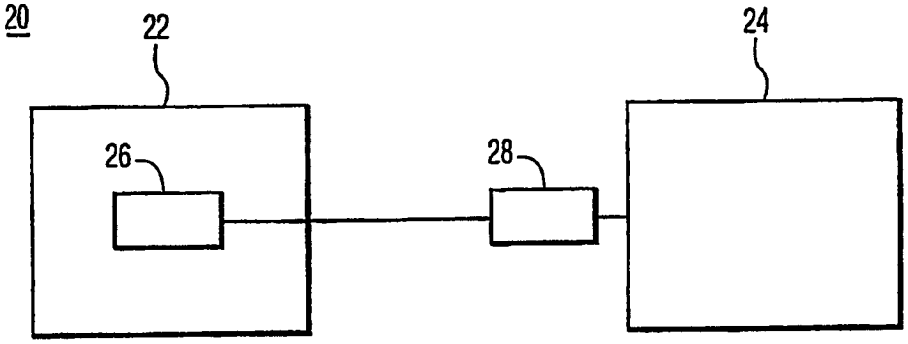

FIG. 2

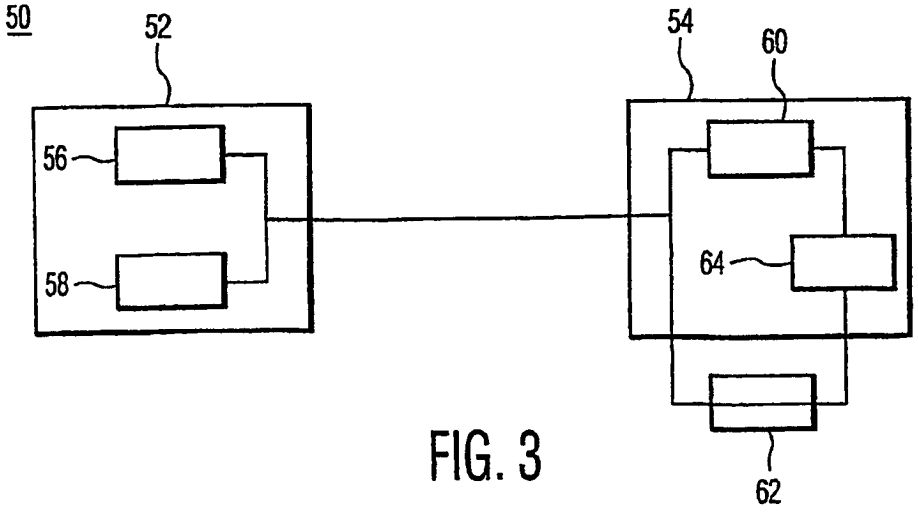

FIG. 3

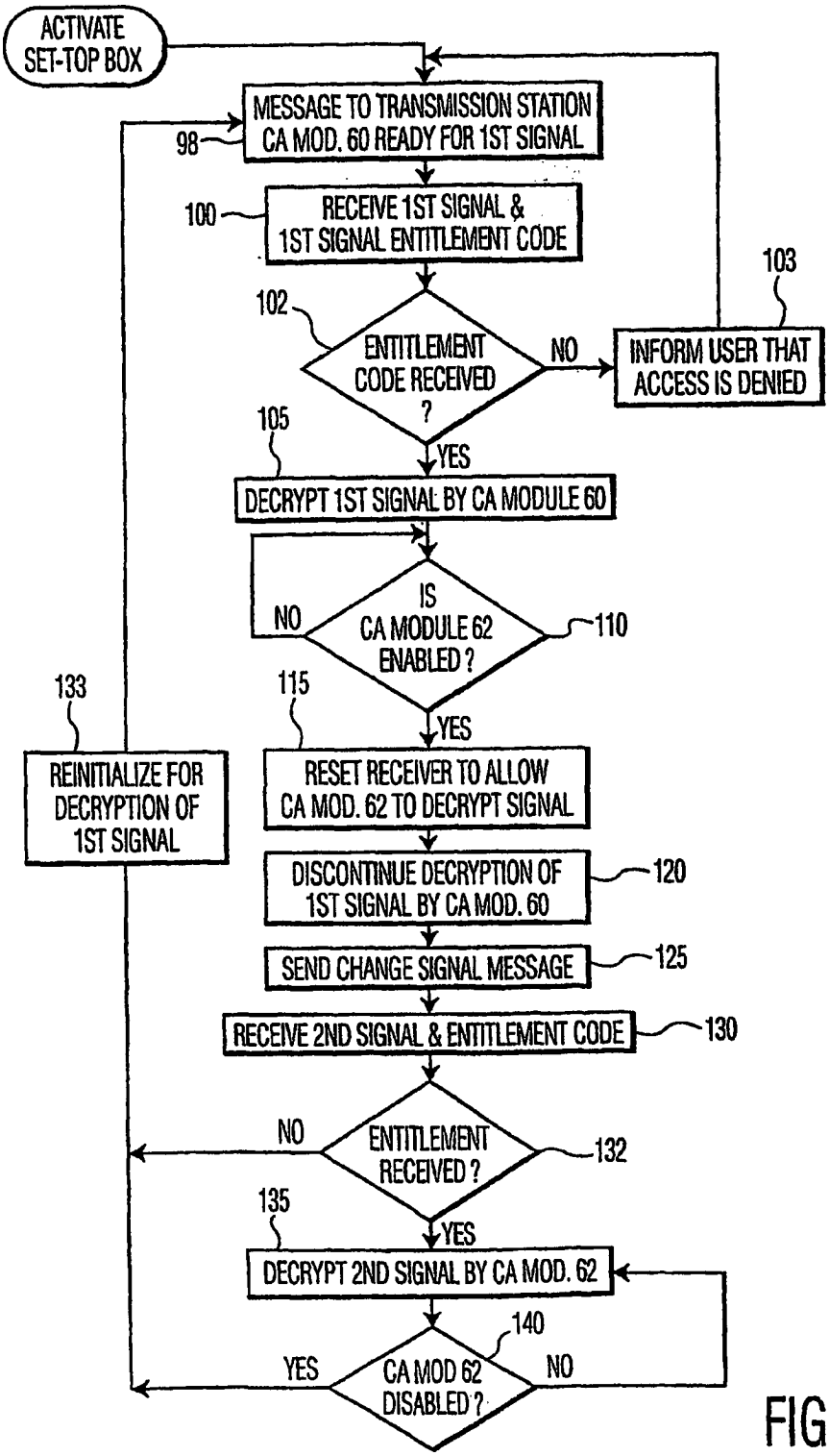
ACTIVATE SET-TOP BOX
MESSAGE TO TRANSMISSION STATION CA MOD. 60 READY FOR 1ST SIGNAL
98
RECEIVE 1ST SIGNAL & 1ST SIGNAL ENTITLEMENT CODE
100
ENTITLEMENT CODE RECEIVED ?
102
NO
INFORM USER THAT ACCESS IS DENIED
103
YES
105
DECRYPT 1ST SIGNAL BY CA MODULE 60
IS CA MODULE 62 ENABLED ?
NO
110
YES
115
REINITIALIZE FOR DECRYPTION OF 1ST SIGNAL
133
RESET RECEIVER TO ALLOW CA MOD. 62 TO DECRYPT SIGNAL
DISCONTINUE DECRYPTION OF 1ST SIGNAL BY CA MOD. 60
120
SEND CHANGE SIGNAL MESSAGE
125
RECEIVE 2ND SIGNAL & ENTITLEMENT CODE
130
NO
ENTITLEMENT RECEIVED ?
132
YES
135
DECRYPT 2ND SIGNAL BY CA MOD. 62
140
YES
CA MOD 62 DISABLED ?
NO

FIG. 4

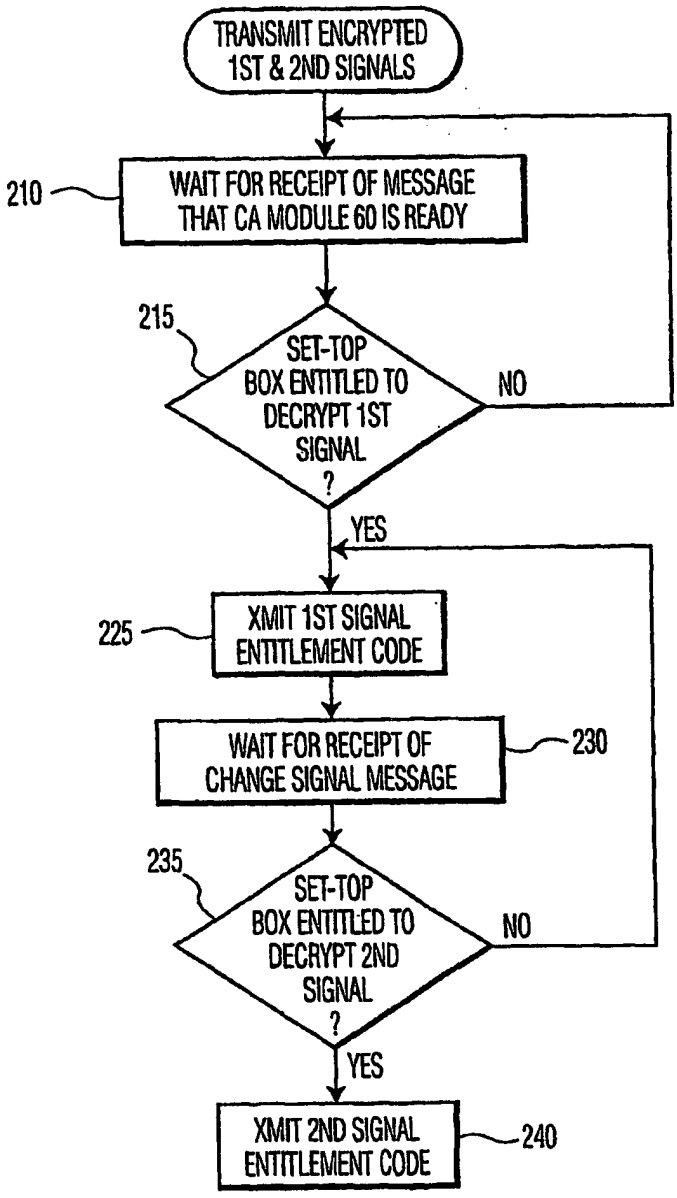
TRANSMIT ENCRYPTED 1ST & 2ND SIGNALS
210
WAIT FOR RECEIPT OF MESSAGE THAT CA MODULE 60 IS READY
215
SET-TOP BOX ENTITLED TO DECRYPT 1ST SIGNAL ?
NO
YES
225
XMIT 1ST SIGNAL ENTITLEMENT CODE
WAIT FOR RECEIPT OF CHANGE SIGNAL MESSAGE
230
235
SET-TOP BOX ENTITLED TO DECRYPT 2ND SIGNAL ?
NO
YES
XMIT 2ND SIGNAL ENTITLEMENT CODE
240

FIG. 5