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

(10) **DE 697 38 628 T2** 2009.05.28

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 023 795 B1**
(21) Deutsches Aktenzeichen: **697 38 628.7**
(86) PCT-Aktenzeichen: **PCT/US97/19890**
(96) Europäisches Aktenzeichen: **97 949 357.4**
(87) PCT-Veröffentlichungs-Nr.: **WO 1998/021852**
(86) PCT-Anmeldetag: **28.10.1997**
(87) Veröffentlichungstag der PCT-Anmeldung: **22.05.1998**
(97) Erstveröffentlichung durch das EPA: **02.08.2000**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **09.04.2008**
(47) Veröffentlichungstag im Patentblatt: **28.05.2009**

(51) Int Cl.[8]: ***H04L 9/00*** (2006.01)

(30) Unionspriorität:
745483 **12.11.1996** **US**

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

(73) Patentinhaber:
Scientific-Atlanta, Inc., Lawrenceville, Ga., US

(74) Vertreter:
TBK-Patent, 80336 München

(72) Erfinder:
THATCHER, William B., Atlanta, GA 30309, US;
WASILEWSKI, Anthony J., Alpharetta, GA 30202, US

(54) Bezeichnung: **KONTROLLE FÜR EINEN GLOBALEN DATENTRANSPORTSTROM**

Beschreibung

HINTERGRUND DER ERFINDUNG

Gebiet der Erfindung

[0001] Die vorliegende Erfindung betrifft Kabelfernsehsysteme mit bedingtem Zugriff. Insbesondere betrifft die Erfindung ein System, mit dem ein lokaler Kabelkopfstellenbetreiber den Zugriff seiner Teilnehmer auf einen globalen oder Inlands-Transportdatenstrom steuern kann.

Beschreibung des Standes der Technik

[0002] Fig. 1A zeigt einen herkömmlichen Verschlüssler **2**. Unverschlüsselte Payload-Daten UPD werden unter Verwendung eines Verschlüsselungsschlüssels EK zu verschlüsselten Payload-Daten an einem Ausgang OUT des Verschlüsslers **2** verarbeitet. Fig. 1B zeigt einen herkömmlichen Entschlüssler **4**. Verschlüsselte Payload-Daten EPD werden unter Verwendung eines Entschlüsselungsschlüssels DK in dem Entschlüssler **4** so verarbeitet, dass an einem Ausgang OUT des Entschlüsslers **4** entschlüsselte Payload-Daten erzeugt werden.

[0003] Fig. 2A zeigt einen herkömmlichen Codierer **10**. Fig. 2B zeigt einen herkömmlichen Decodierer **40**. Die Fig. 2A und Fig. 2B zeigen den firmeninternen Stand der Technik und keinen bereits veröffentlichen Stand der Technik. In Fig. 2A stellt ein Serviceprovider **12** digitale Dienste, beispielsweise MPEG-codierte Bewegtbilder, digitale Tonaufnahmen, Software, Spiele usw., für den Transport zu dem Decodierer **40** bereit. Der Dienst wird mit einem Seed von einem Pseudozufallszahlen-Seed-Generator **14** verschlüsselt. Ein Verschlüssler **22** verarbeitet die Dienstdaten unter Verwendung des Seeds als Verschlüsselungsschlüssel, um einen verschlüsselten Dienst E_{SEED}(SERVICE) zu erzeugen. Der verschlüsselte Dienst wird in einem Multiplexer **20** kombiniert und wird in einen Transportdatenstrom TDS eingestellt. Damit der Decodierer **20** die Dienstdaten aus den verschlüsselten Dienstdaten regenerieren kann, muss der Decodierer **40** den Seed erhalten.

[0004] Der Seed wird in dem Transportdatenstrom TDS im Rundfunkmodus verteilt (d. h., alle Decodierer empfangen den Seed gleichzeitig). Der Seed muss verschlüsselt werden, um eine Nutzung durch mögliche Datenpiraten zu verhindern. Der Seed wird in einem Verschlüssler **24** unter Verwendung eines Multisession-Schlüssels MSK zu einem verschlüsselten Seed E_{MSK}(SEED) verschlüsselt. Der Multisession-Schlüssel MSK kommt von einem Dienstverteiler **16**. Der verschlüsselte Seed E_{MSK}(SEED) wird mit dem Multiplexer **20** im Rundfunkmodus in den Transportdatenstrom TDS eingestellt. Vorzugsweise wird der Seed häufig modifiziert, beispielsweise zehnmal je Sekunde. Daher wird der verschlüsselte Seed E_{MSK}(SEED) beispielsweise zehnmal je Sekunde an alle Decodierer **40** gesendet. Um den Seed zu regenerieren, muss der Decodierer **40** Zugriff auf den Multisession-Schlüssel MSK erlangen.

[0005] Der Multisession-Schlüssel MSK wird über den Transportdatenstrom TDS an autorisierte Decodierer **40** (d. h., Decodierer von Teilnehmern, die ihre Monatsrechnung bezahlt haben) verteilt. Vorzugsweise wird der Multisession-Schlüssel MSK einmal im Monat geändert. Um den Multisession-Schlüssel MSK über den Transportdatenstrom TDS zu verteilen, wird der Multisession-Schlüssel in einem Verschlüssler **26** unter Verwendung einer geheimen laufenden Nummer SSN als Verschlüsselungsschlüssel zu einem verschlüsselten Multisession-Schlüssel E_{SSN}(MSK) verschlüsselt. Da der verschlüsselte Multisession-Schlüssel für die Decodierer nur einmal im Monat bereitgestellt werden muss, kann der verschlüsselte Multisession-Schlüssel an jeden Decodierer einzeln adressiert werden, anstatt den verschlüsselten Seed an alle Decodierer gleichzeitig zu senden. In der Praxis wird der MSK, bevor er benötigt wird, mehrmals im Monat an jeden Decodierer adressiert und gesendet, um unter anderem zu gewährleisten, dass er entschlüsselt und verfügbar wird, wenn er gebraucht wird. Der Multiplexer **20** stellt den verschlüsselten Multisession-Schlüssel E_{SSN}(MSK) nur dann in den Transportdatenstrom TDS ein, wenn der Teilnehmer seine Monatsrechnung bezahlt hat. Jeder Decodierer **40** hat in sich eine eindeutige geheime laufende Nummer SSN und eine entsprechende öffentliche laufende Nummer (die als Adresse verwendet wird) gespeichert. In Fig. 2A werden die geheime laufende Nummer SSN und die öffentliche laufende Nummer PSN für einen bestimmten Decodierer aus einem Speicher **18** abgerufen. Die geheime laufende Nummer SSN wird für den Verschlüssler **26** bereitgestellt, und die öffentliche laufende Nummer PSN wird für den Multiplexer **20** bereitgestellt. Wenn die Rechnung pünktlich bezahlt worden ist, erstellt der Multiplexer **20** den verschlüsselten Multisession-Schlüssel für den Transport zum Decodierer, dessen Adresse die öffentliche laufende Nummer PSN ist.

[0006] In Fig. 2B werden die entsprechende geheime laufende Nummer SSN und die zugehörige öffentliche laufende Nummer PSN in einem Speicher **32** des Decodierers **40** gespeichert. Die öffentliche laufende Nummer PSN wird für einen Demultiplexer **30** bereitgestellt, sodass der Demultiplexer **30** einen an den Decodierer **40** adressierten verschlüsselten Multisession-Schlüssel unter der öffentlichen laufenden Nummer PSN, die der geheimen laufenden Nummer entspricht, aus dem Transportdatenstrom TDS auswählen kann. Der verschlüsselte Multisession-Schlüssel E_{SSN}(MSK) wird in einem Entschlüssler **34** unter Verwendung der geheimen laufenden Nummer SSN aus dem Speicher **32** zu dem Multisessi-

on-Schlüssel MSK entschlüsselt. Der Demultiplexer **30** wählt außerdem den verschlüsselten Seed E_{MSK}(SEED) aus dem Transportdatenstrom TDS aus. Der verschlüsselte Seed wird in einem Entschlüssler **36** unter Verwendung des Multisession-Schlüssels MSK als Entschlüsselungsschlüssel zu einem unverschlüsselten Seed verarbeitet. Der unverschlüsselte Seed ändert sich vorzugsweise mit einer hohen Geschwindigkeit, beispielsweise zehnmal je Sekunde. Der Demultiplexer **30** wählt außerdem den verschlüsselten Dienst E_{SEED}(SERVICE) aus dem Transportdatenstrom TDS aus. Der verschlüsselte Dienst wird in einem Entschlüssler **38** unter Verwendung des Seeds als Entschlüsselungsschlüssel verarbeitet, um den unverschlüsselten Dienst zu regenerieren.

[0007] Zur Bereitstellung des Multisession-Schlüssels MSK sind noch andere Mittel bekannt. Beispielsweise wird in dem Gammie erteilten US-Patent Nr. 5.029.207 der Multisession-Schlüssel MSK an dem Codierer zweimal verschlüsselt und an dem Decodierer zweimal entschlüsselt, zunächst in einem austauschbaren Sicherheitsmodul und dann in einem feststehenden Sicherheitselement des Decodierers.

[0008] Außerdem werden zur Abwehr von Datenpiraten der Speicher **32** und die Entschlüssler **34** und **36** (Fig. 2B) und der Speicher für den Multisession-Schlüssel MSK (nicht dargestellt) in einem sicheren Mikroprozessor mechanisiert, der Piraten den Zugriff auf die Schlüssel SSN und MSK verwehrt. Ein Pirat hätte zwar an den Ausgangsanschlüssen des sicheren Mikroprozessors noch immer Zugriff auf den Seed, aber die Nutzungsdauer des Seeds ist kurz, da er häufig geändert wird, beispielsweise zehnmal je Sekunde.

[0009] Fig. 3 zeigt ein herkömmliches System **50**, das eine Inlandssteuerzentrale **52** hat, die einen Codierer **10** enthält. Ein Transportdatenstrom TDS von dem Codierer **10** wird mit einem Uplink-Sender der Inlandssteuerzentrale **52** an einen Satelliten-Repeater **54** gesendet. Der Satelliten-Repeater **54** sendet dieses Signal erneut, sodass eine Kabelkopfstelle **56** das Signal empfängt. Die Kabelkopfstelle **56** sendet dieses Signal erneut an die Decodierer **40**.

[0010] In dem Inlands-Transportdatenstrom (NTDS) enthält eine Berechtigungsverwaltungsnachricht EMM, die eindeutig an einen einzelnen Decodierer adressierbar ist, den MSK, der mit der SSN des speziellen Decodierers verschlüsselt ist, sowie Dienstautorisierungsinformationen für den speziellen Decodierer. In dem System **50** mit der Inlandssteuerzentrale **52**, die den Inlands-Transportdatenstrom NTDS erzeugt, stellt die Inlandssteuerzentrale **52** sowohl den verschlüsselten MSK (d. h. den E_{SSN}(MSK)) als auch die Decodierer-Dienstautorisierungsinformationen bereit. Die Inlandszentrale erzeugt die entsprechenden Berechtigungsverwaltungsnachrichten und adressiert sie an die einzelnen Codierer. Der Kabelkopfstellenbetreiber fungiert bloß als Kanal für diesen Inlands-Transportdatenstrom.

[0011] Einige Kabelkopfstellenbetreiber wollen jedoch einen lokalen Einfluss auf die Dienstautorisierungsinformationen haben. Sie wollen den bedingten Zugriff eines Decodierers auf Programme und auf spezielle Programme unter lokaler Kontrolle haben. Die lokalen Kabelkopfstellenbetreiber halten es jedoch nicht für notwendig, ihre Programmverschlüsselung selbst durchzuführen. Sie möchten die Programmverschlüsselung beibehalten, die bereits an der Inlandssteuerzentrale durchgeführt worden ist.

[0012] Bei zahlreichen Kabelsystemen, die heute in Gebrauch sind, führt eine Inlandssteuerzentrale das gesamte Multiplexing von Diensten sowie die Verschlüsselung jedes Dienstes und die globale Verschlüsselung des gesamten Payload-Teils des Transportdatenstroms durch. Bei einem solchen System fungieren die Kabelkopfstellenbetreiber im Wesentlichen als Kanäle für dieses Inlandssignal. Die Inlandszentrale erfüllt auch alle anderen Pflichten für den bedingten Zugriff, unter anderem die Einstellung von Dienstautorisierungsinformationen in die Berechtigungsverwaltungsnachrichten, die an jeden Decodierer adressiert werden.

[0013] Andere Systeme, die heute in Gebrauch sind, ermöglichen es dem Kabelkopfstellenbetreiber, lokalen Einfluss auf den bedingten Zugriff und die Verschlüsselung zu nehmen. Einige Betreiber wollen einen lokalen Einfluss nehmen können, aber die hierfür benötigte Ausrüstung ist natürlich teurer.

[0014] Kabelbetreiber werden den Zugang zu verschiedenen Marktsegmenten irgendwie differenzieren oder steuern wollen. Nehmen wir beispielsweise an, dass drei Kabelgesellschaften in einem gegebenen Gebiet arbeiten. Wenn sie alle ein Signal der Inlandszentrale für ihre Teilnehmer bereitstellen, könnte jemand, der Teilnehmer bei einer Gesellschaft ist, seinen Set-Top-Decodierer an jemanden verleihen, der Teilnehmer bei einer anderen Gesellschaft ist. Somit wird ein System benötigt, das es dem Kabelkopfstellenbetreiber ermöglicht, das von der Inlandszentrale bereitgestellte Signal weiter zu verwenden, aber dennoch den Zugang zu anderen Markbereichen oder -segmenten zu kontrollieren.

[0015] Verwiesen sei auf das Dokument AU-A-636039, das die vorkennzeichnenden Merkmale der vorliegenden Erfindung beschreibt.

KURZE DARSTELLUNG DER ERFINDUNG

[0016] Die vorliegende Erfindung ist in den Ansprüchen definiert.

[0017] Ein Vorzug der Erfindung besteht darin, dass sie Mittel bereitstellen kann, mit denen ein lokaler Kabelkopfstellenbetreiber Inlandsprogramm-Dienstdaten verteilen kann und dabei den Zugriff seiner Teilnehmer auf die Daten steuern kann.

KURZE BESCHREIBUNG DER ZEICHNUNGEN

[0018] Die Erfindung wird nachstehend anhand von bevorzugten Ausführungsformen unter Bezugnahme auf die folgenden Figuren näher beschrieben, wobei Fig. 6 eine Ausführungsform der Erfindung darstellt und Fig. 9 eine weitere Ausführungsform unter Einbeziehung der Ausführungsform von Fig. 6 darstellt. Die übrigen Zeichnungen stellen Ausführungsformen dar, die nicht Bestandteil der Erfindung sind. Hierbei sind:

[0019] die Fig. 1A und Fig. 1B Grundfunktionsdiagramme von bekannten Verschlüsslern bzw. Entschlüsslern;

[0020] die Fig. 2A und Fig. 2B Funktionsblockdiagramme bekannter Verschlüssler bzw. Entschlüssler des firmeninternen Standes der Technik;

[0021] Fig. 3 ein Blockdiagramm eines bekannten Informationsverteilungssystems;

[0022] Fig. 4 ein Format-Diagramm, das zeigt, wie Elementardatenströme in Transportpaketen codiert werden;

[0023] Fig. 5 ein Funktionsdiagramm eines Decodierers;

[0024] Fig. 6 ein Funktionsblockdiagramm eines Verschlüsselungssteuersystems nach einer Ausführungsform der vorliegenden Erfindung;

[0025] Fig. 7 ein Funktionsblockdiagramm eines Verschlüsselungssteuersystems nach einer weiteren Ausführungsform;

[0026] Fig. 8 ein Funktionsblockdiagramm eines Verschlüsselungssteuersystems nach einer weiteren Ausführungsform und

[0027] Fig. 9 eine schematische Darstellung eines Informationsverteilungssystems nach einer weiteren Ausführungsform.

DETAILLIERTE BESCHREIBUNG DER BEVORZUGTEN AUSFÜHRUNGSFORMEN

[0028] Fig. 4 ist ein Format-Diagramm eines typischen Transportdatenstroms. Video- und Audiodaten werden in Form eines paketisierten Elementarstroms mit einem Header, einem Darstellungszeitstempel und dem Video selbst bereitgestellt. Der paketisierte Elementarstrom wird dem Payload-Teil eines oder mehrerer Transportpakete zugeteilt. Transportpakete haben vorzugsweise eine Länge von 188 Bit. Die Transportpakete enthalten vorzugsweise einen Synchronisationsblock und Präfix-Daten, an die sich die Payload-Daten anschließen. Ein Standard mit der Bezeichnung MPEG-2 (ISO/IEC 13818-1) definiert spezielle Ausführungsformen des Transportdatenstroms. Ein Multiplexer/Verschlüssler **64** kombiniert einzelne Transportpakete **62** zu einem Datenrahmen **60**.

[0029] Von besonderem Interesse für die vorliegende Erfindung sind Berechtigungsverwaltungsnachrichten EMM und Berechtigungssteuernachrichten ECM. Diese Nachrichten werden in den Transportdatenstrom TDS gemultiplext. Die Berechtigungsverwaltungsnachrichten werden an einen speziellen Decodierer oder eine Gruppe von Decodierern adressiert. Die Berechtigungssteuernachrichten werden an alle Decodierer gesendet. In den Daten, die in den Berechtigungssteuernachrichten übertragen werden, sind Seed-Daten enthalten, die mit einem Multisession-Schlüssel verschlüsselt werden. Die Berechtigungssteuernachricht ECM wird wiederholt mit einer hohen Geschwindigkeit, beispielsweise zehnmal je Sekunde, gesendet. Ein Multisession-Schlüssel MSK, der mit einer geheimen laufenden Nummer verschlüsselt ist, ist in der Berechtigungsverwaltungsnachricht EMM enthalten. Die Berechtigungsverwaltungsnachricht wird an den Decodierer adressiert, der die geheime laufende Nummer gespeichert hat, die zum Verschlüsseln des Multisession-Schlüssels verwendet wird. Die Berechtigungsverwaltungsnachrichten werden selten gesendet, beispielsweise einmal im Monat. In der Praxis wird die Berechtigungsverwaltungsnachricht mehrmals im Monat an jeden Decodierer gesendet, sodass der Decodierer den Multisession-Schlüssel für die kommende Sitzung (z. B. nächster Monat) entschlüsseln und speichern kann. Zu einem bestimmten Zeitpunkt liefert die Berechtigungssteuernachricht Daten, die die Umschaltung auf den neuen Multisession-Schlüssel angeben, der aus einer früheren Berechtigungsverwaltungsnachricht erhalten wurde.

[0030] Fig. 5 zeigt einen Decodierer zum Decodieren des Eingangs-Transportdatenstroms zu entschlüsselten Diensten **109**. Ein Demultiplexer **72** trennt eine Berechtigungssteuernachricht **74**, eine Berechtigungsverwaltungsnachricht **76** und Textdaten **78** von dem Transportdatenstrom. Andere Payload-Teile des Transportdatenstroms werden für einen Entschlüssler **104** bereitgestellt. Der Demultiplexer **72** hat ähnliche Funktionen wie der Demultiplexer **30** (Fig. 2B). Ein Decodierer **70** enthält einen sicheren Mikroprozessor **80**. Der sichere Mikroprozessor **80** enthält einen sicheren Speicher **82**, der eine geheime laufende Nummer SSN und den Multisession-Schlüssel MSK speichert. Bei dem sicheren Mi-

kroprozessor **80** ruft eine Bedingter-Zugriffs-Logik **90** die geheime laufende Nummer SSN aus dem sicheren Speicher **82** ab und stellt die geheime laufende Nummer für einen Entschlüssler **84** bereit. Der Entschlüssler **84** verarbeitet die Berechtigungsverwaltungsnachricht **76** so, dass bei **92** der Multisession-Schlüssel MSK regeneriert wird. Die Bedingter-Zugriffs-Logik **90** speichert den Multisession-Schlüssel MSK in dem sicheren Speicher **82**. Dann liest die Bedingter-Zugriffs-Logik **90** den Multisession-Schlüssel MSK aus dem sicheren Speicher **82** und stellt ihn für einen Entschlüssler **86** bereit. Der Entschlüssler **86** verarbeitet die Berechtigungssteuernachricht **74** so, dass mehrere Seeds und Bedingter-Zugriffs-Daten **88** regeneriert werden. Die Bedingter-Zugriffs-Logik **90** stellt einen globalen Seed **94** der Seeds **88** für den Entschlüssler **104** bereit. Die Bedingter-Zugriffs-Logik **90** verarbeitet die Bedingter-Zugriffs-Daten **88** so, dass sie autorisierte Dienste identifiziert, und stellt ein Dienstwahlsignal **96** für einen Dienst-Demultiplexer **106** bereit. Für die autorisierten Dienste stellt die Bedingter-Zugriffs-Logik **90** verschlüsselte Dienst-Seeds **98** aus den Seeds **88** für einen Entschlüssler **100** zum Entschlüsseln mit dem Mehrdienstschlüssel bereit. Für autorisierte Dienste stellt der Entschlüssler **100** Seeds **102** für Entschlüssler **108** für autorisierte Dienste bereit.

[0031] In Fig. 4 können einzelne Dienste (z. B. Video 1 oder Audio 1) mit entsprechenden Dienst-Seeds verschlüsselt werden. Die verschlüsselten oder unverschlüsselten Dienste werden zu dem Datenrahmen **60** formatiert. Der gesamte Dienst-Teil des Datenrahmens **60** wird mit einem globalen Seed verschlüsselt Der verschlüsselte Teil des Datenrahmens **60** wird in dem Entschlüssler **104** (Fig. 5) unter Verwendung des globalen Seeds **94** so verarbeitet, dass die einzelnen Dienste regeneriert werden. Die einzelnen Dienste können verschlüsselt sein oder können unverschlüsselt sein. Die einzelnen Dienste werden für den Multiplexer **106** (Fig. 5) bereitgestellt, wo die einzelnen verschlüsselten Dienstdaten **107** für die Entschlüssler **108** bereitgestellt werden. Die Entschlüssler **108** verarbeiten die verschlüsselten Dienstdaten **107** unter Verwendung der Seeds **102**, um entschlüsselte Dienste **109** bereitzustellen.

[0032] In Fig. 6 enthält ein Verschlüsselungssteuersystem **110** einen Demultiplexer **112**, einen Multiplexer **114**, einen ersten sicheren Mikroprozessor **120** und einen zweiten Mikroprozessor **130**. Der sichere Mikroprozessor **120** enthält einen Geheime-Laufende-Nummern-Speicher **122**, einen Entschlüssler **124** und einen Multisession-Speicher **126**. Der Geheime-Laufende-Nummern-Speicher **122** funktioniert in der gleichen Weise wie der Geheime-Laufende-Nummern-Speicher **32** (Fig. 2B). Der Entschlüssler **124** funktioniert in der gleichen Weise wie der Entschlüssler **34** (Fig. 2B). Der Speicher **126** funktioniert in der gleichen Weise wie der Speicher **82** (Fig. 5).

[0033] Der zweite sichere Mikroprozessor **130** enthält einen Geheime-Laufende-Nummern-Speicher **132** und einen Entschlüssler **134**. Der Speicher **132** funktioniert in der gleichen Weise wie der Speicher **18** (Fig. 2A), und der Verschlüssler **134** funktioniert in der gleichen Weise wie der Verschlüssler **26** (Fig. 2A). Der Demultiplexer **112** funktioniert in der gleichen Weise wie der Demultiplexer **30** (Fig. 2B). Der Multiplexer **114** funktioniert in der gleichen Weise wie der Multiplexer **20** (Fig. 2A).

[0034] Bei einer typischen Operation wird eine Inlandsquelle des Transportdatenstroms TDS mit einer Satelliten-Repeater-Station geuplinkt. Die Satelliten-Repeater-Station downlinkt die Übertragung des Inlands-Transportdatenstroms TDS mit mehreren Kabelkopfstellenbetreibern, von denen mindestens einer mit dem Verschlüsselungssteuersystem **110** ausgerüstet ist. Der Kabelkopfstellenbetreiber empfängt den Inlands-Transportdatenstrom TDS und demultiplext den Datenstrom zu einem verschlüsselten Inlands-Dienstdatenstrom, einer Inlands-Berechtigungssteuernachricht (Inlands-ECM) und einer Inlands-Berechtigungsverwaltungsnachricht (Inlands-EMM). Die Inlands-Berechtigungsverwaltungsnachricht wird in dem Verschlüsselungssteuersystem **110** zu einer lokalen Berechtigungsverwaltungsnachricht (lokale EMM) verarbeitet. Der Multiplexer **114** reassembliert die verschlüsselten Inlands-Dienstdaten, die Inlands-Berechtigungssteuernachrichtendaten und die lokale Berechtigungsverwaltungsnachricht zu einem lokalen Transportdatenstrom (lokaler TDS).

[0035] Die Inlands-Berechtigungsverwaltungsnachricht wird in dem Entschlüssler **124** so verarbeitet, dass der Multisession-Schlüssel regeneriert wird und in dem Speicher **126** gespeichert wird. Der Multisession-Schlüssel wird über eine sichere Verbindung **116** für den Verschlüssler **134** bereitgestellt. Der Multisession-Schlüssel wird in dem Verschlüssler **134** unter Verwendung der geheimen laufenden Nummer aus dem Speicher **132** verarbeitet und wird dann in die lokale Berechtigungsverwaltungsnachricht eingestellt. Jedoch ist entweder (1) der von dem Verschlüssler **134** verwendete Verschlüsselungsalgorithmus von dem Verschlüsselungsalgorithmus verschieden, der von der Landeszentrale zum Verschlüsseln des Multisession-Schlüssels verwendet wird, oder (2) die in dem Speicher **132** gespeicherten geheimen laufenden Nummern sind von den in der vergleichbaren Datenbank gespeicherten geheimen laufenden Nummern verschieden, die zum Verschlüsseln des Multisession-Schlüssels in der Inlandzentrale verwendet werden, oder (3) beides.

[0036] Die Teilnehmer des Kabelkopfstellenbetreibers werden einen Decodierer mit einem Entschlüssler zum Entschlüsseln des Multisession-Schlüssels

verlangen, der einen Algorithmus hat, der mit dem Verschlüssler **134** (Fig. 6) kompatibel ist. Ebenso haben die Decodierer der Teilnehmer des Kabelkopfstellenbetreibers geheime laufende Nummern gespeichert, die den in dem Speicher **132** (Fig. 6) gespeicherten geheimen laufenden Nummern entsprechen. Erfindungsgemäß kann ein Kabelkopfstellenbetreiber, der mit dem Verschlüsselungssteuersystem **110** ausgerüstet ist, den Multisession-Schlüssel sicher an die Decodierer in seinem System bereitstellen, aber wegen des eindeutigen Verschlüsselungsalgorithmus **134** (d. h., eindeutig für den Kabelkopfstellenbetreiber) und der in dem Speicher **132** gespeicherten Liste der eindeutigen geheimen laufenden Nummern können die für die Teilnehmer des Kabelkopfstellenbetreibers bereitgestellte Decodierer nicht zum Empfangen von verschlüsselten Inlandsdiensten von der Satelliten-Repeater-Station oder einem anderen Kabelkopfstellenbetreiber verwendet werden. Auf diese Weise kann der Kabelkopfstellenbetreiber den Zugriff auf die Inlandsdienste verweigern, beispielsweise wenn der Teilnehmer seine Rechnung nicht bezahlt. Außerdem kann der Decodierer, der für den Teilnehmer des Kabelkopfstellenbetreibers bereitgestellt wird, nicht zum Empfangen von verschlüsselten Diensten von einem Kabelsystem verwendet werden, sodass es unwahrscheinlich ist, dass er verliehen wird.

[0037] Wie in dem US-Patent Nr. 5.029.207 beschrieben, enthalten einige Decodierer Entschlüssler mit umprogrammierbaren Entschlüsselungsalgorithmen und/oder umprogrammierbaren geheimen laufenden Nummern. Diese Entschlüssler sind umprogrammierbar, wenn spezielle adressierte Nachrichten (z. B. die hier beschriebenen Berechtigungsverwaltungsnachrichten) von dem speziellen Decodierer oder der Gruppe von Decodierern, die adressiert werden, empfangen werden. Wenn die Inlandszentrale diesen Decodierertyp verwendet, kann der lokale Kabelkopfstellenbetreiber diesen Decodierertyp erwerben und an seine Teilnehmer weiterverkaufen. Dann kann der Kabelkopfstellenbetreiber entsprechende Berechtigungsverwaltungsnachrichten an einzelne Decodierer senden, um den Algorithmus zu ändern, der zum Entschlüsseln des Multisession-Schlüssels verwendet wird, oder um die Adresse mit der geheimen laufenden Nummer des Decodierers zu ändern. Auf diese Weise ist ein größerer Markt für nur eine Decodierer-Ausführung vorhanden, und der Kabelkopfstellenbetreiber kann aufgrund des größeren Marktes die Decodierer an seine Teilnehmer zu niedrigeren Kosten liefern.

[0038] In Fig. 7 enthält ein Verschlüsselungssteuersystem **140** den Demultiplexer **112**, den Multiplexer **114**, den ersten sicheren Mikroprozessor **120** und den zweiten sicheren Mikroprozessor **130**. Der erste sichere Mikroprozessor **120** enthält den Geheime-Laufende-Nummern-Speicher **122**, den Entschlüssler **124** und den Mehrdienstschlüssel-Speicher **126**, die im Wesentlichen die gleichen Funktionen wie bei dem sicheren Mikroprozessor **120** des Verschlüsselungssteuersystems **110** (Fig. 6) ausführen. Der sichere Mikroprozessor **120** des Verschlüsselungssteuersystems **140** (Fig. 7) enthält außerdem einen Entschlüssler **142** zum Verarbeiten der Inlands-Berechtigungssteuernachricht unter Verwendung des Multisession-Schlüssels, um die Seed-Daten und die Dienstautorisierungsdaten zu regenerieren.

[0039] Der zweite sichere Mikroprozessor **130** des Verschlüsselungssteuersystems **140** (Fig. 7) enthält den Geheime-Laufende-Nummern-Speicher **122**, den Entschlüssler **124**, den Multisession-Schlüssel-Speicher **126** und einen Verschlüssler **144**. Der Speicher **122**, der Entschlüssler **124** und der Speicher **126** führen im Wesentlichen die gleiche Funktion zur Regenerierung des Multisession-Schlüssels wie in dem Speicher **122**, dem Entschlüssler **124** und dem Speicher **126** des sicheren Mikroprozessors **120** des Verschlüsselungssteuersystems **110** (Fig. 6) aus. Der Verschlüssler **144** verarbeitet die Seed- und Dienstautorisierungsdaten unter Verwendung des aus dem Speicher **126** abgerufenen Multisession-Schlüssels, um lokale Berechtigungssteuernachrichten bereitzustellen. Der Multiplexer **144** reformatiert einen lokalen Transportdatenstrom aus dem Inlands-Transportdatenstrom mit der Inlands-Berechtigungssteuernachricht, die durch die lokale Berechtigungssteuernachricht ersetzt wird.

[0040] Kabelkopfstellenbetreiber, die mit dem Verschlüsselungssteuersystem **140** ausgerüstet sind, können an ihre Teilnehmer Decodierer liefern, die einen speziellen (d. h. eindeutigen) Entschlüsselungsalgorithmus zum Entschlüsseln des Seeds unter Verwendung des Multisession-Schlüssels haben. Der Verschlüssler **144** des Verschlüsselungssteuersystems **140** verschlüsselt den Seed unter Verwendung eines Verschlüsselungsalgorithmus, der dem in den Decodierern bereitgestellten Seed-Entschlüsselungsalgorithmus entspricht. Auf diese Weise können die so bereitgestellten Decodierer nur Seeds empfangen, wenn sie mit der Einrichtung des speziellen Kabelkopfstellenbetreibers verbunden sind. Da die lokale Berechtigungssteuernachricht an alle Decodierer in dem System des Kabelkopfstellenbetreibers gesendet wird, ist es nicht möglich, einzelne Decodierer abzuschalten. Aber der Kabelkopfstellenbetreiber kann die in dem Entschlüssler **142** entschlüsselten Dienstautorisierungsdaten ändern, bevor sie in dem Verschlüssler **144** neu verschlüsselt werden, um einen stärker beschränkten Dienst für seine Teilnehmer bereitzustellen (d. h., ihnen einen Dienst zu niedrigeren Kosten anzubieten).

[0041] Wie vorstehend unter Bezugnahme auf Fig. 6 dargelegt, können umprogrammierbare Deco-

dierer für die Teilnehmer des lokalen Kabelkopfstellenbetreibers unter der Bedingung bereitgestellt werden, dass die Inlandszentrale bestimmte spezielle Umprogrammierungsdienste für den lokalen Kabelkopfstellenbetreiber bereitstellt. Vorzugsweise stellt die Inlandszentrale diese Umprogrammierungsdienste bereit, da sie die Berechtigungsverwaltungsnachrichten erstellt, die an jeden einzelnen Teilnehmer adressiert werden. Alternativ könnte der lokale Kabelkopfstellenbetreiber diese Dienste bereitstellen, wenn er die benötigten geheimen laufenden Nummern der Decodierer und die Entschlüsselungsalgorithmen der Decodierer erhält. Mit den von der Inlandszentrale bereitgestellten Diensten soll (im Gegensatz zur Regenerierung des Multisession-Schlüssels) der Entschlüsselungsalgorithmus, der zum Entschlüsseln der Seed-Daten verwendet wird, umprogrammiert werden. Auf diese Weise verschlüsselt der lokale Kabelkopfstellenbetreiber die Seed-Daten in dem Verschlüssler **144** mit einem Verschlüsselungsalgorithmus, der mit dem umprogrammierten Decodierer seines Teilnehmers kompatibel ist. Dadurch entsteht ein großer Markt für den umprogrammierbaren Decodierer, und dabei wird der Nutzen der Mitnahme des umprogrammierbaren Decodierers zu einem anderen Kabelnetzwerk vereitelt. Auf diese Weise ist es weniger wahrscheinlich, dass diejenigen Kabelkopfstellenbetreiber, die diese umprogrammierbaren Codierer bereitstellen, ihre Investition verlieren.

[0042] Die Inlandszentrale kann auch adressierte Berechtigungsverwaltungsnachrichten für die einzelnen Teilnehmer des lokalen Kabelkopfstellenbetreibers mit einem eindeutigen Multisession-Schlüssel versehen und kann diesen Multisession-Schlüssel in einer Berechtigungsverwaltungsnachricht bereitstellen, die an den zweiten sicheren Mikroprozessor **130** des Verschlüsselungssteuersystems **140** (Fig. 7) adressiert ist, sodass die Seed- und Dienstautorisierungsdaten mit diesem speziellen Multisession-Schlüssel verschlüsselt werden. Das heißt, der in dem ersten sicheren Mikroprozessor **120** verwendete Multisession-Schlüssel ist von dem Multisession-Schlüssel verschieden, der in dem zweiten sicheren Mikroprozessor **130** des Verschlüsselungssteuersystems **140** (Fig. 7) verwendet wird. Dieser Prozess zum Liefern des speziellen Multisession-Schlüssels kann durch Vereinbarung zwischen der Inlandszentrale und dem lokalen Kabelkopfstellenbetreiber geregelt werden. In dem Decodierer **70** (Fig. 5) wird der globale Seed **94** fehlerfrei regeneriert. Die verschlüsselten Dienst-Seeds **98** (Fig. 5) sind jedoch mit einem Multisession-Schlüssel verschlüsselt, der an alle Teilnehmer der Inlandszentrale gesendet wird. Dieser entspricht dem Multisession-Schlüssel, der in dem Speicher **126** des sicheren Mikroprozessors **120** des Verschlüsselungssteuersystems **140** (Fig. 7) gespeichert ist. Leider ist es der spezielle Multisession-Schlüssel, der in dem Speicher **126** des zweiten sicheren Mikroprozessors **130** gespeichert ist, der durch spezielle Vereinbarung zwischen der Inlandszentrale und dem lokalen Kopfstellenbetreiber in der Inlands-Berechtigungsverwaltungsnachricht übertragen wird, die an die Decodierer der Teilnehmer des lokalen Kopfstellenbetreibers adressiert ist. Dadurch können die Teilnehmer des lokalen Kopfstellenbetreibers nur den speziellen Multisession-Schlüssel regenerieren und können nicht die Dienst-Seeds **102** (Fig. 5) regenerieren. Diese Vereinbarung kann jedoch nützlich sein, wenn einzelne Dienste unverschlüsselt gesendet werden, wobei der Dienstdaten-Block global verschlüsselt wird.

[0043] In Fig. 8 enthält ein Verschlüsselungssystem **150** den Demultiplexer **112**, den Multiplexer **114**, den ersten sicheren Mikroprozessor **120**, den zweiten sicheren Mikroprozessor **130**, einen Seed-Generator **152**, einen globalen Dienstentschlüssler **154** und einen globalen Dienstverschlüssler **156**. In Fig. 8 wird der globale Seed **94** (Fig. 5) regeneriert und für den globalen Dienstentschlüssler **154** bereitgestellt. Die verschlüsselten Inlands-Dienstdaten werden in dem globalen Dienstentschlüssler **154** unter Verwendung des globalen Seeds **94** so verarbeitet, dass ein unverschlüsselten Dienstdaten-Rahmen regeneriert wird. Der unverschlüsselte Dienstdaten-Rahmen kann zwar einzelne verschlüsselte Dienste haben, aber der Dienstdaten-Rahmen ist unverschlüsselt. Der Seed-Generator **152** stellt gleichzeitig einen neuen Seed für den globalen Dienstverschlüssler **156** und den Seed-Verschlüssler **144** des zweiten sicheren Mikroprozessors **130** des Verschlüsselungssteuersystem **150** bereit.

[0044] Während des Betriebs regeneriert das Verschlüsselungssteuersystem **150** einen unverschlüsselten Dienstdaten-Rahmen von dem globalen Dienstentschlüssler **154** unter Verwendung des globalen Seeds **94**. Dann werden die unverschlüsselten Dienstdaten in dem Dienstverschlüssler **156** unter Verwendung des neuen Seeds neu verschlüsselt. Gleichzeitig wird der neue Seed für den Seed-Verschlüssler **144** bereitgestellt, wo er mit dem Multisession-Schlüssel verschlüsselt wird, der in dem Speicher **126** gespeichert ist und in der lokalen Berechtigungssteuernachricht enthalten ist. Der Multiplexer **114** kombiniert die lokale Berechtigungssteuernachricht mit der Inlands-Berechtigungsverwaltungsnachricht und den lokal neuverschlüsselten Dienstdaten zu einem lokalen Transportdatenstrom. Der Decodierer, beispielsweise der Decodierer **70** von Fig. 5, decodiert verschiedene Dienste, die mit dem neuen Seed verschlüsselt sind, in der gleichen Weise, in der er diese Dienste decodieren würde, wenn der Seed von der Inlandszentrale erzeugt wird. Der Decodierer kann den Unterschied nicht erkennen.

[0045] Ein eindeutiger Verschlüsselungsalgorithmus kann für (1) den globalen Dienstverschlüssler **156** oder (2) den Seed-Verschlüssler **144** oder (3) für

beide verwendet werden. Der eindeutige Verschlüsselungsalgorithmus entspricht dem jeweiligen Entschlüsselungsalgorithmus, der in dem Decodierer **70** (Fig. 5) enthalten ist, der für die Teilnehmer des lokalen Kabelkopfstellenbetreibers bereitgestellt wird. Auf diese Weise wird die Inlands-Berechtigungsverwaltungsnachricht zum Liefern des Multisession-Schlüssels an jeden Decodierer verwendet, unter anderem die Decodierer der Teilnehmer der Kabelkopfstellenbetreiber, die nicht mit dem Verschlüsselungssteuersystem **150** ausgerüstet sind. Decodierer mit Entschlüsselungsalgorithmen, die den Verschlüsselungsalgorithmen entsprechen, die in dem Seed-Verschlüssler **144** und dem globalen Dienstverschlüssler **156** verwendet werden, können jedoch nicht in anderen Kabelsystemen verwendet werden. Und wenn die betreffenden Decodierer durch Vereinbarung zwischen der Inlandszentrale und dem lokalen Kopfstellenbetreiber umprogrammierbar sind, kann die Inlandszentrale in den Decodierern die Entschlüsselungsalgorithmen umprogrammieren, die den Verschlüsselungsalgorithmen entsprechen, die in dem Seed-Verschlüssler **144** und dem globalen Dienstverschlüssler **156** verwendet werden.

[0046] In Fig. 9 umfasst ein Informationsverteilungssystem **160** eine Inlandszentrale **162**, einen Satelliten-Repeater **164**, eine erste Nutzerstation **170** und eine zweite Nutzerstation **180**. Die erste Nutzerstation **170** enthält einen Empfänger **172**, einen Kabelkopfstellenmodulator **174** und mindestens ein digitales Set-Top-Endgerät **176**. Die Nutzerstation **180** enthält einen Empfänger **172**, ein lokales Verschlüsselungssteuersystem **182**, einen Kabelkopfstellenmodulator **174** und ein modernes digitales Set-Top-Endgerät **184**.

[0047] Das Verschlüsselungssteuersystem **182** kann eines der Verschlüsselungssteuersysteme **110**, **140** und **150** sein. Bei einer Variante des Verschlüsselungssystems **110** umfasst ein Multisession-Schlüssel-Verschlüssler **134** eine Zweistufen-Verschlüsselung, bei der eine erste geheime laufende Nummer den Multisession-Schlüssel zu einem einfach verschlüsselten Schlüssel verschlüsselt und dann der einfach verschlüsselte Schlüssel über einen weiteren Verschlüssler unter Verwendung einer zweiten geheimen laufenden Nummer zu einem zweifach verschlüsselten Schlüssel verarbeitet wird. Der zweifache verschlüsselte Schlüssel wird in die lokale Berechtigungsverwaltungsnachricht eingestellt und in dem lokalen Transportdatenstrom (Fig. 6) übertragen. Der lokale Transportdatenstrom wird in dem Kabelkopfstellenmodulator **174** moduliert und wird an das moderne digitale Set-Top-Endgerät **184** gesendet. Das moderne digitale Set-Top-Endgerät **184** ist beispielsweise ein Set-Top-Endgerät mit einem feststehenden Sicherheitselement, das eine Einheit mit dem Decodierer bildet, und einem austauschbaren Sicherheitsmodul (d. h. SmartCard), das in den Decodierer eingesteckt werden kann (siehe beispielsweise das US-Patent Nr. 5.029.207). Das moderne digitale Set-Top-Endgerät **184** enthält zwei Entschlüssler zum Regenerieren des zweifach verschlüsselten Multisession-Schlüssels. Ein Entschlüssler ist in dem feststehenden Sicherheitselement des Set-Top-Endgeräts selbst enthalten (d. h. dem Decodierer), und der andere Entschlüssler ist in dem herausnehmbaren Sicherheitsmodul (d. h. der SmartCard) enthalten.

[0048] In der Praxis kann ein Kabelsystembetreiber, der die gleiche Ausrüstung wie die erste Nutzerstation **170** hat, nur den Inlands-Transportdatenstrom an die lokalen Teilnehmer senden. Ein solcher Betreiber kann seine Ausrüstung dadurch aufrüsten, dass er das Verschlüsselungssteuersystem **182** zusätzlich verwendet und/oder ein entsprechendes austauschbares Sicherheitsmodul (d. h. SmartCard) an seine Teilnehmer verschickt. Es ist nicht erforderlich, alle vorhandenen Set-Top-Endgeräte auszutauschen.

[0049] Fachleute dürften erkennen, dass die in Zusammenhang mit den Fig. 6–Fig. 9 beschriebenen Verfahren gemischt und kombiniert werden können, um jeden gewünschten Grad der Kontrolle zu erreichen. Mit entsprechenden gemischten Verfahren kann der lokale Kabelkopfstellenbetreiber Teilnehmer abschalten, die ihre Rechnungen nicht pünktlich bezahlt haben, und kann durch Modifizieren der Bedingter-Zugriffs-Daten kostengünstige Dienstangebote für die Teilnehmer bereitstellen.

[0050] Nachdem bevorzugte Ausführungsformen einer neuartigen Vorrichtung und eines neuartigen Verfahrens zur lokalen Verschlüsselung eines globalen Transportdatenstroms beschrieben worden sind (die erläuternd und nicht beschränkend sein sollen), sei darauf hingewiesen, dass Modifikationen und Abwandlungen von Fachleuten unter Berücksichtigung der vorstehenden Grundsätze vorgenommen werden können. Es ist daher klar, dass Änderungen in den speziellen Ausführungsformen der beschriebenen Erfindung vorgenommen werden können, die innerhalb des Schutzumfangs der von den beigefügten Ansprüchen definierten Erfindung liegen.

Patentansprüche

1. Verschlüsselungssteuersystem (**110**) zum Verarbeiten eines Eingangs-Transportdatenstroms zu einem Ausgangs-Transportdatenstrom, wobei der Eingangs-Transportdatenstrom erste Berechtigungsverwaltungs-Nachrichtendaten enthält, mit:
einem Eingangsdemultiplexer (**112**) zum Extrahieren der ersten Berechtigungsverwaltungs-Nachrichtendaten aus dem Eingangs-Transportdatenstrom, wobei die ersten Berechtigungsverwaltungs-Nachrichtendaten einen verschlüsselten Multisession-Schlüssel enthalten;

einem ersten sicheren Mikroprozessor (**120**) zum Verarbeiten der ersten Berechtigungsverwaltungs-Nachrichtendaten zum Wiederherstellen des Multisession-Schlüssels durch Entschlüsseln des verschlüsselten Multisession-Schlüssels unter Verwendung eines ersten Algorithmus;
einem zweiten sicheren Mikroprozessor (**130**) und
einem Ausgangsmultiplexer (**114**) zum Bereitstellen von zweiten Berechtigungsverwaltungs-Nachrichtendaten, die die ersten Berechtigungsverwaltungs-Nachrichtendaten ersetzen, für den Ausgangs-Transportdatenstrom aufgrund des Eingangs-Transportdatenstroms,
dadurch gekennzeichnet, dass die zweiten Berechtigungsverwaltungs-Nachrichtendaten von dem zweiten sicheren Mikroprozessor (**130**) erhalten werden, der so gestaltet ist, dass er den Multisession-Schlüssel unter Verwendung eines zweiten Algorithmus erneut verschlüsselt und die zweiten Berechtigungsverwaltungs-Nachrichtendaten aufgrund der ersten Berechtigungsverwaltungs-Nachrichtendaten mit dem erneut verschlüsselten Multisession-Schlüssel formatiert, der den verschlüsselten Multisession-Schlüssel ersetzt.

2. System nach Anspruch 1, das weiterhin einen ersten und einen zweiten Decodierer (**176**, **184**) aufweist, dadurch gekennzeichnet, dass
der erste Decodierer (**174**) eine erste Schaltungsanordnung aufweist, die den Multisession-Schlüssel aus den ersten Berechtigungsverwaltungs-Nachrichtendaten wiederherstellen kann, wobei die erste Schaltungsanordnung den Multisession-Schlüssel nicht aus den zweiten Berechtigungsverwaltungs-Nachrichtendaten wiederherstellen kann, und
der zweite Decodierer (**184**) eine zweite Schaltungsanordnung aufweist, die den Multisession-Schlüssel aus den zweiten Berechtigungsverwaltungs-Nachrichtendaten wiederherstellen kann, wobei die zweite Schaltungsanordnung den Multisession-Schlüssel nicht aus den ersten Berechtigungsverwaltungs-Nachrichtendaten wiederherstellen kann.

3. Verschlüsselungssteuersystem (**110**) zum Verarbeiten eines Eingangs-Transportdatenstroms zu einem Ausgangs-Transportdatenstrom, wobei der Eingangs-Transportdatenstrom erste Berechtigungsverwaltungs-Nachrichtendaten enthält, mit:
einem Eingangsdemultiplexer (**112**) zum Extrahieren der ersten Berechtigungsverwaltungs-Nachrichtendaten aus dem Eingangs-Transportdatenstrom, wobei die ersten Berechtigungsverwaltungs-Nachrichtendaten einen verschlüsselten Multisession-Schlüssel enthalten;
einem ersten sicheren Mikroprozessor (**120**) zum Verarbeiten der ersten Berechtigungsverwaltungs-Nachrichtendaten zum Wiederherstellen des verschlüsselten Multisession-Schlüssels durch Entschlüsseln des verschlüsselten Multisession-Schlüssels unter Verwendung einer ersten geheimen laufenden Nummer;
einem zweiten sicheren Mikroprozessor (**130**) und
einem Ausgangsmultiplexer (**114**) zum Bereitstellen von zweiten Berechtigungsverwaltungs-Nachrichtendaten, die die ersten Berechtigungsverwaltungs-Nachrichtendaten ersetzen, für den Ausgangs-Transportdatenstrom aufgrund des Eingangs-Transportdatenstroms,
dadurch gekennzeichnet, dass die zweiten Berechtigungsverwaltungs-Nachrichtendaten von dem zweiten sicheren Mikroprozessor (**130**) erhalten werden, der so gestaltet ist, dass er den Multisession-Schlüssel unter Verwendung einer zweiten geheimen laufenden Nummer erneut verschlüsselt und die zweiten Berechtigungsverwaltungs-Nachrichtendaten aufgrund der ersten Berechtigungsverwaltungs-Nachrichtendaten mit dem erneut verschlüsselten Multisession-Schlüssel formatiert, der den verschlüsselten Multisession-Schlüssel ersetzt.

Es folgen 10 Blatt Zeichnungen

Anhängende Zeichnungen

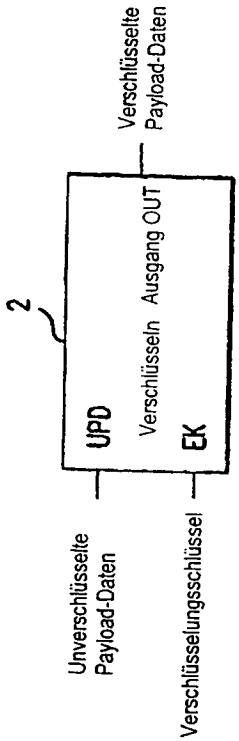

FIG. 1A
STAND DER TECHNIK

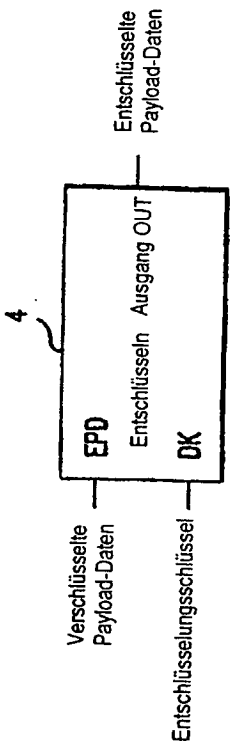

FIG. 1B
STAND DER TECHNIK

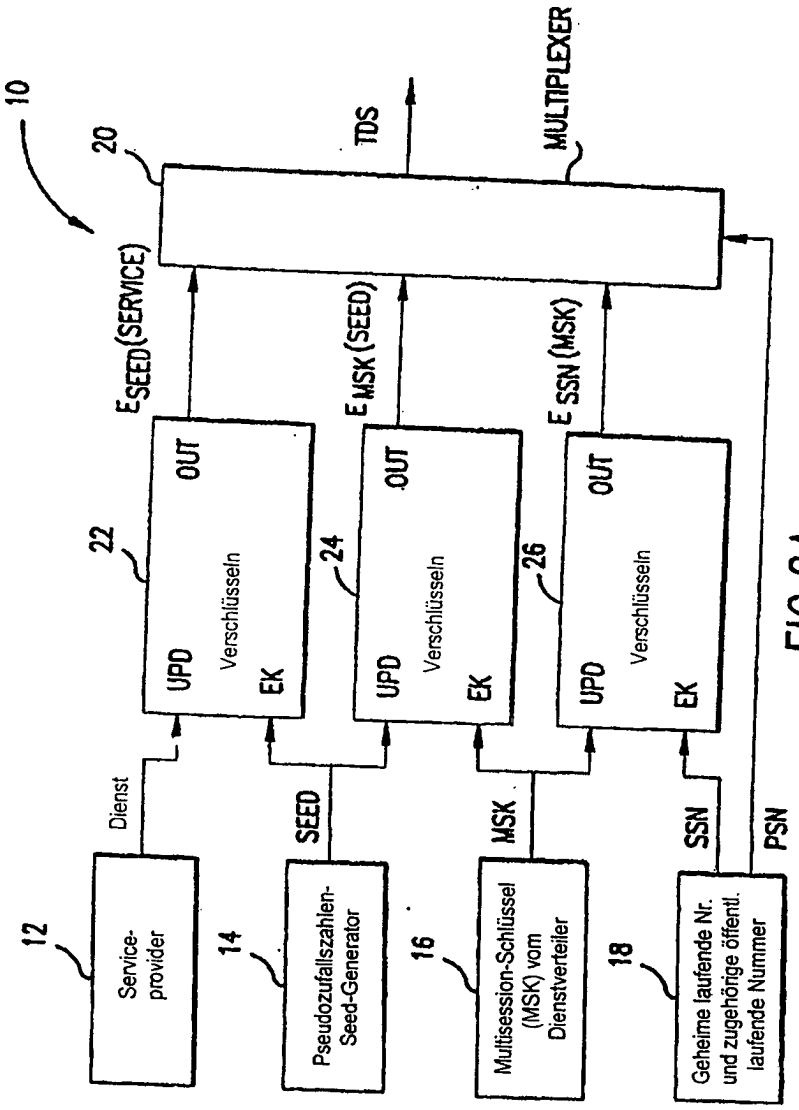

FIG.2A
STAND DER TECHNIK

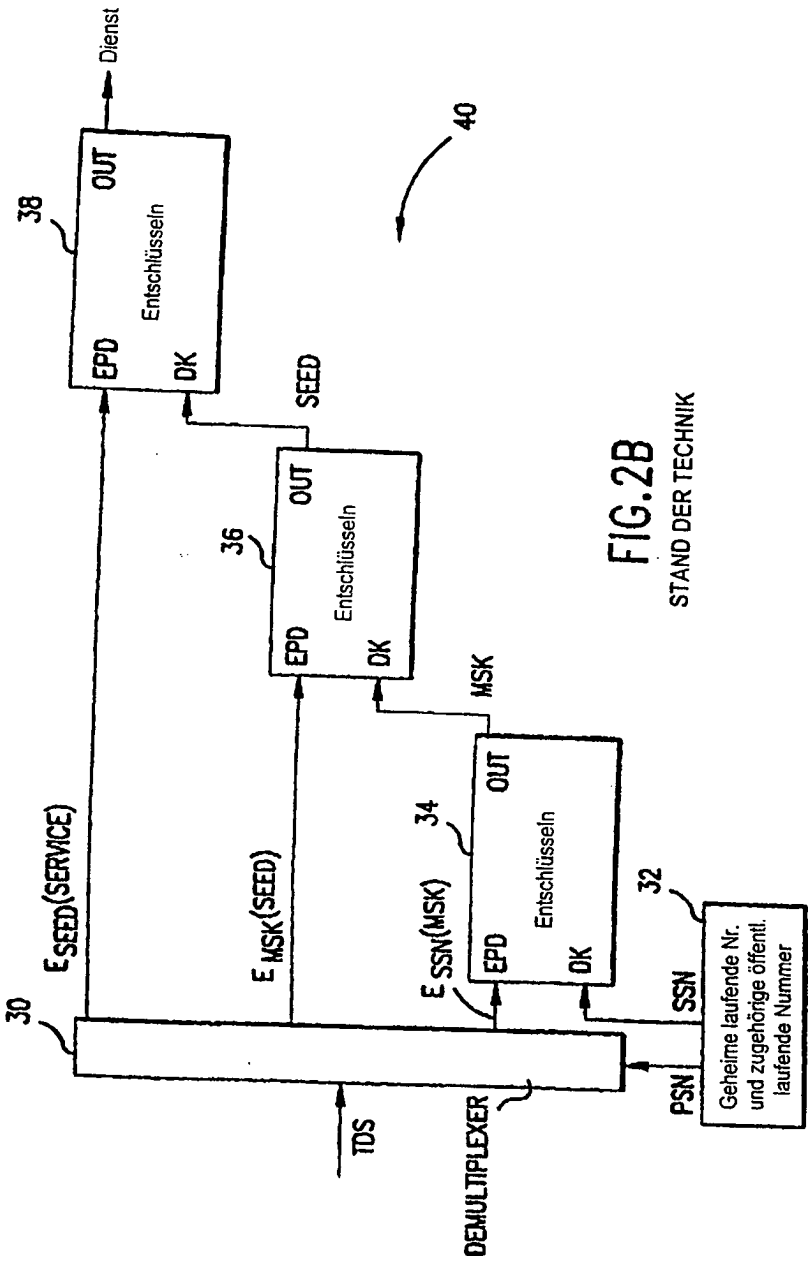

FIG.2B
STAND DER TECHNIK

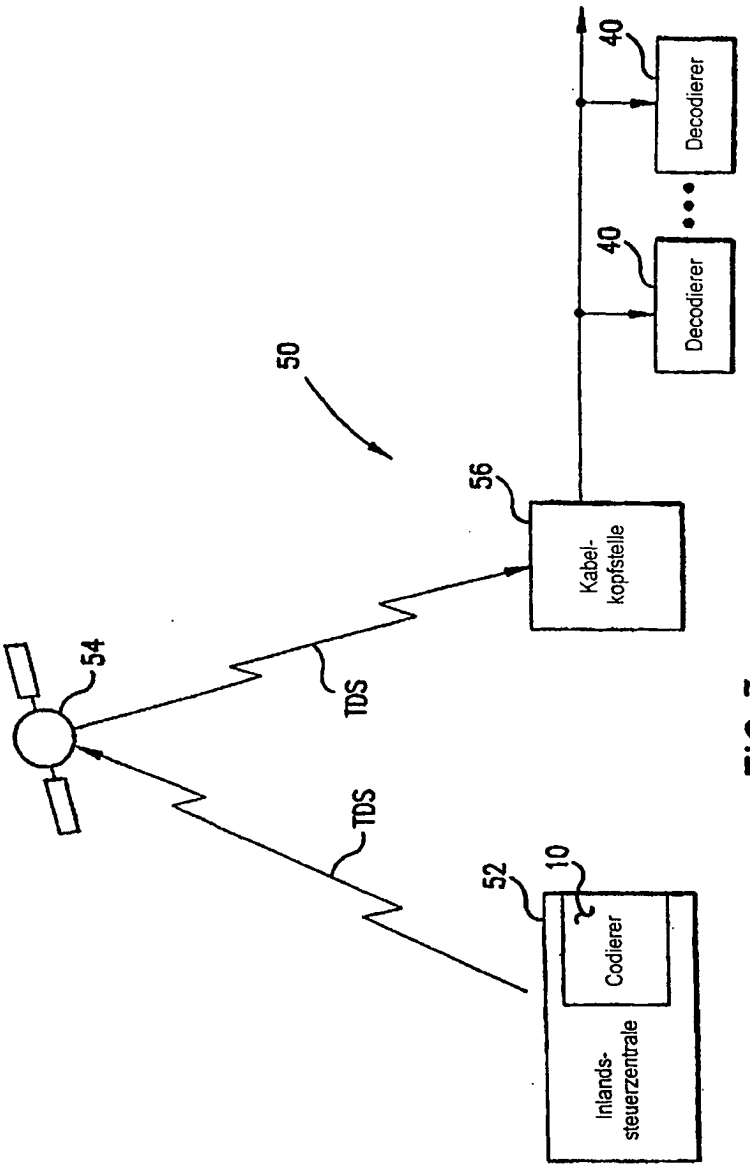

FIG.3
STAND DER TECHNIK

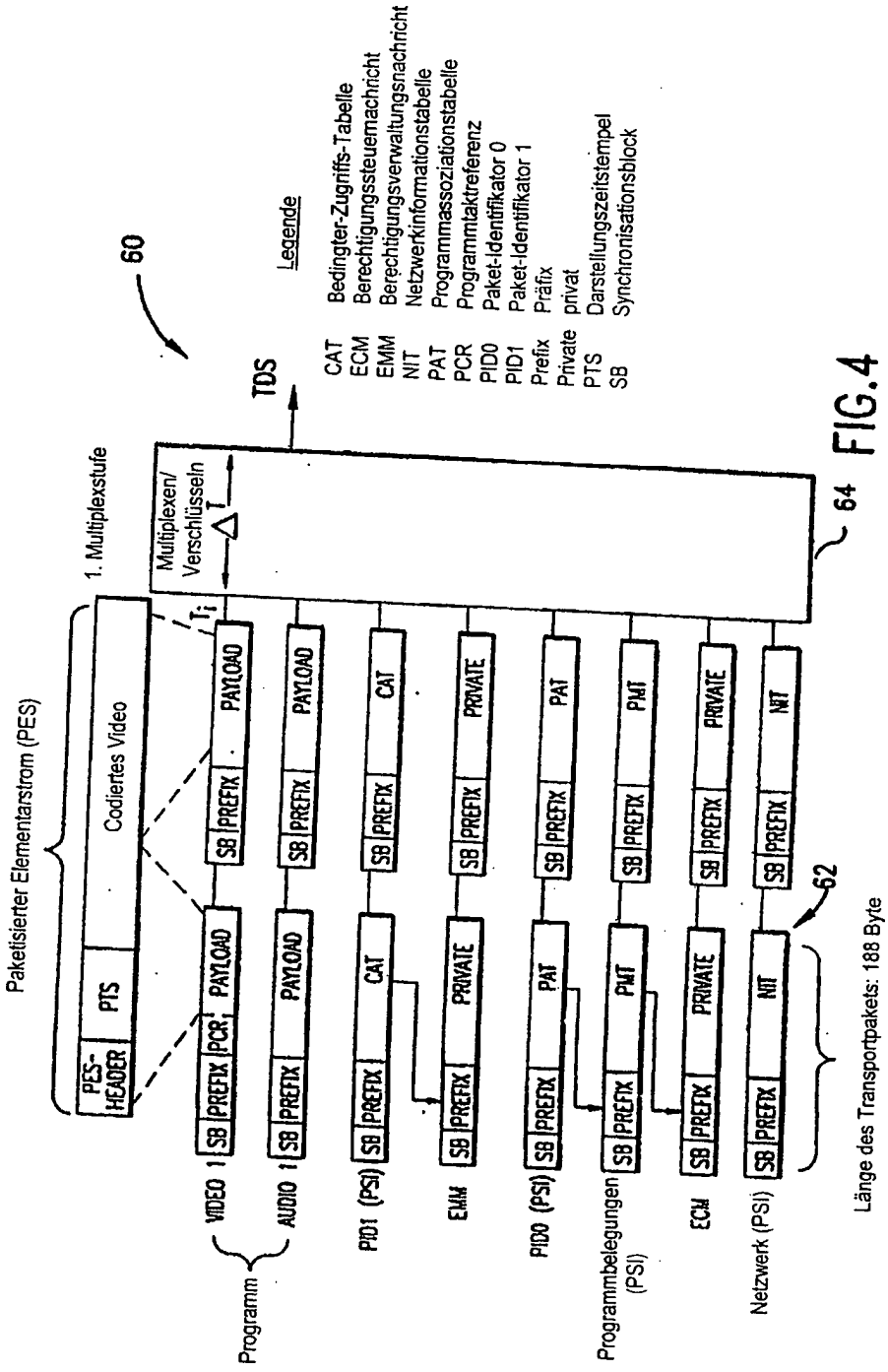
60
Legende
CAT Bedingter-Zugriffs-Tabelle
ECM Berechtigungssteuernachricht
EMM Berechtigungsverwaltungsnachricht
NIT Netzwerkinformationstabelle
PAT Programmassoziationstabelle
PCR Programmtaktreferenz
PID0 Paket-Identifikator 0
PID1 Paket-Identifikator 1
Prefix Präfix
Private privat
PTS Darstellungszeitstempel
SB Synchronisationsblock
TDS
1. Multiplexstufe
Multiplexen/ Verschlüsseln
Δ T
64
Paketisierter Elementarstrom (PES)
PES-HEADER
PTS
Codiertes Video
SB PREFIX PCR PAYLOAD
SB PREFIX PAYLOAD
SB PREFIX CAT
SB PREFIX PRIVATE
SB PREFIX PAT
SB PREFIX PMT
SB PREFIX PRIVATE
SB PREFIX NIT
VIDEO 1
AUDIO 1
Programm
PID1 (PSI)
EMM
PID0 (PSI)
Programmbelegungen (PSI)
ECM
Netzwerk (PSI)
62
Länge des Transportpakets: 188 Byte

FIG.4

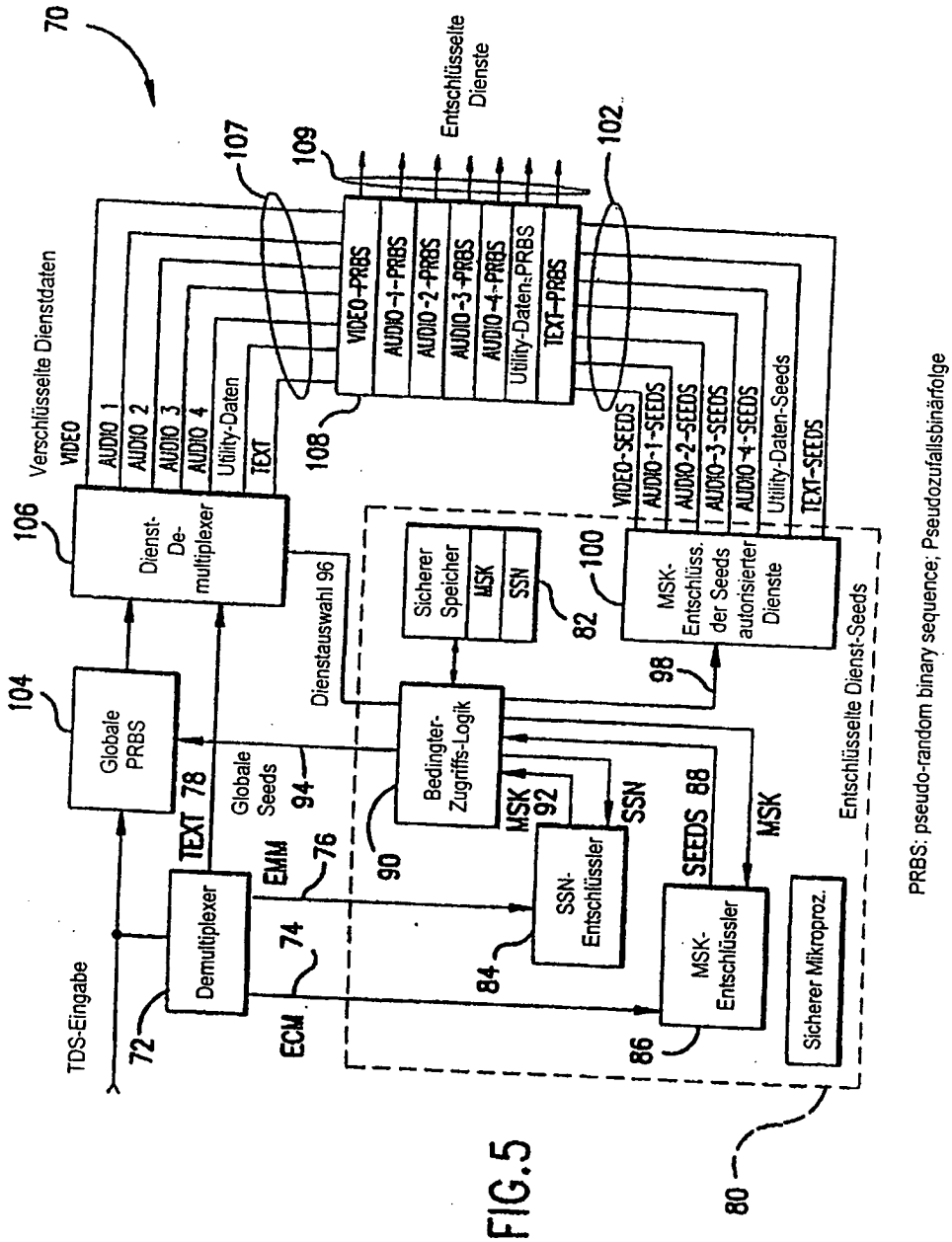
70
Verschlüsselte Dienstdaten
VIDEO
AUDIO 1
AUDIO 2
AUDIO 3
AUDIO 4
Utility-Daten
TEXT
106
Dienst-De-multiplexer
104
Globale PRBS
TDS-Eingabe
72
Demultiplexer
ECM
74
EMM
76
TEXT 78
Globale Seeds
94
Dienstauswahl 96
Bedingter-Zugriffs-Logik
90
MSK
92
SSN
SSN-Entschlüssler
84
SEEDS 88
MSK
MSK-Entschlüssler
86
Sicherer Mikroproz.
Sicherer Speicher
MSK
SSN
82
MSK-Entschlüss. der Seeds autorisierter Dienste
98
100
Entschlüsselte Dienst-Seeds
80
107
109
Entschlüsselte Dienste
VIDEO+PRBS
AUDIO-1+PRBS
AUDIO-2+PRBS
AUDIO-3+PRBS
AUDIO-4+PRBS
Utility-Daten+PRBS
TEXT+PRBS
108
102
VIDEO-SEEDS
AUDIO-1-SEEDS
AUDIO-2-SEEDS
AUDIO-3-SEEDS
AUDIO-4-SEEDS
Utility-Daten-Seeds
TEXT-SEEDS
PRBS: pseudo-random binary sequence; Pseudozufallsbinärfolge

FIG.5

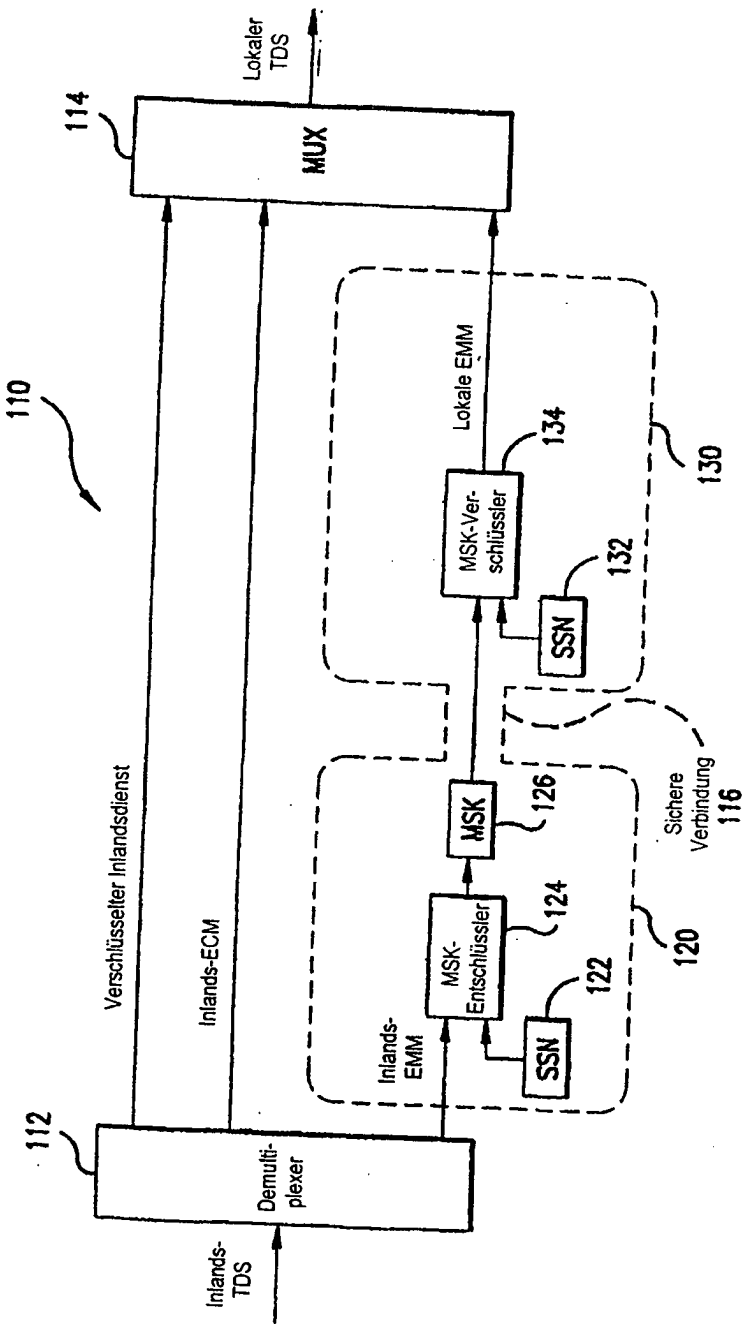
110
112
114
MUX
Demulti-plexer
Lokaler TDS
Inlands-TDS
Verschlüsselter Inlandsdienst
Inlands-ECM
Inlands-EMM
Lokale EMM
MSK-Ver-schlüssler
MSK-Entschlüssler
MSK
SSN
SSN
120
122
124
126
130
132
134
Sichere Verbindung
116

FIG.6

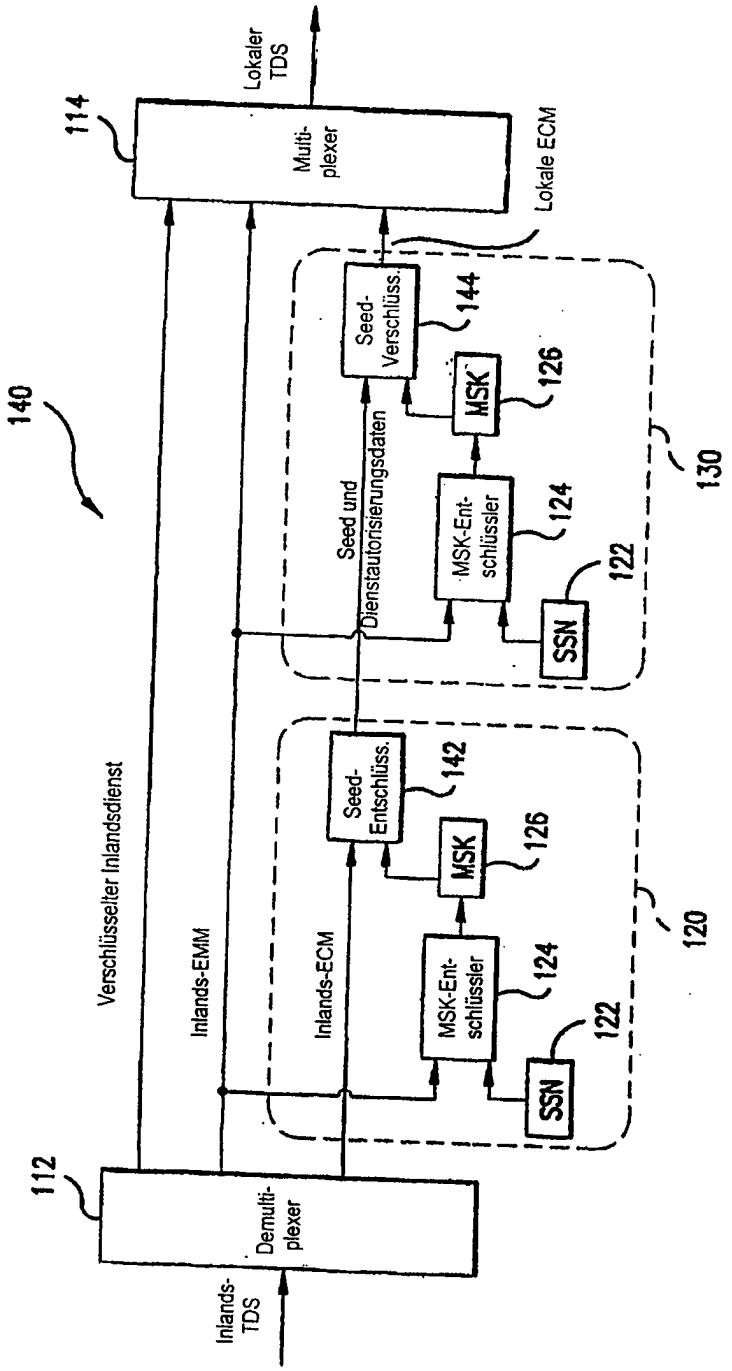
Inlands-TDS
Demulti-plexer
112
Inlands-ECM
Inlands-EMM
Verschlüsselter Inlandsdienst
Seed-Entschlüss.
142
MSK
126
MSK-Ent-schlüssler
124
SSN
122
120
Seed und Dienstautorisierungsdaten
Seed-Verschlüss.
144
MSK
126
MSK-Ent-schlüssler
124
SSN
122
130
140
Lokale ECM
Multi-plexer
114
Lokaler TDS

FIG.7

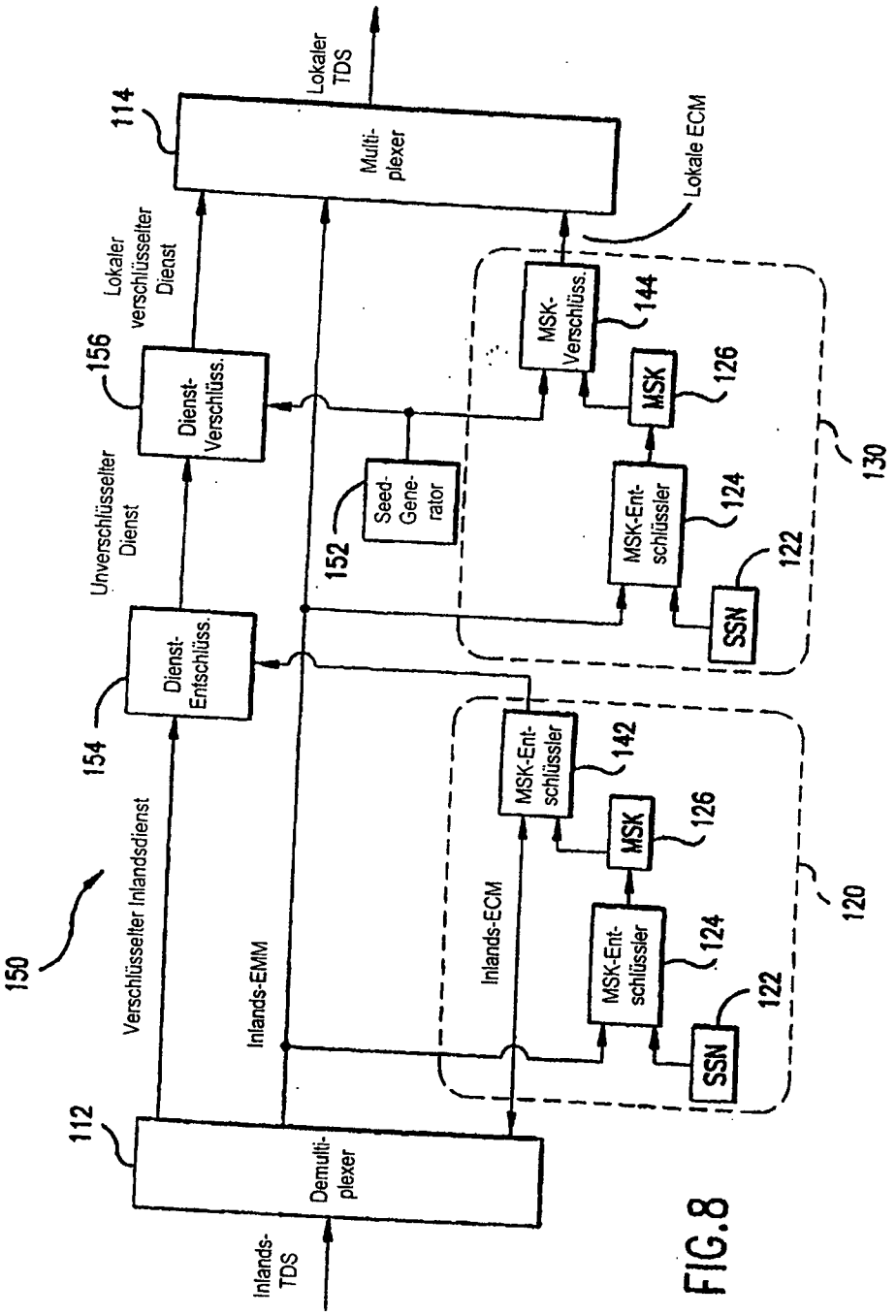
Lokaler TDS
Multi-plexer
114
Lokale ECM
Lokaler verschlüsselter Dienst
156
Dienst-Verschlüss.
MSK-Verschlüss.
144
MSK
126
Seed-Gene-rator
152
MSK-Ent-schlüssler
124
130
Unverschlüsselter Dienst
Dienst-Entschlüss.
154
SSN
122
MSK-Ent-schlüssler
142
MSK
126
MSK-Ent-schlüssler
124
SSN
122
120
150
Verschlüsselter Inlandsdienst
Inlands-EMM
Inlands-ECM
112
Demulti-plexer
Inlands-TDS

FIG.8

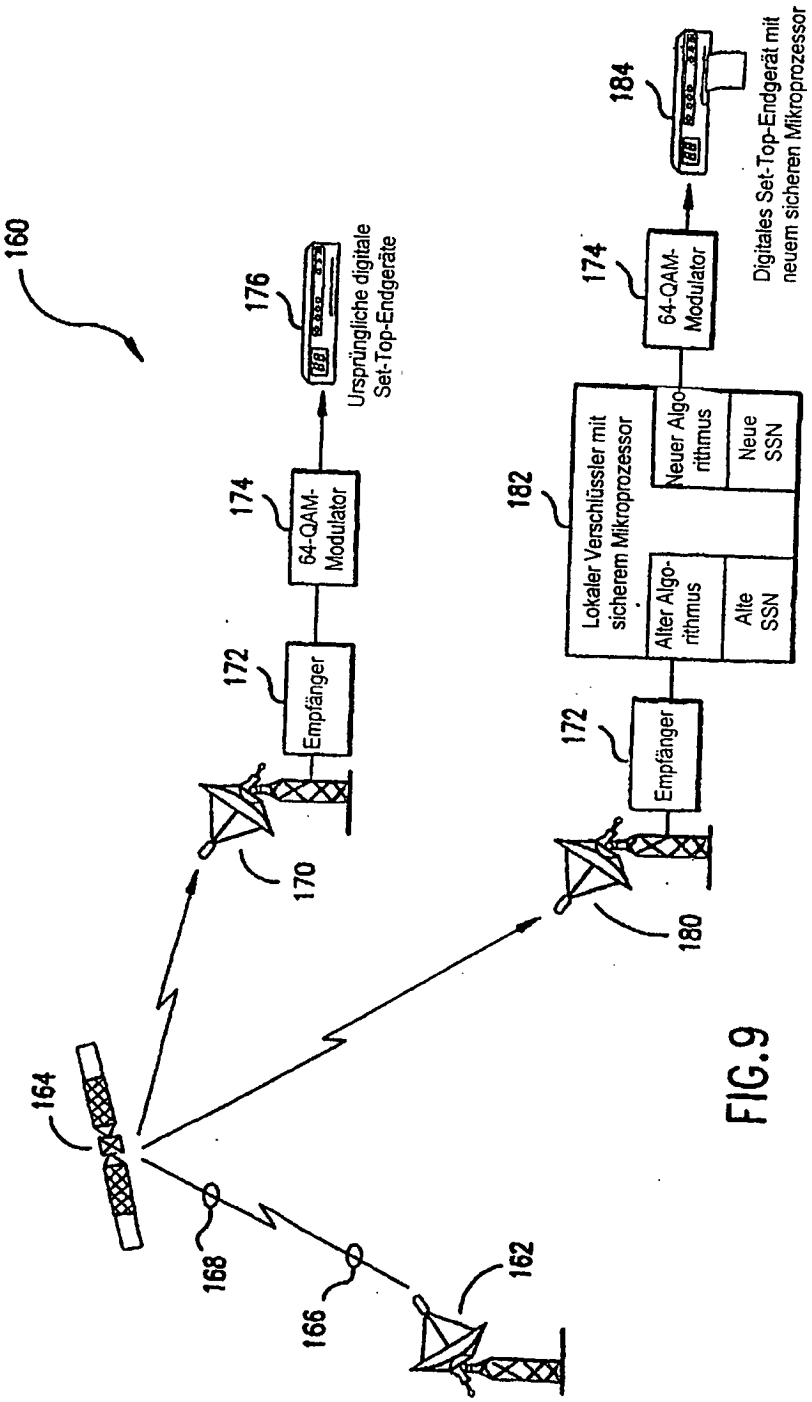
160
164
168
166
162
170
172
Empfänger
174
64-QAM-Modulator
176
Ursprüngliche digitale Set-Top-Endgeräte
180
182
Lokaler Verschlüssler mit sicherem Mikroprozessor
Alter Algo-rithmus
Alte SSN
Neuer Algo-rithmus
Neue SSN
184
Digitales Set-Top-Endgerät mit neuem sicheren Mikroprozessor

FIG.9