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

(10) **DE 696 32 243 T2** 2005.01.13

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 0 794 496 B1**
(21) Deutsches Aktenzeichen: **696 32 243.9**
(86) PCT-Aktenzeichen: **PCT/JP96/01675**
(96) Europäisches Aktenzeichen: **96 917 719.5**
(87) PCT-Veröffentlichungs-Nr.: **WO 97/002531**
(86) PCT-Anmeldetag: **18.06.1996**
(87) Veröffentlichungstag der PCT-Anmeldung: **23.01.1997**
(97) Erstveröffentlichung durch das EPA: **10.09.1997**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **21.04.2004**
(47) Veröffentlichungstag im Patentblatt: **13.01.2005**

(51) Int Cl.[7]: **G06F 12/14**
G06F 3/06, G11B 20/10

(30) Unionspriorität:

16669895	**30.06.1995**	**JP**
18796795	**30.06.1995**	**JP**

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

(73) Patentinhaber:
Sony Corp., Tokio/Tokyo, JP

(74) Vertreter:
Mitscherlich & Partner, Patent- und Rechtsanwälte, 80331 München

(72) Erfinder:
SAKO, Yoichiro, Tokyo 141, JP; KAWASHIMA, Isao, Tokyo 141, JP; KURIHARA, Akira, Tokyo 141, JP; OSAWA, Yoshitomo, Tokyo 141, JP; OWA, Hideo, Tokyo 141, JP

(54) Bezeichnung: **DATENAUFZEICHNUNGSVORRICHTUNG UND -VERFAHREN, DATENAUFZEICHNUNGSMEDIUM UND DATENWIEDERGABEVORRICHTUNG UND -VERFAHREN**

Beschreibung

[0001] Die vorliegende Erfindung bezieht sich auf ein Datenaufzeichnungsverfahren und Gerät, einen Datenaufzeichnungsträger und ein Datenwiedergabeverfahren und Wiedergabegerät, die anwendbar sind, das Kopieren oder eine nichtautorisierte Verwendung zu verhindern sowie auf ein Bezahlungssystem.

[0002] Mit einer ansteigenden Kapazität und mit der weiter ansteigenden Verwendung eines digitalen Aufzeichnungsträgers (Aufzeichnung beschreibbar oder aufgezeichnet) wird der Verhinderung des Kopierens oder des Verbietens einer nichtautorisierten Verwendung eine steigende Wichtigkeit beigemessen. Das heißt, da digitale Audiodaten oder digitale Videodaten vervielfältigt werden können, die keine Verschlechterung durch Kopieren erleiden, da Computerdaten leicht kopiert werden können, um die gleichen Daten wie die Ursprungsdaten zu erzeugen, wird nicht autorisiertes Kopieren häufig durchgeführt.

[0003] Um nichtautorisiertes Kopieren der Digitaldaten oder Videodaten zu vermeiden, ist ein Standard bekannt, beispielsweise ein sogenanntes serielles Kopierverwaltungssystem (SCMS) oder Kopiererzeugungs-Verwaltungssystem (CGMS). Da diese Systeme ein Kopierverhinderungsflag auf einem speziellen Bereich der Aufzeichnungsdaten setzen, besteht ein Problem dahingehend, dass Daten durch Speicherkopieren extrahiert werden können, was das Kopieren eines Zwei-Pegel-Digitalsignals in seiner Gesamtheit ist.

[0004] Es ist außerdem in der Praxis so, den Inhalt einer Datei selbst im Fall von Computerdaten zu verschlüsseln und lediglich die Verwendung durch reguläre registrierte Benutzer zu erlauben, wie beispielsweise im offengelegten japanischen Patent Nr. SHO-60- 116 030 offenbart ist. Dies ist verbunden mit einem System, bei dem ein digitaler Aufzeichnungsträger, auf welchem verschlüsselte Information aufgezeichnet ist, als Informationszirkulationsform verteilt wird und bei dem der Benutzer eine Gebühr für die Information, die er braucht, zahlt, um einen Schlüssel zu erwerben, um die Information zur Verwendung zu entschlüsseln. Für dieses System war in vereinfachtes nützliches Verfahren zum Verschlüsseln ein Wunschtraum.

[0005] Im Hinblick auf den oben angegebenen Stand der Technik ist es eine Aufgabe der vorliegenden Erfindung, ein Datenaufzeichnungsverfahren und Gerät bereitzustellen, einen Datenaufzeichnungsträger und ein Datenwiedergabeverfahren und Gerät, mit denen das Verschlüsseln durch eine vereinfachte Struktur realisiert werden kann, das Kopieren verhindert werden kann oder eine nichtautorisierte Verwendung durch eine vereinfachte Konfiguration erreicht werden kann, das Entschlüsseln schwierig gemacht werden kann und eine relative Fähigkeit oder eine Verschlüsselungstiefe leicht gesteuert werden kann.

[0006] Die EP-A 0 533 204 offenbart ein Aufzeichnungs-/Wiedergabegerät, welches eine Fehlerkorrekturcodier-Decodierschaltung und erste und zweite Datenumsetzungsschaltungen aufweist. Die erste Datenumsetzungsschaltung ist so eingerichtet, um die Daten, die auf einem Aufzeichnungsträger aufgezeichnet werden sollen, zu drehen, zu ersetzen und bezüglich von Bits umzukehren. Die zweite Datenumsetzungsschaltung ist so eingerichtet, eine entsprechende Drehung, einen Ersatz und eine Umkehr für die Daten einzuführen, welche vom Träger reproduziert werden, um die Ursprungsdaten wiederherzustellen.

[0007] Verschiedene Merkmale und Gesichtspunkte der vorliegenden Erfindung sind in den beigefügten Patentansprüchen definiert.

[0008] Ausführungsformen der vorliegenden Erfindung können ein Aufzeichnungsverfahren bereitstellen, bei dem ein Eingangssignal in zumindest einem eines Sektorbildungsschritts zum Unterteilen von Digitaldaten hinsichtlich eines vorher festgelegten Datenvolumens als Einheit, einem Datenkopf-Anhängungsschritt, einem Fehlerkorrekturcode- und Decodierschritt, einem Modulationsschritt zum Ausüben der Modulation gemäß einem vorher festgelegten Modulationssystem, oder einem Synchronisationsanhängungsschritt zum Anhängen eines Synchronisationsmusters verschlüsselt wird. Ein Verschlüsselungsschritt zum Ausüben von zufallsbedingter Anordnung zum Beseitigen des gleichen Musters kann unter den Schritten enthalten sein, welche zum Verschlüsseln verwendet werden können.

[0009] Dieses Datenaufzeichnungsverfahren kann bei einem Datenaufzeichnungsgerät angewandt werden.

[0010] Ausführungsformen der vorliegenden Erfindung umfassen ein Datenwiedergabeverfahren, wobei das Verfahren die Wiedergabe eines Datenaufzeichnungsträgers umfasst, der im obigen Datenaufzeichnungsverfahren beschrieben wurde, bei dem ein Eingangssignal in einem Aufzeichnungsschritt entsprechend zumindest einem von einem Synchronisationstrennungsschritt, einem Demodulationsschritt, einem Fehlerkorrektur- und Decodierschritt, einem Sektorauflösungsschritt und einem Datenkopftrennungsschritt verschlüsselt wurde, und bei dem das Eingangssignal in einem Wiedergabeschritt entsprechend dem Aufzeichnungsschritt, der beim Verschlüsseln verwendet wurde, decodiert wird. Ein Entschlüsselungsschritt zum Entschlüsseln zum Verschlüsseln, der für das Aufzeichnen verwendet wur-

de, kann unter den Schritten enthalten sein, welche zum Verschlüsseln verwendet wurden.

[0011] Das Datenwiedergabeverfahren kann bei einem Datenwiedergabegerät angewandt werden.

[0012] Mit dem Datenaufzeichnungsverfahren gemäß den Ausführungsformen der vorliegenden Erfindung wird die obige Aufgabe durch Verschlüsseln der Daten erreicht, wobei eine vorher festgelegte Schlüsselinformation verwendet wird, und durch Verwenden der Information, welche in einem Bereich geschrieben ist, der von einem Datenaufzeichnungsbereich des Aufzeichnungsträgers verschieden ist, als zumindest einem Bereich der Schlüsselinformation zum Verschlüsseln. Dies kann bei dem Datenaufzeichnungsgerät und bei einem Datenaufzeichnungsträger angewandt werden.

[0013] Ausführungsformen der vorliegenden Erfindung können außerdem ein Datenwiedergabeverfahren bereitstellen, bei dem beim Wiedergeben des Digitalsignals, welches während dem Aufzeichnen verschlüsselt wurde, das Verschlüsseln unter Verwendung der Schlüsselinformation von zumindest einem Teil durchgeführt wird, bei dem die Information in einem Bereich geschrieben ist, der von einem Datenaufzeichnungsbereich des Aufzeichnungsträgers verschieden ist.

[0014] Dies kann bei einem Datenwiedergabegerät angewandt werden.

[0015] Das Datenaufzeichnungsverfahren gemäß den Ausführungsformen umfasst außerdem das Variieren von zumindest einem Anfangswert des Verschlüsselungsschritts oder das Erzeugen eines Polynoms in Abhängigkeit von der Schlüsselinformation zum Verschlüsseln.

[0016] Das Datenwiedergabeverfahren gemäß den Ausführungsformen der vorliegenden Erfindung umfasst außerdem das Entschlüsseln durch Variieren von zumindest einem Anfangswerts oder des Erzeugens eines Polynoms auf der Basis der Schlüsselinformation, die zum Aufzeichnen verwendet wurde.

[0017] Das Eingangsdigitalsignal ist in Sektoren hinsichtlich eines vorher festgelegten Datenvolumens als Einheit unterteilt, und die resultierenden Daten werden mit einer Datenkopfanhängung, einer Fehlerkorrektur und Codierung, einer Modulation durch ein vorher festgelegtes Modulationssystem und das Anhängen eines Synchronisationsmusters verarbeitet, um auf einem Aufzeichnungsträger eine Aufzeichnung zu bilden. Durch Verschlüsseln eines Eingangssignals in zumindest einem der obigen Schritte wird der besondere Schritt, bei dem das Verschlüsseln durchgeführt wurde, auch zu einem Schlüssel, um zu verschlüsseln, wodurch die Schwierigkeit beim Entschlüsseln gesteigert wird.

[0018] Zumindest ein Bereich der Schlüsselinformation zum Verschlüsseln ist in einem Bereich geschrieben, der vom Aufzeichnungsbereich auf dem Aufzeichnungsträger verschieden ist. Dieser Bereich der Schlüsselinformation wird im Wiedergabezeitpunkt ausgelesen und zum Entschlüsseln verwendet. Da die Schlüsselinformation nicht mit der Information im Datenaufzeichnungsbereich auf dem Aufzeichnungsträger abgeschlossen ist, wird die Schwierigkeit beim Entschlüsseln gesteigert.

[0019] Zumindest eines des Erzeugungspolynominals oder des Anfangswerts wird in Abhängigkeit vom Schlüssel zum Verschlüsseln im Zeitpunkt des Verschlüsselns variiert, der beim zufallsbedingten Anordnen beabsichtigt ist, um das gleiche Muster in einer Datenfolge zu beseitigen. Es kann jegliches konventionelles Verschlüsseln zum Verschlüsseln verwendet werden.

[0020] **Fig.** 1 ist ein schematisches Blockdiagramm, welches den Aufbau einer ersten Ausführungsform des Datenaufzeichnungsgeräts der vorliegenden Erfindung zeigt;

[0021] **Fig.** 2 ist ein Blockdiagramm, welches einen beispielhaften Aufbau zum Realisieren des Verschlüsselns von geradzahligen und ungeradzahligen Bytes in einer Sektorbildungsschaltung zeigt;

[0022] **Fig.** 3 das Verschlüsseln von geradzahligen und ungeradzahligen Bytes zeigt;

[0023] **Fig.** 4 ein Beispiel eines Verschlüsslers zeigt;

[0024] **Fig.** 5 ein Beispiel von vorher festgelegten Werten des Verschlüsslers zeigt;

[0025] **Fig.** 6 ein Beispiel eines Verschlüsslers zeigt, der variable Erzeugungspolynome hat;

[0026] **Fig.** 7 ein Beispiel eines Sektorformats zeigt;

[0027] **Fig.** 8 ein Beispiel des Verschlüsselns in einem Synchronisationsbereich in einem Sektor zeigt;

[0028] **Fig.** 9 ein Beispiel eines Datenkopfbereichs in einem Sektor zeigt;

[0029] **Fig.** 10 eine schematische Struktur einer Sektorkorrektur-Codierschaltung zeigt;

[0030] **Fig.** 11 einen speziellen Aufbau einer Fehlerkorrektur-Codierschaltung zeigt;

[0031] **Fig.** 12 ein weiteres Beispiel einer Fehlerkorrektur-Codierschaltung zeigt;

[0032] **Fig.** 13 ein Beispiel zum Verschlüsseln in einer Modulationsschaltung zeigt;

[0033] **Fig.** 14 ein spezielles Beispiel eines Synchronisationsworts zeigt, welches an ein Modulationssignal angehängt ist;

[0034] **Fig.** 15 ein Beispiel zum Verschlüsseln in einer Synchronisationsanhängungsschaltung zeigt;

[0035] **Fig.** 16 ein Beispiel eines Datenaufzeichnungsträgers zeigt;

[0036] **Fig.** 17 ein Blockdiagramm ist, welches eine schematische Struktur einer ersten Ausführungsform eines Datenwiedergabegeräts gemäß der vorliegenden Erfindung zeigt;

[0037] **Fig.** 18 ein Beispiel zum Entschlüsseln durch eine Demodulationsschaltung zeigt;

[0038] **Fig.** 19 eine schematische Struktur eines Beispiels einer Fehlerkorrektur-Decodierschaltung zeigt;

[0039] **Fig.** 20 eine spezielle Struktur eines Beispiels einer Fehlerkorrektur-Decodierschaltung zeigt;

[0040] **Fig.** 21 ein weiteres Beispiel einer Fehlerkorrektur-Decodierschaltung zeigt;

[0041] **Fig.** 22 ein Beispiel einer Entschlüsselungsschaltung zeigt;

[0042] **Fig.** 23 ein weiteres Beispiel eines Verschlüsslexs zeigt;

[0043] **Fig.** 24 ein Beispiel von vorher festgelegten Werten des Verschlüsslers von **Fig.** 23 zeigt;

[0044] **Fig.** 25 ein Beispiel eines Datenkopfbereichs in einem Sektor in einem Sektorformat von **Fig.** 25 zeigt;

[0045] **Fig.** 26 ein Beispiel eines Datenkopfbereichs in einem Sektor in einem Sektorformat von **Fig.** 25 zeigt;

[0046] **Fig.** 27 ein Blockdiagramm ist, welches ein weiteres Beispiel einer Fehlerkorrektur-Codierschaltung zeigt;

[0047] **Fig.** 28 einen Produktcode als spezielles Beispiel des Fehlerkorrekturcodes zeigt;

[0048] **Fig.** 29 ein Beispiel eines Sektorssignalformats zeigt;

[0049] **Fig.** 30 ein weiteres spezielles Beispiel eines Synchronisationsworts zeigt, welches an das Modulationssignal angehängt ist;

[0050] **Fig.** 31 ein weiteres Beispiel zum Verschlüsseln in einer Synchronisationsanhängungsschaltung zeigt; und

[0051] **Fig.** 32 ein Blockdiagramm ist, welches ein weiteres Beispiel einer Fehlerkorrektur-Decodierschaltung zeigt.

[0052] Mit Hilfe der Zeichnungen werden nun bevorzugte Ausführungsformen der Erfindung ausführlich erläutert.

[0053] **Fig.** 1 zeigt schematisch eine erste Ausführungsform der vorliegenden Erfindung.

[0054] Gemäß **Fig.** 1 werden Digitaldaten, beispielsweise Daten, die bei einer digitalen Umsetzung eines Analogsignals oder von Videosignalen oder Computerdaten erhalten werden, einem Eingangsanschluss **11** zugeführt. Die gelieferten Digitaldaten werden über eine Schnittstellenschaltung **12** zu einer Sektorbildungsschaltung **13** geliefert, wo sie in Sektoren in Form von einem vorher festgelegten Datenvolumen gebildet werden, beispielsweise 2048 Bytes als Einheit. Die Daten, die somit in Sektoren gebildet sind, werden zu einer Verschlüsselungsschaltung **14** zum Verschlüsseln geliefert. Zum Verschlüsseln werden die gelieferten Daten zufallsbedingt angeordnet, so dass das gleiche Bytemuster nicht aufeinanderfolgend erzeugt wird, d.h., so dass die gleichen Muster ausgeschieden werden, mittels der zufallsbedingten Anordnung, um zu ermöglichen, dass das Signal passend gelesen und aufgezeichnet wird. Die verschlüsselten oder zufallsbedingten angeordneten Daten werden zu einer Datenkopfanhängungsschaltung **15** geliefert, wo die Datenkopfdaten, welche am Anfang jedes Sektors ausgereiht werden, angehängt werden und die resultierenden Daten zu einer Fehlerkorrektur-Codierschaltung **16** geliefert werden. Die Fehlerkorrektur-Codierschaltung **16** verzögert die Daten und erzeugt eine Parität, um die erzeugte Parität anzuhängen. Die nächste Schaltung, d.h., eine Modulationsschaltung **17**, setzt die 8-Bit-Daten in 16 kanalbit-modulierte Daten gemäß einer vorher festgelegten Modulationsregel um und sendet die resultierenden modulierten Daten zu einer Synchronisationsanhängungsschaltung **18**. Die Synchronisationsanhängungsschaltung **18** hängt ein Synchronisationssignal, welches die Modulationsregel des oben festgelegten Modulationssystems verletzt, d.h., ein sogenanntes Außerregel-Muster-Synchronisationssignal, hinsichtlich eines vorher festgelegten Datenvolumens als Einheit an und sendet das resultierende Synchronisationssignal über eine Ansteuerschaltung, d.h., einen Treiber **19** zu einem Aufzeichnungskopf **20**. Der Aufzeichnungskopf **20** führt optische oder magneto-optische Aufzeichnungen durch und zeichnet das modulierte Signal auf dem Aufzeich-

nungsträger auf. Der plattenförmige Aufzeichnungsträger **21** wird durch einen Spindelmotor **22** drehbar angetrieben.

[0055] Die Verschlüsselungsschaltung **14** ist nicht wesentlich. Die Verschlüsselungsschaltung **14** kann stromabwärts der Datenkopfanhängungsschaltung **15** eingefügt werden, um die Digitaldaten, an denen der Datenkopf angehängt wurde, zu verschlüsseln. Die Digitaldaten, denen der Datenkopf angehängt wurde, können zur Fehlerkorrektur-Codierschaltung **16** geliefert werden.

[0056] Es sei angemerkt, das zumindest eine von der Sektorbildung **13**, der Verschlüsselungsschaltung **14**, der Datenkopf-Anhängungsschaltung **15**, der Fehlerkorrektur-Codierschaltung **16**, der Modulationsschaltung **17** und der Synchronisations-Anhängungsschaltung **18** zum Verschlüsseln eines Eingangssignals und zum Ausgeben des resultierenden verschlüsselten Signals konfiguriert ist. Vorzugsweise werden zwei oder mehrere Schaltungen zum Verschlüsseln verwendet. Die Verschlüsselungsinformation für diese Verschlüsselung verwendet als zumindest einen Bereich davon die Identifikationsinformation, welche in einem Bereich geschrieben ist, der von dem Datenaufzeichnungsbereich des Aufzeichnungsträgers **21** verschieden ist, beispielsweise die Identifikationsinformation, die dem Träger eigen ist, die Herstelleridentifikationsinformation, die Händleridentifikationsinformation, die Identifikationsinformation, die zum Aufzeichnungsgerät gehört oder zum Codierer, die Identifikationsinformation, die zum Trägerherstellergerät gehört, beispielsweise eine Schneidemaschine oder einen Stempel, die Gebietsinformation, beispielsweise ein Ländercode oder die Identifikationsinformation, die von außenher eingerichtet wird. Diese Identifikationsinformation, welche in dieser Art und Weise in einem Bereich mit Ausnahme des Datenaufzeichnungsbereichs des Aufzeichnungsträgers geschrieben ist, ist die Information, welche von der Schnittstellenschaltung **12** über eine Inhaltserzeugungsschaltung (TOC) **23** zu einem Anschluss **24** geliefert wird, und ist die Information, welche unmittelbar von der Schnittstellenschaltung **12** zu einem Anschluss **25** geliefert wird. Die Identifikationsinformation von diesen Anschlüssen **24**, **25** wird als ein Bereich der Schlüsselinformation zum Verschlüsseln verwendet. Zumindest eine oder vorzugsweise zwei oder mehrere der Schaltung **13** bis **18** führen das Verschlüsseln bezüglich der Eingangsdaten unter Verwendung der Schlüsselinformation durch. Die Identifikationsinformation von diesen Anschlüssen **24**, **25** wird wie geeignet zu dem Aufzeichnungskopf **20** zum Aufzeichnen auf einem Aufzeichnungsträger **21** geliefert.

[0057] In diesem Fall zeigt, welche der Schaltungen **13** bis **1b** das Verschlüsseln durchgeführt hat, dies eine der Alternativen, und man fühlt, dass dies ein Schlüssel ist, der notwendig ist, das regulär reproduzierte Signal bei der Reproduktion zu erzeugen. Das heißt, wenn das Verschlüsseln in einer der Schaltungen durchgeführt wurde, es notwendig wird, eine der sechs Alternativen auszuwählen, während, wenn das Verschlüsseln in zwei der Schaltungen ausgeführt wurde, es notwendig wird, eine der fünfzehn Alternativen entsprechend der Anzahl von Kombinationen von zwei aus den sechs Schaltungen auszuwählen. Wenn es die Möglichkeit eines Verschlüsselungsbetriebs gibt, der in der ersten bis sechsten von den sechs Schaltungen **13** bis **18** durchgeführt wird, wird die Anzahl von Alternativen weiter erhöht, so dass es schwierig wird, die Kombination durch ein Versuch-Fehler-Verfahren herauszufinden, wodurch die Aufgabe des Verschlüsselns erfüllt wird.

[0058] Die Schlüsselinformation zum Verschlüsseln kann in einem vorher festgelegten Zeitablauf umgeschaltet werden, beispielsweise auf Sektorbasis. Beim Umschalten der Schlüsselinformation im vorher festgelegten Zeitablauf kann, ob das Umschalten durchgeführt wird oder nicht, die Umschaltperiode oder die Umschaltsequenz der mehreren Schlüsselinformationsposten auch als Schlüssel verwendet werden, um den Verschlüsselungspegel, die Leichtigkeit oder Schwierigkeit des Verschlüsselns oder Schwierigkeiten beim Entschlüsseln weiter anzuheben.

[0059] Der Aufbau der Schaltungen **13** bis **18** und spezielle Beispiele zum Verschlüsseln werden anschließend erläutert.

[0060] Zunächst kann die Sektorbildungsschaltung **13** zum Verschachteln von geradzahligen und ungeradzahligen Bytes bestimmt werden, wie beispielsweise in **Fig.** 2 gezeigt ist. Das heißt, in **Fig.** 2 wird ein Ausgangssignal der Schnittstellenschaltung **12** von **Fig.** 1 zu einem Umschalter **31** für zwei Ausgangssignale geliefert, von dem ein Ausgangssignal über einen geradzahligen/ungeradzahligen Verschachteler **33** zu einer Sektorbildungsschaltung **34** geliefert wird und von dem das andere Ausgangssignal unmittelbar zur Sektorbildungsschaltung **34** geliefert wird. Die Sektorbildungsschaltung **34** sammelt die gelieferten Daten hinsichtlich von 2048 Bytes als Einheit, um einen Sektor zu bilden. Der Umschaltbetrieb des Umschalters **32** der Sektorbildungsschaltung **13** wird durch ein 1-Bit-Steuersignal gesteuert, welches als Schlüssel arbeitet. Der geradzahlige/ungeradzahlige Verschachteler **33** teilt einen Sektor der gelieferten Daten, der geradzahlige Bytes **36a** und ungeradzahlige Bytes **36f** aufweist, welche abwechselnd aufgereiht sind, wie in **Fig.** 3A gezeigt ist, in einen geradzahligen Datenbereich **37a** und einen ungeradzahligen Datenbereich **37b** auf, wie in **Fig.** 3 gezeigt ist, und gibt diese Datenbereiche aus. Insbesondere kann ein spezieller Bereich **39** in einem Sektor durch die Schlüsselinformation angegeben wer-

den, und Daten lediglich in diesem speziellen Bereich **39** können einen geradzahligen Datenbereich **39a** und einen ungeradzahligen Datenbereich **39b** verteilt werden. In diesem Fall kann die Art und Weise des Angebens des Bereichs **39** so festgelegt werden, dass diese in mehreren Verfahren ausgewählt wird, um weiter die Anzahl der Alternativen der Schlüsselinformation zu erhöhen, um den Verschlüsselungspegel anzuheben.

[0061] Die Verschlüsselungsschaltung **14** kann einem Verschlüssler der sogenannten parallelen Blocksynchronisationsart verwenden, bei dem ein 15-Bit-Schieberegister verwendet wird, wie beispielsweise in **Fig.** 4 gezeigt ist. Ein Dateneingangsanschluss **15** des Verschlüsslers wird mit Daten von der Sektorbildungsschaltung **13** beliefert in einer Reihenfolge, in welcher das niedrigstwertige Bit (LSB) vorübergehend zuerst kommt, d.h., in der sogenannten ersten LSB-Ordnung. Ein 15-Bit-Schieberegister **14a** zum Verschlüsseln ist mit einer exklusiven ODER-Schaltung (ExOR) **14b** verknüpft, um die Rückführung gemäß dem Erzeugungspolynom $x^{15} + x + 1$ anzuwenden. Somit wird ein vorher festgelegter Wert oder ein Anfangswert, wie in **Fig.** 5 gezeigt ist, im 15-Bit-Schieberegister **14a** festgelegt. Die Auswahlnummer des vorher festgelegten Werts von **Fig.** 5 kann auf Sektorbasis in Verbindung mit beispielsweise dem Wert der unteren vier Bits der Sektoradresse umgeschaltet werden. Ausgangsdaten des Schieberegisters **14a** und Eingangsdaten an einem Anschluss **35** werden durch die ExOR-Schaltung **14c** gemäß der ExOR-Schaltung verarbeitet, und werden an einem Anschluss **14d** herausgenommen und zu einer Datenkopfanhängungsschaltung **15** von **Fig.** 1 geliefert.

[0062] Das erzeugte Polynom und der vorher festgelegte Wert (Anfangswert) können gemäß der Schlüsselinformation variiert werden, beispielsweise der vorher festgelegten Identifikationsnummer. Das heißt, um das erzeugte Polynom zu verändern, kann der Aufbau, wie in **Fig.** 6 gezeigt, verwendet werden. In **Fig.** 6 werden Ausgangssignale der entsprechenden Bits des 15-Bit-Schieberegisters **14a** zu festen Anschlüssen des Umschalters **14f** geliefert, der beispielsweise durch 4-Bit-Steuerungsdaten von einem Steuerungsanschluss **14g** gesteuert wird. Ein Ausgangssignal des Umschalters **14f** wird zur ExOR-Schaltung **14b** geliefert. Durch Ändern der Steuerungsdaten des Steuerungsanschlusses **14g** wird es möglich, den Wert n im erzeugten Polynom $x^{15} + x^n + 1$ zu ändern. Um den vorher festgelegten Wert zu ändern, können vorher festgelegte Werte der vorher festgelegten Werttabelle von **Fig.** 5 mit einem Rechenbetrieb mit jedem Bytewert der 16-Byte-Identifikationsinformation verarbeitet werden. Die Identifikationsinformation kann durch die Identifikationsinformation, die zum Träger gehört, nummeriert werden, der Erzeugeridentifikationsinformation, der Händleridentifikationsinformation, der Identifikationsinformation, die zum Aufzeichnungsgerät gehört, oder des Codierers, der Identifikationsinformation, die zum Trägererzeugungsgerät gehört, der Landinformation oder der Identifikationsinformation, welche von außerhalb eingerichtet wird. Die obige Information kann in Kombination miteinander oder mit der anderen Information verwendet werden. Die Konfiguration zum Variieren des erzeugten Polynoms ist nicht auf die Konfiguration von **Fig.** 6 beschränkt, so dass die Anzahl der Anzapfungen oder Stufen des Schieberegisters wie gewünscht geändert werden kann.

[0063] Es wird nun die Datenkopfanhängungsschaltung **15** erläutert.

[0064] **Fig.** 7 zeigt ein spezielles Beispiel des Sektorformats. Jeder Sektor besteht aus einem 2048-Byte-Benutzerdatenbereich **41**, an den ein 4-Byte-Synchronisationsbereich **42**, ein 16-Byte-Datenkopfbereich **43** und ein 4-Byte-Fehlerermittlungscode (EDC) **44** angehängt ist. Der Fehlerermittlungscode des Fehlerermittlungscodebereichs **44** besteht aus einem 32-Bit-CRC-Code, der für den Benutzerdatenbereich **41** erzeugt wird, und dem Datenkopfbereich **43**. Das Verschlüsseln in der Datenkopfanhängungsschaltung **15** kann bezüglich eines Synchronisationssignals durchgeführt werden, d.h., sogenannter Datensynchronisation, einer Sektoradresse oder CRC.

[0065] Als Beispiel des Verschlüsselns des Sektorsynchronisationssignals oder der Datensynchronisation kann, wenn Bytemuster, welche entsprechenden Bytes des 4-Byte-Synchronisationsbereichs **42** zugeordnet sind, durch A, B, C und D in **Fig.** 8 bezeichnet sind, der Inhalt dieser vier Bytes auf der Bytebasis unter Verwendung der 2-Bit-Schlüsselinformation verschoben oder gedreht werden. Das heißt, durch Umschalten auf ABCD, BCDA, CDAB oder auf DABC für den 2-Bit-Schlüssel aus 0, 1, 2 oder 2 kann die Sektorsynchronisation nicht erhalten werden, wodurch die Schlüsseldatenübereinstimmung fehl läuft, so dass die reguläre Reproduktion nicht realisiert werden kann. Für die Bytemuster A bis D können beispielsweise Codes des I5O646 verwendet werden.

[0066] Im Datenkopfhereich **43** sind entsprechende Schichten für CRC **45**, beispielsweise ein sogenannter zyklischer Redundanzcode, die Kopierinformation **46** zum Kopieren der Erlaubnis/Nichterlaubnis, oder die Verwaltung der Kopiergeneration, eine Schicht **47** zum Anzeigen einer speziellen Schicht einer Mehrfachschichtplatte, eine Adresse **48** und eine Reserve **49**, wie in **Fig.** 9 gezeigt ist, gebildet. Das Verschlüsseln kann durch Bitverschlüsselung durchgeführt werden, hier durch Vertauschen auf Bitbasis bezüglich 32 Bits der Adresse **48**. Wenn $x^{16} + x^{15} + x^2 + 1$ als Erzeugungspolynom für CRC **45** verwendet wird, kann das Verschlüsseln auch dadurch ausgeführt

werden, dass 15 Bits von x^{15}– x, die für den Verschlüssler verantwortlich sind, anstelle den zweiten Ausdruck x^{15} und des dritten Ausdruck x^2 zu variieren. Das Verschlüsseln kann auch durch Verarbeitung von 16 Bits des CRC **45** und durch die Verschlüsselungsinformation durch Rechenoperationen durchgeführt werden.

[0067] Die Schlüsselinformation kann durch die Identifikationsinformation, welche zum Träger gehört, durch die Erzeugeridentifikationsinformation, durch die Händleridentifikationsinformation, durch die Identifikationsinformation, welche zum Aufzeichnungsgerät gehört, dem Codierer oder dem Trägerzeugungsgerät , der Landinformation oder der Identifikationsinformation, welche von außerhalb eingerichtet wird, aufgezählt werden. die obige Information kann in Kombination miteinander oder mit der anderen Information verwendet werden.

[0068] **Fig.** 10 und 11 zeigen eine spezielle Ausführungsform der Fehlerkorrektur-Codierschaltung **16**.

[0069] In **Fig.** 10 und 11 werden Daten von einer Datenkopfanhängungsschaltung **15** von

[0070] **Fig.** 1 über einen Eingangsanschluss **51** einem C1-Codierer **52** zugeführt. Bei der vorliegenden speziellen Ausführungsform besteht jeder Rahmen der Fehlerkorrektur und Codierung aus 148 Bytes oder 148 Symboldaten. Die Digitaldaten am Eingangsanschluss **51** werden alle 148 Bytes gesammelt und zu einem C1-Codierer **52** als eine erste Codiereinheit geliefert. Im C1-Codierer **52** wird eine 8-Byte-Parität angehängt, und die resultierenden Daten werden über eine Verzögerungsschaltung **53** zum Verschachteln zu einem C2-Codierer **54** als zweite Codiereinheit geliefert. Die C2-Codiereinheit **54** hängt eine 14-Byte-Q-Parität an die Daten an, welche über eine Verzögerungsschaltung **55** zurück zum C1-Codierer **52** geliefert werden. Vom C1-Codierer **52** werden 170 Bytes, welche P- und Q-Paritäten enthalten, herausgenommen und über eine Verzögerungsschaltung **56** und eine Umordnungsschaltung **57**, die einen Inverter **57a** an einem Ausgangsanschluss **58** hat, ausgegeben, wonach sie zu einer Modulationsschaltung **17** von **Fig.** 1 geliefert werden.

[0071] Zum Verschlüsseln in der oben beschriebenen Fehlerkorrektur-Codierschaltung kann man in Erwägung ziehen, eine Auswahl zu treffen, ob Inverter als Antwort auf die Verschlüsselungsschlüsselinformation bei jedem Byte des Invertierungsbereichs **57a** in der Umordnungsschaltung **57** eingefügt werden sollten oder nicht. Das heißt, obwohl 22-Byte-P- und Q-Paritäten durch die Inverter des Inverterbereichs **57a** der Umordnungsschaltung **57** im Basisaufbau invertiert werden, können einige dieser Inverter beseitigt werden oder es kann eine Anzahl von Invertern bezüglich der C1-Daten eingefügt werden, um die Ausgangsparitäten zu invertieren.

[0072] Wenn diese Datenumsetzung durchgeführt wird, wird die Wahrscheinlichkeit einer unmöglichen Fehlerkorrektur in Abhängigkeit vom Grad des Unterschieds gegenüber der Basiskonfiguration variiert, d.h., wenn diese Differenz klein ist, wird die Wahrscheinlichkeit des Auftretens eines Fehlers im allerletzten reproduzierten Ausgangssignal lediglich leicht vergrößert, während, wenn es viele Unterschiede gibt, die Fehlerkorrektur insgesamt schwierig wird, so dass die Reproduktion beinahe unmöglich wird. Beispielsweise beträgt im Fall des C1-Codierers der Abstand, der einen Index angebende Fehlerkorrekturfähigkeit angibt, 9, so dass eine Fehlerermittlung und Korrektur bis zu 4 Bytes maximal möglich ist, und, wenn es einen Löschpunkt gibt, die Korrektur bis 8 Bytes maximal möglich. Wenn somit es 5 oder mehrere Unterschiede gibt, wird die Korrektur immer mit dem C1-Code unmöglich. Wenn es vier Unterschiede gibt, tritt ein kritischer Zustand der Korrektur, welche durch zumindest einen weiteren Fehler unmöglich wird, auf. Wenn der Unterschied von drei über zwei bis eins vermindert wird, steigt die Wahrscheinlichkeit der Fehlerkorrektur, die vorstellbar wird, in dieser Reihenfolge an. Wenn dies verwendet wird, ist der Zustand der Reproduktion, bei dem Audio- oder Videosoftware-Reproduktion geliefert wird, bis zu einem bestimmten Ausmaß möglich, jedoch nicht unmerklich und manchmal können Störungen positiv erzeugt werden. Dies kann ausgewertet werden, um den Benutzer über lediglich die Inhaltsangabe der Software zu informieren.

[0073] In diesem Fall ist es möglich, dieses Verfahren zu verwenden, bei dem Änderungsstandorte der Inverter vorgeschrieben sind, bei beispielsweise zwei Standorten, ein Verfahren, in welchem Standortänderungen zufallsmäßig in Abhängigkeit von der Schlüsselinformation ausgewählt werden und die kleinste Anzahl der Änderungsstandorte auf zwei Standorte beschränkt ist, oder ein Verfahren, welches aus einer Kombination der beiden Verfahren besteht.

[0074] Die Positionen zum Einfügen oder zur Modifikation der Inverter ist nicht auf diejenigen in der Umordnungsschaltung **57** in **Fig.** 10 und 11 beschränkt, sondern es können beliebige willkürliche Positionen stromaufwärts oder stromabwärts vom C1-Codierer **52** oder Kombination davon verwendet werden. Wenn es mehrere Positionen gibt, können unterschiedliche Schlüssel verwendet werden. Wie für die Datenumsetzung kann eine Bithinzufügung oder ähnliche logische Operationen anstelle der Verwendung von Invertern verwendet werden, Daten können in Abhängigkeit von der Schlüsselinformation zum Verschlüsseln vertauscht werden, oder Daten können in Abhängigkeit von der Schlüsselinformation zum Verschlüsseln ersetzt werden. Natürlich können eine Vielzahl von Verschlüsselungsverfahren, bei-

spielsweise die Umsetzung durch Schieberegister oder durch verschiedene Funktionsverarbeitung alleine oder in Kombination verwendet werden.

[0075] **Fig.** 12 zeigt eine weitere spezielle Ausführungsform der Fehlerkorrektur-Codierschaltung **16**, bei der ein Satz von exklusiven ODER-Schaltungen (ExOR) **61** stromabwärts des Inverters **57a** innerhalb der Umordnungsschaltung **57** eingefügt ist und bei der ein weiterer Satz exklusiver ODER-Schaltungen **61** stromaufwärts, d.h., auf der Eingangsseite des C1-Codierers **52** eingefügt ist.

[0076] Insbesondere führen die ExOR-Schaltungssätze **61** eine Datenumsetzung eines ExOR-Betriebs bezüglich 170-Byte-Daten durch, welche vom C1-Codierer **52** über die Verzögerungsschaltung **56** und den Inverterbereich **57a** der Umordnungsschaltung **57** herausgenommen wurden, d.h., bezüglich der Informationsdaten $C_{170n+169}$ –$C_{170n+32}$ und Paritätsdaten $P_{170n+21}$ – $P_{170n+14}$, $Q_{170n+13}$ – Q_{170n}, während die ExOR-Schaltungssätze **66** eine Datenumsetzung des ExOR-Betriebs bezüglich der 148-Byte-Eingangsdaten B_{148n} – $B_{148n+147n}$ durchführen. Die ExOR-Schaltungen, welche in diesen ExOR-Schaltungssätzen **61**, **66** verwendet werden, werden die ExOR-1-Byte- oder 8-Bit-Eingangsdaten und die vorher festgelegten 8-Bit-Daten, die durch 1-Bit-sTeuerungsdaten angegeben werden, 170 und 148 dieser 8-Bit-ExOR-Schaltungen ((Äquivalent einer Inverterschaltung, wenn die vorher festgelegten 8-Bit-Daten alle null sind) für die ExOR-Schaltungssätze **61**, **66** entsprechend verwendet.

[0077] In **Fig.** 12 wird die 170-Bit-Schlüsselinformation zu einem Anschluss **62** geliefert und über eine sogenannte D-Latch-Schaltung **63** zu den 170 ExOR-Schaltungen in den ExOR-Schaltungssätzen **61** geleitet. Die D-Latch-Schaltung **63** spricht auf das 1-Bit-Verschlüsselungssteuerungsignal an, welche s zu einem Freigabeanschluss **64** geliefert wird, um zwischen dem Senden der 170-Bit-Schlüsselinformation vom Anschluss **62** unmittelbar auf die ExOR-Schaltungssätze **61** und dem Einstellen aller 170 auf "0" umzuschalten. Von den 170 ExOR-Schaltungen der ExOR-Schaltungssätzen **61** gibt die ExOR-Schaltung, welche mit "0" von der D-Latch-Schaltung **63** beliefert wird, unmittelbar Daten vom Inverterbereich **57a** in der Umordnungsschaltung **57** aus, während die ExOR-Schaltung, welche mit "1" von der D-Latch-Schaltung **63** beliefert wird, Daten vom Inverterbereich **57a** in der Anordnungsschaltung **57** invertiert und ausgibt. Wenn alle Daten null sind, werden diese vom Inverterbereich **57a** in der Umordnungsschaltung **57** unmittelbar ausgegeben. Die ExOR-Schaltungssätze **66** sind ähnlich den ExOR-Schaltungssätzen **61** mit Ausnahme, dass diese 148 ExOR-Schaltungen hat und die Schlüsselinformation von 148 Bits hat. Somit wird die 148-Bit-Schlüsselinformation, welche zu einem Anschluss **67** geliefert wird, über eine D-Latch-Schaltung **68** zu allen ExOR-Schaltungssätzen in den ExOR-Schaltungssätzen geliefert. Die D-Latch-Schaltung **68** wird auf die 148-Bit-Schlüsselinformation oder alle Nullen umgeschaltet durch das Verschlüsselungssteuerungssignal eines Freigabeanschlusses **69**.

[0078] In der Schaltung von **Fig.** 12 führen die ExOR-Schaltungssätze **61** eine Datenumsetzung des ExOR-Betriebs bezüglich 170Byte-Daten durch, die vom C1-Codierer **52** über die Verzögerungsschaltung **56** und den Inverterbereich **57a** der Umordnungsschaltung **57** herausgenommen wurden, d.h., bezüglich Informationsdaten $C_{170n+169}$ – $C_{170n+22}$ und Paritätsdaten $P+_{170n+21}$ – $P_{170n+14}$, $Q_{170n+13}$ – Q_{170n} Alternativ können die ExOR-Schaltungssätze **61** dazu bestimmt werden, eine Datenumsetzung bezüglich der 148-Byte-Informationsdaten $C_{170n+169}$ – $C_{170n+22}$ in Abhängigkeit von der 148-Bit-Schlüsselinformation durchzuführen, ohne eine Datenumsetzung bezüglich der Paritätsdaten auszuführen.

[0079] Mit der Schaltung von **Fig.** 12 kann der Betrieb und eine Wirkung ähnlich der von **Fig.** 10 und 11 realisiert werden. Es ist auch möglich, eine der ExOR-Schaltungen **61** und **66** zu verwenden oder die Auswahl einer oder beider der ExOR-Schaltungen als Verschlüsselungsschlüssel zu verwenden.

[0080] Die Schlüsselinformation kann durch die Identifikationsinformation, die zum Träger gehört, die Erzeugeridentifrkationsinformation, die Vertreiberidentifikationsinformation, die Identifikationsinformation, welche zum Aufzeichnungsgerät, zum Codier- oder zum Trägerwiedergabegerät gehört, die Länderinformation oder die Identifikationsinformation, die von außerhalb geliefert wird, aufgezählt werden. Die obige Information kann in Kombination miteinander oder mit anderen Informationen verwendet werden.

[0081] Anstelle der ExOR-Schaltungen **61** und **66** als Datenumsetzungseinrichtung können UND-, ODER-, NAND-, NOR- oder Inverterschaltungen ebenfalls als obige Datenumsetzungseinrichtung verwendet werden. Zusätzlich zum Durchführen einer logischen Verarbeitung durch die 1-Bit-Schlüsselinformation oder die Verschlüsselungsdaten auf 8-Bit-Basis kann die logische Verarbeitung auch bezüglich 8-Bit-Informationsdaten durchgeführt werden. Alternativ können die UND-, ODER-, ExOR-, NAND- NOR- oder die Inverterschaltungen in Kombination für entsprechende der 8-Bits verwendet werden, die einem Wort der Informationsdaten entsprechen. In diesem Fall werden 148 × 8 Bitschlüsseldaten für 148-Bitdaten verwendet, d.h., 148 × 8-Bit-Daten. Wenn die UND-, ODER-, ExOR-, NAND-, NOR- oder die Inverterschaltungen in Kombination verwendet werden, können diese Kombinationen selbst ebenfalls als Schlüssel verwendet werden. Verschie-

dene Verschlüsselungsverfahren, beispielsweise die Umsetzung durch Schieberegister oder eine unterschiedliche Funktionsverarbeitung können natürlich verwendet werden, so dass diese ebenfalls in Kombination verwendet werden können.

[0082] Obwohl ein Beispiel eines Kreuzverschachtelungs-Fehlerkorrekturcodes bei der ersten Ausführungsform erläutert wurde, kann dieses auch bei einem Produktcode angewandt werden, wie später als zweite Ausführungsform der vorliegenden Erfindung erläutert wird.

[0083] Mit Hilfe von **Fig.** 13 wird nun das Verschlüsseln durch Demodulationsschaltung **17** von **Fig.** 1 erläutert. In dieser Figur werden Daten von der Fehlerkorrektur-Codierschaltung **16** alle 8 Bits (1 Byte) zu einem Anschluss **71** geführt, während die 8-Bit-Schlüsselinformation zu einem Eingangsanschluss **72** geführt wird. Diese 8-Bit-Daten werden zu einer ExOR-Schaltung **73** geführt, als Beispiel der logischen Verarbeitungsschaltung, um einen ExOR-Betrieb auszuführen. Ein 8-Bit-Ausgangssignal der ExOR-Schaltung **73** wird zu einem Modulator eines vorher festgelegten Modulationssystems geliefert, beispielsweise einer 8-16-Umsetzungsschaltung **74**, zur Umsetzung auf 16 Kanalbits. Ein Beispiel des 8-16-Umsetzungssystems durch die 8-16-Umsetzungsschaltung **74** wird als EFM-Plus-Modulationssystem bezeichnet.

[0084] Obwohl das Verschlüsseln unter Verwendung der 8-Bit-Schlüsselinformation vor der Datenmodulation durchgeführt wird, ist die Anzahl von Bits der Schlüsselinformation nicht auf 8 beschränkt, wobei die Eingangs-Ausgangs-Korrelation einer Umsetzungstabelle, welche für die 8-16-Umsetzung verwendet wird, als Antwort auf die Schlüsselinformation variiert werden kann. Für die Schlüsselinformation kann natürlich die Identifikationsinformation, die zum Aufzeichnungsträger wie oben beschrieben gehört, verwendet werden.

[0085] Es wird nun die Synchronisationsanhängungsschaltung **18** erläutert.

[0086] Die Synchronisationsanhängungsschaltung **18** nimmt die Synchronisation, die für vier Arten von Synchronisationswörtern S0 bis S3 verwendet wird, die in **Fig.** 14 gezeigt ist, hinsichtlich von Rahmen der 8-16-Modulation als Einheit. Beispielsweise werden zu 85 Datensymbolen oder 1360 Kanalbits als ein Rahmen der 8-16-Modulation ein Synchronisationswort von 32 Kanalbits hinzugefügt, dieser Rahmen wird durch Verbindung mit dem C1- oder C2-Code strukturiert und es wird veranlasst, dass das Synchronisationswort des Anfangsrahmens der C1-Codefolge sich von dem Synchronisationswort des anderen Rahmens unterscheidet, um die vier Arten von Synchronisationswörtern S0 bis S3 zu erzeugen. Diese Synchronisationswörter S0 bis S3 besitzen entsprechend zwei Synchronisationsmuster a und b in Abhängigkeit vom Zustand "1" oder "0" des unmittelbar vorhergehenden Worts, was als sogenannte digitale Summe oder als dc-Wert bezeichnet wird.

[0087] Die Auswahl dieser vier Synchronisationswörter S0 bis S3 kann in Abhängigkeit von zwei Bits der Schlüsselinformation **75** unter Verwendung beispielsweise der in **Fig.** 15 gezeigten Schaltung geändert werden, um das Verschlüsseln auszuführen. Das heißt, die jeweiligen Bits von zwei Bit-Daten **76**, welche die vier Synchronisationswörter S0 bis S3 bestimmen, und die entsprechenden Bits der 2-Bit-Schlüsselinformation werden durch zwei ExOR-Schaltungen **77**, **78** gemäß ExOR verarbeitet, um ein neues Synchronisationswort zu erzeugen, welches die Daten **79** bezeichnet. Dies modifiziert die Art und Weise, das Synchronisationswort in der oben beschriebenen Rahmenstruktur zu verwenden oder die Position für die Verwendung verschiedener Arten der Synchronisationswörter in der oben beschriebenen Rahmenstruktur, um das Verschlüsseln auszuüben.

[0088] Es ist außerdem möglich, die Anzahl der Arten des Synchronisationsworts zu steigern und die Art und Weise zu bestimmen, wie die vier Arten der Synchronisationswörter unter diesen Synchronisationswörtern in Abhängigkeit vom Verschlüsselungsschlüssel herausgenommen werden. Die oben erwähnte Identifikationsinformation, die zum Aufzeichnungsträger gehört, kann als diese Verschlüsselungsinformation verwendet werden.

[0089] **Fig.** 16 zeigt einen plattenförmigen Aufzeichnungsträger **101**, beispielsweise eine optische Platte als Beispiel des Aufzeichnungsträgers. Dieser plattenförmiger Aufzeichnungsträger **101** besitzt eine Mittenöffnung **102**, in welcher ein Einlaufbereich **103** gebildet ist, beispielsweise ein Inhaltstabellenbereich (TOC) oder ein Programmverwaltungsbereich, ein Programmbereich **104** zum Aufzeichnen von Programmdaten und einen Programmendbereich oder Auslaufbereich **105**, wenn man von dem inneren Rand in Richtung auf den äußeren Rand sieht. In einer optischen Platte zum Wiedergeben von Audiosignalen oder Videosignalen sind Audio- oder Videodaten im Programmbereich aufgezeichnet, und die Zeitinformation für die Audio- oder Videodaten werden durch den Einlaufbereich **103** verwaltet.

[0090] Als Teil der Schlüsselinformation kann die Identifikationsinformation, die in einen Bereich geschrieben ist, der vom Programmbereich verschieden ist, als Datenaufzeichnungsbereich als Teil der Schlüsselinformation verwendet werden. Insbesondere können die Identifikationsinformation einschließlich der Identifikationsinformation wie die Produktionsnummer, die zum Aufzeichnungsträger ge-

hört, die Identifikationsinformation für den Hersteller, die Identifikationsinformation für den Händler, die Identifikationsinformation, die zur Aufzeichnungseinrichtung gehört oder die Codier- oder Identifikationsinformation, welche zur Einrichtung zum Erzeugen des Aufzeichnungsträgers gehört, beispielsweise eine Schneidemaschine oder ein Stempel, in den Einlaufbereich **103** als TOC-Bereich oder in den Auslaufbereich **105** geschrieben sein. Ein Signal, welches beim Verschlüsseln in zumindest einer und vorzugsweise zwei von den oben erwähnten sechs Schaltungen **13** bis **18** erhalten wird, ist im Programmbereich **104** als Datenaufzeichnungsbereich aufgezeichnet. Zur Wiedergabe kann die obige Identifikationsinformation zum Entschlüsseln verwendet werden. Die Identifikationsinformation kann außerdem physikalisch oder chemisch innerhalb des Einlaufbereichs **103** geschrieben sein und während der Wiedergabe ausgelesen werden, um so als Schlüsselinformation zum Decodieren verwendet zu werden.

[0091] Mit Hilfe von **Fig.** 17 werden bevorzugte Ausführungsformen des Datenwiedergabeverfahrens und des Datenwiedergabegeräts gemäß der vorliegenden Erfindung erläutert.

[0092] In **Fig.** 17 wird der plattenförmige Aufzeichnungsträger **101** als Beispiel des Aufzeichnungsträgers drehbar durch einen Spindelmotor **108** angetrieben, so dass dessen Aufzeichnungsinhalt durch eine Wiedergabekopfeinrichtung **109**, beispielsweise eine optische Abtasteinrichtung gelesen werden.

[0093] Die Digitalsignale, welche durch die Wiedergabekopfeinrichtung **109** gelesen werden, werden zu einem TOC-Decoder **111** und zu einem Verstärker **112** geliefert. Vom TOC-Decoder **111** werden die Identifikationsinformation einschließlich der Identifikationsinformation, beispielsweise die Herstellernummer, die zum Aufzeichnungsträger gehört, die Identifikationsinformation für den Hersteller, die Identifikationsinformation für den Händler, die Identifikationsinformation, die zur Aufzeichnungseinrichtung gehört, oder die Codier- oder Identifikationsinformation, die zur Einrichtung gehört, um den Aufzeichnungsträger herzustellen, beispielsweise eine Schneidemaschine oder ein Stempel, gelesen, die als zumindest ein Bereich der Schlüsselinformation zum Decodieren der Verschlüsselung verwendet werden. Die Identifikationsinformation, die zum Wiedergabegerät gehört, oder die Identifikationsinformation von außerhalb kann von einer CPU 122 im Wiedergabegerät ausgegeben werden, so dass sie zumindest als ein Bereich der Schlüsselinformation verwendet wird. Die Identifikationsinformation von außerhalb umfasst die Identifikationsinformation, welche über das Kommunikationsnetzwerk oder den Übertragungsweg empfangen wird, und die Identifikationsinformation, die beim Lesen einer sogenannten IC-Karte, einer ROM-Karte, einer Magnetkarte oder einer optischen Karte erhalten wird.

[0094] Das Digitalsignal, welches von der Wiedergabekopfeinrichtung **109** über den Verstärker **112** und einer Phasenverriegelungsschaltung (PLL) **113** herausgenommen wird, wird zu einer Synchronisationstrennschaltung **114** geliefert, um das Synchronisationssignal, welches durch die Synchronisationsanhängungsschaltung **18** von **Fig.** 1 angehängt wurde, zu trennen. Das Digitalsignal von der Synchronisationstrennschaltung **114** wird zu einer Demodulationsschaltung **115** geliefert, um einen Betrieb durchzuführen, der die Umkehrung der Modulation ist, der durch die Modulationsschaltung **17** von **Fig.** 1 ausgeführt wird. Insbesondere setzt dieser Betrieb **16** Kanalbits in 8 Bit-Daten um. Die Digitaldaten von der Demodulationsschaltung **115** werden zu einer Fehlerkorrektur-Decodierschaltung **116** geliefert, um ein Decodieren durchzuführen, beispielsweise einen Umkehrbetrieb der Codierung, der durch die Fehlerkorrektur-Codierschaltung **16** von **Fig.** 1 ausgeführt wurde. Die decodierten Daten werden in Sektoren durch eine Sektorauflösungsschaltung **117** ausgelöst und ein Datenkopf am Anfang jedes Sektors wird durch die Datenkopftrennschaltung **118** getrennt. Die Datenkopfauflösungsschaltung **177** und die Datenkopftrennschaltung **118** sind Gegenstücke der Sektorbildungsschaltung **13** und der Kopfanhängungsschaltung **15** von **Fig.** 1 entsprechend. Eine Entschlüsselungsschaltung **119** führt dann das Entschlüsseln als Umkehrbetrieb des Verschlüsselns durch, der durch die Verschlüsselungsschaltung **14** von **Fig.** 1 durchgeführt wurde, so dass die reproduzierten Daten über eine Schnittstellenschaltung **120** an einem Ausgangsanschluss **121** ausgegeben werden.

[0095] Es sei angemerkt, dass das Verschlüsseln während des Aufzeichnens in zumindest einer von der Sektorbildungsschaltung **13**, der Verschlüsselungsschaltung **14**, der Datenanhängungsschaltung **15**, der Fehlerkorrektur-Codierschaltung **16**, der Modulationsschaltung **17** und der Synchronisationsanhängungsschaltung **18** ausgeführt wird, so dass ein Entschlüsselungsbetrieb in den wiedergabeseitigen Schaltungen **114** bis **119** als Gegenstücke der Verschlüsselungsschaltungen erforderlich ist. Das heißt, wenn das Verschlüsseln durch die Sektorbildungsschaltung **13** von **Fig.** 1 ausgeführt wird, ist es für die Sektorauflösungsschaltung **117** notwendig, das Verschlüsseln unter Verwendung der Schlüsselinformation durchzuführen, die für das Verschlüsseln verwendet wird. Ähnlich wird das Entschlüsseln durch die Entschlüsselungsschaltung **119**, durch die Datenkopftrennschaltung **118**, durch die Fehlerkorrektur-Decodierschaltung **116**, durch die Demodulationsschaltung **115** und durch die Synchronisationstrennschaltung **114** in Verbendung mit dem Verschlüsseln durch die Verschlüsselungsschaltung **14**,

die Datenkopfanhängungsschaltung **15**, die Fehlerkorrektur-Codierschaltung **16**, die Modulationsschaltung **17** und durch die Synchronisationsanhängungsschaltung **18** von **Fig.** 1 entsprechend notwendig.

[0096] Die Entschlüsselung durch Synchronisationstrennschaltung **114** wird durch Ermitteln der Art und Weise durchgeführt, wie mehrere beispielsweise vier unterschiedliche Arten von den Synchronisationswörtern verwendet werden, oder der Position der Verwendung der verschiedenen Synchronisationswörter in einer Rahmenstruktur, welche gemäß der Schlüsselinformation zum Verschlüsseln modifiziert wurden, wie mit Hilfe von **Fig.** 14 und 15 erläutert wurde.

[0097] Beim Entschlüsselungsbetrieb durch die Demodulationsschaltung **115** werden die 8-Bit-Daten, welche von der Synchronisationstrennschaltung **114** zu einer 16-8-Umsetzungsschaltung **131** geliefert werden, um so von den 16-Kanalbits umgesetzt zu werden, zu einer ExOR-Schaltung **132** geliefert, als Gegenstück der ExOR-Schaltung **73** von **Fig.** 13, so dass sie mit der 8-Bit-Verschlüsselungsinformation von einem Anschluss **133** ExOR-verarbeitet werden, um die Daten, welche den 8-Bit-Daten entsprechen, die zum Eingangsanschluss **71** von **Fig.** 13 geliefert werden, wiederherzustellen, wie in **Fig.** 18 gezeigt ist. Die wiederhergestellten Daten werden zu einer Fehlerkorrektur-Decodierschaltung **116** geliefert.

[0098] Die Fehlerkorrektur-Decodierschaltung **116** führt einen Umkehrbetrieb der Fehlerkorrektur-Codierung durch, die in **Fig.** 10 und 11 gezeigt ist, durch den Aufbau von **Fig.** 19 und 20.

[0099] Gemäß **Fig.** 19 und 20 werden demodulierte Daten von der Demodulationsschaltung **115** in Form von 170 Bytes oder 170 Symbolen als Einheit über eine Umordnungsschaltung **142**, die einen Inverter **142a** aufweist, und über ein Verzögerungsschaltung **143** zu einem C1-Decodierer **144** als ersten Decoder geliefert. Von den 170 Bytes der Daten, welche zu diesem C1-Decoder **144** geliefert werden, sind 22 Bytes P-Paritätsdaten und Q-Paritätsdaten. Der C1-Decoder **144** führt das Decodieren unter Verwendung von diesen Paritätsdaten durch. Der C 1-Paritätsdatendecoder gibt 170 Byte-Daten über eine Verzögerungsschaltung **145** zu einem C2-Decoder **146** als zweiten Decoder aus, wo die Fehlerkorrektur und das Decodieren unter Verwendung dieser Paritätsdaten durchgeführt werden. Ausgangsdaten des C2-Decoders **146** werden zu einer C1-Verzögerungsdecodierschaltung **140** von **Fig.** 19 geliefert. Diese Schaltung ist ähnlich der Verzögerungsschaltung **143** und dem C1-Decoder **144** und fuhrt wiederholt den Betrieb ähnlich dem durch, der durch die Verzögerungsschaltung **143** und den C 1-Decoder **144** durchgeführt würde, um die Fehlerkorrektur und das Decodieren durchzuführen. In der Ausführungsform von **Fig.** 20 ist die C1-Verzögerungsdecodierschaltung **140** als Verzögerungsschaltung **147** und ein C3-Decoder **148** als dritter Decoder gezeigt. Die Verzögerungsschaltung **147** und der C3-Decoder **148** oder die C 1-Verzögerungsdecodierschaltung **140** führen eine endgültige Fehlerkorrektur und Decodierung durch, so dass 148-Byte-Daten ohne Parität an einem Ausgangsanschluss **149** ausgegeben werden. Die 148-Byte-Daten entsprechen den 148 Byte-Daten, die in den C1-Decoder **52** von **Fig.** 11 betreten.

[0100] Wenn das Verschlüsseln im Inverterbereich **57a** der Umordnungsschaltung **57** der Fehlerkorrektur-Codierschaltung von **Fig.** 10 und 11 durchgeführt ist, ist es notwendig, dass der Inverterbereich **142a** in der Umordnungsschaltung **142** der Fehlerkorrektur- und Decodierschaltung von **Fig.** 19 und 10 entsprechendes Entschlüsseln durchführt. Es ist natürlich notwendig, das Entschlüsseln als Umkehrbetrieb der verschiedenen Arten von Verschlüsselung auszuführen, welche mit Hilfe von **Fig.** 10 und 11 erläutert wurden.

[0101] **Fig.** 21 zeigt einen beispielhaften Aufbau der Fehlerkorrektur-Decodierschaltung als Gegenstück des beispielhaften Ausbaus der Fehlerkorrektur-Codierschaltung, die in **Fig.** 12 gezeigt ist.

[0102] Gemäß **Fig.** 21 werden ExOR-Schaltungssätze **151** in eine Eingangsseite des Inverterbereichs **142a** der Umordnungsschaltung **142** und in die Eingangsseite der Verzögerungsschaltung **143** in Verbindung mit den ExOR-Schaltungssätzen **61**, die in die Ausgangsseite des Inverterbereichs **57a** der Umordnungsschaltung **57** von **Fig.** 12 eingefügt, während ExOR-Schaltungssätze **156** auf der Ausgangsseite des C 1-Decoders **148** in Verbindung mit den Ex-OR-Schaltungen **66** eingefügt werden, die auf der Eingangsseite des C 1-Decoderss **52** von **Fig.** 12 eingefügt wurden.

[0103] Diese ExOR-Schaltungssätze **151**, **156** sind zur Datenumsetzung konfiguriert, um die Datenumsetzung zu decodieren, welche durch die Ex-OR-Schaltungssätze **61**, **66** von **Fig.** 12 ausgeführt wurde. Von diesen bestehen die ExOR-Schaltungssätze **151** aus beispielsweise 170 8-Bit-ExOR-Schaltungen, während die ExOR-Schaltungen **156** aus beispielsweise 148 8-Bit-ExOR-Schaltungen bestehen. Wenn die Datenumsetzung als Antwort auf die Schlüsselinformation für die 148-Byte-Informationsdaten mit Ausnahme der Paritätsdaten durch die Ex-OR-Schaltungen **61** der aufzeichnungsseitigen Fehlerkorrektur-Codierschaltung von **Fig.** 12 durchgeführt wurde, werden die ExOR-Schaltungssätze natürlich durch 148 8-Bit-ExOR-Schalgungen gebildet.

[0104] Zu einem Anschluss **152** von **Fig.** 21 wird die 170-Bit-Schlüsselinformation geliefert, die der

Schlüsselinformation entspricht, welche zum Anschluss **62** von **Fig.** 12 geliefert wird. Die Schlüsselinformation wird über eine D-Latch-Schaltung **153** zu allen 170 ExOR-Schaltungen innerhalb der ExOR-Schaltungen **151** geliefert. Die D-Latch-Schaltung **153** wird als Antwort auf das 1-Bit-Verschlüsselungssteuersignal, welches zu einem Freigabeanschluss **154** geliefert wird, zwischen dem Senden des 170-Bit-Schlüsselinformation von dem Anschluss **152** unmittelbar zu den ExOR-Schaltungssätzen **151** und dem Setzen der 170 Bits auf "0" in ihrer Gesamtheit umgeschaltet. Dagegen sind die ExOR-Schaltungssätze **156** ähnlich den ExOR-Schaltungssätzen **151** mit Ausnahme davon, dass die ExOR-Schaltungssätze **156** 148 ExOR-Schaltungssätze **151** haben und die 148-Bit-Schlüsselinformation, die ähnlich der Schlüsselinformation ist, welche zum Anschluss **12** von **Fig.** 12 geliefert wird. Die 148-Bit-Schlüsselinformation, welche zu einem Anschluss **157** geliefert wird, wird über eine Latch-Schaltung **158** zu allen 148 ExOR-Schaltungen **156** über die D-Latch-Schaltung **158** geliefert. Die D-Latch-Schaltung **158** wird wiederum als Antwort auf das Verschlüsselungssteuersignal von einem Freigabeanschluss **159** zwischen der 148-Bit-Schlüsselinformation und Gesamtnull umgeschaltet.

[0105] Durch Verwenden der ExOR-Schaltungen oder des Inverters der Fehlerkorrekturschaltung wird es möglich, ein einfaches und signifikantes Verschlüsseln zu realisieren. Außerdem kann man mit Steuern der Anzahl der Inverter, normalerweise nicht reproduzierbare Daten des Verschlüsselungspegels oder Daten, welche in einem schlechten Fehlerzustand nicht reproduzierbar sind, mit der Antwort auf den Befehl für den Sicherheitspegel fertig werden. Das heißt, durch Steuern der Anzahl der Inverter oder der ExOR-Schaltungen kann die Steuerung in einer Weise durchgeführt werden, dass die Reproduktion möglich bzw. unmöglich für die besseren bzw. schlechteren Fehlerzustände wird. Der reproduzierbare Zustand, der nicht durch die Fehlerkorrektur selbst abgedeckt werden kann, kann ebenfalls erzeugt werden. Wie für den Verschlüsselungsschlüssel kann die Anzahl von Bits sogar 100 oder mehr pro Codierstandort erreichen, wie bei der obigen gezeigten Ausführungsform, daher wird das Codieren mit der großen Anzahl von Bits des Schlüssels möglich, wodurch somit die Datensicherheit verbessert wird. Durch Vorsehen der Fehlerkorrektur-Codierschaltung und der Fehlerkorrektur-Decodierschaltung innerhalb einer LSI- oder IC-Chiphardware kann der Zugriff auf den Aufzeichnungsträger von den Benutzern allgemein schwieriger gemacht werden, wodurch somit wieder die Datensicherheit angehoben wird.

[0106] Die Sektorauflösungsschaltung **117** führt das sogenannte Entschachteln durch, welches ein Umkehrbetrieb zum geradzahligen oder nicht geradzahligen Verschachteln ist, wenn das Verschlüsseln durch diese geradzahlige oder ungeradzahlige Byte-Verschachtelung durchgeführt wurde, um durch die Sektorbildungsschaltung **13** aufgezeichnet zu werden, wie mit Hilfe von **Fig.** 2 und 3 erläutert wurde.

[0107] Die Datenkopftrennschaltung **118** führt das entsprechende Entschlüsseln durch, wenn das Verschlüsseln, welches mit Hilfe von **Fig.** 7 bis 9 erläutert wurde, d.h., die Datensynchronisationsbyte-Mustervertauschung, welche die Sektorsynchronisation darstellt, die Adressänderung oder die CRC-Änderung während des Aufzeichnens durch die Datenkopfanhängungsschaltung **15** durchgeführt wurde.

[0108] **Fig.** 22 zeigt eine beispielhafte Ausführungsform der Entschlüsselungsschaltung **119**. Zu einem Anschluss **161** werden Digitaldaten von der Datenkopftrennschaltung **118** von **Fig.** 17 geliefert. Die Digitaldaten von dem Anschluss **161** werden durch einen Verschlüssler **163** entschlüsselt, der aufgebaut ist, wie in **Fig.** 4 gezeigt ist, die an einem Ausgangsanschluss **164** herausgenommen werden. Das Entschlüsseln kann durch Ändern eines Polynoms **165** und eines vorher festgelegten Werts oder des Anfangswerts **166** durchgeführt werden, wie mit Hilfe von **Fig.** 4 für den Verschlüssler **163** in Abhängigkeit von der Verschlüsselungsschlüsselinformation von einem Autorisierungsmechanismus **171** erläutert wurde. Der Autorisierungsmechanismus **171** erzeugt die Verschlüsselungsschlüsselinformation in Abhängigkeit vom Inhalt der Kopierinformation **46** der Datenkopfinformation **167**, die Identifikationsinformation, welche zum Aufzeichnungsträger oder zum Wiedergabegerät gehört, die gemeinsame Identifikationsinformation **173**, welche zum Hersteller oder zum Händler der externen Identifikationsinformation **174** gehört, welche von außerhalb geliefert wird, um das Erzeugungspolynom cib 165 oder den vorher festgelegten Wert **166** in Abhängigkeit von der Schlüsselinformation zu steuern.

[0109] Die Information, für welche n dieser Schaltungen 114 bis 119 zum Entschlüsseln erforderlich ist, kann zeigen, ob sie die Schlüsselinformation zum Verschlüsseln ist, wie oben erläutert wurde. Außerdem kann die Verschlüsselungsschlüsselinformation in einer vorher festgelegten Periode umgeschaltet werden, beispielsweise in jedem Sektor. Das Ausmaß der Leichtigkeit oder Schwierigkeit beim Verschlüsseln wird unter Verwendung gesteigert, ob das Umschalten durchgeführt wird oder nicht, oder der Umschaltperiode, beispielsweise der Verschlüsselung.

[0110] Durch Kombinierung der Herstelleridentifikationsinformation, der Händleridentifikationsinformation oder der Einrichtungsidentifikationsinformation mit der Kopierschutzinformation oder der Belastungsin-

formation, die separat eingestellt werden, wie oben beschrieben, um Daten zu verschlüsseln und um die verschlüsselten Daten aufzeichnen, kann das Verhindern des Kopierens, einer gestohlenen Ausgabe oder schwarzen Verwendung bezüglich des körperlichen Formatpegels realisiert werden. Zusätzlich befindet sich die Information, welche die Datensicherheitsfunktion, die Kopiererlaubnis-Nichterlaubnisfunktions-Information oder die Belastungs-/belastungsfreie-Information auf einem Aufzeichnungsträger oder in einem realen Format des Aufzeichnungs-/Wiedergabesystems.

[0111] Das heißt, durch vorheriges Aufzeichnen der Sicherheits-Belastungsinformation auf dem Aufzeichnungsträger und durch Kombinieren dieser mit der Datenverschlüsselung unter Verwendung Aufzeichnungs-/Nichtaufzeichnungsinformation für den Aufzeichnungsträger kann die Kopierverhinderung und die Vermeidung von einer nichtlegalen Verwendung mit einer vereinfachten Struktur realisiert werden. Das Decodieren kann durch verborgene Einbindung im körperlichen Format schwierig gemacht werden. Die Struktur ist gegenüber einer Stapelkopierung sicher, da diese im verschlüsselten Zustand verbleibt. Die Struktur kann auf Sektorbasis variiert werden, auf der Dateibasis, auf Zonenbasis oder auf Schichtbasis. Die Schlüsselsteuerung kann durch Kommunikation, durch die IC-Karte oder durch eine Fernsteuerung durchgeführt werden. Eine Nachwirkung kann auch gegenüber Piraterie verbleiben.

[0112] Es wird nun die zweite Ausführungsform der vorliegenden Erfindung erläutert. Die zweite Ausführungsform ist eine Teilmodifikation der oben beschriebenen ersten Ausführungsform. Der Gesamtaufbau ist so, wie in **Fig.** 1 gezeigt ist. Es werden lediglich die modifizierten Bereiche der Schaltungen **13** bis **18** der Konfiguration von **Fig.** 1 anschließend erläutert.

[0113] Die Sektorbildungsschaltung **13** von **Fig.** 1 kann wie bei der ersten oben beschriebenen Ausführungsform ausgebildet sein. Die Verschlüsselungsschaltung **14** ist jedoch so konfiguriert, wie in **Fig.** 23 gezeigt ist.

[0114] In der Verschlüsselungsschaltung **14** werden, wie in **Fig.** 23 gezeigt ist, Daten von der Sektorbildungsschaltung **13** von **Fig.** 1 in einer Sequenz, in welcher das niedrigwertigste Bit (LSB) zeitweise zuerst kommt, d.h., in der ersten LSB-Reihenfolge zum Dateneingangsanschluss **35** geliefert. Ein 15-Bit-Schieberegister **14a** zum Verschlüsseln ist so aufgebaut, dass die Rückführung durch das Erzeugungspolynom $x^{15} + x^4 + 1$ angewandt wird, wobei eine exklusive ODER-Schaltung (ExOR) **14b** verwendet wird, während ein vorher festgelegter Wert oder ein Anfangswert, wie in **Fig.** 24 gezeigt ist, im 15-Bit-Schieberegister **14a** gesetzt wird. Die Auswahlnummern der vorher festgelegten Werte, die in **Fig.** 24 gezeigt sind, werden so ausgewählt, dass die vorher festgelegten Werte auf Sektorbasis in Verbindung mit beispielsweise den Werten der unteren vier Bits der Sektoradresse umgeschaltet werden können. Die Ausgangsdaten des Schieberegisters **14a** und die Eingangsdaten vom Anschluss **35** werden durch die ExOR-Schaltung **14c** gemäß ExOR verarbeitet, von denen ein Ausgangssignal an einem Ausgangsanschluss **14d** ausgegeben wird, welches zur Datenkopfanhängungsschaltung **15** von **Fig.** 1 geliefert wird.

[0115] Der vorher festgelegte Wert (Anfangswert) kann in Abhängigkeit von der Schlüsselinformation, beispielsweise der vorher festgelegten Identifikationsnummer variiert werden. Das heißt, die vorher festgelegten Werte der 16-Byte-Identifikationsinformation der vorher festgelegten Werttabelle von **Fig.** 24 können logisch mit entsprechenden Byte-Werten der 16-Byte-Identifikationsifnormation verarbeitet werden. Die Identifikationsinformation in diesem Fall kann die Identifikationsinformation enthalten, beispielsweise die Produktionsnummer, die zum Aufzeichnungsträger gehört, die Identifikationsinformation für den Hersteller, die Identifikationsinformation für den Händler, die Identifikationsinformation, die zu der Aufzeichnungseinrichtung oder zum Codierer gehört, oder die Identifikationsinformation, welche zur Einrichtung gehört, um den Aufzeichnungsträger zu erzeugen, die Landinformation, die Identifikationsinformation, welche von außerhalb geliefert wird, alleine oder in Kombination. Die obige Information verschiedener Arten kann außerdem in Kombination mit anderen Arten der Information verwendet werden. Die logische Verarbeitung umfasst das exklusive OR (ExOR), das logische Produkt (AND), die logische Summe (OR) oder das Verschieben.

[0116] Das Sektorformat für die zweite Ausführungsform kann so aufgebaut sein, wie beispielsweise in **Fig.** 25 gezeigt ist.

[0117] Wie in **Fig.** 25 gezeigt ist, besteht jeder Sektor aus 12 Reihen, wobei jede aus 172 Bytes besteht, insgesamt 2064 Bytes, von denen 2048 Bytes Hauptdaten darstellen. An einer Anfangsposition der ersten der 12 Reihen sind 4-Byte-identifikationsdaten (ID), ein 2-Byte-ID-Fehelrermittlungscode (IED) und 6-Byte-Reservedaten (RSV) in dieser Reihenfolge aufgereiht. An einer Anschlussposition der letzten Reihe ist ein 4-Byte-Fehlerermittlungscode (EDC) aufgereiht.

[0118] Wie in **Fig.** 26 gezeigt ist, bestehen die 4 Bytes der Identifikationsdaten (ID) aus dem ersten Byte (Bits b31 bis b24), welches durch die Sektorinformation gebildet ist, und den verbleibenden 3 Bytes (Bits b23 bis b0), welche durch die Sektornummern

gebildet sind. Die Sektorinformation besteht aus 1 Bit der Sektorformatart, 1 Bit des Spurführungsverfahrens, 1 Bit der Reflektivität, 1 Bit der Reserveinformation, 2 Bits des Bereichstypus und 2 Bits der Schichtnummer.

[0119] Die Datenkopfanhängungsschaltung **15** von **Fig.** 1 führt die Vertauschung, d.h., das Verschachteln auf Bit-Basis bezüglich der 14 Bits der Sektornummer in den Identifikationsdaten (ID) im Sektorformat aus, als Antwort auf die Verschlüsselungsinformation zum Bewirken der Verschlüsselung. Zusätzlich kann das Erzeugungspolynom des 2-Byte-ID-Fehlerermittlungscodes (IED) oder des Erzeugungspolynoms des 4-Byte-Fehlerermittlungscodes (EDC) in Abhängigkeit von der Schlüsselinformation oder logisch mit der Schlüsselinformation modifiziert werden, um das Verschlüsseln auszuführen.

[0120] Die Fehlercodier-Korrekturschaltung **16** von **Fig.** 1 kann so aufgebaut sein, wie in **Fig.** 27 gezeigt ist. Zum Codieren wird der Produktcode oder der Blockcode, wie in **Fig.** 28 gezeigt ist, verwendet.

[0121] Betrachtet man nun **Fig.** 27, so werden die Daten von der Datenkopfanhängungsschaltung **15**, welche in **Fig.** 1 gezeigt ist, zu einem Eingangsanschluss **210** geliefert. Diese Eingangsdaten werden zu einem PO-Codierer **211** als erste Codiereinheit geliefert. Die Eingangsdaten zum PO-Codierer **211** sind 172 Bytes × 192 Reihen oder $B_{0,0}$ bis $B_{191,172}$. Der PO-Codierer **211** hängt einen RS-Außencode (PO) von RS (208, 192, 17) als 16-Byte-Reed-Solomon-code (RS-Code) an alle 192 Bytes aller 172 spalten an, wie in **Fig.** 28 gezeigt ist. Die Ausgangsdaten des PO-Codierers **211** werden über die Datenumsetzungsschaltung zum Verschlüsseln **212** wie oben beschrieben, zu einer Entschachtelungsschaltung **213** geliefert, um Verschachtelungsdaten zu bilden, welche zu einem PI-Codierer **214** geliefert werden. Die PI-Codierer **214** hängt einen RS-Innencode (PI) von RS (182, 172, 11) (RS-Code) an jede Reihe der 172 Bytes der 172 Bytes × 208 Reihen an. Damit gibt der PI-Codierer **214** Daten von 182 Bytes × 208 Reihen aus. Diese Ausgangsdaten werden an einem Ausgangsanschluss **216** über eine Datenumsetzungsschaltung **215** zum Verschlüsseln wie oben beschrieben ausgegeben.

[0122] Da der PO-Codierer **211** die 16-Byte-PO-Parität an die 192-Byte-Eingangsdaten für jede Spalte anhängt, um 208-Byte-Daten auszugeben, führt die Datenumsetzungsschaltung **212** die Datenumsetzung wie oben beschrieben bezüglich der 16-Byte-Parität oder der 208-Byte-Daten in ihrer Gesamtheit durch, um das Verschlüsseln auszuführen. Diese Datenumsetzung kann als Antwort auf die Schlüsselinformation durchgefihrt werden, welche über einen Anschluss **218** geliefert wird. Da die Datenumsetzungsschaltung **215** 10-Byte-PI-Parität den 172-Byte-Daten jeder Reihe anhängt, um 182-Byte-Daten auszugeben, kann die Datenumsetzungsschaltung **215** das Verschlüsseln dadurch ausführen, dass die Datenumsetzung bezüglich der 10-Byte-Daten oder der 182-Byte-Daten in ihrer Gesamtheit ausgeführt wird. Die Datenumsetzung kann als Antwort auf die Schlüsselinformation, welche über den Anschluss **219** geliefert wird, wie oben beschrieben ausgeführt werden.

[0123] Die obige Datenumsetzung kann durch Anordnen eines Inverters an einer vorher festgelegten Position durchgeführt werden, durch selektives Invertieren von Daten durch die ExOR-Schaltungssätze als Antwort auf die Schlüsselinformation oder durch Verwenden der UND-, ODER-, oder NAND-Schaltungen. Zusätzlich zur logischen Verarbeitung bezüglich der 8-Bit-Informationsdaten durch die 1-Bit-Schlüsselinformationsdaten oder durch die Schlüsseldaten kann die logische Verarbeitung bezüglich der 8-Bit-Informationsdaten durch die 8-Bit-Schlüsselinformationsdaten durchgeführt werden, oder es können UND, OR, ExOR, NAND, NOR- oder Inverterschaltungen in Kombination für alle 8 Bits verwendet werden, um ein Wort der Informationsdaten zu bilden. Natürlich können eine Vielzahl von Verschlüsselungsverfahren, beispielsweise die Umsetzung durch Schieberegister oder die Funktionsverarbeitung alleine oder in Kombination angewandt werden. Wenn die UND-, ODER-, ExOR-, NAND-, NOR- oder die Inverterschaltungen in Kombination verwendet werden, kann die Kombination selbst als Schlüssel verwendet werden. Zusätzlich zur logischen Verarbeitung kann die Vertauschung der Änderungsdatenpositionen oder den Ersatz von Ersatzdatenwerten ebenfalls für die Datenumsetzung verwendet werden. Natürlich kann eine Vielzahl von Verschlüsselungsverfahren, beispielsweise die Umsetzung des Schieberegisters oder die Funktionsverarbeitung alleine oder in Kombination angewandt werden.

[0124] Die 182 Bytes × 208 Reihen von Daten, die aus der Fehlerkorrektur-Codierung resultieren, werden in bezug auf die Reihen verschachtelt und in 16 13-Reihengruppen getrennt, wobei jede mit einem Aufzeichnungssektor verknüpft ist. Jeder Sektor, der aus 182 Bytes × 13 Reihen, d.h. insgesamt 2366 Bytes besteht, wird moduliert, und es werden 2 Synchronisationscodes SY pro Reihe angehängt, wie in **Fig.** 29 gezeigt ist. Für die Modulation wird die 8-16-Umsetzung wie bei der oben erläuterten ersten Ausführungsform verwendet. Jede Reihe wird in 2 Synchronisationsrahmen unterteilt, wobei jede aus einem 32-Kanalbit-Synchronisationscode SY und einem 1456-Kanalbit-Datenbereich besteht. **Fig.** 29 zeigt eine Datenstruktur für einen Sektor, der bei der Modulation und dem Anhängen der Synchronisationsdaten erhalten wird. Die 38688-Kanalbits jedes Sektors, der in **Fig.** 29 gezeigt ist, entsprechen den 2418 Bytes vor der Modulation.

[0125] Das modulierte Ausgangssignal von **Fig.** 28 verwendet acht Arten der Synchronisationscodes SYO bis SY7. Diese Synchronisationscodes SYO bis SY7 zeigen Synchronisationsmuster von **Fig.** 30(a) und **Fig.** 30(b) für die 8-16-Umsetzungszustände 1, 2 und für die 8-16-Umsetzungszustände 3 und 4 in Abhängigkeit von den oben beschriebenen 8-16-Umsetzungszuständen entsprechend.

[0126] Die Auswahl der acht Arten der Synchronisationscodes SYO bis SY7 kann als Antwort auf die 3-Bit-Verschlüsselungsinformation geändert werden, um das Verschlüsseln auszuführen. Das heißt, die entsprechenden Bits der 3-Bit-Daten **221**, welche die acht Arten der Synchronisationscodes SYO bis SY7 zeigen, und die entsprechenden Bits der 3-Bit-Schlüsselinformation **222** werden durch die drei ExOR-Schaltungen **223**, **224**, **225** gemäß ExOR-verarbeitet, um neue Synchronisationscode-Bestimmungsdaten **226** zu erzeugen. Dies modifiziert die Art und Weise, den Synchronisationscode in der obigen Rahmenstruktur zu verwenden oder die Position, die verschiedenen Variationscodes in der Rahmenstruktur zu verwenden, um das Verschlüsseln durchzuführen. Natürlich können Daten der drei Bits vertauscht, substituiert oder durch eine Schieberegister oder eine Funktionsumsetzung in Abhängigkeit von der Schlüsselinformation umgesetzt werden.

[0127] Die Basisstruktur einer Wiedergabeseite, als Gegenstück zur Aufzeichnungsseite der oben beschriebenen zweiten Ausführungsform der vorliegenden Erfindung ist ähnlich der, die in **Fig.** 17 beschrieben wurde, und es wird ein Umkehrbetrieb, der zu modifizierten Bereichen in der zweiten Ausführungsform passt, durchgeführt. Beispielsweise kann der Umkehrbetrieb als Gegenstück der Fehlerkorrektur-Codierung, welche in **Fig.** 27 gezeigt ist, durch eine Fehlerkorrektur-Decodierschaltung, welche in **Fig.** 32 gezeigt ist, ausgeführt werden.

[0128] In dieser Figur werden Daten des Produktscodes von 182 Bytes × 208 Reihen von **Fig.** 28 entsprechend einem Ausgangssignal des Ausgangsanschlusses **216** von **Fig.** 27, d.h., ein Ausgangssignal der Demodulationsschaltung **115** von **Fig.** 17 zu einem Eingangsanschluss **230** geliefert. Diese Daten vom Eingangsanschluss **230** werden zu einer Datenumsetzungsschaltung **231** geliefert, wo ein Umkehrbetrieb des Betriebs ausgeführt wird, der durch die Datenumsetzungsschaltung **215** von **Fig.** 27 durchgefihrt wurde. Ausgangsdaten der Daten-Zurückumsetzungsschaltung **231** werden zu einem PI-Decoder (Innencode) **232** geliefert, wo das Decodieren, wie die Umkehroperation der Operation, welche durch den PI-Codierer **214** von **Fig.** 27 durchgeführt wurde, d.h., die Fehlerkorrektur unter Verwendung des PI-Codes, zum Erzeugen von 172 Bytes × 208 Reihen von Daten ausgeführt wird, die in **Fig.** 28 gezeigt sind. Ausgangsdaten des PI-Decoders **232** werden durch eine Operation verarbeitet, welche die Umkehrung der Operation ist, die durch die Datenumsetzungsschaltung **213** durchgeführt wurde, und anschließend zu einem PO-Decoder (Außencode-Decoder) **235** geliefert. Der PO-Decoder **235** führt eine Decodieroperation als Umkehroperation der Operation durch den PO-Codierer **211** von **Fig.** 27 durch, d.h., die Fehlerkorrektur unter Verwendung des PO-Codes, um die ursprünglichen 172 Bytes × 182 Reihen der Daten von **Fig.** 28 an einem Ausgangsanschluss **236** herauszunehmen. Wenn die Schlüsselinformation zur Datenumsetzung durch die Datenumsetzungsschaltungen **212**, **215** von **Fig.** 27 verwendet wird, kann die Schlüsselinformation, welche zu allen Anschlüssen **218**, **219** geliefert wird, zu den Anschlüssen **239**, **238** der Daten Rückumsetzungsschaltungen **234**, **231** von **Fig.** 32 geliefert werden, um eine Datenrückumsetzung in Abhängigkeit von der Schlüsselinformation zu bewirken.

[0129] Die vorteilhafte Wirkung der oben beschriebenen zweiten Ausführungsform der vorliegenden Erfindung ist ähnlich der der oben beschriebenen ersten Ausführungsform.

[0130] Bei der oben beschriebenen Ausführungsform des Datenaufzeichnungsverfahrens gemäß der vorliegenden Erfindung werden Eingangsdaten durch Verschlüsseln in zumindest einem Sektorbildungsschritt verarbeitet, um die digitalen Eingangsdaten hinsichtlich einer vorher festgelegten Datenmenge zu unterteilen, einem Datenkopfanhängungsschritt, um den Datenkopf anzuhängen, einen Fehlerkorrektur-Codierschritt, einem Modulationsschritt zum Modulieren gemäß einem vorher festgelegten Modulationssystem, und einem Synchronisationsanhängungsschritt, um das Synchronisationsmuster anzuhängen, und die resultierenden Schlüsseldaten werden ausgegeben, so dass der besondere Schritt, in welchem das Verschlüsseln durchgeführt wurde, auch zum Schritt zum Verschlüsseln wird, wodurch der Grad der Leichtigkeit oder die Schwierigkeit beim Verschlüsseln angehoben wird. Der Verschlüsselungsschritt zum zufallsbedingten Anordnen der Daten zum Beseitigen des gleichen Musters kann außerdem in den Verschlüsselungsschritten enthalten sein. Es gibt außerdem ein Verdienst, dass die Verschlüsselung leicht dadurch realisiert werden kann, indem das Teil der vorher existierenden Konfiguration modifiziert wird. Diese Effekte können mit dem Datenaufzeichnungsgerät, dem Aufzeichnungsträger, dem Datenwiedergabeverfahren oder dem Datenwiedergabegerät realisiert werden.

[0131] Da die Datenumsetzung bezüglich zumindest eines Bereichs der Daten durchgeführt wird, die während der Fehlerkorrektur-Codierung gehandhabt werden, kann in Abhängigkeit von der Schlüsselinformation zum Verschlüsseln das Verschlüsseln eines gewünschten Werts zwischen dem Wert, für welchen

die Datenwiederherstellung möglich ist, bis zu einem gewissen Ausmaß, durch die Fehlerkorrektur-Codierung, und einem Wert, für welchen die Datenwiederherstellung nicht möglich ist, realisiert werden. Dies macht es eine Steuerung möglich, bei der die Reproduktion möglich ist oder nicht, hinsichtlich eines akzeptabeln Fehlerzustands oder eines nichtakzeptablen Fehlerzustands, wodurch eine Unterbringen gemäß der Verwendung von Daten oder Sicherheitspegels ermöglicht wird.

[0132] Außerdem wird das Verschlüsseln mit einer großen Anzahl von Verschlüsselungsbits bei der Fehlerkorrektur möglich, und das Verschlüsseln wird in einer riesigen schwarzen Box, beispielsweise Fehlerkorrektur-Codierung oder Decodierungs-IC oder LSI durchgeführt, wodurch es für den allgemeinen Benutzer schwierig wird, das Verschlüsseln zu decodieren, wodurch signifikant die Datensicherheit angehoben wird.

[0133] Zusätzlich werden Daten unter Verwendung der vorher festgelegten Verschlüsselungsinformation verschlüsselt und zumindest ein Bereich der Verschlüsselungsinformation zum Verschlüsseln wird in einen Bereich geschrieben, der vom Datenaufzeichnungsbereich auf dem Aufzeichnungsträger verschieden ist, so dass dieser Bereich der Verschlüsselungsinformation während der Reproduktion gelesen wird und zum Entschlüsseln verwendet wird. Die Schlüsselinformation ist nicht innerhalb der Information im Datenaufzeichnungsbereich des Aufzeichnungsträgers abgeschlossen, wodurch die Verschlüsselungsschwierigkeit ansteigt.

[0134] Während des Verschlüsselungsbetriebs, der hauptsächlich durch zufallsbedingtes Anordnen der Daten vorgenommen wird, um die gleichen Muster in der Datenfolge zu entfernen, wird zumindest eines des Erzeugungspolynoms oder des Anfangswerts als Antwort auf den Verschlüsselungsschlüssel geändert, so dass das vorher existierende Verschlüsseln unmittelbar zum Verschlüsseln verwendet wird, um das Verschlüsseln durch einen vereinfachten Aufbau zu realisieren.

[0135] Durch das oben beschriebene Datenverschlüsseln kann das Verhindern eines Kopierens oder einer illegalen Verwendung durch eine vereinfachten Aufbau durchgeführt werden, während die Anwendung bezüglich Sicherheit oder des Belastungssystems leicht realisiert werden kann.

[0136] Die vorliegende Erfindung ist nicht auf die oben beschriebenen Ausführungsformen beschränkt. Beispielsweise kann die Datenumsetzung auch durch Bit-Addition oder durch eine Veränderung von logischen Operationen zusätzlich durch die Inverter oder die ExOR-Schaltungen wie oben beschrieben sein. Eine Vielzahl von Verschlüsselungsverfahren, beispielsweise Datensubstitution oder Vertauschung als Antwort auf die Verschlüsselungsschlüssel-Informationsumsetzung durch Schieberegister oder durch verschiedene Funktionsverarbeitungen können ebenfalls alleine oder in Kombination angewandt werden.

Patentansprüche

1. Datenaufzeichnungsverfahren, welches aufweist:
einen Sektorbildungsschritt zum Unterteilen von digitalen Eingangsdaten in Form eines vorher festgelegten Datenvolumens als Einheit;
einen Datenkopf-Anhängungsschritt zum Anhängen eines Datenkopfs an die in Sektoren unterteilten Digitaldaten;
einen Fehlerkorrektur-Codierschritt zum Anhängen eines Fehlerkorrekturcodes an die Digitaldaten, an welche der Datenkopf angehängt wurde;
einen Modulationsschritt zum Modulieren der fehlerkorrigierten codierten Digitaldaten gemäß einem vorher festgelegten Modulationssystem;
einen Synchronisationsanhängungsschritt zum Anhängen eines Synchronisationsmusters an das modulierte Digitalsignal; und
einen Aufzeichnungsschritt zum Aufzeichnen des Digitalsignals, an welches das Synchronisationsmuster angehängt wurde, auf einem Aufzeichnungsträger;
dadurch gekennzeichnet, dass
ein Eingangssignal in zumindest einem vom Sektorbildungsschritt, vom Datenkopfanhängungsschritt, vom Fehlerkorrektur-Codierschritt, vom Modulationsschritt und vom Synchronisationsanhängungsschritt verschlüsselt wird und die resultierenden verschlüsselten Daten ausgegeben werden, wobei mehrere Arten von Schlüsselinformation bei diesem Verschlüsseln verwendet werden und festgelegt werden und in einem vorher festgelegten Zeitablauf umgeschaltet werden.

2. Datenaufzeichnungsverfahren nach Anspruch 1, welches außerdem einen Verschlüsselungsschritt zum zufallsbedingten Anordnen der Digitaldaten, welche in Sektoren im Sektorbildungsschritt unterteilt wurden, oder der Digitaldaten, an welche der Datenkopf im Datenkopfanhängungsschritt angehängt wurde, aufweist, um das gleiche Muster zu beseitigen; wobei ein Eingangssignal in zumindest einem vom Sektorbildungsschritt, Datenkopfanhängungsschritt, Fehlerkorrektur-Codierschritt, Modulationsschritt, Synchronisationsanhängungsschritt und dem Verschlüsselungsschritt verschlüsselt wird und die resultierenden verschlüsselten Daten ausgegeben werden.

3. Datenaufzeichnungsverfahren nach Anspruch 1, wobei in welchem einen vom Sektorbildungsschritt, vom Datenkopfanhängungsschritt, vom Fehlerkorrektur-Codierschritt, vom Modulationsschritt

und vom Synchronisationsanhängungsschritt das Verschlüsseln durchgeführt wurde, dies als die Schlüsselinformation verwendet wird.

4. Datenaufzeichnungsverfahren nach Anspruch 1, wobei von Daten, welche während der Fehlerkorrekturcodierung des Fehlerkorrektur-Codierschritts gehandhabt wurden, zumindest der Teil, der mit der Schlüsselinformation zum Verschlüsseln übereinstimmt, mit Datenumsetzung verarbeitet wird.

5. Datenaufzeichnungsverfahren nach Anspruch 1, wobei der Fehlerkorrekturcode der Produktcode ist.

6. Datenaufzeichnungsgerät, welches aufweist:
eine Sektorbildungseinrichtung (**13**) zum Unterteilen von digitalen Eingangsdaten in Form eines vorher festgelegten Datenvolumens als Einheit;
eine Datenkopf-Anhängungseinrichtung (**15**) zum Anhängen eines Datenkopfs an die Digitaldaten, welche durch die Sektorbildungseinrichtung (**13**) ausgegeben werden;
eine Fehlerkorrektur-Codiereinrichtung (**16**) zum Anhängen eines Fehlerkorrekturcodes an die Digitaldaten, die durch die Datenkopfanhängungseinrichtung (**15**) ausgegeben werden;
eine Modulationseinrichtung (**17**) zum Modulieren der Digitaldaten, welche durch die Datenkopf-Anhängungseinrichtung (**15**) ausgegeben werden;
eine Synchronisationsanhängungseinrichtung (**18**) zum Anhängen eines Synchronisationsmusters an das Digitalsignal, weiches durch die Modulationseinrichtung (**17**) ausgegeben wird; und
eine Aufzeichnungseinrichtung (**19**, **20**, **21**, **22**) zum Aufzeichnen des Digitalsignals, welches durch die Modulationseinrichtung (**17**) ausgegeben wird, auf einem Aufzeichnungsträger (**21**); dadurch gekennzeichnet, dass
zumindest eine von der Sektorbildungseinrichtung, der Datenkopf-Anhängungseinrichtung, der Fehlerkorrektur-Codiereinrichtung, der Modulationseinrichtung und der Synchronisationsmuster-Anhängungseinrichtung ein Eingangssignal verschlüsselt und die resultierenden verschlüsselten Daten ausgibt, wobei mehrere Arten von Schlüsselinformation bei dem diesem Verschlüsseln verwendet werden und festgelegt sind und mit einem vorher festgelegten Zeitablauf umgeschaltet werden.

7. Datenaufzeichnungsgerät nach Anspruch 6, welches außerdem eine Verschlüsselungseinrichtung (**14**) aufweist, um die Digitaldaten, welche in Sektoren durch die Sektorbildungseinrichtung unterteilt sind, oder die Digitaldaten, denen der Datenkopf durch die Datenkopf-Anhängungseinrichtung angehängt wurde, zufallsbedingt anzuordnen, um das gleiche Muster zu beseitigen; wobei ein Eingangssignal durch zumindest eine von der Sektorbildungseinrichtung, der Datenkopfanhängungseinrichtung, der Fehlerkorrektur-Codiereinrichtung, der Modulationseinrichtung, der Synchronisationsanhängungseinrichtung und der Verschachtelungseinrichtung verschlüsselt wird und die resultierenden verschlüsselten Daten ausgegeben werden.

8. Datenaufzeichnungsgerät nach Anspruch 7, welches außerdem eine Datenumsetzungseinrichtung aufweist, um zumindest den Teil von Daten umzusetzen, welche in dem Fehlerkorrektur-Codierzeitpunkt gehandhabt werden und welche mit der Schlüsselinformation zum Verschlüsseln übereinstimmen.

9. Datenaufzeichnungsträger, auf welchem Daten aufgezeichnet sind, die durch Bilden von digitalen Eingangsdaten zu Sektoren in Form eines vorher festgelegten Datenvolumens als Einheit, durch Anhängen eines Datenkopfs an jeden Sektor und durch Verarbeiten resultierender Daten mit Datenkopfanhängung, Fehlerkorrektur und Codierung, durch Modulation gemäß einem vorher festgelegten Modulationssystem und Anhängen eines Synchronisationsmusters erhalten werden, wobei die resultierenden verarbeiteten Daten dann im Zeitpunkt der Sektorbildung, der Datenkopfanhängung, der Fehlerkorrektur und Codierung, der Modulation oder des Anhängens des Synchronisationsmusters verschlüsselt werden, wobei das Verschlüsseln unter Verwendung mehrerer Arten von Schlüsselinformation durchgeführt wird, welche in einem vorher festgelegten Zeitablauf umgeschaltet werden, wobei die mehreren Arten von Schlüsselinformation als Teil der aufgezeichneten Daten enthalten sind.

10. Datenwiedergabeverfahren, welches aufweist:
einen Synchronisationstrennungsschritt, um ein Synchronisationssignal von einem Digitalsignal zu trennen, welches von einem Datenaufzeichnungsträger ausgelesen wird;
einen Demodulationsschritt, um das Digitalsignal, welches vom Synchronisationssignal getrennt wurde, gemäß einem vorher festgelegten Demodulationssystem zu demodulieren;
einen Fehlerkorrektur-Decodierschritt zum Fehlerkorrigieren und zum Decodieren der demodulierten Digitaldaten;
einen Sektoranalysierungsschritt, um die fehlerkorrigierten und decodierten Digitaldaten in vorher festgelegten Sektoren zu analysieren; und
einen Datenkopftrennungsschritt, um einen Datenkopfteil einer Sektorstruktur der Digitaldaten zu trennen, welche in Sektoren analysiert wurden;
wobei ein Eingangssignal in einem Schritt zum Aufzeichnen in Verbindung mit zumindest einem vom Synchronisationstrennungsschritt, vom Demodulationsschritt, vom Fehlerkorrektur-Decodierschritt, vom Sektoranalysierungsschritt oder vom Datenkopftrennungsschritt verschlüsselt wurde;

dadurch gekennzeichnet, dass
das Eingangssignal in einem Schritt zur Wiedergabe in Verbindung mit dem Schritt zum Aufzeichnen, in welchem das Verschlüsseln im Aufzeichnungszeitpunkt durchgeführt wurde, entschlüsselt wird, wobei mehrere Arten der Verschlüsselungsinformation, die bei der Verschlüsselung verwendet wird, festgesetzt werden und mit einem vorher festgelegten Zeitablauf umgeschaltet werden, wobei das Verschlüsseln die mehreren Schlüsselinformationen gemäß dem vorher festgelegten Zeittakt verwendet.

11. Datenwiedergabeverfahren nach Anspruch 10, welches außerdem einen Entschachtelungsschritt aufweist, um Digitaldaten, welche im Aufzeichnungspunkt verschachtelt wurden, zu entschachteln, wobei die Digitaldaten in Sektoren im Sektoranalysierungsschritt analysiert wurden oder vom Datenkopf im Datentrennungsschritt getrennt wurden; wobei ein Eingangssignal in einem Schritt zum Aufzeichnen in Verbindung mit zumindest einem vom Synchronisationstrennungsschritt, vom Modulationsschritt, vom Fehlerkorrektur-Decodierschritt, vom Sektoranalysierungsschritt, vom Datenkopftrennungsschritt oder vom Entschachtelungsschritt entschachtelt wurde, und wobei die Eingangsdaten in einem Schritt zur Wiedergabe in Verbindung mit dem Schritt zur Aufzeichnung entschlüsselt werden, bei dem das Verschlüsseln im Aufzeichnungszeitpunkt getan wurde.

12. Datenwiedergabegerät, welches aufweist:
eine Synchronisationstrenneinrichtung (**114**), um ein Synchronisationssignal von einem Digitalsignal zu trennen, welches von einem Datenaufzeichnungsträger (**101**) gelesen wird;
eine Demodulationseinrichtung (**115**), um das Digitalsignal, welches durch die Synchronisationstrenneinrichtung ausgegeben wird, gemäß einem vorher festgelegten Demodulationssystem zu demodulieren;
eine Fehlerkorrektur-Decodiereinrichtung (**116**) zur Fehlerkorrektur, und zum Decodieren der Digitaldaten, welche durch die Demodulationseinrichtung (**115**) ausgegeben werden;
eine Sektoranalysierungseinrichtung (**117**), um die Digitaldaten, welche durch Fehlerkorrektur-Decodiereinrichtung (**116**) ausgegeben werden, in vorher festgelegten Sektoren zu analysieren; und
eine Datenkopftrenneinrichtung (**118**), um ein Datenkopfteil einer Sektorstruktur der Digitaldaten, die durch die Sektortrenneinrichtung (**117**) ausgegeben werden, zu trennen;
dadurch gekennzeichnet, dass
ein Eingangssignal verschlüsselt wurde in einem Schritt zum Aufzeichnen in Verbindung mit zumindest einer von der Synchronisationstrenneinrichtung (**114**), der Demodulationseinrichtung (**115**), der Fehlerkorrektur-Decodiereinrichtung (**116**), der Sektoranalysierungseinrichtung (**117**) und der Datenkopftrenneinrichtung (**118**); und wobei
das Eingangssignal durch eine Einrichtung zur Reproduktion in Verbindung mit dem Schritt zum Aufzeichnen entschlüsselt wird, in welcher das Verschlüsseln im Aufzeichnungszeitpunkt gemacht wurde, wobei mehrere Arten der Schlüsselinformation, welche beim Verschlüsseln verwendet werden, festgelegt sind und mit einem vorher festgelegten Zeitablauf umgeschaltet werden, wobei das Entschlüsseln die mehreren Schlüsselinformationen gemäß dem vorher festgelegten Zeitablauf verwendet.

13. Datenwiedergabegerät nach Anspruch 12, welches außerdem eine Entschachtelungseinrichtung aufweist, um Digitaldaten im Aufzeichnungszeitpunkt zu entschachteln, wobei die Digitaldaten durch die Sektoranalysierungseinrichtung oder die Datenkopftrenneinrichtung ausgegeben werden, wobei ein Eingangssignal durch eine Einrichtung zum Aufzeichnen in Verbindung mit zumindest einer von der Synchronisationstrenneinrichtung, der Modulationseinrichtung, der Fehlerkorrektur-Decodiereinrichtung, der Sektoranalysierungseinrichtung, der Datenkopftrenneinrichtung und der Entschachtelungseinrichtung verschlüsselt wurde; und wobei das Eingangssignal durch eine Einrichtung zur Wiedergabe in Verbindung mit der Einrichtung zur Aufzeichnung entschlüsselt wird, in welcher das Verschlüsseln im Aufzeichnungspunkt gemacht wurde.

Es folgen 29 Blatt Zeichnungen

Anhängende Zeichnungen

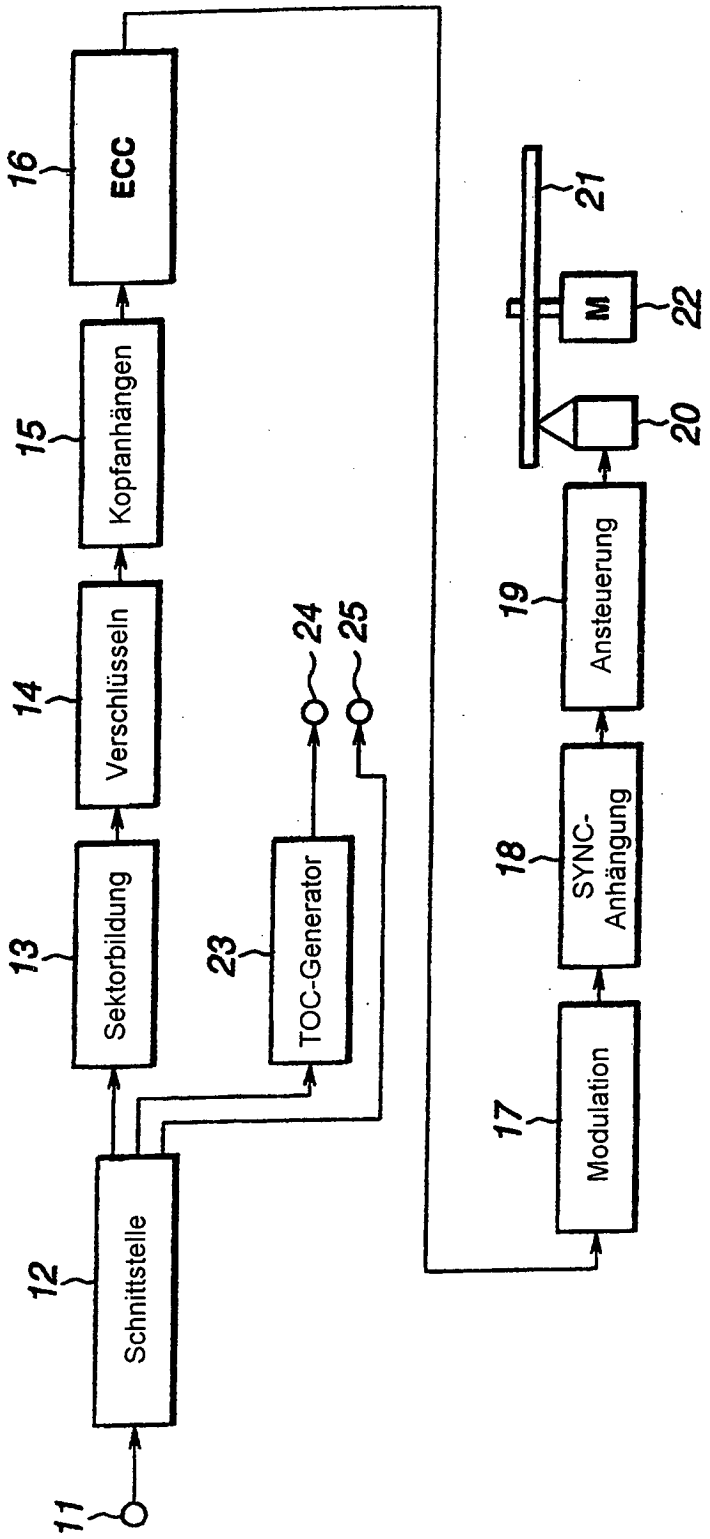

FIG.1

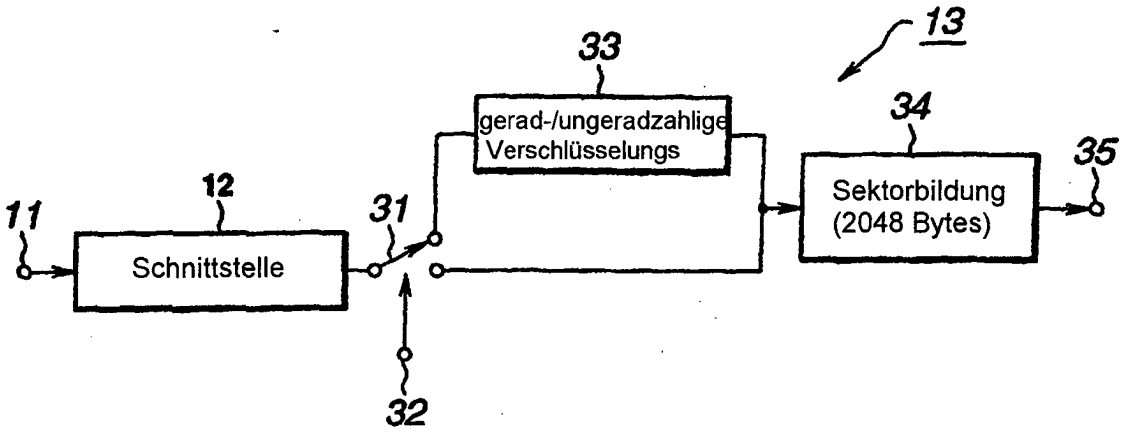
13
33
gerad-/ungeradzahlige Verschlüsselungs
34
35
Sektorbildung (2048 Bytes)
11
12
Schnittstelle
31
32

FIG.2

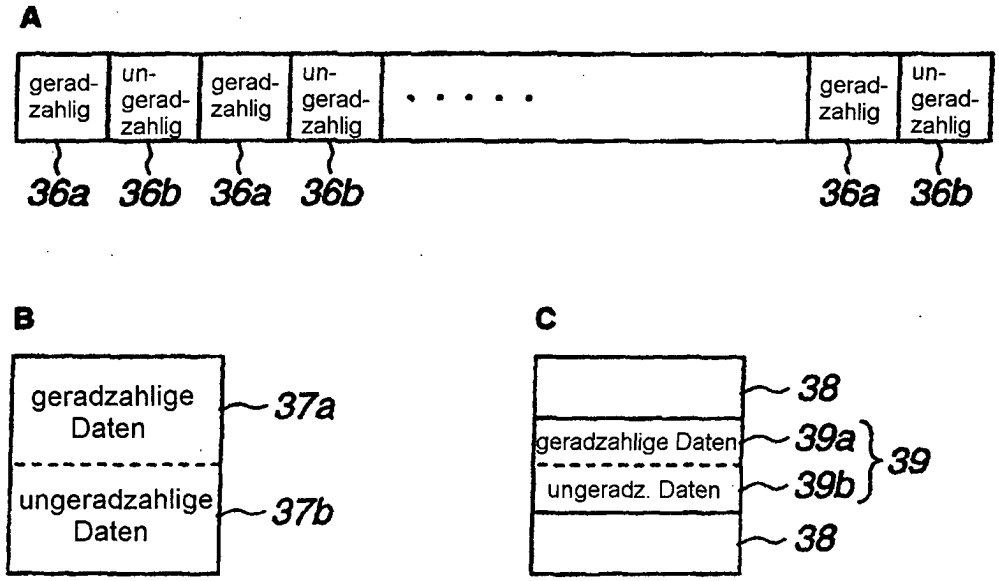
A
gerad-zahlig
un-gerad-zahlig
gerad-zahlig
un-gerad-zahlig
gerad-zahlig
un-gerad-zahlig
36a
36b
36a
36b
36a
36b
B
geradzahlige Daten
37a
ungeradzahlige Daten
37b
C
38
geradzahlige Daten
39a
ungeradz. Daten
39b
39
38

FIG.3

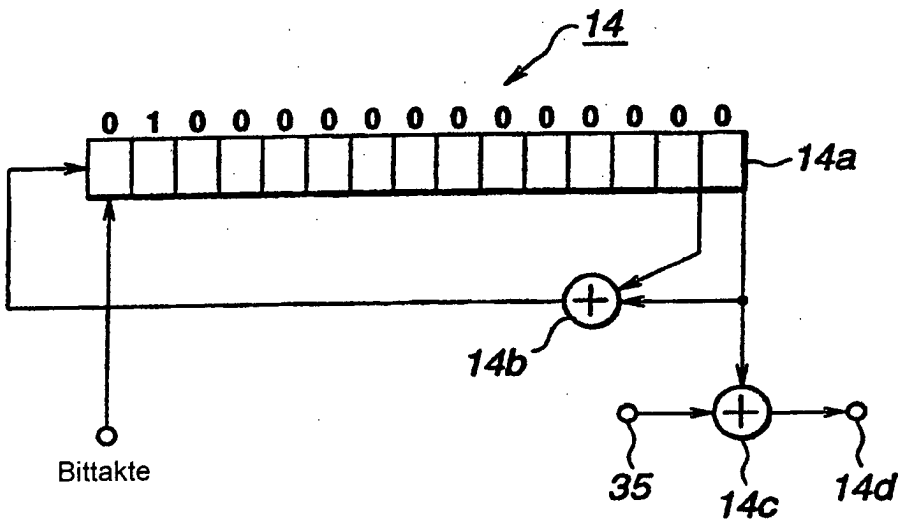

FIG.4

Auswahl-zahlen	vorher fest-gelegte Werte	Auswahl-zahlen	vorher fest-gelegte Werte
0	**$0001**	**8**	**$4080**
1	**$4000**	**9**	**$2040**
2	**$2000**	**10**	**$1020**
3	**$1000**	**11**	**$0810**
4	**$0800**	**12**	**$0408**
5	**$0400**	**13**	**$0204**
6	**$0200**	**14**	**$0102**
7	**$0100**	**15**	**$4081**

FIG.5

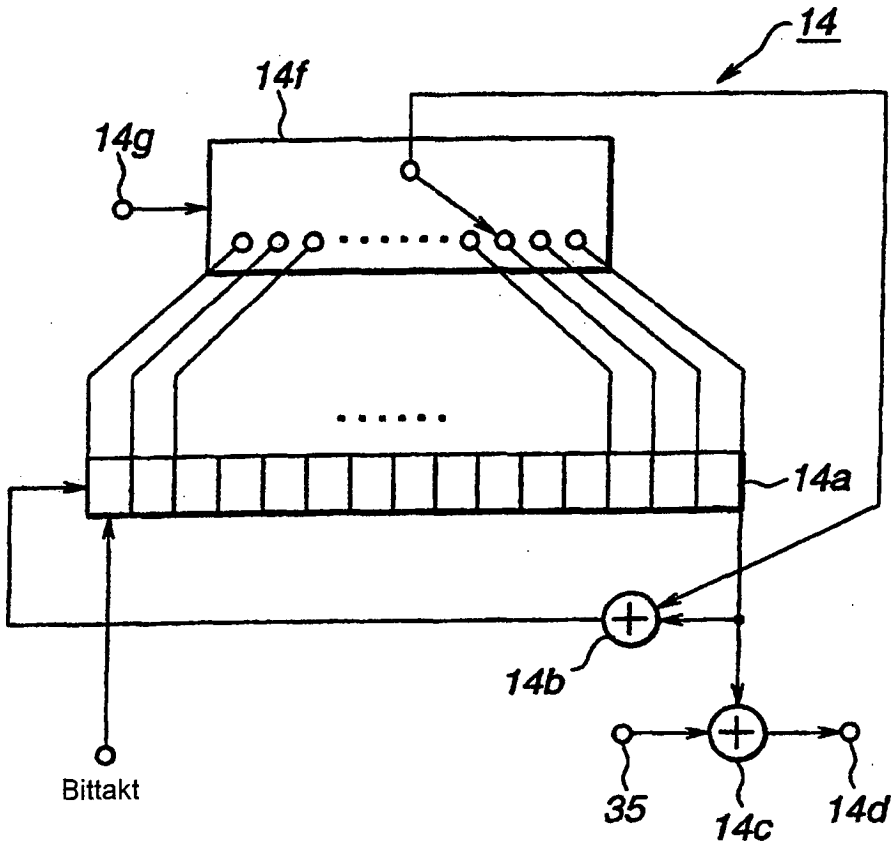

FIG.6

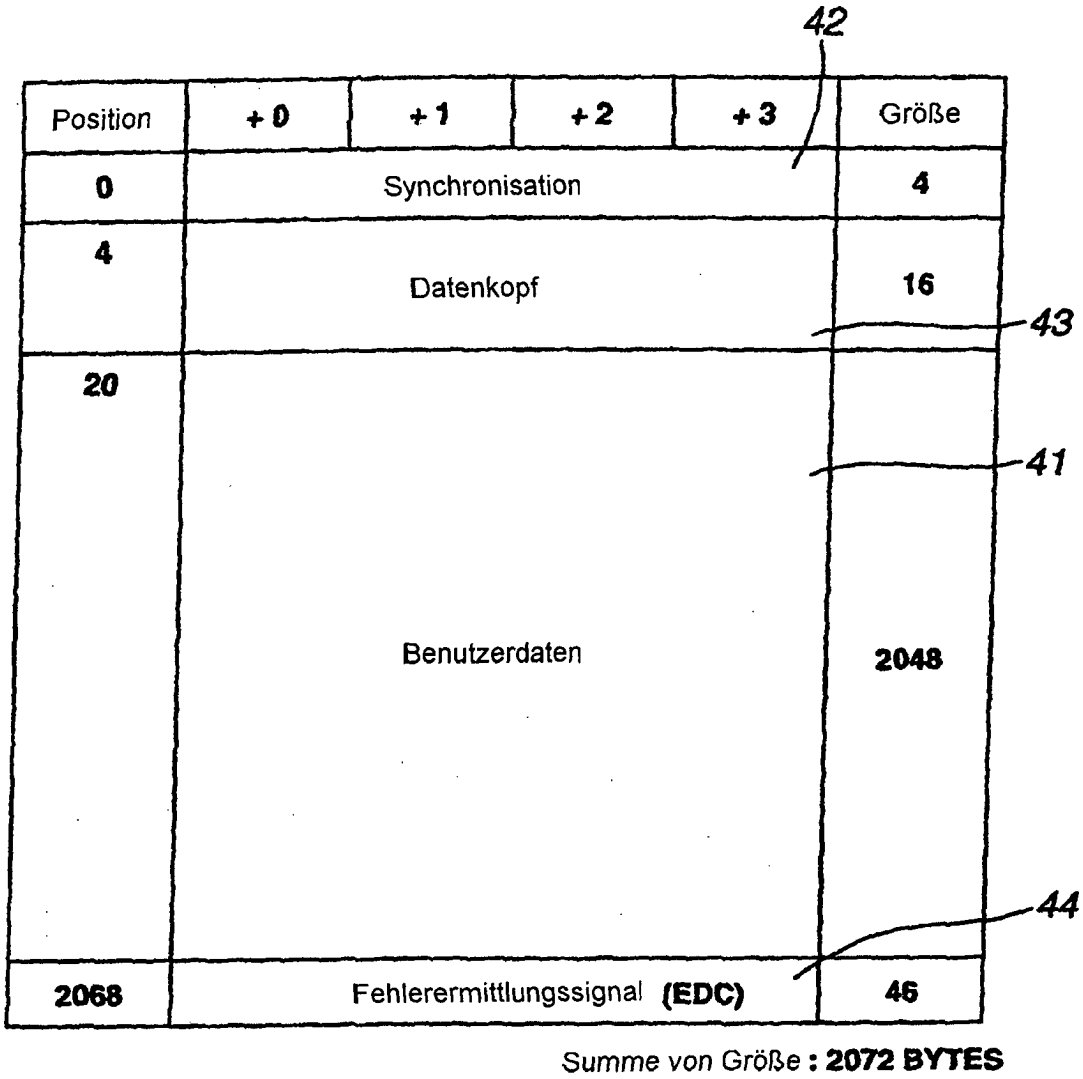
42
Position
+0
+1
+2
+3
Größe
0
Synchronisation
4
4
Datenkopf
16
43
20
41
Benutzerdaten
2048
44
2068
Fehlerermittlungssignal (EDC)
46
Summe von Größe : 2072 BYTES

FIG.7

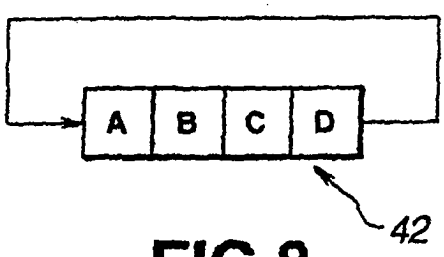
A
B
C
D
42

FIG.8

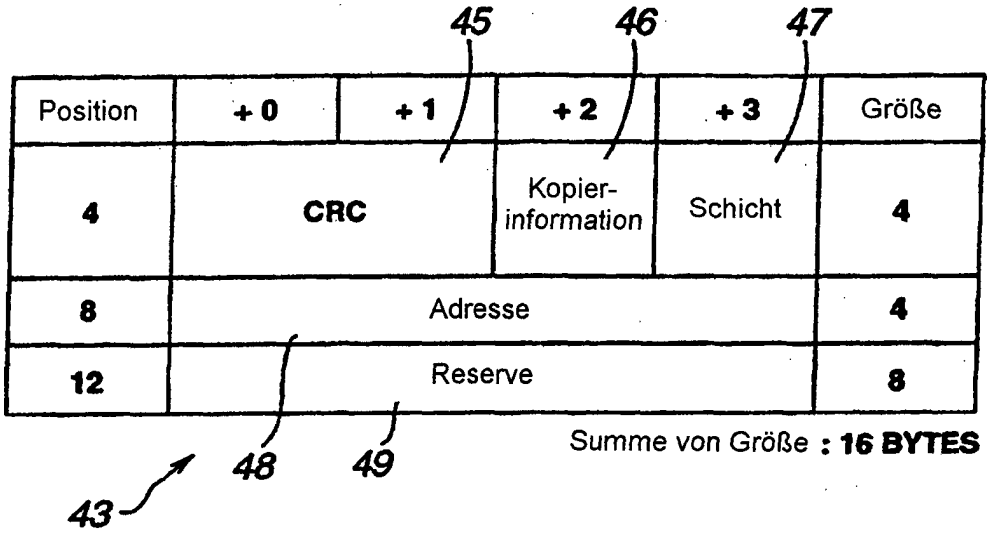
45
46
47
Position
+ 0
+ 1
+ 2
+ 3
Größe
4
CRC
Kopier-information
Schicht
4
8
Adresse
4
12
Reserve
8
Summe von Größe : 16 BYTES
48
49
43

FIG.9

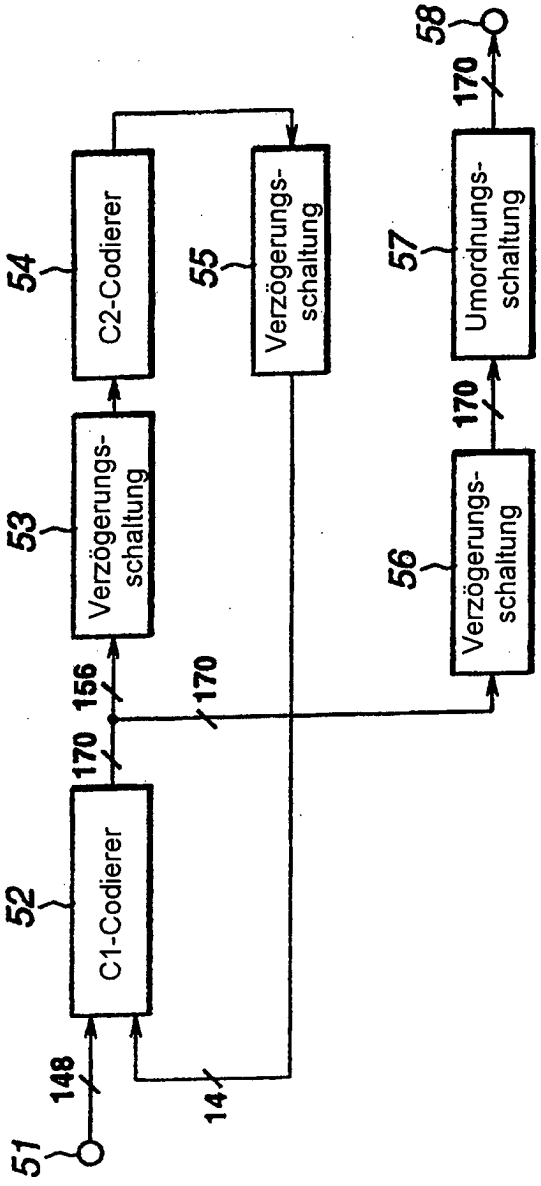
51
148
52
C1-Codierer
170
156
53
Verzögerungs-schaltung
54
C2-Codierer
14
55
Verzögerungs-schaltung
170
56
Verzögerungs-schaltung
170
57
Umordnungs-schaltung
170
58

FIG.10

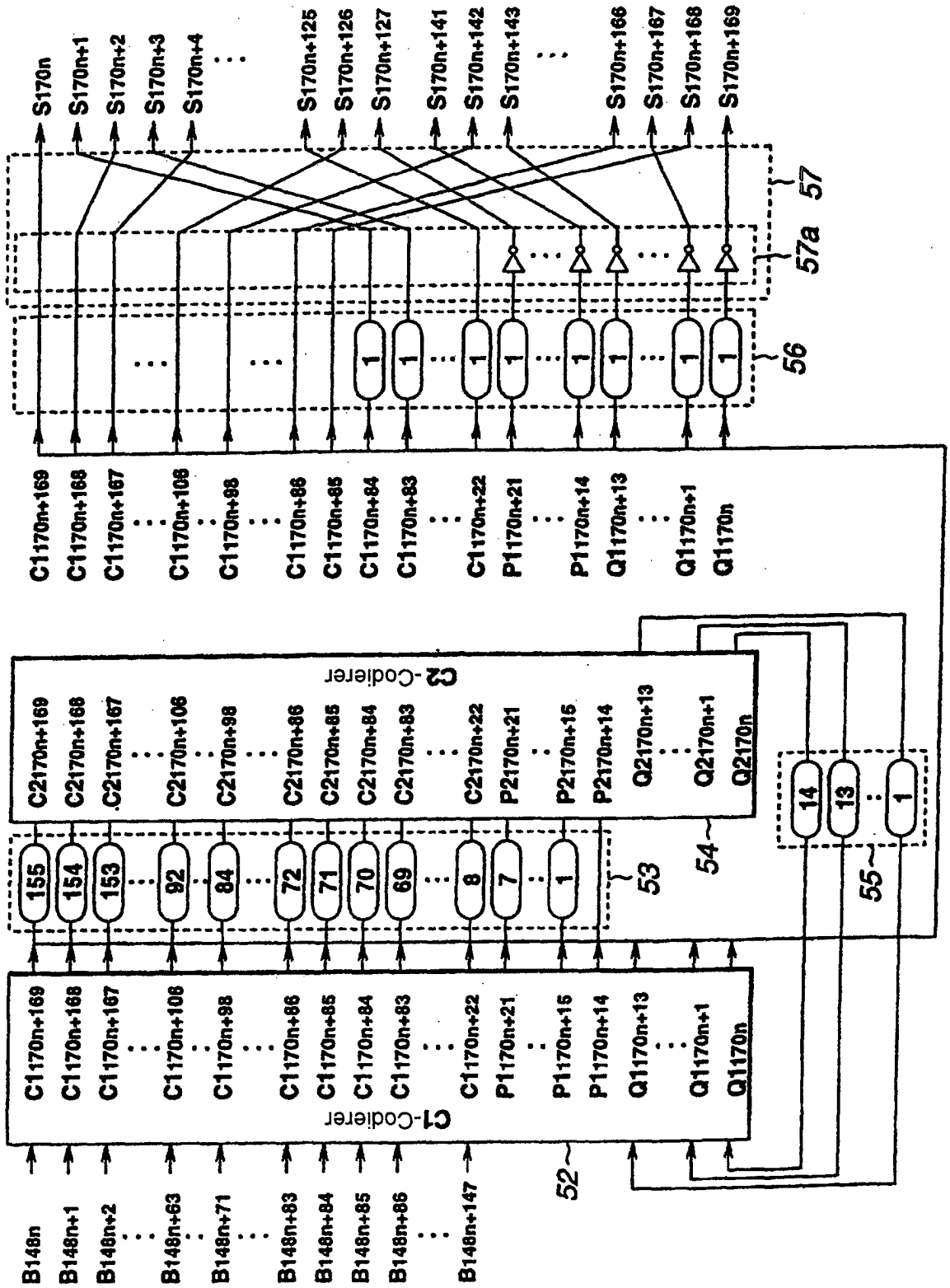
B148n
B148n+1
B148n+2
B148n+63
B148n+71
B148n+83
B148n+84
B148n+85
B148n+86
B148n+147
C1-Codierer
C2-Codierer
C1170n+169
C1170n+168
C1170n+167
C1170n+106
C1170n+98
C1170n+86
C1170n+85
C1170n+84
C1170n+83
C1170n+22
P1170n+21
P1170n+15
P1170n+14
Q1170n+13
Q1170n+1
Q1170n
C2170n+169
C2170n+168
C2170n+167
C2170n+106
C2170n+98
C2170n+86
C2170n+85
C2170n+84
C2170n+83
C2170n+22
P2170n+21
P2170n+15
P2170n+14
Q2170n+13
Q2170n+1
Q2170n
155
154
153
92
84
72
71
70
69
8
7
1
14
13
1
52
53
54
55
56
57
57a
S170n
S170n+1
S170n+2
S170n+3
S170n+4
S170n+125
S170n+126
S170n+127
S170n+141
S170n+142
S170n+143
S170n+166
S170n+167
S170n+168
S170n+169

FIG.11

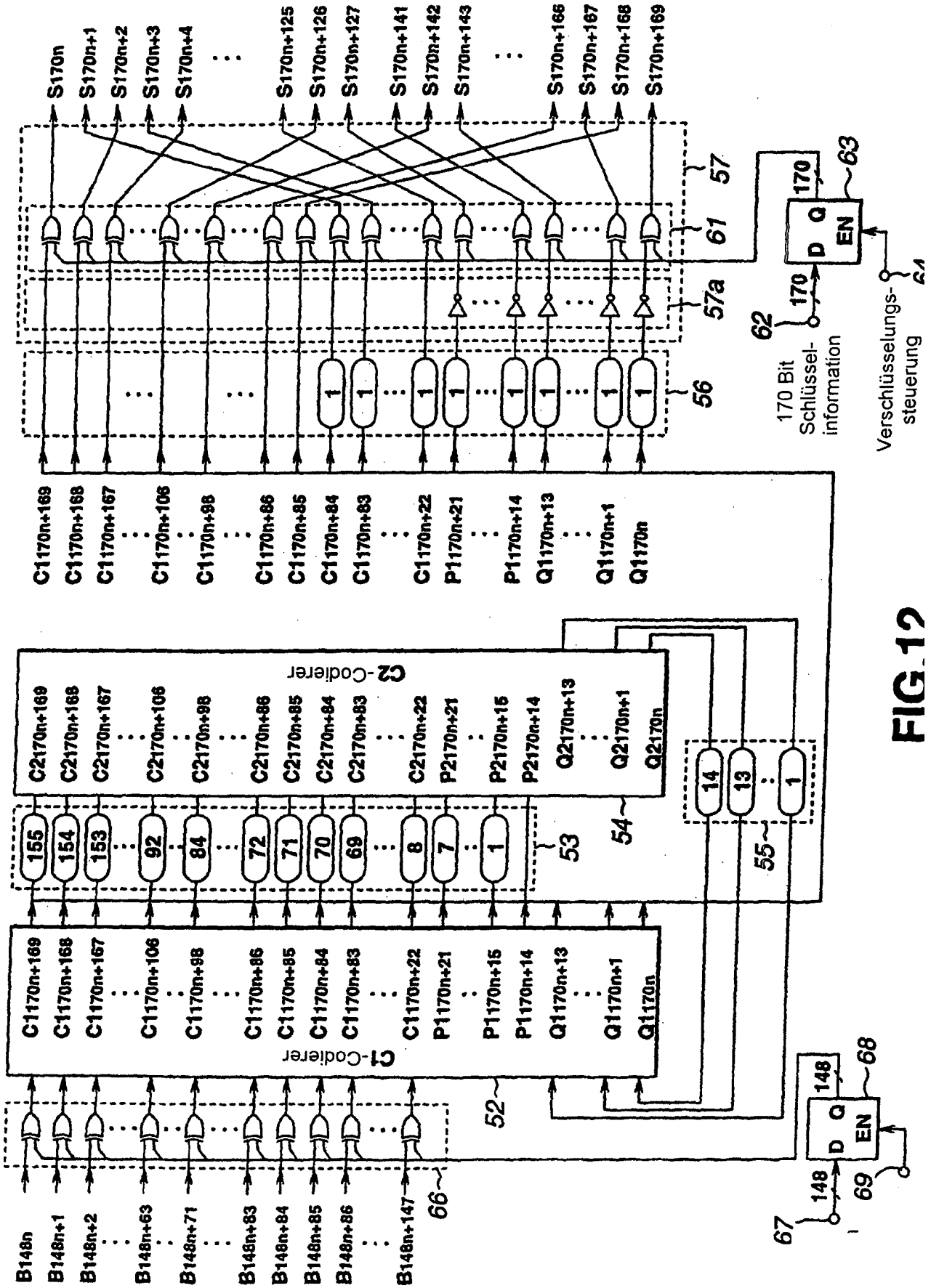
S170n
S170n+1
S170n+2
S170n+3
S170n+4
S170n+125
S170n+126
S170n+127
S170n+141
S170n+142
S170n+143
S170n+166
S170n+167
S170n+168
S170n+169
57
61
57a
56
63
62
170 Bit Schlüssel-information
Verschlüsselungs-steuerung
C1170n+169
C1170n+168
C1170n+167
C1170n+106
C1170n+98
C1170n+86
C1170n+85
C1170n+84
C1170n+83
C1170n+22
P1170n+21
P1170n+14
Q1170n+13
Q1170n+1
Q1170n
C2-Codierer
C2170n+169
C2170n+168
C2170n+167
C2170n+106
C2170n+98
C2170n+86
C2170n+85
C2170n+84
C2170n+83
C2170n+22
P2170n+21
P2170n+15
P2170n+14
Q2170n+13
Q2170n+1
Q2170n
155
154
153
92
84
72
71
70
69
8
7
1
53
54
14
13
1
55
C1-Codierer
52
68
69
67
B148n
B148n+1
B148n+2
B148n+63
B148n+71
B148n+83
B148n+84
B148n+85
B148n+86
B148n+147
66

FIG 12

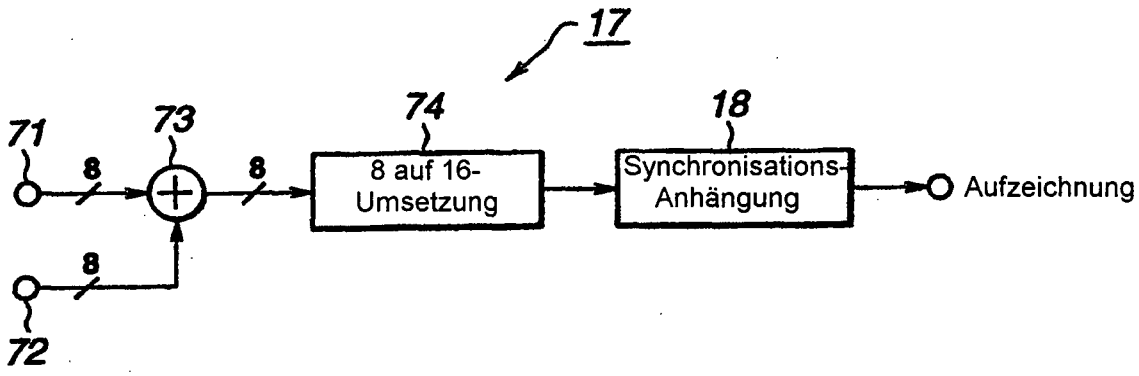
17
71
73
74
18
8
8
8 auf 16-
Umsetzung
Synchronisations-
Anhängung
Aufzeichnung
72

FIG.13

Synchronisationswörter	Codewörter			
	Synchronisationsmuster a		Synchronisationsmuster b	
	msb	**lsb**	**msb**	**lsb**
S0	**0001001001000000000010000000001**		**1001001001000000000010000000001**	
S1	**0001000001000000000010000000001**		**1001000001000000000010000000001**	
S2	**0000100001000000000010000000001**		**1000010001000000000010000000001**	
S3	**0001000001000000000010000000001**		**1000100001000000000010000000001**	

FIG.14

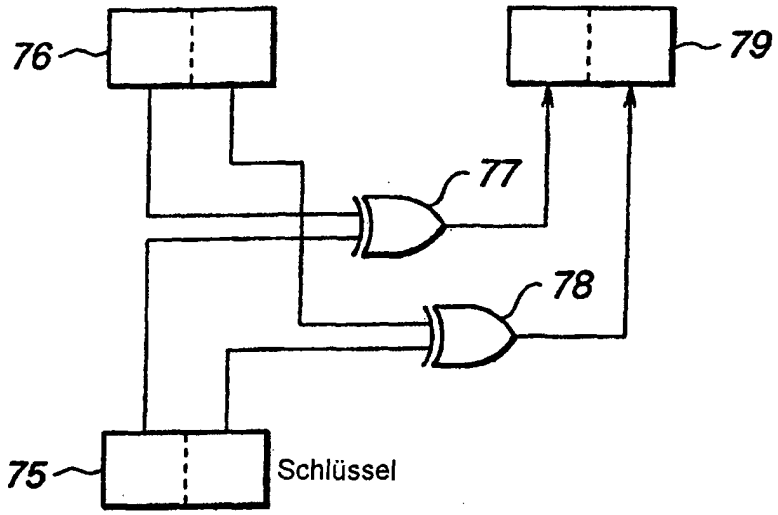

FIG.15

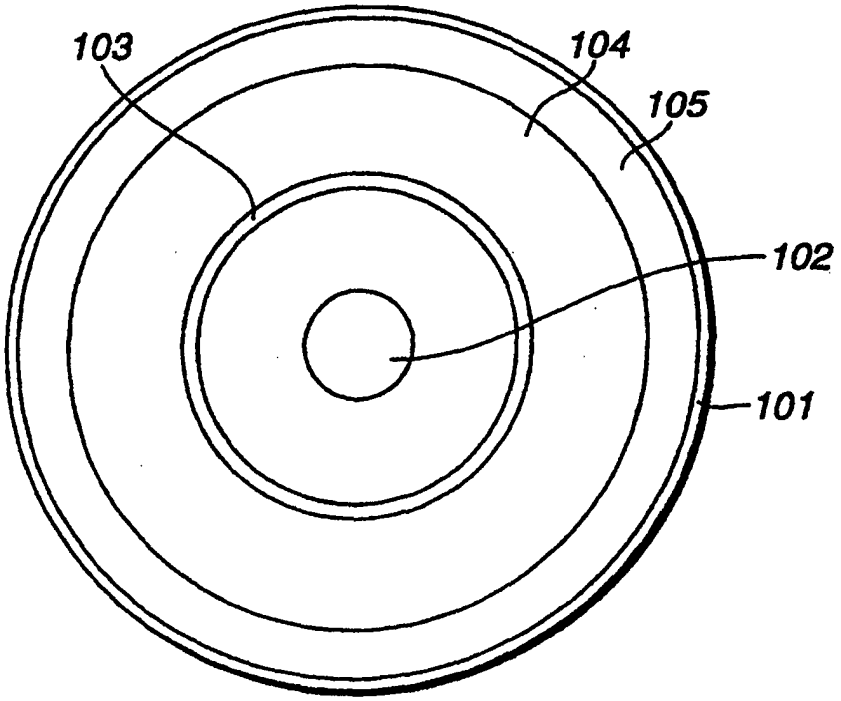

FIG.16

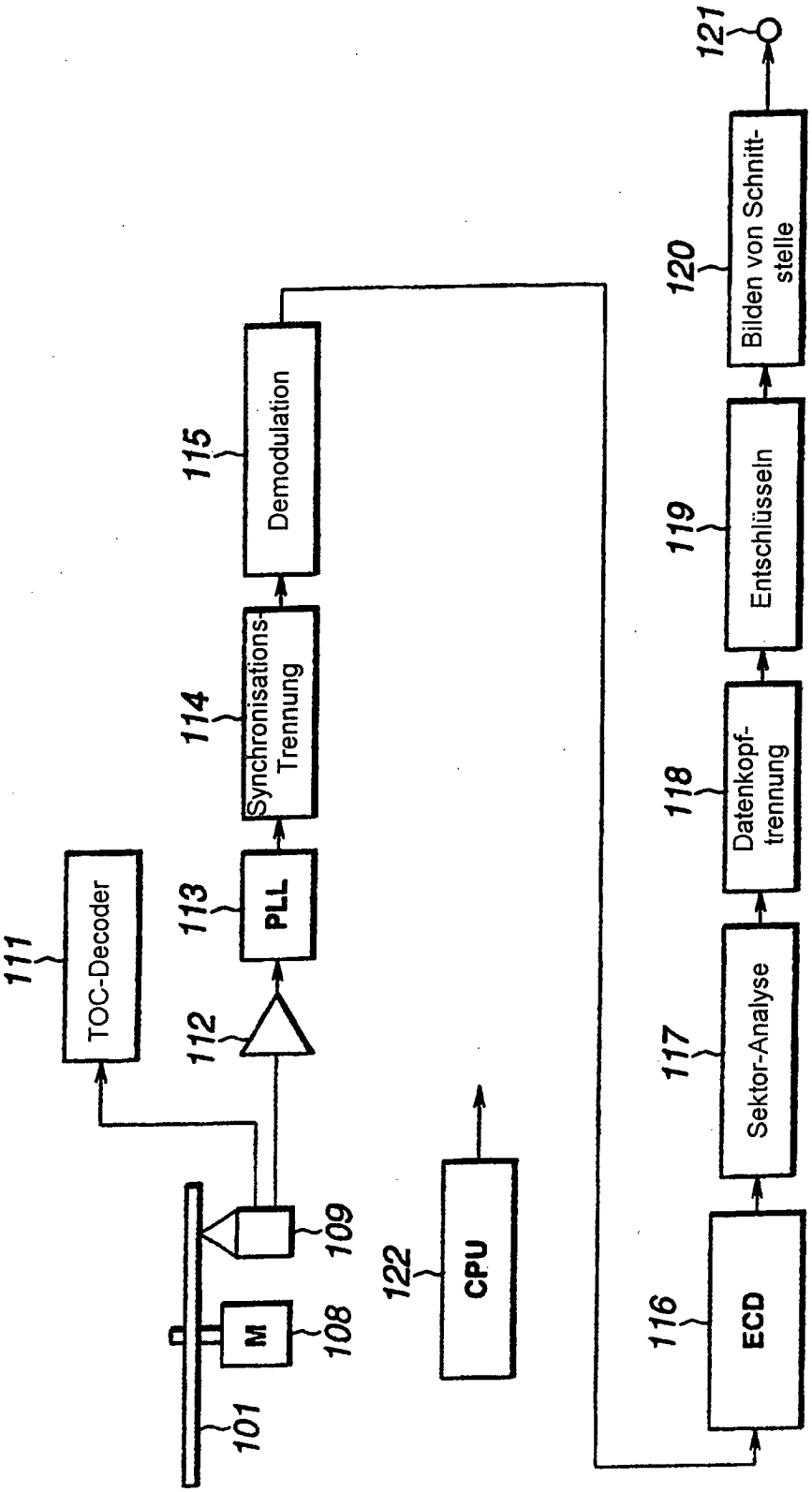
101
M
108
109
111
TOC-Decoder
112
113
PLL
114
Synchronisations-Trennung
115
Demodulation
116
ECD
117
Sektor-Analyse
118
Datenkopf-trennung
119
Entschlüsseln
120
Bilden von Schnitt-stelle
121
122
CPU

FIG.17

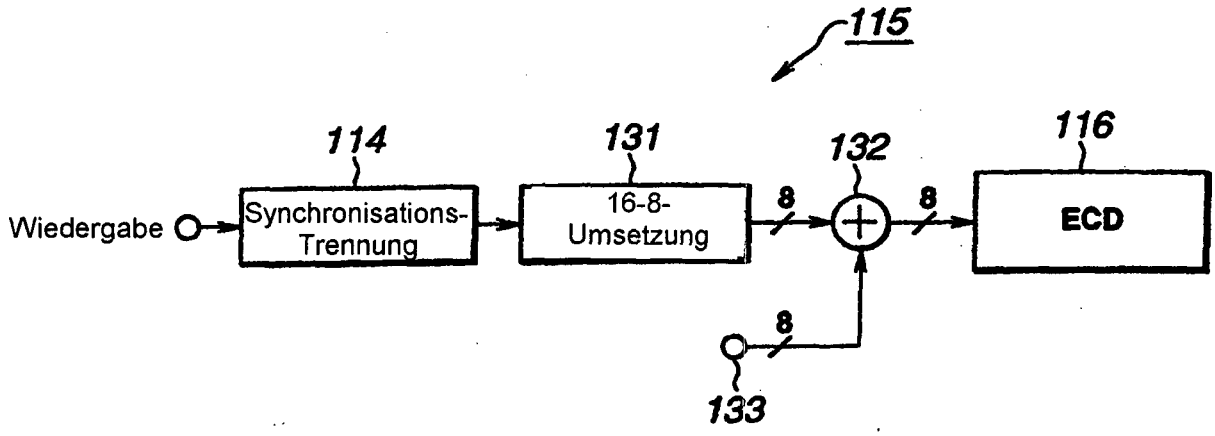
115
114
131
132
116
Wiedergabe
Synchronisations-
Trennung
16-8-
Umsetzung
8
8
ECD
8
133

FIG.18

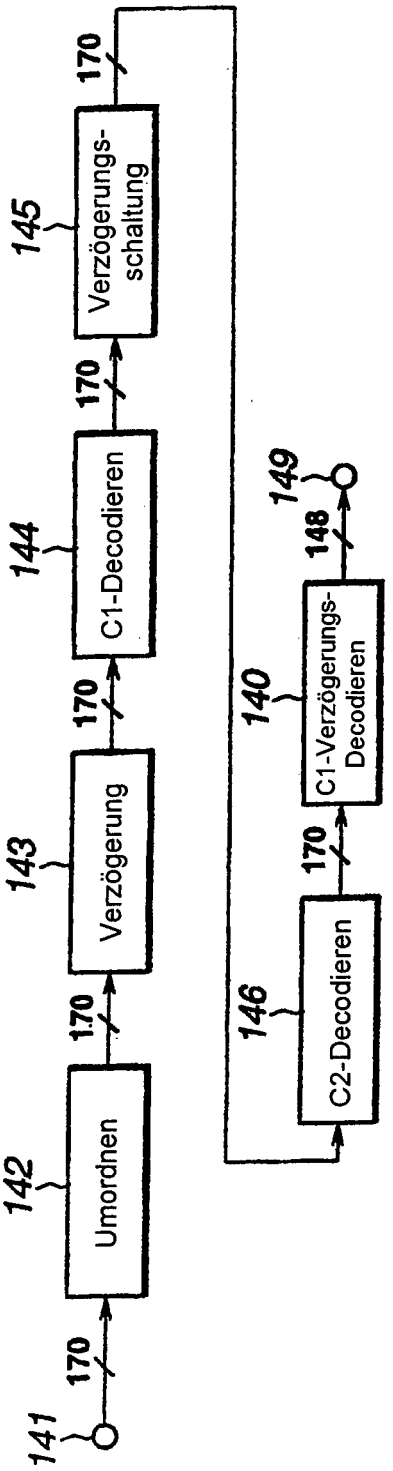
141
170
142
Umordnen
170
143
Verzögerung
170
144
C1-Decodieren
170
145
Verzögerungs-schaltung
170
146
C2-Decodieren
170
140
C1-Verzögerungs-Decodieren
148
149

FIG.19

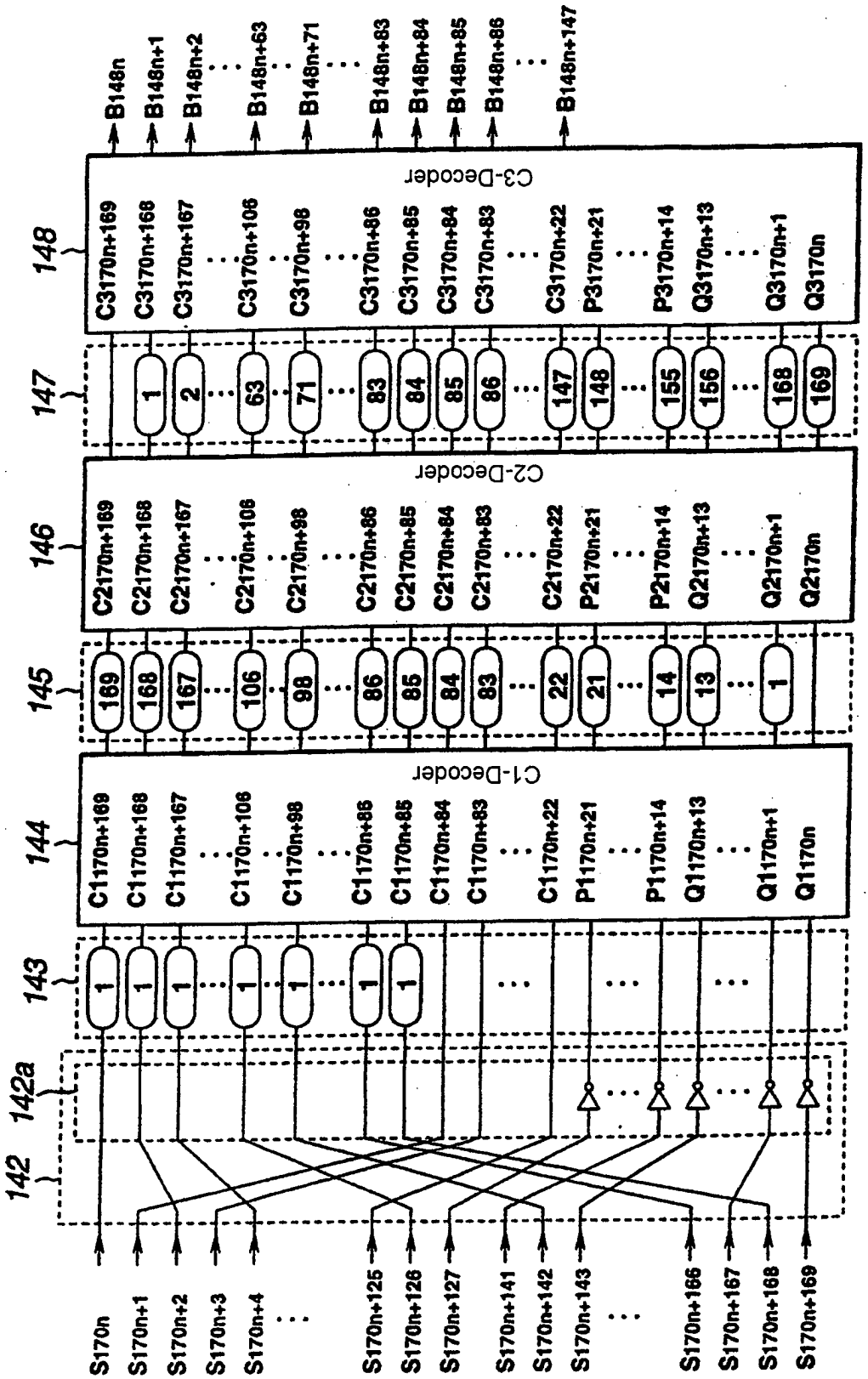
142
142a
143
144
145
146
147
148
S170n
S170n+1
S170n+2
S170n+3
S170n+4
S170n+125
S170n+126
S170n+127
S170n+141
S170n+142
S170n+143
S170n+166
S170n+167
S170n+168
S170n+169
C1-Decoder
C2-Decoder
C3-Decoder
B148n
B148n+1
B148n+2
B148n+63
B148n+71
B148n+83
B148n+84
B148n+85
B148n+86
B148n+147

FIG.20

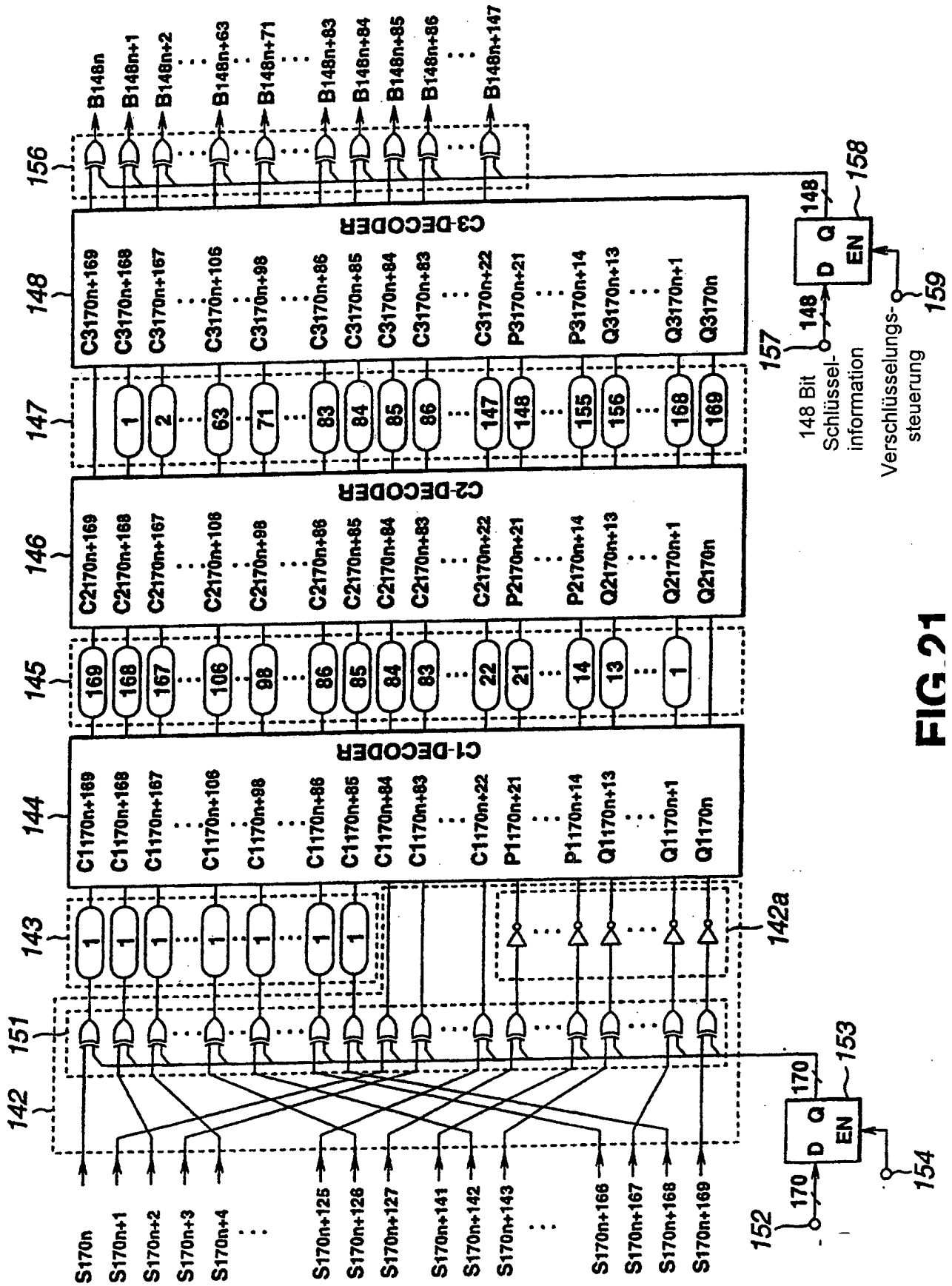
C1-DECODER
C2-DECODER
C3-DECODER
148 Bit Schlüssel-information
Verschlüsselungs-steuerung
D Q EN

FIG 21

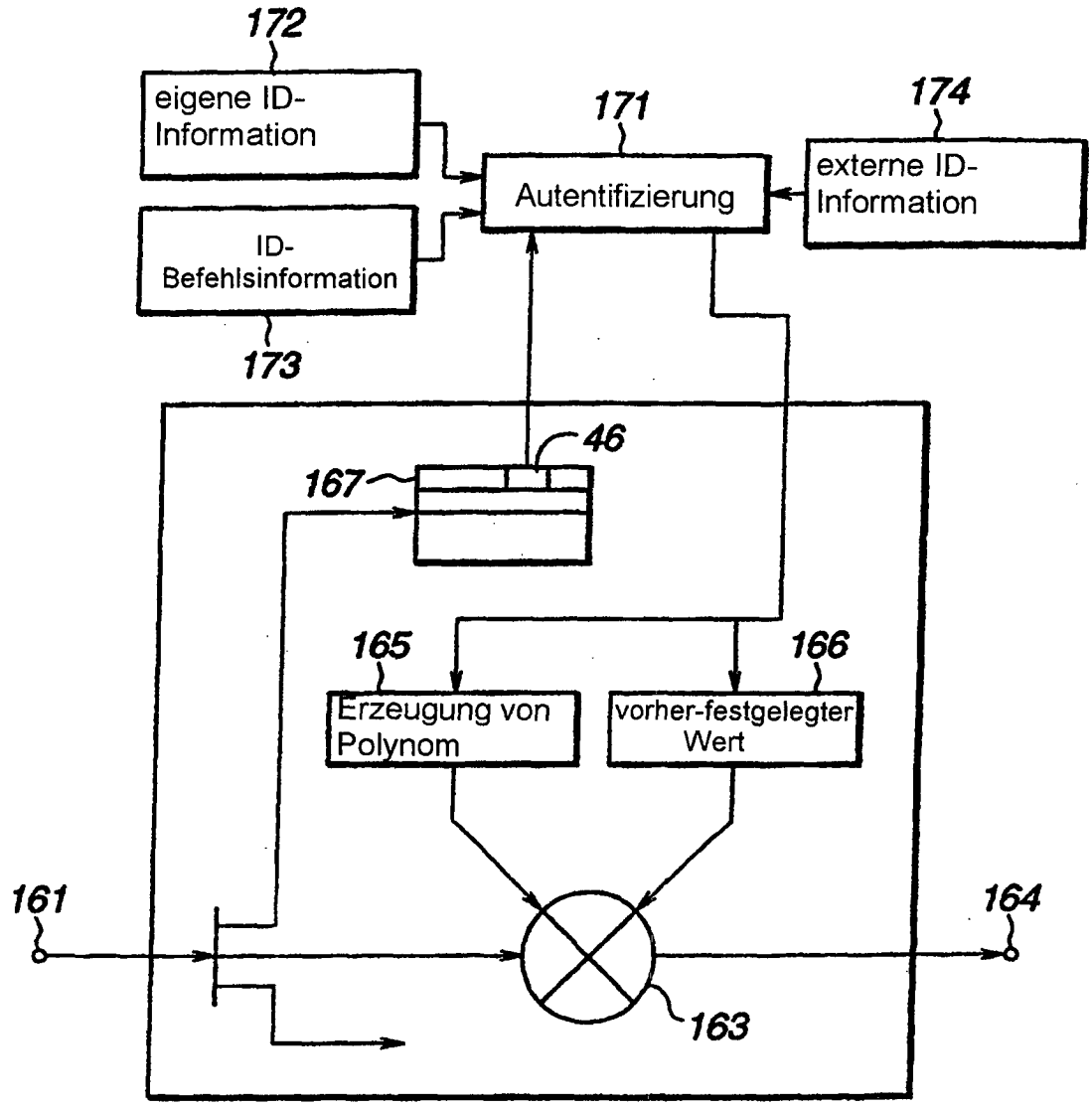
172
eigene ID-Information
171
174
Autentifizierung
externe ID-Information
ID-Befehlsinformation
173
46
167
165
166
Erzeugung von Polynom
vorher-festgelegter Wert
161
164
163

FIG.22

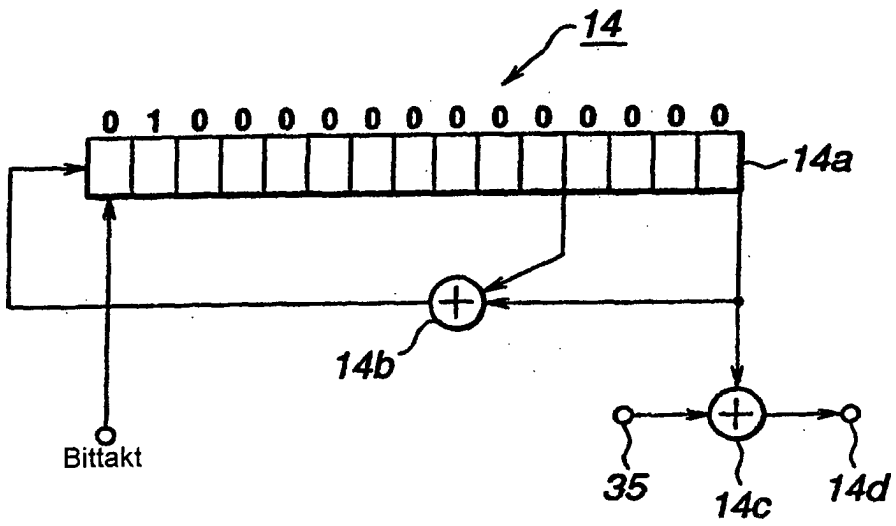

FIG.23

Auswahl-zahlen	vorher fest-gelegter Wert	Auswahl-zahlen	vorher fest-gelegter Wert
0	$0001	8	$0010
1	$5500	9	$5000
2	$0002	10	$0020
3	$2A00	11	$2001
4	$0004	12	$0040
5	$5400	13	$4002
6	$0008	14	$0080
7	$2800	15	$0005

FIG.24

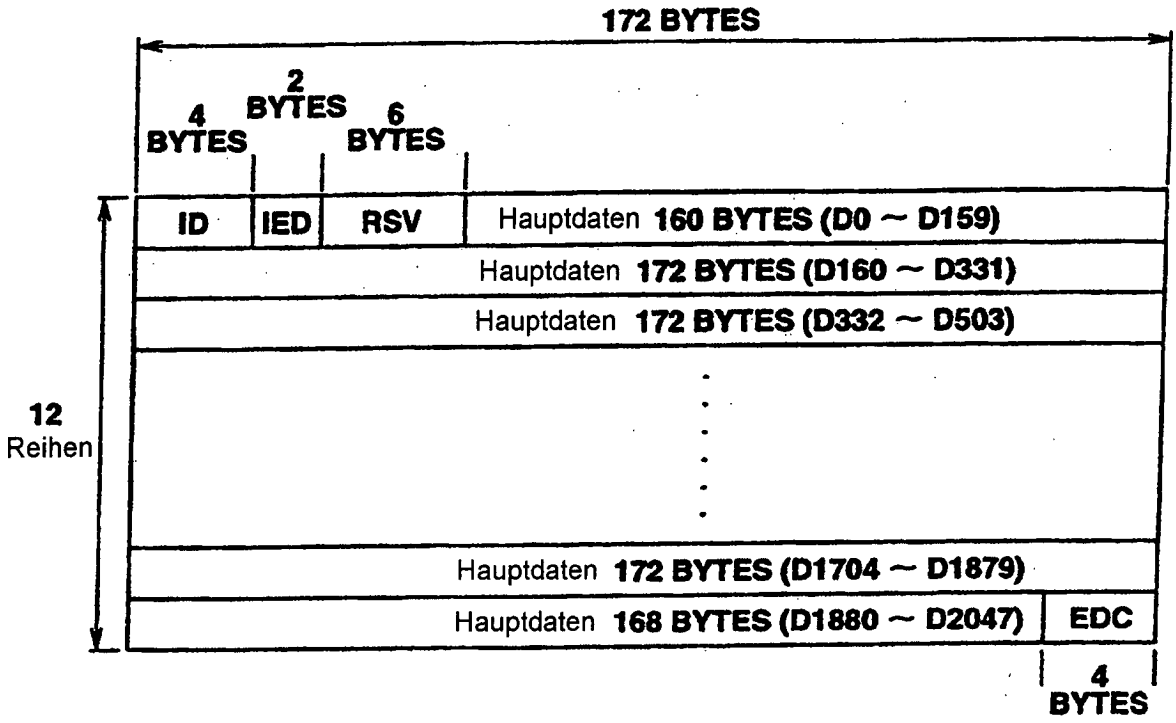
172 BYTES
4 BYTES
2 BYTES
6 BYTES
ID
IED
RSV
Hauptdaten 160 BYTES (D0 ~ D159)
Hauptdaten 172 BYTES (D160 ~ D331)
Hauptdaten 172 BYTES (D332 ~ D503)
Hauptdaten 172 BYTES (D1704 ~ D1879)
Hauptdaten 168 BYTES (D1880 ~ D2047)
EDC
4 BYTES
12 Reihen

FIG.25

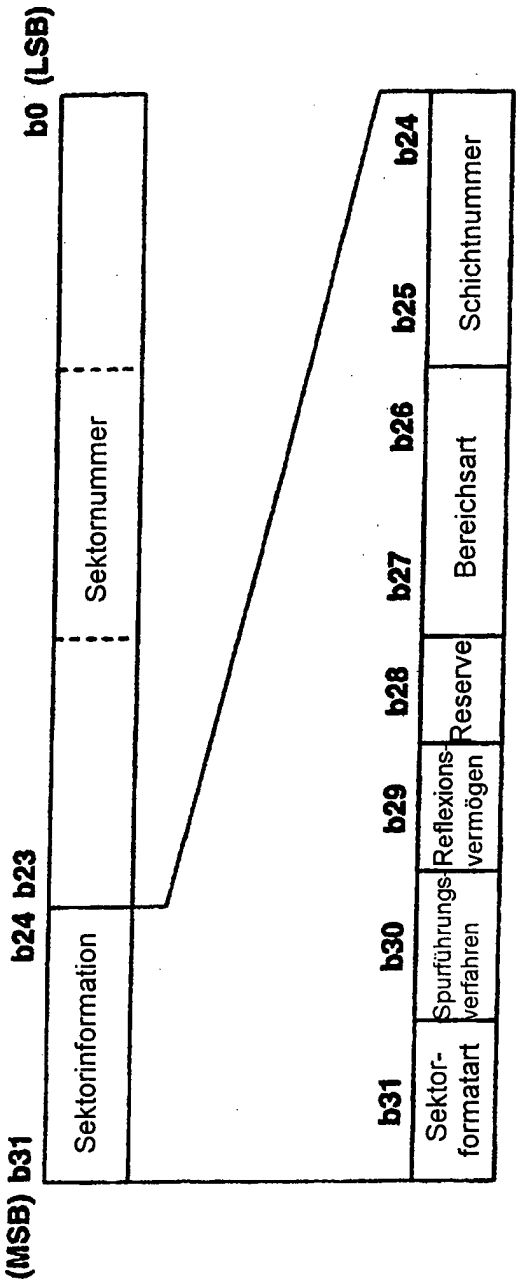
b0 (LSB)
b24 b23
(MSB) b31
Sektorinformation
Sektornummer
b31
b30
b29
b28
b27
b26
b25
b24
Sektor-formatart
Spurführungs-verfahren
Reflexions-vermögen
Reserve
Bereichsart
Schichtnummer

FIG.26

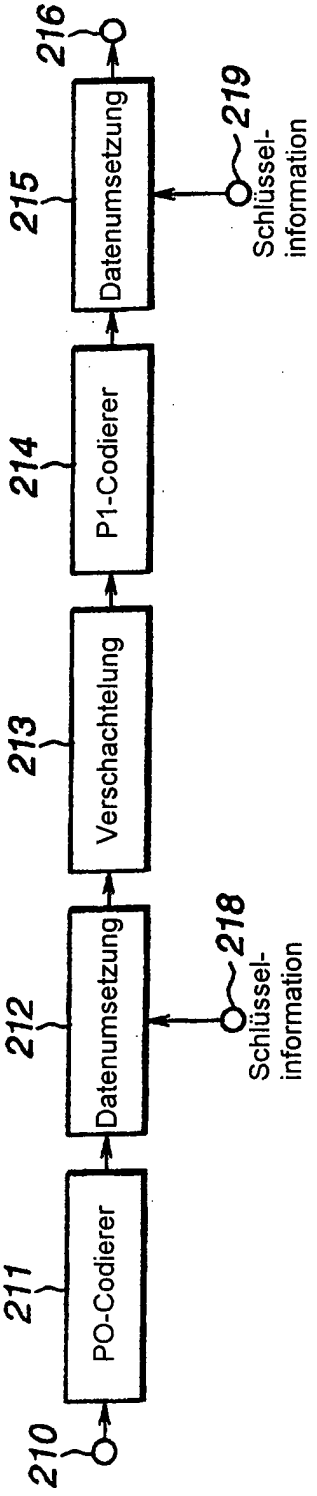
210
211
PO-Codierer
212
Datenumsetzung
218
Schlüssel-information
213
Verschachtelung
214
P1-Codierer
215
Datenumsetzung
219
Schlüssel-information
216

FIG.27

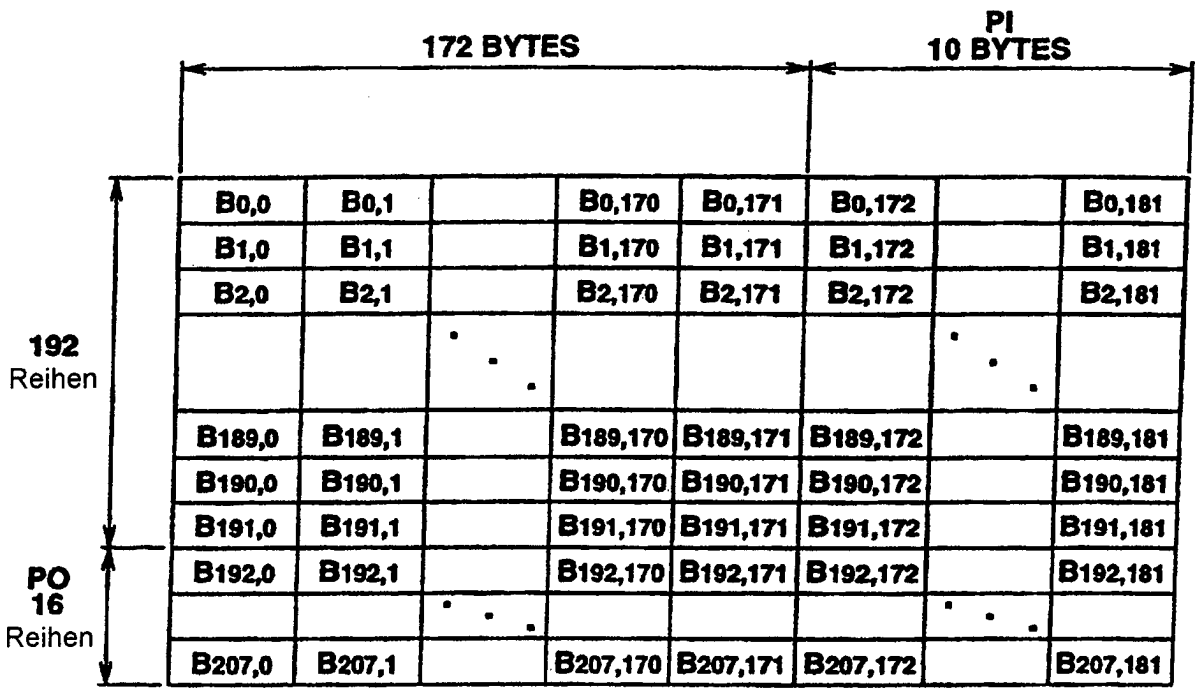
172 BYTES
PI
10 BYTES
192
Reihen
PO
16
Reihen
B0,0 B0,1 B0,170 B0,171 B0,172 B0,181
B1,0 B1,1 B1,170 B1,171 B1,172 B1,181
B2,0 B2,1 B2,170 B2,171 B2,172 B2,181
B189,0 B189,1 B189,170 B189,171 B189,172 B189,181
B190,0 B190,1 B190,170 B190,171 B190,172 B190,181
B191,0 B191,1 B191,170 B191,171 B191,172 B191,181
B192,0 B192,1 B192,170 B192,171 B192,172 B192,181
B207,0 B207,1 B207,170 B207,171 B207,172 B207,181

FIG.28

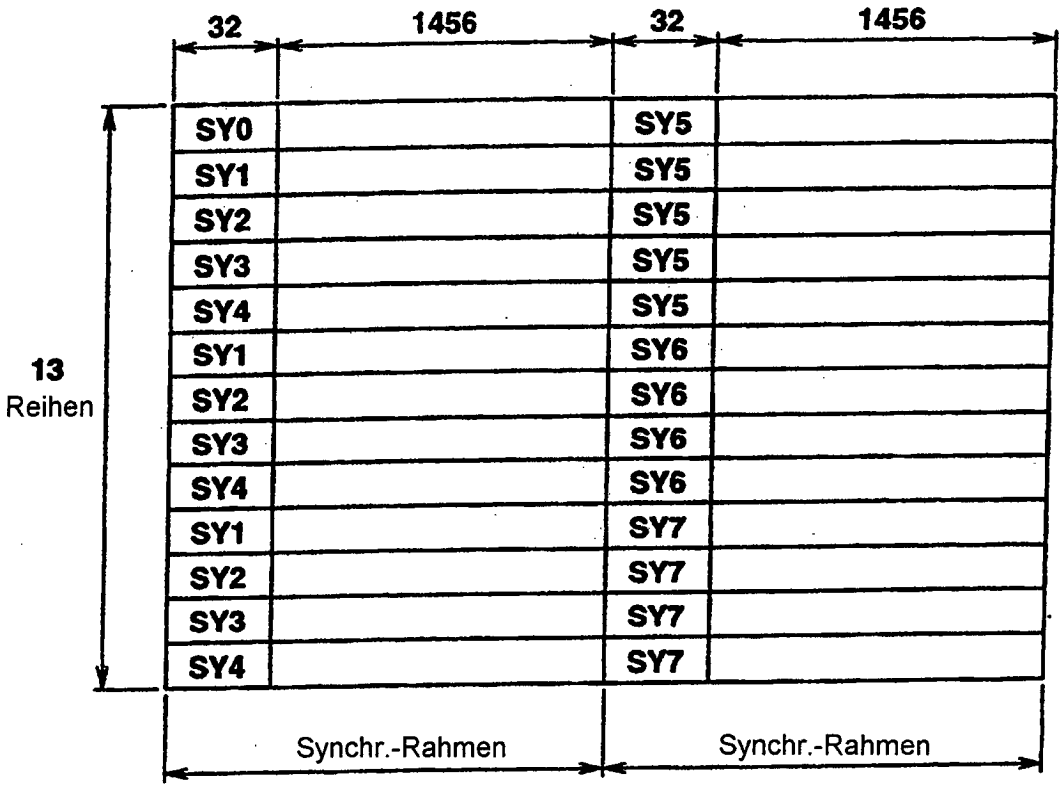
32
1456
32
1456
SY0
SY1
SY2
SY3
SY4
SY1
SY2
SY3
SY4
SY1
SY2
SY3
SY4
SY5
SY5
SY5
SY5
SY5
SY6
SY6
SY6
SY6
SY7
SY7
SY7
SY7
13
Reihen
Synchr.-Rahmen
Synchr.-Rahmen

FIG.29

Zustände 1 und 2

	(MSB)	(LSB)	(MSB)	(LSB)
SY0 =	0001001001000100	0000000000010001 /	0001001000000100	0000000000010001
SY1 =	0000100000000100	0000000000010001 /	0000010001000100	0000000000010001
SY2 =	0001000000000100	0000000000010001 /	0001000001000100	0000000000010001
SY3 =	0000100000000100	0000000000010001 /	0000100000100100	0000000000010001
SY4 =	0010000000000100	0000000000010001 /	0010000001000100	0000000000010001
SY5 =	0010001001000100	0000000000010001 /	0010001000000100	0000000000010001
SY6 =	0010010010000100	0000000000010001 /	0010000010000100	0000000000010001
SY7 =	0010010001000100	0000000000010001 /	0010010000000100	0000000000010001

FIG.30A

Zustände 3 und 4

	(MSB)	(LSB)	(MSB)	(LSB)
SY0 =	1001001000000100	0000000000010001 /	1001001001000100	0000000000010001
SY1 =	1000010001000100	0000000000010001 /	1000010000000100	0000000000010001
SY2 =	1001000001000100	0000000000010001 /	1001000000000100	0000000000010001
SY3 =	1000001001000100	0000000000010001 /	1000001000000100	0000000000010001
SY4 =	1000100001000100	0000000000010001 /	1000100000000100	0000000000010001
SY5 =	1000100100000100	0000000000010001 /	1000000100000100	0000000000010001
SY6 =	1001000010000100	0000000000010001 /	1000000001000100	0000000000010001
SY7 =	1000100010000100	0000000000010001 /	1000000010000100	0000000000010001

FIG.30B

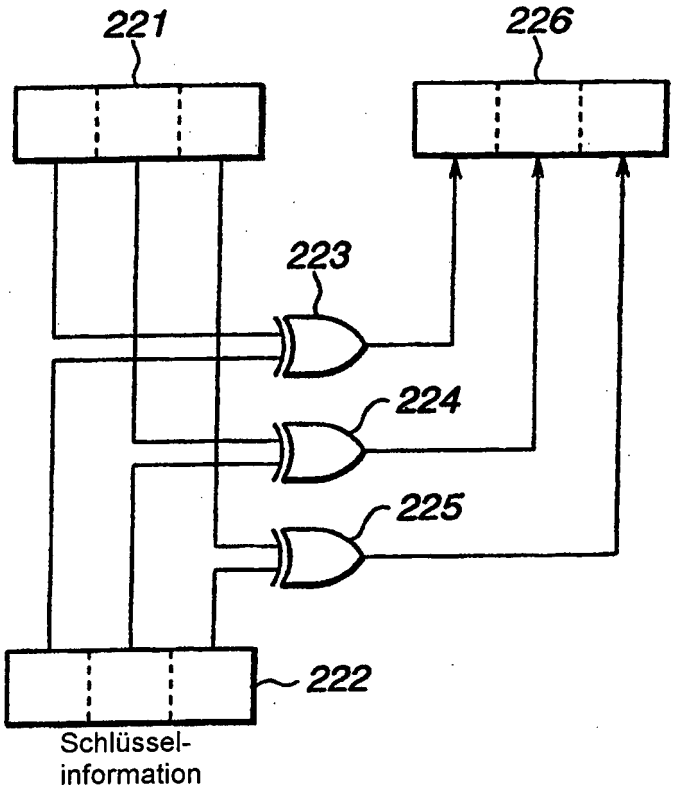

FIG.31

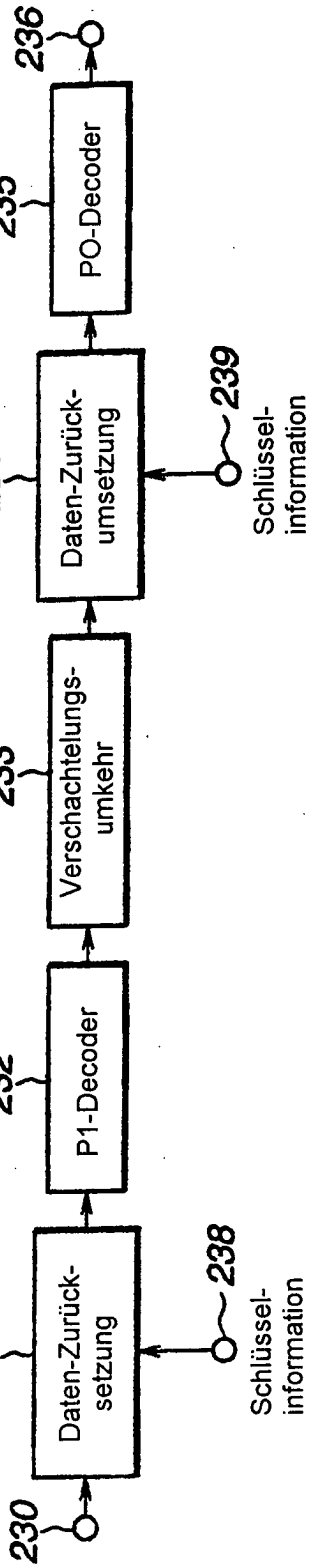
230
231
Daten-Zurück-setzung
238
Schlüssel-information
232
P1-Decoder
233
Verschachtelungs-umkehr
234
Daten-Zurück-umsetzung
239
Schlüssel-information
235
PO-Decoder
236

FIG.32