(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第3796772号

(P3796772)

(45)発行日　平成18年7月12日(2006.7.12)　(24)登録日　平成18年4月28日(2006.4.28)

(51)Int.Cl.			F I		
H04L	9/18	(2006.01)	H04L	9/00	651
G09C	1/00	(2006.01)	G09C	1/00	660D
G11B	20/10	(2006.01)	G11B	20/10	H
G06F	21/24	(2006.01)	G06F	12/14	540C
			G06F	12/14	550B

請求項の数 7　(全 19 頁)

(21)出願番号　特願平7-206084
(22)出願日　平成7年8月11日(1995.8.11)
(65)公開番号　特開平9-55730
(43)公開日　平成9年2月25日(1997.2.25)
審査請求日　平成14年7月16日(2002.7.16)

前置審査

(73)特許権者　000002185
ソニー株式会社
東京都品川区北品川６丁目７番３５号
(74)代理人　100067736
弁理士　小池　晃
(74)代理人　100086335
弁理士　田村　榮一
(74)代理人　100096677
弁理士　伊賀　誠司
(72)発明者　佐古　曜一郎
東京都品川区北品川６丁目７番３５号　ソニー株式会社内
(72)発明者　大澤　義知
東京都品川区北品川６丁目７番３５号　ソニー株式会社内

最終頁に続く

(54)【発明の名称】データ処理方法、データ記録装置及びデータ再生装置

(57)【特許請求の範囲】

【請求項１】

入力ディジタルデータに暗号化処理を施すデータ処理方法において、

データ変換手段により、第１の鍵情報をデータ変換して第２の鍵情報を生成するデータ変換工程と、

第１の暗号化処理手段により、上記第１及び第２の鍵情報のいずれか一方を用いて上記入力ディジタルデータに第１の暗号化処理を施す第１の暗号化工程と、

第２の暗号化処理手段により、上記第１の暗号化処理を施されたディジタルデータに、上記第１及び第２の鍵情報のいずれか他方を用いて、上記第１の暗号化処理と異なる第２の暗号化処理を施す第２の暗号化工程とを有する

ことを特徴とするデータ処理方法。

【請求項２】

上記第１の鍵情報と上記第２の鍵情報とが切り換えられて暗号化に用いられる

ことを特徴とする請求項１記載のデータ処理方法。

【請求項３】

上記第１の鍵情報は、少なくとも一部に識別情報を含む

ことを特徴とする請求項１記載のデータ処理方法。

【請求項４】

少なくとも上記第１の鍵情報をデータ信号と共に出力する

ことを特徴とする請求項１記載のデータ処理方法。

【請求項５】
　上記第２の鍵情報のみデータ信号と共に出力する
　ことを特徴とする請求項１記載のデータ処理方法。
【請求項６】
　入力ディジタルデータに暗号化処理を施して記録媒体に記録するデータ記録装置において、
　暗号化の第１の鍵情報と、この第１の鍵情報をデータ変換して得られる第２の鍵情報とを出力する鍵情報出力手段と、
　この鍵情報出力手段からの上記第１及び第２の鍵情報のいずれか一方を用いて上記入力ディジタルデータに第１の暗号化処理を施し、この暗号化処理を施されたディジタルデータに、上記第１及び第２の鍵情報のいずれか他方を用いて、上記第１の暗号化処理と異なる第２の暗号化処理を施す暗号化手段とを有する
　ことを特徴とするデータ記録装置。
【請求項７】
　入力ディジタルデータに対して暗号化処理が施されて記録媒体に記録された信号を再生するデータ再生装置において、
　上記暗号化処理の際に用いられる第１の鍵情報と、この第１の鍵情報をデータ変換して得られる第２の鍵情報とを出力する鍵情報出力手段と、
　この鍵情報出力手段からの上記第１及び第２の鍵情報のいずれか一方を用いて第１の復号化処理を施し、この復号化処理を施されたディジタルデータに、上記第１及び第２の鍵情報のいずれか他方を用いて、上記第１の復号化処理と異なる第２の復号化処理を施す暗号復号化手段とを有する
　ことを特徴とするデータ再生装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
　本発明は、伝送あるいは記録再生されるディジタルデータのコピー防止や不正使用の阻止、あるいは課金システムに適用可能なデータ処理方法、データ記録装置及びデータ再生装置に関する。
【０００２】
【従来の技術】
近年において、光ディスク等のディジタル記録媒体の大容量化と普及により、不法なコピーの防止や不正使用の阻止が重要とされてきている。すなわち、ディジタルオーディオデータやディジタルビデオデータの場合には、コピーあるいはダビングにより劣化のない複製物を容易に生成でき、また、コンピュータデータの場合には、元のデータと同一のデータが容易にコピーできるため、既に不法コピーによる弊害が生じてきているのが実情である。
【０００３】
ディジタルオーディオデータやディジタルビデオデータの不法コピー等を回避するためには、例えばいわゆるＳＣＭＳ（シリアルコピー管理システム）やＣＧＭＳ（コピー世代管理システム）の規格が知られているが、これは記録データの特定部分にコピー禁止フラグを立てるようなものであるため、いわゆるダンプコピー等の方法によりデータを抜き出される問題がある。
【０００４】
また、コンピュータデータ等のファイル内容自体を暗号化し、それを正規の登録された使用者にのみ使用許諾することが行われている。これは、情報流通の形態として、情報が暗号化されて記録されたディジタル記録媒体を配布したり、暗号化されたディジタル信号を有線、無線の伝送路を介して容易に入手可能にしておき、使用者が必要とした内容について料金を払って鍵情報を入手し、暗号を解いて利用可能とするようなシステムに結び付くものであるが、簡単で有用な暗号化の手法の確立が望まれている。

【０００５】
【発明が解決しようとする課題】
ところで、暗号化の手法としては、種々の方式が提案されており、また暗号化の鍵を公開するような公開鍵暗号方式も知られている。
【０００６】
しかしながら、上記公開鍵暗号を除けば、鍵の管理が難しく、また、公開鍵暗号は処理が複雑化するという問題がある。
【０００７】
さらに、公開鍵暗号においては、鍵が公開されているため、ネットワーク社会においては多くのコンピュータを用いてパラレルに解読を進めることで破られる虞れがあるため、必ずしも安全とはいえなくなってきているのが現状である。
【０００８】
本発明は、上述したような実情に鑑みてなされたものであり、簡単な構成で暗号化が行え、暗号の解読を困難にできるようなデータ処理方法、データ記録装置及びデータ再生装置の提供を目的とする。
【０００９】
【課題を解決するための手段】
上述の目的を達成するために、本発明は、入力ディジタルデータに暗号化処理を施すデータ処理方法において、データ変換手段により、第１の鍵情報をデータ変換して第２の鍵情報を生成するデータ変換工程と、第１の暗号化処理手段により、上記第１及び第２の鍵情報のいずれか一方を用いて上記入力ディジタルデータに第１の暗号化処理を施す第１の暗号化工程と、第２の暗号化処理手段により、上記第１の暗号化処理を施されたディジタルデータに、上記第１及び第２の鍵情報のいずれか他方を用いて、上記第１の暗号化処理と異なる第２の暗号化処理を施す第２の暗号化工程とを有することを特徴としている。
【００１０】
この場合、第１の鍵情報と第２の鍵情報とをそれぞれ異なる場所での暗号化に用いたり、切り換えて用いるようにすることが好ましい。また、第１の鍵情報のみ、第２の鍵情報のみ、あるいは両方の鍵情報を記録する等の伝送を行うようにすることが挙げられる。
【００１１】
単一の鍵情報でデータに２重以上の暗号化が可能となり、第１の鍵情報と第２の鍵情報とで異なる場所又はタイミングで暗号化を施して、鍵情報の取り扱いを簡略化しながら暗号の解読を困難にする。
【００１２】
【発明の実施の形態】
以下、本発明の好ましい実施の形態について図面を参照しながら説明する。
【００１３】
図１は、本発明の実施の形態の基本構成を示すブロック図である。
この図１において、入力端子１に供給された入力ディジタルデータは、信号処理回路２、３を介して出力端子４に送られている。鍵情報供給部５からの第１の鍵情報K_{E1}は、データ変換回路６に送られてデータ変換され、第２の鍵情報K_{E2}となる。これらの第１、第２の鍵情報K_{E1}、K_{E2}は、一方が第１の信号処理回路２に送られ、他方が第２の信号処理回路３に送られる。図１の例では、鍵情報供給部５からの第１の鍵情報K_{E1}を信号処理回路２に、データ変換回路６からの第２の鍵情報K_{E2}を信号処理回路３にそれぞれ送っているが、図中の破線に示すように、第１の鍵情報K_{E1}を信号処理回路３に、第２の鍵情報K_{E2}を信号処理回路２にそれぞれ送るようにしてもよい。これらの信号処理回路２、３では、入力に対して供給された暗号化の鍵情報K_{E1}、K_{E2}に応じたデータ変換を施すと共に、必要に応じて他の信号処理を施して出力する。出力端子４から取り出された信号は、記録媒体に対して記録再生されたり、通信媒体を介して送信受信されたりすることで伝送される。
【００１４】

伝送された信号は、再生側あるいは受信側の入力端子７に供給され、信号処理回路８、９を介して出力端子１０に送られている。信号処理回路８では、記録側あるいは送信側の信号処理回路３に対応する逆の処理あるいはデコード処理が行われ、データ変換回路６からの上記第２の鍵情報K_{E2}に応じた暗号化の復号化処理が施される。また、信号処理回路９では、信号処理回路２に対応する逆の処理あるいはデコード処理が行われ、鍵情報供給部５からの上記第１の鍵情報K_{E1}に応じた暗号化の復号化処理が施される。

【００１５】

データ変換回路６でのデータ変換としては、他の暗号化の鍵あるいは固定値を用いた暗号化処理を挙げることができる。例えば、上記第１の鍵情報K_{E1}を８ビットとし、他の８ビットの鍵あるいは固定値とのかけ算を行うことにより、第２の鍵情報K_{E2}を得ることができる。具体例として、８ビットの第１の鍵情報K_{E1}を“01001100”とし、これをデータ変換するための他の８ビットの鍵あるいは固定値を“10000111”とするとき、これらをかけ算することで、第２の鍵情報K_{E2}として“010011111100100” を得ることができる。この他、論理演算等により８ビットを８ビットに変換するようにしてもよい。

【００１６】

ここで鍵情報として、上記第１、第２の鍵情報K_{E1}、K_{E2}の両方を伝送する以外に、上記第１の鍵情報K_{E1}のみ、又は上記第２の鍵情報K_{E2}のみを伝送するようにしてもよい。すなわち、第１の鍵情報K_{E1}のみを伝送する場合には、再生側でこの第１の鍵情報K_{E1}をデータ変換して第２の鍵情報K_{E2}を得るようにすればよい。また、データ変換が復号化あるいは逆変換可能なものである場合には、上記第２の鍵情報K_{E2}のみを伝送して、再生側でこの第２の鍵情報K_{E2}を復号化あるいは逆変換する、すなわち上記データ変換回路６での変換処理の逆の処理を施すことにより、上記第１の鍵情報K_{E1}を復元するようにすればよい。

【００１７】

このように、単一の鍵情報でデータに対して２重の暗号化が可能である。また、第１の鍵情報K_{E1}と第２の鍵情報K_{E2}とで異なる場所での暗号化を実施しているため、解読が困難になる。

【００１８】

また、第１の鍵情報K_{E1}と第２の鍵情報K_{E2}とを切り換えて暗号化に用いるようにしてもよく、この場合にも暗号の解読を困難にすることができる。

【００１９】

次に、図２は、本発明の実施の形態が適用されるデータ記録装置の具体例を示すブロック図である。

この図２において、入力端子１１には、例えばアナログのオーディオ信号やビデオ信号をディジタル変換して得られたデータやコンピュータデータ等のディジタルデータが供給されている。この入力ディジタルデータは、インターフェース回路１２を介して、セクタ化回路１３に送られ、所定データ量単位、例えば２０４８バイト単位でセクタ化される。セクタ化されたデータは、スクランブル処理回路１４に送られてスクランブル処理が施される。この場合のスクランブル処理は、同一バイトパターンが連続して表れないように、すなわち同一パターンが除去されるように、入力データをランダム化して、信号を適切に読み書きできるようにすることを主旨としたランダム化処理のことである。スクランブル処理あるいはランダム化処理されたデータは、ヘッダ付加回路１５に送られて、各セクタの先頭に配置されるヘッダデータが付加された後、誤り訂正符号化回路１６に送られる。誤り訂正符号化回路１６では、データ遅延及びパリティ計算を行ってパリティを付加する。次の変調回路１７では、所定の変調方式に従って、例えば８ビットデータを１６チャンネルビットの変調データに変換し、同期付加回路１８に送る。同期付加回路１８では、上記所定の変調方式の変調規則を破る、いわゆるアウトオブルールのパターンの同期信号を所定のデータ量単位で付加し、駆動回路すなわちドライバ１９を介して記録ヘッド２０に送っている。記録ヘッド２０は、例えば光学的あるいは磁気光学的な記録を行うものであり、ディスク状の記録媒体２１に上記変調された記録信号の記録を行う。このディスク状記

録媒体２１は、スピンドルモータ２２により回転駆動される。

【００２０】

なお、上記スクランブル処理回路１４は、ヘッダ付加回路１５の後段に挿入して、ヘッダ付加されたディジタルデータに対してスクランブル処理を施して誤り訂正符号化回路１６に送るようにしてもよい。

【００２１】

ここで、セクタ化回路１３、スクランブル処理回路１４、ヘッダ付加回路１５、誤り訂正符号化回路１６、変調回路１７、及び同期付加回路１８のいずれか少なくとも１つの回路は、入力に対して暗号化処理を施して出力するような構成を有している。好ましくは、２つ以上の回路で暗号化処理を施すことが挙げられる。この暗号化処理の鍵情報は、記録媒体２１のデータ記録領域とは別の領域に書き込まれた識別情報、例えば媒体固有の識別情報、製造元識別情報、販売者識別情報、あるいは、記録装置やエンコーダの固有の識別情報、カッティングマシンやスタンパ等の媒体製造装置の固有の識別情報、外部から供給される識別情報等を少なくとも一部に用いている。このように、媒体のデータ記録領域以外に書き込まれる識別情報は、例えば上記インターフェース回路１２からＴＯＣ（Table of contents ）生成回路２３を介して端子２４ａに送られる情報であり、また、インターフェース回路１２から直接的に端子２４ｂに送られる情報である。これらの端子２４ａ、２４ｂからの識別情報が鍵情報供給回路２５に送られて、第１の鍵情報K_{E1}が取り出され、この第１の鍵情報K_{E1}がデータ変換回路２６に送られてデータ変換されることで、第２の鍵情報K_{E2}が得られる。これらの第１、第２の鍵情報K_{E1}、K_{E2}は、回路１３～１８の互いに異なる２以上の回路に送られ、各回路では、これらの鍵情報K_{E1}、K_{E2}を用いた入力データに対する暗号化処理が施される。

【００２２】

この場合、回路１３～１８のどの回路において暗号化処理が施されたかも選択肢の１つとなっており、再生時に正常な再生信号を得るために必要な鍵と考えられる。すなわち、１つの鍵情報について、１つの回路で暗号化処理が施されていれば、６つの選択肢の１つを選ぶことが必要となり、２つの回路で暗号化処理が施されていれば、３０個の選択肢の１つを選ぶことが必要となる。２つの鍵情報K_{E1}、K_{E2}が用いられ、６つの回路１３～１８の内のいずれか回路で暗号化処理が施される可能性がある場合には、さらに選択肢が増大し、この組み合わせを試行錯誤的に見つけることは困難であり、充分に暗号の役割を果たすものである。

【００２３】

また、暗号化の第１の鍵情報K_{E1}と、第２の鍵情報K_{E2}とを所定タイミング、例えばセクタ周期で切り換えることが挙げられる。この所定タイミングで鍵情報を切り換える場合に、切り換えを行うか否かや、切換周期、複数の鍵情報の切換順序等の情報も鍵として用いることができ、暗号化のレベルあるいは暗号の難易度、解き難さ、解読の困難さをさらに高めることができる。

【００２４】

次に、各回路１３～１８の構成及び暗号化処理の具体例について説明する。

【００２５】

先ず、セクタ化回路１３においては、例えば図３に示すような偶数・奇数バイトのインターリーブ処理を行わせることが挙げられる。すなわち、図３において、上記図１のインターフェース回路１２からの出力を、２出力の切換スイッチ３１に送り、この切換スイッチ３１の一方の出力を偶奇インターリーバ３３を介してセクタ化器３４に送り、切換スイッチ３１の他方の出力をそのままセクタ化器３４に送っている。セクタ化器３４では、例えば入力データの２０４８バイト単位でまとめて１セクタとしている。このセクタ化回路１３の切換スイッチ３２の切換動作を、鍵となる１ビットの制御信号で制御するわけである。偶奇インターリーバ３３は、図４のＡに示すような偶数バイト３６ａと奇数バイト３６ｂとが交互に配置された入力データの１セクタ分を、図４のＢに示すように、偶数データ部３７ａと奇数データ部３７ｂとに分配して出力する。さらに、図４のＣに示すように、

１セクタ内の所定の領域３９を鍵情報により特定し、この領域３９内のデータについてのみ偶数データ部３９ａと奇数データ部３９ｂとに分配するようにしてもよい。この場合には、領域３９の特定の仕方を複数通り選択できるように設定することもでき、鍵情報の選択肢をさらに増加させて暗号化のレベルをより高めることもできる。

【００２６】

次に、スクランブル処理回路１４には、例えば図５に示すように、１５ビットのシフトレジスタを用いたいわゆるパラレルブロック同期タイプのスクランブラを用いることができる。このスクランブラのデータ入力用の端子３５には、ＬＳＢ（最下位ビット）が時間的に先となる順序、いわゆるＬＳＢファーストで、上記セクタ化回路１３からのデータが入力される。スクランブル用の１５ビットのシフトレジスタ４１は、排他的論理和（ExOR）回路４２を用いて生成多項式$x^{15}+x+1$に従ったフィードバックがかけられ、１５ビットのシフトレジスタ４１には、図６に示すようなプリセット値（あるいは初期値）が設定されるようになっており、図６のプリセット値の選択番号は、例えばセクタアドレスの下位側４ビットの値に対応させて、セクタ単位でプリセット値が切り換えられるようになっている。シフトレジスタ４１からの出力データと端子３５からの入力データとは、ExOR回路４３により排他的論理和がとられて、端子４４より取り出され、図２のヘッダ付加回路１５に送られる。

【００２７】

ここで、上記生成多項式及びプリセット値（初期値）を、所定の識別番号等の鍵情報に応じて変化させるようにすることができる。すなわち、上記生成多項式を変化させるには、例えば図７に示すような構成を用いればよい。この図７において、１５ビットのシフトレジスタ４１の各ビットからの出力が切換スイッチ４６の各被選択端子に送られ、この切換スイッチ４６は制御端子４７からの例えば４ビットの制御データによって切換制御され、切換スイッチ４６からの出力はExOR回路４２に送られている。このような構成の制御端子４７の制御データを変化させることにより、生成多項式$x^{15}+x^{n}+1$ のｎを変化させることができる。また、上記プリセット値を変化させるには、上記図６のプリセット値テーブルの各プリセット値を、例えば１６バイトの識別情報の各バイト値と論理演算することが挙げられる。この場合の識別情報としては、上述したような媒体固有の識別情報、製造元識別情報、販売者識別情報や、記録装置やエンコーダの固有の識別情報、媒体製造装置固有の識別情報、外部から供給される識別情報等、あるいはこれらの組み合わせや他の情報との組み合わせ等を用いることができ、また上記論理演算としては、排他的論理和（ExOR）や、論理積（AND ）、論理和（OR）、シフト演算等を使用できる。なお、生成多項式を変化させるための構成は図７の構造に限定されず、シフトレジスタの段数や取り出すタップ数を任意に変更してもよい。

【００２８】

次に、ヘッダ付加回路１５について説明する。

先ず、図８はセクタフォーマットの具体例を示しており、１セクタは、２０４８バイトのユーザデータ領域４１に対して、４バイトの同期領域４２と、１６バイトのヘッダ領域４３と、４バイトの誤り検出符号（ＥＤＣ）領域４４とが付加されて構成されている。誤り検出符号領域４４の誤り検出符号は、ユーザデータ領域４１及びヘッダ領域４３に対して生成される３２ビットのＣＲＣ符号から成っている。ヘッダ付加回路１５での暗号化処理としては、同期いわゆるデータシンクに対して、ヘッダのアドレス及びＣＲＣに対して施すことが挙げられる。

【００２９】

セクタの同期すなわちデータシンクに対して暗号化処理を施す一例としては、４バイトの同期領域４２の各バイトに割り当てられたバイトパターンを、図９の「Ａ」、「Ｂ」、「Ｃ」、「Ｄ」にてそれぞれ表すとき、２ビットの鍵情報を用いて、この４バイトの内容をバイト単位でシフトあるいはローテートすることが挙げられる。すなわち、２ビットの鍵が「０」のとき「ＡＢＣＤ」、「１」のとき「ＢＣＤＡ」、「２」のとき「ＣＤＡＢ」、「３」のとき「ＤＡＢＣ」のように切り換えることにより、この鍵が合致しないとセクタ

の同期がとれなくなり、正常な再生が行えない。なお、上記バイトパターン「Ａ」～「Ｄ」としては、例えばＩＳＯ６４６のキャラクタコード等を使用できる。

【００３０】

ヘッダ領域４３内には、図８に示すように、いわゆる巡回符号であるＣＲＣ４５、コピーの許可／不許可やコピー世代管理等のためのコピー情報４６、多層ディスクのどの層かを示す層４７、アドレス４８、予備４９の各領域が設けられている。この内で、アドレス４８の３２ビットにビットスクランブル、この場合には、ビット単位での転置処理を施すことにより、暗号化が行える。また、ＣＲＣ４５の生成多項式として、$x^{16}+x^{15}+x^{2}+1$ が用いられている場合、第２、第３項のx^{15}、x^{2} の代わりに、x^{14}～x^{3} に対応する１２ビットを鍵に応じて変化させることが挙げられる。また、ＣＲＣ４５の１６ビットと鍵情報とを論理演算することも挙げられる。

【００３１】

次に、誤り訂正符号化回路１６の具体例を図１０に示す。

この図１０において、誤り訂正符号化の１フレームは１４８バイトあるいは１４８シンボルのデータから成り、上記ヘッダ付加回路１５からのディジタルデータが１４８バイト毎にまとめられて、第１の符号化器であるＣ１エンコーダ５２に供給される。Ｃ１エンコーダ５２では８バイトのＰパリティが付加され、インターリーブのための遅延回路５３を介して第２の符号化器であるＣ２エンコーダ５４に送られる。Ｃ２エンコーダ５４では１４バイトのＱパリティが付加され、このＱパリティは遅延回路５５を介してＣ１エンコーダ５２に帰還されている。このＣ１エンコーダ５２からのＰ、Ｑパリティを含む１７０バイトが取り出されて、遅延回路５６を介し、インバータ群５７を介して出力され、図２の変調回路１７に送られる。

【００３２】

このような誤り訂正符号化回路において暗号化処理を施す場合には、例えばインバータ群５７内の各バイト毎に、暗号の鍵情報に応じてインバータを入れるか入れないかの選択を行わせるようにすることが挙げられる。すなわち、基準構成においては、２２バイトのＰ、Ｑパリティに対してインバータ群５７のインバータによる反転が行われて出力されるが、これらのインバータのいくつかを無くしたり、Ｃ１データ側にいくつかのインバータを入れて反転して出力させたりすることが挙げられる。この場合、基準構成からの違いの程度によって誤り訂正不能確率が変化し、違いが少ないときには最終的な再生出力におけるエラー発生確率がやや高くなる程度であるのに対し、違いが多いときには全体的にエラー訂正が行われなくなって殆ど再生できなくなるような状態となる。すなわち、例えばＣ１エンコーダについて見ると、誤り訂正能力を示す指標であるいわゆるディスタンスが９であるため、最大４バイトまでのエラー検出訂正が行え、消失（イレージャ）ポインタがあれば最大８バイトまでの訂正が可能であることから、違いが５箇所以上あると、Ｃ１符号では常に訂正不可となる。違いが４箇所の場合は、他に１バイトでもエラーが生じると訂正不可という微妙な状態となる。違いが３、２、１箇所と減少するにつれて、誤り訂正できる確率が増えてゆく。これを利用すれば、オーディオやビデオのソフトを提供する場合等に、ある程度は再生できるが完璧ではなく時々乱れる、といった再生状態を積極的に作り出すことができ、該ソフトの概要だけを知らせる用途等に使用することができる。

【００３３】

この場合、予めインバータの変更を行う場所を例えば２箇所程度規定しておく方法と、変更箇所を鍵情報に応じてランダムに選び、最低個数を２箇所程度に制限する方法と、これらを複合する方法とが挙げられる。

【００３４】

さらに、インバータの挿入あるいは変更位置としては、図１０のインバータ群５７の位置に限定されず、例えばＣ１エンコーダ５２の前段や後段等の他の位置やこれらの位置を組み合わせるようにしてもよい。複数の位置の場合に、異なる鍵を用いるようにしてもよい。また、上記データ変換としては、インバータを用いる以外に、ビット加算や種々の論理演算を用いるようにしたり、データを暗号化の鍵情報に応じて転置するようにしたり、デ

ータを暗号化の鍵情報に応じて置換するようにしてもよい。

【００３５】

ここで、図１１は、上記誤り訂正符号化回路１６の他の具体例として、インバータ群５７の後段すなわち出力側の位置に排他的論理和（ExOR）回路群６１を挿入し、Ｃ１エンコーダ５２の前段すなわち入力側の位置にもExOR回路群６６を挿入した例を示している。

【００３６】

この図１１においては、１７０ビットの鍵情報が端子６２に供給され、いわゆるＤラッチ回路６３を介してExOR回路群６１内の１７０個の各ExOR回路にそれぞれ供給されている。Ｄラッチ回路６３は、イネーブル端子６４に供給された１ビットの暗号化制御信号に応じて、端子６２からの１７０ビットの鍵情報をそのままExOR回路群６１に送るか、オールゼロ、すなわち１７０ビットの全てを“０”とするかが切換制御される。ExOR回路群６１の１７０個の各ExOR回路の内、Ｄラッチ回路６３から“０”が送られたExOR回路は、インバータ群５７からのデータをそのまま出力し、Ｄラッチ回路６３から“１”が送られたExOR回路は、インバータ群５７からのデータを変換して出力する。オールゼロのときには、インバータ群５７からのデータをそのまま出力することになる。また、ExOR回路群６６については、１４８個のExOR回路を有し、鍵情報が１４８ビットであること以外は、上記ExOR回路群６１の場合と同様であり、端子６７に供給された１４８ビットの鍵情報がＤラッチ回路６８を介してExOR回路群６６内の１４８個のExOR回路にそれぞれ送られると共に、Ｄラッチ回路６８はイネーブル端子６９の暗号化制御信号により１４８ビットの鍵情報かオールゼロかが切換制御される。

【００３７】

この図１１の回路においても、上記図１０の場合と同様な作用効果が得られることは勿論である。また、ExOR回路群６１、６６のいずれか一方のみを使用するようにしたり、いずれか一方あるいは双方の選択も暗号化の鍵として用いるようにすることもできる。

【００３８】

なお、上記データ変換手段としてのExOR回路群６１、６６の代わりに、ＡＮＤ、ＯＲ、ＮＡＮＤ、ＮＯＲ、インバート回路群等を使用してもよい。また、８ビット単位で１ビットの鍵情報あるいは鍵データによる論理演算を行う以外にも、８ビットの情報データに対して８ビットの鍵データで論理演算を行わせてもよく、さらに、情報データの１ワードに相当する８ビットの内の各ビットに対してそれぞれＡＮＤ、ＯＲ、ＥｘＯＲ、ＮＡＮＤ、ＮＯＲ、インバート回路を組み合わせて使用してもよい。この場合には、例えば１４８バイトすなわち１４８×８ビットのデータに対して、１４８×８ビットの鍵データが用いられることになり、さらにＡＮＤ、ＯＲ、ＥｘＯＲ、ＮＡＮＤ、ＮＯＲ、インバート回路を組み合わせて使用する場合には、これらの組み合わせ自体も鍵として用いることができる。また、論理演算以外に、データの位置を変える転置や、データの値を置き換える置換等も上記データ変換として使用できる。

【００３９】

このように、誤り訂正符号化の際に取り扱われる中間データ等について、暗号化の鍵情報に応じた一部のデータに対してインバータ等でデータ変換を施すことにより、訂正不能誤りの発生確率が変化し、データ変換を施すデータ数に応じて暗号化のレベル、深度、解読の困難さ等が変化することになる。すなわち、用途に応じて必要とされる暗号化の深度や難易度を、データ変換を施すデータ数により任意に設定でき、概要をサンプルとして提供したい場合や、正規ユーザ以外には再生不可能としたい場合や、セキュリティレベルの要求等に応じて種々の対応が図れる。

【００４０】

次に、図２の変調回路１７での暗号化処理について、図１２を参照しながら説明する。この図１２において、入力端子７１には、上記誤り訂正符号化回路１６からのデータが８ビット（１バイト）毎に供給され、入力端子７２には８ビットの鍵情報が供給されており、これらの８ビットデータは、論理演算回路の一例としてのExOR回路７３に送られて排他的論理和がとられる。このExOR回路７３からの８ビット出力が、所定の変調方式の変調器、

例えば８－１６変換回路７４に送られて、１６チャンネルビットに変換される。この８－１６変換回路７４での８－１６変調方式の一例としてはいわゆるＥＦＭプラス変調方式が挙げられる。

【００４１】

この図１２の例では、データ変調の前に８ビットの鍵情報を用いた暗号化処理を施しているが、鍵情報のビット数は８ビットに限定されず、また、８－１６変調の際の変換テーブルの入出力の対応関係を鍵情報に応じて変化させるようにしてもよい。鍵情報には、上述した媒体固有の識別情報等を使用できることは勿論である。

【００４２】

次に、同期付加回路１８について説明する。

同期付加回路１８では、例えば図１３に示すような４種類の同期ワードＳ０～Ｓ３を用いて、上記８－１６変調のフレーム単位で同期をとっている。この８－１６変調フレーム（例えばＥＦＭプラスフレーム）は、例えば８５データシンボルである１３６０チャンネルビットから成り、この１フレーム１３６０チャンネルビット毎に３２チャンネルビットの同期ワードが付加されると共に、このフレームを上記Ｃ１符号やＣ２符号に対応させて構造化し、Ｃ１符号系列の先頭フレームの同期ワードと他のフレームの同期ワードを異ならせる等して、上記４種類の同期ワードＳ０～Ｓ３を使い分けている。これらの同期ワードＳ０～Ｓ３は、直前のワードの“１”、“０”の状態やいわゆるデジタルサムあるいは直流値等に応じてそれぞれ２つの同期パターンａ、ｂを有している。

【００４３】

このような４種類の同期ワードＳ０～Ｓ３の選択を、例えば図１４に示すような回路を用いて、２ビットの鍵情報７５に応じて変更することにより、暗号化が行える。すなわち、上記４種類の同期ワードＳ０～Ｓ３を指定する２ビットデータ７６の各ビットと、上記２ビットの鍵情報７５の各ビットとが、２つのExOR回路７７、７８によりそれぞれ排他的論理和され、新たな同期ワード指定データ７９となる。これにより、上記フレーム構造における同期ワードの使い方あるいはフレーム構造内での各種同期ワードの使用位置が変更され、暗号化がなされることになる。

【００４４】

なお、同期ワードの種類数をさらに増やしてそれらの内から４種類の同期ワードを取り出す取り出し方を暗号化の鍵により決定するようにしてもよい。この鍵情報としては、上述した媒体固有の識別情報等が使用できる。

【００４５】

これらの各回路１３～１８において用いられる鍵情報は、上述した第１の鍵情報K_{E1}又は第２の鍵情報K_{E2}のいずれかであり、これら２つの鍵情報K_{E1}、K_{E2}は異なる場所で用いられる。例えば、第１の鍵情報K_{E1}を各回路１３～１８のいずれかに用いて暗号化を施し、この第１の鍵情報K_{E1}を用いた暗号化を行わなかった回路の少なくとも１つに第２の鍵情報K_{E2}を用いた暗号化を施すようにすればよい。

【００４６】

次に図１５は、記録媒体の一例としての光ディスク等のディスク状記録媒体１０１を示している。このディスク状記録媒体１０１は、中央にセンタ孔１０２を有しており、このディスク状記録媒体１０１の内周から外周に向かって、プログラム管理領域であるＴＯＣ（table of contents ）領域となるリードイン（lead in ）領域１０３と、プログラムデータが記録されたプログラム領域１０４と、プログラム終了領域、いわゆるリードアウト（lead out）領域１０５とが形成されている。オーディオ信号やビデオ信号再生用光ディスクにおいては、上記プログラム領域１０４にオーディオやビデオデータが記録され、このオーディオやビデオデータの時間情報等が上記リードイン領域１０３で管理される。

【００４７】

上記鍵情報の一部として、データ記録領域であるプログラム領域１０４以外の領域に書き込まれた識別情報等を用いることが挙げられる。具体的には、ＴＯＣ領域であるリードイン領域１０３や、リードアウト領域１０５に、識別情報、例えば媒体固有の製造番号等の

識別情報、製造元識別情報、販売者識別情報、あるいは、記録装置やエンコーダの固有の識別情報、カッティングマシンやスタンパ等の媒体製造装置の固有の識別情報を書き込むようにすると共に、これを上記第１の鍵情報K_{E1}として上述した６つの回路１３～１８の少なくとも１つで暗号化処理を施し、この第１の鍵情報K_{E1}をデータ変換して得られる第２の鍵情報K_{E2}を用いて残りの回路の少なくとも１つで暗号化処理を施し、これらの暗号化処理が施されて得られた信号をデータ記録領域であるプログラム領域１０４に記録するようにする。再生時には、上記識別情報を、暗号を復号するための上記第１の鍵情報K_{E1}として用いるようにすればよい。また、リードイン領域１０３よりも内側に、物理的あるいは化学的に識別情報を書き込むようにし、これを再生時に読み取って、暗号を復号するための鍵情報として用いるようにしてもよい。また、上記第２の鍵情報K_{E2}のみをディスク状記録媒体１０１の所定位置に記録するようにし、再生側ではこの第２の鍵情報K_{E2}を復号化して第１の鍵情報K_{E1}を得るようにしてもよい。

【００４８】

次に、本発明のデータ再生方法、データ再生装置の実施例について、図１６を参照しながら説明する。

【００４９】

図１６において、記録媒体の一例としてのディスク状記録媒体１０１は、スピンドルモータ１０８により回転駆動され、光学ピックアップ装置等の再生ヘッド装置１０９により媒体記録内容が読み取られる。

【００５０】

再生ヘッド装置１０９により読み取られたディジタル信号は、ＴＯＣデコーダ１１１及びアンプ１１２に送られる。ＴＯＣデコーダ１１１からは、ディスク状記録媒体１０１の上記リードイン領域１０３にＴＯＣ情報の一部として記録された上記識別情報、例えば媒体固有の製造番号等の識別情報、製造元識別情報、販売者識別情報、あるいは、記録装置やエンコーダの固有の識別情報、カッティングマシンやスタンパ等の媒体製造装置の固有の識別情報が読み取られ、この識別情報が暗号を復号化するための鍵情報の少なくとも一部として用いられる。この他、再生装置内部のＣＰＵ１２２から、再生装置固有の識別情報や、外部からの識別情報を出力するようにし、この識別情報を鍵情報の少なくとも一部として用いるようにしてもよい。なお、外部からの識別情報としては、通信回線や伝送路等を介して受信された識別情報や、いわゆるＩＣカード、ＲＯＭカード、磁気カード、光カード等を読み取って得られた識別情報等が挙げられる。

【００５１】

この鍵情報の具体例として、図１６の例では、ＴＯＣデコーダ１１１からの出力やＣＰＵ１２２からの出力を鍵情報供給回路１２５に送るようにし、この鍵情報供給回路１２５から第１の鍵情報K_{E1}を得て、これをデータ変換回路１２６に送りデータ変換することで、第２の鍵情報K_{E2}を得るようにしている。これらの第１、第２の鍵情報K_{E1}、K_{E2}は、上記図２の記録側の各回路１３～１８の内の暗号化が施された回路に対応する回路１１４～１１９について、それぞれ暗号化に用いられた鍵情報に対応したものが用いられる。

【００５２】

この図１６において、再生ヘッド装置１０９からアンプ１１２を介し、ＰＬＬ（位相ロックループ）回路１１３を介して取り出されたディジタル信号は、同期分離回路１１４に送られて、上記図２の同期付加回路１８で付加された同期信号の分離が行われる。同期分離回路１１４からのディジタル信号は、復調回路１１５に送られて、上記図２の変調回路１７の変調を復調する処理が行われる。具体的には、１６チャンネルビットを８ビットのデータに変換するような処理である。復調回路１１５からのディジタルデータは、誤り訂正復号化回路１１６に送られて、図２の誤り訂正符号化回路１６での符号化の逆処理としての復号化処理が施される。以下、セクタ分解回路１１７によりセクタに分解され、ヘッダ分離回路１１８により各セクタの先頭部分のヘッダが分離される。これらのセクタ分解回路１１７及びヘッダ分離回路１１８は、上記図２のセクタ化回路１３及びヘッダ付加回路１５に対応するものである。次に、デスクランブル処理回路１１９により、上記図２のス

クランブル処理回路１４におけるスクランブル処理の逆処理としてのデスクランブル処理が施され、インターフェース回路１２０を介して出力端子１２１より再生データが取り出される。

【００５３】

ここで、上述したように、記録時には、上記図２のセクタ化回路１３、スクランブル処理回路１４、ヘッダ付加回路１５、誤り訂正符号化回路１６、変調回路１７、及び同期付加回路１８のいずれか少なくとも１つの回路において第１の鍵情報K_{E1}を用いた暗号化処理が施されており、この暗号化処理が施された回路に対応する再生側の回路１１４～１１９にて、第１の鍵情報K_{E1}を用いて暗号を復号化する処理が必要とされる。また、残りの回路の内のいずれか少なくとも１つの回路において第２の鍵情報K_{E2}を用いた暗号化処理が施されており、この暗号化処理が施された回路に対応する再生側の回路にて、第２の鍵情報K_{E2}を用いて暗号を復号化する処理が必要とされる。すなわち、上記図１のセクタ化回路１３にて第１の鍵情報K_{E1}又は第２の鍵情報K_{E2}のいずれかを用いた暗号化処理が施されている場合には、セクタ分解回路１１７にて暗号化の際の鍵情報を用いた暗号の復号化処理が必要とされる。以下同様に、図１のスクランブル処理回路１４での暗号化処理に対応してデスクランブル処理回路１１９での暗号復号化処理が、図１のヘッダ付加回路１５での暗号化処理に対応してヘッダ分離回路１１８での暗号復号化処理が、図１の誤り訂正符号化回路１６での暗号化処理に対応して誤り訂正復号化回路１１６での暗号復号化処理が、図１の変調回路１７での暗号化処理に対応して復調回路１１５での暗号復号化処理が、さらに図１の同期付加回路１８での暗号化処理に対応して同期分離回路１１４での暗号復号化処理が、それぞれ暗号化の際に用いられた鍵情報と同じ鍵情報を用いて行われることが必要とされる。

【００５４】

なお、図１６のセクタ分解回路１１７をデスクランブル処理回路１１９の後段に設ける構成でもよい。

【００５５】

同期分離回路１１４での暗号復号化処理は、上記図１３や図１４と共に説明したように、複数種類、例えば４種類の同期ワードの使い方あるいはフレーム構造内での各種同期ワードの使用位置が鍵情報に応じて変更され、暗号化がなされたものを、鍵情報に応じて検出することで行われる。

【００５６】

次に、復調回路１１５での暗号復号化処理は、図１７に示すように、同期分離回路１１４から１６－８変換回路１３１に送られて１６チャンネルビットが８ビットデータに変換されたものを、上記図１２のExOR回路７３に対応するExOR回路１３２に送り、端子１３３からの８ビットの鍵情報との排他的論理和をとることで、図１２の入力端子７１に供給された８ビットデータに相当するデータが復元され、これが誤り訂正復号化回路１１６に送られる。

【００５７】

次に、誤り訂正復号化回路１１６では、例えば上記図１０の誤り訂正符号化処理の逆処理が、図１８の構成により行われる。

【００５８】

この図１８において、上記復調回路１１５にて復調されたデータの１７０バイトあるいは１７０シンボルを１まとまりとして、インバータ群１４２を介し、遅延回路１４３を介して第１の復号器であるＣ１デコーダ１４４に送られている。このＣ１デコーダ１４４に供給される１７０バイトのデータの内２２バイトがＰ，Ｑパリティであり、Ｃ１デコーダ１４４では、これらのパリティデータを用いた誤り訂正復号化が施される。Ｃ１デコーダ１４４からは、１７０バイトのデータが出力されて、遅延回路１４５を介して第２の復号器であるＣ２デコーダ１４６に送られ、パリティデータを用いた誤り訂正復号化が施された後、さらに遅延回路１４７を介して第３の復号器であるＣ３デコーダ１４８に送られる。ここで、遅延回路１４７及びＣ３デコーダ１４８は、上記遅延回路１４３及びＣ１デコー

ダ１４４と同様のものであり、この遅延回路とＣ１デコーダの組を複数組設けるようにしてもよい。このＣ３デコーダ１４８で最終的な誤り訂正復号化が施され、パリティ無しの１４８バイトのデータが取り出される。この１４８バイトのデータは、上記図１０のＣ１エンコーダ５２に入力される１４８バイトのデータに相当するものである。

【００５９】

そして、図１０の誤り訂正符号化回路のインバータ群５７で、インバータの有無による暗号化が施されている場合には、図１８の誤り訂正復号化回路のインバータ群１４２にて、対応する暗号復号化を行うことが必要とされる。この他、図１０と共に説明した各種暗号化処理に対応して、その暗号化を解くための逆処理となる暗号復号化が必要とされることは勿論である。

【００６０】

ここで、図１９は、上記図１１の誤り訂正符号化回路の具体的構成に対応する誤り訂正復号化回路の具体的な構成を示す図である。

【００６１】

この図１９において、上記図１１のインバータ群５７の出力側に挿入されたExOR回路群６１に対応して、インバータ群１４３の入力側にExOR回路群１５１が挿入され、図１１のＣ１エンコーダ５２の入力側に挿入されたExOR回路群６６に対応して、Ｃ３デコーダ１４８の出力側にExOR回路群１５６が挿入されている。

【００６２】

この図１９の端子１５２には、図１１の端子６２に供給される鍵情報に相当する１７０ビットの鍵情報が供給され、いわゆるＤラッチ回路１５３を介してExOR回路群１５１内の１７０個の各ExOR回路にそれぞれ供給されている。Ｄラッチ回路１５３は、イネーブル端子１５４に供給された１ビットの暗号化制御信号に応じて、端子１５２からの１７０ビットの鍵情報をそのままExOR回路群１５１に送るか、オールゼロ、すなわち１７０ビットの全てを“０”とするかが切換制御される。また、ExOR回路群１５６については、１４８個のExOR回路を有し、鍵情報が図１１の端子６７に供給される鍵情報と同様の１４８ビットであること以外は、上記ExOR回路群１５１の場合と同様であり、端子１５７に供給された１４８ビットの鍵情報がＤラッチ回路１５８を介してExOR回路群１５６内の１４８個のExOR回路にそれぞれ送られると共に、Ｄラッチ回路１５８はイネーブル端子１５９の暗号化制御信号により１４８ビットの鍵情報かオールゼロかが切換制御される。

【００６３】

次に、セクタ分解回路１１７においては、上記図３、図４と共に説明したように、記録時に上記セクタ化回路１３で偶数・奇数バイトのインターリーブによる暗号化が施されている場合に、この偶奇インターリーブを解くような逆の処理、いわゆるデインターリーブ処理を施すものである。

【００６４】

また、ヘッダ分離回路１１８においては、記録時に、上記ヘッダ付加回路１５において、上記図８、図９と共に説明したような暗号化処理、すなわちセクタ同期となるデータシンクのバイトパターンの転置や、アドレス、ＣＲＣの変更がなされている場合に、これを復元するような暗号復号化処理を施すものである。

【００６５】

次に、デスクランブル処理回路１１９では、上記図５～図７と共に説明したような暗号化処理を復元するような暗号復号化処理を施している。

【００６６】

これらの各回路１１４～１１９のいずれで暗号復号化処理が必要とされるかの情報も、暗号の鍵情報となることは前述した通りである。また、暗号の鍵情報を所定周期、例えばセクタ周期で切り換えることができ、この切換を行うか否かや、切換周期等も鍵とすることにより、暗号化の難易度が高められる。

【００６７】

以上説明したように、第１の鍵情報K_{E1}と、これをデータ変換して得られる第２の鍵情報

K_{E2}とを用いて暗号化が施され、これらの第１、第２の鍵情報K_{E1}、K_{E2}を用いて暗号復号化が施されるため、暗号解読を複雑にして破られ難くすることができると共に、暗号化の鍵情報の取り扱いを簡便化できる。

【００６８】

また、製造者識別情報、販売者識別情報、装置識別情報等と、別途設定されるコピープロテクト情報、課金情報を組み合わせて、データを暗号化して記録しておくことにより、コピー防止、海賊盤防止、不正使用の防止等を物理フォーマットレベルで実現し得るようにしている。また、データセキュリティ機能の情報、例えばコピーの許可／不許可情報、有償／無償情報を、記録媒体及び記録／再生システムの物理フォーマットにインプリメントしている。

【００６９】

すなわち、セキュリティ／課金情報を予め媒体に記録しておき、媒体に記録又は未記録の識別情報を用いて、それをデータの暗号化と組み合わせることにより、簡単な仕組みでコピー防止、不正使用防止が実現できるようになる。また、物理フォーマットにそれを内在させることにより、解読が困難になる。また、ダンプコピーされても暗号化されたままであるので安全である。さらに、セクタ単位やファイル単位、ゾーン単位、レイヤ単位等で可変にできる。またさらに、通信やＩＣカードやリモコン等で鍵がコントロールできる。さらに、海賊盤に対して履歴が残せる。

【００７０】

なお、本発明は上記実施の形態のみに限定されるものではなく、例えば、データ変換としては、インバータやExORの例を示しているが、この他、ビット加算や、各種論理演算等によりデータ変換を行わせてもよいことは勿論である。また、データを記録媒体に対する記録再生のみならず通信媒体を介した送受信等を含むような、一般のデータ伝送に本発明を適用できることは勿論である。この他、本発明の要旨を逸脱しない範囲で種々の変更が可能である。

【００７１】

【発明の効果】

本発明によれば、第１の鍵情報を用いて暗号化処理を施すと共に、この第１の鍵情報をデータ変換して得られた第２の鍵情報を用いて暗号化処理を施すようにしているため、単一の鍵情報でデータに２重以上の暗号化が可能となり、第１の鍵情報と第２の鍵情報とで異なる場所で暗号化を施しているため、鍵情報の取り扱いを簡略化しながら暗号の解読を困難にすることができ、データセキュリティを高めることができる。

【００７２】

また、第１の鍵情報を伝送することにより、この第１の鍵情報に識別情報や認証情報を用いる場合に、認証が暗号復号化処理を必要とせずにできるため高速化でき、認証後に第２の鍵情報を利用した安全な暗号復号化処理が行える。

【００７３】

さらに、第２の鍵情報のみを伝送することにより、この第２の鍵情報が漏れても暗号が破られることがなく、より解読を困難化できる。

【図面の簡単な説明】

【図１】本発明の実施の形態の基本構成を示すブロック図である。

【図２】本発明の実施の形態が適用可能なデータ記録装置の概略構成を示すブロック図である。

【図３】セクタ化回路における偶数・奇数バイトのインターリーブを実現するための構成例を示すブロック図である。

【図４】偶数・奇数バイトのインターリーブを説明するための図である。

【図５】スクランブラの一例を示す図である。

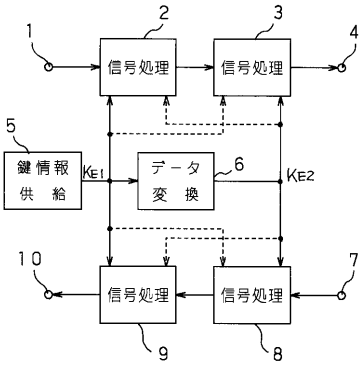
【図６】スクランブラのプリセット値を示す図である。

【図７】生成多項式が可変のスクランブラの一例を示す図である。

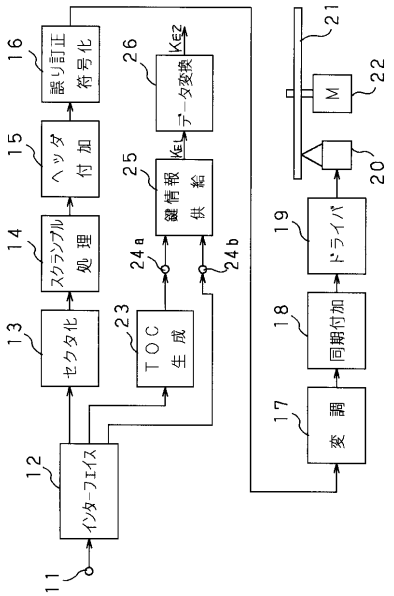
【図８】セクタフォーマットの一例を示す図である。

【図９】セクタ内の同期領域での暗号化の一例を説明するための図である。
【図１０】誤り訂正符号化回路の一例を示す図である。
【図１１】誤り訂正符号化回路の他の例を示す図である。
【図１２】変調回路での暗号化処理の一例を説明するための図である。
【図１３】変調信号に付加される同期ワードの具体例を示す図である。
【図１４】同期付加回路での暗号化の一例を説明するための図である。
【図１５】データ記録媒体の一例を示す図である。
【図１６】本発明のデータ再生装置の一実施例の概略構成を示すブロック図である。
【図１７】復調回路での暗号化処理の一例を説明するための図である。
【図１８】誤り訂正復号化回路の一例を示す図である。
【図１９】誤り訂正復号化回路の他の例を示す図である。
【符号の説明】
５、２５、１２５　鍵情報供給回路
６、２６、１２６　データ変換回路
１３　セクタ化回路
１４　スクランブル処理回路
１５　ヘッダ付加回路
１６　誤り訂正符号化回路
１７　変調回路
１８　同期付加回路
５７、１４２　インバータ群
６１、６６、１５１、１５６　ExOR回路群
１１４　同期分離回路
１１５　復調回路
１１６　誤り訂正復号化回路
１１７　セクタ分解回路
１１８　ヘッダ分離回路
１１９　デスクランブル処理回路

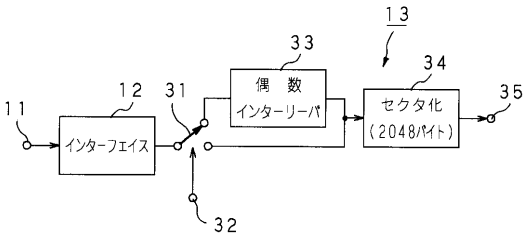
【図１】


1
2
3
4
信号処理
信号処理
5
鍵情報供給
KE1
データ変換
6
KE2
10
7
信号処理
信号処理
9
8

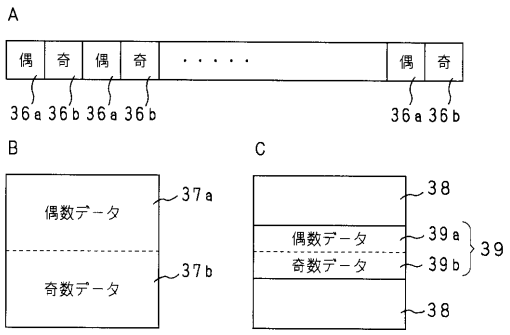
【図２】


16
誤り訂正符号化
15
ヘッダ付加
14
スクランブル処理
13
セクタ化
12
インターフェイス
11
26
KE2
データ変換
25
KE1
鍵情報供給
24a
24b
23
TOC生成
21
M
22
20
19
ドライバ
18
同期付加
17
変調

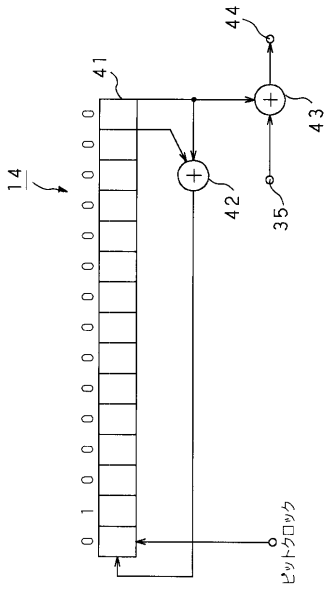
【図３】


13
33
34
11
12
31
偶数インターリーバ
セクタ化(2048バイト)
35
インターフェイス
32

【図４】


A
偶
奇
偶
奇
・・・・・
偶
奇
36a 36b 36a 36b
36a 36b
B
偶数データ
37a
奇数データ
37b
C
38
偶数データ
39a
奇数データ
39b
39
38

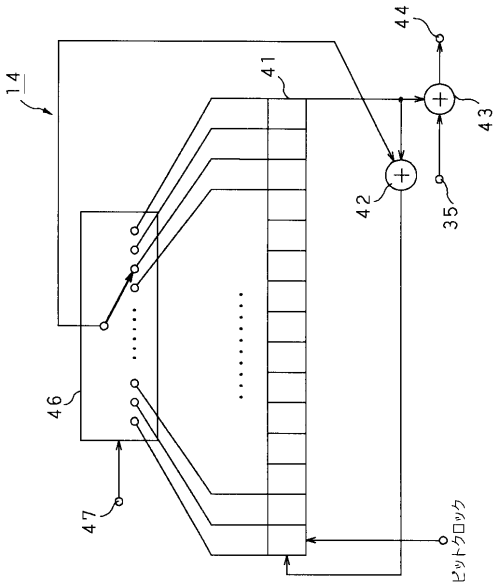
【図５】


44
41
14
0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0
43
42
35
ビットクロック

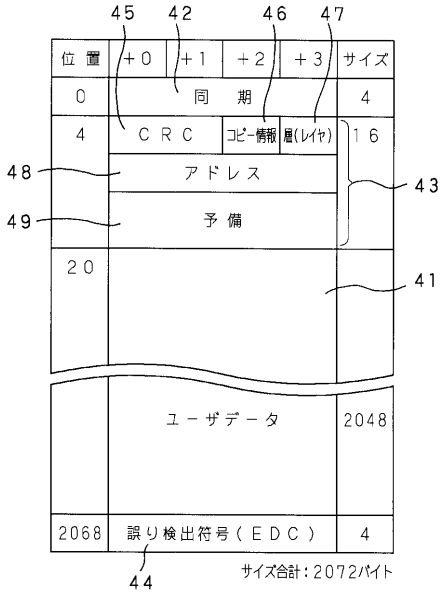
【図６】

選択番号	プリセット値	選択番号	プリセット値
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

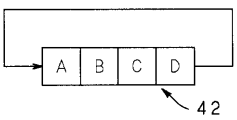
【図７】



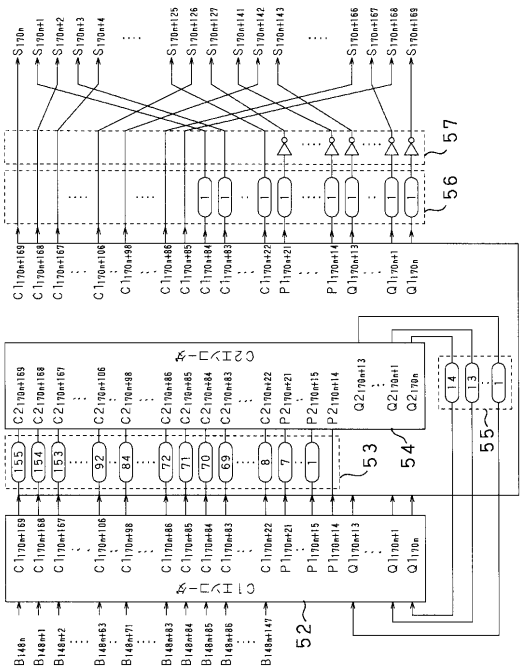
【図８】



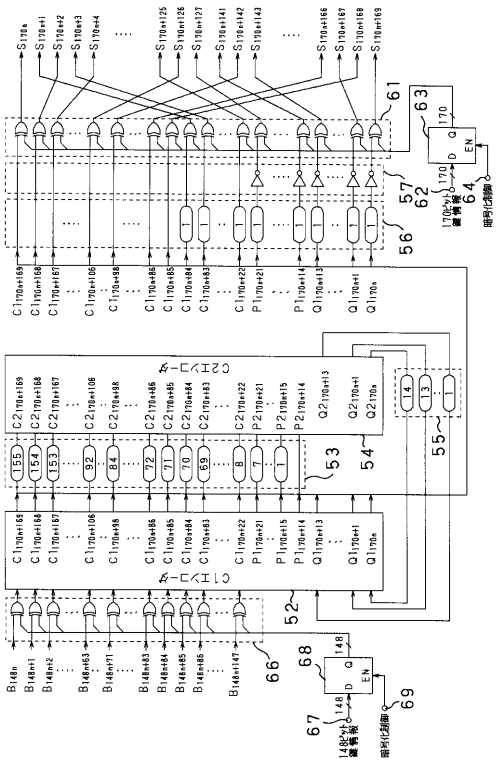
【図９】



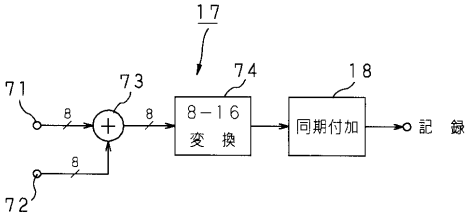
【図１０】



【図１１】



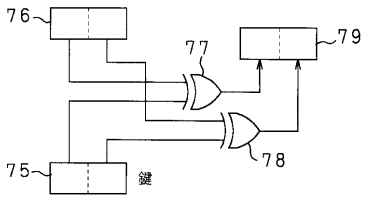
【図１２】



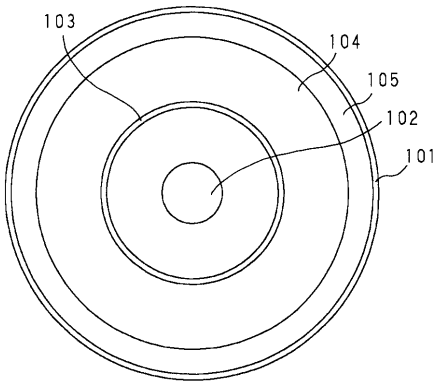
【図１３】

同期ワード	符号ワード			
	msb	同期パターンa	lsb	msb	同期パターンb	lsb
S0	00010010010000000001000000000001			10010010010000000001000000000001		
S1	00010000010000000001000000000001			10000100010000000001000000000001		
S2	00000100010000000001000000000001			10000100001000000001000000000001		
S3	00001000010000000001000000000001			10001000010000000001000000000001		

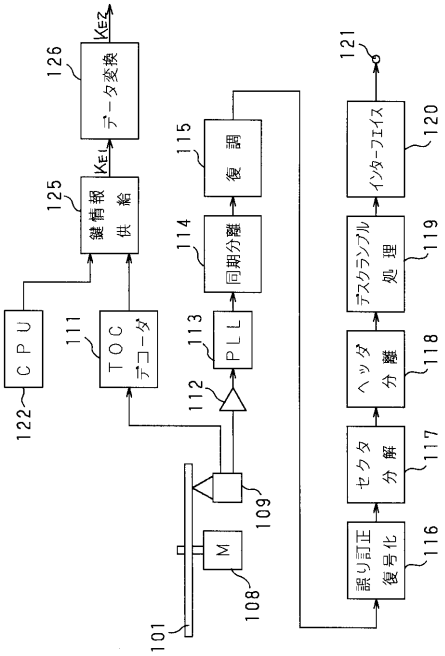
【図１４】



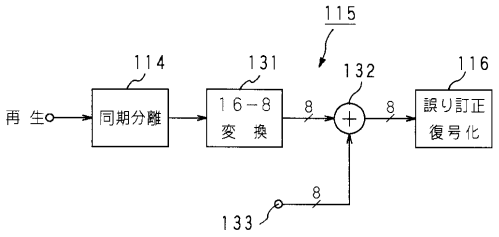
【図１５】



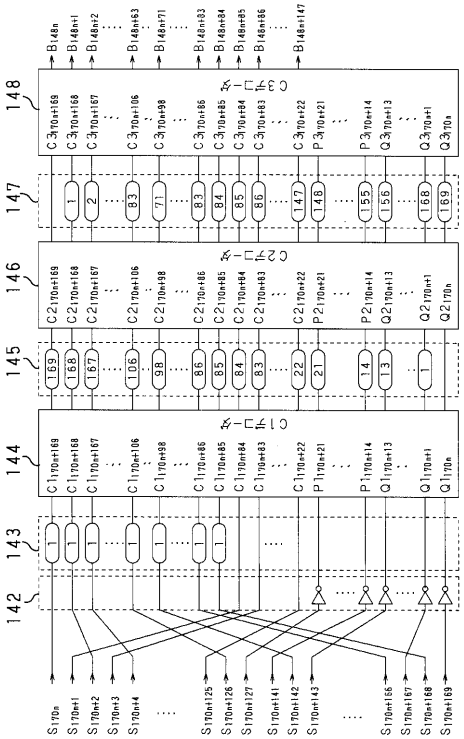
【図１６】



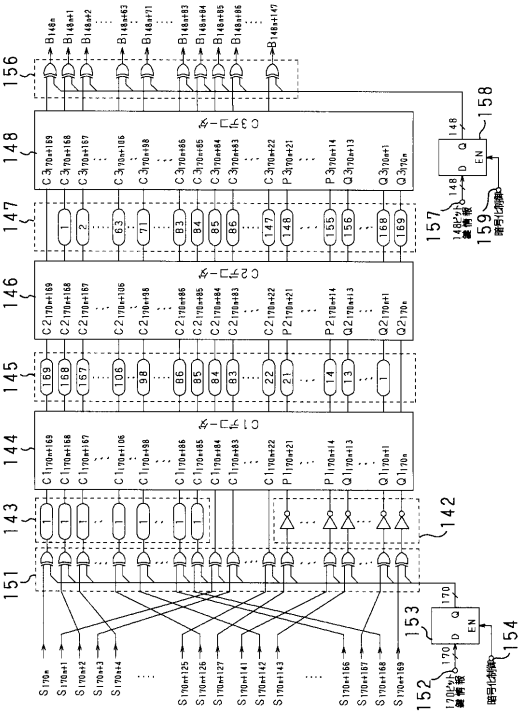
【図１７】



【図１８】



【図１９】



フロントページの続き

(72)発明者　栗原　章
東京都品川区北品川６丁目７番３５号　ソニー株式会社内
(72)発明者　川嶋　功
東京都品川区北品川６丁目７番３５号　ソニー株式会社内

審査官　石田　信行

(56)参考文献　特開平０３－１２９３８４（ＪＰ，Ａ）
特開平０７－０７８１８７（ＪＰ，Ａ）
特開平０５－２５７８１６（ＪＰ，Ａ）
特開平２－３０２５９（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L 9/18
G06F 21/24
G09C 1/00
G11B 20/10