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

特許第4150886号
(P4150886)

(45)発行日　平成20年9月17日(2008.9.17)　(24)登録日　平成20年7月11日(2008.7.11)

(51)Int.Cl.　　F I
G09C 1/00 (2006.01)　　G09C 1/00 610B
G06F 1/12 (2006.01)　　G09C 1/00 650Z
　　G06F 1/04 340D

請求項の数 3　(全 9 頁)

(21)出願番号　特願2002-118508(P2002-118508)
(22)出願日　平成14年4月19日(2002.4.19)
(65)公開番号　特開2003-316260(P2003-316260A)
(43)公開日　平成15年11月7日(2003.11.7)
審査請求日　平成17年3月14日(2005.3.14)

(73)特許権者　000002185
ソニー株式会社
東京都港区港南１丁目７番１号
(74)代理人　100091546
弁理士　佐藤　正美
(72)発明者　松田　寛美
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　細井　隆史
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　田中　理生
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】暗号化復号化演算装置およびデータ受信装置

(57)【特許請求の範囲】
【請求項１】
入力データをラッチする第１のラッチ手段と、
この第１のラッチ手段の出力データに、ビット単位の並べ替えを施す初期転置手段と、
この初期転置手段の出力データと、後記の別データとの、いずれかを選択する第１の選択手段と、
この第１の選択手段の出力データ中の上位ビットと下位ビットのうちの一方と、鍵データとを演算する第１の演算手段と、
この第１の演算手段の出力データをラッチする第２のラッチ手段と、
この第２のラッチ手段の出力データを演算する第２の演算手段と、
この第２の演算手段の出力データと、前記第１の選択手段の出力データ中の上位ビットと下位ビットのうちの他方とを演算する第３の演算手段と、
この第３の演算手段の出力データと、前記第１の選択手段の出力データ中の上位ビットと下位ビットのうちの一方とを、上位ビットと下位ビットを入れ替えて合成する入れ替え合成手段と、
この入れ替え合成手段の出力データをラッチして、前記の別データとして前記第１の選択手段に入力する第３のラッチ手段と、
前記第１の演算手段から前記第３の演算手段までの関数変換を複数ｎ回、繰り返した後のデータに、ビット単位の並べ替えを施す逆転置手段と、
前記第１の演算手段に供給される前記鍵データを生成する鍵生成部と

を備え、
前記鍵生成部は、
もとの鍵データをラッチする第４のラッチ手段と、
この第４のラッチ手段の出力データをビットシフトするシフトレジスタと、
このシフトレジスタの出力を複数ｎ段の出力データに変換する複数ｎ個の変換回路と、
このｎ個の変換回路の出力データを、前記第１の演算手段に供給される前記鍵データとして選択して出力する第２の選択手段と
を備える暗号化復号化演算装置。
【請求項２】
請求項１の暗号化復号化演算装置において、前記第１および第４のラッチ手段へのラッチ用のクロックと、前記第２のラッチ手段へのラッチ用のクロックは、位相がずれたものとされる暗号化復号化演算装置。
【請求項３】
請求項１または２の暗号化復号化演算装置を備え、受信された暗号化されたデータを当該暗号化復号化演算装置によって復号化して出力するデータ受信装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
この発明は、データの暗号化または復号化のためにデータを演算する装置、および、この暗号化復号化演算装置を備えるデータ受信装置に関する。
【０００２】
【従来の技術】
ＤＥＳ（Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）の暗号アルゴリズムによる暗号化復号化装置として、図５に示すような装置が考えられている。
【０００３】
鍵データ（秘密鍵）および入力データ（平文データまたは暗号文データ）は、いずれも６４ビットで、それぞれクロックＣＬＫによってラッチ回路８１および８２にラッチされる。また、暗号化か、復号化かを示すモード信号が、クロックＣＬＫによってラッチ回路８３にラッチされる。
【０００４】
ラッチ回路８１の出力の鍵データは、鍵生成部９０に供給され、鍵生成部９０から、それぞれ４８ビットの１６段分の鍵データＫ１～Ｋ１６が順次出力される。
【０００５】
具体的に、ラッチ回路８１の出力の６４ビットの鍵データが、変換回路９１で５６ビットの鍵データに変換され、その上位２８ビットおよび下位２８ビットのデータが、シフト回路９３および９４において、１ビットまたは２ビット、シフトされた後、５６ビットの鍵データに合成され、その５６ビットの鍵データが、変換回路９５で４８ビットの鍵データに変換されて、第１段の鍵データが生成される。
【０００６】
以下、同様のビットシフトおよび変換が実行されて、１６段分の鍵データが生成され、セレクタ９９に入力される。そして、ラッチ回路８３の出力のモード信号によって、セレクタ９９が制御されて、セレクタ９９から、それぞれ４８ビットの１６段分の鍵データＫ１～Ｋ１６が、クロックＣＬＫのパルスごとに順次出力される。
【０００７】
ラッチ回路８２の出力データ（平文データまたは暗号文データ）は、演算部１００に供給され、演算部１００において、以下のように演算される。
【０００８】
まず、ラッチ回路８２の出力の６４ビットのデータが、初期転置回路１０１においてビット単位で並べ替えられ、その初期転置後の６４ビットのデータ中の下位３２ビットが、第

１段の変換回路１０２で鍵データＫ１と演算され、関数Ｆによって変換された後、ＸＯＲ（排他的論理和）回路１０３で、変換回路１０２の出力の３２ビットのデータと、初期転置後の６４ビットのデータ中の上位３２ビットとがＸＯＲ演算される。

【０００９】

次いで、ＸＯＲ回路１０３の出力の３２ビットのデータが、第２段の変換回路１０４で鍵データＫ２と演算され、関数Ｆにより変換された後、ＸＯＲ回路１０５で、変換回路１０４の出力の３２ビットのデータと、初期転置後の６４ビットのデータ中の下位３２ビットとがＸＯＲ演算される。

【００１０】

以下、同様に、上位３２ビットと下位３２ビットが入れ替えられて、第３段以下の演算が実行された後、第１６段の変換回路１０７に入力された３２ビットのデータと、第１６段のＸＯＲ回路１０８の出力の３２ビットのデータとが合成され、その合成後の６４のデータが、逆転置回路１０９においてビット単位で並べ替えられる。

【００１１】

その逆転置後の６４ビットのデータが、クロックＣＬＫによってラッチ回路８４にラッチされて、ラッチ回路８４から、出力データとして、暗号化または復号化されたデータが得られる。

【００１２】

【発明が解決しようとする課題】

しかしながら、上述した暗号化復号化演算装置では、鍵生成部９０が、ラッチ回路（サンプリング回路）を含まない非同期回路であって、入力された鍵データから１６段の鍵データを一度に生成し、セレクタ９９で選択するだけであるので、鍵生成部９０の出力の鍵データＫ１～Ｋ１６は、変化点付近でノイズ（信号線電位の変化）が多く重畳されたものとなり、演算部１００での消費電力が大きくなる。

【００１３】

そこで、この発明は、消費電力の著しく少ない演算装置を実現できるようにしたものである。

【００１４】

【課題を解決するための手段】

この発明においては、

入力データをラッチする第１のラッチ手段と、

この第１のラッチ手段の出力データに、ビット単位の並べ替えを施す初期転置手段と、

この初期転置手段の出力データと、後記の別データとの、いずれかを選択する第１の選択手段と、

この第１の選択手段の出力データ中の上位ビットと下位ビットのうちの一方と、鍵データとを演算する第１の演算手段と、

この第１の演算手段の出力データをラッチする第２のラッチ手段と、

この第２のラッチ手段の出力データを演算する第２の演算手段と、

この第２の演算手段の出力データと、前記第１の選択手段の出力データ中の上位ビットと下位ビットのうちの他方とを演算する第３の演算手段と、

この第３の演算手段の出力データと、前記第１の選択手段の出力データ中の上位ビットと下位ビットのうちの一方とを、上位ビットと下位ビットを入れ替えて合成する入れ替え合成手段と、

この入れ替え合成手段の出力データをラッチして、前記の別データとして前記第１の選択手段に入力する第３のラッチ手段と、

前記第１の演算手段から前記第３の演算手段までの関数変換を複数ｎ回、繰り返した後のデータに、ビット単位の並べ替えを施す逆転置手段と、

前記第１の演算手段に供給される前記鍵データを生成する鍵生成部と

を備え、

前記鍵生成部は、

もとの鍵データをラッチする第４のラッチ手段と、
この第４のラッチ手段の出力データをビットシフトするシフトレジスタと、
このシフトレジスタの出力を複数ｎ段の出力データに変換する複数ｎ個の変換回路と、
このｎ個の変換回路の出力データを、前記第１の演算手段に供給される前記鍵データとして選択して出力する第２の選択手段と
を備える暗号化復号化演算装置
とするものである。

【００１５】
上記の構成の演算装置では、第１の演算手段の出力データが第２のラッチ手段でラッチされることによって、非同期回路からのデータのノイズが吸収されて、第２のラッチ手段の出力信号としては、ラッチ用のクロックの変化点でのみ電位が変化するものとなり、第２のラッチ手段以降の第２の演算手段での消費電力が著しく少なくなる。

【００１６】
【発明の実施の形態】
〔暗号化復号化演算装置の実施形態：図１～図３〕
図１および図２は、この発明による暗号化復号化演算装置の一実施形態を示し、図２は図１の演算部６０中の変換回路７０の部分を詳細に示したものである。

【００１７】
この実施形態の暗号化復号化演算装置の暗号アルゴリズムは、ＤＥＳの暗号アルゴリズムに従うものである。

【００１８】
鍵データ（秘密鍵）および入力データ（平文データまたは暗号文データ）は、いずれも６４ビットで、それぞれクロックＣＬＫ１によってラッチ回路４１および４６にラッチされる。

【００１９】
また、暗号化か、復号化かを示すモード信号が、クロックＣＬＫ１によってラッチ回路４２にラッチされる。さらに、１６段のカウンタ４４によって、スタート信号の時点から，クロックＣＬＫ１がカウントされる。

【００２０】
ラッチ回路４１の出力の鍵データ、ラッチ回路４２の出力のモード信号、およびカウンタ４４の出力信号は、鍵生成部５０に供給され、鍵生成部５０から、それぞれ４８ビットの１６段分の鍵データＫ１～Ｋ１６が順次出力される。

【００２１】
具体的に、ラッチ回路４１の出力の６４ビットの鍵データが、変換回路５１で５６ビットの鍵データに変換され、その５６ビットの鍵データが、シフトレジスタ５３において、ラッチ回路４２の出力信号によって、１ビットまたは２ビットずつ順次、シフトされて、それぞれ５６ビットの鍵データが１６個得られる。

【００２２】
さらに、この１６個の、それぞれ５６ビットの鍵データが、それぞれ変換回路５５で４８ビットの鍵データに変換され、その１６個の、それぞれ４８ビットの鍵データが、セレクタ５７において、カウンタ４４の出力信号によって、クロックＣＬＫ１のパルスごとに順次選択されて、上記の鍵データＫ１～Ｋ１６が、クロックＣＬＫ１のパルスごとに順次得られる。

【００２３】
このように、鍵生成部５０では、入力された鍵データから１６段の鍵データを一度に生成し、セレクタ５７で選択するだけであるので、鍵生成部５０の出力の鍵データＫ１～Ｋ１６は、変化点付近でノイズ（信号線電位の変化）が多く重畳されたものとなる。

【００２４】
ラッチ回路４６の出力データ（平文データまたは暗号文データ）は、演算部６０に供給さ

れる。演算部６０は、１段分の演算回路によって１６段の演算が循環的に繰り替えされる構成とされる。

【００２５】

すなわち、最初は、ラッチ回路４６の出力の６４ビットのデータが、初期転置回路６１においてビット単位で並べ替えられ、その初期転置後の６４ビットのデータが、カウンタ４４によって制御されるセレクタ６２から出力され、その出力された６４ビットのデータ中の下位３２ビットが、変換回路７０で鍵データＫ１と演算され、関数Ｆによって変換される。

【００２６】

具体的に、変換回路７０では、図２に示すように、下位３２ビットのデータが、拡大転置回路７１において、ビット単位で並べ替えられるとともに、同じビットが複数回選択されることによって４８ビットのデータに変換された後、ＸＯＲ回路７３で、その４８ビットのデータと、同じく４８ビットの鍵データＫ１とがＸＯＲ演算される。

【００２７】

さらに、ＸＯＲ回路７３の出力の４８ビットのデータが、上記のクロックＣＬＫ１に対して位相がずれたクロックＣＬＫ２によって、ラッチ回路７５にラッチされる。

【００２８】

このようにクロックＣＬＫ１と位相の異なるクロックＣＬＫ２でＸＯＲ回路７３の出力データをラッチするのは、図３に示すように、クロックＣＬＫ１の変化点（立ち上がりエッジ）に対して、鍵生成部５０の出力の鍵データＫ１～Ｋ１６、および拡大転置回路７１の出力データが遅れ、ＸＯＲ回路７３の出力データも遅れるため、クロックＣＬＫ１でＸＯＲ回路７３の出力データをラッチした場合には、１クロック前のデータがラッチされてしまうからである。具体的に、例えば、クロックＣＬＫ２はクロックＣＬＫ１に対して逆相とする。

【００２９】

そして、このようにＸＯＲ回路７３の出力データをラッチ回路７５でラッチすることによって、鍵生成部５０の出力の鍵データＫ１～Ｋ１６の上述したノイズが吸収されて、ラッチ回路７５の出力信号としては、クロックＣＬＫ２の変化点でのみ電位が変化するものとなり、ラッチ回路７５以降の回路部での消費電力が著しく少なくなる。

【００３０】

ラッチ回路７５の出力の４８ビットのデータは、６ビットずつ８分割され、その分割された、それぞれ６ビットのデータが、それぞれルックアップテーブル７７によって４ビットのデータに置き換えられる。

【００３１】

さらに、その置き換え後の、それぞれ４ビットの８個のデータが、３２ビットのデータに合成され、その３２ビットのデータが、転置回路７９においてビット単位で並べ替えられる。

【００３２】

以上で、第１段の演算中の、変換回路７０での処理を終了する。第１段の演算としては、さらに、ＸＯＲ回路６４で、転置回路７９の出力の３２ビットのデータと、初期転置後のセレクタ６２から出力された６４ビットのデータ中の上位３２ビットとがＸＯＲ演算される。

【００３３】

以上で、第１段の演算を終了する。そして、入れ替え合成回路６６で、上位３２ビットと下位３２ビットが入れ替えられるように、拡大転置回路７１に入力された３２ビットのデータと、ＸＯＲ回路６４の出力の３２ビットのデータとが合成され、その合成後の６４ビットのデータが、クロックＣＬＫ１によってラッチ回路４７にラッチされる。

【００３４】

第２段以降の演算では、初期転置回路６１の出力データに代えて、このラッチ回路４７の出力の６４ビットのデータが、セレクタ６２から出力され、鍵データＫ１に代えて、鍵デ

ータＫ２以降の鍵データが変換回路７０のＸＯＲ回路７３に入力されて、第１段の演算と同様の演算が実行される。

【００３５】

そして、第１６段の演算後は、入れ替え合成回路６６による上位３２ビットと下位３２ビットの入れ替えは不要であるので、入れ替え合成回路６６による入れ替え合成後の６４ビットのデータは、入れ替え回路６７で、上位３２ビットと下位３２ビットが入れ替えられた後、逆転置回路６９においてビット単位で並べ替えられる。

【００３６】

その逆転置後の６４ビットのデータが、クロックＣＬＫ１によってラッチ回路４８にラッチされて、ラッチ回路４８から、出力データとして、暗号化または復号化されたデータが得られる。

【００３７】

この実施形態の暗号化復号化演算装置では、上述したように消費電力が著しく少なくなる。しかも、演算部６０は、１段分の演算回路によって１６段の演算が循環的に繰り替えされる構成であるので、演算装置のゲート数を減少させることができ、回路規模を縮小することができる。

【００３８】

なお、上述した実施形態は、ＤＥＳ暗号アルゴリズムに従う場合であるが、必ずしもＤＥＳ暗号アルゴリズムと同じである必要はなく、入力データ（平文データまたは暗号文データ）および鍵データのビット長や、演算の段数などを、増加させるなどの変更を行ってもよい。

【００３９】

〔データ受信装置の実施形態：図４〕

図４は、この発明の暗号化復号化演算装置を備える、この発明のデータ受信装置の一実施形態としての記録再生装置を含むデータ受信システムを示す。

【００４０】

この例のデータ受信システムでは、記録媒体１からのリッピングや、インターネットを利用した配信システム２からのダウンロードなどによって、ＰＣなどの端末１０で、符号化され、かつ秘密鍵によって暗号化されたデータが受信される。

【００４１】

その受信された暗号文データは、端末１０から、端末１０のＵＳＢ（Ｕｎｉｖｅｒｓａｌ　Ｓｅｒｉａｌ　Ｂｕｓ）端子に接続された記録再生装置２０に送信される。

【００４２】

記録再生装置２０は、記録媒体５上にデータを記録し、記録媒体５上からデータを再生するもので、これに暗号化復号化装置３０が設けられる。

【００４３】

暗号化復号化装置３０は、図１および図２に示して上述した暗号化復号化演算装置を、暗号化復号化処理部４０として備えるほか、ＣＰＵ３１を備え、そのバス３２に、ＣＰＵ３１が実行すべきコマンド送受や暗号化復号化処理などのプログラムや必要な固定データなどが書き込まれたＲＯＭ３３、ＣＰＵ３１のワークエリアなどとして機能するＲＡＭ３４、端末１０との間でコマンドを送受し、端末１０からデータを取り込むＵＳＢインタフェース３６、記録再生装置本体部のＤＳＰ（Ｄｉｇｉｔａｌ　Ｓｉｇｎａｌ　Ｐｒｏｃｅｓｓｏｒ）２６にデータを出力するためのインタフェース３７、および記録再生装置本体部のＣＰＵ２１との間でコマンドを送受するためのインタフェース３９が接続される。

【００４４】

この暗号化復号化装置３０は、ワンチップＬＳＩ（大規模集積回路）として形成される。

【００４５】

記録再生装置本体部は、ＣＰＵ２１のバス２２に、ＣＰＵ２１が実行すべきプログラムや必要な固定データなどが書き込まれたＲＯＭ２３、ＣＰＵ２１のワークエリアなどとして機能するＲＡＭ２４、および上記のＤＳＰ２６が接続され、ＤＳＰ２６に、記録再生処理

部２７、および出力処理部２８が接続される。

【００４６】

暗号化復号化装置３０では、ＵＳＢインタフェース３６を介して端末１０から取り込まれた、符号化され、かつ秘密鍵によって暗号化されたデータが、暗号化復号化処理部４０において、上述したように復号化され、その復号化された平文データとしての、符号化されたデータが、インタフェース３７を介してＤＳＰ２６に送出され、ＤＳＰ２６で処理された後、記録再生処理部２７によって記録媒体５上に記録され、または出力処理部２８によってアナログ信号に変換されて出力端子２９に導出される。

【００４７】

記録媒体５としては、光ディスク、ハードディスク、フレキシブルディスク、磁気テープ、メモリカード、半導体メモリなど、いずれでもよい。

【００４８】

また、このような記録再生装置に限らず、暗号化されたデータを受信し、復号化して、再生するだけで、記録機能を備えない装置にも、この発明を適用することができる。

【００４９】

【発明の効果】

上述したように、この発明によれば、消費電力の著しく少ない演算装置を実現することができる。

【図面の簡単な説明】

【図１】　この発明による暗号化復号化演算装置の一実施形態を示す図である。

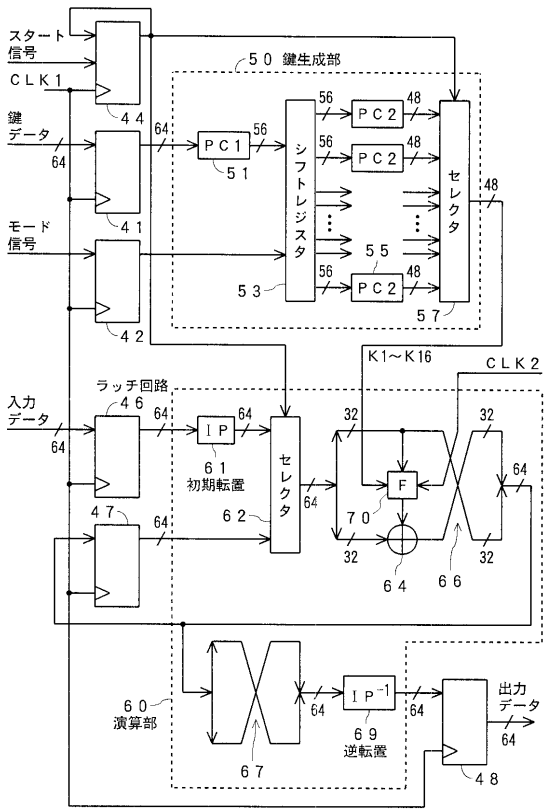
【図２】　図１の暗号化復号化演算装置の要部を示す図である。

【図３】　図１の暗号化復号化演算装置の動作の説明に供する図である。

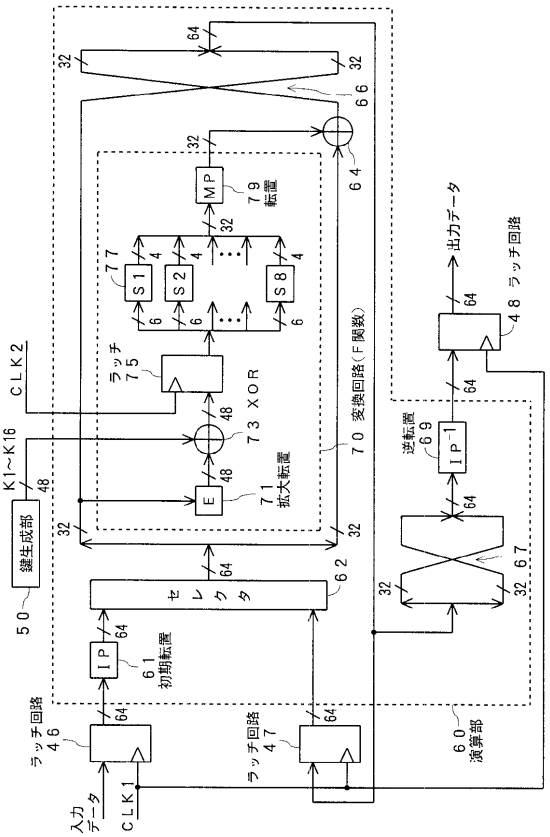
【図４】　この発明のデータ受信装置の一実施形態としての記録再生装置を示す図である。

【図５】　従来の暗号化復号化演算装置を示す図である。

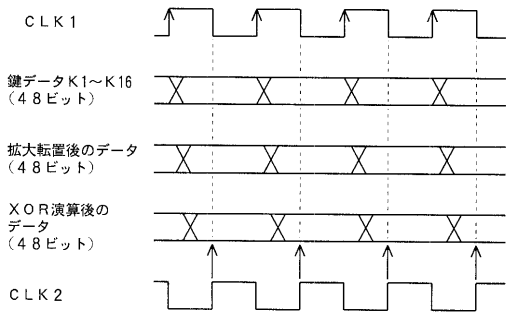
【図１】



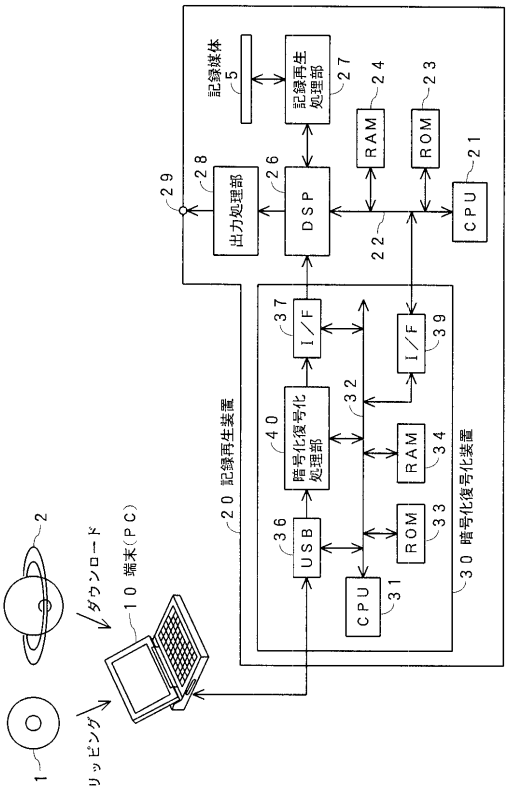
【図２】



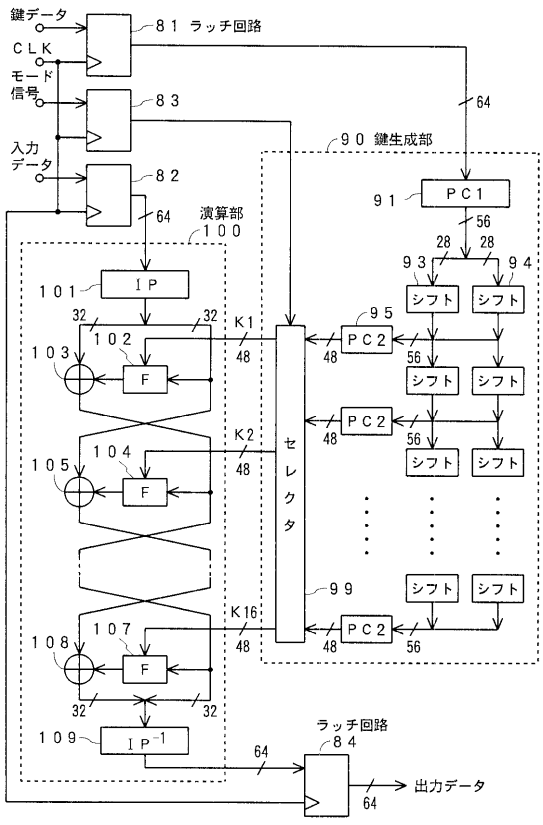
【図３】


ＣＬＫ１
鍵データＫ１～Ｋ１６
（４８ビット）
拡大転置後のデータ
（４８ビット）
ＸＯＲ演算後の
データ
（４８ビット）
ＣＬＫ２

【図４】


記録媒体
5
記録再生
処理部
27
RAM
24
ROM
23
CPU
21
29
28
出力処理部
26
DSP
22
37
I／F
39
32
40
暗号化復号化
処理部
RAM
34
36
USB
ROM
33
CPU
31
20 記録再生装置
30 暗号化復号化装置
2
ダウンロード
10 端末（ＰＣ）
リッピング
1

【図５】


鍵データ
81 ラッチ回路
ＣＬＫ
モード
信号
83
64
入力
データ
82
90 鍵生成部
64
演算部
100
91
ＰＣ１
56
28
28
93
94
101
ＩＰ
シフト
シフト
32
32
K1
95
102
ＰＣ２
48
48
56
103
Ｆ
シフト
シフト
K2
ＰＣ２
56
105
104
Ｆ
シフト
シフト
セレクタ
99
K16
ＰＣ２
107
108
Ｆ
32
32
109
IP^{-1}
ラッチ回路
84
64
出力データ
64

フロントページの続き

(72)発明者　今　孝安
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　青木　重徳

(56)参考文献　特開平１０－３３３５６９（ＪＰ，Ａ）
特開平１０－０２２９９０（ＪＰ，Ａ）
特開２０００－００４１４７（ＪＰ，Ａ）
岡本龍明，山本博資，“シリーズ／情報科学の数学　現代暗号”，産業図書株式会社，１９９８年　6月３０日，第2版，ｐ．８２－８５

(58)調査した分野(Int.Cl.，ＤＢ名)
G09C　1/00
G06F　1/12