(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3621604号
(P3621604)
(45)発行日　平成17年2月16日(2005.2.16)　(24)登録日　平成16年11月26日(2004.11.26)

(51)Int.Cl.[7]　F I
H04L 9/20　H04L 9/00　653

請求項の数 9　(全 15 頁)

(21)出願番号　特願平11-167597
(22)出願日　平成11年6月15日(1999.6.15)
(65)公開番号　特開2000-31941(P2000-31941A)
(43)公開日　平成12年1月28日(2000.1.28)
審査請求日　平成12年9月8日(2000.9.8)
(31)優先権主張番号　09/097782
(32)優先日　平成10年6月15日(1998.6.15)
(33)優先権主張国　米国(US)

前置審査

(73)特許権者　596092698
ルーセント　テクノロジーズ　インコーポレーテッド
アメリカ合衆国．０７９７４－０６３６　ニュージャーシィ，マレイ　ヒル，マウンテン　アヴェニュー　６００
(74)代理人　100064447
弁理士　岡部　正夫
(74)代理人　100085176
弁理士　加藤　伸晃
(74)代理人　100106703
弁理士　産形　和央
(74)代理人　100096943
弁理士　臼井　伸一

最終頁に続く

(54)【発明の名称】音声暗号化コーダ

(57)【特許請求の範囲】
【請求項１】
第１のレベルの符号化された音声ビットを有する第１のブロックと、第２のレベルの符号化された音声ビットを有する第２のブロックとを含むメッセージフレームを暗号化する装置であって、
該第１のブロックを暗号化して、第１の暗号文ブロックを生成する手段と、
反復された第１の暗号文ブロックを生成するために、該第１の暗号文ブロックの少なくとも一部分を該第１の暗号文ブロックに付加することにより鍵ストリームビットを生成する手段であって、該鍵ストリームビットを生成するために該第１の暗号文ブロックの一部分を用いて該反復された第１の暗号文ブロックを暗号化する手段をさらに有する鍵ストリームビットを生成する手段と、
該鍵ストリームビットを用いて、該第２のブロックを暗号化して、第２の暗号文ブロックを生成する手段と、
該第１の暗号文ブロックを用いて、エラー制御ビットを生成する手段とを備えることを特徴とする装置。
【請求項２】
前記第２のブロックが、さらに第１のレベルの符号化された音声ビットを含む請求項１に記載の装置。
【請求項３】
前記第１のブロックが４８個の第１のレベルのビットを含む請求項１に記載の装置。

【請求項４】
前記第２のブロックが５２個の第２のレベルのビットを含む請求項１に記載の装置。
【請求項５】
前記メッセージフレームが、さらに第１のレベルの符号化された音声ビットと第２のレベルの符号化された音声ビットを有する第３のブロックを含み、前記装置が、さらに
前記第３のブロックを前記キー鍵ストリームビットを用いて暗号化して、第３の暗号文ブロックを生成する手段を備える請求項１に記載の装置。
【請求項６】
前記第１のブロックを暗号化する手段が、
前記暗号文ブロックの第２の部分を暗号同期入力として用いて前記第１の暗号文ブロックの第１の部分を暗号化して、第１の出力を生成する手段と、
２進演算を用いて前記第１の出力を前記第一の暗号文ブロックの第３の部分と結合することにより、第２の出力を生成する手段と、
前記第２の出力を暗号同期入力として用いて前記第１の暗号文ブロックの前記第１の部分と第２の部分を暗号化することにより、第１の部分及び第２の部分を有する第３の出力を生成する手段と、
前記第３の出力の前記第２の部分を暗号同期入力として用いて前記第２の出力と前記第３の出力の前記第１の部分を暗号化することにより、第１の部分と第２の部分を有する第４の出力を生成する手段と、
前記第４の出力の前記第１の部分を暗号同期入力として用いて前記第４の出力の前記第１の部分と前記第３の前記第２の部分を暗号化することにより、第５の出力を生成する手段とを備える請求項１に記載の装置。
【請求項７】
前記第１の暗号文ブロックが、前記第５の出力および前記第４の出力の前記第１の部分を含む請求項６に記載の装置。
【請求項８】
前記暗号文ブロックの前記第２の部分を暗号同期入力として用いて前記第１の暗号文ブロックの前記第一の部分を暗号化する手段が、第１のＥＭＣＥＡ機能呼を用いて行われる請求項６に記載の装置。
【請求項９】
前記第１の出力を前記第１の暗号文ブロックの前記第３の部分と結合する手段が、ＸＯＲ演算器を用いて行われる請求項６に記載の装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、一般的には、通信システム、より詳細には、無線通信システムにおいて利用されるエンクリプション（暗号化）技法に関する。
【０００２】
【従来の技術】
無線通信システムは、加入者に対して機密な通信手段を提供するために暗号法（クリプトグラフィ）を用いる。暗号法においては、意図される受信者のみが許可された送信者によって送信されるメッセージ（例えば、音声データ、ユーザデータ、ＦＡＣＣＨ／ＡＳＣＣＨメッセージ）の内容を解読することができ、許可された送信者のみが意図される受信者にメッセージを送信できるようにすることで機密が確保される。暗号法においては、いかにしてメッセージの内容を意図される受信者のみが解読できる形式に変換するかが重要となり、これを送信者と受信者の両方にとって経済的な方法にて達成することが要求される。同時に、無許可の受信者（つまり、意図されない受信者）にとっては、内容を解読することが（時間的および／あるいは装置の点で）非常に困難であることが要求される。無許可の受信者および送信者は、ますます巧妙になってきており、機密の通信に対する要請はますます増大する傾向にある。

【０００３】
図１は、周知の遠隔通信産業協会（Ｔｅｌｅｃｏｍｍｕｎｉｃａｔｉｏｎ　Ｉｎｄｕｓｔｒｉａｌ　Ａｓｓｏｃｉａｔｉｏｎ：ＴＩＡ）の時分割多重アクセス（ＴＤＭＡ）に対するＩＳ－１３６（およびこれらの修正）標準および代数コード励起線形予測（ＡＣＥＬＰ）に対するＩＳ－６４１標準に基づく送信機１０内に組み込まれた音声暗号化プロセッサのアーキテクチャを示す。送信機１０は、音声コーダ（符号器）１２、７－ビット巡回冗長コーダ（７－ビットＣＲＣ）１４、ハーフレート畳み込みコーダ（１／２－レートＣＣ）１６、パンクチャ１８、音声サイファー（暗号化器）２０および２－スロットインタリーバ２２を含む。音声コーダ１２は、特徴として１６０個の１６－ビット音声サンプルから成るメッセージフレーム（音声サンプル）を符号化することで、１４８個の符号化された音声ビットを生成する。これら１４８個の符号化された音声ビットは、９６個のクラス１Ａビットと、５２個のクラス２ビットから成る。特徴として、クラス１ビットは、４８個のクラス１Ａビットと、４８個のクラス１Ｂビットから成る。クラス１ビットは、重要なビット（例えば、ピッチ、イントネーション等を表すビット）であり、これらは、無線リンクを通じて伝送される際にエラー制御保護を必要とする。特徴として、エラー制御保護は、巡回冗長コーティング、畳み込みコーティング、およびビットインタリービングを用いて実現される。このためには、最初に、クラス１Ａビットを、入力として７－ビットＣＲＣ１４に供給することで、７個のエラー制御ビットが生成される。次に、エラー制御ビット、クラス１ビット、および５個のテールビット（特徴としてテールビットは畳み込みコード状態情報から成る）を、入力として１／２－レートＣＣ１６に供給することで、２１６個のコード語ビットが生成される。次に、これら２１６個のコード語ビットに、（パンクチャ１８）を介して、エレージャ挿入を施すことで、２０８個のパンクチャリングされたコード語ビットが生成される。
【０００４】
次に、音声サイファー（暗号化器）２０を用いることで、メッセージが、意図された受信者（受信機）のみがメッセージの内容を解読できるように秘匿化される。より詳細には、パンクチャリングされたコード語ビットおよびクラス２ビットが、入力として音声サイファー（暗号化器）２０に供給される。音声サイファー（暗号化器）２０は、この入力を、意図される受信者（受信機）と関連する２６０ビット固定機密マスクを用いて暗号化することで、２６０個の暗号化されたビットを生成する。より詳細には、このエンクリプション（暗号化）は、パンクチャリングされたコード語ビットとクラス２ビットに、機密マスクを用いて、ＸＯＲ二進演算を施すことで遂行される。次に、暗号化されたビットを（ビットインタリーバ２２にて）ビットインタリーブすることで、２８０個のインタリーブされたビットが生成される。このメッセージが、次に、送信機１０によって、多重化および変調された後に、送信される。
【０００５】
送信されたメッセージは、受信機（図示せず）によって受信され、受信機において、送信機１０と逆の機能が遂行される。つまり、送信されたメッセージを受信すると、受信機は、送信されたメッセージを復調およびデマルチプレキシング（分離）することで、２８０個のインタリーブされたビットを得る。次に、（ビットデインタリーバによって）ビットインタリービングプロセスの逆を遂行することで、２６０個の暗号化されたビットが得られる。次に、これら２６０個の暗号化されたビットを、（音声デサイファー（暗号解読器）によって）解読することで、２０８個のパンクチャリングされたコード語ビットと、５２個のクラス２ビットから成る出力が得られる。受信者が、送信機によって採用される上述の２６０ビット固定機密マスクを知らない場合（つまり、受信者が意図される受信者でない場合は）、受信者は、これら暗号化されたビットを正しく解読することはできない。
【０００６】
次に、パンクチャリングされたコード語ビットが１／２－レート畳み込みデコーダに供給される。１／２－レート畳み込みデコーダにおいて、これらパンクチャリングされたコード語ビットに、逆畳み込み操作を施すことで、９６個のクラス１ビット（特徴として、ク

ラス１ビットは、４８個のクラス１Ａビットと４８個のクラス１Ｂビットから成る）と、７個のエラー制御ビットから形成される出力が得られる。受信機の所には、エレージャ挿入プロセスの逆の機能は存在しないことに注意する。エレージャ挿入に起因するビット損失は、当分野において周知のように、逆畳み込みプロセスによって回復される。

【０００７】

次に、クラス１Ａビットが受信機の所の７－ビットＣＲＣに供給され、第二のセットの７個のエラー制御ビットが生成される（特徴として、第一のセットの７個のエラー制御ビットは、１／２－レート畳み込みデコーダの出力の部分から成る）。次に、これら第一と第二のセットのエラー制御ビットを（ＣＲＣチェックを用いて）比較することで、クラス１Ａビットの伝送にエラーが発生したか否か（つまり、不良フレームが存在するか否か）決定される。伝送エラーが発生してない場合は、クラス１ビットと、（音声デサイファーからの）クラス２ビットは、音声デコーダにパスされ、復号される。伝送エラーが発生した場合（つまり、不良フレームが検出された場合）は、クラス１Ａビットと３２個の最上位のクラス１Ｂビットは破棄され、代わりに、直前の良好なフレームのクラス１Ａビットおよび３２個の最上位のクラス１Ｂビットのある関数あるいは挿間が音声デコーダにパスされる。次に、（音声デサイファーからの）クラス２ビットと、（１／２－レート畳み込みデコーダからの）１６個の最下位のクラス１Ｂビットが音声デコーダにパスされ、音声デコーダ内で、これらが、パスされた直前の良好なフレームのクラス１Ａビットと３２個の最上位のクラス１Ｂビットの関数あるいは挿間と共に復号される。クラス２ビットと１６個の最下位のクラス１Ｂビット内にビットエラーが存在した場合でも、これらエラーは、残りのクラス１Ｂとクラス１Ａビット内のエラーと比較して、音声品質に与える知覚的な影響は小さい。

【０００８】

音声サイファー（暗号化器）を組み込む従来の技術による暗号アーキテクチャは幾つかの長所を持つ。第一に、両方の端（つまり、送信機と受信機）の所で２６０ビット固定機密マスクを同期するために、外部源からの暗号同期入力（以降、“外部暗号同期入力（ｅｘｔｅｒｎａｌ　ｃｒｙｐｔｏｓｙｎｃ）”と呼ぶ）は必要とされない。ここで、暗号同期入力とは、２つの暗号アルゴリズムが互いに同期されることを確保するためのデータ入力である。第二に、伝送エラーが発生した場合でも音声品質の劣化はない。つまり、クラス１Ａビットと３２個の最上位のクラス１Ｂビットの伝送エラーは、直前の良好なフレームのクラス１Ａビットと３２個の最上位のクラス１Ｂビットのある関数あるいは挿間を用いてマスクすることができる。

【０００９】

【発明が解決しようとする課題】

ただし、従来の技術によるエンクリプション（暗号）アーキテクチャは、以下の２点において機密の問題に弱い。第一に、２６０ビット固定機密マスクは、既知の平文（つまり、音声サイファーへの入力）を用いて決定することができ、次に、これを用いて、暗号化されたビットを解読（あるいはデクリプト）することができ、従って、送信されたメッセージの機密性には問題が残る。第二に、既知の平文がない場合でも、単に、隣接する２６０ビットフレームにＸＯＲを施すことで固定機密マスクを除去し、ＡＣＥＬＰ音声アルゴリズムのパラメータがどのように変化しているかの情報を得ることができる。従って、外部暗号同期入力を用いる必要がなく、音声の劣化が最小で、しかも、改善された機密性を達成することができる音声プロセッサアーキテクチャに対する必要性が存在する。

【００１０】

【課題を解決するための手段】

本発明は、外部暗号同期入力を用いる必要がなく、音声の劣化が最小で、しかも、改善された機密性を達成することができる音声暗号プロセッサアーキテクチャに関する。本発明によると、これは、送信機側に、（例えば、音声サイファー内に実現される固定機密マスクエンクリプション（暗号）スキームの代わりに）、ブロックエンクリプタ（暗号化器）と、キー（鍵）ストリーム発生器を組み込み、これによって、符号化された音声ビットを

暗号化することによって達成される。ブロックエンクリプタ（暗号化器）は、インバーチブル（逆変換可能な）クリプトグラフィック（暗号）アルゴリズムと、内部暗号同期入力を用いて、第一のブロックの符号化された音声ビットを、第一の暗号文ブロックに変換する。特徴として、第一のブロックの符号化された音声ビットは、伝送においてエラーが発生した場合、直前の良好なフレームからのある関数あるいは挿間の代わりに、これら誤ったビットを用いた場合は、音声品質に重大な知覚上の劣化を与える第一のレベルのビットを含む。

【００１１】

次に、第一の暗号文ブロックが、入力としてキー（鍵）ストリーム発生器と巡回冗長チェック（コーダ）に供給される。キーストリーム発生器は、キード一方向機能として用いられるインバーチブル暗号アルゴリズムと内部暗号同期入力を用いて、第一の暗号文ブロックをキー（鍵）ストリームに変換する。特徴として、このキー（鍵）ストリームは、暗号化された第一の暗号文ブロックから成る。その後、このキー（鍵）ストリームを用いて、第二と第三のブロックの符号化された音声ビットを暗号化することで、それぞれ、第二と第三の暗号文ブロックが生成される。特徴として、第三のブロックの符号化された音声ビットは、第一の暗号文ブロックの伝送においてエラーが発生した場合でも、音声品質に、殆ど、あるいは、全く、知覚上の悪影響を与えない第二のレベルのビットを含み、第二のブロックの符号化された音声ビットは、第一と第二のレベルのビットを含む。

【００１２】

巡回冗長チェックにおいては、第一の暗号文ブロックを用いて、エラー制御ビットが生成される。このエラー制御ビットは、第一の暗号文ブロックの伝送にエラーが発生したか否か、つまり、第一の暗号文ブロックが、あるタイプの伝送エラー検出機構によって保護されているか否かを決定するために用いられる。次に、第一、第二、および第三の暗号文ブロックと、エラー制御ビットが、処理され、送信される。

【００１３】

受信機においては、エラー制御ビットと受信された第一の暗号文ブロックを用いて、第一の暗号文ブロックの伝送にエラーが発生したか否か決定される。エラーが検出されなかった場合は、ブロックデクリプタ（暗号解読器）によって受信された第一の暗号文ブロックが解読され、次に、解読された第一の暗号文ブロックを用いて、受信された第二と第三の暗号文ブロックが（送信機側のキーストリーム発生器と同一のキーストリーム発生器を介して）解読される。エラーが検出された場合は、（第一と第二の暗号文ブロック内の）第一のレベルのビットは、一つあるいは複数の直前の良好な第一のレベルのビットのある関数あるいは挿間を用いてマスクされる。（第二と第三の暗号文ブロック内の）第二のレベルのビットは、処理サイクルを節約するために、（誤差を伴って）解読することなく、直接に音声デコーダにパスされる。

【００１４】

長所として、本発明のこの実施例は、第一のレベルのビット内のエラーを拡大することはない。より詳細には、受信された第一の暗号文ブロック内に任意のビットにエラーが発生した場合でも、このエラーは、第一のレベルのビットの全てが一つあるいは複数の直前の良好なフレームの第一のレベルのビットのある関数あるいは挿間によってマスクされるために、他の第一のレベルのビットに拡大することはない。受信された第一の暗号文ブロック内の任意のビットに発生したエラーは、第二のレベルのビットには拡大するが、ただし、このエラーは、音声品質に、殆ど、あるいは全く、知覚的な悪影響を与えることはない。他方、受信された第一の暗号文ブロックのビットにエラーが全く存在しない場合も、エラーは、他の第一のレベルあるいは第二のレベルのビットに拡大することはない。さらに、第二と第三の受信された暗号文ブロック内の任意のエラーも、キーストリームが平文とＸＯＲ処理される本発明のキーストリーム発生器アーキテクチャのために他のビットには拡大することはない。

【００１５】

さらに、本発明のブロックエンクリプタ（暗号化器）とキー（鍵）ストリーム発生器は、

長所として、従来の技術において用いられる音声サイファー（暗号化器）に採用される２６０ビット固定機密マストと比較して、暗号方式上遙かに機密なクリプトグラフィック（暗号）アルゴリズム（すなわち、キード一方向機能）を採用する。このため、本発明の音声暗号化プロセッサアーキテクチャは、従来の技術と比較して、暗号方式上遙かに安全である。加えて、エンクリプティング（暗号）アルゴリズムとデクリプティング（暗号解読）アルゴリズムとを同期させるためには、内部暗号同期入力が用いられ、従って、外部暗号同期入力は必要とされない。

本発明の特徴、様々な面、および長所が、以下の詳細な説明、特許請求の範囲、および付録の図面を参照することでより良く理解できるものである。

【００１６】

【発明の実施の形態】

図２は、本発明において用いられる送信機３０内に組み込まれる音声プロセッサアーキテクチャを示す。本発明は、ここでは、解説の目的で、周知の時分割多重アクセス（ＴＤＭＡ）に対するＩＳ－１３６（およびこれらの修正）標準およびＡｌｇｅｂｒａｉｃ Ｃｏｄｅ Ｅｘｃｉｔｅｄ Ｌｉｎｅａｒ Ｐｒｅｄｉｃｔｉｏｎ（代数的コード励起線形予測）（ＡＣＥＬＰ）に対するＩＳ－６４１標準に基づく音声プロセッサアーキテクチャとの関連で説明されるが、ただし、これは、本発明をどのようにも限定するものではないことに注意する。

【００１７】

送信機３０内に組み込まれる音声プロセッサアーキテクチャは、音声コーダ（符号化器）３２、ブロックエンクリプタ（暗号化器）３４、キー（鍵）ストリーム発生器３６、ＸＯＲオペレータ３８、４０、７－ビット巡回冗長コーダ（７－ビットＣＲＣ）４２、ハーフレート畳み込みコーダ（１／２－レートＣＣ）４４、パンクチャ４６、および２－スロットインタリーバ４８を含む。この音声プロセッサアーキテクチャは、コンピュータプロセッサ上で実行するソフトウエア、アプリケーションスペシフィック集積チップ、その他、として実現することができる。音声コーダ３２、ＸＯＲオペレータ３８、４０、７－ビットＣＲＣ４２、１／２－レートＣＣ４４、パンクチャ４６、および２－スロットインタリーバ４８は、当分野において周知である。ブロックエンクリプタ３４およびキーストリーム発生器３６については後に説明される。

【００１８】

音声コーダ３２は、送信されるべきメッセージフレームを受信するが、これは、特徴として、１６０個の１６－ビット音声サンプルである。“音声サンプル（ｓｐｅｅｃｈ ｓａｍｐｌｅｓ）”なる用語は、この明細書の目的に対しては、音声データ、ユーザデータ、チャネル制御（制御チャネル）メッセージ等を含むが、ただし、これに限定されるものではない。このフレームを音声コーダ３２によって符号化することで、出力$_{32}$が生成される。この出力$_{32}$は、特徴として、１４８個の符号化された音声ビットから構成され、これら音声ビットは、第一と第二のレベルの符号化された音声ビットから成り、特徴として、第一のレベルの（符号化された音声）ビットは、第一のブロック内の任意のビットに伝送エラーが発生した場合、音声品質を知覚的に劣化させる音声特性を持ち、第二のレベルの（符号化された音声）ビットは、第一のブロック内のビットに伝送エラーが発生した場合でも音声品質を知覚的に劣化させない音声特性を持つ。より詳細には、この明細書において特徴として言及される符号化された音声ビットについて記述する図３のテーブル４５を参照されたい。

【００１９】

符号化された音声ビットは、次に、３つのブロックに割り振られ、処理される。第一のブロック（ここでは、クラス１Ａビットあるいは出力$_{32-1}$とも呼ばれる）は、４８個の第一のレベルのビットを含み；第二のブロック（ここでは、クラス１Ｂビットあるいは出力$_{32-2}$とも呼ばれる）は、３２個の第一のレベルのビットと１６個の第二のレベルのビットを含み；第三のブロック（ここでは、クラス２ビットあるいは出力$_{32-3}$とも呼ばれる）は、５２個の第二のレベルのビットを含む。より詳細には、第二のブロックに関

しては、第一のレベルのビットは、３２個の最上位ビットから選択され、第二のレベルのビットは、１６個の最下位ビットから選択される。ただし、本発明は、符号化された音声ビットが割り振られるブロックの数、あるいは各ブロック内のビットの数によって限定されるものではない。第一のレベルのビットは伝送エラーが発生した場合、音声品質を知覚的に劣化させる。このため、可能な限り多くのこれらビットに、エラー制御保護が適用され、特徴として、このエラー制御保護は、例えば、巡回冗長コーティングおよび畳み込みコーティングを介して実現される。

【００２０】

音声コーダ３２から、クラス１Ａビット（第一のブロック）は、入力としてブロックエンクリプタ（暗号化器）３４に供給され、クラス１Ｂビット（第二のブロック）は、入力としてＸＯＲオペレータ３８に供給され、クラス２ビット（第三のブロック）は、入力としてＸＯＲオペレータ４０に供給される。ブロックエンクリプタ３４（暗号化器）は、意図される受信機と関連するキー（鍵）を持つインバーチブル（逆変換可能な）暗号アルゴリズムを用いて、ブロックの平文をブロックの暗号文に暗号化（エンクリプト）する。このような暗号アルゴリズムの例としては、ＲＣ５および改良型セルラメッセージング暗号化アルゴリズム（ＥＣＭＥＡ）が含まれる。ＲＣ５は、ロン　リベスト（Ｒｏｎ　Ｒｉｖｅｓｔ）によって開発されたものであり、当分野において周知である。ＥＣＭＥＡは、ロバート　ランス、ダニエル　ビーア、セムヨン　モジコフスキーら（Ｒｏｂｅｒｔ　Ｒａｎｃｅ、Ｄａｎｉｅｌ　Ｈｅｅｒ、Ｓｅｍｙｏｎ　Ｍｉｚｉｋｏｖｓｋｙ）によって開発されたものである。ＥＣＭＥＡは、１９９７年１０月２８日に、ＴＩＡのメンバーが出席したＴＩＡ　ＴＲ４５専門認証委員会（ＴＩＡ　ＴＲ４５　Ａｄ－Ｈｏｃ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｇｒｏｕｐ）の会議において開示されたものであり、合衆国商務省の輸出管轄区の管理下で、輸出管理規制（タイトル１５ＣＲＦパーツ７３０～７７４）の規定に基づいて制限付きで入手できる。

【００２１】

ブロックエンクリプタ（暗号化器）３４内で、クラス１Ａビットが暗号化され、出力$_{34}$が生成されるが、この出力$_{34}$は、特徴として、４８個のクラス１Ａ暗号文ビット（すなわち第一の暗号文ブロック）から成る。図４は、本発明の一つの実施例によるＥＣＭＥＡを採用して４８ビットの平文を暗号文に暗号化するブロックエンクリプタ３４の基本ブロック図を示す。このブロックエンクリプタ３４は、第一、第二、および第三の機能呼５２、５４、５８（入力を暗号化するために暗号化モードにて動作する）、およびＸＯＲオペレータ５６を含む。クラス１Ａビットの第一と、第二の１６ビット部分（以降、それぞれ、第一と、第二のクラス１Ａ部分と呼ぶ）は、入力として、それぞれ、第一と第二のＥＣＭＥＡ機能呼５２、５４に供給される。第一のＥＣＭＥＡ機能呼５２は、第一のクラス１Ａ部分を、第二のクラス１Ａ部分を暗号同期入力として用いて、暗号化することで、１６ビット出力$_{52}$を生成する。

【００２２】

当分野においては周知のように、暗号同期入力は、暗号化（エンクリプティング）アルゴリズムと暗号解読（デクリプティング）アルゴリズムを同期する目的で用いられる。ただし、ＥＣＭＥＡにおいては、加えて、暗号同期入力は、ＥＣＭＥＡの暗号強度を強化するためのキーイングビットとしても用いられる。この機能に対しては、ＥＣＭＥＡは、キードハッシュ機能として用いられ、これによって、第一と第二のクラス１Ａ部分のエントロピーが濃縮されると共に、４８－ビットブロックエンクリプタの暗号強度が増加される。

【００２３】

ＸＯＲオペレータ５６内で、出力$_{52}$と、クラス１Ａビットの第三の１６ビット部分（以降、第三のクラス１Ａ部分と呼ぶ）とに、ＸＯＲ演算を施すことで、１６ビット出力$_{56}$が生成される。

【００２４】

出力$_{56}$は、入力として、第二と第三のＥＣＭＥＡ機能呼５４、５８に供給される。第二のＥＣＭＥＡ機能呼５４は、出力$_{56}$を暗号同期入力として用いて、それぞれ、第一と第

二のクラス１Ａ部分を暗号化することで、それぞれ、１６ビット出力$_{54-1}$と、１６ビット出力$_{54-2}$を生成する。第三のＥＣＭＥＡ機能呼５８は、出力$_{54-2}$を暗　号同期入力として用いて、出力$_{56}$と出力$_{54-1}$を暗号化することで、３２ビットの出力５８を生成する。図５は、図４に示すブロックエンクリプタ３４と逆の機能を遂行する４８ビットデクリプタ３５の機能ブロック図を示す。

【００２５】

出力$_{58}$と出力$_{54-2}$は、集合的に、ブロックエンクリプタ３４の出力$_{34}$を形成する。出力$_{34}$は、入力として、７－ビットＣＲＣ４２、１／２－レートＣＣ４４、キー（鍵）ストリーム発生器３６に供給される。７－ビットＣＲＣ４２内では、出力$_{34}$を用いて　出力$_{42}$が生成されるが、出力$_{42}$は、特徴として、エラー制御ビットを形成する。出力$_{42}$は、その後、入力として１／２－レートＣＣ１４に供給される。

【００２６】

キー（鍵）ストリーム発生器３６は、意図される受信機と関連するキー（鍵）を持つＲＣ５やＥＣＭＥＡ等のインバーチブル暗号アルゴリズムあるいは適当な非インバーチブルキード一方向機能を用いて、キー（鍵）ストリームのビットを出力する。一方向機能は、一般タイプの暗号化動作であり、実際には、インバーチブル暗号アルゴリズムをサブクラスとして含む。キード一方向機能の出力を観察する人物は、キー（鍵）も入力も推測することはできない。

【００２７】

キー（鍵）ストリーム発生器３６は、４８個の１Ａ暗号文ビット（つまり、出力$_{34}$）によって駆動されるが、これが、キーストリーム発生器の入力の所で、与えられた１０４ビットブロックを満たすために十分な回数だけ反復される。キーストリーム発生器３６内では、クラス１Ａ暗号文ビットを暗号化することでキー（鍵）ストリーム出力$_{36}$が生成される。この出力$_{36}$は、特徴として、１００ビットの暗号化されたクラス１Ａ暗号文ビットから成る。より詳細には、出力$_{36}$は、（キーストリーム発生器３６によって採用される）暗号アルゴリズムをランし、公知の擬似ランダムデータを暗号化することで生成されるが、この公知の擬似ランダムデータは、実際には、クラス１Ａ暗号文ビットである。（特徴として、１０４ビットである）クラス１Ａ暗号文ビットの内の４ビットは、ＥＣＭＥＡ（および他の殆どのブロックアルゴリズム）は、整数個のバイトしか暗号化しないために、破棄されることに注意する。

【００２８】

図６は、本発明の一つの実施例によるＥＣＭＥＡを採用するキー（鍵）ストリーム発生器３６の機能ブロック図を示す。キーストリーム発生器３６は、ＥＣＭＥＡ機能６２を含む。ＥＣＭＥＡ機能６２は、１０４ビットブロック入力を受信するが、この入力は、特徴として、ブロックエンクリプタ３４からの反復出力$_{34}$から成る。ブロックエンクリプタ３４からの出力を、付加あるいは自身に連結することで、９６個のビットが得られ、さらにこれをもう一度、部分的に付加することで、キーストリーム発生器への１０４ビット入力が得られる。この１０４ビットのブロック入力を、ＥＣＭＥＡ機能呼６２によって、出力$_{34}$の１６個の最上位ビット（つまり４８個のクラス１Ａ暗号文ビットの内の１６個の最上位ビット）を暗号同期入力として用いて、暗号化することで、出力$_{36}$が生成される。

【００２９】

出力$_{36}$は、入力として、ＸＯＲオペレータ３８と、ＸＯＲオペレータ４０に供給される。より詳細には、出力$_{36}$の４８ビット部分は、入力としてＸＯＲオペレータ３８に供給され、出力$_{36}$の５２ビット部分は、入力としてＸＯＲオペレータ４０に供給される。ＸＯＲオペレータ３８内においては、クラス１Ｂビット（つまり、第二のブロック）と、出力$_{36}$の４８ビット部分とのＸＯＲ演算が遂行され、出力$_{38}$が生成される。出力$_{38}$は、特徴として、４８個のクラス１Ｂ暗号ビット（つまり、第二の暗号文ブロック）から成る。出力$_{38}$は、次に、入力として、１／２－レートＣＣ４４に供給される。同様に、ＸＯＲオペレータ４０内においては、クラス２ビット（つまり、第三のブロック　）と、出力$_{36}$の５２ビット部分とのＸＯＲ演算が遂行され、出力$_{40}$が生成される。出力$_{40}$は

、特徴として、５２個のクラス２暗号文ビット（つまり、第三の暗号文ブロック）から成る。出力$_{40}$は、次に、入力として、２－スロットインタリーバ４８に供給される。

【００３０】

１／２－レートＣＣ４４内においては、出力$_{42}$、出力$_{34}$、および出力$_{38}$を５個のテールビット（特徴として、これは、畳み込みコード状態情報から成る）と共に用いることで、出力$_{44}$が生成される。出力$_{44}$は、特徴として、２１６個のコード語ビットから成る。次に、出力$_{44}$は、パンクチャ４６に供給され、パンクチャ４６によって、出力$_{46}$が生成される。出力$_{46}$は、特徴として、２０８個のパンクチャリングされたコード語ビットから成る。出力$_{46}$は、次に、２－スロットインタリーバ４８に供給され、ここで、これを、出力$_{40}$とビットインタリーブすることで、出力$_{48}$が生成される。出力$_{48}$は、特徴として、２８０個のインタリーブされたビットから成る。出力$_{48}$は、次に、送信機３０によって、多重化および変調された後に、送信される。

【００３１】

送信されたメッセージは、受信機によって受信され、受信機内で、送信機１０と逆の機能が遂行される。図７は、本発明において用いられる受信機７０内に組み込まれる音声プロセッサアーキテクチャを示す。受信機７０内に組み込まれる音声プロセッサアーキテクチャは、音声デコーダ（復号器）７２、ブロックデクリプタ（暗号解読器）７４、キー（鍵）ストリーム発生器７６、ＸＯＲオペレータ７８、８０、７－ビットＣＲＣ８２、１／２－レート畳み込みデコーダ８４、および２－スロットビットデインタリーバ８６を含む。この音声プロセッサアーキテクチャは、コンピュータプロセッサ上で実行するソフトウエア、アプリケーションスペシフィック集積チップ、その他、として実現することができる。音声デコーダ７２、ＸＯＲオペレータ７８、８０、７－ビットＣＲＣ８２、１／２－レート畳み込みデコーダ８４、および２－スロットビットデインタリーバ８６は、当分野において周知である。ブロックデクリプタ（暗号解読器）７４とキー（鍵）ストリーム発生器７６については後に詳細に説明される。

【００３２】

送信されたメッセージを受信すると、受信機は、送信されたメッセージを復調およびデマルチプレキシング（分離）することで、出力$_{48'}$（つまり、２６０個のインタリーブされたビット）を得る。ここで、プライム表記（’）は、送信バージョンに対応する受信バージョンを示すことに注意する。２－スロットビットデインタリーバ８６は、出力$_{48'}$を用いて、出力$_{46'}$（つまり、２０８個のパンクチャリングされたコード語ビット、および、５２個のクラス２暗号文ビットすなわち第三の暗号文ブロック）を生成する。２０８個のパンクチャリングされたコード語ビットは、次に、１／２－レート畳み込みデコーダ８４に供給される。１／２－レート畳み込みデコーダ８４よって、逆畳み込み演算を施すことで、５個のテールビット、出力$_{42'}$（つまり、７個のエラー制御ビット）、出力$_{34'}$（つまり、４８個のクラス１Ａ暗号文ビット、すなわち第一の暗号文ブロック）、および出力$_{38'}$（つまり、４８個のクラス１Ｂ暗号文ビット、すなわち第二の暗号文ブロック）が得られる。注意すべき点として、受信機７０においては、パンクチャ４６のエレージャ挿入プロセスの逆を遂行する動作は存在せず、エレージャ挿入に起因するビット損失は、受信機内においては、１／２－レート畳み込みデコーダによって回復される。

【００３３】

出力$_{34'}$は、入力として、７－ビットＣＲＣ８２に供給され、これによって、第二のセットの７個のエラー制御ビットが生成される。（特徴として、第一のセットの７個のエラー制御ビットは、集合的に出力$_{42'}$を形成し、これらは１／２－レート畳み込みデコーダによって出力される７ビットのエラー制御ビットから成る）。これら第一と第二のセットのエラー制御ビットを調べることで、第一の暗号文ブロック（すなわち、クラス１Ａ暗号文ビット）の伝送に、エラーが発生したか否か（つまり、不良フレームが存在するか否か）決定される。伝送エラーが発生してない場合は、出力$_{34'}$（すなわち、クラス１Ａ暗号文ビット）は、ブロックデクリプタ（暗号解読器）７４と、キー（鍵）ストリーム発生器７７にパスされる。ブロックデクリプタ（暗号解読器）７４は、ブロックエンクリプ

タ３４の逆の機能を遂行する。これに関しては、図４に示すブロックエンクリプタ３４の逆の機能を遂行する４８ビットデクリプタ３５の機能ブロック図を示す図５を参照されたい。

【００３４】

ブロックデクリプタ（暗号解読器）７４内で、出力$_{34'}$を解読することで、出力$_{32-1'}$（すなわち、４８個のクラス１Ａビット）が得られる。キーストリーム発生器７６内で、出力$_{34'}$を用いることで、キー（鍵）ストリーム出力$_{36'}$（すなわち、１００個の暗号化されたクラス１Ａ暗号化ビット）が生成される。次に、このキー（鍵）ストリームと、出力$_{38'}$（すなわち、クラス１Ｂ暗号文ビット）とのＸＯＲ演算により、出力$_{32-2'}$（すなわち、クラス１Ｂビット）が得られ、このキー（鍵）ストリームと出力$_{40'}$（つまり、クラス２暗号文ビット）とのＸＯＲ演算により、出力$_{32-3'}$（すなわち、クラス２ビット）が得られる。次に、出力$_{32-1'}$、出力$_{32-2'}$、および出力$_{32-3'}$（すなわち、クラス１Ａビット、クラス１Ｂビット、およびクラス２ビット）を、音声デコーダ７２によって復号することで、元のメッセージフレームが得られる。

【００３５】

伝送エラーが発生した場合は、第一のレベルのビット（つまり、クラス１Ａビット、および３２個の最上位のクラス１Ｂビット）は破棄され、代わりに、（周知のＩＳ－６４１標準において記述されるように）一つあるいは複数の直前の良好なフレームの第一のレベルのビットのある関数あるいは挿間が音声デコーダにパスされる。ＣＲＣに失敗した場合は、クラス１Ａビットのブロック解読、並びに（キーストリーム発生器を用いての）キーストリームの発生は、これらデータは無効とされるために必要ない。従って、この場合は、第二のレベルのビット（つまり、クラス２ビットおよび１６個の最下位のクラス１Ｂビット）の解読も行なわれない。これらタスクの回避は、プロセッササイクルの節約となる。これら第二のレベルのビットが暗号化されたままに留まることに起因する音声品質の劣化によって、知覚的な悪影響が出ることは、殆どあるいは全くない。

【００３６】

本発明によって、音声プライバシーと類似するやり方で、暗号同期データが外部からではなく内部的に発生されるＦＡＣＣＨおよびＳＡＣＣＨメッセージのプライバシーを実現することもできるここに注意する。この場合は、各ＦＡＣＣＨおよびＳＡＣＣＨメッセージの第一の語は、８ビットのメッセージタイプ（Ｍｅｓｓａｇｅ　Ｔｙｐｅ）を含み、これらは、暗号化されないままに留められることを必要とされる。この実現においては、例えば、各ＦＡＣＣＨあるいはＳＡＣＣＨメッセージの第一の語に対しては、図８（および図９）に示すように、４０ビットブロックエンクリプタ（暗号化器）８０（およびデクリプタ（暗号解読器）９０）が用いられ、残りの語に対しては、図４の４８ビットブロックエンクリプタ（暗号化器）が用いられる。

【００３７】

本発明が幾つかの実施例との関連でかなり詳細に説明されたが、他のバージョンも可能である。例えば、他のエンクリプタ（暗号化器）およびデクリプタ（暗号解読器）を用いることも可能である。例えば、図１０には、ＲＣ５を採用する４８ビットブロックエンクリプタ（暗号化器）１００が示される。当業者においては明らかなように、本発明の概念は、他のタイプの音声コーダ、エラー制御機構、およびエンクリプションおよび／あるいはクリプトグラフィック（暗号）アルゴリズムを利用する音声プロセッサアーキテクチャにも適用することができる。従って、本発明の精神および範囲は、ここに含まれる実施例の説明に限定されるものではない。

【図面の簡単な説明】

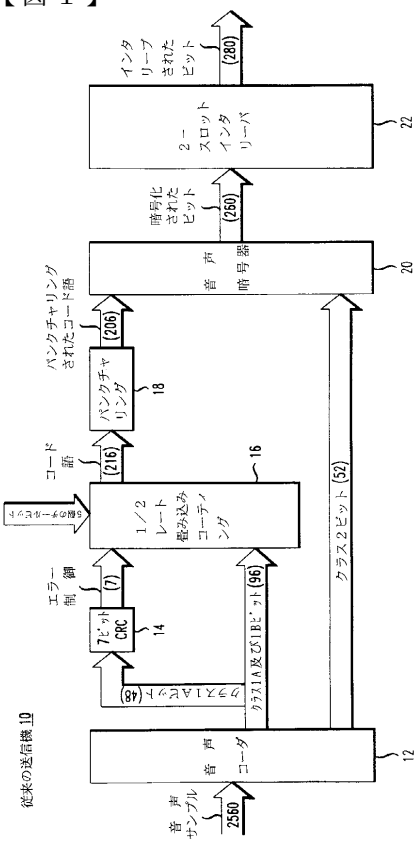
【図１】従来の技術による音声プロセッサ、エラー保護、音声暗号化アーキテクチャを示す図である。

【図２】本発明において用いられる送信機内に組み込まれる音声プロセッサアーキテクチャを示す図である。

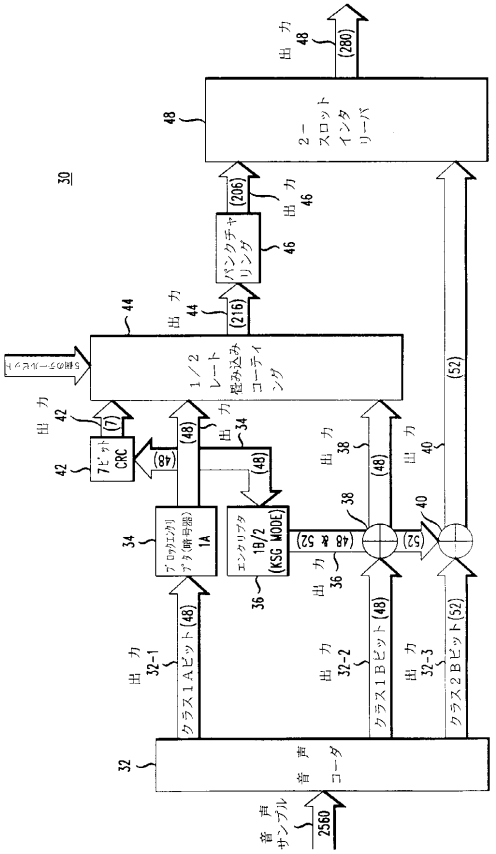
【図３】この明細書において言及される本発明に特徴的な符号化された音声ビットについ

て記述する表である。
【図４】本発明による４８ビットブロックを平文から暗号文に暗号化するための改良されたセルラメッセージング暗号化アルゴリズム（ＥＣＭＥＡ）を採用するブロックエンクリプタ（暗号化器）の機能ブロック図である。
【図５】図４に示すブロックエンクリプタ（暗号化器）の逆の機能を遂行するための４８ビットブロックデクリプタ（暗号解読器）の機能ブロック図である。
【図６】本発明の一つの実施例によるＥＣＭＥＡを採用するキー（鍵）ストリーム発生器の機能ブロック図を示す図である。
【図７】本発明において採用される受信機内に組み込まれる音声プロセッサアーキテクチャを示す図である。
【図８】本発明の一つの実施例によるＥＣＭＥＡを採用する４０ビットブロックエンクリプ　タ（暗号化器）の機能ブロック図である。
【図９】図８に示すブロック暗号化器の逆の機能を遂行するための４０ビットブロックデクリプタ（暗号解読器）の機能ブロック図である。
【図１０】本発明の一つの実施例によるＲＣ５を採用する４８ビットブロックエンクリプタ（暗号化器）の機能ブロック図である。
【符号の説明】
３０　送信機
３２　音声コーダ（符号器）
３４　ブロックエンクリプタ（暗号化器）
３６　キー（鍵）ストリーム発生器
３８、４０、７８、８０　ＸＯＲオペレータ
４２、８２　７－ビット巡回冗長コーダ（７－ビットＣＲＣ）
４４　ハーフレート畳み込みコーダ（１／２－レートＣＣ）
４６　パンクチャ
４８　２－スロットインタリーバ
７０　受信機
７２　音声デコーダ（復号器）
７４　ブロックデクリプタ（暗号解読器）
７６　キー（鍵）ストリーム発生器
８４　１／２－レート畳み込みデコーダ
８６　２－スロットビットデインタリーバ

【図１】



【図２】

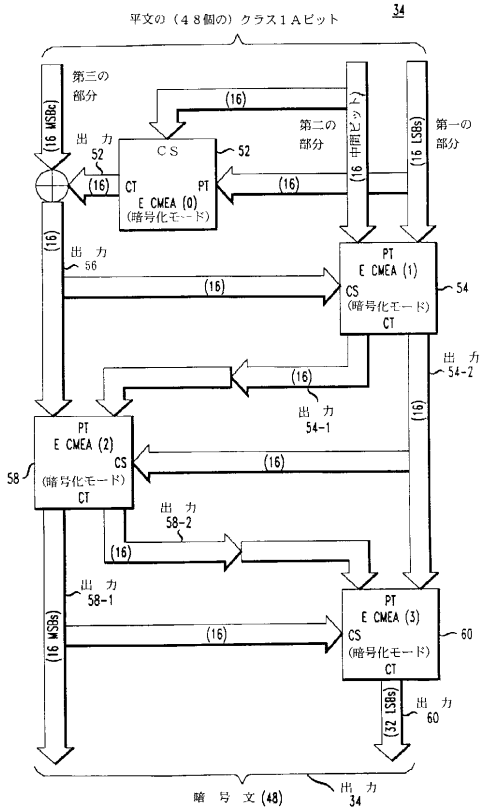


【図３】

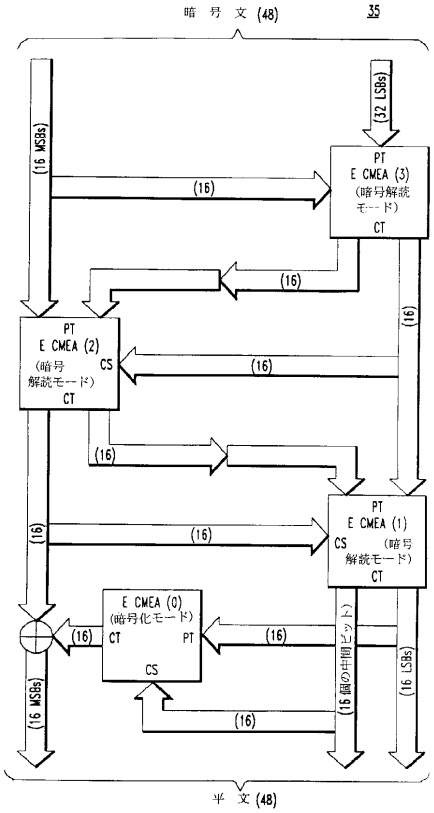
45

１４８個の符号化された音声ビット		
８０個の第一のレベルのビット	６８個の第二のレベルのビット	
出　力 32-1	出　力 32-2	出　力 32-3
第一のブロック	第二のブロック	第三のブロック
４８個のクラス１Aビット	４８個のクラス１B 32個の第一のレベルのビット 16個の第二のレベルのビット	５２個のクラス２ビット

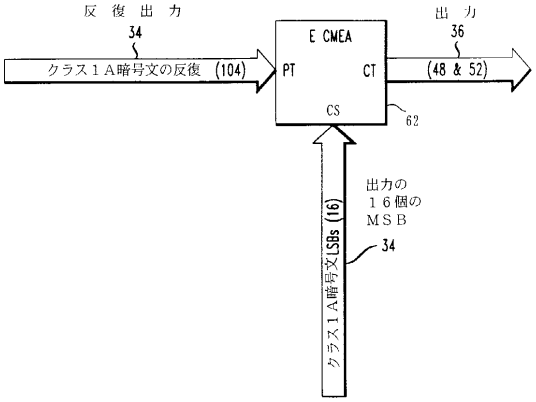
【図４】



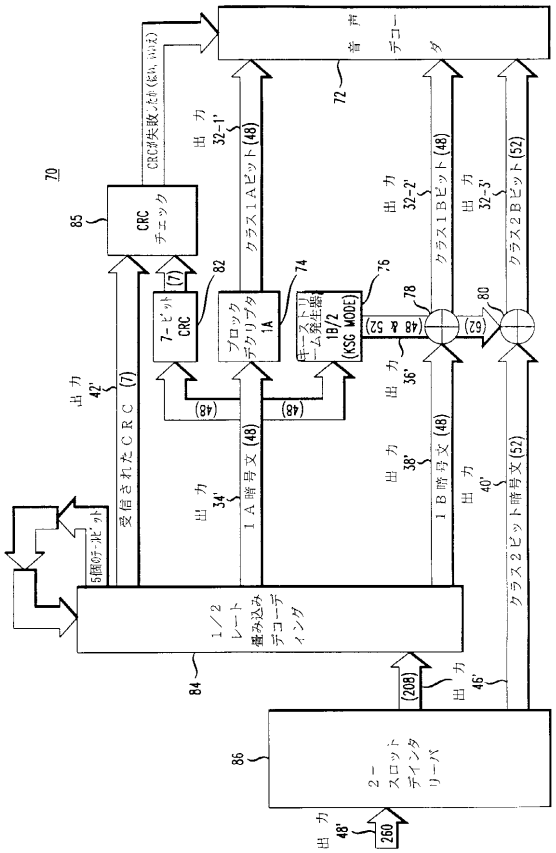
【図５】


暗号文(48)
35
(16 MSBs)
(32 LSBs)
PT
E CMEA (3)
(暗号解読モード)
CT
(16)
PT
E CMEA (2)
(暗号解読モード)
CS
CT
PT
E CMEA (1)
CS
(暗号解読モード)
CT
E CMEA (0)
(暗号化モード)
CT
PT
CS
(16 MSBs)
(16 個の中間ビット)
(16 LSBs)
平文(48)

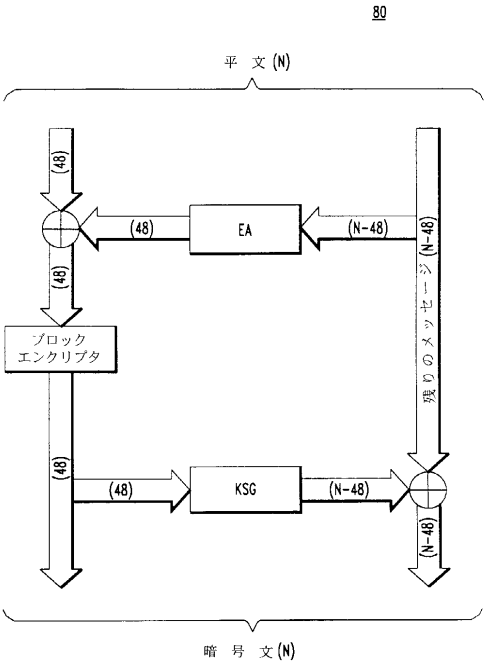
【図６】


反復出力
34
クラス１Ａ暗号文の反復 (104)
E CMEA
PT
CT
CS
62
出力
36
(48 & 52)
出力の
１６個の
ＭＳＢ
34
クラス１Ａ暗号文LSBs (16)

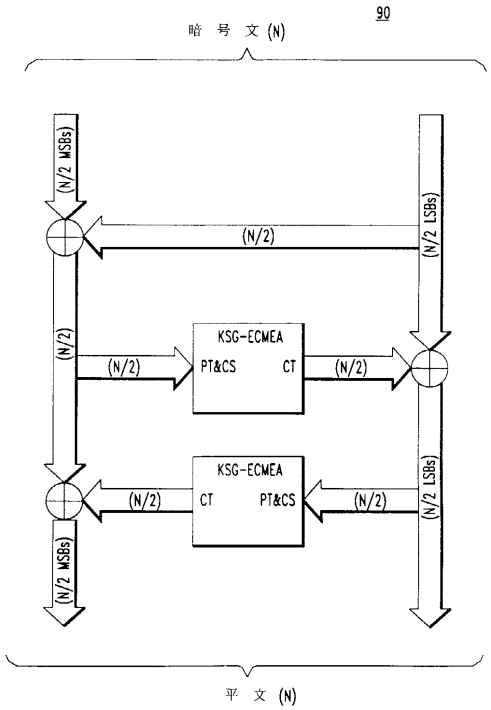
【図７】


70
音声デコーダ
72
CRCが失敗したか(はい、いいえ)
CRCチェック
85
出力 32-1'
クラス１Ａビット(48)
出力 32-2'
クラス１Ｂビット(48)
出力 32-3'
クラス２Ｂビット(52)
7-ビット CRC
(7)
82
ブロックデクリプタ 1A
74
キーストリーム発生器 1B/2 (KSG MODE)
76
(48 & 52)
78
(62)
80
出力 42'
受信されたＣＲＣ (7)
(48)
(48)
出力 36'
出力 34'
１Ａ暗号文 (48)
出力 38'
１Ｂ暗号文 (48)
出力 40'
クラス２ビット暗号文(52)
5個のテールビット
１／２レート畳み込みデコーディング
84
(208)
出力 46'
２－スロットデインタリーバ
86
出力 48'
260

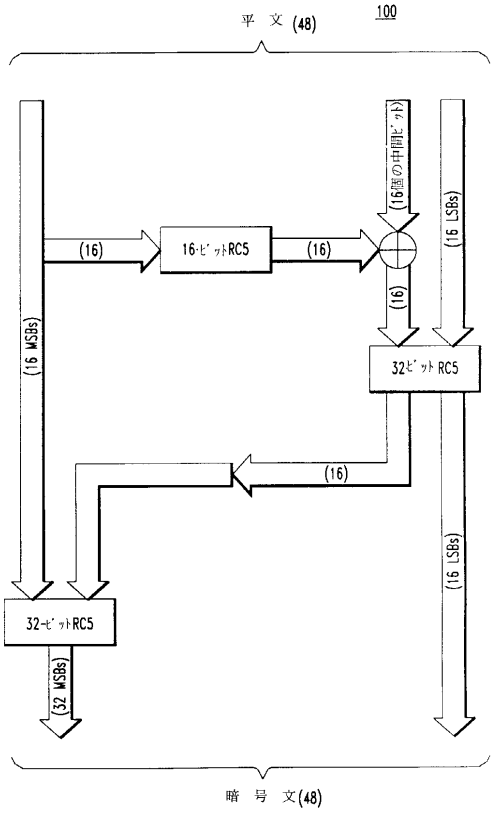
【図８】


80
平文(N)
(48)
EA
(N-48)
(48)
(N-48)
ブロックエンクリプタ
残りのメッセージ
(48)
KSG
(N-48)
(N-48)
暗号文(N)

【図９】


90
暗 号 文 (N)
(N/2 MSBs)
(N/2 LSBs)
(N/2)
KSG-ECMEA
PT&CS
CT
(N/2)
(N/2)
(N/2)
KSG-ECMEA
CT
PT&CS
(N/2)
(N/2)
(N/2 LSBs)
(N/2 MSBs)
平 文 (N)

【図１０】


100
平 文 (48)
(16)
16-ビットRC5
(16)
(16個の中間ビット)
(16 LSBs)
(16)
(16 MSBs)
32ビットRC5
(16)
(16 LSBs)
32-ビットRC5
(32 MSBs)
暗 号 文(48)

フロントページの続き

(74)代理人 100101498
弁理士 越智 隆夫
(74)代理人 100096688
弁理士 本宮 照久
(74)代理人 100104352
弁理士 朝日 伸光
(72)発明者 アダム エル. ベレンズウェイグ
アメリカ合衆国 １０００３ ニューヨーク，ニューヨーク，ナンバー１２－０，イースト ツエルヴス ストリート ７０
(72)発明者 スチーヴン アンソニー ファルコ
アメリカ合衆国 ０７９５０ ニュージャーシィ，モリス プレインズ，ピーチ ストリート ６
(72)発明者 セムヨン ビー. ミズコヴスキー
アメリカ合衆国 ０７７５１ ニュージャーシィ，モーガンヴィル，イエローナイフ ロード ２２７
(72)発明者 ウィンストン エドワード ペクラル
アメリカ合衆国 ０８８５４ ニュージャーシィ，ピスカッタウェイ，ルトガーズ ロード ８５－ビー
(72)発明者 ロバート ジョン ランス
アメリカ合衆国 ０１８１０ マサチューセッツ，アンドーヴァー，ウインターグリーン サークル ６
(72)発明者 ドナルド ジョセフ ユートカス
アメリカ合衆国 ０７９２０ ニュージャーシィ，バスキング リッジ，ジェームスタウン ロード ８２

審査官 中里 裕正

(56)参考文献 特開平０４－１７２０３０（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.[7]，ＤＢ名)
H04L 9/20