(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-325677
(P2004-325677A)
(43)公開日　平成16年11月18日(2004.11.18)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G09C 1/00	G09C	1/00　610A	5J104

審査請求 未請求　請求項の数 30　ＯＬ　（全 33 頁）

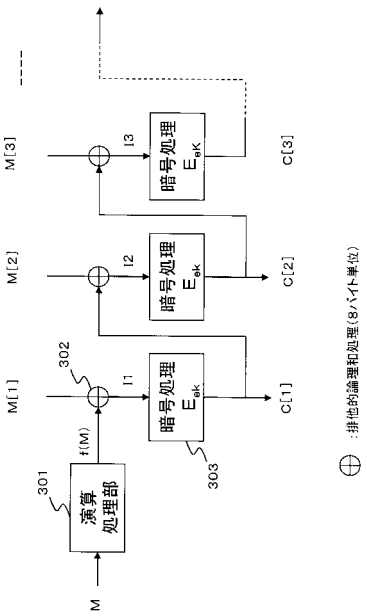
(21)出願番号　特願2003-118873(P2003-118873)
(22)出願日　平成15年4月23日(2003.4.23)

(71)出願人　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　100093241
弁理士　宮田　正昭
(74)代理人　100101801
弁理士　山田　英治
(74)代理人　100086531
弁理士　澤田　俊夫
(72)発明者　末松　俊成
東京都品川区北品川６丁目７番３５号　ソニー株式会社内

Ｆターム(参考)　5J104 JA05

(54)【発明の名称】暗号処理装置および暗号処理方法、並びにコンピュータ・プログラム

(57)【要約】
【課題】暗号処理における高度な解読困難性を実現する暗号処理装置および方法を実現する。
【解決手段】入力平文の全体または一部を演算処理部に入力し、演算処理を実行して、平文要約値をチェックサムやＭＡＣ、ＭＤＣ、ＣＲＣ等の算出により求め、この値を初期値、または中間データとして適用して、各ブロックとともに暗号処理を実行する構成とした。また、乱数、入力平文の要約値と、入力平文ブロックに対応するアドレス等の固有値に基づくハッシュ値を算出し、このハッシュ値を適用して、各ブロックとともに暗号処理を実行する構成とした。入力ブロックが同一アドレス、同一データを含む場合においても出力を異ならせることが可能となり、安全性を向上させた暗号処理が可能となる。
【選択図】　図５



【特許請求の範囲】
【請求項１】
ブロックデータ単位での暗号処理を実行する暗号処理装置であり、
入力平文に基づいて平文変換データを生成する演算手段と、
前記演算手段によって生成する平文変換データと、入力平文ブロックデータとを含むデータに基づいて出力暗号文を生成するデータ処理手段と、
を有することを特徴とする暗号処理装置。
【請求項２】
前記暗号処理装置は、ＣＢＣ（Ｃｉｐｈｅｒ　Ｂｌｏｃｋ　Ｃｈａｉｎｉｎｇ）モードでの暗号処理を実行する構成を有し、
前記データ処理手段は、
排他的論理和手段と、暗号鍵を適用した暗号処理を実行する暗号処理手段とを含み、
前記演算手段において生成した平文変換データと、平文ブロックデータとを前記排他的論理和手段に入力し、該排他的論理和手段の出力を前記暗号処理手段に入力して暗号処理を実行し、該暗号処理手段の出力を暗号文ブロックデータとして出力する構成であることを特徴とする請求項１に記載の暗号処理装置。
【請求項３】
前記暗号処理装置は、ＣＦＢ（Ｃｉｐｈｅｒ　Ｆｅｅｄｂａｃｋ）またはＯＦＢ（Ｏｕｔｐｕｔ　Ｆｅｅｄｂａｃｋ）モードでの暗号処理を実行する構成を有し、
前記データ処理手段は、
レジスタと、暗号鍵を適用した暗号処理を実行する暗号処理手段と、ビット選択部と、排他的論理和手段とを含み、
前記演算手段において生成した平文変換データを前記レジスタを介して前記暗号処理手段に入力して暗号処理を実行し、該暗号処理手段の出力を前記ビット選択部に入力し、該ビット選択部の出力と平文ブロックデータとを前記排他的論理和手段に入力し、該排他的論理和手段の出力を暗号文ブロックデータとして出力する構成であることを特徴とする請求項１に記載の暗号処理装置。
【請求項４】
前記暗号処理装置は、ＣＢＣ（Ｃｉｐｈｅｒ　Ｂｌｏｃｋ　Ｃｈａｉｎｉｎｇ）モード、ＣＦＢ（Ｃｉｐｈｅｒ　Ｆｅｅｄｂａｃｋ）、およびＯＦＢ（Ｏｕｔｐｕｔ　Ｆｅｅｄｂａｃｋ）モード、いずれかの暗号処理を実行する構成を有し、
前記演算手段によって生成する平文変換データを初期値として設定した構成を有することを特徴とする請求項１に記載の暗号処理装置。
【請求項５】
前記演算処理手段は、入力平文に対する一方向性関数を適用した演算を実行して平文変換データを生成する構成であることを特徴とする請求項１に記載の暗号処理装置。
【請求項６】
前記演算処理手段は、入力平文に対するチェックサム算出処理、ＭＡＣ（Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅ）算出処理、ＭＤＣ（Ｍｅｓｓａｇｅ　Ｄｉｇｅｓｔ　Ｃｏｄｅ）算出処理、ＣＲＣ（Ｃｙｃｌｉｃ　Ｒｅｄｕｎｄａｎｃｙ　Ｃｈｅｃｋ）算出処理の少なくともいずれかを実行する構成であることを特徴とする請求項１に記載の暗号処理装置。
【請求項７】
ブロックデータ単位での暗号処理を実行する暗号処理装置であり、
乱数生成処理を実行する乱数生成手段と、
前記乱数生成手段によって生成する乱数と、入力平文ブロックデータに対応する固有値とを含むデータについてのデータ変換を実行するデータ変換手段と、
前記データ変換手段の出力と、入力平文ブロックデータとから生成されるデータに対する暗号処理を実行し、出力暗号文ブロックデータを生成する暗号処理手段と、
を有することを特徴とする暗号処理装置。

【請求項８】
前記データ変換手段は、
前記乱数生成手段によって生成する乱数と、入力平文ブロックデータに対応する固有値との排他的論理和演算処理を実行する排他的論理和手段と、該排他的論理和手段の出力に対するハッシュ値を算出するハッシュ値生成手段とを有し、
前記暗号処理手段は、
前記ハッシュ値生成手段の出力と、入力平文ブロックデータとの排他的論理和を入力して出力暗号文ブロックデータを生成する構成であることを特徴とする請求項７に記載の暗号処理装置。
【請求項９】
前記入力平文ブロックデータに対応する固有値は、入力平文ブロックデータのメモリ格納アドレス、または入力平文ブロックデータ毎に異なる値として設定されたカウンタ値のいずれかであることを特徴とする請求項７に記載の暗号処理装置。
【請求項１０】
ブロックデータ単位での暗号処理を実行する暗号処理装置であり、
入力平文に基づいて平文変換データを生成する第１のデータ変換手段と、
前記第１のデータ変換手段によって生成する第１変換データと、入力平文ブロックデータに対応する固有値とを含むデータについての第２のデータ変換を実行する第２データ変換手段と、
前記第２データ変換手段の出力と、入力平文ブロックデータとから生成されるデータに対する暗号処理を実行し、出力暗号文ブロックデータを生成する暗号処理手段と、
を有することを特徴とする暗号処理装置。
【請求項１１】
前記第１データ変換手段は、入力平文に対するチェックサム算出処理、ＭＡＣ（Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅ）算出処理、ＭＤＣ（Ｍｅｓｓａｇｅ　Ｄｉｇｅｓｔ　Ｃｏｄｅ）算出処理、ＣＲＣ（Ｃｙｃｌｉｃ　Ｒｅｄｕｎｄａｎｃｙ　Ｃｈｅｃｋ）算出処理の少なくともいずれかを実行する構成であることを特徴とする請求項１０に記載の暗号処理装置。
【請求項１２】
前記第２データ変換手段は、
前記第１データ変換手段によって生成する第１変換データと、入力平文ブロックデータに対応する固有値との排他的論理和演算処理を実行する排他的論理和手段と、該排他的論理和手段の出力に対するハッシュ値を算出するハッシュ値生成手段とを有し、
前記暗号処理手段は、
前記ハッシュ値生成手段の出力と、入力平文ブロックデータとの排他的論理和を入力して出力暗号文ブロックデータを生成する構成であることを特徴とする請求項１０に記載の暗号処理装置。
【請求項１３】
前記第２データ変換手段は、
前記第１データ変換手段によって生成する第１変換データと、入力平文ブロックデータに対応する固有値との結合データ生成処理を実行する演算手段と、該演算手段の出力に対するハッシュ値を算出するハッシュ値生成手段とを有し、
前記暗号処理手段は、
前記ハッシュ値生成手段の出力と、入力平文ブロックデータとの排他的論理和を入力して出力暗号文ブロックデータを生成する構成であることを特徴とする請求項１０に記載の暗号処理装置。
【請求項１４】
前記入力平文ブロックデータに対応する固有値は、入力平文ブロックデータのメモリ格納アドレス、または入力平文ブロックデータ毎に異なる値として設定されたカウンタ値のいずれかであることを特徴とする請求項１０に記載の暗号処理装置。

【請求項１５】
ストリーム暗号処理を実行する暗号処理装置であり、
入力平文に基づいて平文変換データを生成する第１のデータ変換手段と、
前記第１のデータ変換手段によって生成する第１変換データと、入力平文ブロックデータに対応する固有値とを含むデータについての第２のデータ変換を実行する第２データ変換手段と、
前記第２データ変換手段の出力と、入力平文ブロックデータとの排他的論理和データを出力暗号文として出力する構成を有することを特徴とする暗号処理装置。
【請求項１６】
前記第１データ変換手段は、入力平文に対するチェックサム算出処理、ＭＡＣ（Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅ）算出処理、ＭＤＣ（Ｍｅｓｓａｇｅ　Ｄｉｇｅｓｔ　Ｃｏｄｅ）算出処理、ＣＲＣ（Ｃｙｃｌｉｃ　Ｒｅｄｕｎｄａｎｃｙ　Ｃｈｅｃｋ）算出処理の少なくともいずれかを実行する構成であることを特徴とする請求項１５に記載の暗号処理装置。
【請求項１７】
前記第２データ変換手段は、
前記第１データ変換手段によって生成する第１変換データと、入力平文ブロックデータに対応する固有値との排他的論理和または結合データ生成処理を実行する演算手段と、該演算手段の出力に対するハッシュ値を算出するハッシュ値生成手段とを有し、
前記ハッシュ値生成手段の出力と、入力平文ブロックデータとの排他的論理和データを出力暗号文として出力する構成を有することを特徴とする請求項１５に記載の暗号処理装置。
【請求項１８】
前記入力平文ブロックデータに対応する固有値は、入力平文ブロックデータのメモリ格納アドレス、または入力平文ブロックデータ毎に異なる値として設定されたカウンタ値のいずれかであることを特徴とする請求項１５に記載の暗号処理装置。
【請求項１９】
ブロックデータ単位での暗号処理を実行する暗号処理装置であり、
入力平文に基づいて平文変換データを生成する第１のデータ変換手段と、
前記第１のデータ変換手段によって生成する第１変換データと、入力平文ブロックデータに対応する固有値と、入力平文ブロックデータとを含むデータについての第２のデータ変換を実行する第２データ変換手段と、
前記第２データ変換手段の出力に対する暗号処理を実行し、出力暗号文ブロックデータを生成する暗号処理手段と、
を有することを特徴とする暗号処理装置。
【請求項２０】
前記第１データ変換手段は、入力平文に対するチェックサム算出処理、ＭＡＣ（Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅ）算出処理、ＭＤＣ（Ｍｅｓｓａｇｅ　Ｄｉｇｅｓｔ　Ｃｏｄｅ）算出処理、ＣＲＣ（Ｃｙｃｌｉｃ　Ｒｅｄｕｎｄａｎｃｙ　Ｃｈｅｃｋ）算出処理の少なくともいずれかを実行する構成であることを特徴とする請求項１９に記載の暗号処理装置。
【請求項２１】
ブロックデータ単位での暗号処理を実行する暗号処理方法であり、
入力平文に基づいて平文変換データを生成する演算ステップと、
前記演算ステップにおいて生成する平文変換データと、入力平文ブロックデータとを含むデータに基づいて出力暗号文を生成するデータ処理ステップと、
を有することを特徴とする暗号処理方法。
【請求項２２】
ブロックデータ単位での暗号処理を実行する暗号処理方法であり、
乱数生成処理を実行する乱数生成ステップと、

前記乱数生成ステップにおいて生成する乱数と、入力平文ブロックデータに対応する固有値とを含むデータについてのデータ変換を実行するデータ変換ステップと、
前記データ変換ステップにおける出力と、入力平文ブロックデータとから生成されるデータに対する暗号処理を実行し、出力暗号文ブロックデータを生成する暗号処理ステップと、
を有することを特徴とする暗号処理方法。
【請求項２３】
ブロックデータ単位での暗号処理を実行する暗号処理方法であり、
入力平文に基づいて平文変換データを生成する第１のデータ変換ステップと、
前記第１のデータ変換ステップにおいて生成する第１変換データと、入力平文ブロックデータに対応する固有値とを含むデータについての第２のデータ変換を実行する第２データ変換ステップと、
前記第２データ変換ステップにおける出力と、入力平文ブロックデータとから生成されるデータに対する暗号処理を実行し、出力暗号文ブロックデータを生成する暗号処理ステップと、
を有することを特徴とする暗号処理方法。
【請求項２４】
ストリーム暗号処理を実行する暗号処理方法であり、
入力平文に基づいて平文変換データを生成する第１のデータ変換ステップと、
前記第１のデータ変換ステップにおいて生成する第１変換データと、入力平文ブロックデータに対応する固有値とを含むデータについての第２のデータ変換を実行する第２データ変換ステップと、
前記第２データ変換ステップにおける出力と、入力平文ブロックデータとの排他的論理和データを出力暗号文として出力するステップと、
を有することを特徴とする暗号処理方法。
【請求項２５】
ブロックデータ単位での暗号処理を実行する暗号処理方法であり、
入力平文に基づいて平文変換データを生成する第１のデータ変換ステップと、
前記第１のデータ変換ステップにおいて生成する第１変換データと、入力平文ブロックデータに対応する固有値と、入力平文ブロックデータとを含むデータについての第２のデータ変換を実行する第２データ変換ステップと、
前記第２データ変換ステップにおける出力に対する暗号処理を実行し、出力暗号文ブロックデータを生成する暗号処理ステップと、
を有することを特徴とする暗号処理方法。
【請求項２６】
ブロックデータ単位での暗号処理を実行するコンピュータ・プログラムであり、
入力平文に基づいて平文変換データを生成する演算ステップと、
前記演算ステップにおいて生成する平文変換データと、入力平文ブロックデータとを含むデータに基づいて出力暗号文を生成するデータ処理ステップと、
を有することを特徴とするコンピュータ・プログラム。
【請求項２７】
ブロックデータ単位での暗号処理を実行するコンピュータ・プログラムであり、
乱数生成処理を実行する乱数生成ステップと、
前記乱数生成ステップにおいて生成する乱数と、入力平文ブロックデータに対応する固有値とを含むデータについてのデータ変換を実行するデータ変換ステップと、
前記データ変換ステップにおける出力と、入力平文ブロックデータとから生成されるデータに対する暗号処理を実行し、出力暗号文ブロックデータを生成する暗号処理ステップと、
を有することを特徴とするコンピュータ・プログラム。
【請求項２８】

ブロックデータ単位での暗号処理を実行するコンピュータ・プログラムであり、
入力平文に基づいて平文変換データを生成する第１のデータ変換ステップと、
前記第１のデータ変換ステップにおいて生成する第１変換データと、入力平文ブロックデータに対応する固有値とを含むデータについての第２のデータ変換を実行する第２データ変換ステップと、
前記第２データ変換ステップにおける出力と、入力平文ブロックデータとから生成されるデータに対する暗号処理を実行し、出力暗号文ブロックデータを生成する暗号処理ステップと、
を有することを特徴とするコンピュータ・プログラム。
【請求項２９】
ストリーム暗号処理を実行するコンピュータ・プログラムであり、
入力平文に基づいて平文変換データを生成する第１のデータ変換ステップと、
前記第１のデータ変換ステップにおいて生成する第１変換データと、入力平文ブロックデータに対応する固有値とを含むデータについての第２のデータ変換を実行する第２データ変換ステップと、
前記第２データ変換ステップにおける出力と、入力平文ブロックデータとの排他的論理和データを出力暗号文として出力するステップと、
を有することを特徴とするコンピュータ・プログラム。
【請求項３０】
ブロックデータ単位での暗号処理を実行するコンピュータ・プログラムであり、
入力平文に基づいて平文変換データを生成する第１のデータ変換ステップと、
前記第１のデータ変換ステップにおいて生成する第１変換データと、入力平文ブロックデータに対応する固有値と、入力平文ブロックデータとを含むデータについての第２のデータ変換を実行する第２データ変換ステップと、
前記第２データ変換ステップにおける出力に対する暗号処理を実行し、出力暗号文ブロックデータを生成する暗号処理ステップと、
を有することを特徴とするコンピュータ・プログラム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、暗号処理装置および暗号処理方法、並びにコンピュータ・プログラムに関する。特に、データストリームを固定長データブロック単位の複数ブロックに分割し、それぞれのブロック単位での暗号化／復号処理を行なう暗号処理装置および暗号処理方法、並びにコンピュータ・プログラムに関する。
【０００２】
【従来の技術】
近年のインターネット等、通信網の発達に伴い、暗号通信分野における研究も盛んに行われている。暗号処理アルゴリズムには様々なものがあるが、大きく分類すると、暗号化鍵と復号化鍵を異なる鍵、例えば公開鍵と秘密鍵として設定する公開鍵暗号方式と、暗号化鍵と復号化鍵を共通の鍵として設定する共通鍵暗号方式とに分類される。
【０００３】
共通鍵ブロック暗号のアルゴリズムとしては、例えばＤＥＳ（Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）がよく知られている。ブロック暗号の最も簡単な処理例について、図１を参照して説明する。図１に示す処理は、ＥＣＢ（Ｅｌｅｃｔｒｏｎｉｃ　Ｃｏｄｅ　Ｂｏｏｋ）モードと呼ばれるものである。
【０００４】
以下の説明において、ブロック暗号のブロックサイズをｎビット、平文のブロック数をｍブロックと表すことにする。このとき平文：Ｍの全長はｎ×ｍビットとなる。図１中、Ｍ［ｉ］１０１がｍ個のブロックに分割されたｉ番目のブロックの平文である。ｉ（１≦ｉ≦ｍ）はブロックにつけられた番号を示す。Ｍ［１］，Ｍ［２］，…，Ｍ［ｍ］が各ブロ

ックの平文を示す。
【０００５】
平文ブロックの暗号化後のデータがＣ［ｉ］１０２である。Ｍ［１］，Ｍ［２］，…，Ｍ［ｍ］の各平文ブロックに対する暗号文のブロックが、Ｃ［１］，Ｃ［２］，…，Ｃ［ｍ］として示される。
【０００６】
図１中、平文ブロック：Ｍ［１］，Ｍ［２］，…，Ｍ［ｍ］は、暗号処理部１００において暗号処理がなされ、暗号文ブロック：Ｃ［１］，Ｃ［２］，…，Ｃ［ｍ］を出力する。暗号処理部１００におけるE_{eK}は、暗号鍵ｅＫを適用したブロック暗号処理：Ｅ（）を実行することを示す。
【０００７】
このような暗号処理構成、すなわちＥＣＢモードでブロック暗号を使用したとき、例えば平文の分割ブロックＭ［１］，…，Ｍ［ｍ］が全て同じ値だったような場合、暗号化した後の暗号文ブロックＣ［１］，…，Ｃ［ｍ］も全て同じ値になる。すなわち同じ入力平文を与えた場合、出力が同じとなってしまう。このような場合、共通鍵ブロック暗号に対する代表的な攻撃法である差分攻撃および線形攻撃などにより、暗号処理部１００における暗号処理アルゴリズムが露呈してしまう可能性が高い、すなわち、平文の統計的性質などの特徴が暗号文にも残ってしまい、攻撃に対して弱いものとなる。
【０００８】
これを改善するための手段として、ＣＢＣ（Ｃｉｐｈｅｒ Ｂｌｏｃｋ Ｃｈａｉｎｉｎｇ）、ＣＦＢ（Ｃｉｐｈｅｒ Ｆｅｅｄｂａｃｋ）、ＯＦＢ（Ｏｕｔｐｕｔ Ｆｅｅｄｂａｃｋ）などの暗号利用モードが知られている。これらの技法は、各ブロックの暗号文を入力側にフィードバックすることで、ブロック暗号のストリーム化を図り、解読作業をより困難にするものである。
【０００９】
ＤＥＳ－ＣＢＣモードの暗号処理手法の概略について図２を用いて説明する。まず、暗号処理を施すデータ（メッセージ）をｘバイト（例えば８バイト）単位に分割しブロックデータとする。（以下、分割されたブロックデータをＭ［１］、Ｍ［２］、・・・、Ｍ［ｍ］とする）。そして、初期値（Ｉｎｉｔｉａｌ Ｖａｌｕｅ（以下、ＩＶとする））とＭ［１］を排他的論理和部１５１において排他的論理和する（その結果をＩ１とする）。次に、Ｉ１をＤＥＳ暗号処理部１５２に入れ、所定の鍵（ｅＫ）を用いて暗号化し出力をＣ［１］を得る。続けて、Ｃ［１］およびＭ［２］を排他的論理和し、その出力Ｉ２をＤＥＳ暗号処理部へ入れ、鍵ｅＫを用いて暗号化する（出力Ｃ［２］）。以下、これを繰り返し、全てのメッセージに対して暗号化処理を施す。このように暗号文を連鎖させる方式のことをＣＢＣ（Ｃｉｐｈｅｒ Ｂｌｏｃｋ Ｃｈａｉｎｉｎｇ）モードと呼ぶ。
【００１０】
ＣＦＢ（Ｃｉｐｈｅｒ Ｆｅｅｄｂａｃｋ）、ＯＦＢ（Ｏｕｔｐｕｔ Ｆｅｅｄｂａｃｋ）の暗号処理構成を図３に示す。（ａ）ＣＦＢ（Ｃｉｐｈｅｒ Ｆｅｅｄｂａｃｋ）モードは、レジスタ２１１、暗号処理部２１２、ビット選択部２１３、排他的論理和部２１４を有し、入力平文ブロックＭ［ｉ］と、先行するブロックの暗号処理結果の特定の選択ビットとの排他的論理和を行い出力暗号ブロックＣ［ｉ］を生成するとともに、レジスタ２１１にフィードバック格納し、暗号処理部２１２において暗号処理を実行し、ビット選択部２１３において選択されたビットを後続平文ブロックと排他的論理和する処理を繰り返し実行し、暗号文ブロック：Ｃ［１］，Ｃ［２］，…，Ｃ［ｍ］を出力する方式である。
【００１１】
（ｂ）ＯＦＢ（Ｏｕｔｐｕｔ Ｆｅｅｄｂａｃｋ）モードは、レジスタ２２１、暗号処理部２２２、ビット選択部２２３、排他的論理和部２２４を有し、入力平文ブロックＭ［ｉ］に、ランダム系列を加えた結果を暗号文とするものであり、レジスタ２２１、暗号処理部２２２、ビット選択部２２３の循環により、各入力平文ブロックＭ［ｉ］に加える、すなわち排他的論理和部２２４で演算するランダム系列を変更して暗号文ブロック：Ｃ［１

］，Ｃ［２］，…，Ｃ［ｍ］を出力する方式である。

【００１２】

しかし、これらの暗号利用モードを持ってしても選択平文攻撃や選択暗号文攻撃に対する安全性は十分とは言えず、より安全性の高い方式が望まれている。

【００１３】

安全性の高い暗号処理構成についての研究は盛んに行われており、例えば非特許文献１には、暗号化の前にデータのアドレスから求めた値をハッシュした値を加える方式が示されている。また、特許文献１には、冗長データとメッセージからなる平文をブロック化し、秘密鍵から乱数を生成し、乱数ブロックと平文ブロックとの演算結果を順次フィードバックして暗号処理を実行する構成が記載されている。さらに、特許文献２には、乱数、秘密情報を適用して生成した暗号鍵を用いて平文ブロックに対する暗号化処理を実行する構成が記載されている。

【００１４】

暗号の安全性を評価するときの基準として、擬似ランダム置換（ＰＲＰ：Ｐｓｅｕｄｏｒａｎｄｏｍ　Ｐｅｒｍｕｔａｔｉｏｎ）との区別が可能か否かによって判断する方法が知られている。この手法を用いて、図２に示すＤＥＳ－ＣＢＣモードの暗号処理における初期値：ＩＶが固定の場合の安全性について検討する。初期値：ＩＶ固定のＣＢＣに対しては、次の選択平文攻撃によってＰＲＰではないことが判別可能であり、安全性に問題がある。

【００１５】

［選択平文攻撃１］

ＣＢＣまたはＰＲＰのいずれかの処理を実行する処理部としてのオラクルｇが存在するとする。

ブロックＡとブロックＢからなる２ブロッククエリー

ブロックＡとブロックＣからなる２ブロッククエリー

の２つのクエリーＡＢ，ＡＣをオラクルｇに入力し、得られた出力ブロックをＷＸ，ＹＺとする。

【００１６】

このとき出力の先行ブロックが等しい、すなわちＷ＝Ｙであれば１、そうでなければ０を返すとする。初期値ＩＶ固定のＣＢＣの場合は、先頭ブロックが両者ともＡであり、図２の構成から明らかなように、同一の初期値ＩＶを排他的論理和し、その結果に対して同一の暗号処理を施すことになるので、その結果としての出力ブロックＷ、Ｙは同一の値となる。従って、常に１を返す。一方擬似ランダム置換（ＰＲＰ：Ｐｓｅｕｄｏｒａｎｄｏｍ　Ｐｅｒｍｕｔａｔｉｏｎ）の場合、１を返す確率はほぼ０に近いと考えられるため、ＰＲＰでは無いことが容易に判断できてしまう。

【００１７】

また、ＣＢＣに対しては非特許文献２には、別の選択平文攻撃方法と選択暗号文攻撃の例が示されており、安全性の不十分な点が指摘されている。また、非特許文献１に示されている暗号処理マイクロプロセッサとしてのＣＭＰ（Ｃｒｙｐｔｏ　Ｍｉｃｒｏｐｒｏｃｅｓｓｏｒ）の中で使用されている暗号処理手段は、図４に示す構成を持つ。これをＥＣＭＰと呼ぶことにする。

【００１８】

ＥＣＭＰは、図４に示すように、暗号化する平文のデータＭ［ｉ］のアドレスＡｄｒ［ｉ］（カウンタ値ｉでも良い）のハッシュ値をハッシュ値生成部２５１において生成し、排他論理和部２５２において、入力平文ブロックＭ［ｉ］に加えてから暗号処理部２５３において暗号化して暗号文ブロックＣ［ｉ］を出力する。

【００１９】

この構成とすることで、同じ入力値を持つブロックデータであっても、そのデータ格納場所であるアドレスが違えば暗号結果としての出力を異ならせることが可能であり、前述のＥＣＢに比べると安全性は向上している。しかし、この方式に対しても、先に説明した選

択平文攻撃１によってＰＲＰと違うことが簡単に判別できてしまう。また、ＥＣＭＰに対しては、さらに次の攻撃も有効である。

【００２０】

［選択平文攻撃１Ｂ］

２ブロックのクエリーＡＣ，ＢＣをオラクルｇに入力し、得られた出力をＷＸ，ＹＺとする。このときＸ＝Ｚであれば１、そうでなければ０を返す。先に説明した［選択平文攻撃１］との違いは、入力平文ブロックの後ろのブロックデータが一致している点である。ここで、クエリーＡＣのＡとＣは、それぞれ入力平文ブロックＭ［１］とＭ［２］に対応し、ＡのアドレスはＡｄｒ［１］、ＣのアドレスはＡｄｒ［２］となる。また、クエリーＢＣのＢとＣは、それぞれ入力平文ブロックＭ［１］とＭ［２］に対応し、ＢのアドレスはＡｄｒ［１］、ＣのアドレスはＡｄｒ［２］となる。ＥＣＭＰにおける出力ＷＸ，ＹＺにおいて、ＸとＺを計算するための入力Ｍ［２］とＡｄｒ［２］が共に等しいためＸ＝Ｚとなるので、常に１を返す。一方ＰＲＰの場合１を返す確率はほぼ０に近いと考えられるため、ＰＲＰでは無いことが容易に判断できてしまう。

【００２１】

なお、ＣＢＣはこの攻撃に対し常に０を返すが、ＰＲＰが０を返す確率が非常に低いため、この違いを判別するのは困難であり、この攻撃に対しては安全と考えられる。さらに、ＥＣＭＰにおいてはＡｄｒ［ｉ］を入力するハッシュ関数Ｈの鍵は固定で、その処理内容は誰でも知ることができる。このため、次の攻撃も可能である。

【００２２】

［選択平文攻撃２］

次のクエリーＭを用意する。

Ｍ［１］＝Ｈ（Ａｄｒ［１］）

Ｍ［２］＝Ｈ（Ａｄｒ［２］）

Ｍ：Ｍ［１］．．．Ｍ［ｍ］

ただし、Ｍ［３］以降の値は任意

【００２３】

Ｈ（Ａｄｒ［ｉ］）は、図４におけるハッシュ値生成部２５１の出力に相当する。図４の構成を持つＥＣＭＰまたは擬似ランダム置換（ＰＲＰ）からなるオラクルｇに対して上記した平文ブロック系列Ｍを入力して出力ブロック系列Ｃ［１］，Ｃ［２］を得た後、これらを比較する。Ｃ［１］＝Ｃ［２］ならば１を返し、そうでなければ０を返す。

【００２４】

この攻撃に対しＥＣＭＰは下記のようにＣ［１］＝Ｃ［２］＝Ｅ（ｅＫ，0^n）となり、必ず一致する。なお、0^nは、ビット０がｎ個連続していることを示している。

【００２５】

【数１】

$$C[1] = E(eK, H(Adr[1]) \oplus M[1]) = E(eK, 0^n)$$

$$C[2] = E(eK, H(Adr[2]) \oplus M[2]) = E(eK, 0^n)$$

【００２６】

一方ＰＲＰの場合１を返す確率はほぼ０に近いと考えられるため、ＥＣＭＰとＰＲＰとの違いが容易に判断できてしまう。

【００２７】

ＥＣＭＰが、上述の［選択暗号文攻撃２］に対して弱いのは、ハッシュ値（Ｈ）生成部に

おいて適用するハッシュ生成鍵が固定なため、それを利用して攻撃されるためである。ハッシュ生成鍵を暗号化鍵と共に毎回選択できるようにすれば、［平文選択攻撃２］は防ぐことができる。ただし、この場合も［選択平文攻撃１／１Ｂ］に対しては効果が無い。

【００２８】

以上に示したようにＣＢＣ，ＥＣＭＰともに多くの攻撃方法が存在し、安全性の面で不安があると言わざるを得ない。詳細は割愛するが、ＣＦＢ，ＯＦＢなどの暗号利用モードについても同様のことが言える。

【００２９】

【特許文献１】

特許公開２００２－３０５５１７号公報

【特許文献２】

特開平１０－３１３３０６号公報

【非特許文献１】

末松俊成，今井秀樹：”ＣＭＰ（Ｃｒｙｐｔｏ Ｍｉｃｒｏｐｒｏｃｅｓｓｏｒ） の一構成方法とその応用例”，ＩＳＥＣ９８－８（１９９８－０５）

【非特許文献２】

Ｍ．Ｂａｌｌａｒｅ，Ａ．Ｂｏｌｄｙｒｅｖａ，Ｌ．Ｋｎｕｄｓｅｎ，Ｃ．Ｎａｍｐｒｅｍｐｒｅ：”Ｏｎｌｉｎｅ Ｃｉｐｈｅｒｓ ａｎｄ ｔｈｅ Ｈａｓｈ－ＣＢＣ Ｃｏｎｓｔｒｕｃｔｉｏｎ”，ＣＲＹＰＴＯ ２００１，ＬＮＣＳ２１３９，ｐｐ．２９２－３０９（２００１）．

【００３０】

【発明が解決しようとする課題】

上述したように暗号化に際し例えばＣＢＣモード等の連鎖技法を用いることは、ブロック暗号の安全性を高める１つの有効な方法ではあるが、入力されたブロックに対する暗号文を次の入力ブロックにフィードバックするという固定的な連鎖関係による暗号化手法は高い解読困難性を持つとは言い難い。

【００３１】

本発明は、上述の問題点に鑑みてなされたものであり、データブロック単位での暗号化／復号処理を行なう暗号処理において、解読困難なブロック暗号化手法を実現する暗号処理装置および暗号処理方法、並びにコンピュータ・プログラムを提供するものである。

【００３２】

【課題を解決するための手段】

本発明の第１の側面は、

ブロックデータ単位での暗号処理を実行する暗号処理装置であり、

入力平文に基づいて平文変換データを生成する演算手段と、

前記演算手段によって生成する平文変換データと、入力平文ブロックデータとを含むデータに基づいて出力暗号文を生成するデータ処理手段と、

を有することを特徴とする暗号処理装置にある。

【００３３】

さらに、本発明の暗号処理装置の一実施態様において、前記暗号処理装置は、ＣＢＣ（Ｃｉｐｈｅｒ Ｂｌｏｃｋ Ｃｈａｉｎｉｎｇ）モードでの暗号処理を実行する構成を有し、前記データ処理手段は、排他的論理和手段と、暗号鍵を適用した暗号処理を実行する暗号処理手段とを含み、前記演算手段において生成した平文変換データと、平文ブロックデータとを前記排他的論理和手段に入力し、該排他的論理和手段の出力を前記暗号処理手段に入力して暗号処理を実行し、該暗号処理手段の出力を暗号文ブロックデータとして出力する構成であることを特徴とする。

【００３４】

さらに、本発明の暗号処理装置の一実施態様において、前記暗号処理装置は、ＣＦＢ（Ｃｉｐｈｅｒ Ｆｅｅｄｂａｃｋ）またはＯＦＢ（Ｏｕｔｐｕｔ Ｆｅｅｄｂａｃｋ）モードでの暗号処理を実行する構成を有し、前記データ処理手段は、レジスタと、暗号鍵を適

用した暗号処理を実行する暗号処理手段と、ビット選択部と、排他的論理和手段とを含み、前記演算手段において生成した平文変換データを前記レジスタを介して前記暗号処理手段に入力して暗号処理を実行し、該暗号処理手段の出力を前記ビット選択部に入力し、該ビット選択部の出力と平文ブロックデータとを前記排他的論理和手段に入力し、該排他的論理和手段の出力を暗号文ブロックデータとして出力する構成であることを特徴とする。

【００３５】

さらに、本発明の暗号処理装置の一実施態様において、前記暗号処理装置は、ＣＢＣ（Ｃｉｐｈｅｒ Ｂｌｏｃｋ Ｃｈａｉｎｉｎｇ）モード、ＣＦＢ（Ｃｉｐｈｅｒ Ｆｅｅｄｂａｃｋ）、およびＯＦＢ（Ｏｕｔｐｕｔ Ｆｅｅｄｂａｃｋ）モード、いずれかの暗号処理を実行する構成を有し、前記演算手段によって生成する平文変換データを初期値として設定した構成を有することを特徴とする。

【００３６】

さらに、本発明の暗号処理装置の一実施態様において、前記演算処理手段は、入力平文に対する一方向性関数を適用した演算を実行して平文変換データを生成する構成であることを特徴とする。

【００３７】

さらに、本発明の暗号処理装置の一実施態様において、前記演算処理手段は、入力平文に対するチェックサム算出処理、ＭＡＣ（Ｍｅｓｓａｇｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｃｏｄｅ）算出処理、ＭＤＣ（Ｍｅｓｓａｇｅ Ｄｉｇｅｓｔ Ｃｏｄｅ）算出処理、ＣＲＣ（Ｃｙｃｌｉｃ Ｒｅｄｕｎｄａｎｃｙ Ｃｈｅｃｋ）算出処理の少なくともいずれかを実行する構成であることを特徴とする。

【００３８】

さらに、本発明の第２の側面は、

ブロックデータ単位での暗号処理を実行する暗号処理装置であり、

乱数生成処理を実行する乱数生成手段と、

前記乱数生成手段によって生成する乱数と、入力平文ブロックデータに対応する固有値とを含むデータについてのデータ変換を実行するデータ変換手段と、

前記データ変換手段の出力と、入力平文ブロックデータとから生成されるデータに対する暗号処理を実行し、出力暗号文ブロックデータを生成する暗号処理手段と、

を有することを特徴とする暗号処理装置にある。

【００３９】

さらに、本発明の暗号処理装置の一実施態様において、前記データ変換手段は、前記乱数生成手段によって生成する乱数と、入力平文ブロックデータに対応する固有値との排他的論理和演算処理を実行する排他的論理和手段と、該排他的論理和手段の出力に対するハッシュ値を算出するハッシュ値生成手段とを有し、前記暗号処理手段は、前記ハッシュ値生成手段の出力と、入力平文ブロックデータとの排他的論理和を入力して出力暗号文ブロックデータを生成する構成であることを特徴とする。

【００４０】

さらに、本発明の暗号処理装置の一実施態様において、前記入力平文ブロックデータに対応する固有値は、入力平文ブロックデータのメモリ格納アドレス、または入力平文ブロックデータ毎に異なる値として設定されたカウンタ値のいずれかであることを特徴とする。

【００４１】

さらに、本発明の第３の側面は、

ブロックデータ単位での暗号処理を実行する暗号処理装置であり、

入力平文に基づいて平文変換データを生成する第１のデータ変換手段と、

前記第１のデータ変換手段によって生成する第１変換データと、入力平文ブロックデータに対応する固有値とを含むデータについての第２のデータ変換を実行する第２データ変換手段と、

前記第２データ変換手段の出力と、入力平文ブロックデータとから生成されるデータに対する暗号処理を実行し、出力暗号文ブロックデータを生成する暗号処理手段と、

を有することを特徴とする暗号処理装置にある。

【００４２】

さらに、本発明の暗号処理装置の一実施態様において、前記第１データ変換手段は、入力平文に対するチェックサム算出処理、ＭＡＣ（Ｍｅｓｓａｇｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｃｏｄｅ）算出処理、ＭＤＣ（Ｍｅｓｓａｇｅ Ｄｉｇｅｓｔ Ｃｏｄｅ）算出処理、ＣＲＣ（Ｃｙｃｌｉｃ Ｒｅｄｕｎｄａｎｃｙ Ｃｈｅｃｋ）算出処理の少なくともいずれかを実行する構成であることを特徴とする。

【００４３】

さらに、本発明の暗号処理装置の一実施態様において、前記第２データ変換手段は、前記第１データ変換手段によって生成する第１変換データと、入力平文ブロックデータに対応する固有値との排他的論理和演算処理を実行する排他的論理和手段と、該排他的論理和手段の出力に対するハッシュ値を算出するハッシュ値生成手段とを有し、前記暗号処理手段は、前記ハッシュ値生成手段の出力と、入力平文ブロックデータとの排他的論理和を入力して出力暗号文ブロックデータを生成する構成であることを特徴とする。

【００４４】

さらに、本発明の暗号処理装置の一実施態様において、前記第２データ変換手段は、前記第１データ変換手段によって生成する第１変換データと、入力平文ブロックデータに対応する固有値との結合データ生成処理を実行する演算手段と、該演算手段の出力に対するハッシュ値を算出するハッシュ値生成手段とを有し、前記暗号処理手段は、前記ハッシュ値生成手段の出力と、入力平文ブロックデータとの排他的論理和を入力して出力暗号文ブロックデータを生成する構成であることを特徴とする。

【００４５】

さらに、本発明の暗号処理装置の一実施態様において、前記入力平文ブロックデータに対応する固有値は、入力平文ブロックデータのメモリ格納アドレス、または入力平文ブロックデータ毎に異なる値として設定されたカウンタ値のいずれかであることを特徴とする。

【００４６】

さらに、本発明の第４の側面は、

ストリーム暗号処理を実行する暗号処理装置であり、

入力平文に基づいて平文変換データを生成する第１のデータ変換手段と、

前記第１のデータ変換手段によって生成する第１変換データと、入力平文ブロックデータに対応する固有値とを含むデータについての第２のデータ変換を実行する第２データ変換手段と、

前記第２データ変換手段の出力と、入力平文ブロックデータとの排他的論理和データを出力暗号文として出力する構成を有することを特徴とする暗号処理装置にある。

【００４７】

さらに、本発明の暗号処理装置の一実施態様において、前記第１データ変換手段は、入力平文に対するチェックサム算出処理、ＭＡＣ（Ｍｅｓｓａｇｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｃｏｄｅ）算出処理、ＭＤＣ（Ｍｅｓｓａｇｅ Ｄｉｇｅｓｔ Ｃｏｄｅ）算出処理、ＣＲＣ（Ｃｙｃｌｉｃ Ｒｅｄｕｎｄａｎｃｙ Ｃｈｅｃｋ）算出処理の少なくともいずれかを実行する構成であることを特徴とする。

【００４８】

さらに、本発明の暗号処理装置の一実施態様において、前記第２データ変換手段は、前記第１データ変換手段によって生成する第１変換データと、入力平文ブロックデータに対応する固有値との排他的論理和または結合データ生成処理を実行する演算手段と、該演算手段の出力に対するハッシュ値を算出するハッシュ値生成手段とを有し、前記ハッシュ値生成手段の出力と、入力平文ブロックデータとの排他的論理和データを出力暗号文として出力する構成を有することを特徴とする。

【００４９】

さらに、本発明の暗号処理装置の一実施態様において、前記入力平文ブロックデータに対応する固有値は、入力平文ブロックデータのメモリ格納アドレス、または入力平文ブロッ

クデータ毎に異なる値として設定されたカウンタ値のいずれかであることを特徴とする。

【００５０】

さらに、本発明の第５の側面は、

ブロックデータ単位での暗号処理を実行する暗号処理装置であり、

入力平文に基づいて平文変換データを生成する第１のデータ変換手段と、

前記第１のデータ変換手段によって生成する第１変換データと、入力平文ブロックデータに対応する固有値と、入力平文ブロックデータとを含むデータについての第２のデータ変換を実行する第２データ変換手段と、

前記第２データ変換手段の出力に対する暗号処理を実行し、出力暗号文ブロックデータを生成する暗号処理手段と、

を有することを特徴とする暗号処理装置にある。

【００５１】

さらに、本発明の暗号処理装置の一実施態様において、前記第１データ変換手段は、入力平文に対するチェックサム算出処理、ＭＡＣ（Ｍｅｓｓａｇｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｃｏｄｅ）算出処理、ＭＤＣ（Ｍｅｓｓａｇｅ Ｄｉｇｅｓｔ Ｃｏｄｅ）算出処理、ＣＲＣ（Ｃｙｃｌｉｃ Ｒｅｄｕｎｄａｎｃｙ Ｃｈｅｃｋ）算出処理の少なくともいずれかを実行する構成であることを特徴とする。

【００５２】

さらに、本発明の第６の側面は、

ブロックデータ単位での暗号処理を実行する暗号処理方法であり、

入力平文に基づいて平文変換データを生成する演算ステップと、

前記演算ステップにおいて生成する平文変換データと、入力平文ブロックデータとを含むデータに基づいて出力暗号文を生成するデータ処理ステップと、

を有することを特徴とする暗号処理方法にある。

【００５３】

さらに、本発明の第７の側面は、

ブロックデータ単位での暗号処理を実行する暗号処理方法であり、

乱数生成処理を実行する乱数生成ステップと、

前記乱数生成ステップにおいて生成する乱数と、入力平文ブロックデータに対応する固有値とを含むデータについてのデータ変換を実行するデータ変換ステップと、

前記データ変換ステップにおける出力と、入力平文ブロックデータとから生成されるデータに対する暗号処理を実行し、出力暗号文ブロックデータを生成する暗号処理ステップと、

を有することを特徴とする暗号処理方法にある。

【００５４】

さらに、本発明の第８の側面は、

ブロックデータ単位での暗号処理を実行する暗号処理方法であり、

入力平文に基づいて平文変換データを生成する第１のデータ変換ステップと、

前記第１のデータ変換ステップにおいて生成する第１変換データと、入力平文ブロックデータに対応する固有値とを含むデータについての第２のデータ変換を実行する第２データ変換ステップと、

前記第２データ変換ステップにおける出力と、入力平文ブロックデータとから生成されるデータに対する暗号処理を実行し、出力暗号文ブロックデータを生成する暗号処理ステップと、

を有することを特徴とする暗号処理方法にある。

【００５５】

さらに、本発明の第９の側面は、

ストリーム暗号処理を実行する暗号処理方法であり、

入力平文に基づいて平文変換データを生成する第１のデータ変換ステップと、

前記第１のデータ変換ステップにおいて生成する第１変換データと、入力平文ブロックデ

ータに対応する固有値とを含むデータについての第２のデータ変換を実行する第２データ変換ステップと、
前記第２データ変換ステップにおける出力と、入力平文ブロックデータとの排他的論理和データを出力暗号文として出力するステップと、
を有することを特徴とする暗号処理方法にある。
【００５６】
さらに、本発明の第１０の側面は、
ブロックデータ単位での暗号処理を実行する暗号処理方法であり、
入力平文に基づいて平文変換データを生成する第１のデータ変換ステップと、
前記第１のデータ変換ステップにおいて生成する第１変換データと、入力平文ブロックデータに対応する固有値と、入力平文ブロックデータとを含むデータについての第２のデータ変換を実行する第２データ変換ステップと、
前記第２データ変換ステップにおける出力に対する暗号処理を実行し、出力暗号文ブロックデータを生成する暗号処理ステップと、
を有することを特徴とする暗号処理方法にある。
【００５７】
さらに、本発明の第１１の側面は、
ブロックデータ単位での暗号処理を実行するコンピュータ・プログラムであり、
入力平文に基づいて平文変換データを生成する演算ステップと、
前記演算ステップにおいて生成する平文変換データと、入力平文ブロックデータとを含むデータに基づいて出力暗号文を生成するデータ処理ステップと、
を有することを特徴とするコンピュータ・プログラムにある。
【００５８】
さらに、本発明の第１２の側面は、
ブロックデータ単位での暗号処理を実行するコンピュータ・プログラムであり、
乱数生成処理を実行する乱数生成ステップと、
前記乱数生成ステップにおいて生成する乱数と、入力平文ブロックデータに対応する固有値とを含むデータについてのデータ変換を実行するデータ変換ステップと、
前記データ変換ステップにおける出力と、入力平文ブロックデータとから生成されるデータに対する暗号処理を実行し、出力暗号文ブロックデータを生成する暗号処理ステップと、
を有することを特徴とするコンピュータ・プログラムにある。
【００５９】
さらに、本発明の第１３の側面は、
ブロックデータ単位での暗号処理を実行するコンピュータ・プログラムであり、
入力平文に基づいて平文変換データを生成する第１のデータ変換ステップと、
前記第１のデータ変換ステップにおいて生成する第１変換データと、入力平文ブロックデータに対応する固有値とを含むデータについての第２のデータ変換を実行する第２データ変換ステップと、
前記第２データ変換ステップにおける出力と、入力平文ブロックデータとから生成されるデータに対する暗号処理を実行し、出力暗号文ブロックデータを生成する暗号処理ステップと、
を有することを特徴とするコンピュータ・プログラムにある。
【００６０】
さらに、本発明の第１４の側面は、
ストリーム暗号処理を実行するコンピュータ・プログラムであり、
入力平文に基づいて平文変換データを生成する第１のデータ変換ステップと、
前記第１のデータ変換ステップにおいて生成する第１変換データと、入力平文ブロックデータに対応する固有値とを含むデータについての第２のデータ変換を実行する第２データ変換ステップと、

前記第２データ変換ステップにおける出力と、入力平文ブロックデータとの排他的論理和データを出力暗号文として出力するステップと、
を有することを特徴とするコンピュータ・プログラムにある。
【００６１】
さらに、本発明の第１５の側面は、
ブロックデータ単位での暗号処理を実行するコンピュータ・プログラムであり、
入力平文に基づいて平文変換データを生成する第１のデータ変換ステップと、
前記第１のデータ変換ステップにおいて生成する第１変換データと、入力平文ブロックデータに対応する固有値と、入力平文ブロックデータとを含むデータについての第２のデータ変換を実行する第２データ変換ステップと、
前記第２データ変換ステップにおける出力に対する暗号処理を実行し、出力暗号文ブロックデータを生成する暗号処理ステップと、
を有することを特徴とするコンピュータ・プログラムにある。
【００６２】
【作用】
本発明の構成に従えば、入力平文の全体または一部を演算処理部に入力し、演算処理を実行して、平文要約値をチェックサムやＭＡＣ、ＭＤＣ、ＣＲＣ等の算出により求め、この値を初期値、または中間データとして適用して、各ブロックとともに暗号処理を実行する構成としたので、入力平文ブロックの一部が同一データであった場合においても出力暗号文ブロックを異ならしめることが可能となり、差分攻撃や線形攻撃などにより、暗号処理アルゴリズムや適用鍵が露呈してしまう可能性を低減させた安全な暗号処理が可能となる。
【００６３】
さらに、本発明の構成によれば、乱数、あるいは、入力平文の要約値と、入力平文ブロックに対応するメモリ格納アドレス等の固有値に基づくハッシュ値を算出し、このハッシュ値を適用して、各ブロックとともに暗号処理を実行する構成としたので、入力平文ブロックの一部が例えば同一アドレスの同一データを含む場合においても出力暗号文ブロックを異ならしめることが可能となり、差分攻撃や線形攻撃などにより、暗号処理アルゴリズムが露呈してしまう可能性を低減させた安全な暗号処理が可能となる。
【００６４】
なお、本発明のコンピュータ・プログラムは、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ可読な形式で提供する媒体、例えば、ＣＤやＦＤ、ＭＯなどの記憶媒体に格納されて提供可能であり、またネットワークなどの伝送媒体などによっても提供可能なコンピュータ・プログラムである。
【００６５】
このようなプログラムは、プロセッサ制御の下でプログラムの読み取りに基づき、システムの有する各種機能の実行を規程するとともに、システム上の協働的作用を発揮するものであり、本発明の他の側面と同様の作用効果を得ることができるものである。
【００６６】
本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。なお、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。
【００６７】
【発明の実施の形態】
本発明の暗号処理装置および暗号処理方法、並びにコンピュータ・プログラムの実施例について、以下、図面を参照しながら説明する。
【００６８】
［実施例１］
本発明の暗号処理装置の第１実施例の構成を図５に示す。実施例１は、暗号化に先立ち平

文全体：Ｍ、または一部を入力とする所定の処理によって平文：Ｍの要約にあたる値を導き出し、暗号化処理の過程でこの平文要約値を利用することを特徴とする暗号化方式である。

【００６９】

図５に示す構成は、ＣＢＣ（Ｃｉｐｈｅｒ　Ｂｌｏｃｋ　Ｃｈａｉｎｉｎｇ）モードの暗号処理構成を基本としている。従来構成のＣＢＣモード暗号処理構成（図２参照）において用いた固定された初期値（ＩＶ：Ｉｎｉｔｉａｌ　Ｖａｌｕｅ）を用いることなく、入力平文：Ｍ全体を演算処理部３０１に入力し、その演算結果ｆ（Ｍ）を初期値の代わりに適用する。

【００７０】

なお、入力平文：Ｍは、平文ブロック：Ｍ［１］，Ｍ［２］，…，Ｍ［ｍ］の全体を意味する。演算処理部３０１の演算処理の一例として、平文：Ｍからのチェックサム（ｓｕｍ）算出処理がある。平文：Ｍからのチェックサム（ｓｕｍ）算出は、例えば下記式に従って実行される。

ｓｕｍ＝Ｍ［１］＋Ｍ［２］＋…＋Ｍ［ｍ］

である。あるいは、各ブロックの排他的論理和を算出してもよい。

ｓｕｍの計算結果が入力平文ブロックＭ［ｉ］のビット数（ｎ）を超える場合は、下位ｎビットを選択するなどの処理によってｎビットにする。この平文：Ｍからのチェックサム（ｓｕｍ）が平文の要約値となり、この要約値を演算手段３０１からの出力値ｆ（Ｍ）として排他的論理和手段３０２において先頭平文ブロックＭ［１］と、排他的論理和する。

【００７１】

本実施例の暗号処理シーケンスについて、図５を用いて説明する。まず、暗号処理を施すデータ（メッセージ）：Ｍをｎビット単位に分割しブロックデータとする。（以下、分割されたブロックデータをＭ［１］、Ｍ［２］、・・・、Ｍ［ｍ］とする）。

【００７２】

演算処理部３０１に入力平文：Ｍを入力し、上述した演算に従って平文：Ｍからのチェックサム（ｓｕｍ）を算出する。算出した結果をｆ（Ｍ）とする。算出値ｆ（Ｍ）と平文ブロックの先頭ブロックＭ［１］を排他的論理和部３０２において排他的論理和する（その結果をＩ１とする）。次に、Ｉ１を暗号処理部３０３に入れ、所定の鍵（ｅＫ）を用いて暗号化し出力Ｃ［１］を得る。続けて、Ｃ［１］およびＭ［２］を排他的論理和し、その出力Ｉ２を暗号処理部へ入れ、鍵ｅＫを用いて暗号化する（出力Ｃ［２］）。以下、これを繰り返し、全てのメッセージに対して暗号化処理を施す。

【００７３】

この実施例１の暗号の安全性について、従来技術の欄で説明したと同様の手法を適用して評価する。［選択平文攻撃１］を行なった場合について考察する。すなわち、上述の実施例１に対応する構成を持つ改良されたＣＢＣまたはＰＲＰのいずれかの処理を実行する処理部としてのオラクルｇが存在するとする。

ブロックＡとブロックＢからなる２ブロッククエリー

ブロックＡとブロックＣからなる２ブロッククエリー

の２つのクエリーＡＢ，ＡＣをオラクルｇに入力し、得られた出力ブロックをＷＸ，ＹＺとする。

【００７４】

このとき出力の先行ブロックが等しい、すなわちＷ＝Ｙであれば１、そうでなければ０を返すとする。前述したように、従来構成、すなわち、初期値ＩＶ固定のＣＢＣの場合は、先頭ブロックが両者ともＡであり、図２の構成から明らかなように、同一の初期値ＩＶを排他的論理和し、その結果に対して同一の暗号処理を施すことになるので、その結果としての出力ブロックＷ、Ｙは同一の値となる。従って、常に１を返す。一方擬似ランダム置換（ＰＲＰ：Ｐｓｅｕｄｏｒａｎｄｏｍ　Ｐｅｒｍｕｔａｔｉｏｎ）の場合、１を返す確率はほぼ０に近いと考えられるため、ＰＲＰでは無いことが容易に判断できてしまう。

【００７５】

一方、本実施例の構成においては、２ブロックのクエリーＡＢを図５に示す演算処理部３０１に入力して得られるチェックサム（ｓｕｍ１）と、クエリーＡＣを演算処理部３０１に入力して得られるチェックサム（ｓｕｍ２）とは異なる値となる。

【００７６】

従ってこれらをオラクルｇに入力して得られる出力ＷＸ，ＹＺのＷとＹが偶然一致する確率は極めて低くなり、この攻撃に対する安全性を向上でき、固定初期値ＩＶを使用する従来構成に比べ安全性が向上することが証明される。

【００７７】

従来技術の欄において説明したように、初期値ＩＶが固定だとＣＢＣは、上述した選択平文攻撃１を防ぐことができない。このため、従来は初期値ＩＶの値を毎回変える事でこのような攻撃を防ぐことが考えられてきた。このとき初期値ＩＶとして乱数やカウンタ値などが使用されていたが、カウンタ値のように、次に使用される初期値ＩＶが容易に推測される場合は、平文の最初のデータを初期値ＩＶと同じ値にするなどの方法によって攻撃することが可能になり、高い安全性を維持することはできない。

【００７８】

また、乱数を用いる場合も、もし攻撃者に発生する乱数の系列を事前に知られてしまうと同様の攻撃が可能になるため、安全性には限界がある。このような攻撃方法は、初期値ＩＶを生成する系列が平文とは無関係に決められるために可能となる。

【００７９】

例えば、乱数発生方法として、ＰＮ（Ｐｓｅｕｄｏ　Ｎｏｉｓｅ）系列等の擬似ランダム信号を利用する手法が広く知られている。ＰＮ系列は、シフトレジスタと排他的論理和（Ｅｘｃｌｕｓｉｖｅ　ＯＲ）回路によって生成されるが、シフトレジスタの初期値が同じ場合には、乱数生成処理開始後、毎回全く同じタイミングで全く同一の乱数が発生することになり、相互認証時や暗号化通信に使用する鍵生成時において、安全性が著しく損なわれてしまう。

【００８０】

また、乱数生成処理開始時からある一定期間内に乱数が確定するようなシステムの場合、発生する乱数が擬似ランダム信号の持つ周期に対してある特定の期間内に発生する乱数のみに偏ってしまうため、総当たり攻撃に対する耐性が低下してしまうという問題が生じる。

【００８１】

図６にシフトレジスタと排他的論理和（Ｅｘｃｌｕｓｉｖｅ　ＯＲ）回路によって構成されるＰＮ系列発生手段例を示す。

【００８２】

図６（ａ）に示す例は、３ビットの乱数を発生する周期７のＰＮ系列発生手段例であり、シフトレジスタ３５１，３５２，３５３の各レジスタにセットされる１または０の値をあるタイミングで乱数値として取り出す、

【００８３】

シフトレジスタ３５１の値は、シフトレジスタ３５２に出力され、シフトレジスタ３５２の値は、シフトレジスタ３５３に出力され、シフトレジスタ３５３の値は、排他的論理和演算手段３５４に入力され、シフトレジスタ３５１の値との排他的論理和演算が実行され、その結果がシフトレジスタ３５１に入力される。これら各シフトレジスタ間のデータ入出力は、所定のクロックタイミングに基づいて制御されることになる。その結果、図６（ａ）の構成を持つＰＮ系列発生手段は、図６（ｂ）に示す７種の値を周期的に発生することになる。

【００８４】

従って、シフトレジスタの初期値が同じ場合には、乱数生成処理開始後、毎回全く同じタイミングで全く同一の乱数が発生することになり、相互認証時や暗号化通信に使用する鍵生成時において、安全性が著しく損なわれてしまうという問題点が発生する。

【００８５】

本実施例のように、初期値ＩＶとして平文のチェックサムのような要約値を用いることで、平文を変えたときに初期値ＩＶが必然的に変化するため、このような攻撃を防ぐことが可能となる。

【００８６】

なお、上述した実施例１においては、入力平文の演算処理部３０１における演算処理として、チェックサムを算出する例を示したが、入力平文の演算処理部３０１における演算処は、チェックサム算出に限るものではなく、ＭＡＣ（Ｍｅｓｓａｇｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｃｏｄｅ）またはＭＤＣ（Ｍｅｓｓａｇｅ Ｄｉｇｅｓｔ Ｃｏｄｅ）等の一方向性関数、ＣＲＣ（Ｃｙｃｌｉｃ Ｒｅｄｕｎｄａｎｃｙ Ｃｈｅｃｋ）等さまざまな方法で求めた値を利用することができる。

【００８７】

また、入力平文の演算処理部３０１における演算処理によって、求めたチェックサムやＭＡＣ、ＭＤＣ、ＣＲＣ等の値としてのｆ（Ｍ）を、さらにハッシュ処理を実行した結果としての値：Ｈ（ｆ（Ｍ））を求め、この値Ｈ（ｆ（Ｍ））を排他的論理和部３０２において排他的論理和する構成としてもよい。

【００８８】

なお、上述した例では、入力平文の全体：Ｍを演算処理部３０１に入力し、演算処理を実行する構成としたが、演算処理部３０１に入力データを入力平文の全体：Ｍから選択した一部のブロックあるいは一部のデータ：Ｍ’とし、平文部分データ：Ｍ’からチェックサムやＭＡＣ、ＭＤＣ、ＣＲＣ等の値としてのｆ（Ｍ’）を求め、この値を排他的論理和部３０２において排他的論理和する構成としてもよい。

【００８９】

いずれにしても平文の全体または一部を入力とし、平文の要約値を導き出し、これを従来構成におけるＣＢＣモードの初期値ＩＶの代わりに適用する。このように、平文要約値を使用することで初期値ＩＶが固定の場合に比べて安全性は向上できる。

【００９０】

ただし、上述した実施例１の構成において、演算処理部３０１の出力する平文要約値の種類によっては別の攻撃が可能な場合がある。例えば、チェックサムの場合について考えてみると、これは同じ値を導く平文が比較的簡単に偽造できるため、図５に示す改良ＣＢＣモード構成を持つ暗号処理アルゴリズムに対しては以下に説明する攻撃の可能性がある。

【００９１】

３ブロック構成の２つのクエリーＰ：ＡＢＣおよびＱ：ＡＣＢを想定する。クエリーＰ，ＱともブロックＡ，Ｂ，Ｃから構成され順番が異なるのみの構成である。これらの２つのクエリーを上述した実施例１の改良ＣＢＣモード構成を持つ暗号処理アルゴリズムあるいは、擬似ランダム置換（ＰＲＰ）からなるオラクルｇに入力し、得られた結果をＵＶＷ、およびＸＹＺとする。

【００９２】

オラクルｇからの出力ブロックの先頭ブロックを比較し、Ｕ＝Ｘなら１、そうでなければ０を返すとする。

【００９３】

上述した実施例１の改良ＣＢＣモード構成を持つ暗号処理アルゴリズムの場合、２つのクエリーのチェックサム（ｓｕｍ）が同じ値になるため、Ｕ＝Ｘとなり、常に１を返す。一方ＰＲＰの場合１を返す確率はほぼ０であるため、上述した実施例１の改良ＣＢＣモード構成を持つ暗号処理アルゴリズムとＰＲＰとの違いが判断できる。

【００９４】

このように、同じ平文要約値を得る平文：Ｍを偽造することが容易な場合には、図５に示す改良ＣＢＣモード構成を持つ暗号処理アルゴリズムは安全性の面で問題が残る。この場合には、平文要約値としてＭＡＣやＭＤＣのような一方向性関数で、要約値から平文を偽造することが困難な値を使用することによって安全性を向上できる。

【００９５】

また平文要約値は一般に、受信側で復号したデータが正しいかどうかの検証にも利用できるので、一石二鳥の働きを持つという利点がある。

【００９６】

上述したように、入力平文の全体または一部を図５に示す構成中の演算処理部３０１に入力し、演算処理を実行して、平文要約値をチェックサムやＭＡＣ、ＭＤＣ、ＣＲＣ等の算出により求め、この値を排他的論理和部３０２において排他的論理和する構成とすることで、初期値ＩＶが固定の場合に比べて安全性の向上した暗号処理が可能となる。

【００９７】

なお、上述した実施例においては、ＣＢＣモードの処理例を代表例として説明したが、ＣＦＢ、ＯＦＢにおいても、固定初期値ＩＶの代わりに平文要約値を使用して安全性を向上させることが可能である。

【００９８】

図７を参照して、本実施例に係る改良型ＣＦＢ（Ｃｉｐｈｅｒ　Ｆｅｅｄｂａｃｋ）、改良型ＯＦＢ（Ｏｕｔｐｕｔ　Ｆｅｅｄｂａｃｋ）の暗号処理構成を説明する。（ａ）改良型ＣＦＢ（Ｃｉｐｈｅｒ　Ｆｅｅｄｂａｃｋ）モードを実行する暗号処理装置は、演算処理部３７１、レジスタ３７２、暗号処理部３７３、ビット選択部３７４、排他的論理和部３７５を有する。

【００９９】

入力平文の全体または一部（Ｍとする）を演算処理部３７１に入力し、演算処理を実行して、平文要約値をチェックサムやＭＡＣ、ＭＤＣ、ＣＲＣ等の算出により求め、この演算結果としての要約値：ｆ（Ｍ）をレジスタ３７２に格納する。その後、要約値：ｆ（Ｍ）の暗号処理部３７３における暗号処理結果をビット選択部３７４において選択した特定ビットの選択結果と、入力平文ブロックＭ［１］とを排他的論理和部３７５に入力し、排他的論理和を行い出力暗号ブロックＣ［１］を生成する。

【０１００】

その後は、従来のＣＦＢモードと同様、出力暗号ブロックＣ［ｉ］をレジスタ３７２にフィードバック格納し、暗号処理部３７３において暗号処理を実行し、ビット選択部３７４において選択されたビットを後続平文ブロックと排他的論理和する処理を繰り返し実行し、暗号文ブロック：Ｃ［１］，Ｃ［２］，…，Ｃ［ｍ］を出力する。

【０１０１】

（ｂ）改良型ＯＦＢ（Ｏｕｔｐｕｔ　Ｆｅｅｄｂａｃｋ）モードを実行する暗号処理装置は、演算処理部３８１、レジスタ３８２、暗号処理部３８３、ビット選択部３８４、排他的論理和部３８５を有する。

【０１０２】

入力平文の全体または一部（Ｍとする）を演算処理部３８１に入力し、演算処理を実行して、平文要約値をチェックサムやＭＡＣ、ＭＤＣ、ＣＲＣ等の算出により求め、この演算結果としての要約値：ｆ（Ｍ）をレジスタ３８２に格納する。その後、要約値：ｆ（Ｍ）の暗号処理部３８３における暗号処理結果をビット選択部３８４において選択した特定ビットの選択結果（ランダム系列）と、入力平文ブロックＭ［１］とを排他的論理和部３８５に入力し、排他的論理和を行い出力暗号ブロックＣ［１］を生成する。

【０１０３】

ビット選択部３８４において選択した特定ビットの選択結果（ランダム系列）は、レジスタ３８２にフィードバック格納される。以下の処理は、従来のＯＦＢモードに従った処理として実行され、レジスタ３８２、暗号処理部３８３、ビット選択部３８４の循環によりランダム系列を変更して、各入力平文ブロックＭ［ｉ］との排他的論理和を実行して暗号文ブロック：Ｃ［１］，Ｃ［２］，…，Ｃ［ｍ］を出力する。

【０１０４】

このように、ＣＦＢまたはＯＦＢモードでも、平文データ全体または一部を演算処理部に入力し、演算処理を実行して、平文要約値をチェックサムやＭＡＣ、ＭＤＣ、ＣＲＣ等の算出により求め、この演算結果としての要約値：ｆ（Ｍ）を固定された初期値ＩＶの代わ

りに適用することで、固定された初期値に起因する入出力の因果関係が解消され、安全性を高めることが可能となる。

【０１０５】

なお、ＣＢＣは暗号としてだけでなくＭＡＣの生成にも広く利用されている（ＣＢＣ－ＭＡＣと呼ばれる）。従って、平文要約値としてＣＢＣ－ＭＡＣを使用する場合、ＭＡＣの計算と暗号化に同じＣＢＣの回路を使用することも可能となる。この場合、ＭＡＣの計算には任意の初期値ＩＶを使い、求めたＭＡＣを暗号化の初期入力値：ｆ（Ｍ）として使用することになる。なお、暗号処理部において適用する鍵はＭＡＣ生成と暗号化で同じものを使用しても良いし、変えても良い。同じ鍵を使用すれば、鍵と回路を兼用でき効率的になる。

【０１０６】

なお、上述した実施例では、平文データ全体または一部を演算処理部に入力し、演算処理を実行して、平文要約値をチェックサムやＭＡＣ、ＭＤＣ、ＣＲＣ等の算出により求め、この演算結果としての要約値：ｆ（Ｍ）を固定された初期値ＩＶの代わりに適用する構成例を説明したが、平文要約値：ｆ（Ｍ）を初期値の変わりに適用するのではなく、暗号処理過程中で任意の方法で利用できる。

【０１０７】

例えば図８に示すように、演算処理部３９１の演算処理結果としての要約値：ｆ（Ｍ）、すなわち、平文データ全体または一部を演算処理部３９１に入力し、演算処理を実行して算出したチェックサムやＭＡＣ、ＭＤＣ、ＣＲＣ等を排他的論理和部３９２に入力し、平文ブロックＭ［ｉ］の入力と排他的論理和演算を行い、その後、さらに、初期値、あるいは前段の結果出力としてのＣ［ｉ－１］と排他的論理和部３９３において排他的論理和演算を行い、結果を暗号処理部３９４に入れ、暗号化処理を行ってＣ［ｉ］を得る。続けて、Ｃ［ｉ］を次段に入力する。

【０１０８】

このように、各段において、平文データ全体または一部の演算処理を実行して算出したチェックサムやＭＡＣ、ＭＤＣ、ＣＲＣ等を入力値として適用する。

【０１０９】

図８に示すように、平文データ全体または一部を演算処理部３９１に入力し、演算処理を実行して算出したチェックサムやＭＡＣ、ＭＤＣ、ＣＲＣ等を暗号化処理の過程で使用する構成によっても、暗号の安全性を向上させることができる。

【０１１０】

なお、演算処理部で算出する平文要約値：ｆ（Ｍ）は平文全体を入力とし、平文のどこか一部でも変われば値が変化するものが安全性の観点から望ましいのであるが、処理速度を優先するなどの事情がある場合、平文の一部を入力とした演算によって求めた値を利用する構成としてもよい。具体的には、平文データの構成ビットの所定ビットを選択して、演算処理部に入力し、平文要約値を計算する手法が可能である。この場合、演算処理部前段にビット選択部を設け、その出力を演算処理部に入力する構成とする。

【０１１１】

［実施例２］

次に、本発明の暗号処理装置の実施例２の構成について説明する。実施例２の暗号処理の特徴は、暗号処理の過程で、暗号化の対象となる平文の他に、個々の平文ごとに変化する値を利用すること、さらに平文または各ブロックに対応する固有値、例えば個々のデータ位置（アドレス）に関わる情報を利用する構成としたことである。

【０１１２】

図９を参照して、本実施例の暗号処理の構成について説明する。図９に示す構成は、暗号処理マイクロプロセッサとしてのＣＭＰ（Ｃｒｙｐｔｏ　Ｍｉｃｒｏｐｒｏｃｅｓｓｏｒ）の中で使用されている暗号処理手段（ＥＣＭＰ）（図４参照）の改良型である。

【０１１３】

図において、ハッシュ値生成部５０３中の、$H_{h\ K}$は、鍵ｈＫを持つハッシュ関数Ｈ（）

を実行することを示す。暗号処理部５０５中のＥ$_{ｅＫ}$は、鍵ｅＫを持つブロック暗号Ｅ（）を実行することを示している。ｒｎｄは乱数であり、個々の入力平文：Ｍごとに乱数生成部５０１において、生成し異なる乱数を適用するものとする。なお、必要であれば、乱数ｒｎｄを一つの平文の中でさらに小さい単位（例えば平文ブロックＭ［ｉ］）ごとに変更する構成としてもよい。

【０１１４】

ここでは１つの処理対象平文：Ｍに対して１つの乱数ｒｎｄを適用した例について説明する。図９中、Ａｄｒ［ｉ］は平文ブロックデータＭ［ｉ］の記憶部の格納アドレス情報を示す。

【０１１５】

図９に示す改良型ＥＣＭＰは、暗号化する平文のデータＭ［ｉ］のアドレスＡｄｒ［ｉ］（カウンタ値ｉでも良い）と、乱数生成部５０１において生成した乱数ｒｎｄとを排他的論理和部５０２において、排他的論理和し、その結果をハッシュ値生成部５０３に入力してハッシュ値を生成し、生成したハッシュ値と、入力平文ブロックＭ［ｉ］とを排他論理和部５０４において、排他的論理和し、その結果を暗号処理部５０５において暗号化して暗号文ブロックＣ［ｉ］を出力する。

【０１１６】

この構成とすることで、同じ入力値を持つブロックデータであっても、そのデータ格納場所であるアドレスが違えば暗号結果としての出力を異ならせることが可能となるとともに、同一データ、同一アドレスを持つブロックデータを入力とした場合であっても適用する乱数ｒｎｄを異ならせることで安全性が向上する。

【０１１７】

なお、この改良型ＥＣＭＰは、前述したように、暗号処理マイクロプロセッサとしてのＣＭＰ（Ｃｒｙｐｔｏ　Ｍｉｃｒｏｐｒｏｃｅｓｓｏｒ）の中で使用されている暗号処理手段である。ＣＭＰの構成例について、図１０を参照して説明する。

【０１１８】

図１０は、ＣＭＰの一構成例を示すブロック図である。ＣＭＰ５１０は、各データ処理部の統括的制御、データ入出力制御を実行するＣＰＵ５１１、保護が必要な重要データを格納するための内部メモリ５１２、外部メモリとＣＰＵ５１１間で入出力されるデータに対して暗号処理を実行する暗号処理部５１６、秘密鍵５１７、秘密鍵５１７の復号により暗号処理に適用する鍵５１９を生成する復号部５１８、暗号処理部５１６の制御を実行する制御部５１５、アドレスのオフセット値を格納し、アドレス算出部５１４に出力するオフセットレジスタ５１３、オフセットレジスタ５１３からの入力アドレスオフセット値に基づいて各データブロックのアドレスを算出し、暗号処理部５１６に出力するアドレス算出部５１４を有する。処理対象データ、プログラムなどは外部メモリに置かれ、データ入力の際はＣＰＵ５１１のアドレスバスにより指定されたデータが暗号処理部５１６によって復号されてＣＰＵ５１１に取り込まれる。データ出力の際はＣＰＵ５１１のデータが暗号処理部５１６によって暗号化されてアドレスバスにより指定された外部メモリに出力される。この機能により、外部メモリにおいては暗号化された状態のデータやプログラムを逐次暗号化または復号しながら処理することができる。図９に示す改良型ＥＣＭＰ構成は、図１０に示す暗号処理部５１６の詳細構成を示すものである。

【０１１９】

図９に示す構成を持つ改良型ＥＣＭＰの安全性について考察する。従来技術の欄で説明したと同様の手法［選択平文攻撃１］を行なった場合について考察する。上述の実施例２に対応する構成を持つ改良型ＥＣＭＰまたはＰＲＰのいずれかの処理を実行する処理部としてのオラクルｇが存在するとして、オラクルｇに、

ブロックＡとブロックＢからなる２ブロッククエリー

ブロックＡとブロックＣからなる２ブロッククエリー

の２つのクエリーＡＢ，ＡＣを入力し、得られた出力ブロックをＷＸ，ＹＺとする。ここで、クエリーＡＣのＡとＣは、それぞれ入力平文ブロックＭ［１］とＭ［２］に対応し、

ＡのアドレスはＡｄｒ［１］、ＣのアドレスはＡｄｒ［２］となる。また、クエリーＢＣのＢとＣは、それぞれ入力平文ブロックＭ［１］とＭ［２］に対応し、ＢのアドレスはＡｄｒ［１］、ＣのアドレスはＡｄｒ［２］となる。

【０１２０】

このとき出力の先行ブロックが等しい、すなわちＷ＝Ｙであれば１、そうでなければ０を返すとする。本実施例の構成においては、２つのクエリーＡＢ，ＡＣに対して異なる乱数ｒｎｄ１、ｒｎｄ２が適用されるため、２つのクエリーＡＢ，ＡＣの先行ブロックＡのデータおよびアドレスが等しい場合でも、出力ＷＸ，ＹＺについてＷ＝Ｙは成立しなくなり、この攻撃に対して常に０を返すようになる。従って、改良型ＥＣＭＰまたはＰＲＰであるかの判別は困難となる。すなわち、改良型ＥＣＭＰは、高い安全性を持つ。

【０１２１】

同様に、従来技術の欄で説明した［選択平文攻撃１Ｂ］も防ぐことができる。［選択平文攻撃１Ｂ］は、２ブロックのクエリーＡＣ，ＢＣをオラクルｇに入力し、得られた出力をＷＸ，ＹＺとし、このときＸ＝Ｚであれば１、そうでなければ０を返すものである。［選択平文攻撃１］との違いは、入力平文ブロックの後ろのブロックデータが一致している点である。ここで、クエリーＡＣのＡとＣは、それぞれ入力平文ブロックＭ［１］とＭ［２］に対応し、Ａのアドレスはａｄｒ［１］、ＣのアドレスはＡｄｒ［２］となる。また、クエリーＢＣのＢとＣは、それぞれ入力平文ブロックＭ［１］とＭ［２］に対応し、ＢのアドレスはＡｄｒ［１］、ＣのアドレスはＡｄｒ［２］となる。２ブロックのクエリーＡＣ，ＢＣの両者ともブロックＣのアドレスはＡｄｒ［２］であるが、２つのクエリーＡＣ，ＢＣに対して異なる乱数ｒｎｄ１、ｒｎｄ２が適用されるため、改良型ＥＣＭＰにおける出力ＷＸ，ＹＺにおいて、Ｘ＝Ｚとならず、この攻撃に対して常に０を返すようになる。従って、改良型ＥＣＭＰまたはＰＲＰであるかの判別は困難となる。すなわち、改良型ＥＣＭＰは、高い安全性を持つ。

【０１２２】

また、ハッシュ値生成部５０３の実行するハッシュ関数Ｈ（）において適用する鍵ｈＫが秘密であるため、選択平文攻撃２に対しても安全である。［選択平文攻撃２］は、クエリーＭとして、

Ｍ［１］＝Ｈ（Ａｄｒ［１］）

Ｍ［２］＝Ｈ（Ａｄｒ［２］）

Ｍ：Ｍ［１］．．．Ｍ［ｍ］

ただし、Ｍ［３］以降の値は任意

を設定した処理である。

【０１２３】

図９の構成を持つ改良型ＥＣＭＰまたは擬似ランダム置換（ＰＲＰ）からなるオラクルｇに対して上記した平文ブロック系列Ｍを入力して出力ブロック系列Ｃ［１］，Ｃ［２］を得た後、これらを比較する。Ｃ［１］＝Ｃ［２］ならば１を返し、そうでなければ０を返す。

【０１２４】

この攻撃に対し先に説明した従来型ＥＣＭＰ（図４）は、Ｃ［１］＝Ｃ［２］＝Ｅ（ｅＫ，０^{n}）となり、必ず一致し、ＥＣＭＰとＰＲＰとの違いが容易に判断できてしまうという脆弱性をもっていたが、本実施例に係る改良型ＥＣＭＰは、ハッシュ値生成部５０３の実行するハッシュ関数Ｈ（）において適用する鍵ｈＫを秘密に設定したため、入力値として、Ｍ［１］＝Ｈ（Ａｄｒ［１］）、Ｍ［２］＝Ｈ（Ａｄｒ［２］）を設定することが不可能であり、選択平文攻撃２に対しても安全となる。なお、０^{n}は、ビット０がｎ個連続していることを示している。

【０１２５】

このように、個々の平文ごとに異なる乱数ｒｎｄを適用することで、改良型ＥＣＭＰは、乱数を用いない従来のＥＣＭＰに比較して安全性を向上することができる。

【０１２６】

ところで乱数ｒｎｄは、平文とは無関係に選ばれるが、万一この発生パターンを攻撃者に知られてしまうと、既知のパターンを利用した攻撃によって安全性が危うくなる可能性がある。そこで、個々の平文ごとに変化する値として、乱数の代わりに、入力平文：Ｍに基づいて生成したＭＡＣ（Ｍｅｓｓａｇｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｃｏｄｅ）を使用した構成例について、以下説明する。

【０１２７】

図１１において、ハッシュ値生成部５５３中の、H_{hK}は、鍵ｈＫを持つハッシュ関数Ｈ（）を実行することを示す。暗号処理部５５５中のE_{eK}は、鍵ｅＫを持つブロック暗号Ｅ（）を実行することを示している。ＭＡＣ算出部５５１は、処理対象の平文：Ｍを入力し、ＭＡＣ（Ｍｅｓｓａｇｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｃｏｄｅ）を出力する。

【０１２８】

図１１に示すＭＡＣ適用改良型ＥＣＭＰは、暗号化する平文のデータＭ［ｉ］のアドレスＡｄｒ［ｉ］（カウンタ値ｉでも良い）と、ＭＡＣ算出部５５１において入力平文に基づいて生成したＭＡＣとを排他的論理和部５５２において、排他的論理和し、その結果をハッシュ値生成部５５３に入力してハッシュ値を生成し、生成したハッシュ値と、入力平文ブロックＭ［ｉ］とを排他論理和部５５４において、排他的論理和し、その結果を暗号処理部５５５において暗号化して暗号文ブロックＣ［ｉ］を出力する。

【０１２９】

この構成とすることで、同じ入力値を持つブロックデータであっても、そのデータ格納場所であるアドレスが違えば暗号結果としての出力を異ならせることが可能となる。また同一アドレスを持つブロックデータを含む異なる平文を入力とした場合であっても、ＭＡＣ算出部５５１において入力平文に基づいて生成したＭＡＣは異なることになり、結果として出力する暗号文ブロックＣ［ｉ］を異ならせることが可能となり、安全性が向上する。

【０１３０】

図１１に示す暗号処理構成において実行する暗号化および復号化の処理を下式に示す。

［暗号化］

【数２】

$$
\begin{aligned}
&ECMP(eK, hK, aK, M)\\
&M : M[1]..M[m] \quad m \geq 1\\
&mac = MAC(aK, M)\\
&for\ i = 1,...,m \quad do\\
&\qquad P[i] \leftarrow H(hK, Adr[i] \oplus mac) \oplus M[i]\\
&\qquad C[i] \leftarrow E(eK, P[i])\\
&end\ for\\
&return\ C[1]...C[m]
\end{aligned}
$$

【０１３１】

［復号化］

【数３】

$$ECMP^{-1}(eK, hK, mac, C)$$
$$C : C[1]...C[m] \quad m \geq 1$$
$$for\ i = 1,...,m \quad do$$
$$P[i] \leftarrow E^{-1}(eK, C[i])$$
$$M[i] \leftarrow H(hK, Adr[i] \oplus mac) \oplus P[i]$$
$$end\ for$$
$$return\ M[1]...M[m]$$

【０１３２】
なお、上記各式において、ｅＫは、図１１に示す暗号処理部５５５において適用する鍵、ｈＫは、ハッシュ値生成部５５３において適用するハッシュ生成鍵、ａＫは、ＭＡＣ生成部５５１において適用するＭＡＣ生成鍵である。
【０１３３】
この方式は、先に図９を参照して説明した改良型ＥＣＭＰにおける乱数の代わりに平文に基づくＭＡＣを適用した点である。このＭＡＣ適用改良型ＥＣＭＰ方式によっても、上述した改良型ＥＣＭＰの安全性評価の説明と同様の理由が成立し、選択平文攻撃１、１Ｂ、２に対する安全性が保障される。
【０１３４】
なお、このＭＡＣ適用改良型ＥＣＭＰ方式において、暗号文の復号処理には、暗号処理において生成した平文に基づくＭＡＣ値が必要であるため、これを受信者に渡す必要がある。ＭＡＣ値の送り方は基本的には自由であり、暗号文と共に送る、または、暗号処理部において適用する秘密鍵：ｅＫなどの鍵と一緒に送るなどの方法が考えられる。安全性を重視する場合はＭＡＣ値を暗号文と一緒に送らずに秘密鍵と一緒にセキュアなデータ通信処理として実行される鍵キー交換プロトコルを適用して安全に送るようにすることが望ましい。
【０１３５】
なお、図１１に示す構成では、個々の平文ごとに変化する値として、ＭＡＣ値を適用したが、ＭＡＣ値の代わりにチェックサム、ＭＤＣ（Ｍｅｓｓａｇｅ Ｄｉｇｅｓｔ Ｃｏｄｅ）、ＣＲＣ（Ｃｙｃｌｉｃ Ｒｅｄｕｎｄａｎｃｙ Ｃｈｅｃｋ）等を入力平文：Ｍに基づいて算出して、算出値と、個々のデータＭ［ｉ］の位置を示す情報Ａｄｒ［ｉ］とを排他的論理和（ＸＯＲ）して、その結果をハッシュ値生成部５５３に入力する処理構成としてもよい。
【０１３６】
また、図１１に示す構成では、個々の平文ごとに変化する値であるＭＡＣ値と、個々のデータＭ［ｉ］の位置を示す情報Ａｄｒ［ｉ］を排他的論理和（ＸＯＲ）して、その結果をハッシュ値生成部５５３に入力する形式としているが、本方式はこれに限るものではなく、例えば図１２に示すようにＭＡＣ生成部５５１において生成した平文Ｍに基づくＭＡＣ値を演算処理部５７１に入力し、ＭＡＣ値とＡｄｒ［ｉ］の連結データ［ＭＡＣ‖Ａｄｒ［ｉ］］を算出して、これをハッシュ値生成部５５３に入力する構成としてもよい。ハッシュ関数は通常、入力データの長さに関わらず固定長のハッシュ値を生成することができるため、このような構成でも問題は無い。なお、演算処理部５７１において生成する連結データは、［ＭＡＣ‖Ａｄｒ［ｉ］］または、［Ａｄｒ［ｉ］‖ＭＡＣ］のいずれかの態様とすることが可能である。

【０１３７】
また、ハッシュ値生成部５５３によって生成されるハッシュ値は擬似ランダム系列と考えることができるので、暗号処理部を省略してストリーム暗号として使用する図１３のような構成も可能である。
【０１３８】
さらに、図１４に示すように、ハッシュ値生成部を省略した構成としてもよい。図１４に示す構成では、ＭＡＣ算出部５８１において入力平文に基づいて生成したＭＡＣとを排他的論理和部５８２において、排他的論理和し、その結果と、暗号化する平文のデータＭ［ｉ］のアドレスＡｄｒ［ｉ］（カウンタ値ｉでも良い）とを排他的論理和部５８３において、さらに排他的論理和し、その結果を暗号処理部５８４において暗号化して暗号文ブロックＣ［ｉ］を出力する。
【０１３９】
本構成においても、同じ入力値を持つブロックデータであっても、そのデータ格納場所であるアドレスが違えば暗号結果としての出力を異ならせることが可能となる。また同一アドレスを持つブロックデータを含む異なる平文を入力とした場合であっても、ＭＡＣ算出部５８１において入力平文に基づいて生成したＭＡＣは異なることになり、結果として出力する暗号文ブロックＣ［ｉ］を異ならせることが可能となり、安全性が向上する。
【０１４０】
以上、本実施例２のいくつかの具体的構成例を図９～図１４を参照して説明した。上述した実施例においては、個々の入力平文ごとに変化する値としてＭＡＣを用いた例に関する種々の構成例を示したが、上述したように、ＭＡＣの代わりに乱数や平文のカウンタを使用したり、ＭＤＣ、チェックサム、ＣＲＣのような平文要約値を使用しても良い。個々の平文ごとに変化する値としては、ここに示した例に限るものではなく、どのような手段によって求めた値でも利用することができる。なお、安全性の面からはＭＡＣやＭＤＣのような偽造に強い一方向性関数によって求めた値を使用することが望ましい。
【０１４１】
Ａｄｒ［ｉ］は平文内の個々のデータＭ［ｉ］の位置ｉ（ｉ＝１，２，…，ｍ）に関わる情報を表すものであり、個々のデータごとに違う値を取るものであればどんなものでも良い。例えば、データＭ［ｉ］のカウンタ値ｉ、すなわち、入力平文ブロックデータ毎に異なる値として設定されたカウンタ値や、データＭ［ｉ］のメモリ上のアドレスなどを適用することが可能である。
【０１４２】
なお、暗号文Ｃ［１］，Ｃ［２］，…，Ｃ［ｍ］から求めたＭＡＣを暗号文に付加するようにしておき、受信側でＭＡＣの検査を行なった結果、不正と判断された場合には復号しないことにすれば、暗号文の改ざん検証が可能であり、より安全性を高めた通信が可能となる。
【０１４３】
上述した実施例１または実施例２の構成を持つ暗号処理部を持ち、インターネット等の通信網を介したデータ送受信可能な情報処理装置の一構成例について図１５を参照して説明する。
【０１４４】
情報処理装置７１０において、ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）７０１は、ＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）７０２、またはＨＤＤ７０４等に記憶されているプログラムに従って、各種の処理を実行し、各種のデータ処理、あるいは通信制御処理を実行する。ＲＡＭ７０３には、ＣＰＵ７０１が実行するプログラムやデータが適宜記憶される。ＣＰＵ７０１、ＲＯＭ７０２、およびＲＡＭ７０３、ＨＤＤ７０４は、バスを介して相互に接続されている。
【０１４５】
バスには、通信インタフェース７０５が接続されており、インターネット、あるいはＬＡＮ等の各種通信網を介したデータ通信を実行する。上述した実施例１、実施例２において

説明した暗号処理構成は、セキュアモジュール７１５に構成され、暗号化または復号化処理、乱数生成処理等を実行する暗号／復号化部７２２、暗号鍵、ハッシュ値生成鍵、ＭＡＣ生成鍵等の鍵データを格納した内部メモリ７２３、暗号処理、復号処理におけるデータ転送制御、シーケンス制御を実行する制御部７２１を有する。

【０１４６】

通信Ｉ／Ｆを介して入出力するデータ、あるいはハードディスク（ＨＤＤ）７０４の格納データについて、ＣＰＵ７０１の制御の下、セキュアモジュール７１５に暗号化または復号化対象データが入力され、上述した実施例に従った暗号処理が実行される。

【０１４７】

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【０１４８】

なお、明細書中において説明した一連の処理はハードウェア、またはソフトウェア、あるいは両者の複合構成によって実行することが可能である。ソフトウェアによる処理を実行する場合は、処理シーケンスを記録したプログラムを、専用のハードウェアに組み込まれたコンピュータ内のメモリにインストールして実行させるか、あるいは、各種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させることが可能である。

【０１４９】

例えば、プログラムは記憶媒体としてのハードディスクやＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）に予め記録しておくことができる。あるいは、プログラムはフレキシブルディスク、ＣＤ－ＲＯＭ（Ｃｏｍｐａｃｔ Ｄｉｓｃ Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ），ＭＯ（Ｍａｇｎｅｔｏ ｏｐｔｉｃａｌ）ディスク，ＤＶＤ（Ｄｉｇｉｔａｌ Ｖｅｒｓａｔｉｌｅ Ｄｉｓｃ）、磁気ディスク、半導体メモリなどのリムーバブル記録媒体に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体は、いわゆるパッケージソフトウエアとして提供することができる。

【０１５０】

なお、プログラムは、上述したようなリムーバブル記録媒体からコンピュータにインストールする他、ダウンロードサイトから、コンピュータに無線転送したり、ＬＡＮ（Ｌｏｃａｌ Ａｒｅａ Ｎｅｔｗｏｒｋ）、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを受信し、内蔵するハードディスク等の記憶媒体にインストールすることができる。

【０１５１】

なお、明細書に記載された各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。

【０１５２】

【発明の効果】

以上、説明したように、本発明の構成によれば、入力平文の全体または一部を演算処理部に入力し、演算処理を実行して、平文要約値をチェックサムやＭＡＣ、ＭＤＣ、ＣＲＣ等の算出により求め、この値を初期値、または中間データとして適用して、各ブロックとともに暗号処理を実行する構成としたので、入力平文ブロックの一部が同一データであった場合においても出力暗号文ブロックを異ならしめることが可能となり、差分攻撃や線形攻撃などにより、暗号処理アルゴリズムや適用鍵が露呈してしまう可能性を低減させた安全な暗号処理が可能となる。

【０１５３】

さらに、本発明の構成によれば、乱数、あるいは、入力平文の要約値と、入力平文ブロックに対応するメモリ格納アドレス等の固有値に基づくハッシュ値を算出し、このハッシュ

値を適用して、各ブロックとともに暗号処理を実行する構成としたので、入力平文ブロックの一部が例えば同一アドレスの同一データを含む場合においても出力暗号文ブロックを異ならしめることが可能となり、差分攻撃や線形攻撃などにより、暗号処理アルゴリズムが露呈してしまう可能性を低減させた安全な暗号処理が可能となる。

【図面の簡単な説明】

【図１】ＥＣＢ（Ｅｌｅｃｔｒｏｎｉｃ　Ｃｏｄｅ　Ｂｏｏｋ）モードによる暗号処理を説明する図である。

【図２】ＣＢＣ（Ｃｉｐｈｅｒ　Ｂｌｏｃｋ　Ｃｈａｉｎｉｎｇ）モードによる暗号処理構成を説明する図である。

【図３】ＣＦＢ（Ｃｉｐｈｅｒ　Ｆｅｅｄｂａｃｋ）、ＯＦＢ（Ｏｕｔｐｕｔ　Ｆｅｅｄｂａｃｋ）モードによる暗号処理構成を説明する図である。

【図４】ＣＭＰ（Ｃｒｙｐｔｏ　Ｍｉｃｒｏｐｒｏｃｅｓｓｏｒ）の中で使用されている暗号処理手段構成例を示す図である。

【図５】本発明の暗号処理装置におけるＣＢＣ（Ｃｉｐｈｅｒ　Ｂｌｏｃｋ　Ｃｈａｉｎｉｎｇ）モードを基本とした暗号処理構成を説明する図である。

【図６】ＰＮ（Ｐｓｅｕｄｏ　Ｎｏｉｓｅ）系列等の擬似ランダム信号生成処理について説明する図である。

【図７】本発明の改良型ＣＦＢ（Ｃｉｐｈｅｒ　Ｆｅｅｄｂａｃｋ）、改良型ＯＦＢ（Ｏｕｔｐｕｔ　Ｆｅｅｄｂａｃｋ）の暗号処理構成を説明する図である。

【図８】本発明の暗号処理装置におけるＣＢＣ（Ｃｉｐｈｅｒ　Ｂｌｏｃｋ　Ｃｈａｉｎｉｎｇ）モードを基本とし、中間データとして平文変換データを適用した構成を説明する図である。

【図９】本発明の暗号処理装置の実施例２としての、暗号処理マイクロプロセッサとしてのＣＭＰ（Ｃｒｙｐｔｏ　Ｍｉｃｒｏｐｒｏｃｅｓｓｏｒ）の中で使用可能な改良型暗号処理手段（ＥＣＭＰ）の構成例を示す図である。

【図１０】暗号処理マイクロプロセッサとしてのＣＭＰ（Ｃｒｙｐｔｏ　Ｍｉｃｒｏｐｒｏｃｅｓｓｏｒ）構成例を示す図である。

【図１１】入力平文：Ｍに基づいて生成したＭＡＣ（Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅ）を使用した改良型暗号処理手段（ＥＣＭＰ）の構成例を示す図である。

【図１２】ＭＡＣ値とＡｄｒ［ｉ］の連結データ［ＭＡＣ‖Ａｄｒ［ｉ］］を算出して、ハッシュ値生成部に入力する構成とした改良型暗号処理手段（ＥＣＭＰ）の構成例を示す図である。

【図１３】暗号処理部を省略してストリーム暗号として使用する構成例を示す図である。

【図１４】ハッシュ値生成部を省略した構成例を示す図である。

【図１５】通信網を介したデータ送受信可能な情報処理装置の一構成例について示す図である。

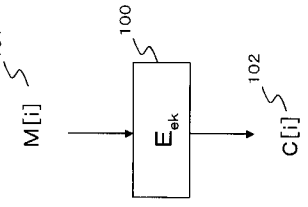
【符号の説明】

１００　暗号処理部
１０１　平文ブロックデータ
１０２　暗号文ブロックデータ
１５１　排他的論理和部
１５２　暗号処理部
２１１　レジスタ
２１２　暗号処理部
２１３　ビット選択部
２１４　排他的論理和部
２２１　レジスタ
２２２　暗号処理部
２２３　ビット選択部

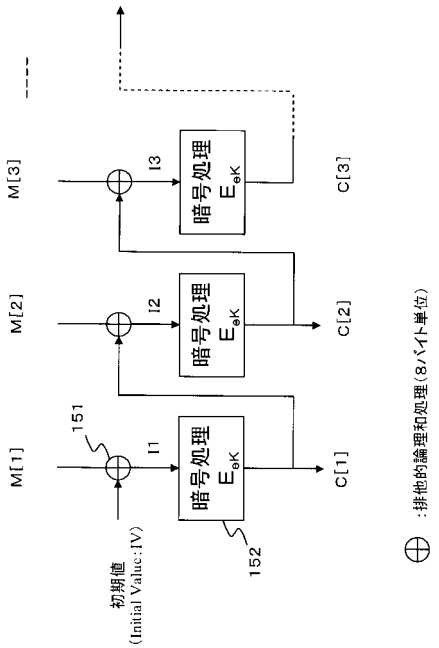
２２４　排他的論理和部
２５１　ハッシュ値生成部
２５２　排他的論理和部
２５３　暗号処理部
３０１　演算処理部
３０２　排他的論理和部
３０３　暗号処理部
３５１～３５３　シフトレジスタ
３５４　排他的論理和部
３７１　演算処理部
３７２　レジスタ
３７３　暗号処理部
３７４　ビット選択部
３７５　排他的論理和部
３８１　演算処理部
３８２　レジスタ
３８３　暗号処理部
３８４　ビット選択部
３８５　排他的論理和部
３９１　演算処理部
３９２，３９３　排他的論理和部
３９４　暗号処理部
５０１　乱数生成部
５０２　排他的論理和部
５０３　ハッシュ値生成部
５０４　排他的論理和部
５０５　暗号処理部
５１０　ＣＭＰ（Ｃｒｙｐｔｏ　Ｍｉｃｒｏｐｒｏｃｅｓｓｏｒ）
５１１　ＣＰＵ
５１２　メモリ
５１３　オフセットレジスタ
５１４　アドレス出力部
５１５　制御部
５１６　暗号処理部
５１７　秘密鍵
５１８　復号部
５１９　鍵
５５１　ＭＡＣ生成部
５５２　排他的論理和部
５５３　ハッシュ値算出部
５５４　排他的論理和部
５５５　暗号処理部
５７１　演算処理部
５８１　ＭＡＣ生成部
５８２，５８３　排他的論理和部
５８４　暗号処理部
７１０　情報処理装置
７０１　ＣＰＵ
７０２　ＲＯＭ
７０３　ＲＡＭ

７０４　ＨＤＤ
７０５　通信Ｉ／Ｆ
７１５　セキュアモジュール
７２１　制御部
７２２　暗号／復号化部
７２３　内部メモリ

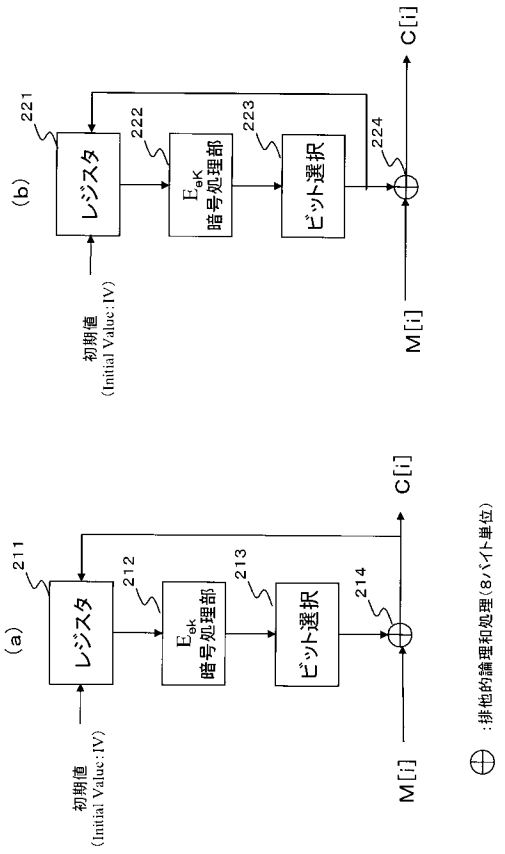
【図１】



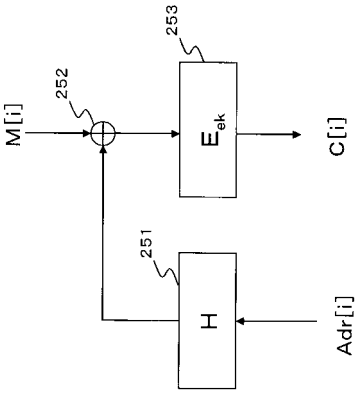
【図２】



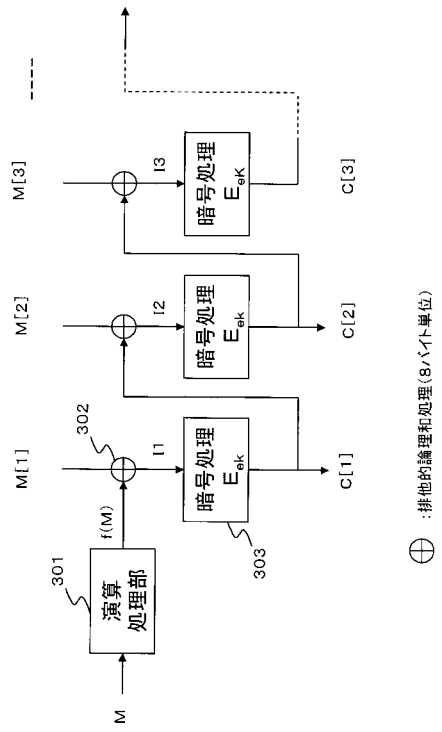
【図３】


(b)
221
レジスタ
222
E_{eK}
暗号処理部
223
ビット選択
224
C[i]
初期値
(Initial Value:IV)
M[i]
(a)
211
レジスタ
212
E_{ek}
暗号処理部
213
ビット選択
214
C[i]
初期値
(Initial Value:IV)
M[i]
:排他的論理和処理(8バイト単位)

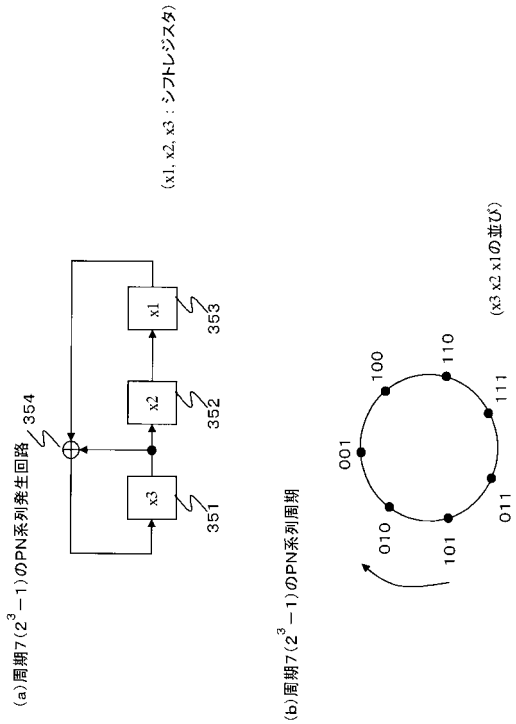
【図４】


M[i]
252
253
E_{ek}
C[i]
251
H
Adr[i]

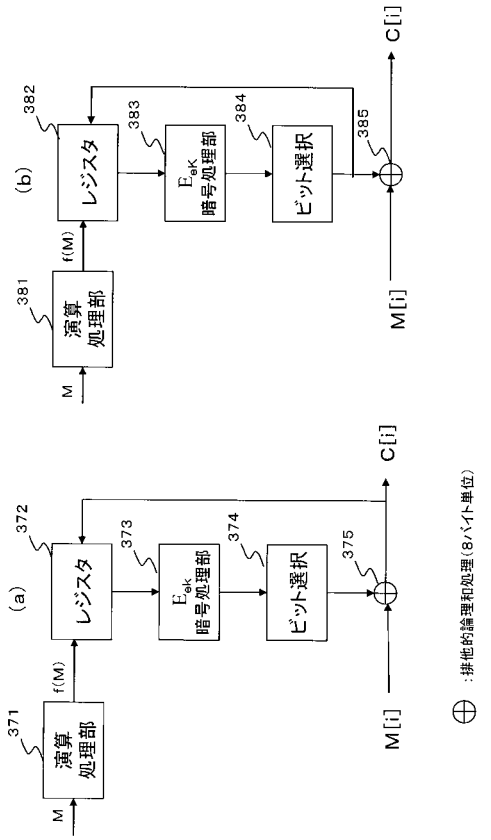
【図５】


M
演算
処理部
301
f(M)
M[1]
302
I1
暗号処理
E_{ek}
303
C[1]
M[2]
I2
暗号処理
E_{ek}
C[2]
M[3]
I3
暗号処理
E_{eK}
C[3]
:排他的論理和処理(8バイト単位)

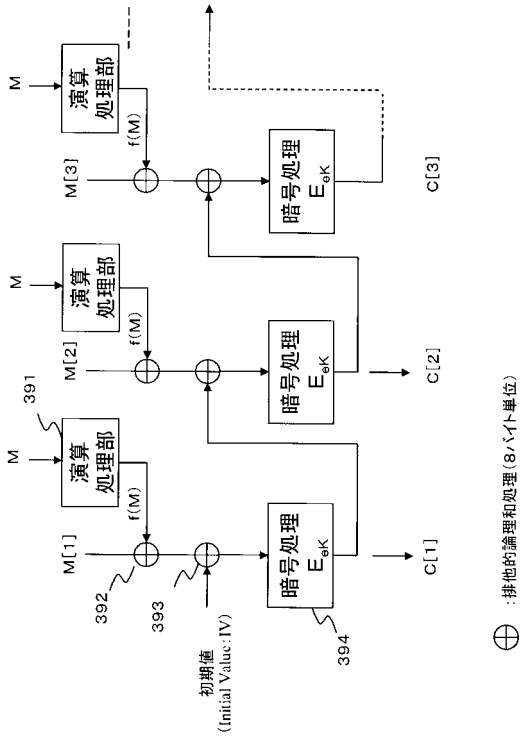
【図６】


(x1, x2, x3 : シフトレジスタ)
(a)周期7(2^3-1)のPN系列発生回路
354
x3
351
x2
352
x1
353
(b)周期7(2^3-1)のPN系列周期
001
100
110
010
111
101
011
(x3 x2 x1の並び)

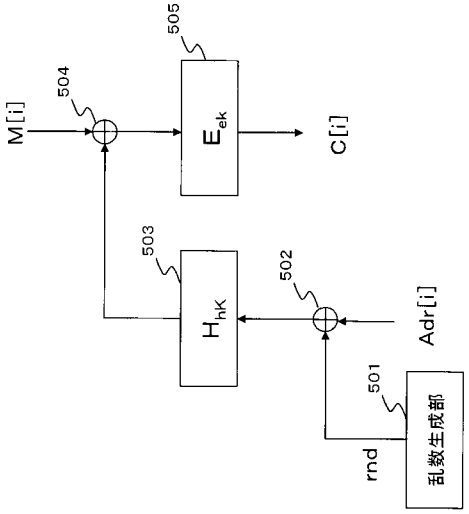
【図７】


(a)
(b)
演算処理部
レジスタ
暗号処理部
ビット選択
M
f(M)
M[i]
C[i]
:排他的論理和処理(8バイト単位)

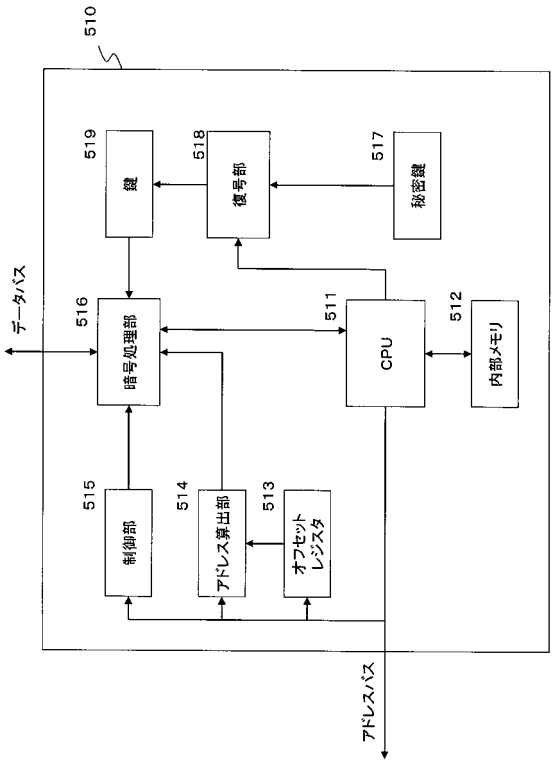
【図８】


演算処理部
暗号処理
M
f(M)
M[1]
M[2]
M[3]
C[1]
C[2]
C[3]
初期値
(Initial Value:IV)
:排他的論理和処理(8バイト単位)

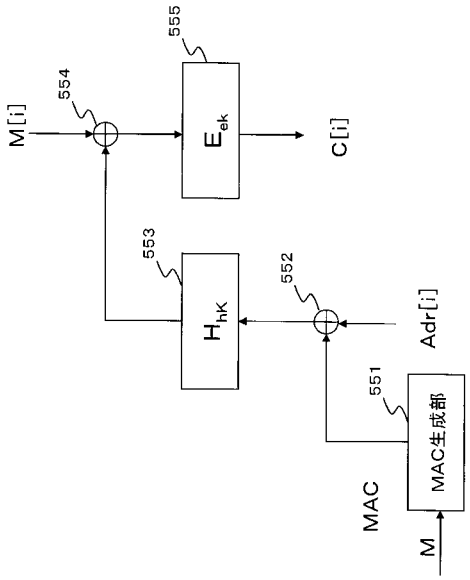
【図９】


M[i]
C[i]
Adr[i]
rnd
乱数生成部

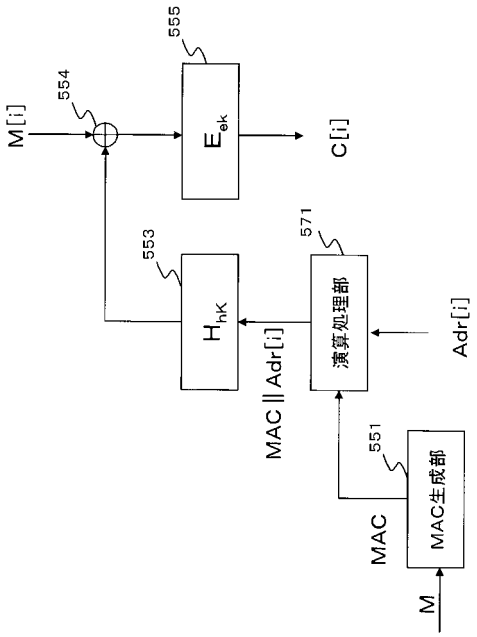
【図１０】


データバス
アドレスバス
暗号処理部
CPU
内部メモリ
鍵
復号部
秘密鍵
制御部
アドレス算出部
オフセットレジスタ

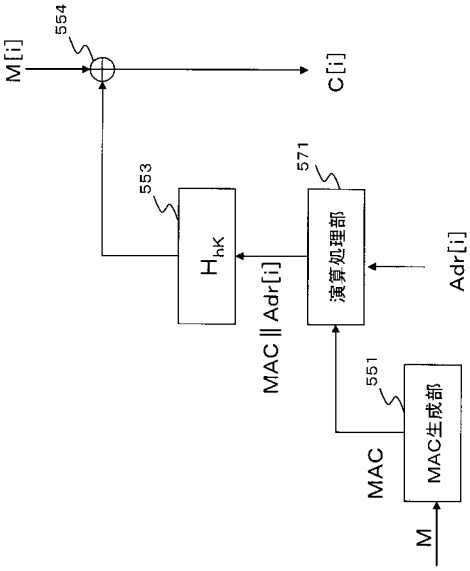
【図１１】



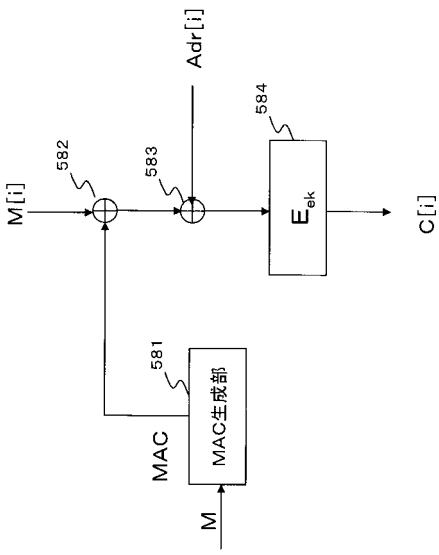
【図１２】



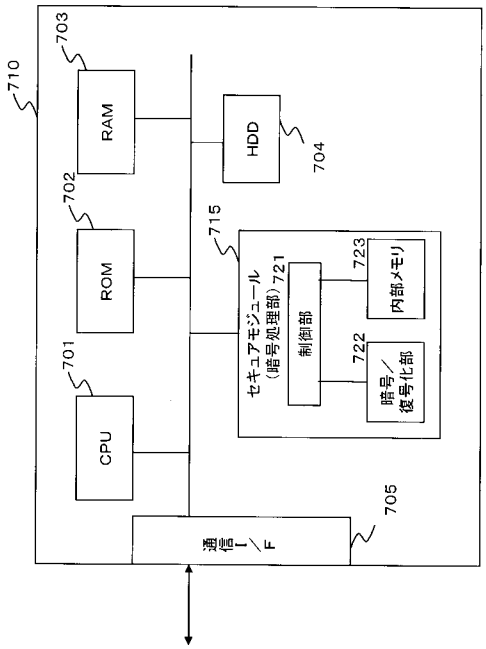
【図１３】



【図１４】



【図１５】


710
703
RAM
HDD
704
702
ROM
715
セキュアモジュール
（暗号処理部）721
制御部
723
内部メモリ
722
暗号／
復号化部
701
CPU
705
通信I／F