(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2005-31471
(P2005-31471A)
(43)公開日　平成17年2月3日(2005.2.3)

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

審査請求 未請求　請求項の数 13　ＯＬ　（全 21 頁）

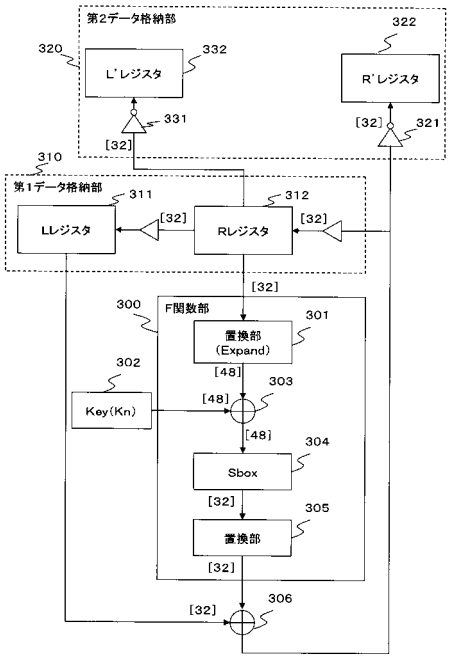
(21)出願番号　特願2003-271525(P2003-271525)
(22)出願日　平成15年7月7日(2003.7.7)

(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　阿部　譲司
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　金丸　昌司
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 AA18　AA47　JA13

(54)【発明の名称】暗号処理装置、および暗号処理方法

(57)【要約】
【課題】　消費電力の測定による暗号解析を困難としセキュリティレベルの高い暗号処理装置および方法を実現する。
【解決手段】　例えば複数段のラウンド関数部からなる共通鍵暗号処理を実行する暗号処理装置おいて、各段のＦ関数出力、すなわちＳボックスから置換部を介した中間データ出力値を、第１データ格納部のＲレジスタおよびＬレジスタにそのまま格納し、第２データ格納部のＲ’レジスタ、およびＬ’レジスタに出力値の反転データを格納する。本構成により、レジスタ格納処理におけるハミングウェイトの和を一定に保つことができる。その結果、デバイス消費電力の変化の観察に基づく鍵情報等、秘密情報に関するハミングウェイト情報の取得困難性が高まり、暗号解析困難性を高めることができる。
【選択図】　図６



【特許請求の範囲】
【請求項１】
暗号処理装置であり、
入力データのデータ処理を実行するデータ処理部と、
前記データ処理部におけるデータ処理によって生成される中間データを構成するビットデータの反転データを生成する反転データ生成手段と、
前記中間データに対応する非反転ビットデータおよび反転ビットデータを各々格納する複数のデータ記憶部と、
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、共通鍵暗号処理方式に従った暗号処理を実行する暗号処理装置であり、
前記データ処理部は、複数段のデータ変換部を構成し、
前記中間データは、前記データ変換部各段の出力データ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】
前記複数のデータ記憶部は、
前記中間データを構成するビットデータを全く反転することなく格納する第１データ記憶部と、
前記中間データを構成するビットデータを全て反転して格納する第２データ記憶部とからな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】
前記複数のデータ記憶部は、
前記中間データを構成するビットデータについて、ビット単位で反転または非反転したデータを格納する第１データ記憶部と、
前記中間データを構成するビットデータについて、前記第１データ記憶部に格納されるビットデータのビット単位の反転データを格納する第２データ記憶部とからな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】
前記反転データ生成手段は、インバータであり、
前記複数のデータ記憶部中、一方のデータ記憶部はインバータを介して反転したデータを記憶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】
前記暗号処理装置は、さらに、
前記複数のデータ記憶部中、前記データ処理部に対してデータを出力する中間データ記憶手段としてのデータ記憶部の出力段に出力データ反転処理手段を有し、
中間データ記憶手段としてのデータ記憶部に格納されたデータが、反転データである場合に、前記出力データ反転処理手段を介して再反転したデータを前記データ処理手段に出力する構成とした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】
前記暗号処理装置は、
前記複数のデータ記憶部に対するデータ格納処理におけるハミングウェイトの和を一定に保持するように、前記中間データの非反転データおよび反転データ格納処理を実行する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８】
暗号処理方法であり、
入力データのデータ処理を実行するデータ処理ステップと、
前記データ処理ステップにおけるデータ処理によって生成される中間データを構成するビットデータの反転データを生成する反転データ生成ステップと、
前記中間データに対応する非反転ビットデータおよび反転ビットデータを、各々複数の

データ記憶部に格納するデータ記憶ステップと、
を有することを特徴とする暗号処理方法。
【請求項９】
前記暗号処理方法は、共通鍵暗号処理方式に従った暗号処理を実行する暗号処理方法であり、
前記データ処理ステップは、複数段のデータ変換ステップを有し、
前記中間データは、前記データ変換ステップ各段の出力データであることを特徴とする請求項８に記載の暗号処理方法。
【請求項１０】
前記データ記憶ステップは、
前記中間データを構成するビットデータを全く反転することなく格納する第１データ記憶ステップと、
前記中間データを構成するビットデータを全て反転して格納する第２データ記憶ステップとからなることを特徴とする請求項８に記載の暗号処理方法。
【請求項１１】
前記データ記憶ステップは、
前記中間データを構成するビットデータについて、ビット単位で反転または非反転したデータを格納する第１データ記憶ステップと、
前記中間データを構成するビットデータについて、前記第１データ記憶ステップにおいて記憶部に格納されるビットデータのビット単位の反転データを格納する第２データ記憶ステップとからなることを特徴とする請求項８に記載の暗号処理方法。
【請求項１２】
前記暗号処理方法は、
データ記憶部の格納データが反転データであり、データ処理に適用すべきデータである場合に、格納データの再反転処理を行い、前記データ処理ステップは、該再反転データに対するデータ処理を実行することを特徴とする請求項８に記載の暗号処理方法。
【請求項１３】
前記暗号処理方法は、
前記複数のデータ記憶部に対するデータ格納処理におけるハミングウェイトの和を一定に保持するように、前記中間データの非反転データおよび反転データ格納処理を実行することを特徴とする請求項８に記載の暗号処理方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、暗号処理装置および暗号処理方法に関する。さらに詳細には、暗号処理を実行する例えばＩＣモジュール等の演算回路における電力解析に基づく暗号解析に対する耐性の高い暗号処理を実現する暗号処理装置および暗号処理方法に関する。
【背景技術】
【０００２】
昨今、ネットワーク通信、電子商取引の発展に伴い、通信におけるセキュリティ確保が重要な問題となっている。セキュリティ確保の１つの方法が暗号技術であり、現在、様々な暗号化手法を用いた通信が実際に行なわれている。
【０００３】
例えばＩＣカード等の小型の装置中に暗号処理モジュールを埋め込み、ＩＣカードと、データ読み取り書き込み装置としてのリーダライタとの間でデータ送受信を行ない、認証処理、あるいは送受信データの暗号化、復号化を行なうシステムが実用化されている。
【０００４】
暗号処理モジュールにおいては、例えば、平文を入力し暗号文を出力するデータ暗号化処理、あるいは暗号文を入力し平文を出力する復号化処理が実行される。これらの暗号処理は、暗号処理モジュールを構成するハードウェア、例えば半導体による電気的な処理を

含む。従って、このような半導体モジュールにおいて暗号処理が実行される際の電力消費を解析することで、暗号処理の適用鍵や、アルゴリズムが解析されてしまうという恐れがある。

【０００５】

例えば、ＩＣ等の演算処理装置に対する攻撃、すなわち暗号解読攻撃として、処理時間を解析することによる秘密情報を推定するタイミングアタック（ＴＡ：Ｔｉｍｉｎｇ ａｔａｃｋ）、暗号処理時の消費電力の観測により秘密情報を推定する単純電力解析（ＳＰＡ：Ｓｉｍｐｌｅ Ｐｏｗｅｒ Ａｎａｌｙｓｉｓ）、さらに、大量のデータに対する暗号処理における消費電力を測定し、それらの測定データを統計的に解析することにより秘密情報を推定する電力差分解析（ＤＰＡ：Ｄｉｆｆｅｒｅｎｔｉａｌ Ｐｏｗｅｒ Ａｎａｌｙｓｉｓ）等がある。

【０００６】

一般的な暗号処理装置は、データ入力部と記憶部と暗号処理部、およびデータ出力部とから構成されており、例えば入力データの暗号化を行う場合は、次のように動作する。すなわち、データ入力部から暗号処理部に平文が入力される。暗号処理部は、例えばＤＥＳ（Data Encryption Standard）などの暗号処理アルゴリズムを実行する処理部において一定の暗号処理アルゴリズムに従ったデータ処理がなされる。

【０００７】

暗号処理アルゴリズムの実行過程において生成される中間データを逐次、記憶部に格納し、また記憶部に格納した中間データを取得して予め定められた一定の処理順序に従って暗号化処理が実行される。暗号処理部において、予め定められた一連の暗号処理アルゴリズムが終了すると、生成暗号文が出力部を介して出力される。

【０００８】

このような暗号処理装置において、暗号化処理の開始時から特定の暗号化中間処理手続きが開始されるまでに要する時間は、おおよそ一定になる。なお、暗号アルゴリズムの実装方法については、例えば非特許文献１に詳しく述べられている。

【０００９】

このような暗号処理装置は、前述した単純電力解析（シンプル・パワー・アナリシス）や電力差分解析（ディファレンシャル・パワー・アナリシス）と呼ばれる暗号解析法を適用することで、暗号処理に適用する鍵情報や、アルゴリズムが解析される恐れがある。

【００１０】

単純電力解析および電力差分解析は、現在のメモリやレジスタ等の半導体デバイスにおいて、特定の時刻に、半導体デバイスの保持する値に変化が生じた場合と、保持する値に変化が生じなかった場合とで、消費電力に差が発生するという特徴を利用して、暗号処理装置が暗号処理を実行している様々なタイミングにおいて消費電力を測定することにより、暗号処理装置が保持している暗号鍵等の秘密情報を特定する暗号解析法である。

【００１１】

単純電力解析や電力差分解析が有効に機能する条件としては、第１に消費電力を測定している各時点で行われている暗号処理手続きが特定できること、第２に各時刻で測定した消費電力の値が当該時刻において暗号化装置内で行われている暗号化処理の演算結果を顕著に反映していること、の２点が挙げられる。

【００１２】

従来の暗号化装置、復号化装置および暗号化・復号装置等の暗号処理装置においては、上記の２点の条件が満たされてしまうために、単純電力解析や電力差分解析が有効に機能し、暗号の解読が可能になりうるという問題点が存在した。

【００１３】

この問題に対処するため、いくつかの方法が提案されてきた。例えば特許文献１には差分解読や線形解読を防止することを目的としたデータの暗号化方法及び装置が記載されている。本文献には、データを複数ブロックに分割して、ブロックを順次、暗号化する構成において、暗号処理対象のブロックに適用する鍵を、前の処理ブロックの中間結果から導

く構成とすることにより、ブロック毎に異なる鍵を適用した処理を行うものであり、結果として統計的な鍵推定を困難としたものである。

【００１４】

また、特許文献２には、暗号処理に適用する鍵情報の漏洩を防止した構成が示されている。本文献に記載の構成は、暗号化された鍵情報を不揮発性メモリに格納し、電源投入時に不揮発性メモリから暗号化された鍵情報を復号し、復号の結果としての鍵情報を揮発性メモリに格納して、これを暗号処理に適用するとともに、電源遮断時に揮発性メモリから鍵情報を能動的に消去することにより、鍵情報の漏洩を防止したものである。

【００１５】

また、特許文献３には、電力解析および電力差分解析等の消費電力の測定による暗号解析に対して耐性のある暗号化装置が示されている。本文献に記載の構成は、中間データ制御手段が、暗号処理において生成される中間データを乱数によって変化させ、この乱数によって変化した中間データに基づく暗号処理を実行する構成とし、さらに最終的な出力（暗号文）については、乱数に依存しないデータとすることを可能としたものである。本構成においては、暗号処理デバイスの状態変化は、乱数によって変化した中間データに基づく変化となり、その結果、電力解析および電力差分解析等、消費電力の測定による暗号解析の困難性が高まるというものである。

【００１６】

上述したように、暗号鍵あるいはアルゴリズムの漏洩に対する対策についての提案は様々存在するが、例えば特許文献１に記載の構成は、ブロック単位で、処理済みブロックから中間データを抽出し、新たな鍵を生成するといった複雑な処理が必要となり、演算処理効率の低下、処理遅延という問題を発生させる恐れがある。また、特許文献２に記載の構成は、鍵データそのものの漏洩を防止する効果は有するものの、暗号処理実行中の単純電力解析および電力差分解析等、消費電力の測定による暗号解析に対する対策とはなっていない。さらに、特許文献３に記載の乱数を利用した方法については、高階電力差分解析と呼ばれる暗号解析法によって攻撃が可能なことがＭｅｓｓｅｒｇｅｓによって既に示されている。例えば、［“ＵｓｉｎｇＳｅｃｏｎｄ－Ｏｒｄｅｒ Ｐｏｗｅｒ Ａｎａｌｙｓｉｓ ｔｏ Ａｔｔａｃｋ ＤＰＡＲｅｓｉｓｔａｎｔ Ｓｏｆｔｗａｒｅ”，Ｔ．Ｓ．Ｍｅｓｓｅｒｇｅｓ，ＣＨＥＳ２０００］に説明が記述されている。

【００１７】

暗号処理を実行する例えばＩＣモジュールは、例えば駅の改札などの様々なゲート、あるいはショッピングセンターなどで盛んに利用されるようになっており、小型化および処理の迅速化の要求が厳しくなってきている。従って、処理アルゴリズムを複雑化させることなく、かつ、電力差分解析や、高階電力差分解析に対する耐性のある構成が必要とされている。

【特許文献１】特開平９－２３０７８６号公報
【特許文献２】特開平８－５０４０６７号公報
【特許文献３】特開２０００－３０５４５３号公報
【非特許文献１】『「Ａｐｐｌｉｅｄ Ｃｒｙｐｔｏｇｒａｐｈｙ」（ＢｒｕｃｅＳｈｎｅｉｅｒ 著） Ｊｏｈｎ Ｗｉｅｌｅｙ＆ Ｓｏｎｓ，Ｉｎｃ．，１９９６，ＩＳＢＮ ０－４７１－１１７０９－９，ｐｐ．６２３－６７３』

【発明の開示】

【発明が解決しようとする課題】

【００１８】

本発明は、上記問題点に鑑みてなされたものであり、処理アルゴリズムを複雑化させることなく、暗号処理シーケンスの持つ規則的な処理に伴う消費電力変動の検出等に基づく単純電力解析、電力差分解析や高階電力差分解析による暗号解析の困難性を高めることを可能とした暗号処理装置および暗号処理方法を提供することを目的とする。

【課題を解決するための手段】

【００１９】

本発明の第１の側面は、
暗号処理装置であり、
入力データのデータ処理を実行するデータ処理部と、
前記データ処理部におけるデータ処理によって生成される中間データを構成するビットデータの反転データを生成する反転データ生成手段と、
前記中間データに対応する非反転ビットデータおよび反転ビットデータを各々格納する複数のデータ記憶部と、
を有することを特徴とする暗号処理装置にある。

【００２０】

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、共通鍵暗号処理方式に従った暗号処理を実行する暗号処理装置であり、前記データ処理部は、複数段のデータ変換部を構成し、前記中間データは、前記データ変換部各段の出力データであることを特徴とする。

【００２１】

さらに、本発明の暗号処理装置の一実施態様において、前記複数のデータ記憶部は、前記中間データを構成するビットデータを全く反転することなく格納する第１データ記憶部と、前記中間データを構成するビットデータを全て反転して格納する第２データ記憶部とからなることを特徴とする。

【００２２】

さらに、本発明の暗号処理装置の一実施態様において、前記複数のデータ記憶部は、前記中間データを構成するビットデータについて、ビット単位で反転または非反転したデータを格納する第１データ記憶部と、前記中間データを構成するビットデータについて、前記第１データ記憶部に格納されるビットデータのビット単位の反転データを格納する第２データ記憶部とからなることを特徴とする。

【００２３】

さらに、本発明の暗号処理装置の一実施態様において、前記反転データ生成手段は、インバータであり、前記複数のデータ記憶部中、一方のデータ記憶部はインバータを介して反転したデータを記憶する構成であることを特徴とする。

【００２４】

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、さらに、前記複数のデータ記憶部中、前記データ処理部に対してデータを出力する中間データ記憶手段としてのデータ記憶部の出力段に出力データ反転処理手段を有し、中間データ記憶手段としてのデータ記憶部に格納されたデータが、反転データである場合に、前記出力データ反転処理手段を介して再反転したデータを前記データ処理手段に出力する構成としたことを特徴とする。

【００２５】

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、前記複数のデータ記憶部に対するデータ格納処理におけるハミングウェイトの和を一定に保持するように、前記中間データの非反転データおよび反転データ格納処理を実行する構成を有することを特徴とする。

【００２６】

さらに、本発明の第２の側面は、
暗号処理方法であり、
入力データのデータ処理を実行するデータ処理ステップと、
前記データ処理ステップにおけるデータ処理によって生成される中間データを構成するビットデータの反転データを生成する反転データ生成ステップと、
前記中間データに対応する非反転ビットデータおよび反転ビットデータを、各々複数のデータ記憶部に格納するデータ記憶ステップと、
を有することを特徴とする暗号処理方法にある。

【００２７】

さらに、本発明の暗号処理方法の一実施態様において、前記暗号処理方法は、共通鍵暗号処理方式に従った暗号処理を実行する暗号処理方法であり、前記データ処理ステップは、複数段のデータ変換ステップを有し、前記中間データは、前記データ変換ステップ各段の出力データであることを特徴とする。

【００２８】

さらに、本発明の暗号処理方法の一実施態様において、前記データ記憶ステップは、前記中間データを構成するビットデータを全く反転することなく格納する第１データ記憶ステップと、前記中間データを構成するビットデータを全て反転して格納する第２データ記憶ステップとからなることを特徴とする。

【００２９】

さらに、本発明の暗号処理方法の一実施態様において、前記データ記憶ステップは、前記中間データを構成するビットデータについて、ビット単位で反転または非反転したデータを格納する第１データ記憶ステップと、前記中間データを構成するビットデータについて、前記第１データ記憶ステップにおいて記憶部に格納されるビットデータのビット単位の反転データを格納する第２データ記憶ステップとからなることを特徴とする。

【００３０】

さらに、本発明の暗号処理方法の一実施態様において、前記暗号処理方法は、データ記憶部の格納データが反転データであり、データ処理に適用すべきデータである場合に、格納データの再反転処理を行い、前記データ処理ステップは、該再反転データに対するデータ処理を実行することを特徴とする。

【００３１】

さらに、本発明の暗号処理方法の一実施態様において、前記暗号処理方法は、前記複数のデータ記憶部に対するデータ格納処理におけるハミングウェイトの和を一定に保持するように、前記中間データの非反転データおよび反転データ格納処理を実行することを特徴とする。

【００３２】

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。

【発明の効果】

【００３３】

本発明の構成によれば、処理アルゴリズムを複雑化することなく、様々な解析攻撃に対する耐性の高い暗号処理装置および暗号処理方法が実現される。

【００３４】

本発明の構成によれば、データの暗号化や復号を行う際に当該装置の消費電力を測定することによって暗号化鍵や復号鍵等の秘密情報を得る暗号解析法、すなわち、電力解析や電力差分解析等の消費電力の測定による暗号解析を困難とし、かつ、高階電力差分攻撃の適用についても困難とすることが可能となる。

【００３５】

本発明の構成によれば、例えば複数段のラウンド関数部からなる共通鍵暗号処理を実行する暗号処理装置おいて、各段のＦ関数出力、すなわちＳボックスから置換部を介した中間データ出力値を、第１データ格納部のＲレジスタおよびＬレジスタにそのまま格納し、第２データ格納部のＲ’レジスタ、およびＬ’レジスタに出力値の反転データを格納する。本構成により、レジスタ格納処理におけるハミングウェイトの和を一定に保つことができる。その結果、デバイス消費電力の変化の観察に基づく鍵情報等、秘密情報に関するハミングウェイト情報の取得困難性が高まり、暗号解析困難性を高めることができる。

【発明を実施するための最良の形態】

【００３６】

以下、本発明の暗号処理装置および暗号処理方法の詳細について説明する。

【実施例１】
【００３７】
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。
【００３８】
共通鍵暗号方式の１つに共通鍵をベースとして複数の鍵を生成して、生成した複数の鍵を用いて暗号処理を繰り返し実行する方式がある。このような鍵生成方式を適用したアルゴリズムの代表的なものが共通鍵ブロック暗号方式である。
【００３９】
共通鍵ブロック暗号のアルゴリズムは、主として、入力データの変換を実行するラウンド関数部と、ラウンド関数部の各ラウンドで適用する鍵を生成する鍵スケジュール部とに分けることができる。ラウンド関数部の各ランウドで適用する鍵（副鍵）は、１つの主鍵に基づいて、鍵スケジュール部に入力されて生成され、各ラウンド関数部で適用される。この共通鍵暗号方式の代表的な方式に米国連邦標準暗号方式としてのＤＥＳ（Data Encryption Standard）がある。
【００４０】
ＤＥＳ暗号処理の基本構造について、図を参照して説明する。ＤＥＳ暗号処理は、変換関数の単純な繰り返しにより、平文を暗号文に変換する構造を持つ。図１にＤＥＳ暗号処理の基本構成を示す。入力データの変換を実行するラウンド関数部１１０と、ラウンド関数部の各ラウンドで適用する鍵を生成する鍵スケジュール部１２０とによって構成される。
【００４１】
ラウンド関数部１１０において、平文（６４ビット）は、まず、初期置換部１１１において、Ｌ，Ｒ各３２ビットに分割され、分割されたＬ，Ｒ３２ビットが、第１段変換部１１２に入力され、鍵スケジュール部１２０の第１段鍵生成部１２２から入力する鍵Ｋ（１）に基づいて変換処理がなされる。変換処理結果は、次段の第２段変換部１１３に入力される。
【００４２】
鍵スケジュール部１２０においては、まず、選択置換部１２１により入力主鍵（６４ビット）のパリティ８ビットが取り除かれ、残り５６ビットの入れ替え処理が実行されて第１段鍵生成部１２２に入力される。第１段鍵生成部１２２では、入力ビット列のシフト処理およびパリティビットの除去等が実行され、４８ビットの副鍵Ｋ（１）を生成し、生成した副鍵Ｋ（１）をラウンド関数部１１０の第１段変換部１１２に出力する。第１段鍵生成部１２２では、シフト処理による上位ビット列（２８ビット）と下位ビット列（２８ビット）とを下段の第２段鍵生成部１２３に出力する。
【００４３】
ラウンド関数部は、１６段の変換部を有し、それぞれ前段の変換部の出力を入力として鍵スケジュール部１２０から入力する鍵を適用した変換処理を実行し、変換結果を後段の変換部に出力する。１６段の変換部で変換された出力が逆置換部１１４に入力され、初期置換部１１１の逆置換処理が実行されて、暗号文として出力される。
【００４４】
ラウンド関数部１１０の各ラウンドを構成する変換部の構成を図２に示す。図２に示すように、変換部は、前段（ｎ－１段）の変換部から２つの入力、Ｌ（ｎ－１）、Ｒ（ｎ－１）を入力し、鍵スケジュール部から鍵（ｋ（ｎ））を入力する。Ｆ関数部１５１において、鍵スケジュール部から入力する鍵（ｋ（ｎ））を用いて、前段変換部から入力するビット列（Ｒ（ｎ－１））の変換処理がなされ、変換結果が、前段変換部から入力する残りのビット列（Ｌ（ｎ－１））と排他論理和が実行されて、次段の変換部の出力Ｒ（ｎ）が生成される。次段の変換部には、Ｒ（ｎ－１）をＬ（ｎ）としたビット列と、上述のＦ関数および排他論理和演算により生成されたＲ（ｎ）が入力され同様の処理が繰り返される

。
【００４５】
Ｆ関数の構成を図３に示す。Ｆ関数は、非線形処理を実行する複数のＳボックス（Ｓｂｏｘ）を有する。ラウンド関数部の前段からの入力値Ｒ（ｎ－１）は置換部１７１によって４８ビットに拡大され、さらに鍵スケジュール部から入力する鍵（４８ビット）と排他論理和が実行され、その出力が６ビットずつ非線形変換処理を実行する複数のＳボックス１８１－１～８に入力される。各Ｓボックスでは、例えば変換テーブルを適用した６ビットから４ビットへの非線形変換処理が実行される。
【００４６】
Ｓボックス１８１－１～８からの出力ビット４×８＝３２ビットは、置換部１７２に入力されて、ビット位置の入れ替え処理がなされ、Ｆ関数出力３２ビットを生成して出力する。
【００４７】
図１～３を参照して説明したように複数段（１６段）の変換処理によってＤＥＳ暗号処理が実行される。このＤＥＳ暗号処理をさらに暗号強度を高めるため複数繰り返し実行する構成、例えば３回のＤＥＳ暗号処理を実行するトリプルＤＥＳ暗号処理が様々な分野、例えばインターネットを介したデータ通信機器間の相互認証処理や、ＩＣカードとリーダライタ間の相互認証処理等に適用する暗号処理として多く採用されている。なお、トリプルＤＥＳ暗号処理と区別するため、１回のＤＥＳ暗号処理をシングルＤＥＳ暗号処理と呼ぶ。
【００４８】
トリプルＤＥＳ（Ｔｒｉｐｌｅ　ＤＥＳ）暗号処理構成は、図４に示すように、図１～３を参照して説明したＤＥＳ暗号処理を３回繰り返して実行することにより、平文から暗号文を生成する。シングルＤＥＳ暗号処理部１８５、１８６，１８７のそれぞれが上述した１６段のラウンド関数部を持ち、Ｓボックスを持つＦ関数による処理を１６回繰り返す。
【００４９】
通常、トリプルＤＥＳ暗号処理では、最初のシングルＤＥＳ暗号処理部１８５と、最後のＤＥＳ暗号処理部１８７においては同じ主鍵（Ｋ１）を適用し、中間のＤＥＳ暗号処理部１８６には異なる主鍵（Ｋ２）を適用する。このように、ＤＥＳ暗号処理を複数回繰り返し実行することで、暗号強度を向上させることができる。
【００５０】
しかし、このような共通鍵暗号処理においては、暗号解析による鍵、あるいは暗号アルゴリズムの漏洩が問題となっている。暗号解析手法としては、複数の種類がある。まず、単純電力解析（ＳＰＡ：Ｓｉｍｐｌｅ　Ｐｏｗｅｒ　Ａｎａｌｙｓｉｓ）について説明する。スマートカードなどの耐タンパデバイスのほとんどはトランジスタで構成された論理回路からなり、ゲートに電圧が加えられたときに電流が流れ、電力が消費される。一般に回路の消費電力は、実行している演算と用いられているデータの値に関係する。例えば、乗法演算は０を書き込む場合よりも１を書き込む場合のほうが消費電力が大きくなり、乗法演算と平方演算ではそれぞれ異なる電力を消費する。
【００５１】
このように演算やデータ値に応じて電力消費量が変動することから、秘密情報を用いた演算を行っているデバイスの消費電力の変化を観察することで、秘密情報に関してハミングウェイトなどの情報を得ることが可能となり、エントロピーを小さくすることができる。消費電力の変化を直接解析に用いる方法を単純電力解析と呼ぶ。
【００５２】
デバイスの消費電力は、デバイスと電源または接地との間に抵抗を直列に挿入し、抵抗を流れる電流値から求めることができる。実際に共通鍵暗号の演算を行っているスマートカードに対して消費電力測定を行うと、測定波形より共通鍵暗号の各段の演算がはっきり確かめられる。さらに、消費電力波形を詳しく解析することにより鍵レジスタの交換等の

情報を得ることができる。

【００５３】

次に、電力差分解析（ＤＰＡ：Ｄｉｆｆｅｒｅｎｔｉａｌ　Ｐｏｗｅｒ　Ａｎａｌｙｓｉｓ）について説明する。耐タンパデバイスの消費電力は一般に演算内容と演算に用いられている秘密情報に依存する。しかしこれらの内容に依存した消費電力の変化は小さく、測定誤差やノイズなどから見分けることは一般に困難である。

【００５４】

そこでＫｏｃｈｅｒらは大量の測定値の平均をとって測定誤差やノイズなどの影響を小さくし、全データの平均値との差分を取ることで演算プロセスによる電力消費の影響を除いて、用いられる秘密情報による消費電力の変化のみを取り出す方法（電力差分解析）を提案した。

【００５５】

ＫｏｃｈｅｒらはＤＥＳに対する適用例を示している。まず、ラウンド関数部の第１段、または第１６段に入る鍵の一部のビットについて予想し、第１段、または第１６段の最後にメモリに書きこまれると予想されるデータの１ビットの値に注目して、その値に従って消費電力の観測データを分類する。次にそれぞれのグループについて測定値の平均をとり、それらの差分をとる。予想が正しい場合注目したビットが演算に用いられるとき消費電力の差分が大きくなる。予想が異なる場合目立った差分は確認されない。

【００５６】

電力差分解析は、具体的には、以下の手順（ステップ１～ステップ７）に従った解析が行われる。

（ステップ１）

ｍ回暗号化プロセスを観測し、それぞれ第１６段の消費電力の変化Ｔ１，・・・，Ｔｍを観測する。さらに、暗号文Ｃ１，・・・，Ｃｍを記録する。第１６段の消費電力の変化を解析に用いる場合、平文の情報は必要ない。なお、ｍは１０００程度で十分である。

【００５７】

（ステップ２）

鍵に依存した分配関数Ｄ（Ｋｓ，Ｃ）を選択する。ただし、Ｋｓは何らかの鍵情報、Ｃは暗号文である。

例えば、最終段のＳボックス１の出力の１ビット目の値に着目し、Ｓボックス１に供給される６ビットの部分鍵を推定する場合を考える。この場合、関数Ｄは次式で与えられる。

【００５８】

【数１】

$$D(C_1, C_6, K_{16}) = C_1 \oplus SBOX_1(C_6 \oplus K_{16})$$

【００５９】

ただし、

Ｋ１６は、第１６段にＳボックス１に供給される６ビットの部分鍵の予想値、

Ｃ６はＫ１６と排他論理和（ＸＯＲ）される暗号文の６ビット、

ＳＢＯＸ１（ｘ）はＳボックス１に６ビットｘが供給された場合の出力結果の１ビット目、

Ｃ１はＳＢＯＸ１の出力結果に排他論理和（ＸＯＲ）される暗号文の１ビットである。

【００６０】

（ステップ３）

関数Ｄを用いてＴ１，・・・，Ｔｍを２つのグループに分ける。
Ｓ０＝｛Ｔｉ｜Ｄ（・，・，・）＝０｝
Ｓ１＝｛Ｔｉ｜Ｄ（・，・，・）＝１｝
【００６１】
次に、それぞれのグループについて消費電力の平均値を取る。
【００６２】
【数２】

$$A_0 = \frac{1}{|S_0|} \sum_{T_i \in S_0}$$

$$T_1 = \frac{1}{|S_1|} \sum_{T_i \in S_1} T_i$$

【００６３】
ただし、｜Ｓ０｜＋｜Ｓ１｜＝ｍである。
【００６４】
（ステップ４）
Ａ０とＡ１の差分をとり、電力差分信号ΔＤを得る。
ΔＤ＝Ａ$_0$－Ａ$_1$
【００６５】
（ステップ５）
部分鍵の予想値Ｋｓが正しくない場合、Ｄ（・，・，・）は暗号文に対してほぼランダムに“０”と“１”を出力する。従って十分多くのサンプルを取ると、ΔＤの値は０に近づいていく。ただし、実際には正しい予想値Ｋｓとの相互作用のため、ΔＤの波形は完全にはフラットにならない。Ｋｓが正しい場合は、Ｄ（・，・，・）は注目したビットの実際の値と同じ値を取るため、ｍ→∞とすることで、ΔＤは注目したビットを用いるときに消費する電力に近づいていく。
【００６６】
他のデータ値や測定誤差などＤ（・，・，・）に依存しないものは０に近づいていく。消費電力はデータのビット値に依存するため、Ｄ（・，・，・）の波形は注目したビットが用いられる領域でパルスを見せ、それ以外の領域では平坦になる。
【００６７】
（ステップ６）
以上を繰り返し、Ｓボックス１に供給される部分鍵を推定する。反復の最大値は2^6＝６４回である。
【００６８】
（ステップ７）
同様の作業を残り７つのＳボックスについて行い、秘密鍵について４８ビットの情報を得る。残りの８ビットの鍵情報は全探索によって求める。これは、ＤＥＳに関する例であるが、Ｃａｍｅｌｌｉａ等で利用されている８×８Ｓｂｏｘについても同様に適用が可能である。

【００６９】
次に、高階電力差分解析について説明する。
上に述べた電力差分解析はサンプルの一つのイベントに基づいた情報に対して解析を行っているが、高次電力差分解析は複数のイベントに基づいた情報を関連付けて解析に用いる。分配関数Ｄはサンプルごとにそれぞれ異なる重み付けをしたり、２つ以上のグループ分けをしたりすることができる。そのような関数は多くの防御策を封じ、平文や暗号文の情報が不完全な場合でも解析が可能な場合がある。また、特徴的な統計的性質を持つサンプルに対しては、単純に平均をとるのではなく別の処理を行うことが有効である。
【００７０】
図１～図４を参照して説明した複数段（１６段）の変換処理によって暗号処理が実行される場合、各段の処理結果、すなわち中間データが、一旦、記憶部としてのレジスタに格納され、次の処理段での処理の開始時にレジスタから中間データが取り出されて次段の処理が実行される。すなわち、レジスタへの中間データの格納、およびレジスタからの中間データの取り出しが繰り返し実行されることになる。
【００７１】
具体的な処理について、図５を参照して説明する。図５には、Ｓボックス（Ｓｂｏｘ）２０４を持つＦ関数の構成および中間データ記憶部としてのレジスタ２０７，２０８を持つ暗号処理デバイスの構成例である。
【００７２】
図１～図４を参照して説明した複数段（１６段）の変換処理を実行する場合、各処理段毎に生成する中間データがレジスタ２０７，２０８に格納され、次の処理段では、レジスタ２０７およびレジスタ２０８から中間データが取り出されて処理が実行される。
【００７３】
図５（ａ）は図２に示す変換処理部に相当し、その詳細および中間データ記憶部としてのレジスタを示したのが図５（ｂ）である。前段（ｎ－１段）の処理結果、すなわち、Ｌ（ｎ－１）、Ｒ（ｎ－１）は、それぞれＬレジスタ２１１、Ｒレジスタ２１２に格納され、Ｒレジスタ２１２の３２ビットデータがＦ関数部２００に入力され、置換部２０１において、３２ビットから４８ビットに拡大置換される。置換部２０１は、図３の置換部１７１に相当する。
【００７４】
さらに置換部２０１の出力に対して、鍵スケジュール部から鍵（ｋ（ｎ））２０２が適用されて、排他論理和（ＸＯＲ）部２０３において排他論理和演算処理がなされ、処理結果がＳボックス２０４に入力される。Ｓボックスにおいて非線形変換が実行され、Ｓボックス２０４出力が置換部２０５でビット入れ替え等の置換処理が実行された後、置換結果が、排他論理和（ＸＯＲ）部２０６においてＬレジスタ２１１の格納値と排他論理和演算処理がなされ、その結果が、Ｒレジスタ２１２、Ｌレジスタ２１１に格納される。これらの格納データがさらに次の段の処理において取り出されて同様の処理が繰り返されることになる。
【００７５】
単純電力解析、電力差分解析、高階電力差分解析に対する対処を考慮しない、図５に示すような実装では、Ｆ関数部２００の出力が直接レジスタに蓄えられ、後段の処理には、レジスタからのデータ取り出しを実行して取り出したデータに基づく処理が実行される。
【００７６】
これらの処理を実行するデバイスは、トランジスタで構成された論理回路であり、前述したように、実行している演算と用いられているデータの値に関係する消費電力が発生する。例えば、レジスタに対するデータ書き込みにおいて、０を書き込む場合と１を書き込む場合とで異なる消費電力を示すことになる。従って、レジスタに対する中間データの書き込み、読み取りを繰り返し実行する演算を行っているデバイスの消費電力の変化を観察することで、秘密情報の解析を行うことが可能となる。
【００７７】

本発明に係る暗号処理装置のデータ処理部としての変換処理部およびデータ記憶部としてのレジスタに対するデータ記憶構成の具体的構成例を図６に示す。図６に示す本発明の暗号処理装置構成においては、上述した、単純電力解析、電力差分解析、高階電力差分解析に対処するため、Ｓボックス３０４の出力に基づくＦ関数部３００からの出力は配線によって２つに分岐され、一方は、出力値を変更することなく、第１データ格納部３１０に入力されて、Ｒレジスタ３１２およびＬレジスタ３１１に格納される。もう一方は第２データ格納部３２０に入力され、インバータ３２１，３２２を介して出力値が反転された後、Ｒ’レジスタ３２２、およびＬ’レジスタ３３２に格納される。

【００７８】

レジスタにビット値を保存する際に消費される電力はＳボックス３０４の出力のハミングウェイトに比例する（より厳密には相関が大きい）ので、このように出力値をそのまま格納する第１データ格納部３１０のＲレジスタ３１２およびＬレジスタ３１１と、出力値の反転データを格納する第２データ格納部３２０のＲ’レジスタ３２２、およびＬ’レジスタ３３２に分岐させてデータを格納することにより、双方のハミングウェイトの和を常に一定に保つことができ、上述したデバイスの消費電力の変化を観察することによる秘密情報に関するハミングウェイトの情報取得が困難となり、消費電力の変化に基づく解析の困難性を高めることができる。

【００７９】

なお、各レジスタに対する非反転データおよび反転データの格納タイミングは、ずれのないタイミングで並列に実行することが好ましい。このようなタイミング制御を行うことで、時間軸に沿ったデバイスの消費電力の変化に関するハミングウェイトの情報取得が困難となる。

【００８０】

図６に示す構成に基づく処理について説明する。図６の構成は、暗号処理を実行する複数段の変換処理を繰り返し実行するＦ関数を含む変換処理部および中間データ記憶部としてのレジスタを示す図である。

【００８１】

前段（ｎ－１段）の処理結果、すなわち、Ｌ（ｎ－１）、Ｒ（ｎ－１）は、それぞれ第１データ格納部３１０のＬレジスタ３１１、Ｒレジスタ３１２に格納され、Ｒレジスタ３１２の３２ビットデータがＦ関数部３００に入力され、置換部３０１において、３２ビットから４８ビットに拡大置換される。置換部３０１は、図３の置換部１７１に相当する。

【００８２】

さらに置換部３０１の出力に対して、鍵スケジュール部から鍵（ｋ（ｎ））３０２が適用されて、排他論理和（ＸＯＲ）部３０３において排他論理和演算処理がなされ、処理結果がＳボックス３０４に入力される。Ｓボックス３０４において非線形変換が実行され、Ｓボックス３０４出力が置換部３０５でビット入れ替え等の置換処理が実行された後、置換結果が、排他論理和（ＸＯＲ）部３０６において第１データ格納部３１０のＬレジスタ３１１の格納値と排他論理和演算処理がなされる。

【００８３】

その結果は、第１データ格納部３１０のＲレジスタ３１２、Ｌレジスタ３１１に格納され、これらの格納データがさらに次の段の処理において取り出されて同様の処理が繰り返される。さらに、本実施例の構成では、Ｓボックス３０４から置換部３０５を介した出力値が、インバータ３２１によってビットデータが反転され、第２データ格納部３２０のＲ’レジスタ３２２に格納される。Ｒ’レジスタ３２２に格納される値は、Ｒレジスタ３１２に格納される３２ビットデータを反転した３２ビットデータとなる。

【００８４】

さらに、第１データ格納部３１０のＬレジスタ３１１に格納される３２ビットデータに対応して、インバータ３３１によってビットデータが反転され、第２データ格納部３２０のＬ’レジスタ３３２に格納される。Ｌ’レジスタ３３２に格納される値は、Ｌレジスタ３１１に格納される３２ビットデータを反転した３２ビットデータとなる。

【００８５】
第２データ格納部３２０のＲ’レジスタ３２２、およびＬ’レジスタ３３２に格納されたビットデータは、次の段の処理には利用されない。
【００８６】
このように、本実施例の構成では、Ｓボックス３０４から置換部３０５を介した出力値が、第１データ格納部３１０のＲレジスタ３１２およびＬレジスタ３１１にそのまま格納されるとともに、第２データ格納部３２０のＲ’レジスタ３２２、およびＬ’レジスタ３３２に出力値の反転データを格納する構成としたので、レジスタ格納処理における双方のハミングウェイトの和を常に一定に保つことができる。その結果、デバイスの消費電力の変化の観察による秘密情報に関するハミングウェイト情報の取得困難性が高まり、結果として、消費電力の変化に基づく解析の困難性を高めることができる。
【実施例２】
【００８７】
次に、本発明の実施例２の構成について説明する。本実施例に係る暗号処理装置の変換処理部およびレジスタに対するデータ記憶構成の具体的構成例を図７に示す。図７に示す本発明の暗号処理装置構成においては、上述した、単純電力解析、電力差分解析、高階電力差分解析に対処するため、実施例１と同様、Ｓボックス４０４の出力に基づくＦ関数部４００からの出力を配線によって２つに分岐し、第１データ格納部４１０および第２データ格納部４２０に入力する。
【００８８】
この実施例２においては、第１データ格納部４１０および第２データ格納部４２０に入力する値を反転データとするか非反転データとするかを選択可能としている。第１データ格納部４１０に入力する値を非反転データとした場合、第２データ格納部４２０に入力する値を反転データとする。また、第１データ格納部４１０に入力する値を反転データとした場合、第２データ格納部４２０に入力する値を非反転データとする。
【００８９】
なお、第１データ格納部４１０および第２データ格納部４２０の各レジスタ入力段にそれぞれスイッチ４５１，４５２，４６２，４７２を設け、レジスタ格納値をインバータ４２１，４３１，４６１，４７１を介して反転データとするか、あるいはインバータを介さずに非反転データとして格納するかを設定可能としている。
【００９０】
なお、第１データ格納部４１０および第２データ格納部４２０の各レジスタに入力するビットデータはそれぞれ３２ビットデータとなるが、全ビットを反転ビットデータとするかあるいは非反転ビットデータとしてそれぞれのレジスタに入力する構成としてもよいが、３２ビットデータの１ビット毎に反転、非反転ビットデータを生成して、それぞれのレジスタに入力する構成としてもよい。
【００９１】
すなわち、例えば、Ｆ関数部４０１からの出力に基づいて排他論理和（ＸＯＲ）部４０６から出力されるビット列が［０１００１０１１・・］であるとき、全ビットの非反転データを第１データ格納部４１０のＲレジスタ４１２に入力し、反転データを第２データ格納部４２０のＲ’レジスタ４２２に格納する場合は、第１データ格納部４１０のＲレジスタ４１２に入力する値は、出力ビット列［０１００１０１１・・］と同様の値となり、第２データ格納部４２０のＲ’レジスタ４２２に入力する値は、反転ビット列［１０１１０１００・・］となる。
【００９２】
また、Ｆ関数部４０１からの出力に基づいて排他論理和（ＸＯＲ）部４０６から出力されるビット列が［０１００１０１１・・］であるとき、３２ビット中１ビット毎に反転、非反転データを第１データ格納部４１０のＲレジスタ４１２に入力し、そのＲレジスタ４１２に入力されるビットデータと逆のパターンのビットデータを第２データ格納部４２０のＲ’レジスタ４２２に格納する場合は、第１データ格納部４１０のＲレジスタ４１２に

入力する値、および第２データ格納部４２０のＲ’レジスタ４２２に入力する値は、下記のようになる。

出力ビット列　　：［０１００１０１１・・］
Ｒレジスタ格納値　：［０００１１１０・・］
Ｒ’レジスタ格納値：［１１１００００１・・］

【００９３】

上記、記述中、アンダーラインで示したデータが出力値の反転ビットデータである。

【００９４】

全ビットデータの反転データと非反転データの組み合わせでそれぞれ、第１データ格納部および第２データ格納部にビットデータを格納した場合でも、あるいは、上述のようにビット毎に反転データ、非反転データの組み合わせを生成して第１データ格納部および第２データ格納部に格納した場合でも、第１データ格納部および第２データ格納部には３２ビットの各ビットについて、０と１、あるいは１と０のビット対が相互に格納されることになる。

【００９５】

第１データ格納部４１０のＬレジスタ４１１と、第２データ格納部４２０のＬ’レジスタ４３２に格納される値もそれぞれ３２ビットの各ビットについて、０と１、あるいは１と０のビット対が相互に格納されることになる。

【００９６】

前述したように、レジスタにビット値を保存する際に消費される電力はＳボックスの出力のハミングウェイトに比例するので、第１データ格納部４１０のＲレジスタ４１２およびＬレジスタ４１１と、第２データ格納部４２０のＲ’レジスタ４２２、およびＬ’レジスタ４３２に分岐させて、０と１、あるいは１と０のビット対を格納することにより、双方のハミングウェイトの和を常に一定に保つことができ、デバイスの消費電力の変化観察によるハミングウェイトの情報取得が困難となり、消費電力の変化に基づく解析の困難性を高めることができる。

【００９７】

なお、本実施例の場合、第１データ格納部４１０の各レジスタ４１１、４１２に格納されるデータは、次段の処理に適用されることになる。従って、反転ビットデータをこれらのレジスタに格納した場合は、次の段の処理に適用するためのデータ出力の際に、再度、反転処理を実行することが必要であり、そのために、第１データ格納部４１０のＲレジスタ４１２およびＬレジスタ４１１の出力段に、インバータ４８１，４９１およびスイッチ４８２，４９２を設けてある。

【００９８】

第１データ格納部４１０のＲレジスタ４１２およびＬレジスタ４１１に格納されたビットデータが反転データである場合は、インバータ４８１，４９１を介して再度反転したビットデータを次の段の処理に適用する値として出力する。この処理により、ビットデータの反転処理が行われない場合と全く同様の出力結果を得ることが可能となる。

【００９９】

図７に示す構成に基づく処理について説明する。図７の構成は、図６と同様、暗号処理を実行する複数段の変換処理を繰り返し実行するＦ関数を含む変換処理部および中間データ記憶部としてのレジスタを示す図である。

【０１００】

前段（ｎ－１段）の処理結果に基づくビットデータは、それぞれ第１データ格納部４１０のＬレジスタ４１１、Ｒレジスタ４１２に格納される。この値は、予め設定された制御プログラムに従って、反転ビット、あるいは非反転ビットとして格納されている。

【０１０１】

Ｒレジスタ４１２の３２ビットデータは、スイッチ４８２の制御により、格納ビットが反転ビットである場合には、インバータ４８１を介してＦ関数部４００に入力され、格納ビットが非反転ビットである場合には、インバータ４８１を介さずにＦ関数部４００に入

力される。

【０１０２】

Ｆ関数部４００の置換部４０１において、３２ビットから４８ビットに拡大置換される。置換部４０１は、図３の置換部１７１に相当する。さらに置換部４０１の出力に対して、鍵スケジュール部から鍵（ｋ（ｎ））４０２が適用されて、排他論理和（ＸＯＲ）部４０３において排他論理和演算処理がなされ、処理結果がＳボックス４０４に入力される。Ｓボックス４０４において非線形変換が実行され、Ｓボックス４０４出力が置換部４０５でビット入れ替え等の置換処理が実行された後、置換結果が、排他論理和（ＸＯＲ）部４０６において第１データ格納部４１０のＬレジスタ４１１の格納値と排他論理和演算処理がなされる。なお、Ｌレジスタ４１１の３２ビットデータは、スイッチ４９２の制御により、格納ビットが反転ビットである場合には、インバータ４９１を介して排他論理和（ＸＯＲ）部４０６に入力され、格納ビットが非反転ビットである場合には、インバータ４９１を介さずに排他論理和（ＸＯＲ）部４０６に入力される。

【０１０３】

その結果は、第１データ格納部４１０のＲレジスタ４１２、Ｌレジスタ４１１に、反転ビットあるいは非反転ビットとして格納され、その格納ビットパターンと逆のパターンを持つビットデータが、第２データ格納部４２０のＲ’レジスタ４２２、Ｌ’レジスタ４３２に格納される。第２データ格納部４２０のＲ’レジスタ４２２、およびＬ’レジスタ４３２に格納されたビットデータは、次の段の処理には利用されない。

【実施例３】

【０１０４】

上述の実施例ではＤＥＳ暗号処理アルゴリズムに適用する例を中心として説明したが、ＤＥＳに代わる次世代の共通鍵暗号として知られるＡＥＳ（Advanced EncryptionStandard）暗号においても本発明の適用は可能である。ＡＥＳは、鍵長が１２８、１９２、２５６ｂｉｔと、ＤＥＳの６４ｂｉｔ鍵長に比較して長いビット長の鍵を適用した暗号処理であり、強固な安全性を持つものである。

【０１０５】

ＡＥＳでは、鍵長、ブロック長とも１２８、１９２、２５６ｂｉｔと、独立に異なるビット長とした処理が可能であり、上述したＤＥＳと同様、複数のラウンドの処理を繰り返し実行する。

【０１０６】

また、ＡＥＳ暗号処理では、図８に示すように、入力平文５０１に対してプレキー（Ｋ－ｐｒｅ）５０２を適用した初期変換（Ｐｒｅ－ｗｈｉｔｅｎｉｎｇ）を実行した後、複数ラウンドからなるＡＥＳ暗号処理部５０３においてＡＥＳ暗号処理を実行し、さらに、最終的にポストキー（Ｋ－ｐｏｓｔ）５０４を適用した最終変換（Ｐｏｓｔ－ｗｈｉｔｅｎｉｎｇ）を実行して暗号文５０５を出力する構成を持つものであり、解読困難性の高い、すなわち安全性の高い暗号処理である。

【０１０７】

このＡＥＳ暗号処理においても、ＡＥＳ暗号処理の実行過程で発生する中間データの格納において、上述したと同様の反転データを生成してレジスタに格納する構成とすることで、レジスタ格納処理における双方のハミングウェイトの和を常に一定に保つことができる。その結果、デバイスの消費電力の変化の観察による秘密情報に関するハミングウェイト情報の取得困難性が高まり、結果として、消費電力の変化に基づく解析の困難性を高めることができる。

【０１０８】

最後に、上述の暗号処理を実行するデバイスとしてのＩＣモジュール６００の構成例を図９に示す。上述の処理は、例えばＰＣ、ＩＣカード、リーダライタ、その他、様々な情報処理装置において実行可能であり、図９に示すＩＣモジュール６００は、これら様々な機器に構成することが可能である。

【０１０９】

図９に示すＣＰＵ(Central processing Unit)６０１は、暗号処理の開始や、終了、データの送受信の制御、各構成部間のデータ転送制御、その他の各種プログラムを実行するプロセッサである。メモリ６０２は、ＣＰＵ６０１が実行するプログラム、あるいは演算パラメータとしての固定データを格納するＲＯＭ（Read-Only-Memory）、ＣＰＵ６０１の処理において実行されるプログラム、およびプログラム処理において適宜変化するパラメータの格納エリア、ワーク領域として使用されるＲＡＭ（RandomAccess Memory）等からなる。ここに上述した中間テータの格納領域が形成される。また、メモリ６０２は暗号処理に必要な鍵データ等の格納領域として使用可能である。データ等の格納領域は、耐タンパ構造を持つメモリとして構成されることが好ましい。

【０１１０】

暗号処理手部６０３は、例えば上述したＤＥＳ、ＡＥＳに従った暗号処理、復号処理等を実行する。なお、ここでは、暗号処理手段を個別モジュールとした例を示したが、このような独立した暗号処理モジュールを設けず、例えば暗号処理プログラムをＲＯＭに格納し、ＣＰＵ６０１がＲＯＭ格納プログラムを読み出して実行するように構成してもよい。

【０１１１】

乱数発生器６０４は、暗号処理に必要となる鍵の生成などにおいて必要となる乱数の発生処理を実行する。

【０１１２】

送受信部６０５は、外部とのデータ通信を実行するデータ通信処理部であり、例えばリーダライタ等、ＩＣモジュールとのデータ通信を実行し、ＩＣモジュール内で生成した暗号文の出力、あるいは外部のリーダライタ等の機器からのデータ入力などを実行する。

【０１１３】

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。

【０１１４】

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。

【０１１５】

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。また、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。

【産業上の利用可能性】

【０１１６】

本発明は、認証処理、暗号処理を実行するデバイス、例えば暗号処理モジュールを持つＩＣカードあるいはその他の暗号処理装置に適用可能である。本発明の構成を適用することにより、電力解析によるＩＣモジュール内の暗号処理鍵やアルゴリズムの漏洩が困難となるので、セキュリティレベルの高い暗号処理実行機能を持つデバイスあるいは装置が提供可能となる。

【図面の簡単な説明】

【０１１７】

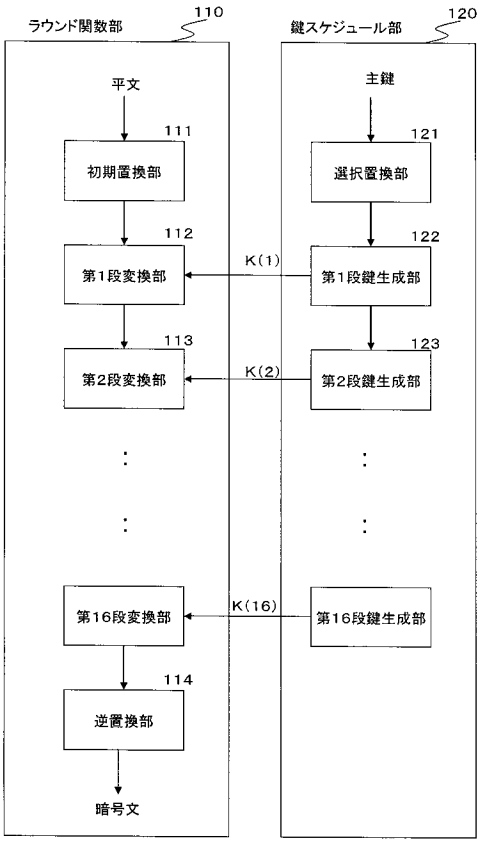
【図１】ＤＥＳ暗号処理の基本構成を示す図である。

【図２】ラウンド関数部の各ラウンドを構成する変換部の構成を示す図である。

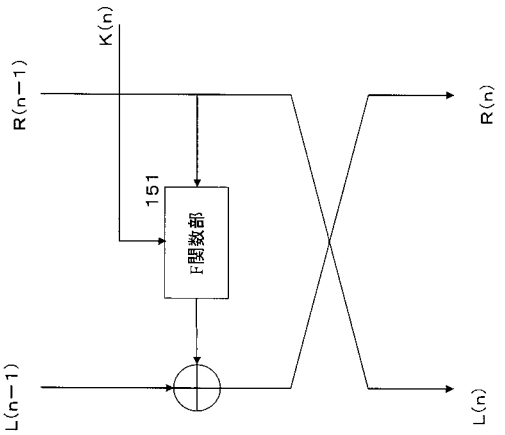
【図３】Ｆ関数の構成を示す図である。
【図４】トリプルＤＥＳ（Ｔｒｉｐｌｅ　ＤＥＳ）暗号処理構成を示す図である。
【図５】Ｓボックス（Ｓｂｏｘ）を持つＦ関数の構成および中間データ記憶部としてのレジスタを持つ暗号処理デバイスの構成例について説明する図である。
【図６】本発明に係る暗号処理装置の変換処理部およびレジスタに対するデータ記憶構成の具体的構成例（実施例１）を示す図である。
【図７】本発明に係る暗号処理装置の変換処理部およびレジスタに対するデータ記憶構成の具体的構成例（実施例２）を示す図である。
【図８】ＡＥＳ暗号処理構成を示す図である。
【図９】本発明の構成が適用可能な暗号処理実行デバイスとしてのＩＣモジュールの構成例を示す図である。
【符号の説明】
【０１１８】
１１０　ラウンド関数部
１１１　初期置換部
１１２，１１３　変換部
１１４　逆置換部
１２０　鍵スケジュール部
１２１　選択置換部
１２２，１２３　鍵生成部
１５１　Ｆ関数部
１７１，１７２　置換部
１８１　Ｓボックス
１８５，１８６，１８７　ＤＥＳ暗号処理部
２００　Ｆ関数部
２０１　置換部
２０２　鍵
２０３　排他論理和（ＸＯＲ）部
２０４　Ｓボックス
２０５　置換部
２０６　排他論理和（ＸＯＲ）部
２１１　Ｌレジスタ
２１２　Ｒレジスタ
３００　Ｆ関数部
３０１　置換部
３０２　鍵
３０３　排他論理和（ＸＯＲ）部
３０４　Ｓボックス
３０５　置換部
３０６　排他論理和（ＸＯＲ）部
３１０　第１データ格納部
３１１　Ｌレジスタ
３１２　Ｒレジスタ
３２０　第２データ格納部
３２１，３３１　インバータ
３２２　Ｒ’レジスタ
３３２　Ｌ’レジスタ
４００　Ｆ関数部
４０１　置換部
４０２　鍵

４０３　排他論理和（ＸＯＲ）部
４０４　Ｓボックス
４０５　置換部
４０６　排他論理和（ＸＯＲ）部
４１０　第１データ格納部
４１１　Ｌレジスタ
４１２　Ｒレジスタ
４２０　第２データ格納部
４２１，４３１，４６１，４７１，４８１，４９１　インバータ
４２２　Ｒ’レジスタ
４３２　Ｌ’レジスタ
４５１，４５２，４６２，４７２，４８２，４９２　スイッチ
５０１　平文
５０２　プレキー
５０３　ＡＥＳ暗号処理部
５０４　ポストキー
５０５　暗号文
６００　ＩＣモジュール
６０１　ＣＰＵ(Central processing Unit)
６０２　メモリ
６０３　暗号処理部
６０４　乱数発生器
６０５　送受信部

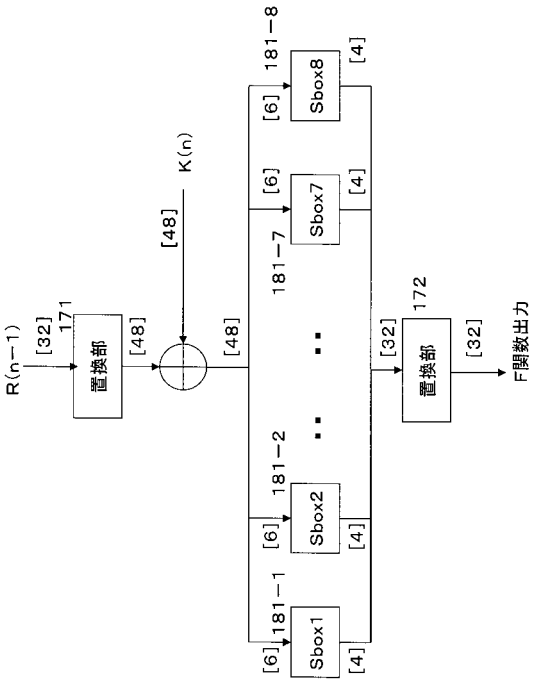
【図１】



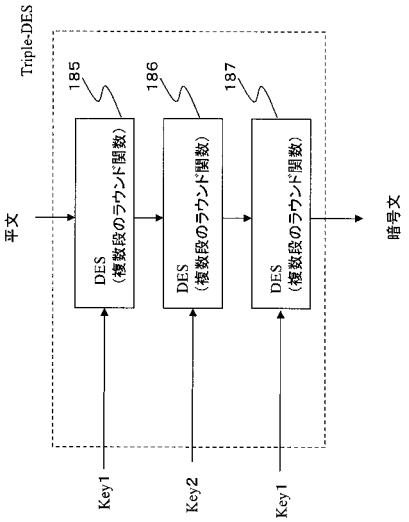
【図２】



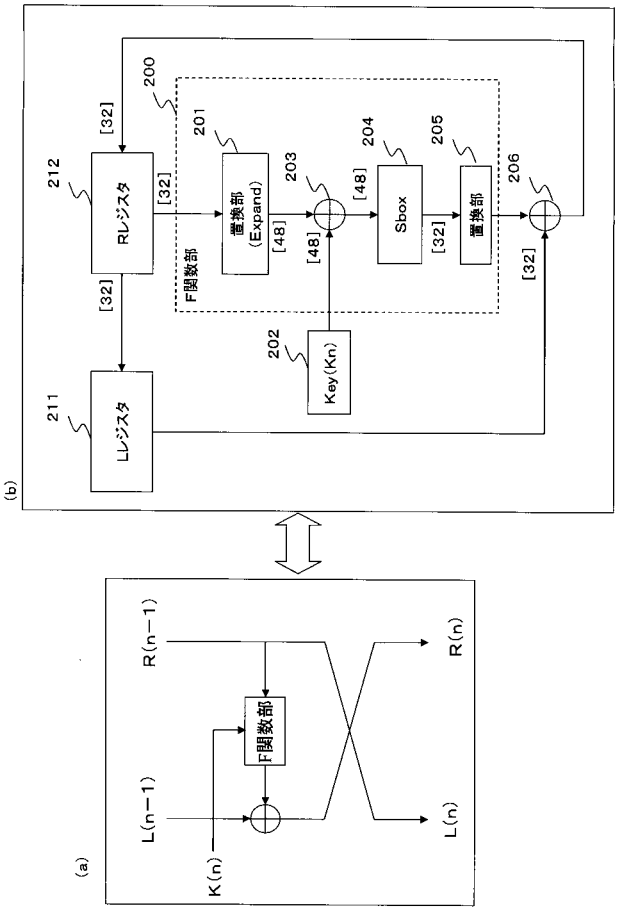
【図３】


R(n−1)
[32]
171
置換部
[48]
K(n)
[48]
181−8
Sbox8
181−7
Sbox7
181−2
Sbox2
181−1
Sbox1
[6]
[4]
[32]
172
置換部
[32]
F関数出力

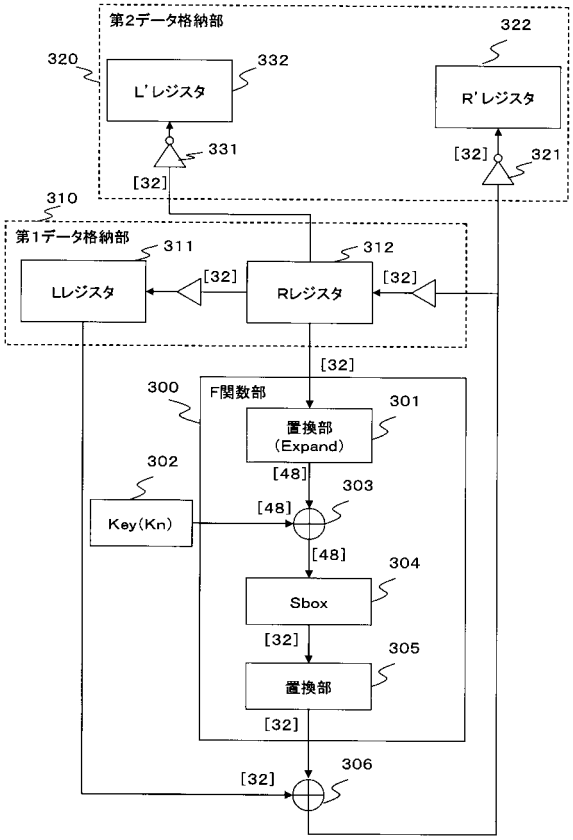
【図４】


Triple-DES
185
186
187
平文
DES
（複数段のラウンド関数）
暗号文
Key1
Key2
Key1

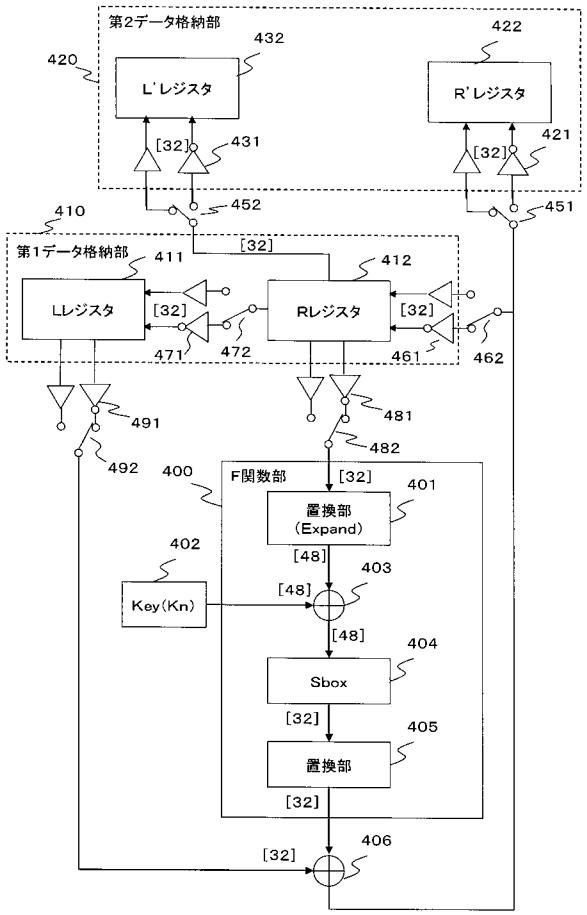
【図５】


(b)
200
201
212
RLジスタ
[32]
置換部
(Expand)
[48]
203
204
Sbox
205
置換部
206
F関数部
202
Key(Kn)
211
LLジスタ
(a)
R(n−1)
R(n)
F関数部
L(n−1)
L(n)
K(n)

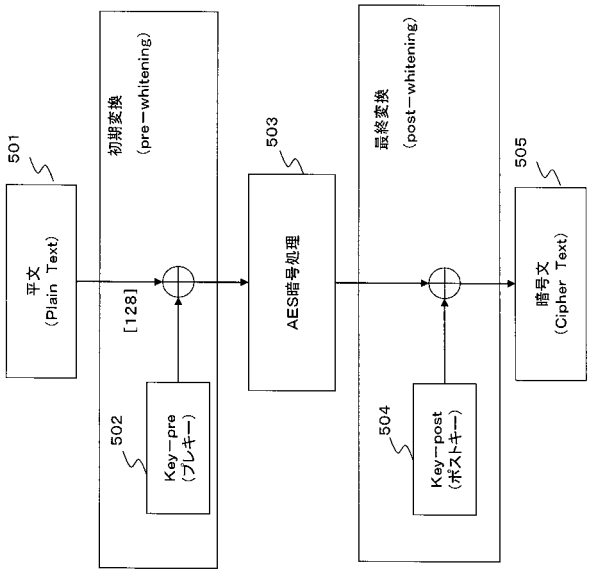
【図６】


第2データ格納部
320
L'レジスタ
332
322
R'レジスタ
331
321
[32]
310
第1データ格納部
311
LLレジスタ
312
Rレジスタ
300
F関数部
301
置換部
(Expand)
302
Key(Kn)
303
304
Sbox
305
置換部
306

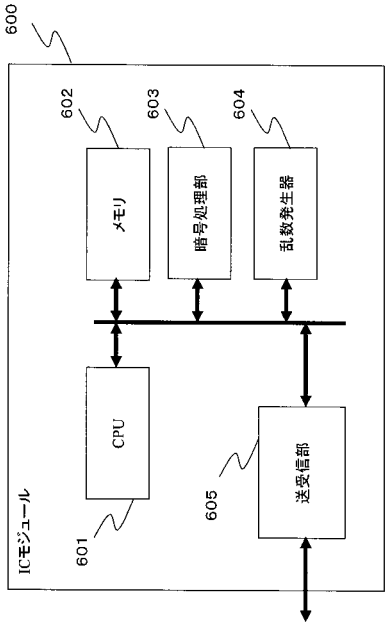
【図７】


第2データ格納部
420
432
L'レジスタ
422
R'レジスタ
[32]
431
421
452
451
410
第1データ格納部
411
412
[32]
Lレジスタ
Rレジスタ
471
472
461
462
491
481
492
482
400
F関数部
[32]
401
置換部
(Expand)
402
[48]
403
Key(Kn)
404
Sbox
405
置換部
406

【図８】


501
平文
(Plain Text)
初期変換
(pre−whitening)
[128]
502
Key−pre
(プレキー)
503
AES暗号処理
最終変換
(post−whitening)
504
Key−post
(ポストキー)
505
暗号文
(Cipher Text)

【図９】


600
602
603
604
メモリ
暗号処理部
乱数発生器
CPU
送受信部
605
601
ICモジュール