(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2010-288233
(P2010-288233A)
(43)公開日　平成22年12月24日(2010.12.24)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/10	(2006.01)	H04L	9/00	621Z	5J104

審査請求 未請求　請求項の数 5　OL　（全 11 頁）

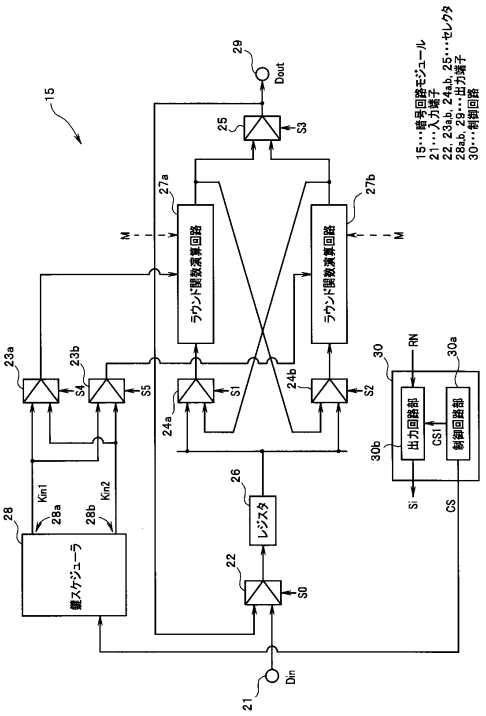
(21)出願番号　特願2009-142622 (P2009-142622)
(22)出願日　平成21年6月15日 (2009.6.15)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(74)代理人　100076233
弁理士　伊藤　進
(72)発明者　本山　雅彦
東京都港区芝浦一丁目１番１号　株式会社東芝内

Ｆターム(参考)　5J104 AA20 AA32 AA43 AA47 JA07 JA13 NA02 NA09 NA10 NA39

(54)【発明の名称】暗号処理装置

(57)【要約】
【課題】電力解析攻撃に対する耐性を確保しつつ、処理時間を短くできる暗号処理装置を提供する。
【解決手段】暗号処理装置１は、それぞれが暗号処理を実行する第１及び第２のラウンド関数演算回路２７ａ、２７ｂと、第１のラウンド関数演算回路２７ａと前記第２のラウンド関数演算回路２７ｂを並列に動作させる並列動作モード（PM）と、第１のラウンド関数演算回路２７ａと第２のラウンド関数演算回路２７ｂを直列に動作させる直列動作モード（SM）とをランダムに切り替えて、第１のラウンド関数演算回路２７ａと第２のラウンド関数演算回路２７ｂを動作させる制御回路３０とを有する。
【選択図】図２



【特許請求の範囲】
【請求項１】
それぞれが暗号処理を実行する第１及び第２の暗号演算回路と、
前記第１の暗号演算回路と前記第２の暗号演算回路を並列に動作させる並列動作モードと、前記第１の暗号演算回路と前記第２の暗号演算回路を直列に動作させる直列動作モードとをランダムに切り替えて、前記第１の暗号演算回路と前記第２の暗号演算回路を動作させる制御回路と、
を有することを特徴とする暗号処理装置。
【請求項２】
前記制御回路は、前記並列動作モードと前記直列動作モードの実行サイクルの間にダミー演算をランダムに挿入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３】
前記第１及び前記第２の暗号演算回路は、それぞれ前記乱数又は前記乱数とは異なる乱数に基づき生成されたマスクデータを用いてデータマスキングを行いながら、前記暗号処理を実行することを特徴とする請求項１又は２に記載の暗号処理装置。
【請求項４】
前記第１及び前記第２の暗号演算回路のそれぞれは、AESを利用した暗号用と復号用のラウンド関数演算回路を含むことを特徴とする請求項１から３のいずれか１つに記載に暗号処理装置。
【請求項５】
前記第１及び前記第２の暗号演算回路は、DESを利用したラウンド関数演算回路であることを特徴とする請求項１から３のいずれか１つに記載に暗号処理装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、暗号処理装置に関し、特に、電力解析攻撃に対する耐性を有する暗号処理装置に関する。
【背景技術】
【０００２】
従来より、暗号処理装置で消費される電力から暗号処理装置で用いられる秘密情報を取り出す電力解析という方法がある。このような解析方法への対策として、例えばデータマスキング法という技術が提案されている（例えば、特許文献１参照）。データマスキング法によれば、乱数発生回路がマスクデータとしての乱数を生成し、暗号処理回路は、その乱数発生回路から供給されるマスクデータを用いてデータマスキングを行いながら、暗号処理を実行する。
【０００３】
データマスキング法は、一般に、入力された平文と乱数であるマスクデータとの排他的論理和等の演算を行うことによって、入力された平文を無関係のデータに変換して暗号処理を行うようにして、電力解析攻撃に対する耐性を高めている。
上記提案に係る暗号処理装置では、DESの暗号演算の一部であるS関数を２つ用いて、その２つのS関数をランダムに切り替えるようにして、電力解析攻撃に対する耐性を持たせている。
【０００４】
しかしながら、その提案の暗号処理装置では、S関数の部分の回路規模が二倍になっているにも拘わらず、処理時間は、それまでの従来の装置と同じである。
【先行技術文献】
【特許文献】
【０００５】
【特許文献１】特開２０００－６６５８５号（特許第３６００４５４号）公報
【発明の概要】

【発明が解決しようとする課題】
【０００６】
そこで、本発明は、電力解析攻撃に対する耐性を確保しつつ、処理時間を短くできる暗号処理装置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】
【０００７】
本発明の一態様によれば、それぞれが暗号処理を実行する第１及び第２の暗号演算回路と、前記第１の暗号演算回路と前記第２の暗号演算回路を並列に動作させる並列動作モードと、前記第１の暗号演算回路と前記第２の暗号演算回路を直列に動作させる直列動作モードとをランダムに切り替えて、前記第１の暗号演算回路と前記第２の暗号演算回路を動作させる制御回路とを有する暗号処理装置を提供することができる。
【発明の効果】
【０００８】
本発明によれば、電力解析攻撃に対する耐性を確保しつつ、処理時間を短くできる暗号処理装置を実現することができる。
【図面の簡単な説明】
【０００９】
【図１】本発明の形態に係わる暗号処理装置１の構成を示す構成図である。
【図２】本発明の実施の形態に係わる暗号回路モジュール１５の構成を示すブロック図である。
【図３】本発明の実施の形態における並列動作モードPMと直列動作モードSMの切り替えによる演算状況の例を説明するための図である。
【図４】本発明の実施の形態の変形例に係る暗号処理装置の暗号回路モジュール１５Aの構成例を示すブロック図である。
【図５】本発明の実施の形態の変形例における並列動作モードPMと直列動作モードSMの切り替えによる演算状況の例を説明するための図である。
【発明を実施するための形態】
【００１０】
以下、図面を参照して本発明の実施の形態を説明する。
（構成）
まず、図１に基づき、本発明の実施の形態に係わる暗号処理回路が搭載される暗号処理装置の構成を説明する。図１は、本実施の形態に係わる暗号処理装置１の構成を示す構成図である。
【００１１】
暗号処理装置１は、中央処理装置（CPU）１１と、プログラム等を記憶したROM１２と、CPU１１の作業用記憶領域としてのRAM１３と、外部とのデータの送受信を行うための送受信インターフェース回路（以下、送受信I/Fと略す）１４と、暗号処理回路を含む暗号回路モジュール１５と、暗号回路モジュール１５とバス１６との暗号回路I/F１７と、乱数を発生する回路である乱数発生回路１８を含んで構成されている。CPU１１と、ROM１２と、RAM１３と、送受信I/F１４と、暗号回路I/F１７は、バス１６を介して互いに接続されている。
【００１２】
暗号処理装置１は、例えば、IC（Integrated Circuit）カードであり、カードリーダ装置等の外部装置（図示せず）からのデータを受信すると、そのデータに対して所定の暗号処理を施し、その暗号処理結果のデータを出力又は送信する。外部装置とのデータの送受信は、送受信I/F１４を介して、例えば、図示しない無線通信用の回路を介して無線通信により行われる。
【００１３】
また、CPU１１と暗号回路モジュール１５間で送受信されるデータも、暗号化される。

暗号回路モジュール１５は、２つの暗号処理回路を含み、暗号化及び／又は復号化の処理、を実行する。本実施の形態の暗号処理回路は、DES（Data Encryption Standard）のラウンド関数を用いた回路である。DESのラウンド関数にはデータ入力の他に、各ラウンドに入力されるラウンド鍵（拡大鍵）が、鍵データとして入力される。

乱数発生回路１８は、乱数を生成して出力する回路である。

【００１４】

また、図２は、暗号回路モジュール１５の構成を示すブロック図である。

図２に示すように、暗号回路モジュール１５は、入力端子２１、選択回路であるセレクタ２２、２３ａ、２３ｂ、２４ａ、２４ｂ、２５、レジスタ２６、所定のラウンド関数を演算するラウンド関数演算回路２７ａ、２７ｂ、鍵スケジューラ２８、出力端子２９、及び制御回路３０を有して構成されている。

【００１５】

入力端子２１は、暗号回路I/F１７からの入力データDinを入力する端子である。セレクタ２２は、ラウンド関数演算の結果出力と入力データDinのいずれか一方を、選択信号S0に応じて選択して出力するための回路である。レジスタ２６は、セレクタ２２の出力を入力し、入力データDin又はラウンド関数演算の中間結果を保持して出力するための回路である。

【００１６】

セレクタ２４ａ、２４ｂは、図２に示すように、それぞれ制御回路３０からの選択信号S1,S2に応じて、レジスタ２６の出力あるいはラウンド関数演算回路２７ｂ、２７ａの出力のいずれか一方を選択して出力するための回路である。

【００１７】

ラウンド関数演算回路２７ａ、２７ｂは、所定の暗号化演算処理あるいは所定の復号化演算処理の暗号処理を実行する回路である。よって、暗号処理は、暗号化処理あるいは復号化処理を意味する。ラウンド関数演算回路２７ａとラウンド関数演算回路２７ｂのそれぞれは、鍵スケジューラ２８からの鍵データであるラウンド鍵Kinを入力する入力端子を有する。

【００１８】

セレクタ２２は、暗号処理を開始するときは、制御回路３０からの選択信号S0により入力端子２１からの入力データDinを選択して、レジスタ２６に出力するように制御され、ラウンド関数演算中は、制御回路３０からの選択信号S0によりラウンド関数演算の演算結果のデータを選択して、レジスタ２６に出力するように制御される。

【００１９】

レジスタ２６は、暗号処理中は、暗号処理の中間結果を保持する。レジスタ２６の出力は、２つのセレクタ２４ａと２４ｂのそれぞれの一方の入力端子に入力される。セレクタ２４ａの他方の入力端子には、ラウンド関数演算回路２７ｂの出力が入力される。セレクタ２４ｂの他方の入力端子には、ラウンド関数演算回路２７ａの出力が入力される。

【００２０】

セレクタ２４ａの出力は、ラウンド関数演算回路２７ａに供給され、セレクタ２４ｂの出力は、ラウンド関数演算回路２７ｂに供給される。

ラウンド関数演算回路２７ａと２７ｂの出力は、セレクタ２５に入力される。セレクタ２５の出力は、セレクタ２２の他方の入力端子に供給され、かつ出力端子２９に供給される。最終的な暗号処理の結果は、出力データDoutとして出力端子２９から出力される。

【００２１】

セレクタ２４ａ、２４ｂ、２５は、それぞれ、制御回路３０からの選択信号S1、S2、S3に応じて２つの入力の一方を選択して出力する。

鍵スケジューラ２８は、制御回路３０からの制御信号CSに基づいて、２つのラウンド鍵Kin1,Kin2を生成して出力する回路である。２つのラウンド鍵Kin1,Kin2は、それぞれ鍵スケジューラ２８の２つの出力端子２８ａ、２８ｂから出力される。２つのラウンド鍵Kin1,Kin2は、２つのセレクタ２３ａ、２３ｂに入力される。２つのセレクタ２３ａと２３ｂ

は、それぞれ、制御回路３０からの選択信号S4とS5に応じて、入力された２つのラウンド鍵Kin1,Kin2のいずれか一方を選択して、ラウンド関数演算回路２７ａ、２７ｂに出力する。

【００２２】

セレクタ２３ａと２３ｂは、２つのラウンド関数演算回路に入力されるラウンド鍵Kin1,Kin2を制御するための回路である。後述するように、並列動作モードPMのときは、セレクタ２３ａと２３ｂは、そのサイクルにおいて実行するラウンド関数演算に使用されるラウンド鍵を選択して出力する。セレクタ２３ａと２３ｂは、直列動作モードSMのときは、そのサイクルにおいて先に演算処理を行うラウンド関数演算回路に最初のラウンド鍵を、後に演算処理を行うラウンド関数演算回路に２番目のラウンド鍵を入力するように、制御される。すなわち、２つのラウンド関数演算回路は、互いに時間をずらして動作する。例えば、あるサイクルにおいて、ラウンド関数演算回路２７ｂが先に処理を行い、かつ第１の出力端子２８ａから最初のラウンド鍵が出力され、第２の出力端子２８ｂから２番目のラウンド鍵が出力されていた場合、セレクタ２３ａと２３ｂは、ラウンド関数演算回路２７ｂに、最初のラウンド鍵が供給され、ラウンド関数演算回路２７ａに２番目のラウンド鍵が供給されるように制御される。

【００２３】

制御回路３０は、制御回路部３０ａと出力回路部３０ｂとを含んで構成されている。制御回路３０は、並列動作モードPMと直列動作モードSMの２つのモードで、暗号処理を実行するように暗号回路モジュール１５を制御するための回路である。

【００２４】

制御回路部３０ａは、暗号処理においてラウンドの状態（例えば、実行サイクルが何ラウンド目であるか等）を管理し、鍵スケジューラ２８への制御信号CSと、出力回路部３０ｂに対する制御信号CS1を出力する回路部である。

さらに、制御回路３０は、乱数発生回路１８からの乱数データRNに基づいて、ラウンド関数演算回路２７ａと２７ｂを、後述する並列動作モードPMと直列動作モードSMでランダムに動作させるようにするための選択信号Si（ここで、ｉは、１から５）を出力する。

【００２５】

図２の場合、乱数データRNは、出力回路部３０ｂに入力される。出力回路部３０ｂは、乱数データの値に応じて、並列動作モードPMと直列動作モードSMのいずれかのモードでラウンド関数演算回路を動作させるように、選択信号Siを生成して出力する回路部である。

【００２６】

例えば、乱数データRNは、「１」と「０」のランダムデータでもよい。乱数データRNの「１」が並列動作モードPM、「０」が直列動作モードSMに対応させて、出力回路部３０ｂは、そのモードに応じた選択信号Siを出力するようにしてもよい。

【００２７】

（動作）

次に図２に示した暗号回路モジュール１５の動作を説明する。

制御回路３０は、乱数発生回路１８からの乱数に応じて、並列動作モードPMと直列動作モードSMをランダムに変化させながら、ラウンド関数演算回路２７ａと２７ｂを動作させる。

【００２８】

並列動作モードPMでラウンド関数演算を行う場合は、セレクタ２４ａと２４ｂは、共にレジスタ２６からの出力を選択する。そのため、制御回路３０からは、レジスタ２６の出力を選択するように、選択信号S1,S2がセレクタ２４ａと２４ｂに出力される。従って、ラウンド関数演算回路２７ａと２７ｂには、レジスタ２６の出力が入力される。ラウンド関数演算回路２７ａと２７ｂには、同じデータが入力され、それぞれ処理が行われる。ラウンド関数演算回路２７ａと２７ｂのそれぞれの出力は、セレクタ２５に出力される。セレクタ２５は、選択信号S3に応じていずれかの一方の出力を選択し、レジスタ２６に出力する。

【００２９】
一方、直列動作モードSMでラウンド関数演算を行う場合は、２つのラウンド関数演算回路２７ａと２７ｂの動作順序によって２通りの場合がある。第１の場合は、一つのサイクルにおいて、ラウンド関数演算回路２７ａを先に演算を行い、引き続き、その結果をラウンド関数演算回路２７ｂが行う場合であり、第２の場合は、一つのサイクルにおいてラウンド関数演算回路２７ｂが先に演算を行い、引き続き、その結果をラウンド関数演算回路２７ａが行う場合である。
【００３０】
ラウンド関数演算回路２７ａが先に演算を行う第１の場合は、セレクタ２４ａは、レジスタ２６からの出力をラウンド関数演算回路２７ａに出力し、ラウンド関数演算回路２７ａは、レジスタ２６からの出力に対して暗号処理を行う。その結果はセレクタ２４ｂにも出力されているので、セレクタ２４ｂは、選択信号S2に応じてラウンド関数演算回路２７ａからの出力をラウンド関数演算回路２７ｂに供給する。ラウンド関数演算回路２７ｂは、ラウンド関数演算回路２７ａからの出力に対して暗号処理を行い、結果をセレクタ２５に出力する。セレクタ２５には、ラウンド関数演算回路２７ａからの出力とラウンド関数演算回路２７ｂからの出力が入力されている。セレクタ２５は、選択信号S3に応じて、ラウンド関数演算回路２７ｂからの出力を選択し、レジスタ２６に出力する。レジスタ２６は、セレクタ２５から出力された結果を保持する。
【００３１】
ラウンド関数演算回路２７ｂが先に演算を行う第２の場合は、セレクタ２４ｂは、レジスタ２６からの出力をラウンド関数演算回路２７ｂに出力し、ラウンド関数演算回路２７ｂは、レジスタ２６からの出力に対して暗号処理を行う。その結果はセレクタ２４ａにも出力されているので、セレクタ２４ａは、選択信号S1に応じてラウンド関数演算回路２７ｂからの出力をラウンド関数演算回路２７ａに供給する。ラウンド関数演算回路２７ａは、ラウンド関数演算回路２７ｂからの出力に対して暗号処理を行い、結果をセレクタ２５に出力する。セレクタ２５には、ラウンド関数演算回路２７ｂからの出力とラウンド関数演算回路２７ａからの出力が入力されている。セレクタ２５は、選択信号S3に応じて、ラウンド関数演算回路２７ａからの出力を選択し、レジスタ２６に出力する。
【００３２】
制御回路３０は、乱数発生回路１８からの乱数に基づいて、暗号処理回路の動作モードを、並列動作モードPMと直列動作モードSMの間で切り替える切り替え制御部を構成する。
【００３３】
制御回路３０は、ラウンドの状態を管理しながら、鍵スケジューラ２８に対して制御信号CSを出力する。制御信号CSは、ラウンドの情報を示すデータを含む。すなわち、鍵スケジューラ２８は、制御回路２８からの制御信号CSに基づいて、ラウンドの状態に応じたラウンド鍵を、２つの出力端子から出力する。
並列動作モードPMの場合は、鍵スケジューラ２８は、同じデータを２つの出力端子２８ａ、２８ｂから出力し、直列動作モードSMの場合は、異なるデータを２つの出力端子２８ａ、２８ｂから出力する。特に、鍵スケジューラ２８は、直列動作モードSMの場合、第１の場合と第２の場合に応じて、２つのラウンド関数演算回路のそれぞれに対応するラウンド鍵を出力する。
例えば、第３ラウンドが並列動作モードPMで実行されるとき、第３のラウンド鍵の鍵データが、鍵スケジューラ２８の２つの出力端子２８ａ、２８ｂから出力される。第４と第５ラウンドが直列動作モードSMで実行されるときは、第４のラウンド鍵の鍵データが、第４ラウンドの暗号演算を実行するラウンド関数演算回路へ鍵スケジューラ２８の一方の出力端子から出力され、第５のラウンド鍵の鍵データが、第５ラウンドの暗号演算を実行するラウンド関数演算回路へ鍵スケジューラ２８の他方の出力端子から出力される。
【００３４】
図３は、本実施の形態における並列動作モードPMと直列動作モードSMの切り替えによる演算状況の例を説明するための図である。

【００３５】
上述した図２に示す暗号回路モジュール１５によれば、並列動作モードPMと直列動作モードSMが乱数RNに基づいてランダムに実行される。言い換えれば、暗号処理回路の動作モードが、並列動作モードPM又は直列動作モードSMにランダムに変化する。例えば、図３の（ａ）に示す例では、最初のサイクルでは直列動作モードSMで第１と第２ラウンドが実行され、次のサイクルでは並列動作モードPMで第３ラウンドが実行され、その次のサイクルも並列動作モードPMで第４ラウンドが実行され、その次のサイクルでは直列動作モードSMで第５と第６ラウンドが実行されている。そして、最後から１つ前のサイクルでは第１４ラウンドは並列動作モードPMで実行され、最後のサイクルでは第１５と第１６ラウンドが直列動作モードSMで実行されて、暗号処理が終了している。
【００３６】
並列動作モードPMと直列動作モードSMは乱数RNに基づいてランダムに実行されるので、全てのサイクルが直列動作モードSMである場合（図３の（ｂ）の場合）もあり得るし、全てのサイクルが並列動作モードPMである場合（図３の（ｃ）の場合）もあり得る。しかし、通常は、全てのサイクルが直列動作モードSMとなる確率（図３の（ｂ）の場合）あるいは全てのサイクルが並列動作モードPMとなる確率（図３の（ｃ）の場合）は低く、並列動作モードPMと直列動作モードSMがランダムに混在する。
【００３７】
従って、通常は、全体の暗号処理時間Tspは、全てのサイクルにおいて直列動作モードSMが実行される図３の（ｂ）の場合の時間Tsよりも長く、全てのサイクルにおいて並列動作モードPMが実行される図３の（ｃ）の場合の時間Tpよりも短くなる。
【００３８】
さらに、ランダムに並列動作モードPMと直列動作モードSMがランダムに切り替わりながら実行されるため、電力解析攻撃への耐性も確保されている。また、２つの動作モードがランダムに組み合わされるので、暗号処理に要する全体の処理時間が変化するため、電力解析のタイミングを合わせることが困難になるので、その点においても電力解析攻撃への耐性は高い。
【００３９】
以上のように、本実施の形態に係る暗号処理装置によれば、電力解析攻撃に対する耐性を確保しつつ、処理時間を短くできる暗号処理装置を提供することができる。
次に、上述した実施の形態に係る暗号処理装置の変形例について説明する。上述した実施の形態に係る暗号処理装置を、以下に説明するように一部変更あるいは追加してもよい。
【００４０】
（変形例１）
本変形例に係る暗号処理装置は、２つの動作モードの実行サイクルの間にダミーのラウンド鍵を用いた暗号演算すなわちダミー演算をランダムに挿入するように構成される。
図４は、本変形例に係る暗号処理装置の暗号回路モジュール１５Aの構成例を示すブロック図である。図２と同じ構成要素については同じ符号を付し説明は省略する。
【００４１】
図４では、鍵スケジューラ２８Aには、乱数発生回路１８からの乱数RN1が入力される。鍵スケジューラ２８Aは、入力された乱数RN1に応じて、直列動作モードSM時に、ダミーのラウンド鍵を生成して出力するダミー生成部２８ｃを含む。なお、乱数RN1は、上述した乱数RNと同じものでもよいし、異なるものでもよい。
【００４２】
DESやAES等のアルゴリズムの特徴として、同じ鍵を用いて暗号化のためのラウンド処理と復号化のためのラウンド処理を行うと、データが元に戻る（すなわち出力データが入力データと同じになる）という性質がある。従って、この性質を利用して、ランダムに発生する直列動作モードSM時に、乱数RN1に基づいて生成されたラウンド鍵を用いて、２つのラウンド関数演算回路はラウンド演算を実行するダミー演算のサイクルを実行する。さら

に、ダミー生成部２８ｃがダミーのラウンド鍵を出力するタイミング（すなわちダミー演算サイクルの挿入されるタイミング）も、乱数RN1に基づいて決定される。

【００４３】

図５は、本変形例における並列動作モードPMと直列動作モードSMの切り替えによる演算状況の例を説明するための図である。

上述した図４に示す暗号回路モジュール１５Aによれば、並列動作モードPMと直列動作モードSMが乱数RNに基づいて混在しながらランダムに実行され、かつダミー演算サイクルが乱数RN1に基づいてランダムに挿入される。例えば、図５の（ａ）に示す例では、最初に直列動作モードSMで第１と第２ラウンドが実行され、次に並列動作モードPMで第３ラウンドが実行され、その次では、直列動作モードSMでダミー演算が実行され、その次では直列動作モードSMで第４と第５ラウンドが実行されている。そして、第１４ラウンドの後にダミー演算が実行され、最後に第１５と第１６ラウンドが直列動作モードSMで実行されて、暗号処理が終了している。

【００４４】

以上のように、並列動作モードPMと直列動作モードSMが乱数RNに基づいて混在しながらランダムに実行されるだけでなく、さらにダミー演算サイクルが乱数に基づいてランダムに挿入されるので、電力解析攻撃に対して上述した実施の形態の場合よりも、より高い耐性を確保しつつ、処理時間を短くできる暗号処理装置を実現することができる。

【００４５】

さらに、暗号演算処理の最初と最後の部分の少なくとも一方には１以上のダミー演算サイクルを必ず追加するようにしてもよい。これは、電力解析は、特に、最初と最後、ここでは第１と第１６ラウンドの実行時に対して行われることが多いからである。

【００４６】

図５の（ｂ）では、暗号演算処理の最初の部分（すなわち第１ラウンドの前の部分）FPに、１以上のダミー演算サイクルが追加されている例が示されている。図５の（ｂ）では、最初の部分FPには、２つのダミー演算サイクルが追加されているが、追加されるダミー演算サイクルの数は、乱数RN1に基づいて決定される。

【００４７】

さらに、図５の（ｂ）では、暗号演算処理の最後の部分（すなわち第１６ラウンドの後の部分）LPに、ダミー演算サイクルが追加されている例を示す。図５の（ｂ）では、最後の部分LPには、１つのダミー演算サイクルが追加されているが、追加されるダミー演算サイクルの数は、乱数RN1に基づいて決定される。

【００４８】

このように、最初と最後の両部分には必ず、あるいは最初と最後の部分の少なくとも一方には、１以上のダミー演算サイクルが追加される。その追加されるダミー演算サイクルの数は、ランダムに決定される。

【００４９】

以上のように、並列動作モードPMと直列動作モードSMの実行サイクルの間へのダミー演算の挿入と、暗号演算処理の最初と最後の部分へのダミー演算の追加を行うことにより、より高い耐性を確保しつつ、処理時間を短くできる暗号処理装置を実現することができる。

【００５０】

なお、ダミー演算の挿入と追加の一方だけを行うようにしても、より高い耐性を確保しつつ、処理時間を短くできる暗号処理装置を実現することができる。

【００５１】

（変形例２）

本変形例に係る暗号処理装置は、ラウンド関数演算にマスクデータを利用して暗号処理を実行するように構成される。

本変形例は、上述した実施の形態あるいは変形例１に係る暗号処理装置において、データマスキング法による暗号処理が適用されて、具体的には、各ラウンド関数演算回路にマ

スクデータが入力され、マスクデータを用いてデータマスキングを行いながら、暗号処理が実行される例である。

【００５２】

図２あるいは図４において、点線で示すように、ラウンド関数演算回路２７ａと２７ｂにマスクデータMが入力される。マスクデータMは、乱数発生回路１８から出力される乱数を用いて生成される。なお、マスクデータMを生成するために用いられる乱数は、上述した乱数RNと同じものでもよいし、異なるものでもよい。

【００５３】

データマスキング法は、特開２０００－６６５８５号（特許第３６００４５４号）公報に示されるような方法を用いることができる。その場合、該公報に示されるような方法とは異なり、第一の暗号演算回路は、第一のマスクパターンのみを用いて暗号演算を行い、第二の暗号演算回路は、第二のマスクパターンのみを用いて暗号演算を行うような回路構成とすることができる。そして、直列動作モードでは、上記公報に記載の方法よりも高速に暗号処理を行うことが可能となり、並列動作モードでは、上記公報に記載の方法と同じ処理速度となる。

【００５４】

本変形例によれば、上述した実施の形態あるいは変形例１に係る暗号処理装置において、データマスキングによる耐性の向上も追加されるので、電力解析攻撃に対して、より高い耐性が確保できる。

【００５５】

なお、上述した実施の形態及び２つの変形例に係る暗号処理装置は、DESのラウンド関数を用いた暗号処理装置であるが、暗号処理方式としてはDESに限らず、他の方式を用いてもよい。

例えば、暗号処理方式としてAES（Advanced Encryption Standard）を用いることができる。DESの場合は、暗号用と復号用で同じ演算回路を用いるが、AESの場合は、２つの暗号演算回路のそれぞれに、暗号用と復号用の２つの演算回路が含まれ、２つの演算回路が切り替えられて実行されるように構成される。その場合は、制御回路３０から暗号用と復号用のいずれの演算回路を用いるかを指示する信号が制御信号に含まれる。上述した変形例１におけるダミーのラウンド鍵を用いる場合は、２つの演算回路の一方を暗号用とし、他方を復号用として、それぞれに異なるラウンド鍵を供給するように、制御回路３０は、２つのラウンド関数演算回路２７ａ、２７ｂと鍵スケジューラ２８Aを制御する。

【００５６】

さらになお、上述した実施の形態及び２つの変形例に係る暗号処理装置では、暗号用の演算回路が２つ（具体的には、ラウンド関数演算回路２７ａと２７ｂ）ある例であるが、３つ以上あってもよい。

【００５７】

また、上述した実施の形態及び各変形例では、各暗号処理装置として、ICカードの例を挙げて説明したが、他の機器でもよい。

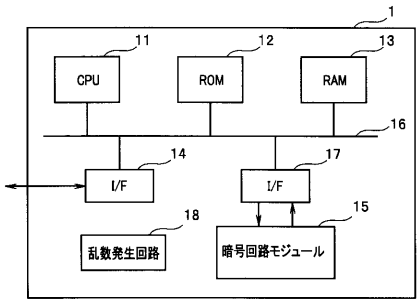
本発明は、上述した実施の形態に限定されるものではなく、本発明の要旨を変えない範囲において、種々の変更、改変等が可能である。

【符号の説明】

【００５８】

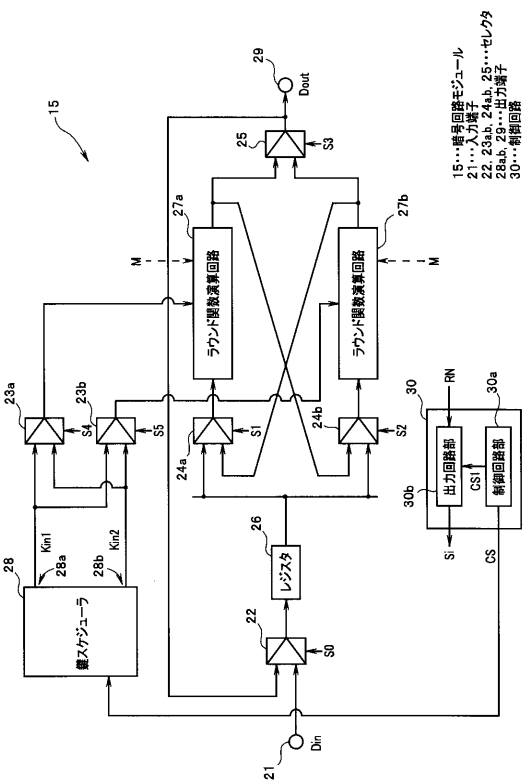
１　暗号処理装置、１５　暗号回路モジュール、１６　バス、２１　入力端子、２２，２３ａ，２３ｂ，２４ａ、２４ｂ、２５　セレクタ、２８ｃ　ダミー生成部、３０　制御回路

【図１】



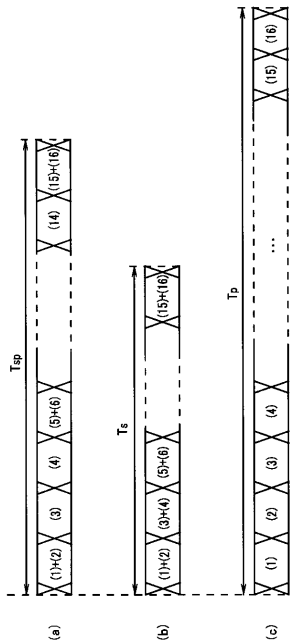
1…暗号処理装置
16…バス

【図２】

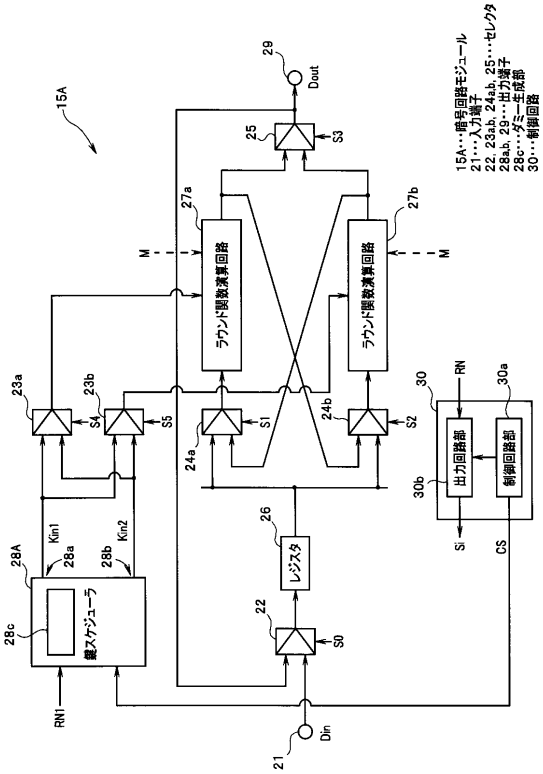


15…暗号回路モジュール
21…入力端子
22, 23a,b, 24a,b, 25…セレクタ
28a,b, 29…出力端子
30…制御回路

【図３】



【図４】



15A…暗号回路モジュール
21…入力端子
22, 23a,b, 24a,b, 25…セレクタ
28a,b, 29…出力端子
28c…ダミー生成部
30…制御回路

【図５】