

(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2007-251483

(P2007-251483A)

(43) 公開日 平成19年9月27日(2007.9.27)

(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 3 O L (全 8 頁)

(21) 出願番号 特願2006-70670 (P2006-70670)  
 (22) 出願日 平成18年3月15日 (2006.3.15)

(71) 出願人 501285133  
 川崎マイクロエレクトロニクス株式会社  
 千葉県千葉市美浜区中瀬一丁目3番地  
 (74) 代理人 100080159  
 弁理士 渡辺 望穂  
 (74) 代理人 100090217  
 弁理士 三和 晴子  
 (72) 発明者 渡部 智宏  
 千葉県千葉市美浜区中瀬一丁目三番地 川崎マイクロエレクトロニクス株式会社幕張本社内  
 Fターム(参考) 5J104 AA32 AA44 AA47 NA07 NA27  
 NA39 NA42

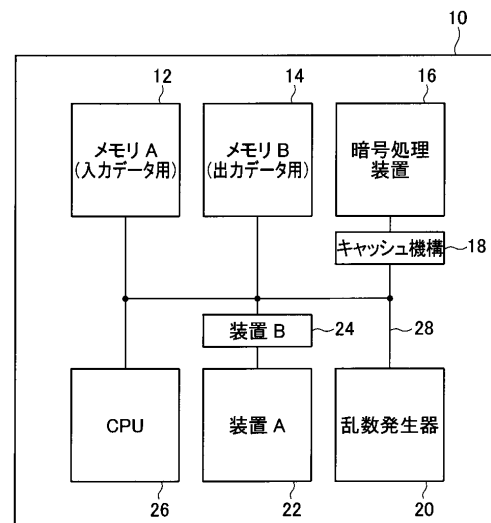
(54) 【発明の名称】 暗号化装置

(57) 【要約】

【課題】DESやAESなどの暗号アルゴリズムの攻撃法の1つであるDPAに対して耐性を有する暗号化装置を提供する。

【解決手段】本発明の暗号化装置は、第1および第2のメモリ(メモリAおよびメモリB)をアクセスするアドレスをランダムに入れ替えるアドレス生成装置(装置Aおよび装置B)によって生成されるアドレスに基づいて、第1のメモリから入力データを読み出してキャッシュ機構に入力し、キャッシュ機構から入力データを暗号処理装置に入力し、暗号処理装置によって入力データを暗号化し、暗号処理装置から出力される出力データをキャッシュ機構に入力し、キャッシュ機構から出力データを読み出して第2のメモリに書き込むことを、全アドレスについて繰り返し行う。

【選択図】 図1



**【特許請求の範囲】****【請求項 1】**

入力データを暗号化し、暗号化後の出力データを出力する暗号処理装置と、  
前記暗号処理装置によって暗号化されていない入力データが入力された場合、該入力データを前記暗号処理装置に入力して、前記入力データと前記暗号処理装置から入力される出力データとを対応付けて保持し、前記暗号処理装置によって既に暗号化されている入力データが入力された場合、該入力データを前記暗号処理装置に入力せず、既に保持されている出力データを出力するキャッシュ機構と、  
乱数データを発生する乱数発生器と、  
前記キャッシュ機構に入力される入力データを格納し、該入力データが所定ワード数よりも少ない場合、不足分の前記入力データのダミーデータとして、前記乱数発生器によって発生された乱数データを格納する第 1 のメモリと、  
前記キャッシュ機構から出力される出力データを格納する第 2 のメモリと、  
前記乱数発生器から入力された乱数データに基づいて、前記第 1 および第 2 のメモリの全アドレスにわたって、該第 1 および第 2 のメモリをアクセスするアドレスをランダムに入れ替える処理を行うアドレス生成装置とを備え、  
前記アドレス生成装置によって生成されるアドレスに基づいて、前記第 1 のメモリから入力データを読み出して前記キャッシュ機構に入力し、該キャッシュ機構から入力データを前記暗号処理装置に入力し、該暗号処理装置によって入力データを暗号化し、前記暗号処理装置から出力される出力データを前記キャッシュ機構に入力し、該キャッシュ機構から出力データを読み出して前記第 2 のメモリに書き込む暗号化処理を、前記全アドレスについて繰り返し行うことを特徴とする暗号化装置。

**【請求項 2】**

前記キャッシュ機構は、前記アドレス生成装置から入力されるアドレスと前記入力データの個数とを比較して、前記入力データがダミーデータであると判断した場合、当該入力データと、これに対応する出力データを保持しないことを特徴とする請求項 1 に記載の暗号化装置。

**【請求項 3】**

前記入力データが所定ワード数よりも多い場合、全ての前記入力データを、所定ワード数の前記入力データからなる複数のブロックに分け、各々の前記ブロックを単位として、上記暗号化処理を繰り返し行うことを特徴とする請求項 1 または 2 に記載の暗号化装置。

**【発明の詳細な説明】****【技術分野】****【0001】**

本発明は、DES (Data Encryption Standard) や AES (Advanced Encryption Standard) などの標準的な暗号アルゴリズムの攻撃法の 1 つである差分電力解析 (DPA: Differential Power Analysis) に対して耐性を有する暗号化装置に関するものである。

**【背景技術】****【0002】**

従来、上記の DES や AES などの標準的な暗号アルゴリズムに対する攻撃法の 1 つとして、例えば非特許文献 1 に開示されているように、DPA と呼ばれる暗号解析法が知られている。

**【0003】**

DPA は、暗号処理装置により生成される暗号文と、この暗号文を生成する際の暗号処理装置における消費電力とを組にしたデータを数千組サンプルし、そのデータに基づいた統計処理を行うことによって暗号鍵を解析するものであり、対策が非常に困難な攻撃である。DPA では、上記の統計処理を行う際に、暗号処理装置の出力である暗号文から、暗号処理装置内に現れる内部データを推定する。

**【0004】**

これを回避するための従来技術としては、特許文献 1 に開示されている "Masking Metho

d”（固定マスク値法）や、非特許文献2に開示されている“Duplication Method”などが有名である。また、DPAを回避するための従来技術として、特許文献2に開示されているように、暗号化を行う度に内部回路を変更し、消費電力の統計的解析を困難にする方策などが知られている。

【0005】

【特許文献1】特開2002-366029号公報

【特許文献2】特開平13-268071号公報

【非特許文献1】Paul Kocher, Joshua Jaffe, Benjamin Jun, “Differential Power Analysis”、[online]、Cryptography Research, Inc.、[平成18年2月27日検索]、インターネット<URL : <http://www.cryptography.com/resources/whitepapers/DPA.pdf>>

10

【非特許文献2】“耐タンパー性に関する標準化調査研究開発 実証実験 報告書 第二部”、p54~78、“第3章 3.3 GoubinらによるDPA対策のソフトウェア実装”、[online]、平成16年3月、財団法人 日本規格協会、情報技術標準化研究センター、株式会社 東芝、[平成18年2月27日検索]、インターネット<URL : [http://www.jisa.or.jp/domestic/instac/committe/H15report/report-contents/01\\_06\\_02.PDF](http://www.jisa.or.jp/domestic/instac/committe/H15report/report-contents/01_06_02.PDF)>

【発明の開示】

【発明が解決しようとする課題】

【0006】

しかしながら、特許文献1の“Masking Method”や、非特許文献2の“Duplication Method”は、暗号処理装置が実装している暗号アルゴリズムを熟知していなければ実装できない。特に、“Duplication Method”については、暗号アルゴリズムによっては実装手段があるかどうかとも保証できない。また、両技術ともに既存の暗号処理装置の内部を変更しないと該技術を実装できず、既存の資産を有効に利用できない。

20

【0007】

また、特許文献2に関しては、回路の書き替えに時間がかかるため、結果として暗号化処理に要する時間が非常に長くなり、実用的であるとは言えない。

【0008】

本発明の目的は、前記従来技術に基づく問題点を解消し、DESやAESなどの暗号アルゴリズムの攻撃法の1つであるDPAに対して耐性を有する暗号化装置を提供することにある。

30

【課題を解決するための手段】

【0009】

上記目的を達成するために、本発明は、入力データを暗号化し、暗号化後の出力データを出力する暗号処理装置と、

前記暗号処理装置によって暗号化されていない入力データが入力された場合、該入力データを前記暗号処理装置に入力して、前記入力データと前記暗号処理装置から入力される出力データとを対応付けて保持し、前記暗号処理装置によって既に暗号化されている入力データが入力された場合、該入力データを前記暗号処理装置に入力せず、既に保持されている出力データを出力するキャッシュ機構と、

乱数データを発生する乱数発生器と、

40

前記キャッシュ機構に入力される入力データを格納し、該入力データが所定ワード数よりも少ない場合、不足分の前記入力データのダミーデータとして、前記乱数発生器によって発生された乱数データを格納する第1のメモリと、

前記キャッシュ機構から出力される出力データを格納する第2のメモリと、

前記乱数発生器から入力された乱数データに基づいて、前記第1および第2のメモリの全アドレスにわたって、該第1および第2のメモリをアクセスするアドレスをランダムに入れ替える処理を行うアドレス生成装置とを備え、

前記アドレス生成装置によって生成されるアドレスに基づいて、前記第1のメモリから入力データを読み出して前記キャッシュ機構に入力し、該キャッシュ機構から入力データを前記暗号処理装置に入力し、該暗号処理装置によって入力データを暗号化し、前記暗号

50

処理装置から出力される出力データを前記キャッシュ機構に入力し、該キャッシュ機構から出力データを読み出して前記第2のメモリに書き込む暗号化処理を、前記全アドレスについて繰り返し行うことを特徴とする暗号化装置を提供するものである。

【0010】

ここで、前記キャッシュ機構は、前記アドレス生成装置から入力されるアドレスと前記入力データの個数とを比較して、前記入力データがダミーデータであると判断した場合、当該入力データと、これに対応する出力データを保持しないことが好ましい。

【0011】

また、前記入力データが所定ワード数よりも多い場合、全ての前記入力データを、所定ワード数の前記入力データからなる複数のブロックに分け、各々の前記ブロックを単位として、上記暗号化処理を繰り返し行うことが好ましい。

10

【発明の効果】

【0012】

本発明によれば、暗号処理装置の暗号アルゴリズムを知らなくても、DPAの対策が可能である。また、既存の暗号処理装置の内部を変更する必要がないため、これまでの設計資産を有効に活用することができる。また、回路の書き替えが不要なため、ある一定以上の数のまとまった入力データを暗号化処理する場合は、処理時間を増加させることなくDPA対策が可能である。

【発明を実施するための最良の形態】

【0013】

以下に、添付の図面に示す好適実施形態に基づいて、本発明の暗号化装置を詳細に説明する。

20

【0014】

図1は、本発明の暗号化装置の構成を表す一実施形態のブロック概略図である。同図に示す暗号化装置10は、第1のメモリ(メモリA)12と、第2のメモリ(メモリB)14と、暗号処理装置16と、キャッシュ機構18と、乱数発生器20と、第1の装置(装置A)22と、第2の装置(装置B)24と、制御装置(CPU:中央処理装置)26とによって構成されている。

【0015】

第1のメモリ12は、キャッシュ機構18に入力される暗号化前の入力データを格納する半導体記憶装置である。また、第2のメモリ14は、キャッシュ機構18から出力される暗号化後の出力データを格納する半導体記憶装置である。本実施形態では、第1のメモリ12に格納される暗号化処理対象の入力データ数(入力データのワード数)をNとし、第1および第2のメモリ12, 14に格納可能な最大データ数(格納可能な最大ワード数)を $N' = 1024$ とする( $N < N'$ )。

30

【0016】

続いて、暗号処理装置16は、DESやAESなどの標準的な暗号アルゴリズムに基づいて、キャッシュ機構18から入力される入力データを暗号化し、暗号化後の出力データをキャッシュ機構18に出力する。

【0017】

キャッシュ機構(キャッシュメモリおよびキャッシュコントローラを含む)18は、暗号処理装置16が何度も繰り返して同一値の入力データを暗号化しないように、暗号処理装置16によって入力データを暗号化した時に、第1のメモリ12から入力される入力データと、暗号処理装置16から入力される出力データ(入力データに対応する出力データ)とを対応付けて保持する。

40

【0018】

ここで、キャッシュ機構18を設けていないと、入力データに同一値が含まれる場合に、攻撃者に後述する順序の入れ替え方に関する手掛かりを与える可能性がある。すなわち、暗号文(本暗号化装置10の出力)に同一値が含まれていた場合、電力消費パターンが似ているN箇所のタイミングを見つければ、そのタイミングで、そのデータが処理されて

50

いたことを知られてしまう。

【0019】

言い換えると、キャッシュ機構18を設けることによって、攻撃者に、順序の入れ替え方に関する手掛かりを与えることを防止することができる。また、キャッシュ機構18を設けることによって、暗号処理装置16が何度も繰り返して同一値の入力データを暗号化するのを防止することができる。また、キャッシュ機構18を設けることによって、処理時間を短縮する効果も得られる。

【0020】

乱数発生器20は、乱数データRを発生する。第1のメモリ12に格納される入力データ数Nが、最大データ数N' (= 1024) よりも少ない場合、その不足分の(N' - N)個(ワード)の入力データのダミーデータとして、乱数データRが第1のメモリ12に格納される。また、乱数データRは、後述するように、第2の装置24が、第1の装置22によって生成されたアドレスを変換する時にも使用される。

10

【0021】

第1の装置22は、第1のメモリ12から入力データを読み出し、第2のメモリ14に出力データを書き込む時に使用するアドレスADR1を生成する、キャッシュ機構18に入力データを書き込む、キャッシュ機構18に暗号化開始コマンドを発行する、キャッシュ機構18から出力データを読み出す、などの処理を行う。第1の装置22は、第1のメモリ12をアドレスの昇順、すなわち、0番地~1023番地の順にアクセスする。

【0022】

なお、第1の装置22が、第1のメモリ12をアドレスの降順、すなわち、1023番地~0番地の順にアクセスするように構成しても良い。

20

【0023】

第2の装置24は、乱数発生器20から入力される乱数データRに基づいて、第1の装置22から入力されるアドレスADR1をアドレスADR2に変換する。言い換えると、第2の装置24は、アドレスADR1が0~1023まで変化する時に、その順序を入れ替える処理を行う。すなわち、アドレスADR2は、アドレスADR1が0~1023まで変化した時に、その順序は異なるが、全アドレス0~1023を1つずつ含む。

【0024】

これら第1および第2の装置22, 24は、本発明のアドレス生成装置を構成する。本発明に関わるアドレス生成装置は、乱数発生器から入力された乱数データに基づいて、第1および第2のメモリの全アドレスにわたって、第1および第2のメモリをアクセス(読み出しおよび書き込み)するアドレスをランダムに入れ替える処理を行うものであれば、その具体的な構成は何ら限定されない。

30

【0025】

制御装置26は、第1のメモリ12にN個の入力データを書き込む、乱数発生器20から(N' - N)個の乱数データRを読み出して、第1のメモリ12に入力データのダミーデータとして書き込む、乱数発生器20から1個の乱数データRを読み出して、第2の装置24に入力する、第1の装置22に暗号化処理の開始を指示する、などの暗号化装置10全体の動作制御を行う。

40

【0026】

第1および第2のメモリ12, 14、キャッシュ機構18、乱数発生器20、第2の装置24、制御装置26は、システムバス28を介して相互に接続されている。また、第1の装置22は第2の装置24に接続され、第2の装置24を介してシステムバス28と接続されている。同様に、暗号処理装置16はキャッシュ機構18に接続され、キャッシュ機構18を介してシステムバス28と接続されている。

【0027】

次に、暗号化装置10の動作を説明する。

【0028】

暗号化処理を行う場合、制御装置26が、暗号化処理対象となるN個の入力データを、

50

アドレス0から昇順に第1のメモリ12に書き込む。すなわち、第1のメモリ12には、そのアドレス0～(N-1)番地まで入力データが書き込まれる。

【0029】

ここで、 $N < N'$  ( $N' = 1024$ )である場合、制御装置26が、乱数発生器20から( $N' - N$ )個の乱数データRを読み出し、読み出した乱数データRを、入力データのダミーデータとして、アドレスN番地から昇順にアドレス( $N' - 1$ )番地まで第1のメモリ12に書き込む。すなわち、第1のメモリ12には、その最大データ数 $N'$ 個の入力データ(ダミーデータを含む)が書き込まれる。

【0030】

続いて、制御装置26が、乱数発生器20から1個の乱数データRを読み出し、これを第2の装置24に書き込む。また、制御装置26は、最大データ数 $N'$ を、第1および第2の装置22, 24に書き込み、入力データ数Nを、キャッシュ機構18に書き込む。

10

【0031】

なお、第2の装置24に書き込む乱数データRの個数は1個に限らず、2個以上の乱数データRを書き込んでも良い。この場合、複数の乱数データRを順次入れ替えて使用したり、複数の乱数データRを組み合わせて使用するなど、どのように使用しても良い。

【0032】

その後、制御装置26は、第1の装置22に処理開始コマンドを発行する。これに応じて、第1の装置22は、内部変数であるアドレスADR1を0に初期化し、このアドレスADR1を第2の装置24に出力する。

20

【0033】

第2の装置24は、第1の装置22からアドレスADR1を受け取ると、制御装置26から書き込まれた乱数データRに基づいて、アドレスADR1をアドレスADR2に変換する。前述の通り、アドレスADR2は、アドレスADR1が0～1023まで変化した時に、0～1023の値を1つずつ含む(アドレスADR1の順序を入れ替える)。第2の装置24から出力されるアドレスADR2は、第1および第2のメモリ12, 14、ならびに、キャッシュ機構18に入力される。

【0034】

続いて、第1の装置22から第1のメモリ12に入力データの読み出しコマンドが発行され、第1のメモリ12から、そのアドレスADR2に格納されている入力データが読み出される。その後、第1の装置22によって、第1のメモリ12から読み出された入力データがキャッシュ機構18に入力され、さらに、第1の装置22からキャッシュ機構18に暗号化開始コマンドが発行される。

30

【0035】

キャッシュ機構18は、暗号処理装置16によって暗号化されていない入力データが入力された場合、入力データを暗号処理装置16に入力して、この入力データと暗号処理装置16から入力される出力データ(入力データに対応する出力データ)とを対応付けて保持する。一方、暗号処理装置16によって既に暗号化されている入力データが入力された場合、その入力データを暗号処理装置16に入力せず、既に保持されている出力データ(入力データに対応する出力データ)を出力する。

40

【0036】

なお、キャッシュ機構18は、アドレスADR2と暗号化処理対象の入力データの個数Nとを比較して、入力データがダミーデータであると判断した場合(すなわち、アドレスADR2 = Nの場合)、この入力データと、これに対応する出力データを保持しない。その理由は、ダミーデータを暗号化した出力データは、暗号化装置10から出力される暗号文として使用されないからであるが、処理時間を短縮する目的から、ダミーデータとその出力データを保持する構成としても良い。

【0037】

続いて、第1の装置22からキャッシュ機構18に出力データの読み出しコマンドが発行され、キャッシュ機構18から、入力データに対応する出力データが読み出される。そ

50

の後、第1の装置22によって、キャッシュ機構18から読み出された出力データが第2のメモリ14に入力され、さらに、第1の装置22から第2のメモリ14に出力データの書き込みコマンドが発行される。

【0038】

第2のメモリ14には、前述の通り、第2の装置24から出力されるアドレスADR2が入力されている。従って、第2のメモリ14のアドレスADR2に出力データが書き込まれる。すなわち、第1のメモリ12の各々のアドレスに格納されている入力データが、暗号処理装置16によって暗号化されて得られる出力データは、第2のメモリ14の同一アドレスに格納される。

【0039】

続いて、第1の装置22において、アドレスADR1が1つ増加される ( $ADR1 = ADR1 + 1$ )。これ以降は、アドレスADR1が、第1および第2の最大データ数  $N' - 1$  である1023になるまで、上記暗号化処理が繰り返し行われる。

【0040】

なお、入力データ数Nが1024よりも多い場合、全入力データ数Nを1024の入力データからなる複数のブロックに分け、各々のブロックを単位として、上記暗号化処理が繰り返し行われる。

【0041】

暗号化装置10では、第1および第2の装置22, 24 (アドレス生成装置) によって、暗号化処理対象の入力データ群が、その処理順序を入れ替えられ、暗号処理装置16によって順次暗号化される。なお、同一値を持つ入力データの暗号処理に関しては、その処理順序を入れ替えても効果がないため、暗号化装置10は、2回以上同じ入力データが暗号処理されないようにキャッシュ機構18を備えている。

【0042】

また、暗号化処理対象のデータ数が少ない場合でも安全性を確保できるように、ある一定数 (所定ワード数) 未満の入力データを暗号化する際には、処理対象の入力データ群にダミーデータを挿入し、十分な数の入力データに対して入れ替え処理を行うことができる。なお、入力データのワード数を多くするに従って安全性は高くなるが、処理時間が増大するので、安全性のレベルを考慮して適宜決定するのが好ましい。

【0043】

以上説明したように、暗号化装置10では、暗号処理装置の暗号アルゴリズムを知らなくても、DPAの対策が可能である。また、既存の暗号処理装置の内部を変更する必要がないため、これまでの設計資産を有効に活用することができる。また、回路の書き換えが不要なため、ある一定以上の数のまとまった入力データを暗号化処理する場合は、処理時間を増加させることなくDPA対策が可能である。

【0044】

なお、第1および第2のメモリ12, 14、暗号処理装置16、キャッシュ機構18、乱数発生器20、第1および第2の装置 (アドレス生成装置) 22, 24、制御装置26の具体的な構成は何ら限定されず、同様の機能を果たす各種構成のものがいずれも利用可能である。また、第1および第2のメモリ12, 14は、1つの半導体記憶装置で構成することも可能である。

【0045】

本発明は、基本的に以上のようなものである。

以上、本発明の暗号化装置について詳細に説明したが、本発明は上記実施形態に限定されず、本発明の主旨を逸脱しない範囲において、種々の改良や変更をしてもよいのはもちろんである。

【図面の簡単な説明】

【0046】

【図1】本発明の暗号化装置の構成を表す一実施形態のブロック概略図である。

【符号の説明】

10

20

30

40

50

## 【 0 0 4 7 】

- 1 0 暗号化装置
- 1 2 第 1 のメモリ (メモリ A)
- 1 4 第 2 のメモリ (メモリ B)
- 1 6 暗号処理装置
- 1 8 キャッシュ機構
- 2 0 乱数発生器
- 2 2 第 1 の装置 (装置 A)
- 2 4 第 2 の装置 (装置 B)
- 2 6 制御装置 (CPU : 中央処理装置)
- 2 8 システムバス

10

【 図 1 】

