(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4885458号
(P4885458)
(45)発行日　平成24年2月29日(2012.2.29)　(24)登録日　平成23年12月16日(2011.12.16)

(51)Int.Cl.　F I
H04L 9/10 (2006.01)　H04L 9/00 621Z

請求項の数 7 (全 14 頁)

(21)出願番号　特願2005-18876(P2005-18876)
(22)出願日　平成17年1月26日(2005.1.26)
(65)公開番号　特開2005-236977(P2005-236977A)
(43)公開日　平成17年9月2日(2005.9.2)
審査請求日　平成20年1月8日(2008.1.8)
(31)優先権主張番号　2004-010975
(32)優先日　平成16年2月19日(2004.2.19)
(33)優先権主張国　韓国(KR)

(73)特許権者　390019839
三星電子株式会社
Ｓａｍｓｕｎｇ　Ｅｌｅｃｔｒｏｎｉｃｓ　Ｃｏ．，Ｌｔｄ．
大韓民国京畿道水原市靈通区梅灘洞４１６
４１６，Ｍａｅｔａｎ－ｄｏｎｇ，Ｙｅｏｎｇｔｏｎｇ－ｇｕ，Ｓｕｗｏｎ－ｓｉ，Ｇｙｅｏｎｇｇｉ－ｄｏ，Ｒｅｐｕｂｌｉｃ　ｏｆ　Ｋｏｒｅａ
(74)代理人　100064908
弁理士　志賀　正武
(74)代理人　100089037
弁理士　渡邊　隆
(74)代理人　100108453
弁理士　村山　靖彦

最終頁に続く

(54)【発明の名称】電力分析攻撃に安全な基本演算装置および方法

(57)【特許請求の範囲】
【請求項１】
電力分析攻撃に安全な基本演算装置において、
ランダムデータを生成するランダムデータ発生部と、
入力データおよび前記ランダムデータを受け入れてランダムマスクデータを生成するランダムマスク部と、
前記ランダムマスクデータまたはランダムデータのみを変数として論理演算を実行し、その結果として、前記入力データに対する基本演算結果をランダムマスク形式に出力する論理演算部を含み、
前記論理演算部は、論理否定（ＮＯＴ）演算装置であり、
前記論理否定（ＮＯＴ）演算装置は、前記入力データに対する論理否定（ＮＯＴ）演算結果をランダムマスク形式に出力する処理を実行し、
前記論理否定（ＮＯＴ）演算装置は、
前記ランダムマスクデータを受け入れてＮＯＴ論理演算を実行する第１論理ゲートと、
第１および第２ランダムデータを受け入れてＸＯＲ論理演算を実行する第２論理ゲートと、
前記第１および第２論理ゲートの結果を受け入れてＸＯＲ論理演算を実行し、その結果として出力データを発生する第３論理ゲートとを含み、
前記ランダムマスク形式のデータは、前記入力データまたは前記入力データに対する演算結果に前記ランダムデータが結合した形態のデータであり、

基本演算とは、ＮＯＴ、ＡＮＤ、ＯＲ、ＮＡＮＤ、ＮＯＲ基本演算であって前記基本演算結果とは前記基本演算の結果を意味し、
前記ランダムデータ発生部は、前記第１および第２のランダムデータを発生させる
ことを特徴とする基本演算装置。
【請求項２】
前記ランダムマスクデータは、前記入力データと前記第１ランダムデータをＸＯＲ論理演算したデータである
ことを特徴とする請求項１に記載の基本演算装置。
【請求項３】
前記ランダムマスクデータと前記第１および第２ランダムデータは、各々ｎビット（ｎは自然数）の桁数で構成され、各々相応するビットの桁の間でＮＯＴ論理演算を実行する
ことを特徴とする請求項２に記載の基本演算装置。
【請求項４】
電力分析攻撃に安全な論理演算方法を請求項１乃至請求項３のいずれか一項に記載の基本演算装置に順次実行させる方法であって、
ａ）前記ランダムデータ発生部がランダムデータを生成する段階と、
ｂ）前記ランダムマスク部が入力データおよび前記ランダムデータを受け入れてランダムマスクデータを生成する段階と、
ｃ）前記論理演算部が前記ランダムマスクデータまたはランダムデータのみを変数として論理演算を実行し、その結果として前記入力データに対する基本演算結果をランダムマスク形式に出力する段階とを、前記基本演算装置に順次実行させ、
前記ランダムマスク形式のデータは、前記入力データまたは前記入力データに対する演算結果に前記ランダムデータが結合した形態のデータであり、
基本演算とは、ＮＯＴ、ＡＮＤ、ＯＲ、ＮＡＮＤ、ＮＯＲ基本演算であって前記基本演算結果とは前記基本演算の結果を意味する
ことを特徴とする基本論理演算方法。
【請求項５】
前記ｃ）段階は、論理否定（ＮＯＴ）演算段階であり、
前記論理否定（ＮＯＴ）演算段階は、前記入力データに対する論理否定（ＮＯＴ）演算結果をランダムマスク形式に出力する処理を実行する
ことを特徴とする請求項４に記載の基本論理演算方法。
【請求項６】
前記論理否定（ＮＯＴ）演算段階は、
ｄ１）前記ランダムマスクデータを受け入れてＮＯＴ論理演算を実行する段階と、
ｅ１）第１および第２ランダムデータを受け入れてＸＯＲ論理演算を実行する段階と、
ｆ１）前記第ｄ１）および第ｅ１）段階の結果を受け入れてＸＯＲ論理演算を実行し、その結果として出力データを発生する段階とを含み、
前記ランダムデータ発生部は、前記第１および第２のランダムデータを発生させる
ことを特徴とする請求項５に記載の基本論理演算方法。
【請求項７】
前記ランダムマスクデータと前記第１および第２ランダムデータは、各々ｎビット（ｎは自然数）の桁数で構成され、各々相応するビットの桁の間でＮＯＴ論理演算を実行する
ことを特徴とする請求項６に記載の基本論理演算方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は暗号化回路に関するものであり、さらに詳細には電力分析攻撃に安全な基本演算装置および方法に関するものである。
【背景技術】
【０００２】

最近暗号アルゴリズムの演算過程で発生される消費電力を測定するか、演算実行時間を測定して秘密キーのような秘密情報を見つける方法が知られた。

【０００３】

暗号アルゴリズムに対する秘密情報の漏出をサイドチャンネル(Ｓｉｄｅ Ｃｈａｎｎｅｌ)といい、サイドチャンネルを利用した攻撃方法をサイドチャンネル攻撃(Ｓｉｄｅ Ｃｈａｎｎｅｌ Ａｔｔａｃｋ)という。サイドチャンネル攻撃は大きく時間攻撃(Ｔｉｍｉｎｇ Ａｔｔａｃｋ)、欠陥注入攻撃(Ｆａｕｌｔ Ｉｎｓｅｒｔｉｏｎ Ａｔｔａｃｋ)、および電力分析攻撃(Ｐｏｗｅｒ Ａｎａｌｙｓｉｓ Ａｔｔａｃｋ)などに分けることができる。特に、暗号専用演算器(ｃｏ-ｐｒｏｃｅｓｓｏｒ)がインストールされたスマートカードシステムでサイドチャンネル攻撃に対する研究が活発に進行されている。スマートカードは秘密データに対する演算が多く行われるのでサイドチャンネルの可能性が高い。

【０００４】

電力分析攻撃は暗号アルゴリムズムの演算過程で消費電力を測定し、これを分析して秘密情報を見つける攻撃法である。この方法はＰａｕｌ Ｋｏｃｈｅｒによって提案された方法として、大きく‘Ｓｉｍｐｌｅ Ｐｏｗｅｒ Ａｎａｌｙｓｉｓ(ＳＰＡ)’と‘Ｄｉｆｆｅｒｅｎｔｉａｌ Ｐｏｗｅｒ Ａｎａｌｙｓｉｓ(ＤＰＡ)’に分けることができる。このうちでＤＰＡがＳＰＡより簡単で、強力なのでＤＰＡに対する防御法を研究することが重要である。

【０００５】

ＤＰＡに対する防御法として代表的な方法は、入力データとランダムデータを論理演算した後に、暗号アルゴリズムに入力する方法である。これをランダムマスキング(Ｒａｎｄｏｍ ｍａｓｋｉｎｇ)という。入力データをランダムマスキングすれば、同一の値が入力されてもアルゴリズム演算過程で消耗される電力が変わるので秘密情報の露出を防止することができる。ランダムマスキング方法には様々であるが、入力データとランダムデータをＸＯＲ論理演算する方法が一般的に使われる。入力データをａといい、ランダムデータをｒといえば、ランダムマスクデータは

【０００６】

【数１】

$$／a = a \oplus r$$

【０００７】

になる。（なお、上記の式で、○の中に＋が記入された記号は、以下、明細書において・XOR・と表す場合もある）

【０００８】

ＤＰＡに安全であり、同時に入力データに対する所望の演算を実行するためには暗号アルゴリズム演算過程で発生されるデータがランダムマスク形式を維持しなければならない。ここで、ランダムマスク形式のデータとは、入力データまたは入力データに対する演算結果にランダムデータが結合した形態のデータを意味する。

【０００９】

例えば、平文ａとキーｋをＸＯＲ論理演算する暗号アルゴリズムがあると仮定する。ＤＰＡを阻むために平文aをそのまま使用せず、ランダムデータｒを生成してランダムマスキングした〔数１〕を使用する。ランダムマスクデータ／ａとキーｋをＸＯＲ論理演算すれば、／ａ・XOR・k＝(ａ・XOR・ｒ)・XOR・ｋになる。ＸＯＲ論理演算は結合法則が成り立つので／ａ・XOR・ｋ＝(ａ・XOR・ｋ)・XOR・ｒになる。これは平文ａに対する情報が露出されず、同時に所望のＸＯＲ論理演算結果(ａ・XOR・ｋ)を得ることができる。また、前記ＸＯＲ論理演算過程がアルゴリズムの最終段階ではなければ、ＸＯＲ論理演算計算結果である(ａ・XOR・ｋ)が露出されてはいけず、出力値がランダムマスク形式(ａ・XOR・ｋ)・XOR・ｒを有するので、このような条件も満足している。

【００１０】

しかし、平文ａとキーｋをＡＮＤ論理演算する暗号アルゴリズムではＸＯＲ論理演算のよ

うな結果が得られない。すなわち、上の例で／ａ∧ｋ＝(ａ・XOR・ｒ)∧ｋが成り立つ。しかし、ＡＮＤ論理演算では結合法則が適用されないので、／ａ∧ｋ＝(ａ∧ｋ)・XOR・rが成り立たない。

【００１１】

したがって、結合法則が成り立たない論理演算(例えば、ＡＮＤ、ＯＲなど)が含まれているアルゴリズムではランダムマスキング方法を使用することができなくなる問題点がある。

【発明の開示】

【発明が解決しようとする課題】

【００１２】

本発明は上述の問題点を解決するために提案されたものであり、本発明の目的は電力分析攻撃に安全な基本演算装置および方法を提供することにある。

【００１３】

本発明の他の目的は結合法則が成り立たない論理演算にもランダムマスキング方法を使うことができる基本演算装置および方法を提供することにある。

【００１４】

本発明のまた他の目的は前記基本演算装置を使用して前記基本演算装置に基づいて作ることができる、より複雑な演算装置を作る方法を提供することにある。

【課題を解決するための手段】

【００１５】

本発明による基本演算装置はランダムマスク装置、ランダムデータ発生装置、および論理演算装置を基本構成とする。本発明は論理演算途中に入力データの露出を防止するためにランダムデータまたはランダムマスクデータまたはランダムマスク形式のデータのみを変数として論理演算を実行し、その結果として前記入力データに対する基本演算結果をランダムマスク形式に出力する。本発明によれば、同一のデータが入力されても消耗される電力が変わるので、電力分析攻撃に対して安全となる。

【００１６】

上述の課題を達成するために本発明による電力分析攻撃に安全な基本演算装置は、ランダムデータを生成するランダムデータ発生装置と、入力データおよび前記ランダムデータを受け入れてランダムマスクデータを生成するランダムマスク装置と、前記ランダムマスクデータまたはランダムデータまたはランダムマスク形式のデータのみを変数として論理演算を実行し、その結果として前記入力データに対する基本演算結果をランダムマスク形式に出力する論理演算装置とを含むことを特徴とする。

【００１７】

この実施形態において、前記論理演算装置は論理否定ＮＯＴ演算装置であることを特徴とする。前記論理否定ＮＯＴ演算装置は、前記ランダムマスクデータを受け入れてＮＯＴ論理演算を実行する第１論理ゲートと、第１および第２ランダムデータを受け入れてＸＯＲ論理演算を実行する第２論理ゲートと、前記第１および第２論理ゲートの結果を受け入れてＸＯＲ論理演算を実行し、その結果として出力データを発生する第３論理ゲートとを含むことを特徴とする。

【００１８】

ここで、前記ランダムマスクデータは前記入力データと前記第１ランダムデータをＸＯＲ論理演算したデータであることを特徴とする。

【００１９】

一方、前記ランダムマスクデータと前記第１および第２ランダムデータは、各々ｎビット(ｎは自然数)の桁数で構成され、各々相応するビットの桁の間でＮＯＴ論理演算を実行することが可能である。

【００２０】

この実施形態において、前記論理演算装置は論理積ＡＮＤ演算装置であることを特徴とする。前記論理積ＡＮＤ演算装置は、第１および第２ランダムマスクデータを受け入れてＡ

ＮＤ論理演算を実行する第１論理ゲートと、前記第１ランダムマスクデータおよび第２ランダムデータを受け入れてＡＮＤ論理演算を実行する第２論理ゲートと、前記第２ランダムマスクデータおよび第１ランダムデータを受け入れてＡＮＤ論理演算を実行する第３論理ゲートと、前記第１および第２ランダムデータを受け入れてＡＮＤ論理演算を実行する第４論理ゲートと、前記第２および第３論理ゲートの結果を受け入れてＸＯＲ論理演算を実行する第５論理ゲートと、前記第４および第５論理ゲートの結果を受け入れてＸＯＲ論理演算を実行する第６論理ゲートと、前記第６論理ゲートの結果および第３ランダムデータ受け入れてＸＯＲ論理演算を実行する第７論理ゲートと、前記第１および第７論理ゲートの結果を受け入れてＸＯＲ論理演算を実行し、その結果として出力データを発生する第８論理ゲートとを含むことを特徴とする。

【００２１】

ここで、前記第１ランダムマスクデータは第１入力データと前記第１ランダムデータをＸＯＲ論理演算したデータであり、前記第２ランダムマスクデータは第２入力データと前記第２ランダムデータをＸＯＲ論理演算したデータであることを特徴とする。

【００２２】

一方、前記第１および第２ランダムマスクデータと前記第１乃至第３ランダムデータは、各々ｎビット(ｎは自然数)の桁数で構成され、各々相応するビットの桁の間でＡＮＤ論理演算を実行することが可能である。

【００２３】

この実施形態において、前記論理演算装置は、論理和ＯＲ演算装置であることを特徴とする。前記論理和ＯＲ演算装置は、第１および第２ランダムマスクデータを受け入れてＯＲ論理演算を実行する第１論理ゲートと、前記第１ランダムマスクデータおよび第２ランダムデータを受け入れてＡＮＤ論理演算を実行する第２論理ゲートと、前記第２ランダムマスクデータおよび第１ランダムデータを受け入れてＡＮＤ論理演算を実行する第３論理ゲートと、前記第１および第２ランダムデータを受け入れてＯＲ論理演算を実行する第４論理ゲートと、前記第２および第３論理ゲートの結果を受け入れてＸＯＲ論理演算を実行する第５論理ゲートと、前記第４および第５論理ゲートの結果を受け入れてＸＯＲ論理演算を実行する第６論理ゲートと、前記第６論理ゲートの結果および第３ランダムデータを受け入れてＸＯＲ論理演算を実行する第７論理ゲートと、前記第１および第７論理ゲートの結果を受け入れてＸＯＲ論理演算を実行し、その結果として出力データを発生する第８論理ゲートとを含むことを特徴とする。

【００２４】

ここで、前記第１ランダムマスクデータは第１入力データと前記第１ランダムデータをＸＯＲ論理演算したデータであり、前記第２ランダムマスクデータは第２入力データと前記第２ランダムデータをＸＯＲ論理演算したデータであることを特徴とする。

【００２５】

一方、前記第１および第２ランダムマスクデータと前記第１乃至第３ランダムデータは、各々ｎビット(ｎは自然数)の桁数で構成され、各々相応するビットの桁の間でＯＲ論理演算を実行することが可能である。

【００２６】

この実施形態において、前記論理演算装置は、否定論理積ＮＡＮＤ演算装置であることを特徴とする。前記否定論理積ＮＡＮＤ演算装置は、論理積ＡＮＤ演算装置と論理否定ＮＯＴ演算装置で構成されることを特徴とする。

【００２７】

この実施形態において、前記論理演算装置は、否定論理和ＮＯＲ演算装置であることを特徴とする。前記否定論理和ＮＯＲ演算装置は、論理和ＯＲ演算装置と論理否定ＮＯＴ演算装置で構成されることを特徴とする。

【００２８】

本発明による電力分析攻撃に安全な基本演算装置の論理演算方法は、ａ)ランダムデータを生成する段階と、ｂ)入力データおよび前記ランダムデータを受け入れてランダムマス

クデータを生成する段階と、ｃ)前記ランダムマスクデータまたはランダムデータまたはランダムマスク形式のデータのみを変数として論理演算を実行し、その結果として前記入力データに対する基本演算結果をランダムマスク形式に出力する段階とを含むことを特徴とする。

【００２９】

この実施形態において、前記 c)段階は論理否定ＮＯＴ演算段階であることを特徴とする。前記論理否定ＮＯＴ演算段階は、ｄ１)前記ランダムマスクデータを受け入れてＮＯＴ論理演算を実行する段階と、ｅ１)第１および第２ランダムデータを受け入れてＸＯＲ論理演算を実行する段階と、ｆ１)前記第ｄ１)および第ｅ１)段階の結果を受け入れてＸＯＲ論理演算を実行し、その結果として出力データを発生する段階とを含むことを特徴とする。一方、前記ランダムマスクデータと前記第１および第２ランダムデータは、各々ｎビット(ｎは自然数)の桁数で構成され、各々相応するビットの桁の間でＮＯＴ論理演算を実行することが可能である。

【００３０】

この実施形態において、前記ｃ)段階は論理積ＡＮＤ演算段階であることを特徴とする。前記論理積ＡＮＤ演算段階は、ｄ２)第１および第２ランダムマスクデータを受け入れてＡＮＤ論理演算を実行する段階と、ｅ２)前記第１ランダムマスクデータおよび第２ランダムデータを受け入れてＡＮＤ論理演算を実行する段階と、ｆ２)前記第２ランダムマスクデータおよび第１ランダムデータを受け入れてＡＮＤ論理演算を実行する段階と、ｇ２)前記第１および第２ランダムデータを受け入れてＡＮＤ論理演算を実行する段階と、ｈ２)前記第２および第３論理ゲートの結果を受け入れてＸＯＲ論理演算を実行する段階と、ｉ２)前記第４および第５論理ゲートの結果を受け入れてＸＯＲ論理演算を実行する段階と、ｊ２)前記第６論理ゲートの結果および第３ランダムデータを受け入れてＸＯＲ論理演算を実行する段階と、ｋ２)前記第１および第７論理ゲートの結果を受け入れてＸＯＲ論理演算を実行し、その結果として出力データを発生する段階とを含むことを特徴とする。一方、前記第１および第２ランダムマスクデータと前記第１乃至第３ランダムデータは、各々ｎビット(ｎは自然数)の桁数で構成され、各々相応するビットの桁の間でＡＮＤ論理演算を実行することが可能である。

【００３１】

この実施形態において、前記c)段階は論理和ＯＲ演算段階であることを特徴とする。 前記論理和ＯＲ演算段階は、ｄ３)第１および第２ランダムマスクデータを受け入れてＯＲ論理演算を実行する段階と、ｅ３)前記第１ランダムマスクデータおよび第２ランダムデータを受け入れてＡＮＤ論理演算を実行する段階と、ｆ３)前記第２ランダムマスクデータおよび第１ランダムデータを受け入れてＡＮＤ論理演算を実行する段階と、ｇ３)前記第１および第２ランダムデータを受け入れてＯＲ論理演算を実行する段階と、ｈ３)前記第２および第３論理ゲートの結果を受け入れてＸＯＲ論理演算を実行する段階と、ｉ３)前記第４および第５論理ゲートの結果を受け入れてＸＯＲ論理演算を実行する段階と、ｊ３)前記第６論理ゲートの結果および第３ランダムデータを受け入れてＸＯＲ論理演算を実行する段階と、ｋ３)前記第１および第７論理ゲートの結果を受け入れてＸＯＲ論理演算を実行し、その結果として出力データを発生する段階とを含むことを特徴とする。一方、前記第１および第２ランダムマスクデータと前記第１乃至第３ランダムデータは、各々ｎビット(ｎは自然数)の桁数で構成され、各々相応するビットの桁の間でＯＲ論理演算を実行することが可能である。

【００３２】

この実施形態において、前記ｃ)段階否定論理積ＮＡＮＤ演算段階であることを特徴とする。前否定論理積ＮＡＮＤ演算段階は、論理積ＡＮＤ演算段階と論理否定ＮＯＴ演算段階で構成されることを特徴とする。

【００３３】

この実施形態において、前記ｃ)段階は否定論理和ＮＯＲ演算段階であることを特徴とする。前記否定論理和ＮＯＲ演算段階は、論理和ＯＲ演算段階と論理否定ＮＯＴ演算段階で

構成されることを特徴とする。
【発明の効果】
【００３４】
本発明による基本演算装置および方法は論理演算途中に秘密情報が露出されなくて、電力分析攻撃に安全である。また本発明による基本演算装置および方法は結合法則が成り立たないＡＮＤ、ＯＲなどの論理演算に使用されるとき、所望の演算をしながら、同時にランダムマスク形態を維持する出力データを得ることができる。したがって、基本演算(ＮＯＴ、ＡＮＤ、ＯＲなど)を基盤とするより複雑なアルゴリズムに応用することができる。
【発明を実施するための最良の形態】
【００３５】
以下、本発明が属する技術分野で通常の知識を持つ者が本発明の技術的思想を容易に実施することができるように詳細に説明するために、本発明の最も望ましい実施形態を添付の図面を参照して説明する。
【００３６】
図１は本発明による基本演算装置を示すブロック図である。図１を参照すれば、前記基本演算装置はランダムマスク装置１００、ランダムデータ発生装置２００、および論理演算装置３００を含む。前記基本演算装置は論理演算途中に入力データに対する情報が露出されないようにしながら、入力データに対する基本演算を実行してその結果をランダムマスク形式に出力する。
【００３７】
前記ランダムマスク装置１００は入力データａｉおよびランダムデータｒｉを受け入れてランダムマスクデータ(／ａ１、／ａ２、．．．　、／ａｍ)を生成する。ここで、前記　ｉ＝１～ｍ　であり、ｍは自然数である。ランダムマスクデータを作る方法は様々であるが、入力データとランダムデータをＸＯＲ論理演算する方法が代表的である。すなわち、／ａ１＝ａ１・XOR・ｒ１、／ａ２＝ａ２・XOR・ｒ２、．．．　、／ａｍ＝ａｍ・XOR・ｒｍ　である。
【００３８】
前記ランダムデータ発生装置２００はランダムデータ(ｒ１、ｒ２、．．．　、ｒｎ)を発生する。
【００３９】
前記論理演算装置３００は前記ランダムマスクデータおよびランダムデータを受け入れて論理演算を実行する。前記論理演算装置３００は論理演算を実行する論理ゲート(例えば、ＮＯＴ、ＡＮＤ、ＯＲ論理ゲートなど)で構成される。前記論理演算装置３００は論理演算途中に秘密情報の漏出を防止するために入力データａｉだけで計算、ないし表現されてはいけない。前記論理演算装置３００は前記ランダムマスクデータまたはランダムデータまたはランダムマスク形式のデータのみを変数として論理演算を実行し、その結果として前記入力データに対する基本演算結果をランダムマスク形式に出力する。
【００４０】
図２は図１に示した論理演算装置の実施形態として論理否定ＮＯＴ演算装置を示すブロック図である。前記論理否定ＮＯＴ演算装置３１０は一つのランダムマスクデータ／ａ１と二つのランダムデータｒ１、ｒ２を受け入れる。そして入力データａ１のＮＯＴ論理演算データ～ａ１をランダムマスク形式～ａ１・XOR・ｒ２に出力する。
【００４１】
図２を参照すれば、前記論理否定ＮＯＴ演算装置３１０は一つのＮＯＴ論理ゲート３１１と二つのＸＯＲ論理ゲート３１２、３１３で構成される。
【００４２】
前記ＮＯＴ論理ゲート３１１はランダムマスクデータ／ａ１を受け入れてＮＯＴ論理演算を実行して第１中間データ～／ａ１を発生する。前記第１ＸＯＲ論理ゲート３１２は第１および第２ランダムデータｒ１、ｒ２を受け入れてＸＯＲ論理演算を実行して第２中間データｒ１・XOR・ｒ２を発生する。前記第２ＸＯＲ論理ゲート３１３は前記第１および第

２中間データを受け入れてＸＯＲ論理演算を実行して出力データ～／ａ１・XOR・(ｒ１・XOR・ｒ２)を発生する。

【００４３】

【数２】

$$\sim/a1 \oplus (r1 \oplus r2) = (\sim/a1 \oplus r1) \oplus r2 = \sim a1 \oplus r2$$

【００４４】

ここで、数２は次の真理表(表１)によって証明される。

【００４５】

【表１】

a1	r1	/a1	～/a1	～/a1⊕r1	～a1
0	0	0	1	1	1
0	1	1	0	1	1
1	0	1	0	0	0
1	1	0	1	0	0

【００４６】

表１を参照すれば、(～／ａ１・XOR・ｒ１)＝～ａ１になって、前記ＮＯＴ演算装置３１０の出力データは図２に示したように(～ａ１・XOR・ｒ２)になる。

【００４７】

前記ＮＯＴ演算装置３１０は論理演算途中に入力データａ１のみで計算、ないし表現されてはいけない。前記ＮＯＴ演算装置３１０の演算順序は電力分析攻撃を阻むのに重要である。もし、図２で、～／ａ１・XOR・ｒ１・XOR・ｒ２のように～／ａ１・XOR・ｒ１を先に計算する場合には～／ａ１・XOR・ｒ１＝～ａ１になって、ａ１に対する情報が露出されることができるためである。

【００４８】

前記ＮＯＴ演算装置３１０はランダムマスクデータ／ａ１およびランダムデータｒ１、ｒ２のみを変数として論理演算を実行し、その結果として前記入力データａ１に対するＮＯＴ論理演算結果をランダムマスク形式に出力する。

【００４９】

一方、前記ランダムマスクデータと前記第１および第２ランダムデータが各々ｎビット(ｎは自然数)のデータの場合には各々同一のビット桁数の間でＮＯＴ論理演算を実行する。例えば、４ビットのランダムマスクデータ／Ａ＝（／ａ３、ａ２、ａ１、ａ０）、４ビットのランダムデータＲ１＝（ｒ３、ｒ２、ｒ１、ｒ０）、Ｒ２＝（ｓ３、ｓ２、ｓ１、ｓ０）であるとき、ＮＯＴ論理演算を実行した出力データは次のとおりである。

【００５０】

【数３】

$$\sim A1 \oplus R2 = \{(\sim a3 \oplus s3), (\sim a2 \oplus s2), (\sim a1 \oplus s1), (\sim a0 \oplus s0)\}$$

【００５１】

図３は図１に示した論理演算装置の実施形態として論理積ＡＮＤ演算装置を示すブロック図である。前記論理積ＡＮＤ演算装置３２０は二つのランダムマスクデータ／ａ１、／ａ２と３個のランダムデータｒ１、ｒ２、ｒ３を受け入れる。そして、入力データａ１、ａ２のＡＮＤ論理演算結果ａ１∧ａ２をランダムマスク形式(ａ１∧ａ２)・XOR・ｒ３に出力する。

【００５２】

図３を参照すれば、前記論理積ＡＮＤ演算装置３２０は４個のＡＮＤ論理ゲート３２１～３２４と４個のＸＯＲ論理ゲート３２５～３２８で構成される。

【００５３】
前記第１ＡＮＤ論理ゲート３２１はランダムマスクデータ／ａ１、／ａ２を受け入れてＡＮＤ論理演算を実行して第１中間データ／ａ１∧／ａ２を発生する。前記第２ＡＮＤ論理ゲート３２２は第１ランダムマスクデータ／ａ１および第２ランダムデータｒ２を受け入れてＡＮＤ論理演算を実行し、第２中間データ／ａ１∧ｒ２を発生する。前記第３ＡＮＤ論理ゲート３２３は第２ランダムマスクデータ／ａ２および第１ランダムデータｒ１を受け入れてＡＮＤ論理演算を実行し、第３中間データ／ａ２∧ｒ１を発生する。前記第４ＡＮＤ論理ゲート３２４は第１および第２ランダムデータｒ１、ｒ２を受け入れてＡＮＤ論理演算を実行し、第４中間データｒ１∧ｒ２を発生する。

【００５４】
前記第１ＸＯＲ論理ゲート３２５は第２中間データ／ａ１∧ｒ２および第３中間データ／ａ２∧ｒ１を受け入れてＸＯＲ論理演算を実行して第５中間データ(／ａ１∧ｒ２)・XOR・(／ａ２∧ｒ１)を発生する。前記第２ＸＯＲ論理ゲート３２６は第４中間データｒ１∧ｒ２および第５中間データ(／ａ１∧ｒ２)・XOR・(／ａ２∧ｒ１)を受け入れてＸＯＲ論理演算を実行して第６中間データ(／ａ１∧ｒ２)・XOR・(／ａ２∧ｒ１)・XOR・(ｒ１∧ｒ２)を発生する。前記第３ＸＯＲ論理ゲート３２７は第６中間データ(／ａ１∧ｒ２)・XOR・(／ａ２∧ｒ１)・XOR・(ｒ１∧ｒ２)および第３ランダムデータｒ３を受け入れてＸＯＲ論理演算を実行して第７中間データ(／ａ１∧ｒ２)・XOR・(／ａ２∧ｒ１)・XOR・(ｒ１∧ｒ２)・XOR・ｒ３)を発生する。前記第４ＸＯＲ論理ゲート３２８は第１中間データ／ａ１∧／ａ２および第７中間データ(／ａ１∧ｒ２)・XOR・(／ａ２∧ｒ１)・XOR・(ｒ１∧ｒ２)・XOR・ｒ３)を受け入れてＸＯＲ論理演算を実行して出力データ(／ａ１∧／ａ２)・XOR・{(／ａ１∧ｒ２)・XOR・(／ａ２∧ｒ１)・XOR・(ｒ１∧ｒ２)・XOR・ｒ３}を発生する。

【００５５】
【数４】

$$
\begin{aligned}
&(/a1\wedge/a2)^{\oplus}\ \{(/a1\wedge r2)^{\oplus}\ (/a2\wedge r1)^{\oplus}\ (r1\wedge r2)^{\oplus}\ r3\}\\
&=\{(/a1\wedge/a2)^{\oplus}(/a1\wedge r2)^{\oplus}(/a2\wedge r1)^{\oplus}\ (r1\wedge r2)\}^{\oplus}\ r3\\
&=(a1\wedge a2)^{\oplus}r3
\end{aligned}
$$

【００５６】
ここで、数４は次の式によって証明される。

【００５７】
【数５】

$$
\begin{aligned}
&\text{i)}\ (/a1\wedge/a2)=(a1^{\oplus}r1)\wedge(a2^{\oplus}r2)\\
&\qquad=(a1\wedge a2)^{\oplus}(a1\wedge r2)^{\oplus}(r1\wedge a2)^{\oplus}(r1\wedge r2)\\
&\text{ii)}\ (/a1\wedge r2)=(a1^{\oplus}\ r1)\wedge r2=(a1\wedge r2)^{\oplus}(r1\wedge r2)\\
&\text{iii)}\ (/a2\wedge r1)=(a2^{\oplus}\ r2)\wedge r1=(a2\wedge r1)^{\oplus}(r1\wedge r2)
\end{aligned}
$$

【００５８】
同一の値をＸＯＲ論理演算すれば、消去されるので、式i)、ii)、iii)を数４に代入すれば、出力データは(ａ１∧ａ２)・XOR・ｒ３になる。

【００５９】
前記ＡＮＤ演算装置３２０は論理演算途中に入力データａ１、ａ２のみで計算、ないし表現されない。前記ＡＮＤ演算装置３２０はランダムマスクデータ／ａ１、／ａ２およびランダムデータｒ１、ｒ２、ｒ３のみを変数として論理演算を実行し、その結果として前記入力データａ１、ａ２に対するＡＮＤ論理演算結果をランダムマスク形式に出力する。

【００６０】
一方、前記ランダムマスクデータおよびランダムデータが各々ｎビット(ｎは自然数)のデ

ータである場合には各々同一のビット桁数の間でＡＮＤ論理演算を実行する。

【００６１】

図４は図１に示した論理演算装置の実施形態として論理和ＯＲ演算装置を示すブロック図である。前記論理和ＯＲ演算装置３３０は二つのランダムマスクデータ／ａ１、／ａ２と３個のランダムデータｒ１、ｒ２、ｒ３を受け入れる。そして入力データａ１、ａ２のＯＲ論理演算結果ａ１∨ａ２をランダムマスク形式(ａ１∨ａ２)・XOR・ｒ３に出力する。

【００６２】

図４を参照すれば、前記論理和ＯＲ演算装置３３０は二つのＯＲ論理ゲート３３１、３３４、二つのＡＮＤ論理ゲート３３２、３３３、および４個のＸＯＲ論理ゲート３３５～３３８で構成される。前記論理和ＯＲ演算装置３３０の動作原理は前記論理積ＡＮＤ演算装置３２０と同一であるので省略する。

【００６３】

前記論理和ＯＲ演算装置３３０は出力データ(／ａ１∨／ａ２)・XOR・{(／ａ１∧ｒ２)・XOR・(／ａ２∧ｒ１)・XOR・(ｒ１∨ｒ２)・XOR・ｒ３}を発生する。

【００６４】

【数６】

$$(/a1 \vee /a2) \oplus \{(/a1 \wedge r2) \oplus (/a2 \wedge r1) \oplus (r1 \vee r2) \oplus r3\}$$
$$= \{(/a1 \vee /a2) \oplus (/a1 \wedge r2) \oplus (/a2 \wedge r1) \oplus (r1 \vee r2)\} \oplus r3$$
$$= (a1 \vee a2) \oplus r3$$

【００６５】

前記ＯＲ演算装置３３０は論理演算途中に入力データａ１、ａ２のみで計算、ないし表現されない。前記ＯＲ演算装置３３０はランダムマスクデータ／ａ１、／ａ２およびランダムデータｒ１、ｒ２、ｒ３のみを変数として論理演算を実行し、その結果として前記入力データａ１、ａ２に対するＯＲ論理演算結果ａ１∨ａ２をランダムマスク形式(ａ１∨ａ２)・XOR・ｒ３に出力する。

【００６６】

一方、前記ランダムマスクデータおよびランダムデータが各々ｎビット(ｎは自然数)のデータである場合には各々同一のビット桁数の間でＯＲ論理演算を実行する。

【００６７】

図５は図１に示した論理演算装置の実施形態として否定論理積ＮＡＮＤ演算装置を示すブロック図である。前記否定論理積ＮＡＮＤ演算装置３４０は二つのランダムマスクデータ／ａ１、／ａ２と ４個のランダムデータｒ１、ｒ２、ｒ３、ｒ４を受け入れる。そして、入力データａ１、ａ２のＮＡＮＤ論理演算結果～(ａ１∧ａ２)をランダムマスク形式(～(ａ１∧ａ２)・XOR・ｒ４)に出力する。

【００６８】

図５を参照すれば、前記ＮＡＮＤ演算装置３４０はＡＮＤ演算装置３４１とＮＯＴ演算装置３４２で構成される。

【００６９】

前記ＡＮＤ演算装置３４１は図３に示したＡＮＤ演算装置３２０と同一である。前記ＡＮＤ演算装置３４１は二つのランダムマスクデータ／ａ１、／ａ２と３個のランダムデータｒ１、ｒ２、ｒ３を受け入れて第１中間データ(ａ１∧ａ２)・XOR・ｒ３を発生する。

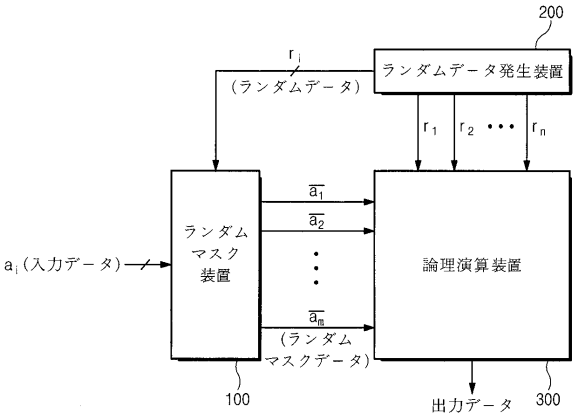
【００７０】

前記ＮＯＴ演算装置３４２は図２に示したＮＯＴ演算装置３１０と同一である。前記第１中間データ(ａ１∧ａ２)・XOR・ｒ３から(ａ１∧ａ２)＝ａ３に置換すれば、前記第１中間データはａ３・XOR・ｒ３になる。前記第１中間データはランダムマスクデータ／ａ３＝ａ３・XOR・ｒ３になる。前記ＮＯＴ演算装置３４２はランダムマスクデータ／ａ３と二つのランダムデータｒ３、ｒ４を受け入れて出力データ～ａ３・XOR・ｒ４を発生する。

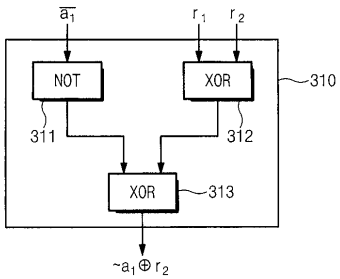
【００７１】
ここで、ａ３＝ａ１∧ａ２であるので、前記ＮＡＮＤ演算装置３４２の出力データは ～(ａ１∧ａ２）・XOR・ｒ４である。
【００７２】
前記ＮＡＮＤ演算装置３４０は論理演算途中に入力データａ１、ａ２のみで計算、ないし表現されない。前記ＮＡＮＤ演算装置３４０はランダムマスクデータ／ａ１、／ａ２ およびランダムデータｒ１、ｒ２、ｒ３、ｒ４のみを変数として論理演算を実行し、その結果として前記入力データａ１、ａ２に対するＮＡＮＤ論理演算結果～（ａ１∧ａ２）をランダムマスク形式（～（ａ１∧ａ２）・XOR・ｒ４）に出力する。
【００７３】
一方、前記ランダムマスクデータおよびランダムデータが各々ｎビット(ｎは自然数)のデータの場合には各々同一のビット桁数の間でＮＡＮＤ論理演算を実行する。
【００７４】
図６は図１に示した論理演算装置の実施形態として否定論理和ＮＯＲ演算装置を示すブロック図である。前記ＮＯＲ演算装置３５０は二つのランダムマスクデータ／ａ１、／ａ２と４個のランダムデータｒ１、ｒ２、ｒ３、ｒ４を受け入れる。
【００７５】
図６を参照すれば、前記ＮＯＲ演算装置３５０はＯＲ演算装置３５１とＮＯＴ演算装置３５２で構成される。前記ＮＯＲ演算装置３５０の動作原理は図５で説明したＮＡＮＤ演算装置３４０と同一であるので省略する。
【００７６】
前記ＮＯＲ演算装置３５０は論理演算途中に入力データａ１、ａ２のみで計算、ないし表現されない。前記ＮＯＲ演算装置３５０はランダムマスクデータ/ａ１、/ａ２およびランダムデータｒ１、ｒ２、ｒ３、ｒ４のみを変数として論理演算を実行し、その結果として前記入力データａ１、ａ２に対するＮＯＲ論理演算結果～（ａ１∨ａ２）をランダムマスク形式～（ａ１∨ａ２）・XOR・ｒ４)に出力する。
【００７７】
前記ランダムマスクデータおよびランダムデータが各々ｎビット(ｎは自然数)のデータである場合には各々同一のビット桁数の間でＮＯＲ論理演算を実行する。
【００７８】
本発明では実施形態としてＮＯＴ、ＡＮＤ、ＯＲ、ＮＡＮＤ、ＮＯＲ基本演算装置に対してだけ説明した。しかし、そのような発明の技術的思想は前記基本演算装置を基づいて作ることができる装置(例えば、全加算器(Ｆｕｌｌ Ａｄｄｅｒ)、半加算器(Ｈａｌｆ Ａｄｄｅｒ)、Ｒｉｐｐｌｅ Ｃａｒｒｙ Ａｄｄｅｒ、コンパレーター（Ｃｏｍｐａｒａｔｏｒ)、一般的なＡＬＵ（Ａｒｉｔｈｍｅｔｉｃ Ｌｏｇｉｃ Ｕｎｉｔ） などにも適用されることができることは本発明の技術分野で通常の知識を持つ者に自明の事実である。
【００７９】
また、本発明の詳細な説明では具体的な実施形態に関して説明したが、本発明の範囲から逸脱しない限度内で様々な変形が可能であることもちろんである。したがって、本発明の範囲は上述の実施形態に限って決められてはならず、上述の特許請求の範囲だけではなく、この発明の特許請求の範囲と均等なものなどによって決められなければならない。
【図面の簡単な説明】
【００８０】
【図１】本発明による基本演算装置を示すブロック図である。
【図２】図１に示した論理演算装置の実施形態としてＮＯＴ演算装置を示すブロック図である。
【図３】図１に示した論理演算装置の実施形態としてＡＮＤ演算装置を示すブロック図である。
【図４】図１に示した論理演算装置の実施形態としてＯＲ演算装置を示すブロック図である。

【図５】図１に示した論理演算装置の実施形態としてＮＡＮＤ演算装置を示すブロック図である。
【図６】図１に示した論理演算装置の実施形態としてＮＯＲ演算装置を示すブロック図である。
【符号の説明】
【００８１】
１００　　ランダムマスク装置
２００　　ランダムデータ発生装置
３００　　論理演算装置
３１０　　ＮＯＴ演算装置
３２０　　ＡＮＤ演算装置
３３０　　ＯＲ演算装置
３４０　　ＮＡＮＤ演算装置
３５０　　ＮＯＲ演算装置

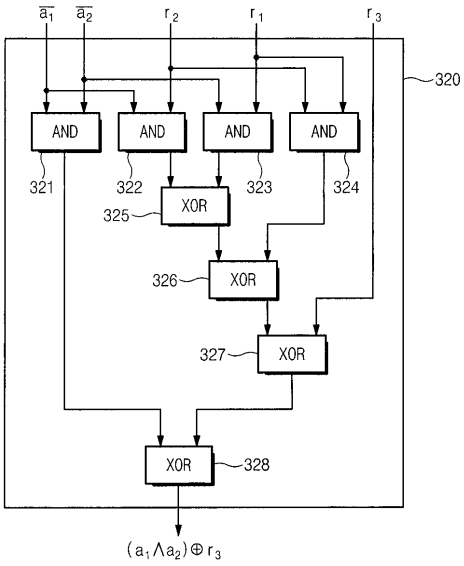
【図１】



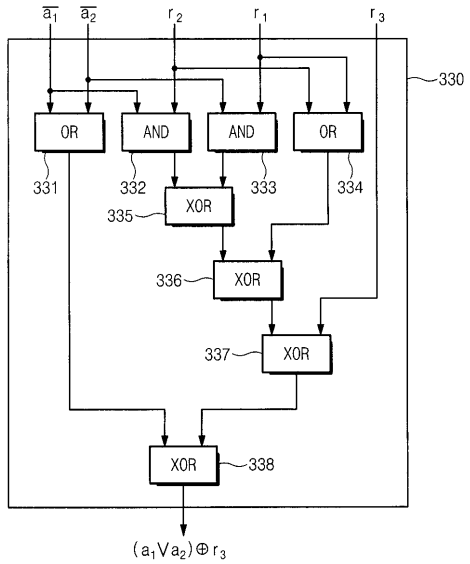
【図２】



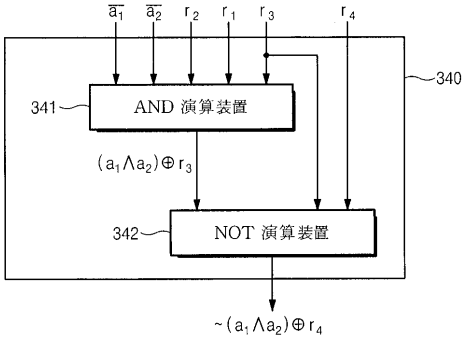
【図３】



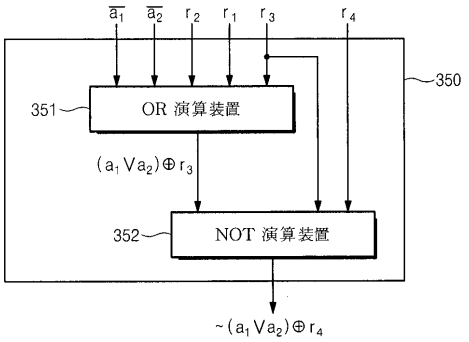
【図４】


$\overline{a_1}$
$\overline{a_2}$
r_2
r_1
r_3
330
OR
AND
AND
OR
331
332
333
334
335
XOR
336
XOR
337
XOR
338
$(a_1 \vee a_2) \oplus r_3$

【図５】


$\overline{a_1}$
$\overline{a_2}$
r_2
r_1
r_3
r_4
340
341
AND 演算装置
$(a_1 \wedge a_2) \oplus r_3$
342
NOT 演算装置
$\sim(a_1 \wedge a_2) \oplus r_4$

【図６】


$\overline{a_1}$
$\overline{a_2}$
r_2
r_1
r_3
r_4
350
351
OR 演算装置
$(a_1 \vee a_2) \oplus r_3$
352
NOT 演算装置
$\sim(a_1 \vee a_2) \oplus r_4$

フロントページの続き

(74)代理人 100110364
弁理士 実広 信哉
(72)発明者 エレナ・トリチナ
大韓民国京畿道水原市靈通区靈通洞（番地なし） シンナムシルアパート５０７－１１０２
(72)発明者 尹 重▲チュル▼
大韓民国ソウル江北区水踰２洞３７２－９

審査官 金沢 史明

(56)参考文献 特開２００２－１４１８９７（ＪＰ，Ａ）
特開２０００－０６６５８５（ＪＰ，Ａ）
特開２００２－３６６０２９（ＪＰ，Ａ）
特表２００３－５２１２０１（ＪＰ，Ａ）
特表２００３－５１３４９０（ＪＰ，Ａ）
特表２００２－５１９７２２（ＪＰ，Ａ）
国際公開第０３／０６０６９１（WO，Ａ１）
国際公開第０１／００８０１２（WO，Ａ１）
国際公開第００／０６７４１０（WO，Ａ１）
E. Trichina, Combinational Logic Design for AES SubByte Transformation on Masked Data, Cryptology ePrint Archive, International Association for Cryptologic Research, ２００３年１１月, Report 2003/236, ［２０１０年１２月２２日検索］, ＵＲＬ, http://eprint.iacr.org/2003/236
Y. Ishai, A. Sahai and D. Wagner, Private Circuits: Securing Hardware against Probing Attacks, Proceedings of CRYPTO 2003, ２００３年 ８月, pp.463-481, ［２０１０年１２月２２日検索］, ＵＲＬ, http://www.iacr.org/cryptodb/archive/2003/CRYPTO/

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｌ ９／１０