(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2005-512240
(P2005-512240A)
(43)公表日　平成17年4月28日(2005.4.28)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06K 19/073	G06K 19/00	P	5B035

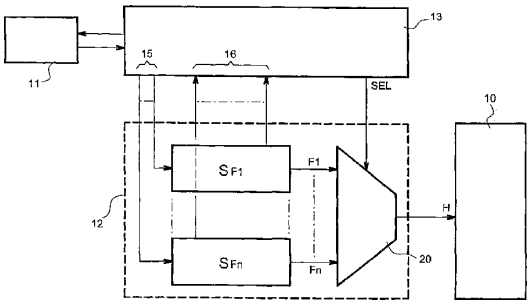
審査請求 未請求　予備審査請求 未請求　（全 10 頁）

(21)出願番号	特願2003-551733 (P2003-551733)
(86)(22)出願日	平成14年12月11日 (2002.12.11)
(85)翻訳文提出日	平成16年6月11日 (2004.6.11)
(86)国際出願番号	PCT/FR2002/004285
(87)国際公開番号	WO2003/050750
(87)国際公開日	平成15年6月19日 (2003.6.19)
(31)優先権主張番号	01/16114
(32)優先日	平成13年12月13日 (2001.12.13)
(33)優先権主張国	フランス(FR)

(71)出願人　504226179
キャナル　プラス　テクノロジーズ
フランス国　エフ－７５０１５　パリ　３４　プラース　ロール　デューティ
(74)代理人　100074332
弁理士　藤本　昇
(74)代理人　100114421
弁理士　薬丸　誠一
(74)代理人　100114432
弁理士　中谷　寛昭
(74)代理人　100117204
弁理士　岩田　徳哉
(72)発明者　ジーン　ラック　デュボイス
フランス国　エフ－７５１１６　パリ　１９　リュー　ユージーン　マニュエル
最終頁に続く

(54)【発明の名称】電気式解析から保護されるデジタル電子部品

(57)【要約】
【課題】　チップカードの演算速度をランダム化させることによって外部からの攻撃を阻止するデジタル電子部品を提供する。
【解決手段】　本発明のデジタル電子部品は、クロックHによって決定される同期成分１０を有する電気及び電磁気式解析から保護されるデジタル電子部品において、少なくとも与えられた時間内に最小値及び最大値間をランダムに周波数を変化させ、前記クロックHを供給する周波数発生器１２、及び前記クロックHの周波数変化のランダム性を制御する手段１３を備えるようにした。



【特許請求の範囲】
【請求項１】
クロック（Ｈ）によって決定される同期成分（１０）を有する電気及び電磁気式解析から保護されるデジタル電子部品において、少なくとも与えられた時間内に最小値及び最大値間をランダムに周波数を変化させ、前記クロック（Ｈ）を供給する周波数発生器（１２）、及び前記クロック（Ｈ）の周波数変化のランダム性を制御する手段（１３）を備えることを特徴とするデジタル電子部品。
【請求項２】
前記周波数発生器は、少なくとも２つの周波数合成器（ＳＦ１，…ＳＦｎ）と、切替手段（２０）とを備えることを特徴とする請求項１記載のデジタル電子部品。
【請求項３】
前記周波数発生器は、少なくとも２つのＰＬＬ回路と、切替手段とを備えることを特徴とする請求項１記載のデジタル電子部品。
【請求項４】
前記同期成分は、チップカードの主要部（１０）であることを特徴とする請求項１記載のデジタル電子部品。
【請求項５】
前記制御装置（１３）は、主要部（１０）によって操作されることを特徴とする請求項４記載のデジタル電子部品。
【請求項６】
前記同期成分はメモリーであることを特徴とする請求項１記載のデジタル電子部品。
【請求項７】
前記同期成分（１０）は、ケーブル同期関数であることを特徴とする請求項１記載のデジタル電子部品。
【請求項８】
前記クロック（Ｈ）の周波数変位は１Ｍｈｚと１００Ｍｈｚの間を含むことを特徴とする請求項１記載のデジタル電子部品。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は電気及び／又は電磁式解析から保護されるデジタル電子部品に係り、より詳しくはチップカードに関するものである。
【背景技術】
【０００２】
発明の属する技術分野は、例えば、消費電流の解析手段により、又は放出された電磁波の解析により、データ抽出（通常、暗号鍵と共に）を有効にするためのメカニズムであるチップカードのようなデジタル電子部品の実施に関する。このような解析には、一般に、ＳＰＡ(Simple Power Analysis)，ＤＰＡ(Differential Power Analysis)又はＳＥＭＡ(Simple Electrical Magnetic Analysis)，ＤＥＭＡ(Differential Electrical Magnetic Analysis)と呼ばれるものがある。
【０００３】
このような解析によって、チップカードの主要部が何を行うか、どのデータが最後に処理されるのかを解明することは可能である。従って、このデータを送信するために使用する、単一の（又は複数の）暗号鍵にアクセスすることは可能である。そのような侵入は、全く危険を伴うものではないかもしれない、なぜならば、構成要素が変わらないままであるので、起こりうることを後で検証することは可能ではないからである。
【０００４】
「差分出力解析入門、及び関連する取り組み」（インターネットサイト：www.cryptography.com、暗号法研究、１９９８）と題する、ポール　コーチャー、ジョシュァ　ジャフェ、そしてベンジャミン　ジュンの記事に記載されているように、この解析法は、大きな

影響があるかもしれない、なぜならば、彼らは、暗号化された通信に使用される暗号鍵を復元することを許可しているからである。さらに、そのような攻撃は、素早く設定されたり、容易に入手可能な装置を使用することで実行されるかもしれない。このような攻撃を実現するための所要時間は、攻撃（ＤＰＡ，ＳＰＡ）の種類によって決まり、そして、熟考された構成要素の機能によって異なる。ＤＰＡ攻撃は何時間もかかるのに対し、ＳＰＡ攻撃は、構成要素が一つであるために２，３秒ですむ。

【０００５】

今日のデジタル電子工学は、このような電気的又は電磁気的解析を鑑みれば、最低限のものであり、保護されるものではない。攻撃の二つのファミリーは、一方が複数のソフトウエア、他方が複数のハードウエアに存在する。データに関しては、チップカードの主要部によって処理される。

【０００６】

一つ目のファミリーによれば、ある技術的解決法は、できる限りランダムに消費電流を提供することにあり、この消費電流は、主要部によって処理されるデータに対し関連する確率は低い。このように、命令の手順をランダム化すること、あるいは処理されたデータを可能な限りランダムに提供することは可能である。

【０００７】

二つ目のファミリーによれば、以下に挙げるいずれか一方を行うことが可能である。

【０００８】

・消費電流及び主要部によって処理される命令の間の関連性を完全に理解するのを困難にするために、可能な限り安定した電流を提供すること。

【０００９】

・主要部の二つの等しい演算を非同期化するために消費電流をランダム化すること。

【００１０】

本発明は、二つ目のケースに属する。

【００１１】

欧州特許出願公開第１１１３３８６号明細書には、このような攻撃に鑑みて、チップカードを保護するための解決法が記載されている。この解決法によれば、二つのcondensatorがチップカードに内蔵されており、それらは、常に一方が、外部の電源装置によって充電され、他方がチップカードの構成要素を起動することによって放電される。二つのcondensatorの役割は、素早く交互に動作し、前記構成要素の演算に関して、少しの情報も取り出せないという意味では、電源装置がチップカードの構成要素から分離される。

【発明の開示】

【発明が解決しようとする課題】

【００１２】

本発明の目的は、例えば、解析が困難な、そして恐らく不可能なＳＰＡ／ＤＰＡ、及び／又はＳＥＭＡ／ＤＥＭＡといった、チップカードのようなデジタル電子部品の演算速度をランダムに変化させることによって、上記記載の問題点を解決することにある。

【課題を解決するための手段】

【００１３】

本発明は、クロックによって決定される同期成分を有する電気及び／又は電磁気式解析から保護されるデジタル電子部品において、少なくとも与えられた時間内に最小値及び最大値間をランダムに周波数を変化させ、前記クロックを供給する発生手段、及び前記クロックの周波数変化のランダム性を制御する手段を備えることを特徴とするデジタル電子部品に関する。

【００１４】

前記クロックの発生手段は、周波数発生器に命令を出すランダム周波数指示発生器を含んでも構わない。

【００１５】

前記周波数発生器は、少なくとも二つの周波数合成器、又はＰＬＬ回路（Phase Locked

Loop）、及びこれらの合成器又は回路間の切換手段を含んでも構わない。

【００１６】

前記同期成分は、チップカードの主要部、メモリー、あるいは、例えばＦＰＧＡタイプ（Field,Programmable Gate Arrays）又はＡＳＩＣタイプ（Application specific integrated Circuit）のようなケーブル同期関数であっても構わない。

【００１７】

周波数変化の範囲は、ＤＰＡ／ＳＰＡ及びＤＥＭＡ／ＳＥＭＡタイプの解析を最大限に阻害するために、可能な限り広くなければならない。考慮されたランダムは、実質的なランダムであり、なぜなら、この場合、クロックの位相又は周波数シフトではなく、操作されたランダム周波数だからである。同期成分の消費電流がこのような方法でクロックを阻害することによって、ランダムにさせる。

【発明を実施するための最良の形態】

【００１８】

図面で説明するように、本発明によれば電気及び／又は電磁気式の攻撃から保護されるデジタル電子部品は、チップカードを例として以下の構成からなる。

【００１９】

つまり、前記チップカードの主要部１０と、ランダム周波数指示発生器１１と、該発生器１１によって操作され、前記主要部にクロックＨを提供し、そして、最小値及び最大値間をランダムに周波数を変化させる周波数発生器１２と、前記クロックＨの周波数を測定し、その周波数変化の実質的なランダムオペレーションを検証することを図る制御装置１３とからなる。

【００２０】

可能な限り大きな前記クロックＨの周波数変位は、１Ｍｈｚ及び１００Ｍｈｚの間に含まれる。

【００２１】

図示された実施例によれば、周波数発生器１２は、制御装置１３のアウトプット１５から供給される信号を制御する、少なくとも二つの周波数合成器ＳＦ１，…ＳＦｎと、これらの合成器ＳＦ１，…ＳＦｎのアウトプット信号Ｆ１…Ｆｎを受け取る多重化及び同期回路２０とから成る。

【００２２】

そして、周波数変化が起こる時に、前記制御装置１３がインプット１６で受け取った信号を解析することによって妨害が起こりえないことを検証し、前記多重化及び同期回路２０にＳＥＬ信号を送ることによって、前記合成器ＳＦ１，…ＳＦｎのアウトプットで複数の周波数の中から一つを選択する。

【００２３】

従って、前記制御装置１３は、以下の方法で操作させてもよい。

【００２４】

まず、ランダム周波数指示発生器１１から新しい値を要求し、前記発生器１１によって制御装置１３に値を与える。そして、前回の値と比較して今回の値のランダム性を制御装置によって検証し、合成器ＳＦ１，…ＳＦｎへ今回の値を送る。

【００２５】

本発明は、演算を実行する主要部の操作をランダム化すること、及びランダムな消費電流の出現を与えることを可能にする。なぜならば、ＳＰＡ／ＤＰＡ及び／又はＳＥＭＡ／ＤＥＭＡを解析することは困難であり、かなり増加する無数の電流解析を必要とするので恐らく無理だからである。

【００２６】

本発明は、主要部を変更しないこと、そして周波数の特有の範囲内で主要部を操作することを許可する。

【００２７】

本発明を保護するための範囲は、前記ランダム周波数指示発生器、及び主要部の指示周

期の範囲に応じた周波数変化の周期に依存する。

【００２８】

有利な実施形態によれば、前記制御装置は、主要部によって操作させてもよい。

【００２９】

その他の手段によれば、もし重要と考えられるならば、与えられた時間内にのみ本発明に従ってクロックＨのランダム周波数変化をアクティブにすることは可能である。

【図面の簡単な説明】

【００３０】

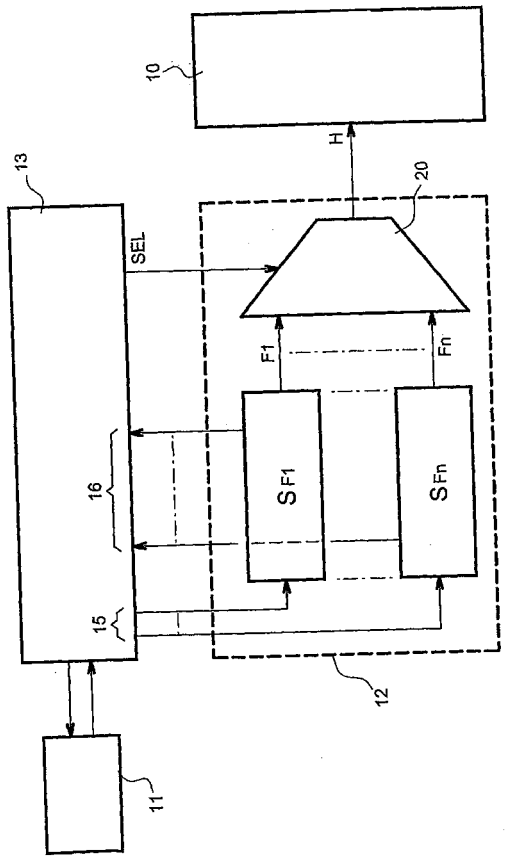
【図１】電気及び／又は電磁気式攻撃から保護されるデジタル電子部品を説明するための図である。

【符号の説明】

【００３１】

１０…主要部
１１…ランダム周波数指示発生器
１２…周波数発生器
１３…制御装置
１５…アウトプット
１６…インプット
２０…多重化及び同期周期
Ｈ…クロック

【図１】



【国際調査報告】

INTERNATIONAL SEARCH REPORT

Int onal Application No
PCT/FR 02/04285

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06K7/00 G06K19/07

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, IBM-TDB, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 97 17667 A (BRITISH TECH GROUP ;CLOETE JACOB PIETER LAURENS (ZA); EEDEN HENDRI) 15 May 1997 (1997-05-15)	1,2,5-8
A	page 5, line 3 - line 16; figure 1	3,4
X	EP 0 772 058 A (SIEMENS AG) 7 May 1997 (1997-05-07) the whole document	1-8
A	EP 0 482 975 A (GEMPLUS CARD INT) 29 April 1992 (1992-04-29) the whole document	1

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
8 April 2003	16/04/2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Degraeve, A

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/FR 02/04285

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9717667 A	15-05-1997	AU 7502396 A	29-05-1997
		BR 9611705 A	23-02-1999
		CN 1201540 A	09-12-1998
		EP 0859989 A1	26-08-1998
		WO 9717667 A1	15-05-1997
		JP 2000500932 T	25-01-2000
		TW 383527 B	01-03-2000
		ZA 9609411 A	12-06-1997
EP 0772058 A	07-05-1997	DE 59610041 D1	13-02-2003
		EP 0772058 A2	07-05-1997
		JP 9133548 A	20-05-1997
		US 5872520 A	16-02-1999
EP 0482975 A	29-04-1992	FR 2667715 A1	10-04-1992
		CA 2053001 A1	10-04-1992
		DE 69100836 D1	03-02-1994
		DE 69100836 T2	09-06-1994
		EP 0482975 A1	29-04-1992
		ES 2065646 T3	16-02-1995
		JP 3155973 B2	16-04-2001
		JP 4263384 A	18-09-1992
		US 5477039 A	19-12-1995

Form PCT/ISA/210 (patent family annex) (July 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Der ›Internationale No
PCT/FR 02/04285

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G06K7/00 G06K19/07

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G06K

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data, PAJ, IBM-TDB, INSPEC

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	WO 97 17667 A (BRITISH TECH GROUP ;CLOETE JACOB PIETER LAURENS (ZA); EEDEN HENDRI) 15 mai 1997 (1997-05-15)	1,2,5-8
A	page 5, ligne 3 - ligne 16; figure 1	3,4
X	EP 0 772 058 A (SIEMENS AG) 7 mai 1997 (1997-05-07) le document en entier	1-8
A	EP 0 482 975 A (GEMPLUS CARD INT) 29 avril 1992 (1992-04-29) le document en entier	1

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
8 avril 2003	16/04/2003

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 Nl. – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Degraeve, A

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale No
PCT/FR 02/04285

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
WO 9717667	A	15-05-1997	AU	7502396 A	29-05-1997
			BR	9611705 A	23-02-1999
			CN	1201540 A	09-12-1998
			EP	0859989 A1	26-08-1998
			WO	9717667 A1	15-05-1997
			JP	2000500932 T	25-01-2000
			TW	383527 B	01-03-2000
			ZA	9609411 A	12-06-1997
EP 0772058	A	07-05-1997	DE	59610041 D1	13-02-2003
			EP	0772058 A2	07-05-1997
			JP	9133548 A	20-05-1997
			US	5872520 A	16-02-1999
EP 0482975	A	29-04-1992	FR	2667715 A1	10-04-1992
			CA	2053001 A1	10-04-1992
			DE	69100836 D1	03-02-1994
			DE	69100836 T2	09-06-1994
			EP	0482975 A1	29-04-1992
			ES	2065646 T3	16-02-1995
			JP	3155973 B2	16-04-2001
			JP	4263384 A	18-09-1992
			US	5477039 A	19-12-1995

フロントページの続き

(81)指定国 AP(GH,GM,KE,LS,MW,MZ,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,IE,IT,LU,MC,NL,PT,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,MZ,NO,NZ,OM,PH,PL,PT,RO,RU,SC,SD,SE,SG,SK,SL,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,YU,ZA,ZM,ZW

(72)発明者 ジュローム ペリーン
フランス国 エフ－９２１００ ボウローン ４６ リュー アンスィアン メイリン

Ｆターム(参考) 5B035 BB09 CA12 CA38