

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.



[12] 发明专利说明书

G06F 11/26 (2006.01)

G01R 31/3181 (2006.01)

G06K 19/073 (2006.01)

专利号 ZL 02824766.3

[45] 授权公告日 2008 年 6 月 25 日

[11] 授权公告号 CN 100397358C

[22] 申请日 2002.12.11 [21] 申请号 02824766.3

[30] 优先权

[32] 2001.12.13 [33] FR [31] 01/16114

[86] 国际申请 PCT/FR2002/004285 2002.12.11

[87] 国际公布 WO2003/050750 法 2003.6.19

[85] 进入国家阶段日期 2004.6.11

[73] 专利权人 卡纳尔技术公司

地址 法国巴黎

[72] 发明人 J·-L·多瓦斯 J·珀赖因

[56] 参考文献

WO97/17667A1 1997.5.15

EP0482975A1 1992.4.29

US5872520A 1999.2.16

审查员 范成博

[74] 专利代理机构 中国专利代理(香港)有限公司

代理人 吴立明 张志醒

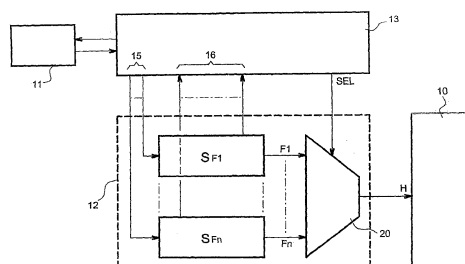
权利要求书 1 页 说明书 4 页 附图 1 页

[54] 发明名称

抗电型分析的数字电子部件

[57] 摘要

本发明涉及到抗电型和/或电磁型分析的数字电子部件。发明部件包括：由时钟(H)控制的同步元件(10)；产生时钟(H)的装置(11, 12)，时钟频率至少在一段给定时间在最小值与最大值之间随机地变化；以及控制时钟(H)频率变化随机性的控制装置(13)。



1. 抗电型和电磁型分析的数字电子部件，该数字电子部件包括：由时钟（H）驱动的同步元件，其特征在于：所述数字电子部件包括提供所述时钟（H）的并由一随机频率指令发生器（11）驱动的频率发生器（12），该时钟频率至少在给定时间段期间在最小值与最大值之间以随机的方式改变，所述数字电子部件还包括控制时钟（H）的频率变化的随机特性的控制器（13）。

2. 根据权利要求1的部件，其中频率发生器包括：至少两个频率合成器（SF1，...SF_n）以及切换装置（20）。

3. 根据权利要求1的部件，其中频率发生器包括：至少两个 PLL 电路以及切换装置。

4. 根据权利要求1的部件，其中所述同步元件是芯片卡的中央单元（10）。

5. 根据权利要求4的部件，其中控制器（13）由中央单元驱动。

6. 根据权利要求1的部件，其中所述同步元件为存储器。

7. 根据权利要求1的部件，其中所述同步元件为有线同步功能件。

8. 根据权利要求1的部件，其中所述时钟（H）的频率偏移在 1Mhz-100Mhz。

抗电型分析的数字电子部件

技术领域

本发明涉及到抗电和/或电磁型分析的数字电子部件，更具体地说涉及到芯片卡领域中的这种部件。

背景技术

发明领域在于在数字电子部件，例如在芯片卡中通过电流消耗分析，或通过所发射之电磁辐射的分析来实现抗击数据摘取（通常用密钥摘取）的机理。这些分析通常称为 SPA（“简单功率分析”）/DPA（“差分功率分析”）或 SEMA（“简单电磁分析”）/DEMA（“差分电磁分析”）。

使用这些分析能够确定芯片卡的中央单元正在做什么，后者正在处理哪个数据。由此能够利用用来传输这一数据的单个（或多个）密钥。可做出这种侵入而没有任何风险，因为由于部件仍保持没有变化，其后将不可能证明曾发生过侵入。

如 Paul Kocher, Joshua Jaffe 和 Benjamin Jun 的标题为 “Introduction to differential power analysis and related attack(差分功率分析和相关攻击的介绍)” 的文章（互联网址：www.cryptography.com, Cryptography Research（加密技术研究），1998）所述，这些分析方法可能具有重要影响，因为它们能够摘取用于加密通信的密钥。此外，使用易于得到的设备可以快速地建立并实施这样的攻击。实现这些攻击所需时间的长短取决于攻击型式（DPA, SPA）并随所考虑部件的变化而改变。对部件来说，SPA 攻击可能要几秒钟，而 DPA 攻击则需许多小时。

现在，数字电子设备极少或没有不受这种电或电磁分析的。存在两种攻击：一种是纯软件的，另一种是纯硬件的。在数据由芯片卡中央单元处理的情况下：

- 在第一种情况，一种技术解决办法是使电流消耗尽可能是随机的，这一电流消耗很少可能与由中央单元处理的数据相联系。这样就能够使指令的顺序随机化，或使处理的数据尽可能是随机的。

- 在第二种情况，能够：

- 或者使电流尽可能地稳定不变以便使实现电流消耗与中央单元所操作的指令之间的联系极其困难,
- 或者使电流消耗随机化以便使中央单元两个相同的操作失去同步。

本发明属于此第二种情况。

欧洲专利申请 EP 1 113 386 说明了保护芯片卡免受这类攻击的解决办法。在这种解决办法中,在芯片卡中嵌入两个电容器使得在任何时候都由外电源对其中一个电容器充电,而通过启动芯片卡的部件使另一电容器放电。两个电容器的作用快速地交替,而在电流消耗的分析不产生有关芯片卡部件操作任何信息的意义上,电源与该部件是隔离开的。

本发明的目的是通过以随机方式改变所考虑的数字电子部件,例如芯片的运作速度来解决上述问题,诸如使 SPA/DPA 和/或 SEMA/DEMA 分析变得困难,或许变得不可能。

发明内容

本发明涉及到抗电和/或电磁型分析的数字电子部件,其包括由时钟驱动的同步元件,部件的特征在于,它包括产生这一时钟的装置,时钟频率至少在一给定时段期间在最小值与最大值之间随机地改变,它还包括控制时钟频率变化随机特性的控制装置。

时钟生成装置可包括控制频率发生器的随机频率指令发生器。

频率发生器可以包括至少两个频率合成器,或 PLL 电路(锁相环路),以及这些合成器或电路之间的切换装置。

同步元件可以是例如型式为 FPGA 型(“现场可编程门阵列”)或 ASIC 型(“专用集成电路”)的芯片卡中央单元,存储器,或有线同步功能件。

频率变化范围必须尽可能宽以便最大限度地干扰 DPA/SPA 以及 DEMA/SEMA 型的分析。所考虑的随机是实随机,因为在这种情况下它不是时钟的相移或频移,而是受驱动的随机频率变化。通过以这种方式来干扰时钟,就使同步元件的电流消耗成为随机的了。

附图说明

仅有的一个图说明了抗电型和/或电磁型攻击的数字电子部件。具体实施方案详述。

具体实施方式

如图所示, 根据本发明的抗电型和/或电磁型攻击的数字电子部件, 例如芯片卡的数字电子部件, 其包括:

- 此芯片卡的中央单元 10,
- 随机频率指令发生器 11,
- 由这个发生器 11 所驱动的频率发生器 12, 该频率发生器 12 向中央单元 10 提供时钟 H, 时钟 H 的频率以随机方式在最小值与最大值之间变化,
- 控制器 13, 其目的在于测量时钟 H 的频率并验证频率变化的随机操作。

时钟 H 的频率偏移, 此偏移应尽可能大, 在 1Mhz-100Mhz。

在图中所示的实施方案实例中, 频率发生器 12 包括频率合成器 SF1...SF_n 中的至少两个频率合成器, 其由控制器 13 输出端 15 所提供的信号控制, 频率发生器还包括一个多路复用与同步电路 20, 其接收这些合成器 SF1...SF_n 的输出 F1...F_n。

出现频率变化时, 在通过把信号 SEL 发送到多路复用与同步电路 20 来在合成器 SF1...SF_n 的输出端选择频率中其中一个频率之前, 控制器 13 通过分析在其输入端 16 所接收的信号来验证不存在可能的干扰。

因此, 控制器 13 可以以下述方式工作:

- 向随机频率指令发生器 11 请求一个新数值,
- 将由此发生器 11 提供的数值发送给控制器 13,
- 与先前的数值相比较, 通过控制器 13 来验证这一数值的随机性,
- 将这个数值发送至合成器 SF1...SF_n。

本发明能够使中央单元进行计算的操作随机化, 并能够给出随机电流消耗的状况。很难或许是不可能进行 SPA/DPA 和/或 SEMA/DEMA 分析, 因为它们需要大大地增加电流分析的数量。

因此, 本发明使得不能对中央单元进行修正, 而只能使其运行在自己的频率范围内。

本发明保护其自己的能力取决于随机频率指令发生器以及频率变化周期, 频率变化周期依中央单元指令周期的长度而定。

在有利的实施方案中，控制器可以由中央单元驱动。

在另一种运行情况，根据本发明只在认为是临界的情况在给定时段期间启动时钟 H 的随机频率变化。

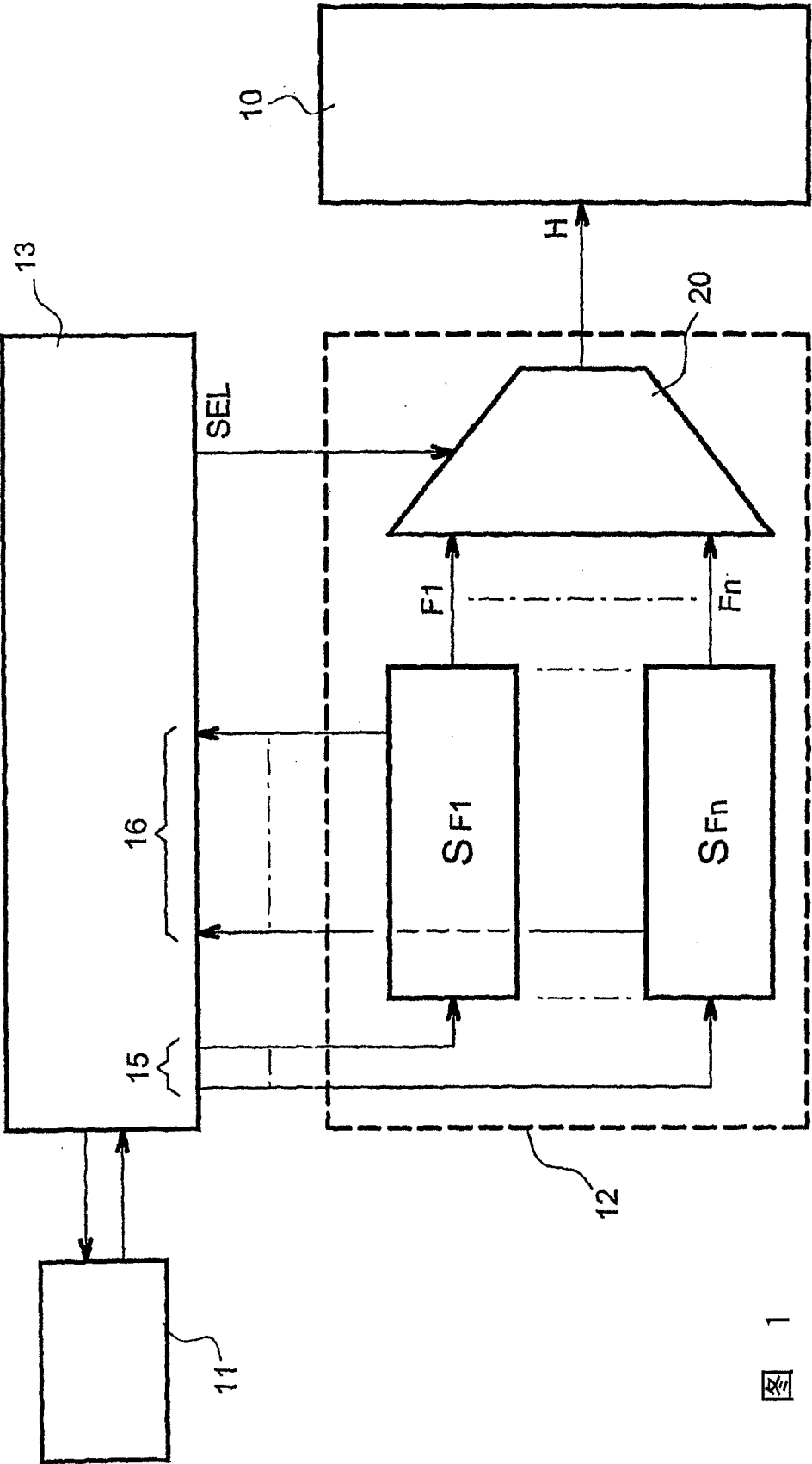


图 1