[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 1/00 (2006.01)

[12] 发明专利说明书

专利号 ZL 02812000.0

[45] 授权公告日 2006 年 3 月 1 日

[11] 授权公告号 CN 1244037C

[22] 申请日 2002.5.16 [21] 申请号 02812000.0
[30] 优先权
[32] 2001.6.13 [33] DE [31] 10128573.6
[86] 国际申请 PCT/EP2002/005428 2002.5.16
[87] 国际公布 WO2002/101520 德 2002.12.19
[85] 进入国家阶段日期 2003.12.15
[71] 专利权人 因芬尼昂技术股份公司
地址 德国慕尼黑
[72] 发明人 C·奥米勒 G·埃克斯泰恩
S·瓦尔泰恩
审查员 刘宇儒

[74] 专利代理机构 中国专利代理(香港)有限公司
代理人 程天正 梁 永

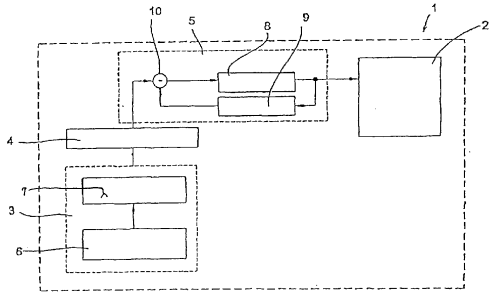
权利要求书 1 页 说明书 3 页 附图 1 页

[54] 发明名称

防止非所欲外部操作侦测的方法和数字集成电路

[57] 摘要

在一数字电路(1)中包含一异步电路(2)，异步电路(2)之电压藉由一随机电压抖动的方式被改变。 供应电压的随机变化造成在异步电路中个别的操作程序一时间抖动，藉此一个别测量的人为的同步化在侧信道攻击得以被预防。



1. 一种在具有一异步电路（2）的数字集成电路（1）中预防外部侦测操作的方法，该方法包含随时间变化该异步电路（2）的一供应电压，以时间位移该异步电路中操作执行时间的步骤。

2. 根据权利要求第 1 项所述的方法，其中该供应电压的时间变化以一随机方式发生。

3. 一种数字集成电路，包含:

一异步电路（2），以及

控制装置（3、4、5）用以随时间变化该异步电路（2）的供应电压以时间位移该异步电路（2）中的操作执行时间。

4. 根据权利要求第 3 项所述的数字集成电路，其中用来时间变化该供应电压的该控制装置（3、4、5）包含一随机数字产生器（7）。

5. 根据权利要求第 4 项所述的数字集成电路，其中用来时间变化该供应电压的该控制装置（3、4、5）更包含一噪声电压来源（6）驱动该随机数字产生器（7）。

6. 根据权利要求第 4 或第 5 项所述的数字集成电路，其中用来时间变化该供应电压的该控制装置（3、4、5）更包含一数字模拟转换器（4）用来将该随机数字产生器（7）所产生的数字数值转变成一模拟电压。

7. 根据权利要求第 3 项所述的数字集成电路，其中用来时间变化该供应电压的该控制装置（3、4、5）更包含一电压调节器（5）。

8. 根据权利要求第 3 项所述的数字集成电路，其中该异步电路（2）被用来执行一编码算法。

防止非所欲外部操作侦测的方法和数字集成电路

技术领域

本发明关于一种预防一数字集成电路中操作的外部侦测的方法以及关于一数字集成电路其中在数字集成电路中非所欲的外部操作侦测得以被预防。本发明特别是关于所谓侧信道攻击的一对策，当其被执行用以分析数字集成电路时。

背景技术

在许多集成电路中，未经授权的人必须被防止分析其操作模式。作为范例的电路其中此攻击方案被避开的是芯片卡 ICs，安全 ICs 或甚至此 ICs 的个别的电路模块，例如，举例来说，保密共处理器。未授权的人必须被防止分析一保密共处理器所执行的编码算法是不需解释的。

未授权的人所使用的典型的攻击方式，例如，尝试分析一保密共处理器实行的编码算法被参考如所谓的侧信道攻击。此侧信道攻击包含，例如，不同的功率消耗分析（DPA=不同功率分析），有关 IC 电磁辐射的侦测以及所谓计时攻击。

与同步电路相比，异步电路，在其中自身计时电路，具有其程序不直接地与一时间周期对象相关的有利的特征，例如时钟。因此，其程序并不显示任何此一时间周期对象的依赖，藉此在异步电路中成功的执行侧信道攻击更加困难。然而，即使在异步电路中，开关组件的数量经常依赖特定操作而被处理，因此在一般处理资料依赖中，其反映在相关发生的电路功率消耗的量变曲线中。

为了使此攻击更加困难，插入所谓的随机等待状态到处理过程中是已知的。亦知道去强迫在 CPU 中操作的执行的阻碍。在随机等待状态的插入中，操作的计时的可能的变化被限制，因为一延迟不能被活化或者一等待状态不能在任何时间被插入。甚至阻碍 CPU 中的执行的测量也不能完全阻挡侧信道攻击，因为此阻碍可被不同的功率消耗变化所侦测。

发明内容

从此先前技艺开始，本发明的目的提供一种防止一包含异步电路的

数字集成电路中外部操作侦测的方法。

本发明的另一目的发展具有一异步电路的一数字集成电路，以此方式在数字电路中非所欲的外部操作侦测被预防。

第一个目的藉由一种在具有一异步电路的数字集成电路中，预防外部侦测操作的方法方法达成，其中，所述的方法包含随时间变化该异步电路（2）的一供应电压，以时间位移该异步电路中操作执行时间的步骤。

第二个目的藉由一种数字集成电路而达成，其中，所述的数字集成电路包含一异步电路，以及控制装置，用以随时间变化该异步电路的供应电压以时间位移该异步电路中的操作执行时间。

本发明提供一种防止一集成电路中包含有一异步电路的外部操作侦测的方法，其包含时间变化异步电路的一供应电压用以及时位移异步电路中执行操作时间的方法步骤。在一本发明较佳的观点中，此供应电压的变化以一随机方式发生。

本发明基于在操作的执行次数中藉由叠上一随机控制的，其非可预测的，在供应电压上的时间抖动所获得的一随机时间抖动的发现，藉此一人为的侧信道攻击中个别测量的同步化被预防。然而，在异步电路中操作执行中的时间抖动并不导致程序错误，因为根据他们的特性，异步电路影响一自动同步化。

根据本发明的一装置观点，数字集成电路包含一异步电路以及一装置用以时间变化供应电压，以其异步电路被提供，藉此异步电路中操作执行时间被时间位移。

附图说明

在下列叙述中，本发明的一较佳的实施例将被详细参考随附的图标。

唯一且只有一个的图标显示一数字集成电路的方块图根据本发明的一较佳实施例。

具体实施方式

发明的数字集成电路整体参考数字编号 1 包含一异步电路 2，一产生器电路 3 用以产生真实随机数字（真实随机数字产生器），一数字模拟转换器 4，在其输入侧上，产生器电路所产生的数字随机数字被供给且在输出侧，制造一相映的模拟目标电压值，以及一电压调节器 5，

在输入侧，模拟目标电压值从数字模拟转换器 4 被供应且，在输出侧，产生一实际电压值形成异步电路 2 的供应电压。用来制造真实随机数字的产生器电路 3，依次，包含一噪声来源 6 产生一噪声电压以及一随机数字产生器 7 藉由噪声来源 6 来驱动。

然而，代替此处所示的噪声来源 6 以及随机数字产生器 7 的结合，任何其它随机产生器可以被使用来产生随机数字当数字模拟转换器输入数量时。

在此处所示较佳实施例中，电压调节器 5 包含一伺服组件 8，一实际值侦测装置 9 以及一差异生成装置 10，对于其输入，一方面来说，模拟目标电压值从数字模拟转换器 4 且，另一方面来说，一输出讯号从实际数值侦测装置 9 被供给。

产生器电路 3，数字模拟转换器 4 以及电压调节器 5 一起来自一装置用以随机地时间变化供应电压或一装置用以叠上一随机时间抖动在供应电压上，以其异步电路 2 被提供，分别地。因为随机变化供应电压，有一随机时间抖动在异步电路的操作执行中，藉此在所谓的侧信道攻击的个别测量的人为的同步化得以被预防或者，至少，使其更加困难。

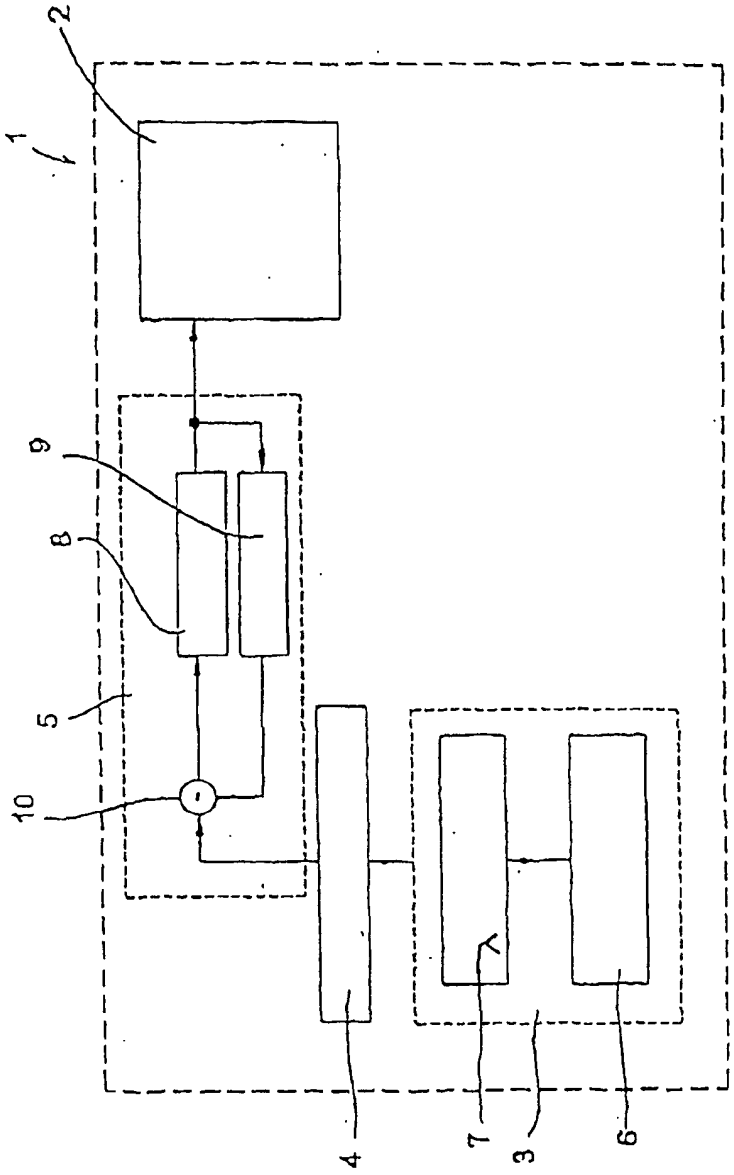


图 1