[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 12/14 (2006.01)

[12] 发明专利说明书

专利号 ZL 02139984.0

[45] 授权公告日 2008 年 10 月 1 日

[11] 授权公告号 CN 100422960C

[22] 申请日 2002.12.16 [21] 申请号 02139984.0

[30] 优先权

[32] 2001.12.19 [33] DE [31] 10162309.7

[73] 专利权人 NXP 股份有限公司

地址 荷兰艾恩德霍芬

[72] 发明人 A·M·G·佩特尔斯

M·福伊泽尔

[56] 参考文献

WO0019353A1 2000.4.6

EP1098471A2 2001.5.9

GB2345229A 2000.6.28

WO0010124A1 2000.2.24

US5404402A 1995.4.4

WO0108088A1 2001.2.1

DE19907575A1 2000.8.24

用于可变供电电压低功率处理中的有效控制器. V. Gutnik, A. Chandrakasan. 关于 VLSI 系统的讨论. 1996

审查员 郑宗玉

[74] 专利代理机构 中科专利商标代理有限责任公司

代理人 王波波

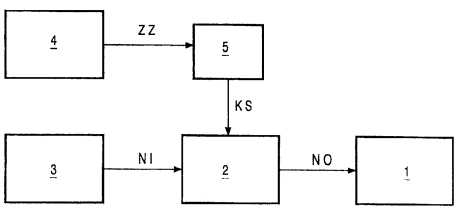
权利要求书 2 页 说明书 9 页 附图 2 页

[54] 发明名称

用于提高电路安全性防止未经授权的访问的方法和装置

[57] 摘要

本发明涉及一种用于提高电路安全性防止未经授权的访问的方法和装置，该方法和装置可以用于，特别是用于提高卡，尤其是智能卡的安全性，防止通过如下所述的微分功率分析方法(DPA)被攻击。 DPA 是一种过程，它不但能使获得完全的功能细节成为可能而且也能使获得存储在集成电路(例如，智能卡控制器)内部的信息成为可能。 大多数非同步类电路有这个特性，该特性是电路自动调整可用电压的性能。 本发明采用一种新的方法，该方法使集成电路尤其是非同步连接逻辑电路被保护防止 DPA。 优点是通过使用特定供电电源产生的自同步逻辑电路的特殊性能而获得的。 因此，在自同步逻辑电路中的过程是以一个不可预料的方式发生的，并且电流消耗被服务器噪音影响以及 DPA 不能被成功的应用。



1．一种用于提高电路安全性防止未经授权的访问的方法，所述电路包括自同步电路，其特征在于

- 由自同步电路中的数据处理操作产生的信号跟踪被退耦；

- 信号跟踪的退耦是通过改变随时间变化的自同步电路或自同步电路中的专用功能单元的时钟频率来实现的，

- 时钟频率随时间的变化是通过改变随时间变化的供电电流和／或供电电压来实现的。

2．如权利要求1所述的方法，其特征在于供电电流或供电电压随着时间的变化被随机数生成器所控制。

3．如权利要求1或2所述的方法，其特征在于随着时间变化的供电电流或供电电压的变化是通过用于芯片卡的读／写装置的一部分的设备被执行，其中在芯片卡上包括卡自同步电路（1），给所述卡自同步电路馈送随着时间变化的电流或提供随着时间变化的电压。

4．如权利要求3所述的方法，其特征在于所述芯片卡是智能卡。

5．一种用于提高电路安全性防止未经授权的访问的装置，所述电路包括至少一个自同步电路，所述装置包括所述电路、用于调节电流的可控制装置（2）以及自同步电路（1）的供电电源（3），其特征在于，用于调节电流的可控制装置（2）被连接到自同步电路（1）的供电电源（3）和自同步电路（1）本身之间，其中通过改变提供给可控制装置的电流和电压中至少一个，来改变自同步电路的时钟频率，以退耦信号跟踪。

6．如权利要求5所述的装置，其特征在于用于调节电流的可控制装置（2）通过数／模转换器（5）被链接到随机数生成器（4）。

7．如权利要求5或6所述的装置，其特征在于自同步电路（1）是以非时钟信号交换逻辑电路形式存在的。

8．如权利要求5或6所述的装置，其特征在于自同步电路（1）是以具有芯片上的延迟线的非时钟电路形式存在的。

9．如权利要求5或6所述的装置，其特征在于自同步电路（1）是

智能卡控制器的一部分。

10．如权利要求 5 或 6 所述的装置，其特征在于供电电源（3），用于调节电流的可控制装置（2），在需要地方还有随机数生成器（4）和数／模转换器（5）是芯片卡的读/写装置的一部分。

用于提高电路安全性防止未经授权的访问的方法和装置

技术领域

本发明涉及一种用来防止未经授权的访问而提高电路安全性的方法和装置，该方法和装置尤其被用于改善卡，特别是智能卡的安全性，以防止被攻击，在此，下述的方法是通过测量电流或电压消耗来获得电子电路内部操作的信息。

背景技术

在七十年代微电子技术的发展使得没有用户接口的信用卡形式的微型计算机的产生成为可能。这种计算机被称作智能卡。在智能卡中，数据存储器和运算以及逻辑单元被集成到在尺寸上仅有几个平方毫米的单个芯片中。智能卡尤其被用作电话卡和 GSM SIM 卡以及用在银行和卫生保健领域中。智能卡也因此变成一种，无论我们在任何地方都可以看到的计算平台。

目前，智能卡主要被认为是一种用来放置秘密数据的安全和保险的地方，并且也是一种用来运行加密参数的安全和保险的平台。为什么卡中的数据和参数被认为享有相对高的安全性和保险性的原因在于卡的硬件结构和对外的接口。从卡的外部看象一个“黑匣子”，它的功能仅被通过明确的硬件和软件接口访问，并且它能强制特定安全策略的遵守。一方面，对数据的访问能被连接到特定的环境下。从外面对危险数据的访问，如，在公共键过程中的密钥，甚至可能被全部设障。另一方面，智能卡能够运行参数，假如没有它，对于从外面被观察到的个人操作的执行将是可能的。参数本身可能被保护在卡上防止被改变或读出。在某种定向目标的意义上，智能卡能被认为是一种抽象数据，它包含一个明确的接口，它以一种特定的方式运转并且本身能确保特定的完整环境，关于它的状态能被观察到。

基本上，有两种不同类型的智能卡。存储卡仅包含一个串行接口，寻址器和安全逻辑电路和 ROM 和 EEPROM 存储器。这种卡仅执行限定的功能并且为特定的应用而使用。这就是为什么生产它们尤其便宜。以微处理器卡形式生

产的智能卡大体上构成了一个完整的通用的计算机。

生产和供应芯片卡的过程能被分成以下阶段：

—芯片的生产，

—芯片的嵌入，

—卡的印刷

—卡的个人化

—卡的发行。

该过程的每个阶段通常被一个专业公司以特定的操作执行。当芯片被生产时，必须小心以确保好的安全性，尤其当相关的卡有硬线安全逻辑时。为了使生产者执行一个合适的最后的测试，整个存储器必须被自由地访问。仅仅当最后的测试是通过传输码使芯片安全。从那之后，对卡存储器的访问仅对知道传输码的授权实体是可能的。但是在窃取崭新的芯片是没有意义的。授权实体可能是卡个人拥有者或发行者。没有进一步确保安全的功能是要求嵌入和印刷操作。对于相关的公司来说，知道传输码是没有必要的。

通常不是卡生产者而是发行实体（如，银行，电话公司，私人或公众保健机构）放个人的数据进入卡。这个过程被称作是个人化并且知道传输码对于卡的执行是必要的。

卡的发行，即，从发行实体到卡持有者的转移，产生了另一个安全问题。确切的说，仅卡的发行，对于持卡者来说，是以亲自签名和身份证或其它个人证明的产生作为回报，是安全的。确实，通过邮局发送经常是比较便宜的，但它也不是非常安全的。另一个问题是通报 PIN 号码的卡持有者，在这种情况下，也不得不像对卡一样小心。

由于潜在危险的与安全相关的信息放在智能卡控制器提供的存储器中，不仅上述的保护措施不得不被采取，而且另外的保护也需要被提供以防止黑客可能的活动，这些保护措施可能覆盖一张智能卡生命的每个阶段，从卡的生产和延伸通过它的传输并且到已经变的没用的卡的处理。

一种获得访问秘密信息的可能的方法是提供所谓的微分功率分析（DPA）给智能卡控制者，目标是通过分析消耗的功率，关于发生在智能卡控制器中内部操作，得出结论。DPA 是一种新的过程，该程序不仅使得得到纯功能性细节成为可能，而且使得得到存储在完整电路（如，智能卡控制器）当中的内部信

息也成为可能。当一个给定的计算被执行时，该过程的基础是分析，除了 I/O 信号，也有完整电路的电流消耗或在功率供给中的峰值。

当具有 k={1,...,A}个不同操作数（根据计算）的，在时间 t（也就是，也有电流或电压）基础上的模拟功率跟踪 S（k,t）能被总结如下时，分析能被成功的执行：

$$T(i,t)=\sum_{k=1}^{A} p(i,k)\cdot S(k,t)$$ 具有系数 p(i,k),i={0,1,2...}

A 的典型值是 10000。当考虑到在给定的时间 $t=t_1$ 中的不同的功率跟踪 S（k_1,t_1），S（k_2,t_1）和 S（k_3,t_1）时，假如整体电路在这些时间段正在执行相同的操作，而操作数 k={1,...,A}是不同的，微分功率分析仅能被成功的赋予。换句话说，对于成功的 DPA 来说，相同的操作不得不在所有的功率追踪 S（k,t）在相同的时间被执行，详细细节见[1]和[2]。

本发明涉及电路的等级，其中，电路的操作或执行自动的适应可用电压。大多数非同步级电路有这个特性并且许多同步电路也有此特性。有自同步逻辑电路的这种电路的例子是：

—自同步电路，该电路能够通过使用一个在芯片上的延迟线得到它们的定时，例如[6]所描述的，

—含有自同步数据路径，如，一个双轨道数据路径的非同步电路，其中，数据的有效性被加密成数据本身（见[4]和[5]），

—非同步电路，含有所谓的“延迟匹配”数据路径，和所谓的“单轨道”电路或者是其中数据被包在一起的电路（见[3，4，5]）。

这三种形式共有的是电路的正确的功能性操作是不依靠常用的功率供给。电路的执行当然是以一个在电压中的变量的函数变化。

变化的过程已经被用来防止秘密数据被黑掉，尤其是通过测量电流消耗或电压供给。

在对公众公开的申请号为 DE19907575A1 中所描写的是电路装置，该装置是用来对一个具有电压供给源的电子电路提供馈电电流的，该电路装置包含一个控制电流源装置，该控制电流源装置能在提供第一个预定的固定电流和第二个预定的固定电流之间变化，第二个固定电流比第一个固定电流高，并且该控制电流源的输入被连接到供给电压源上而它的输出被连接到能量存储元件和电

子电路上；该电路装置还包含一个提供第一参考电压的第一参考电压源和提供第二参考电压的第二参考电压源，该第二参考电压比第一参考电压高；并且包含一个比较装置，该比较装置将馈电电压和第一和第二参考电压比较，该馈电电压在电子电路和被馈电电流供给的能量存储元件中产生，假如馈电电压超过第二参考电压，该比较装置则改变电流源装置到第一电流源，假如馈电电压低于第一参考电压，该比较装置则改变电流源装置到第二电流源。

通过该过程能够得到的是，对电子电路的馈电电压和供给电压不能依靠发生在电子电路中的操作。在处理器的定时有变化的情况下，不能够使用，而一个复杂和昂贵的电路还被要求。

在欧洲专利申请号为 EP1098472A2 中描写的是一个加密装置和它的应用，它能够减少对 DPA 的磁化率。在这种情况下，包含第一功能的关键码被转换，因此而产生一个作为随机数功能的第一临时关键码。用这个临时关键码一个信息被解密，因此而产生一个改变形式的信息。这种改变的信息被一个第二功能变换以便用这种方式解密。这种解密与用非变换码直接解密是等同的。这种临时关键码被不断的变化以防止 DPA。

另一个用来防止被 DPA 技术袭击的系统是在英国专利号 2345229A 中被揭露的。在这儿，通过使用块密码的运算法则解密一个信息是一个问题。一块一块的信息用一块一块的关键码来解密。在每个解密操作或反复阶段，用这种方法合成的块是不断变化的。对于随机变化的合并它是有益的。

这种方法的一个优点是当码被解密时数据变得可访问。

通过使用在卡上的线圈提高对芯片卡的卡保护在 WO00/10124A1 中被描写。线圈防止电压峰值被不当的删除。这种方法能被提供给非接触卡和接触卡。

在相应的信号波之间的相互关系没被破坏而是仅仅变的模糊。

进一步的方法被放在国际专利申请 WO00/19353A1 中。它所描写的是一个数据载体，尤其是一个芯片卡，该卡包含一个数据处理单元和至少一个非接触的接口，通过它数据处理单元能被连接到一个用来交换数据信号和获得用来操作数据处理单元的电子能量的读/写单元，其中，数据处理单元被构造至少主要来自于逻辑模块，该模块以至少大体上的非时钟模式被操作。

国际专利申请 WO01/08088A1 记载了一种微控制器，该控制器用来防止来自于微控制器的电流消耗以一种非授权方式的决定信息的袭击。这种微处理器

可能，例如被加在一个芯片卡上。微处理器除了包含一些通用的，如用于供给电压（VCC）的接头，用于输入和输出的接头，一个处理器和一个存储器，还包含一个用来变换供给电压到处理器的装置。

然而，由于非同步逻辑电路产生了相关的电源跟踪，被描写的方法不得不被进一步的保护措施支持以使DPA能被成功的防止。

发明内容

因此，本发明的一个目的是详细说明一种一般类型的方法和装置，依靠它，传统的保护措施的缺点能被克服，并且尤其是能够防止通过测量电子电路的电流或电压消耗在电子电路的内部操作上获得信息。

根据本发明的第一方面，提供了一种用于提高电路安全性防止未经授权的访问的方法，所述电路包括自同步电路，其特征在于

-由自同步电路中的数据处理操作产生的信号跟踪被退耦;

-信号跟踪的退耦是通过改变随时间变化的自同步电路或自同步电路中的专用功能单元的时钟频率来实现的，

-时钟频率随时间的变化是通过改变随时间变化的供电电流和/或供电电压来实现的。

根据本发明的另一方面，提供了一种用于提高电路安全性防止未经授权的访问的装置，所述电路包括至少一个自同步电路，其特征在于，用于调节电流的可控制装置(2)被连接到自同步电路（1）的供电电源（3）和自同步电路（1）本身之间。

用于提高电路安全性防止未经授权的访问的方法的一个好处在于在自同步电路中通过数据处理产生的信号跟踪被退耦。

用于提高电路的安全性防止未经授权的访问的一种装置通过以下事实区别，该事实指用于调整电流的可控装置被连接在自同步电路供电电源和自同步本身之间。

根据本发明的方法的优选实施例，用于信号跟踪的退耦的设备通过改变自同步电路或在自同步电路中的独立功能单元的时钟频率来获得。假如时钟频率的时间变化是通过变化在时间基础上的供给电流而得到的，它是有利的，换句话说，通过变化在时间基础上的供给电压而使时钟频率的时间变化是同等可能的。

另外，在根据本发明的方法的最优实施例中的设备，用于随时间变化供电电流或供电电压的变化，而该变化被随机数字生成器控制。

也发现随时间变化的供电电流或供电电压的变化产生的好处通过芯片卡的读/写装置的一部分被获得，其中该部分包括在芯片卡，尤其是智能卡上的自同步电路上，该部分被提供给随着时间变化的电流或提供给随着时间变化的电压。

在根据本发明的装置的最优实施例中，最适合用于调整电流的设备通过数/模转换器被连接到随机数发生器上。

根据本发明的装置的最优实施例，自同步电路是非时钟信号交换逻辑电路形式存在。对于自适应电路，采用具有一个芯片上的延迟线的时钟电路形式是等同可能的。

根据本发明的装置的一个优点是自同步电路是智能卡控制器的一部分。

另外有利的是，用于调整电流的可控装置，供电电源，在需要的地方还有随机数字发生器和数/模转换器是用于芯片卡的读/写装置的部件。

本发明采用了一种新方法，该方法使得使用自同步逻辑，特别是所谓的非时钟信号交换逻辑电路的集成电路，被保护以防止 DPA。在这种情况中自同步逻辑电路的特性的好处通过使用一个特殊供电电源被获得。因此在自同步逻辑电路中的处理发生在无法预料的情况下并且电流的消耗被服务器的噪音所影响以及 DPA 不能被成功的应用。

事实上，本发明有许多优点，尤其是，事实上本发明仅仅通过需要很少的额外部分就能对集成电路给予很大宽度的保护。

截止到现在，与被记载的怎样减少 DPA 的磁化系数的观点相比较，本发明在至少协助或推进防止 DPA 的防范措施方面是一个新的方法。该新的方法中值的注意的一个方面是，与其他大多数建议相比，这是廉价的并且容易实现的。变动供电电压允许自同步逻辑电路运行的快或慢的情况是可以的。当供电电压低的时候，自同步逻辑电路比在正常电压运行时更低。本发明利用通过控制供电电压产生的效果并由此、计算性能，较迟的转换计算的相位。在任何一个电源跟踪中与相位计算相关的结果不再可能。

本发明的力度因此依赖于以下事实，该事实是把给定的数据处理操作和信号模式，如随时间变化的电压峰值模式，联系起来变得相当的困难。因此能被

设想：企图得到测量的数字将允许被成功的应用的 DPA 上升到比固定电压或电流供给高很多的数字。

参考下述的具体实施例通过阐述本发明的各个方面将更加清楚。

附图描述

在附图中：

图 1 显示了电源信号轨迹 S（1，t）和 S（2，t）两个例子。

图 2 显示了用在配有电流调节器的自同步电路中的电源供电装置的电路框图。和

图 3 显示了通过随机数字的电流调节。

具体实施方式

本发明最重要的部分是采用了运行电路或特定逻辑模块的自动调节，以这种方式，分配这些临时被分配的峰值电流给数据处理操作或计算，该计算在相关的时间被执行，变得更加相当困难。

本发明背后的构思是去破坏与数据处理操作相关的电源跟踪信号之间的相关性。图 1 显示了两个不同的电源信号轨迹。对于成功的 DPA，各个电源追踪轨迹相互能被相互排列是非常重要的，在这种方式中，被在不同的电源信号轨迹中计算的相对相位占用的时间段是相同的（例如，C11 对应 C21）。在这种情况下，总和 T（i,t）显示了秘密信息（如上所述）。在图 1 中计算的相位不对应。C_{11} 与 C_{21} 不匹配并且 C_{12} 与 C_{22} 不匹配。

如果不采取措施去阻止 DPA，即使自同步逻辑电路也将产生相关的电源信号轨迹。这意味着，对应于计算的相位相互匹配以及形成 T（i,t）的求和可以被成功的应用。

当使用下述的专用的电源供电时，自同步逻辑电路的性能变的相当的不同。图 2 显示了被提供有适合与它的电压的自同步逻辑电路 1，该电压通过电流调节器 2 来自外部供电电源 3。提供给自同步逻辑电路的供电电压随着时间变化。该变化被随机数字发生器 4 控制，该随即数字发生器通过数 / 模转换器 5 连接到电流调节器 2 上。该数 / 模转化器 5 将数字形式的随机号码转换成产生波动供电电压的模拟控制信号。在图 2 中使用的参考数字和字母如下所述；

1 自同步逻辑电路

2 电流调节器

3 外部供电电源

4 随机数字发生器

5 数/模转换器

ZZ 随机数字

KS 控制信号

NI 输入到电流调节器2的输入供电电压

NO 从电流调节器2输出的输出供电电压

在图3中，相对于随机数字ZZ的输出电压AS曲线被显示，其显示了随机产生数据怎样控制供电电压的例子。期待的效果是波动的供电电压引起自同步逻辑电路运行的更快或更慢。当提供的电压低时，自同步逻辑电路比在正常电压是运行的更慢。本发明利用通过控制供电电压引起的效果并由此而产生的计算性能，后述的计算性能在计算相位中引起转变。结果是在任何电源信号轨迹中的计算相位的相关性不再可能。

本发明不限于所示的实施例和在此的描写。通过组合和修改上述的方式和

特征并由此产生的各种各样的实施例并不超出本发明的范围。

参考资料：

[1] “差动功率分析和相关攻击的引论”.P .Kocher,J.Jaffe,B.Jun.从http://www.cryptography.com/dpa/technical获得

[2] “差动功率分析” P .Kocher,J.Jaffe,B.Jun.高级密码学：密码处理‘99，Springer-Verlag,1999,388-397页

[3] “七巧板结构：用于低功率的异步电路”J.Kessels 和A.Peeters.ADPAS处理，2001年2月，255—260页

[4] “异步电路应用”,C.H.van Berkel,M.B.Josephes 和 S.M.Nowick.IEEE处理，87（2），1999年2月，223—233页

[5] “使用自同步电路的低功率操作和供电电压的自适应换算”,L.Nielsen,C.Niessen,J.Sparso 和 K.van Berkel.IEEE关于在VLSI系统中的传输，1994年9月，391—397页

[6] “用于可变供电电压第功率处理中的有效控制器”，V.Gutnik 和A.Chandrakasan.关于 VLSI 系统的讨论，技术章节的摘要，1996 年，158—159

页

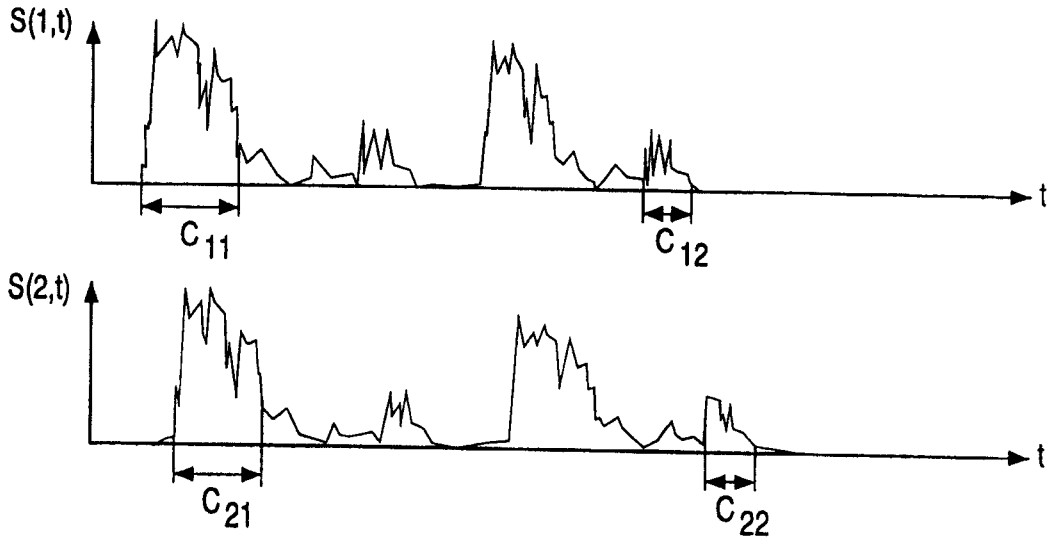


图 1

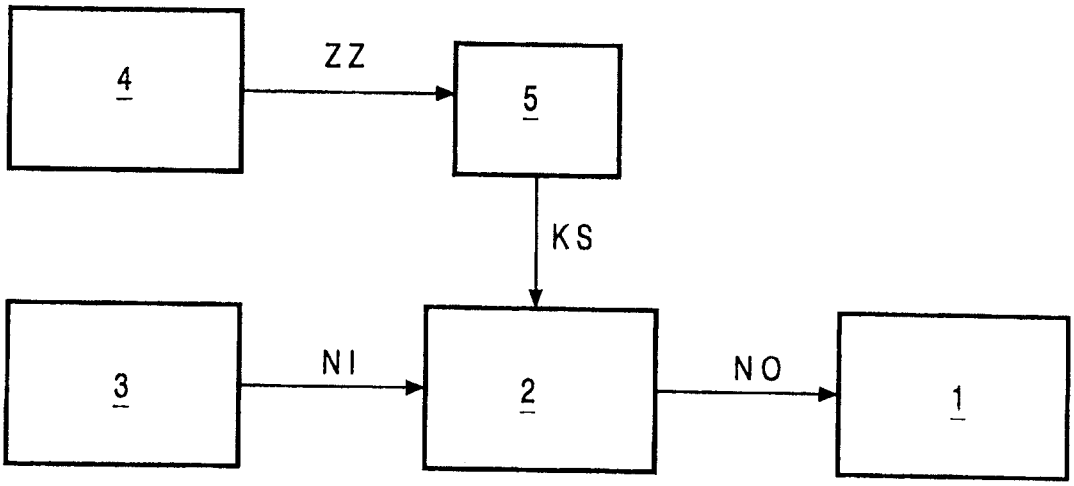


图 2

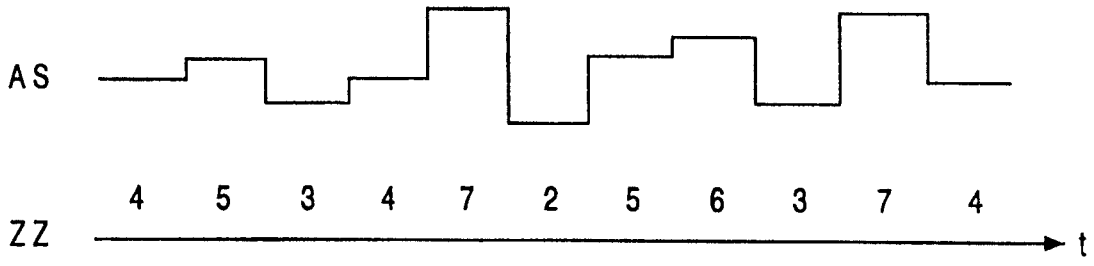


图 3