



[12] 发 明 专 利 说 明 书

[21] ZL 专利号 98811013.X

[45] 授权公告日 2004 年 1 月 14 日

[11] 授权公告号 CN 1134891C

[22] 申请日 1998.9.7 [21] 申请号 98811013.X

[30] 优先权

[32] 1997. 9. 10 [33] FR [31] 97/11210

[86] 国际申请 PCT/FR98/01907 1998.9.7

[87] 国际公布 WO99/13572 法 1999.3.18

[85] 进入国家阶段日期 2000.5.10

[71] 专利权人 内部技术公司

地址 法国圣克里门特里斯普拉瑟斯

[72] 发明人 J·科瓦尔斯基

审查员 杨 蕊

[74] 专利代理机构 中国专利代理(香港)有限公司

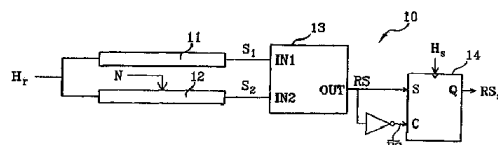
代理人 王 勇 李亚非

权利要求书 1 页 说明书 7 页 附图 3 页

[54] 发明名称 随机信号发生器

[57] 摘要

本发明涉及一种随机信号发生器(10)，它包括用于将电子噪音(N, N1, N2)转换为逻辑信号(RS)的装置(11, 12, 13)，逻辑信号的值依赖电子噪音(N)的随机波动。根据一个实施例，该发生器(10)至少包括两个具有初始平衡时间常数(T)的延迟线(11, 12)。这两个延迟线(11, 12)在其输入端接收参考脉冲信号(Hr)，及至少一个延迟线(11, 12)接收引起其时间常数(T)波动(ΔT)的电子噪音(N1, N2)。两个脉冲信号(S1, S2)之间的时滞由电路(13)检测，以输出一个逻辑信号(RS)，其值是两个脉冲信号(S1, S2)之间相对位移的函数。有利地，电子噪音(N1, N2)是在接地面的两个点(GND1, GND2)上或在电源面的两个点(PV1, PV2)上提取的差分噪音。



1. 随机信号发生器，它被设置用于将电子噪音转换为逻辑信号，该逻辑信号的值依赖电子噪音的随机波动，其特征在于它包括：

5 a) 用于至少将一个电子噪音转换为来自同一参考脉冲信号的至少两个脉冲信号的时滞的电路，所述用于转换的电路包括：

-至少两个具有初始平衡时间常数的延迟线，在其输入端接收所述参考脉冲信号；以及

-将至少一个电子噪音注入至少一个延迟线，以使其时间常数波动的电路，以及

10 b) 具有触发器功能的电路，用于输出逻辑信号，该逻辑信号的值是两个脉冲信号相对滞后的函数。

2. 根据权利要求1的发生器，其中：

-延迟线包括级联的逻辑门，及

15 -至少一个延迟线的至少一个逻辑门接收引起其转换时间常数波动的电子噪音。

3. 根据权利要求2的发生器，其中电子噪音被施加在逻辑门的接地端子或电源端子上。

4. 根据权利要求2的发生器，其中电子噪音被施加在与逻辑门输出端连接的缓冲电容器的接地端子上。

20 5. 根据权利要求1的发生器，其中电子噪音是在接地面的两个点上提取的差分噪音。

6. 根据权利要求1的发生器，其特征在于：电子噪音是在电源面的两个点上提取的差分噪音。

25 7. 根据权利要求1的发生器，其特征在于：该发生器包括至少两个不同的振荡器，以提供两个不相干的振荡信号，这些振荡信号作为互补噪音被注入到延迟线中。

8. 根据权利要求1的发生器，其特征在于：一个延迟线的输出端通过逻辑门被连接到其输入端。

30 9. 根据权利要求1的发生器，其中该发生器包括用于以同步信号速度采样逻辑信号的电路。

随机信号发生器

本发明涉及一种随机信号发生器。

- 5 在电子领域中，尤其在芯片卡领域中，往往需要设置一个装置，它能够产生随机逻辑信号、即包括具有“1”或“0”的位的随机序列的信号。

例如，在芯片卡阅读器的传统鉴别程序中，芯片卡发送一个上述类型的、譬如包括 16 或 32 位的随机信号或“ALEA”给阅读器。芯片卡通过具有密钥 K_s 的鉴别函数 F_{ks} 计算随机转换结果 $R=F_{ks}$ (ALEA)。终端本身执行相同计算并向卡回送一个结果 R' 。如果结果 R 及 R' 相同，卡将视终端为通过鉴别的并同意进行所请求的交易。

在现有技术中，一些有线的随机信号发生器具有包括有限数目内部状态的逻辑机（单元自动装置）。例如，其涉及移位寄存器，它的一些位通过异或门送回输入端。根据一个初始内部状态，借助时钟信号启动逻辑机，并在每个时钟脉冲时抽取逻辑机的一个内部位。

这些逻辑机的缺点是，它们通常具有由它们产生的位序的高重复率，以及涉及“1”和“0”输出的统计偏差。为了克服该缺点，必须设计具有很大大数内部状态的逻辑机，理论上，理想的是逻辑机具有无限数目的内部状态。但是，这种方案与对随机信号发生器简单化、低成本及低损耗的要求背道而驰。

此外，公知了使用电子噪音作为随机信号源的随机信号发生器。事实上，电子噪音由于其特性实际是随机的。另外，由于在电子元件中的热电子扰动及晶体管开关噪音，在所有电子电路中存在噪音。因此，易于实现电子噪音源，例如，借助电子元件，或更简单地，提取在电路内部存在的电子噪音。

图 1 概要地表示根据电子噪音源 N 工作的一个传统的随机信号发生器 1。该发生器 1 包括一个理论增益无限大的比较器 2，在其正输入端接收电子噪音 N 及在其负输入端接收一个参考电压。比较器 2 的输出端输出一个随机逻辑信号 RS 。信号 RS 被施加于一个采样电路 3，后者与时钟信号 H_s 同步地输出随机信号 RS_s 。电路 3 例如是一个由时钟 H_s 的前沿触发的 S-C 触发器。同步触发器 3 从其输入端 S （置

位)接收信号 RS 及通过反相门从其输入端 C (清除)接收反相信号 /RS。信号 RSs 从 S-C 触发器的输出端 Q 提取。

图 2 表示发送器 1 的信号 RS, Hs 和 RSs, 及图 3 噪音 N 相对参照电压 Vref 的波动。信号 RS 在逻辑值 0 及逻辑值 1 (放大器的饱和电压)之间作为噪音 N 的幅值相对参考电压的函数随机地振荡。由于噪音 N 实际上是随机的, 信号 RS 同样是随机的。在时钟 Hs 的每个前沿时, 同步信号 RSs 复制信号 RS 的值并保持该值直到下一时钟前沿为止。信号 RSs 也是与时钟 Hs 同步的一个随机位序, 例如图 2 中所示的位序 “11010110001”。

10 实践表明, 图 1 中的发生器 1 具有各种缺点, 一方面是比较器 2 的电损耗, 另一方面是对作为温度函数出现在放大器 2 中的电压偏差的补偿困难。如图 4 所示, 这些偏差在放大器 2 中引起噪音 N 相对参考电压 Vref 的移动, 由此使信号 RS 处于被锁定在值 1 或 0 上。

15 专利申请 FR 2 390 047 描述了一种随机信号发生器, 其中将电子噪音的幅值与一参考电压相比较, 以产生一个具有随机脉冲宽度的逻辑信号。其工作原理与刚描述的相一致。

因此, 本发明的目的是提供一种将电子噪音转换为随机逻辑信号的装置, 它具有高的工作稳定性及对温度的敏感性小。

20 本发明的一个更具体的目的是该装置具有低的电损耗及实施起来简单。

为了达到该目的, 本发明的构思是: 将电子噪音转换为来自同一参考脉冲信号的两个脉冲信号的时滞, 然后将该时滞转换为一个逻辑信号。

25 专利 US 4 183 088 描述一个包括 14 个随机发生器的随机信号发生器, 它们的输出施加到一个移位寄存器的 14 个输入端。该移位寄存器的内容即随机位逐位地与一个参考移位寄存器的内容相比较, 以产生随机信号。这 14 个随机发生器中每个的工作相应于前述的原理。其工作还具有一个比较脉冲信号的步骤, 但该脉冲信号不是来自于同一参考脉冲信号。

30 于是, 实质上, 本发明提供了一种随机信号发生器, 它被设计用于将电子噪音转换为逻辑信号, 逻辑信号的值依赖电子噪音的随机波动, 该随机信号发生器包括: 用于至少将一个电子噪音转换为来自同

一参考脉冲信号的至少两个脉冲信号的时滞的装置,及用于输出逻辑信号的装置,该逻辑信号的值是两个脉冲信号相对滞后的函数。

根据一个实施例,用于至少转换一个电子噪音的装置至少包括:
5 两个具有初始平衡时间常数的延迟线,在其输入端接收参考脉冲信号;及一个至少将一个电子噪音注入至少一个延迟线,以使其时间常数波动的装置。

根据一种实施例,延迟线包括级联的逻辑门,及至少一个延迟线的至少一个逻辑门接收引起其转换时间常数波动的电子噪音。

根据一种实施例,电子噪音被施加在逻辑门的接地端子或电源端
10 子上。

根据一种实施例,电子噪音被施加在与逻辑门连接的缓冲电容器的接地端子或电源端子上。

有利地,电子噪音是在接地面的两个点上提取的差分噪音。

有利地,电子噪音是在电源面的两个点上提取的差分噪音。

15 根据一种实施例,该发生器包括至少两个不同的振荡器,以提供两个不相干的振荡信号,这些振荡信号作为互补噪音被注入到延迟线中。

根据一种实施例,一个延迟线的输出端通过逻辑门被连接到其输入端,以形成输出参考脉冲信号的振荡器。

20 根据一种实施例,该发生器包括用于以同步信号速度采样逻辑信号的装置。

本发明的这些及其它的特征和优点在以下参照附图对根据本发明的随机信号发生器各实施例的说明中将会更详细地阐明,这些实施例的说明是以非限制性方式给出的,附图为:

25 -图 1 是已被描述的传统随机发生器的电子电路图;

-图 2 表示已被描述的图 1 的发生器中出现的信号;

-图 3 及 4 表示已被描述施加于图 1 中发生器的电子噪音及参考电压;

-图 5 以框图形式表示根据本发明的随机发生器;

30 -图 6 表示图 5 的发生器中出现的各种信号;

-图 7 至 10 表示图 5 中以框图形式所示的根据本发明的延迟线的实施例;

-图 11 是图 5 的发生器中一个单元的电路图。

图 5 表示根据本发明的随机信号 RS 的发生器 10。如上面已指出的，本发明的构思是将电子噪音转换为来自同一参考脉冲信号的两个脉冲信号的时滞，然后将该时滞转换为一个逻辑信号。

5 于是，发生器 10 包括两个延迟线 11 和 12，它们在其输入端接收参考脉冲信号 Hr，及各自输出一个对信号 Hr 的延迟时间为 T 的信号 S1，S2。起初，延迟线 11，12 是平衡的并各具有相同的时间常数 T。因此，通常，信号 S1 及 S2 是同步的并以相同延时 T 复制信号 Hr。根据本发明，将噪音 N 注入到至少一个延迟线、如延迟线 12 中，以致对其时间常数修
10 改了一个随机值 Δt ，根据噪音的幅值该值为正或负。

由于在延迟线 12 中注入噪音 N 而产生位移的脉冲信号 S1，S2 被分别传送到电路 13 的输入端 IN1，IN2。电路 13 在其输出端 OUT 上输出一个逻辑信号 RS，该信号的瞬时值是信号 S1，S2 位移方向的函数。作为选择，然后随机信号 RS 由 S-C 类触发器 14 以时钟信号 Hs 的速率采样，
15 该触发器的输出端 Q 输出同步随机信号 RSs，或 alea。

随机信号发生器 10 的工作用图 6 来描述，该图表示信号 Hr，S1，S2，RS，Hs 及 RSs。可以看到，信号 S2 由延迟线 12（受到噪音）输出，及有时对信号 S1 超前 $+\Delta t$ ，有时对其滞后 $-\Delta t$ 。电路 13 在每次接收到信号 S1 或 S2 的一个脉冲时被触发。当在脉冲 S1 以前接收到脉冲 S2 时，
20 电路 13 将其输出端 OUT 置 1（信号 RS）。当在脉冲 S2 以前接收到脉冲 S1 时，电路 13 将其输出端 OUT 置 0。因此，信号 RS 是其值取决于信号 S1，S2 位移方向的随机信号。同步信号 RSs 在采样时钟 Hs 的每个前沿上复制信号 RS。

现在将参照图 7 至 9 来描述延迟线 11，12 的一个简单实施例及在至少一个延迟线中注入噪音的例子。
25

在图 7 中，延迟线 11 及 12 各分别包括两个级联的反相器门 20，21 及 22，23，并为严格相同的。在制造工艺的限制上，门 20 和门 22 严格相同，及门 21 和门 23 严格相同。门 20 的输出端连接在缓冲电容器 24 的一个端子上，该电容器的另一端子连接到地。该电容器 24 附加于门
30 20 的输出寄生电容器并可以校正延迟线 11 的时间常数 T。延迟线 12 的门 22 的输出端设有一个与电容器 24 严格相同的缓冲

电容器 25。门 20 至 23 由取自供电平面上同一点 PV1 的电压 V_{cc} 供电，并连接到接地平面的同一接地点 GND1。电容器 24 的接地端子连接到接地点 GND1，而电容器 25 的接地端子连接到取自接地平面另一处的接地点 GND2。

- 5 根据本发明，差分电子噪音 N1 被注入到电容器 25 的接地端子。在这里，噪音 N1 等于接地点 GND2 及 GND1 之间的电压差，并引起两个延迟线 11, 12 的时间常数的随机不平衡。延迟线 11, 12 的输出端上的脉冲信号 S1, S2 出现随机位移，如图 6 所示。

- 注入噪音的另一例子被表示在图 8 上。在该图上，除延迟线 12 10 的门 23 外所有的元件被连接在接地点 GND1 上，门 23 的接地端子连接到接地点 GND2。因此，这里差分噪音 N1 被注入到门 23 的接地点，并随机地改变了该门的低（转换到 0）转换阈值电压 V_{TN23} 。该阈值电压 V_{TN23} 的随机改变表现为延迟线 12 时间常数的随机不平衡。此外，所有逻辑门的电源端子连接在供电平面的点 PV1，但门 20 除外，15 其电源端子连接取自供电平面另一处的另一供电点 PV2 上。因此，差分噪音 N2 被注入到门 20 的供电点，并随机地改变了该门的高（转换到 1）转换阈值电压 V_{TP20} ，这就导致延迟线 11 及 12 之间附加的延时不平衡。

- 根据图 9 所示的实施例，将刚才描述的噪音 N1 及 N2 的注入相组合。并且，门 23 及电容 25 的接地端子接收噪音 N1，而门 20 的电源20 端子接收噪音 N2。此外，电容 26 并联地附加在延迟线 11 的电容 24 上及电容 27 并联地附加在延迟线 12 的电容 25 上。电容 26 及 27 相同，但在它们的接地端子上接收由具有不同固有频率的不同振荡器 OSC1, OSC2 输出的振荡信号 H1, H2。因此，信号 H1 将附加噪音 N3 25 注入延迟线 11，及信号 H2 将附加噪音 N4 注入延迟线 12。所产生的差分噪音是一个非随机的周期性噪音，但它具有足够长的周期时间（两个振荡器 OSC1, OSC2 固有频率的倍数）。

- 实际上，根据本发明的延迟线可为各种另外实施变型及改进的对象。尤其是，虽然为了简化说明起见，在图 7 至 9 上所示的延迟线 11, 30 12 仅包括两个级联的反相器门，但显然，该数目可以增大及可根据所需获得的时间常数及逻辑门的转换特性来选择。此外，可以设置多个噪音注入点。

此外, 应该指出, 借助逻辑门、尤其是 CMOS 门来实现延迟线 11, 12, 可以使根据本发明的发生器 10 的损耗得以控制。例如, 在其输出端连接电容 24, 26 及 25, 27 的门 20 和 22 可借助低输出功率的电流发生器 28, 29 被供电, 如图 9 所示 (也可设计其中包括的 PMOS 晶体管漏极的尺寸, 以便限制转换电流)。并且, 由于 CMOS 门仅在转换时消耗电流, 则可在门 21 及 23 的输出端及其输入端之间设置作为加速器的 PMOS 晶体管 30, 31, 如图 9 所示。

最后, 根据图 10 上所示的一个有利实施例, 一个延迟线, 这里为延迟线 12, 其输出通过级联的反相器门 32, 33, 34 返回到其输入端。该组合形成一个振荡环 OL, 它能“就地”地发生施加于延迟线 11, 12 的参考信号 Hr。在图 10 上, 延迟线 12 的输出通过一个受发生器启动信号 ACTIV 驱动的 NAND 门 32 及两个反相器门 33, 34 返回到输入端。振荡环的反相器门总数目根据传统方式应为奇数。

此外, 环 OL 的一个反相器门的输出端, 如门 33 的输出端可包括一个可变速缓冲电容器 Cv。该电容器 Cv 包括相并联的一个电容 35 及可借助 MOS 晶体管通过信号 A, B, C, D 控制转换的电容 36 至 39。这些信号可从集成电路的任何点上提取, 例如从地址母线或数据母线、或发生器 10 的输出端提取。电容 Cv 的改变将引起振荡环 OL 的谐振频率的改变。

图 11 表示图 5 中电路 13 的一个实施例。该电路 13 包括两个存储式反相器 50, 51, 它们的输入端分别通过两个晶体管 52, 53 接地。参考信号 Hr 通过一个反相门控制晶体管 52, 53。反相器 50, 51 的输出端分别驱动 S-C 类触发器 54 的输入端 S 及输入端 C。触发器 54 的输出端 Q 输出信号 RS, 及输出端/Q 输出反相信号/RS。反相器 50 的输出端通过两个串联晶体管 55, 56 接地。晶体管 55 由信号 S1 控制及晶体管 56 由反相器 51 的输出端控制。对称地, 反相器 51 的输出端通过两个晶体管 57, 58 接地。晶体管 57 由信号 S2 控制及晶体管 58 由反相器 50 的输出端控制。

当反相器 50 的输出端转换到 0 时输出端 RS 转换到 1, 及当反相器 51 的输出端转换到 0 时输出端 RS 转换到 0。在参考信号 Hr 的每个周期中, 通过信号 Hr 转换到 0 使反相器 50, 51 的输出端置 1, 信号 Hr 导前信号 S1, S2 的脉冲。在接着的等待周期中, 触发器 54 由

此在电路 13 的输出端上保持信号 RS 的当前值。然后，如果脉冲 S1 在脉冲 S2 之前出现，脉冲 S1 使晶体管 55 闭合，反相器 50 的输出端转换到 0，及信号 RS 转换到 1（或保持 1，视在先的值而定）。相反地，如果脉冲 S2 在脉冲 S1 之前出现，脉冲 S2 使晶体管 57 闭合，反相器 51 的输出端转换到 0，及信号 RS 转换到 0（或保持 0）。可以看出，该电路的结构是这样的，即存储式反相器 50，51 的输出端不会同时变到 0，晶体管 56，58 中的一个被输出为 0 的第一反相器变为不导通。因此，反相器 50，51 可能的三种状态为：

- “11”：接收到信号 Hr 到 0 的脉冲（初始阶段），
 - 10 - “01”：在脉冲 S2 之前接收到脉冲 S1，或
 - “10”：在脉冲 S1 之前接收到脉冲 S2，
- 并分别对应于：保持信号 RS 的在先值，信号 RS 转换到（或保持）1，信号 RS 转换到（或保持）0。

本领域的技术人员可清楚地看到，对本发明易于作出各种实施变
15 型及改进。尤其是，实际上，存在着用于在无电子噪音情况下获得对称性极佳的延迟线的各种方法。这些方法涉及本领域的技术人员的技术知识，为简明起见，不再描述。此外，可注意到，能设置多对并列延迟线，每对具有各自的振荡环或一个公共振荡环，以便按时钟速度输出包括多个并行位的随机字。此外，虽然已公开的根据本发明的延
20 迟线是作为逻辑门构成的，但显然，这些延迟线可用各种其它公知方式实现。最后，应该指出，根据本发明的随机发生器由于其简单及电流损耗低，特别适用于芯片卡的集成电路，尤其适用于由电磁感应供电及具有弱能源的无触点芯片卡的集成电路。

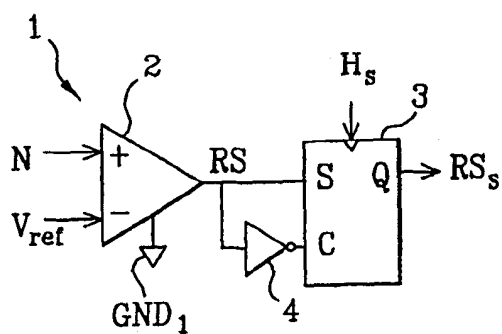


图 1

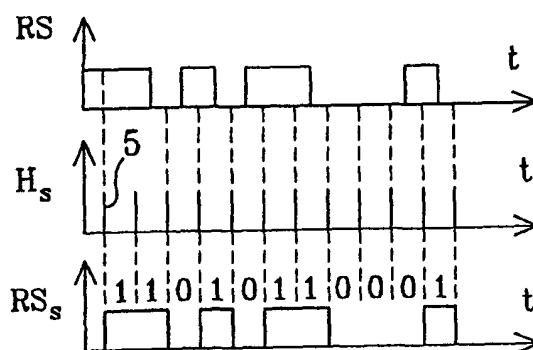


图 2

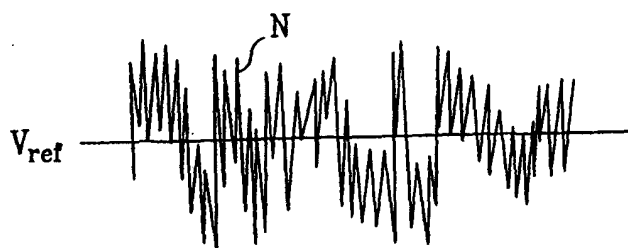


图 3

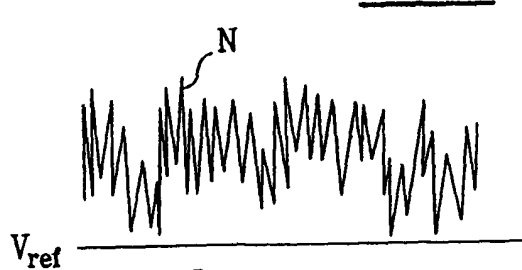


图 4

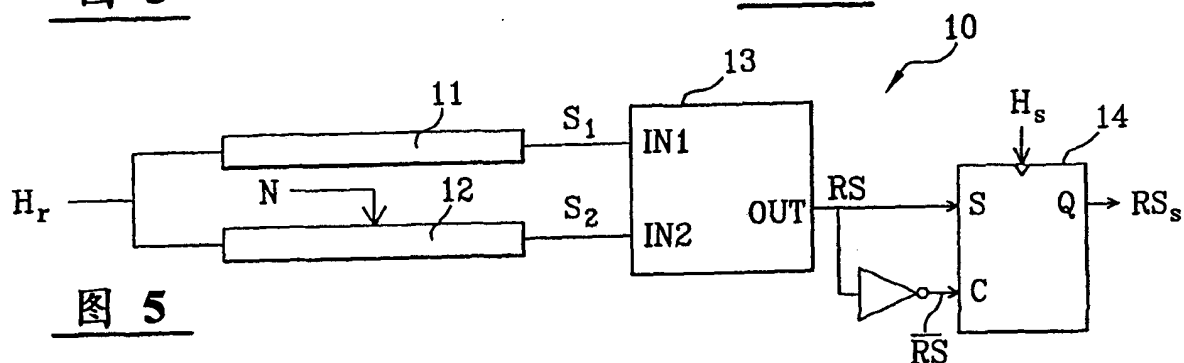


图 5

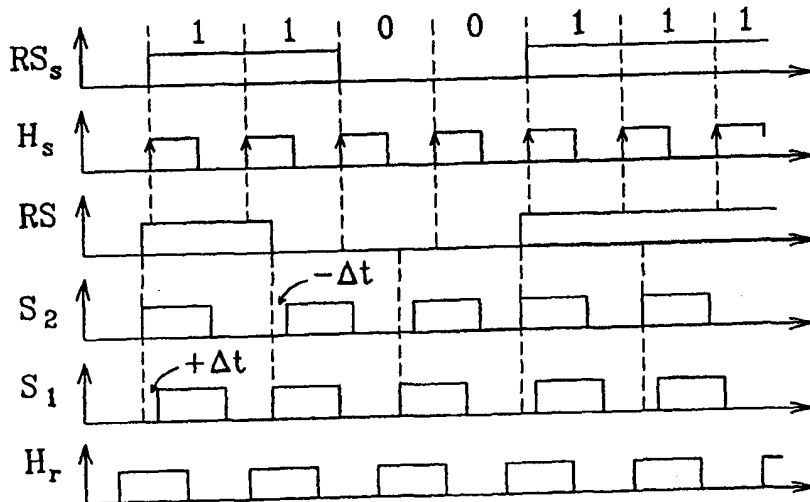
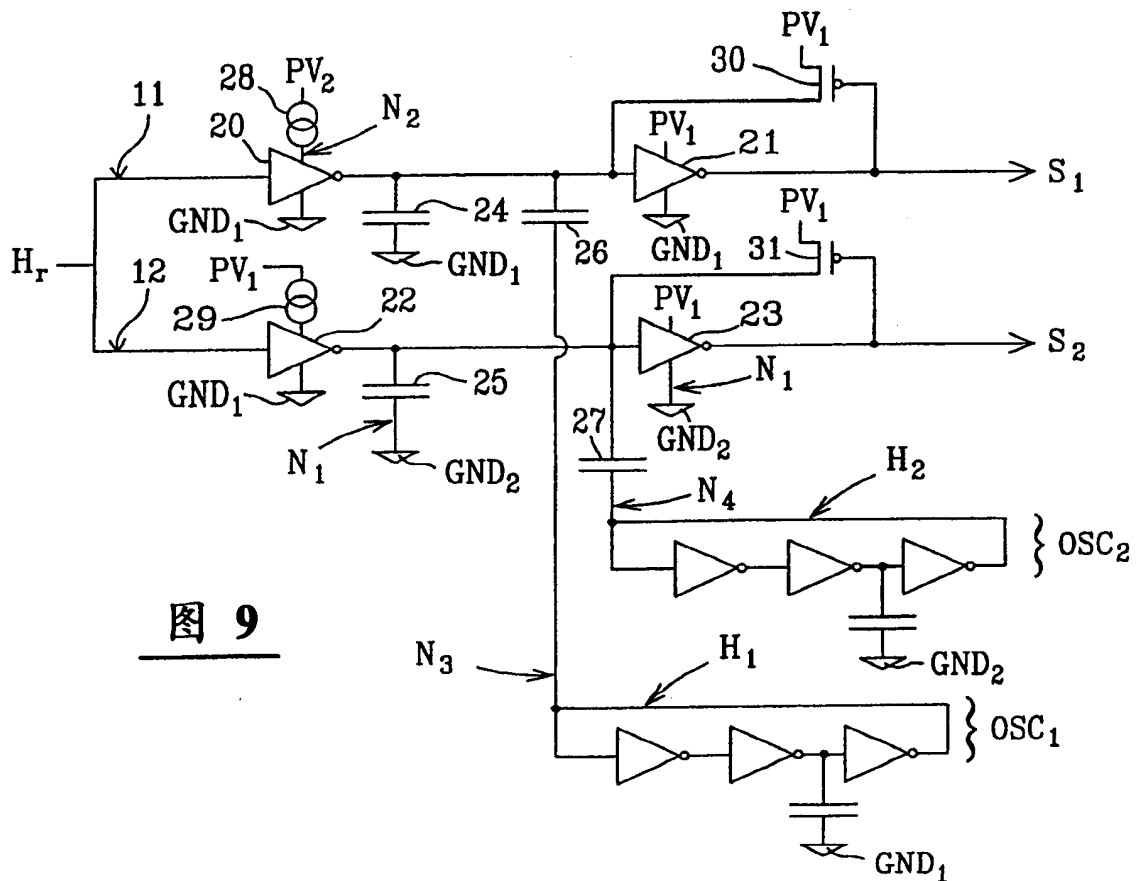
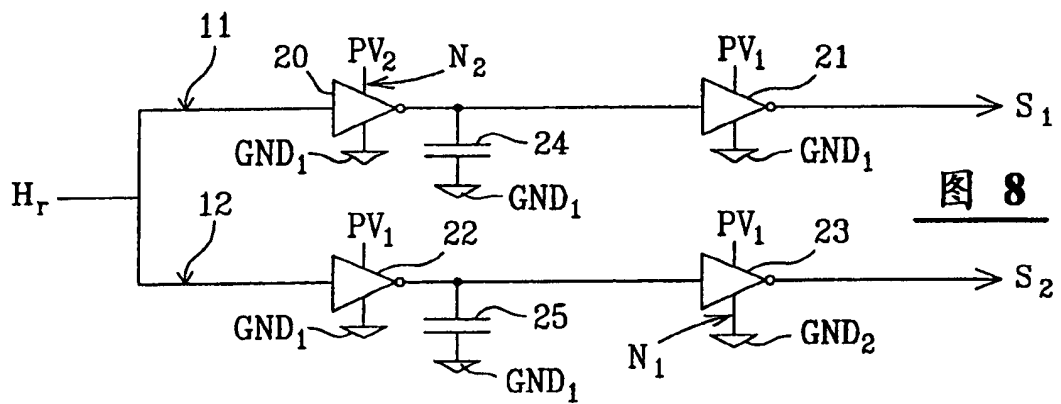
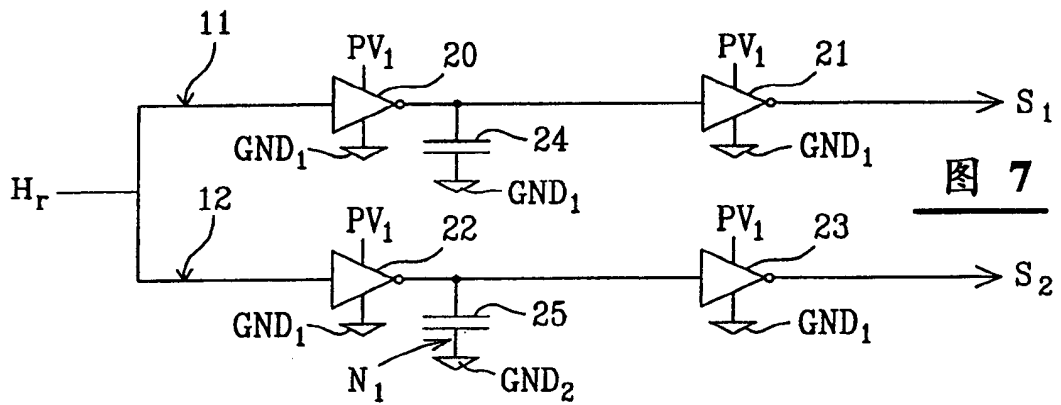


图 6



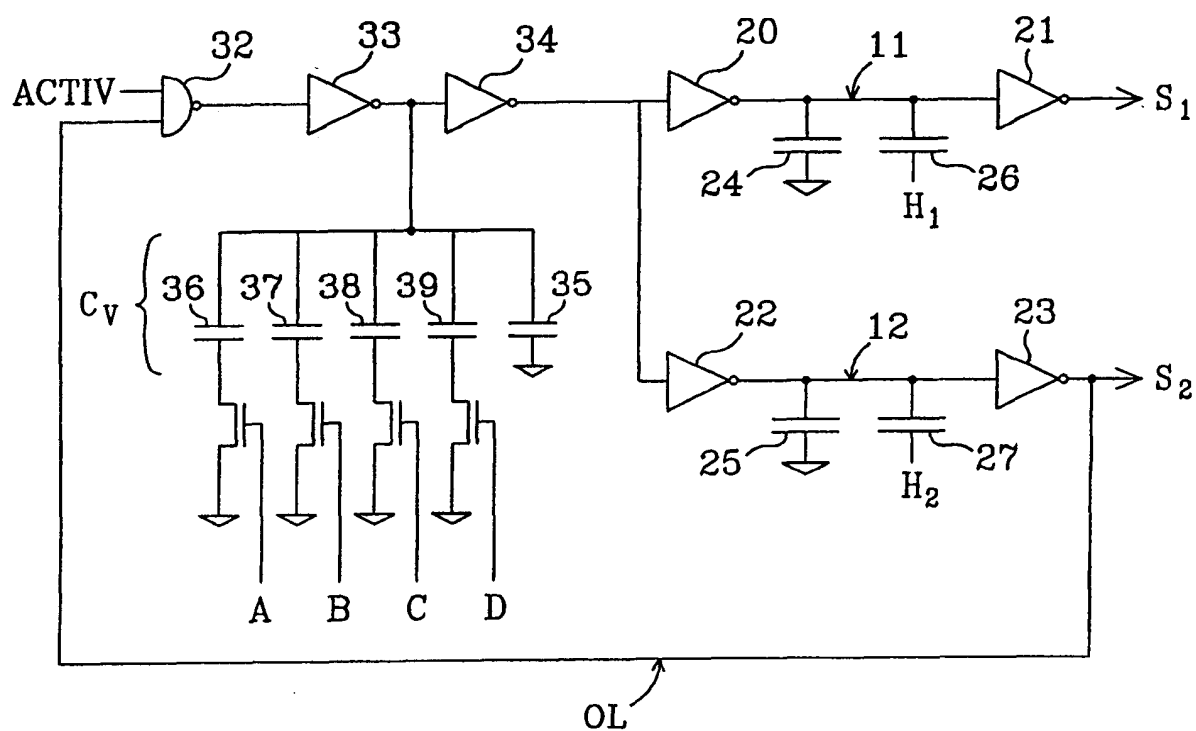


图 10

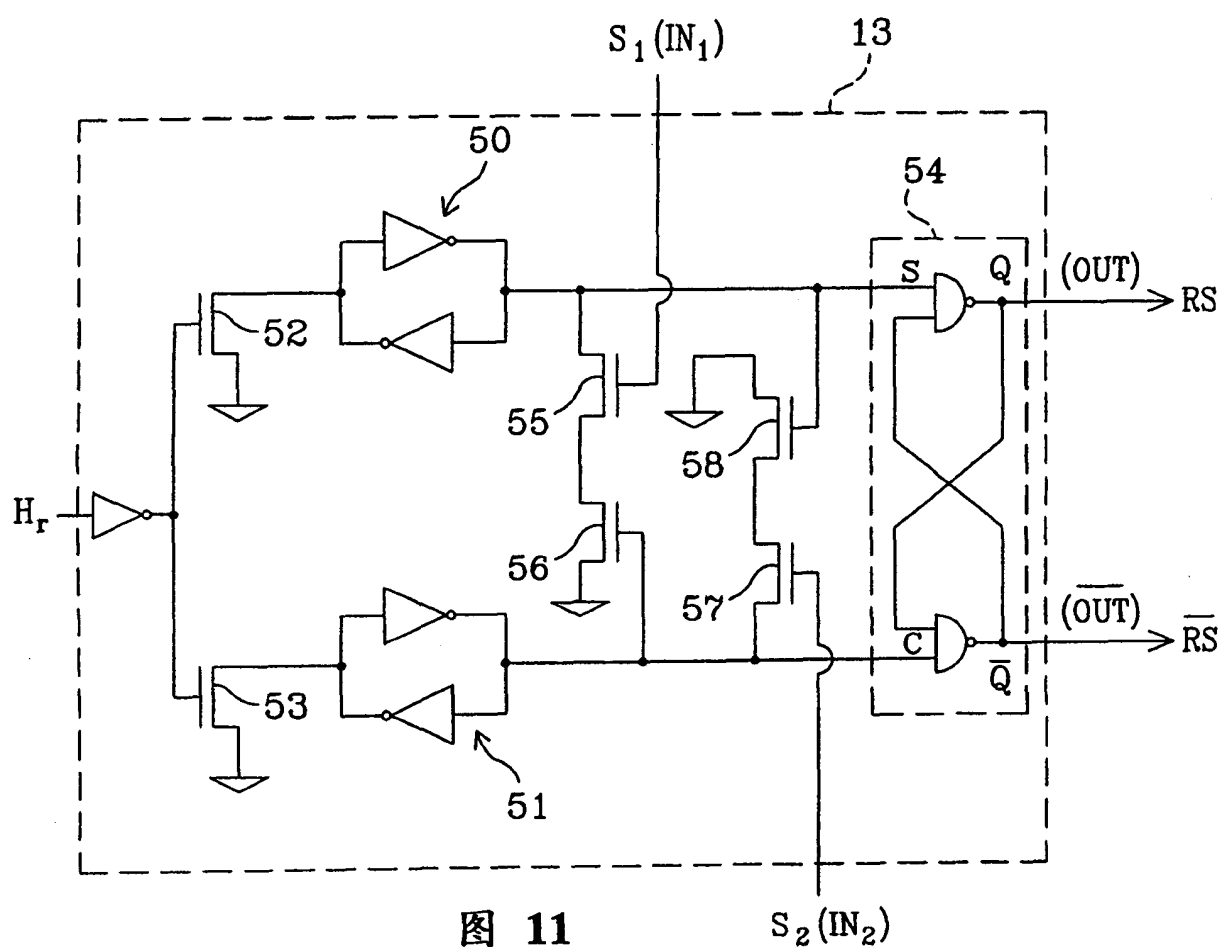


图 11