[19]中华人民共和国国家知识产权局

[51]Int. Cl[6]
H03K 3/84
H03B 29/00

[12]发明专利申请公开说明书

[21]申请号 97194365.6

[43]公开日 1999年5月26日

[11]公开号 CN 1217834A

[22]申请日 97.4.25 [21]申请号 97194365.6
[30]优先权
[32]96.5.6 [33]DE [31]19618098.8
[86]国际申请 PCT/DE97/00831 97.4.25
[87]国际公布 WO97/42706 德 97.11.13
[85]进入国家阶段日期 98.11.3
[71]申请人 西门子公司
地址 联邦德国慕尼黑
[72]发明人 H·-H·维曼

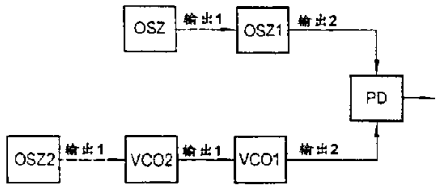
[74]专利代理机构 中国专利代理(香港)有限公司
代理人 马铁良 王忠忠

权利要求书1页 说明书3页 附图页数1页

[54]发明名称 用于产生随机位序列的电路装置

[57]摘要

用于产生随机位序列的电路装置,具有一个第一振荡器(OSZ1)和一个第二振荡器(VCO1),其输出端与准备提供随机位序列的相位检测器(PD)的输入端相连,其中第二振荡器(VCO1)被频率调制。



ISSN1008-4274

权　利　要　求　书

1. 用于产生随机位序列的电路装置，具有一个第一振荡器（OSZ1）和一个第二振荡器（VCO1），其输出端与准备提供随机位序列的相位检测器（PD）的输入端相连，其中第二振荡器（VCO1）被频率调制。

2. 如权利要求 1 的电路装置，其特征在于，第二振荡器（VCO1）作为电压控制的振荡器构成，并且通过第三振荡器（VCO2）控制。

3. 如权利要求 2 的电路装置，其特征在于，第三振荡器（VCO2）作为电压控制的振荡器构成，并且通过第四振荡器（OSZ2）控制。

4. 如上述权利要求之一的电路装置，其特征在于，相位检测器（PD）通过移位寄存器构成。

5. 如权利要求 4 的电路装置，其特征在于，移位寄存器被反馈。

6. 如权利要求 2－5 之一的电路装置，其特征在于，第一振荡器（OSZ1）和第二振荡器（VCO1）大约具有相同的频率，第三振荡器（VCO2）和第四振荡器（OSZ2）以另一频率振荡。

7. 如上述权利要求之一的电路装置，其特征在于，第一振荡器（OSZ1）作为电压控制的振荡器构成并且被频率调制。

说　明　书

用于产生随机位序列的电路装置

在许多数据处理过程中，尤其是在加密技术中，位序列需要随机分配位序列。这种确定随机位序列的长度能够作为随机数而定。

一般应用所谓的伪随机数，其通过反馈的移位寄存器产生。伪随机数是随机的，并且与较大的数相继的伪随机数发生器不能连接到下一个值。其不含有与所应用的移位寄存器的长度有关的周期性。另外移位寄存器的输出数据与输入数据和移位寄存器的结构有关。

到现在为止还不知道数字电路中的有效随机数。

上述发明的任务在于给出用于产生有效随机位序列的电路装置。

此任务通过权利要求 1 的电路装置解决。本发明有利的改进在从属权利要求中给出。

在本发明的电路装置中，输出信号的相应相位分析两个振荡器的数字。一个振荡器以近似恒定的频率振荡，而另一个振荡器以该频率调制。量化噪声支配了所满足的频率偏移。所以所存在的随机位序列能够作为随机数应用。

在本发明的改进中以尤其有利的方式通过其他的优选以另一频率振荡的振荡器进行频率调制。其输出信号优选的含有锯齿波。另一振荡器在本发明的另一改进中能够通过附加的振荡器进行频率调制并且此振荡器能够调制。

频率调制的振荡器以有利的结构作为电压控制的振荡器实现，以致其能够通过另一振荡器的输出信号进行直接控制。

相位的检测能够有利的尤其是以简单的方式通过移位寄存器实现，其数据输入端优选的通过频率调制的振荡器信号并且其时钟输入端通过振荡器信号恒定频率的调制。

具有恒定频率的振荡器在本发明的改进中通过频率调制的振荡器替换。

在本发明的有利改进中移位寄存器进行反馈。

下面通过附图借助于实施例详细解释本发明。图为

图 1 是本发明的电路装置的原理图，

图 2 是电压控制的振荡器的原理图。

按照图 1 相位检测器 PD 的第一输入端通过第一振荡器 OSZ1 的第二输出信号输出 2 加载。相位检测器 PD 的第二输入端通过第一电压控制振荡器 VCO1 的第二输出信号输出 2 加载。

振荡器 OSZ1、VCO1 的第二输出信号输出 2 是矩形波。振荡器 OSZ1、VCO1 提供具有大约锯齿形状的输出信号输出 1。

第一电压控制振荡器 VCO1 通过第二电压控制的振荡器 VCO2 控制，此实际通过另一电压控制的振荡器，其没有示出而是通过划线标明，通过具有第一输出信号输出 1 的自由振荡的第二振荡器 OSZ2 控制。原则上第一振荡器 OSZ1 作为电压控制的振荡器构成，其通过一个或者一链的多个振荡器或者电压控制的振荡器以其输出信号输出 1 控制。这在图 1 中通过划线的振荡器 OSZ 标明。

相位检测器 PD 以有利的方式通过专业人员熟悉的移位寄存器构成。在此以优选的方式第一振荡器 1 的第二输出信号输出 2 传输到移位寄存器的数据输入端，而第一电压控制振荡器的第二输出信号输出 2 传输到移位寄存器的时钟输入端。原则上也是能够的，第一电压控制振荡器 VCO1 的第二输出信号输出 2 施加到数据输入端，并且第一振荡器 OSZ1 的第二输出信号输出 2 施加到起相位检测器 PD 作用的移位寄存器的时钟输入端。

作为相位检测器 PD 的移位寄存器在本发明的有利改进中能够反馈的构成。在此移位寄存器的输出信号通过数据输入信号进行逻辑转换并且然后传输到移位寄存器的输入端。另外能够将移位寄存器的中间抽头信号逻辑的转换并且反馈到输入端。

图 2 示出了数字电压控制的振荡器的原理结构图。反相器 INV 的输出端通过电容 C 与大地端子相连并且另外与作为史密特触发器构成的比较器 ST 的输入端相连。比较器 ST 的输出端输出 2 提供大约矩形的信号并且反馈到反相器 INV 的输入端。如果例如反相器 INV 的输出状态是“1”，电容 C 被充电。如果电容 C 上的电压超过了比较器 ST 的阈值，如此切换：在也构成振荡器输出端的输出端输出 2，表现为逻辑“1”。其可以反馈到反相器 INV 的输入端，以使该状态在输出端变为逻辑“0”。以此重新从电容 C 放电，以致比较器 ST 根据已知的时间重新切换。在此存在一个周期性的振荡状态，其频率主要通过电容 C 的电容量和反相器 INV 的负载电路中的电阻确定。此电阻能够可控制的构成，例如图 1 所示的 p^- 和 n

- MOS 晶体管，其分别接在正的电源电压端子和特有的反相器的 p - MOS 晶体管之间以及反相器的 n - MOS 晶体管和负的电源电压端子之间。此可控制的反相器 INV 必需接入有两个互补的控制信号输入 1、输入 2。

电压控制振荡器的基频通过电容 C 的电容量的大小确定。频率的变化借助于控制信号输入 1、输入 2 通过反相器 INV 的负载的电阻的变化实现。

另外含有一个输出端，其提供具有大约锯齿波形的第一输出信号输出 1，并且与电容 C 相连。

通过本发明的电路装置能够产生有效的随机位序列，其作为随机数能够应用在加密技术的数据处理过程中。

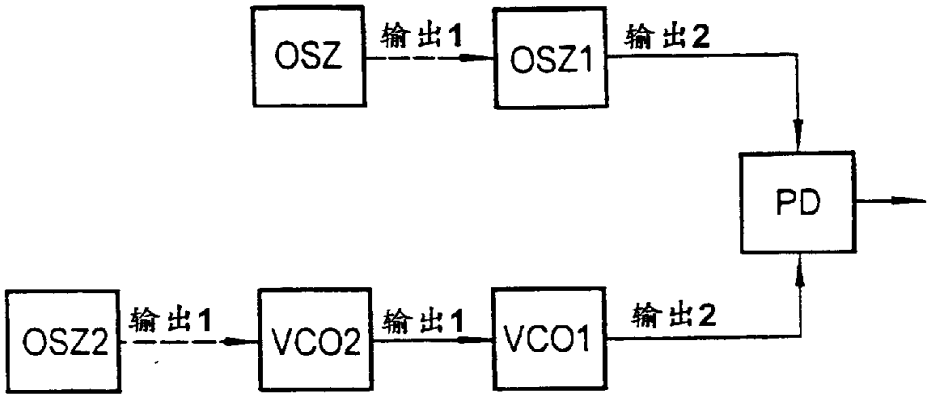

OSZ
输出1
OSZ1
输出2
PD
OSZ2
输出1
VCO2
输出1
VCO1
输出2

图 1

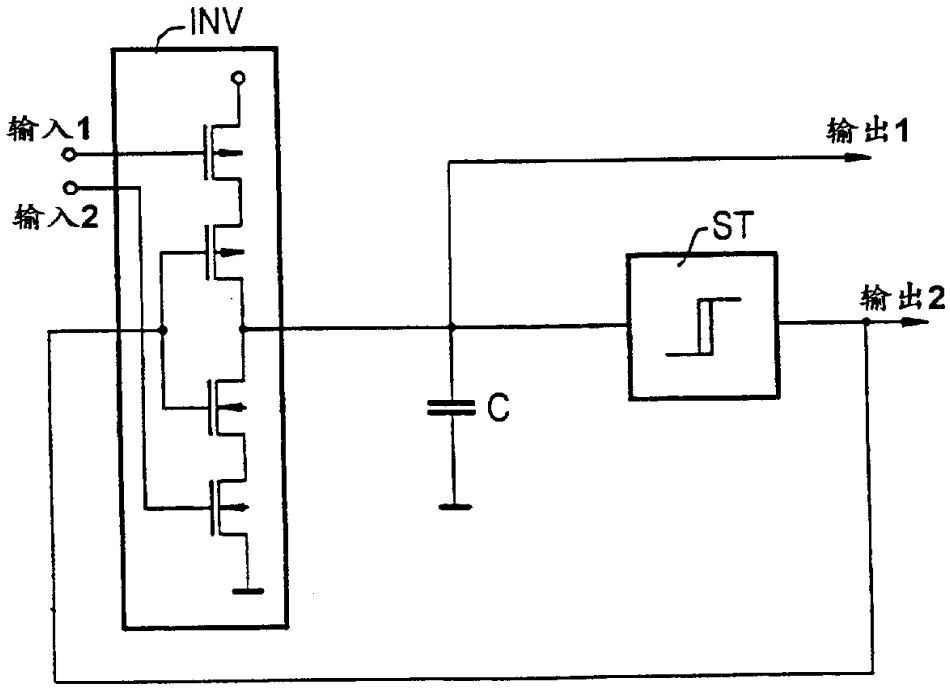

INV
输入1
输入2
输出1
ST
输出2
C

图 2