



(12)发明专利申请

(10)申请公布号 CN 106293617 A

(43)申请公布日 2017.01.04

(21)申请号 201610667018.6

(22)申请日 2016.08.12

(71)申请人 上海坚芯电子科技有限公司

地址 201203 上海市浦东新区郭守敬路498
号12幢21301室

(72)发明人 卢君明 洪享 厉祥春

(74)专利代理机构 上海晨皓知识产权代理事务
所(普通合伙) 31260

代理人 成丽杰

(51)Int.Cl.

G06F 7/58(2006.01)

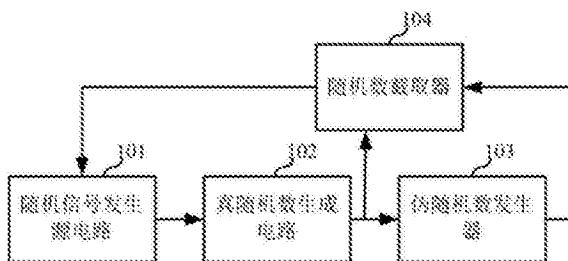
权利要求书2页 说明书7页 附图2页

(54)发明名称

真随机数发生器

(57)摘要

本发明涉及电路技术领域,公开了一种真随机数发生器。该真随机数发生器包括:随机信号发生源电路,用于生成随机数产生源信号;真随机数生成电路,用于对随机数产生源信号进行采样和扩散,得到真随机数序列;PRNG,用于根据输入的真随机数序列输出串行或并行的随机数序列;随机数截取器,用于根据输入的真随机数序列,从PRNG输出的随机数序列中截取预设长度的随机数序列,并反馈至随机信号发生源电路;随机信号发生源电路,还根据随机数截取器反馈的随机数序列调整随机数产生源信号。本发明实施方式的真随机数发生器采用普通逻辑器件即可实现,电路结构简单,且与工艺无关,通用性好,还增加了反馈机制,可消除无反馈时长时间工作出现的伪随机性。



1. 一种真随机数发生器，其特征在于，包括：随机信号发生源电路、真随机数生成电路、伪随机数发生器PRNG与随机数截取器；

所述随机信号发生源电路、所述真随机数生成电路、所述PRNG依次相连；所述随机数截取器的第一输入端与所述真随机数生成电路的输出端连接，第二输入端与所述PRNG的输出端连接，输出端与所述随机信号发生源电路的输入端连接；

所述随机信号发生源电路，用于生成随机数产生源信号；

所述真随机数生成电路，用于对所述随机数产生源信号进行采样和扩散，得到真随机数序列；

所述PRNG，用于根据所述真随机数序列输出串行或并行的随机数序列；

所述随机数截取器，用于从所述随机数序列中截取预设长度的随机数序列，并反馈至所述随机信号发生源电路；

所述随机信号发生源电路，还根据所述随机数截取器反馈的随机数序列调整所述随机数产生源信号。

2. 根据权利要求1所述的真随机数发生器，其特征在于，所述随机信号发生源电路具体包括：环形振荡器阵列以及第一异或门；

其中，所述环形振荡器阵列包括N个环形振荡器，N为自然数；所述N个环形振荡器均与所述第一异或门连接；第*i*个所述环形振荡器包括M_i个反相器，M_i为自然数，M_i的值各不相同，i为环形振荡器并联的次序；

所述N个环形振荡器，用于在接收到第一使能信号时开始工作，还用于将所述反馈的随机数序列作为频率选择开关信号FSEL，并根据所述FSEL选择振荡频率；其中，所述振荡频率由有效串联的反相器数目决定；

所述N个环形振荡器的输出信号经过所述第一异或门进行异或运算后，得到所述随机数产生源信号。

3. 根据权利要求2所述的真随机数发生器，其特征在于，每个所述环形振荡器还包括与门以及多路选择器；

在第*i*个所述环形振荡器中，所述与门、所述M_i个反相器、所述多路选择器依次首尾连接形成第一环路，M_i=4K_i+1，K_i为自然数，K_i的值各不相同；第2K_i+1个反相器的输出端还与所述多路选择器的输入端连接，所述与门、第1个反相器至第2K_i+1个反相器、所述多路选择器依次首尾连接形成第二环路；

所述N个环形振荡器根据所述FSEL选择所述第一环路工作或者选择所述第二环路工作；

在所述第一环路工作时，所述振荡频率为4K_i+3个门延迟产生的频率，在所述第二环路工作时，所述振荡频率为2K_i+3个门延迟产生的频率。

4. 根据权利要求3所述的真随机数发生器，其特征在于，所述N的取值范围为4~10。

5. 根据权利要求3所述的真随机数发生器，其特征在于，所述真随机数生成电路具体包括第二异或门与线性反馈移位寄存器LFSR；

所述第二异或门的第一输入端与所述第一异或门的输出端连接，所述第二异或门的第二输入端与所述LFSR的输出端连接；所述第二异或门的输出端与所述LFSR的输入端连接；所述LFSR的输出端与所述随机数截取器的输入端连接，还与所述PRNG的输入端连接；

所述第二异或门，用于对所述随机数产生源信号与采样得到的所述真随机数序列进行异或运算；

所述LFSR，用于对所述第二异或门的输出信号进行偏移纠正，对所述随机数产生源信号位流进行均衡分配，得到所述真随机数序列。

6. 根据权利要求5所述的真随机数发生器，其特征在于，所述LFSR的长度为48比特，所述LFSR的特征多项式为： $f(x) = x^{48} + x^7 + x^5 + x^4 + x^2 + x + 1$ ；其中，x指示寄存器，x的指数指示所述寄存器的序号。

7. 根据权利要求3所述的真随机数发生器，其特征在于，所述随机数截取器具体包括：信号翻转计数器与数据锁存模块；

所述信号翻转计数器的输入端为所述随机数截取器的输入端，与所述真随机数生成电路的输出端连接，所述信号翻转计数器的输出端与所述数据锁存模块的使能端连接，所述数据锁存模块的输入端与所述PRNG的输出端连接，所述数据锁存模块的输出端为所述随机数截取器的输出端；

所述信号翻转计数器，用于记录真随机数序列信号的翻转次数；

所述数据锁存模块，用于在所述翻转次数达到预设次数时，截取当前的随机数序列，并反馈至所述N个环形振荡器的频率选择开关，作为所述FSEL。

8. 根据权利要求7所述的真随机数发生器，其特征在于，所述翻转次数具体包括：所述真随机数序列信号从1到0的翻转次数以及从0到1的翻转次数。

9. 根据权利要求7所述的真随机数发生器，其特征在于，当所述翻转次数达到预设次数时，第二使能信号为1，对所述当前的随机数序列锁存一次；

在锁存所述当前的真随机数序列后，所述第二使能信号为0，保持所述锁存的数据，对所述信号翻转计数器进行清零，重新计数。

真随机数发生器

技术领域

[0001] 本发明涉及电路技术领域,特别涉及一种真随机数发生器。

背景技术

[0002] 随机数发生器是信息安全芯片或者信息系统中不可缺少的一部分,对于很多加密系统来说,其安全性完全取决于所使用的密钥和一些协议中的参数等。若采用传统模型产生的伪随机序列作为密钥,如果攻击者拥有足够的计算能力,则完全可以预测到伪随机数的产生规律,从而破解密钥。对于使用伪随机数的安全系统来说,采用软件方法产生的伪随机数,并不能保证足够的不确定性,这使得伪随机数成为加密系统性能提高的瓶颈。一个安全系统,即使其他部分足够安全,如果使用了伪随机数进行加密,也会使得整个安全系统变得很脆弱,容易受到攻击。因此,现代密码学中,以维斯特沙米尔阿德勒曼(RSA,Rivest Shamir Adleman)公钥密码算法和数字签名算法为代表的非对称密钥加密体制中,或者其他类型的安全协议中,需要安全可靠的、不可预测的随机数,以防系统被破解,这些系统都需要用到高质量的真随机数发生器。

[0003] 真随机数发生器往往以某一个随机物理过程作为参考随机源,通过特定的电路对随机源的信号进行采样并转化为数字信号。目前随机数发生器方案通常可以归纳为三大类,分别为直接放大法、离散事件混沌法以及振荡器采样法,前两种方法都需要采用模拟电路,十分依赖于工艺技术,主要用于客户订制的单元设计,但无法跨工艺重用,振荡器采样技术可以使用普通逻辑单元,因此在安全芯片设计中比较受欢迎。

[0004] 本申请的发明人发现,目前基于振荡器采样技术的随机数发生器,有的硬件开销小,但是使用了诸如PLL(Phase Locked Loop,锁相环)等特殊功能资源,使得重用性比较差,有的过于依赖于振荡器的抖动特性,使得分布不够均匀,或者需要非常多的硬件资源来消除对振荡器抖动特性的依赖,增加了系统硬件资源开销。

发明内容

[0005] 本发明实施方式的目的在于提供一种真随机数发生器,使得采用普通逻辑器件构成的简易电路结构,不仅产生好的随机数序列,而且与制作工艺无关,可作为单独的数据电路模块,实现在不同工艺的芯片设计中的重用,还增加了反馈机制,可以消除无反馈时长时间工作出现的伪随机性。

[0006] 为解决上述技术问题,本发明的实施方式提供了一种真随机数发生器,包括:

[0007] 随机信号发生源电路、真随机数生成电路、伪随机数发生器PRNG与随机数截取器;

[0008] 所述随机信号发生源电路、所述真随机数生成电路、所述PRNG依次相连;所述随机数截取器的第一输入端与所述真随机数生成电路的输出端连接,第二输入端与所述PRNG的输出端连接,输出端与所述随机信号发生源电路的输入端连接;

[0009] 所述随机信号发生源电路,用于生成随机数产生源信号;

[0010] 所述真随机数生成电路,用于对所述随机数产生源信号进行采样和扩散,得到真

随机数序列；

[0011] 所述PRNG，用于根据所述真随机数序列输出输出串行或并行的随机数序列；

[0012] 所述随机数截取器，用于从所述随机数序列中截取预设长度的随机数序列，并反馈至所述随机信号发生源电路；

[0013] 所述随机信号发生源电路，还根据所述随机数截取器反馈的随机数序列调整所述随机数产生源信号。

[0014] 本发明实施方式相对于现有技术而言，可以通过普通逻辑器件构成的简易电路结构，不仅可以产生好的随机数序列，而且与制作工艺无关，可以作为单独的数据电路模块，实现在不同工艺的芯片设计中的重用，还增加了反馈机制，可以消除无反馈时长时间工作出现的伪随机性。

[0015] 另外，所述随机信号发生源电路具体包括：环形振荡器阵列以及第一异或门；其中，所述环形振荡器阵列包括N个环形振荡器，N为自然数；所述N个环形振荡器均与所述第一异或门连接；第*i*个所述环形振荡器包括 M_i 个反相器， M_i 为自然数， M_i 的值各不相同，*i*为环形振荡器并联的次序；所述N个环形振荡器，用于在接收到第一使能信号时开始工作，还用于将所述反馈的随机数序列作为频率选择开关信号FSEL，并根据所述FSEL选择振荡频率；其中，所述振荡频率由有效串联的反相器数目决定；所述N个环形振荡器的输出信号经过所述第一异或门进行异或运算后，得到所述随机数产生源信号。

[0016] 随机信号发生源电路包括N个环形振荡器构成的环形振荡器阵列和第一异或门，N个环形振荡器的输出信号均与第一异或门连接，经过第一异或门的异或运算后，得到随机数产生源信号。其中，各环形振荡器分别由取值各不相同的 M_i 个反相器串联构成，有效串联的反相器数目决定了各环形振荡器的振荡频率，从而间接影响各环形振荡器的输出信号，并最终影响随机数产生源信号，因此，可以通过控制各环形振荡器有效串联的反相器数目，达到控制随机数产生源信号的目的。同时，N个环形振荡器，还用于将反馈的随机数序列作为频率选择开关信号FSEL，从而可以根据FSEL动态的选择振荡频率，并动态控制随机数产生源信号。

[0017] 另外，每个所述环形振荡器还包括与门以及多路选择器；在第*i*个所述环形振荡器中，所述与门、所述 M_i 个反相器、所述多路选择器依次首尾连接形成第一环路， $M_i=4K_i+1$ ， K_i 为自然数， K_i 的值各不相同；第 $2K_i+1$ 个反相器的输出端还与所述多路选择器的输入端连接，所述与门、第1个反相器至第 $2K_i+1$ 个反相器、所述多路选择器依次首尾连接形成第二环路；所述N个环形振荡器根据所述FSEL选择所述第一环路工作或者选择所述第二环路工作；在所述第一环路工作时，所述振荡频率为 $4K_i+3$ 个门延迟产生的频率，在所述第二环路工作时，所述振荡频率为 $2K_i+3$ 个门延迟产生的频率。

[0018] 每个环形振荡器还包括与门以及多路选择器，与门、 M_i 个反相器及多路选择器的第一输入端依次首尾连接，形成第一环路，与门、第1个反相器至第 $2K_i+1$ 个反相器以及多路选择器的第二输入端依次首尾连接，形成第二环路，其中， $M_i=4K_i+1$ ， K_i 为自然数， K_i 的值各不相同。当各环形振荡器根据FSEL选择第一环路工作时，各环形振荡器的振荡频率为 $4K_i+3$ 个门延迟产生的频率，当N个环形振荡器根据FSEL选择第二环路工作时，各环形振荡器的振荡频率为 $2K_i+3$ 个门延迟产生的频率。这样处理，可以对每个环形振荡器的反向器环长度进行动态的选择配置，实现振荡频率的动态更改，降低产生的随机数对振荡器电路抖动的依

赖性，提高随机数发生器的真随机性。

[0019] 另外，所述真随机数生成电路具体包括第二异或门与线性反馈移位寄存器LFSR；所述第二异或门的第一输入端与所述第一异或门的输出端连接，所述第二异或门的第二输入端与所述LFSR的输出端连接；所述第二异或门的输出端与所述LFSR的输入端连接；所述LFSR的输出端与所述随机数截取器的输入端连接，还与所述PRNG的输入端连接；所述第二异或门，用于对所述随机数产生源信号与采样得到的所述真随机数序列进行异或运算；所述LFSR，用于对所述第二异或门的输出信号进行偏移纠正，对所述随机数产生源信号位流进行均衡分配，得到所述真随机数序列。

[0020] 真随机数生成电路包括第二异或门与线性反馈移位寄存器LFSR，第二异或门对输入的随机数产生源信号及LFSR反馈的真随机数序列进行异或运算后，再将得到的运算结果输入至LFSR中，通过LFSR对随机数产生源信号进行偏移纠正及均衡分配，得到真随机数序列。这种电路结构，一方面，可以实现随机数产生源信号的采样和扩散，另一方面，可以纠正生成随机数产生源信号的过程中，振荡器电路产生的相位偏移，并对随机数位流进行均衡分配。经过上述处理后产生的真随机数序列具有良好的统计性能，极大增强了真随机数序列的随机性。

[0021] 另外，所述随机数截取器具体包括：信号翻转计数器与数据锁存模块；所述信号翻转计数器的输入端为所述随机数截取器的输入端，与所述真随机数生成电路的输出端连接，所述信号翻转计数器的输出端与所述数据锁存模块的使能端连接，所述数据锁存模块的输入端与所述PRNG的输出端连接，输出端为所述随机数截取器的输出端；所述信号翻转计数器，用于记录真随机数序列信号的翻转次数；所述数据锁存模块，用于在所述翻转次数达到预设次数时，截取当前的随机数序列，并反馈至所述N个环形振荡器的频率选择开关，作为所述FSEL。

[0022] 随机数截取器包括信号翻转计数器与数据锁存模块，信号翻转计数器记录输入的真随机数序列信号的翻转次数，并在翻转次数达到预设次数时，使能数据锁存模块截取当前输入的随机数序列，并反馈至N个环形振荡器的频率选择开关，作为FSEL。这样，实现了不定时的截取一段随机数，反馈到环形振荡器阵列中作为FSEL，使得真随机数发生器可以根据反馈的FSEL动态的控制振荡频率，进一步增加了随机信号发生源的随机性，并消除了原有无反馈的反向器环电路由于长时间工作而出现的伪随机性。

附图说明

[0023] 图1是根据本发明第一实施方式的一种真随机数发生器的电路结构示意图；

[0024] 图2是根据本发明第一实施方式的真随机数发生器的电路结构示意图；

[0025] 图3是根据本发明第一实施方式的环形振荡器的电路结构示意图；

[0026] 图4是根据本发明第一实施方式的随机数截取器的电路结构示意图。

具体实施方式

[0027] 为使本发明的目的、技术方案和优点更加清楚，下面将结合附图对本发明的各实施方式进行详细的阐述。然而，本领域的普通技术人员可以理解，在本发明各实施方式中，为了使读者更好地理解本申请而提出了许多技术细节。但是，即使没有这些技术细节和基

于以下各实施方式的种种变化和修改,也可以实现本申请所要求保护的技术方案。

[0028] 本发明的第一实施方式涉及一种真随机数发生器,包括:随机信号发生源电路、真随机数生成电路、伪随机数发生器与随机数截取器,其中,随机信号发生源电路、真随机数生成电路、伪随机数发生器依次相连;随机数截取器的第一输入端与真随机数生成电路的输出端连接,第二输入端与伪随机数发生器的输出端连接,输出端与随机信号发生源电路的输入端连接,具体电路结构如图1所示。

[0029] 随机信号发生源电路101,用于生成随机数产生源信号,同时还用于根据随机数截取器104反馈的随机数序列调整随机数产生源信号。

[0030] 真随机数生成电路102,用于对所述随机数产生源信号进行采样和扩散,得到真随机数序列。

[0031] 伪随机数发生器103,用于根据所述真随机数序列输出串行或并行的随机数序列。

[0032] 随机数截取器104,用于从所述随机数序列中截取预设长度的随机数序列,并反馈至所述随机信号发生源电路。

[0033] 不难发现,在本实施方式中,通过普通逻辑器件构成的简易电路结构,不仅可以产生好的随机数序列,而且与制作工艺技术无关,可以作为单独的数据电路模块,实现在不同工艺的芯片设计中的重用,还增加了反馈机制,可以消除无反馈时长时间工作出现的伪随机性。

[0034] 下面具体介绍随机信号发生源电路、真随机数生成电路及随机数截取器的具体构成。其中,随机信号发生源电路包括N个环形振荡器201至204构成的环形振荡器阵列和第一异或门205,真随机数生成电路包括第二异或门206与线性反馈移位寄存器(LFSR)207,具体电路结构如图2所示。

[0035] 随机信号发生源电路由一个环形振荡器阵列和第一异或门205构成,其中,环形振荡器阵列由环形振荡器21(图2的201)、环形振荡器22(图2的202)、环形振荡器23(图2的203)直至环形振荡器2N(图2的204)并联构成,N为自然数,即环形振荡器阵列包括N个并联的环形振荡器,N个环形振荡器均与第一异或门连接。N个环形振荡器,在接收到第一使能信号EN1时开始工作,N个环形振荡器的输出信号CLKOUT均进入第一异或门205,经过第一异或门205的异或运算后,得到随机数产生源信号。同时,N个环形振荡器还会将反馈的随机数序列作为频率选择开关信号(FSEL),并根据FSEL选择振荡频率,其中,振荡频率由有效串联的反相器数目决定。

[0036] 第*i*个环形振荡器又进一步包括与门、 M_i 个反相器以及多路选择器,具体电路结构如图3所示, M_i 为自然数, M_i 的值各不相同,*i*为环形振荡器并联的次序。与门301、 M_i 个反相器302至306及多路选择器307的第一输入端依次首尾连接形成第一环路,其中, $M_i = 4K_i + 1$, K_i 为自然数, K_i 的值各不相同,*i*为环形振荡器并联的次序。与门301、第1个反相器至第 $2K_i + 1$ 个反相器302至304及多路选择器307的第二输入端依次首尾连接形成第二环路,也即多路选择器307的两路输入分别为第 $4K_i + 1$ 个反向器的输出与第 $2K_i + 1$ 个反向器的输出。当第*i*个环形振荡器根据FSEL选择第一环路工作时,环形振荡器的振荡频率为 $4K_i + 3$ 个门延迟产生的频率,当选择第二环路工作时,环形振荡器的振荡频率为 $2K_i + 3$ 个门延迟产生的频率,实现了振荡频率的动态选择。

[0037] 在图3所示的环形振荡器电路结构中,当使能信号EN为“0”时,环形振荡器的输出

固定为“1”，环形振荡器停止工作。当使能信号EN为“1”时，根据频率选择信号FSEL的状态，分别组成不同的闭合环路，当FSEL为“1”时，器件301、302、303、304、305、306、307组成一个闭合环路(即第一环路)，环形振荡器以第一环路的振荡频率进行自振荡，输出一个高频的振荡时钟信号CLKOUT，也即环形振荡器输出振荡频率为 $4K_i+3$ 个门延迟产生的信号CLKOUT。当FSEL为“0”时，器件301、302、303、304、307组成一个闭合环路(即第二环路)，此时环形振荡器以第二环路的振荡频率进行自振荡，输出一个高频的振荡时钟信号CLKOUT，也即环形振荡器输出振荡频率为 $2K_i+3$ 个门延迟产生的信号CLKOUT。通过FSEL，可以选择环形振荡器输出振荡频率为 $4K_i+3$ 个门延迟产生的频率或者 $2K_i+3$ 个门延迟产生的频率，实现了振荡频率的动态更改。

[0038] N个环形振荡器组成的振荡器阵列中，每个的环形振荡器的参数 K_i 都不相同，实现了对环形振荡器中反向器环长度动态配置，降低了产生的随机数序列对振荡器电路抖动特征的依赖，改善了随机数发生器的真随机性，同时使得每个环形振荡器的两个振荡频率也都不相同，同时每个环形振荡器选用的振荡频率，在随机数序列产生过程中，可以动态切换，最大限度的获取到信号的随机性。

[0039] 真随机数生成电路包括第二异或门206与线性反馈移位寄存器(LFSR)207，其中，第二异或门206的第一输入端与第一异或门205的输出端连接，第二异或门206的第二输入端与LFSR207的输出端连接，第二异或门206的输出端与LFSR207的输入端连接，LFSR的输出端与随机数截取器209的输入端连接，同时还与伪随机数发生器208的输入端连接。第二异或门206，将输入的随机数产生源信号与真随机数序列进行异或运算后，将异或运算结果输出至LFSR207，LFSR207对输入的随机数产生源信号进行偏移纠正及随机数位流均衡分配，输出真随机数序列。

[0040] 目前，在振荡器采样技术的随机数发生器电路设计中，主要是利用振荡器电路在振荡频率上产生的抖动现象和相位漂移，环形振荡器对电源电压波动或输入信号中的直流分量特别敏感，极易受到电源电压波动或输入信号中直流分量的影响，任何的噪声波动，都会影响到振荡器的抖动现象，抖动现象是一个平均值为零的随机变量。除了时钟抖动外，两个独立时钟之间的相位漂移也具有随机特性，因而抖动信号和相位漂移适合在数字电路中作为真随机数发生器的噪声源。通过LFSR对输入的随机数产生源信号进行偏移纠正，可以对位流进行均衡分配，得到具有良好的统计性能的真随机数序列，增强真随机数序列的随机性。

[0041] 如图4所示，随机数截取器209包括信号翻转计数器401与数据锁存模块402，其中，信号翻转计数器的输入端为随机数截取器的输入端，与真随机数生成电路的输出端连接，信号翻转计数器的输出端与数据锁存模块的使能端连接，数据锁存模块的输入端与PRNG的输出端连接，输出端为随机数截取器的输出端。

[0042] 信号翻转计数器401，对输入的真随机数序列信号进行观测，一旦观测到真随机数序列信号有翻转就进行累加计数，以记录真随机数序列的翻转次数，其中，真随机数序列从“1”到“0”的翻转或者从“0”到“1”的翻转均计为一次翻转。当信号翻转计数器记录的翻转次数达到预设次数时，例如100次，使能数据锁存模块402的第二使能信号EN2为有效信号，即第二使能信号为1。数据锁存模块402，在第二使能信号为1时，对当前的随机数序列锁存一次，截取预设长度的当前随机数序列，并反馈至N个环形振荡器的频率选择开关，作为FSEL。

数据锁存模块402在锁存当前的随机数序列后,使能第二使能信号EN2为0,使数据锁存模块402保持锁存的数据,同时将信号翻转计数器401清零,重新开始进行计数,也即数据锁存模块402在第二使能信号为1时,对输入的随机数进行锁存,而在第二使能信号为0时,保持所有数据。

[0043] 随机数截取器209通过信号翻转计数器401和数据锁存模块402,实现了不定时的截取一段随机数,反馈到反环形振荡器阵列中作为FSEL,消除了原有无反馈反向器环电路由于长时间工作出现的伪随机性,同时,使得真随机数发生器可以根据反馈的FSEL动态的控制振荡频率,进一步增加了随机信号发生源的随机性。

[0044] 本实施方式中,N个环形振荡器组成的振荡器阵列中,每个环形振荡器的参数 K_i 都不相同,实现了对环形振荡器中反向器环长度的动态配置,降低了产生的随机数序列对振荡器电路抖动特征的依赖,改善了随机数发生器的真随机性,通过LFSR可以最大可能的消除随机数发生器电路设计中,环形振荡器之间的相位漂移,得到具有良好的统计性能的真随机数序列,增强真随机数序列的随机性,随机数截取器实现了不定时的截取一段随机数,并反馈到反环形振荡器阵列中作为FSEL,消除了原有无反馈反向器环电路由于长时间工作出现的伪随机性,同时,使得真随机数发生器可以根据反馈的FSEL动态的控制振荡频率,进一步增加了随机信号发生源的随机性。

[0045] 本发明的第二实施方式涉及一种真随机数发生器,第二实施方式在第一实施方式的基础上做了进一步改进,主要改进之处在于:在本发明第二实施方式中,通过LFSR对输入的随机数产生源信号进行偏移纠正,可以对位流进行均衡分配,得到具有良好的统计性能的真随机数序列,增强真随机数序列的随机性。

[0046] 线性移位寄存器LFSR为48比特LFSR,并且该LFSR的特征多项式为 $f(x) = x^{48} + x^7 + x^5 + x^4 + x^2 + x + 1$,其中,x指示寄存器,x的指数指示寄存器的序号。通过48比特LFSR对输入的随机数产生源信号进行偏移纠正,可以对输入的随机数产生源信号的位流进行均衡分配,得到具有更好的统计性能的真随机数序列,极大增强真随机数序列的随机性。

[0047] 本发明的第三实施方式涉及一种真随机数发生器,第三实施方式在第二实施方式的基础上做了进一步改进,主要改进之处在于:在本发明第三实施方式中,具体给出了随机信号发生源电路中,环形振荡器阵列的环形振荡器数目的最佳取值范围为:N的取值范围为4~10,这样,可以在资源和性能之间到达折中效果。

[0048] 环形振荡器阵列中环形振荡器的数量会影响随机信号发生源电路采集随机信号的效率,环形振荡器的数目越多,其输出的随机数产生源信号的随机性就会越好,但是环形振荡器的数目越多,所消耗的硬件资源也会越多,所以要在资源和性能之间做一个折中。本发明实施方式的随机信号发生源电路结构中,采用4到10个环形振荡器就足以达到美国国家标准与技术研究院(NIST,National Institute of Standards and Technology)的随机性测试要求。下面以8个环形振荡器组成的环形振荡器阵列为例,介绍各个环形振荡器的参数情况,见表1,其中,表1中的频率按一个门的延时为1ns计算。

[0049]

器件序号	M	K	FSEL=1 时频率(MHz)	FSEL=0 时频率(MHz)
11	5	1	1000/7	1000/5
12	9	2	1000/11	1000/7
13	13	3	1000/15	1000/9

[0050]

14	17	4	1000/19	1000/11
15	21	5	1000/23	1000/13
16	25	6	1000/27	1000/15
17	29	7	1000/31	1000/17
18	33	8	1000/35	1000/19

[0051] 表1

[0052] 本领域的普通技术人员可以理解，上述各实施方式是实现本发明的具体实施例，而在实际应用中，可以在形式上和细节上对其作各种改变，而不偏离本发明的精神和范围。

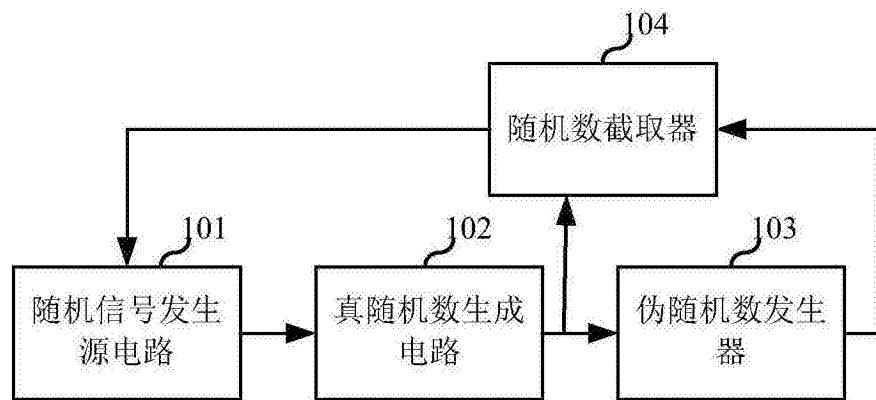


图1

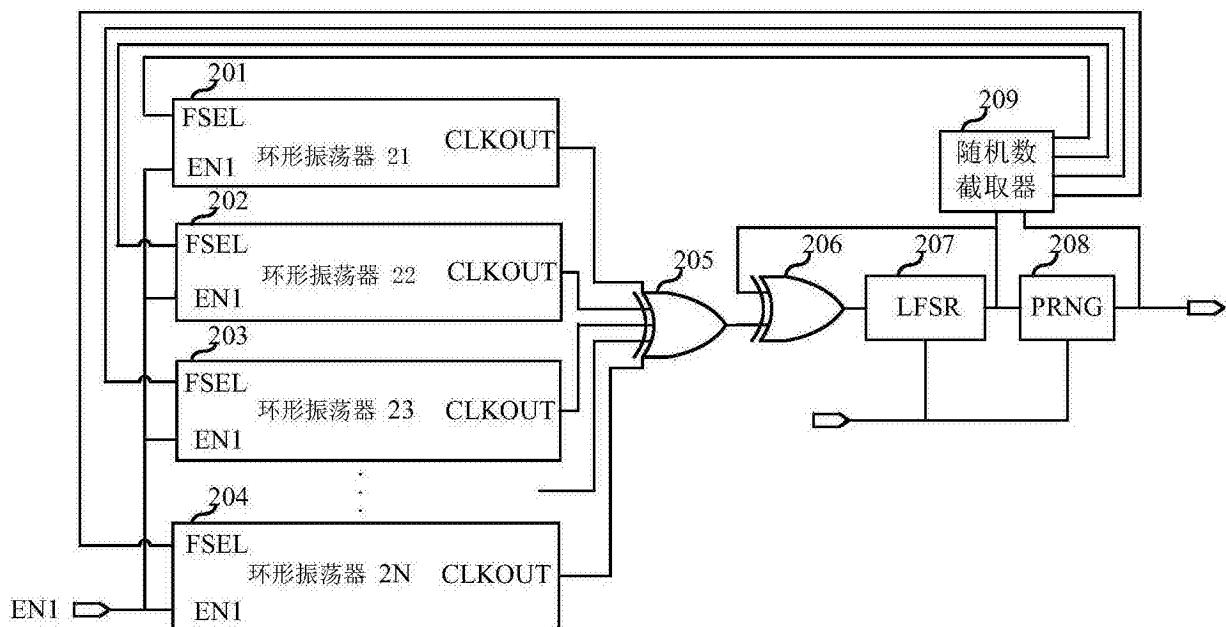


图2

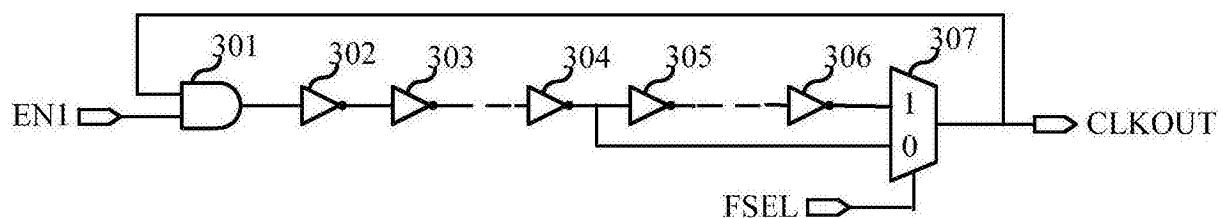


图3

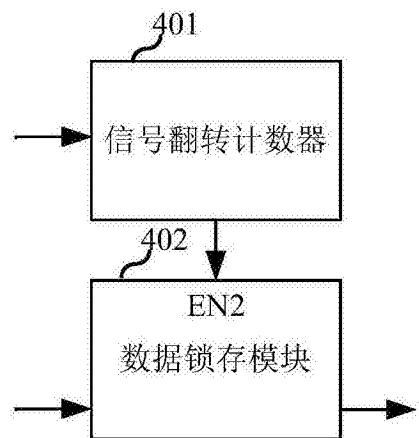


图4