一种基于锁相环的真随机数发生器

周干民 杨盛光* 蒋召宇* 高明伦
(合肥工业大学微电子设计研究所 合肥 230009)
*(南京大学物理系微电子设计研究所 南京 210093)

摘 要：对高质量随机数的要求与日俱增，导致了真随机数发生器受到广泛关注；系统芯片技术的出现和发展，提出了实现片上随机数发生器的需要；鉴于这两个现实状况，该文提出了一种基于锁相环噪声源的随机数发生器实现方法。实验结果表明该方法具有真随机性，易于实现和系统集成。

关键词：锁相环，随机数发生器，压控振荡器，随机性，杂化
中图分类号：TN402 **文献标识码**：A **文章编号**：1009-5896(2005)07-1152-05

A True Random Number Generator Based on PLL

Zhou Gan-min Yang Sheng-guang* Jiang Zhao-yu* Gao Ming-lun
(*Institute of VLSI Design, Hefei University of Technology, Hefei* 230009, *China*)
*(*Institute of VLSI Design, Department of Physics, Nanjing University, Nanjing* 210093, *China*)

Abstract The requirement of high quality random numbers grows day by day, so true random number generator takes great attentions; And the appearance and development of system on a chip needs the realization of on-chip random number generator. Considering the two facts, this paper comes up with a new method of random number generator based on the noise source of PLL.The method can provide a good property: true randomness and easy realization and system integration.

Key words Phase-locked loop, Random number generator, Voltage-controlled oscillator, Randomness, Hash

1 引言

随着加密应用的发展，对高质量随机数的要求也与日俱增。对于伪随机数而言，如果攻击者拥有足够的计算能力，则随机数序列是可预测的。因此使用伪随机数已经成为该类系统性能提高的瓶颈[1]。我们希望，即使攻击者有无限的计算能力，并且已知所有产生的序列，也不能预测系统下一个要产生的随机数，即真随机序列。因此需要用到真随机发生器。

另一方面，通过印刷电路板(Printed Circuit Board, PCB)实现功能芯片的互连以及系统集成的方法，因为其引入的连线延时、噪声等因素成了系统性能的瓶颈，面临着越来越多的困难。随着集成电路工艺和设计技术的发展，现在已经可以把整个系统都集成在一个芯片之上，即系统芯片(System on a Chip, SoC)。系统芯片技术要求充分地利用系统资源，提高综合效率。因此，实现片上随机数发生器也成为一种客观需要。

鉴于安全性和系统芯片技术发展的需要，以及锁相环(Phase-Locked Loop, PLL)已经成为一种通用的系统资源，本文提出了一种基于锁相环相位噪声的真随机数发生器（True Random Number Generator, TRNG）设计方法，并完成了硬件设计，它可以作为一个核应用于加密芯片、智能卡芯片或用该方法实现片上随机数发生器。

2 采用 PLL 方法的理论依据

实现真随机数发生器的方法大致有3类：直接放大，振荡器采样和基于混沌的离散时间序列[2]。常用的是前两种方法，由于直接放大方法，在集成电路环境里缺乏有效的方法屏蔽来自电压源和衬底信号的影响，而振荡器采样方法相对简单易行，因此备受关注。

振荡器采样法[2-6]利用自由振荡器的相位噪声产生随机序列(理想情况下噪声是MOSFET热噪声的附产物)。这种方法的一个例子如图1所示，用一个D触发器作为采样开关，高频振荡器的输出作为输入，低频时钟作为采样时钟，在低频时钟的上升沿采样。振荡器的相位抖动使得采样值具有不确

2004-02-22 收到，2004-11-05 改回
国家自然科学基金(60373076)资助课题

定性，理想的情况每一次采样都能产生一个随机位。而且，这种随机性还可以通过人为地选择高频时钟和低频时钟频率比例来调整。在有确定性影响存在的情况下，由于在采样过程中伴随着非线性的混沌现象，所以振荡器采样的方法被认为是更具优越性的，事实上也得到了证明[6]。然而，文献中针对采用环形振荡器的随机数发生器设计的统计报告显示[2]：该类振荡器产生的相位抖动还不足以产生具有很好统计属性的随机数。通常，伪随机处理的方法被用来对采样输出进行处理，以进一步改善其随机性，潜在地体现出一种系统不确定性与伪随机性的折衷。

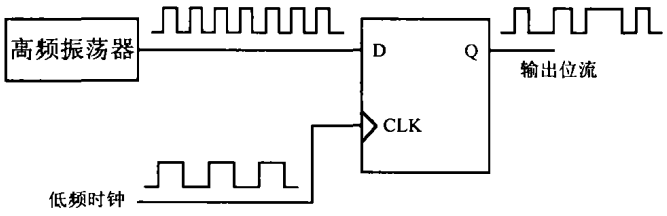

图 1　振荡器采样法的一个例子

由以上介绍可知振荡器采样方法的一些基本特征：利用自由振荡器的相位噪声产生随机序列(两时钟不相关)；自由振荡器的相位抖动使得采样值具有不确定性；随机性可以通过人为地选择噪声时钟和采样时钟频率比例来调整[2,6]。优点：方法简单、容易实现；受环境影响小 。缺点：可能存在随机性不足现象，通常需要伪随机处理方法处理。

于是就产生这样一种想法：利用振荡器采样的方法的方便和易实现性，同时采取必要的措施以改进其随机性不足的缺点。我们利用锁相环来实现随机数发生器，就具有这样的一种效果，而且也迎合了当代系统芯片技术发展的需要。

锁相环的方法，本质上属于振荡器采样法，其关键部件就是压控振荡器(Voltage-Controlled Oscillator, VCO)。噪声行为引起的电压变化加载到 VCO 的输入端会造成其输出端有显著的频率变化，很容易被观测到。国外有研究表明[6]：噪声经 VCO 采样得到随机数序列比噪声直接放大采样得到的随机数序列具有更好的统计属性。

但是，锁相环法与自由振荡器采样法存在着根本的区别：噪声时钟和采样时钟具有相关性。锁相环通常被用来锁定信号或者倍频，它在一定频率带宽范围内具有自我调节相差的能力。理论上讲，只要输入信号稳定，捕捉时间足够长，锁相环的输出和输入之间就能保持着一种平衡关系。锁相环的结构如图 2 所示。理想情况下存在以下平衡关系：

$$f(\text{clk\_fdbk}) = f(\text{clk\_ref}) \tag{1}$$

$$f(\text{clk\_out}) = Nf(\text{clk\_fdbk}) = Nf(\text{clk\_ref}) \tag{2}$$

$$\varphi(\text{clk\_fdbk}) = \varphi(\text{clk\_ref}) \tag{3}$$

但是实际的系统中总是存在着噪声，它使得信号之间的关系偏离以上的平衡关系，这种偏离体现出噪声的行为。只要能够采集到这种偏离，就可以产生真正的随机数。该采样方法是基于比较的原则提取相位噪声，采样对象为相对量（噪声信号相对于采样信号相位超前或滞后），即“噪声”，区别于自由振荡器采样的方法 [2-6]，其采样的对象为“噪声+信号”（其中信号为振荡器无噪输出信号），观察一种绝对量的变化。显然，观察相对量变化要比观察绝对量变化有效，它可以不考虑非噪声信号本身的周期性变化的影响。

针对锁相环具有的平衡关系，我们采用两种采样方案：clk_ref采样慢速时钟clk_fdbk；clk_ref采样快速时钟clk_out。第 2 种方法是，clk_out 经过 N 个时钟周期才被采样一次，噪声灵敏度相对要高一点，但采样时钟一定，对生成随机数速度影响不会太大。设计采用如图 3 所示的开关，可以比较两种方法的结果，择优而从之。

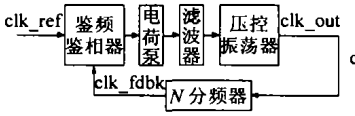

图 2　锁相环结构图

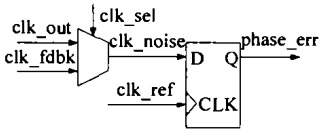

图 3　噪声时钟可选择的采样开关

3　数据处理方案

在理想情况下，对噪声发生器采样输出的随机位出现‘0’和‘1’的几率精确等于1/2。但实际上，由于电路内部其它非高斯型噪声的影响以及外部因素的影响，环境温度变化对系统稳定性的影响等，使得所产生的随机位不可能是严格等概率的，这就将影响形成的随机数序列的分布均匀性。因此必须采取措施对随机位的概率偏差加以修正[7]。得到比较随机的种子后，对种子进行伪随机处理，以改善其统计属性。我们对采样得到的数据设计了如图4所示的数据处理方案，分别满足了偏置纠正和改善统计属性的要求。

(1)冯-诺伊曼校正器[8]：偏置纠正

用D触发器采样到的信号存在着不可避免的缺陷：不能去除确定性噪声造成的固有偏置。采样后，噪声信息的熵值并没有增加，而固有偏置却转化成了随机数序列的相关性。这种相关性降低了信号的熵值。为了集中信号的熵值，通常采取降低随机数产生率的方法来提高信息熵。其中一种方法就是采用冯-诺伊曼校正器，它能去除固有偏置的影响。采样到的原始数据经过冯-诺伊曼校正器的处理后，它们组成的随机数序列中的“0”和“1”会形成一个比较平衡的分布。冯-诺伊

曼校正器将相邻两位数进行比较，视情况进行输出。其功能如图5中所示。

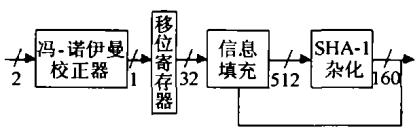

图4 数据处理方案

输入	输出
0,0	none
0,1	1
1,0	0
1,1	none

图5 冯-诺伊曼校正器功能

冯-诺伊曼校正器仅在输入数据流发生变化时才产生一个有效输出，由于发生[0,1]和[1,0]两种转变的机会是一致的，因此，就去除了数据流中的偏置。偏置没有转化成数据流中的相关性，但是却降低了产生数据流的速度。冯-诺伊曼校正器用一个很简单的方法实现了对一个带有偏离的随机序列的校正，产生了一个统计上平衡的输出。这个校正器对防止锁相环输出的固有周期造成的输出的固定偏离特别有效。我们使用这个校正器降低了生成序列中位与位之间的相关性，而这种相关性可能存在于锁相环压控振荡器和采样控制时钟源。

使用冯-诺伊曼校正器一个直接的后果就是使随机数发生器的随机数产生速率成为一个变量，大致每六位原始数据产生一位有效数据。随机数发生器的性能(校正器的输出超过75kbit/s)已经超出了所有标准加密应用对 TRNG 的要求，但是可变的位产生率使得某些应用变得更加复杂。虽然不能严格地证明这样的 TRNG 可以在一个有限的周期内产生一个具有固定位的输出，但是在实际应用中产生一个很大的延迟的可能性是很小的。

另外说明一下，冯-诺伊曼校正器可以将相关性转换成偏置。当采样输出为(010101……)，该信号并没有受到固有偏离的影响，但却是相关的，而校正器的输出可能出现全 0 或全 1，体现出明显的偏置。

校正器的输出送给一个32位的移位寄存器，移位寄存器内数据将作为后端随机数产生器可选的初始种子来源。移位寄存器和随机数产生器的接口能保证采集到的随机数系列被充分地利用，而且不影响随机数产生器的效率，从而保证了高随机性和高速度的要求。

(2)SHA-1 杂化函数：改善统计属性

我们的数据杂化过程使用了一个基于Secure Hash Algorithm (SHA-1)[9]的杂化函数。SHA-1的数据杂化结构在国外的文献中很受推崇，被认为具有很高的安全等级，因此得到了广泛的应用。SHA-1是一种有效的杂化器，可以组合可变长度的信息产生一个独立的输出，并且该输出具有很好的统计分布属性。SHA-1具有的加密属性改变了初始种子原有的统计结构，并且不可能由SHA-1输出计算出初始种子状态。正因为SHA-1具有这种特性，所以可以被用来杂化初始种子产生随机数。

SHA-1算法包括下面几个步骤：首先填充消息使其长度恰好为一个比512的倍数仅小64位的数。填充方法是附一个1在消息后面，后接所要求的多个0，然后在其后附上64位的消息长度(填充前)，使消息长度恰好是512位的整数倍。5个32位变量，用十六进制表示初始化。然后开始算法的主循环，一次处理512位消息，循环次数是消息中512位分组的数目。先把这五个变量复制到另外的变量中，A到a，B到b，C到c，D到d，E到e。主循环有4轮，每轮20次操作，每次操作对a，b，c，d，e中的3个进行一次非线性运算，后进行移位和加运算，运算的过程见图6。a，b，c，d和e分别加上A，B，C，D和E，然后用下一数据分组继续运行算法。最后的输出由A，B，C，D和E级联而成。

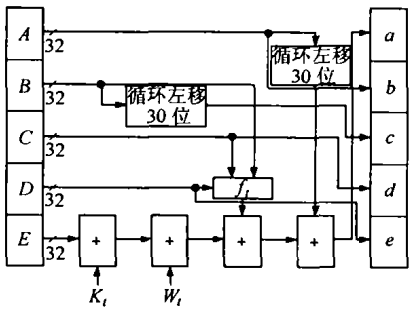

图6 SHA-1算法示意图

为了有效地利用采集到的随机信息和保证随机数的产量，我们设计了一个SHA-1杂化方案，如图7所示。

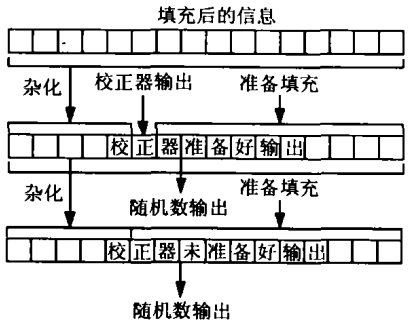

图7 SHA-1 数据杂化方案

该数据杂化方案采用 512 位的初始状态，从冯-诺伊曼校正器接受 32 位的输入，产生 32 位的随机数输出。图 7 中每一格代表 32 位数据。考虑到现实存在的两个情况：冯-诺伊曼校正器产生一个 32 位数输出所需要的时间是一个变量(由采样信号的质量决定)，而且通常大于 64 个时钟周期，必然

影响随机数发生器的产量；因此我们设计了两种工作模式：

(1)校正器准备好输出(New State with Input from Corrector)：信息填充模块将校正器的输出（32位）和数据融合输出（160位）组合进新的初始状态，供下一次杂化使用。

(2)校正器未准备好输出（New State without Input from Corrector)：信息填充模块只将数据融合输出(160 位)组合进新的初始状态，供下一次杂化使用（即自循环产生随机数)。

SHA-1 杂化算法的初始状态包含取自于真实的物理现象的种子，而且每隔一定时间（一个种子的采集时间）补充一次种子。如果采样原始数据随机性好，则发生器一直运行在第一状态，输出具有真随机性：即使进入第二状态，由于 SHA-1 杂化运算不会降低信息的熵值，安全性取决于它的初始状态。由于初始状态取自于自然现象，因此 SHA-1 杂化器的输出还具有真随机数的属性。这样，既保证了真随机性，又获得了稳定的随机数产量。

4　实验结果

根据设计的意图，用 Spectre 模拟器对电路进行数模混合仿真，在不同采样频率、不同噪声时钟条件下采集到 6 组 320 位的数据，用于质量测试。测量数据为采集到的种子值，因为 SHA-1 算法会改变原先数据的统计结构，而目的是想验证用 PLL 作为噪声源的方法产生随机数是否可行。PLL 倍频系数固定为 8，该 6 组数据的采样条件为：

(1)条件1：10MHz clk_ref，采样clk_fdbk

(2)条件2：10MHz clk_ref，采样clk_out

(3)条件3：20MHz clk_ref，采样clk_fdbk

(4)条件4：20MHz clk_ref，采样clk_out

(5)条件5：40MHz clk_ref，采样clk_fdbk

(6)条件6：40MHz clk_ref，采样clk_out

测试方案包括4种测试：比特分布检测：频度检测；运行检验；序列检测。测试结果如表1 – 表4所示。

表1　比特分布检测结果

	*S*1	*S*2	*S*3	*S*4	*S*5	*S*6
*N*0	158	161	169	162	171	167
*N*1	162	159	151	158	149	153

理想值为：*N*0(*T*)=*N*1(*T*)=160；条件 5 偏差稍大些，但在可接受范围，可以认为通过测试。

表2　频度检测结果

	*S*1	*S*2	*S*3	*S*4	*S*5	*S*6
χ_0	0.05	0.125	1.0125	0.05	1.5125	0.6125

允许范围：$\chi_0(T)< 3.841$；通过此项测试。

表3　运行检验结果

	*S*1	*S*2	*S*3	*S*4	*S*5	*S*6
C[0]1/ *C*[1]1/ *C*1	40 /42 /82	50 /52 /102	42 /51 /93	37 /35 /72	47 /54 /101	45 /39 /84
C[0]2/ *C*[1]2/ *C*2	17 /13 /30	25 /22 /47	19 /19 /38	21 /21 /42	18/ 19 /37	17 /24 /41
C[0]3/ *C*[1]3/ *C*3	16 /13 /29	8 /11 /19	19 /11 /30	6 /13 /19	8 / 9 /17	6 /15 /21
C[0]4/ *C*[1]4/ *C*4	3 /9 /12	3 /5 /8	4 /2 /6	6 /3 /9	10/0/ 10	8 /1/9
C[0]5/ *C*[1]5/ *C*5	1 /2 /3	5 /1 /6	3 /3 /6	4 /2 /6	2 /2 /4	3 /2 /5
C[0]6/ *C*[1]6/ *C*6	2 /0 /2	0 /1 /1	0 /1 /1	2 /2 /4	0 /2 /2	0 /2 /2
C[0]7/ *C*[1]7/ *C*7	0 /0 /0	0 /0 /0	0 /0 /0	0 /0 /0	1 /0 /1	2 /0 /2

理想参考值为：*C*1(*T*)= 80.5；*C*1(*T*)= 40.13；*C*1(*T*)= 20；*C*1(*T*)= 9.97；*C*1(*T*)= 4.97；*C*1(*T*)= 2.48；*C*1(*T*)= 1.23；

条件 1，3 偏差稍大些，但在可接受范围，可以认为通过测试。

表4　序列检测结果

	*S*1	*S*2	*S*3	*S*4	*S*5	*S*6
0->1	79	90	87	77	86	81
1->0	79	91	87	77	86	81
0->0	79	70	81	84	85	86
1->1	83	69	65	82	63	72

理想情况下：转换 0->1 和 1->0 次数一致，0->0 和 1->1 次数一致；条件 3，5，6 偏差稍大些，但在可接受范围，可以认为通过测试。

根据以上测试结果作出以下推测：用锁相环作为噪声源产生随机数的方法基本可行，没有出现随机性不足现象；随机性与采样时钟频率有关；利用PLL两个平衡产生结果有差异，快速时钟作为噪声源随机性好些；随机数产生速率跟采样时钟频率成正比，同一采样时钟情况下，快时钟做噪声源

速率略快些；速度不是一个确定量，实验中条件2，4，8速率分别约为2.5Mbit/s，6Mbit/s，14Mbit/s，但已经超出了所有标准加密应用对TRNG的要求(75kbit/s)[8]，采样频率可以取值更低。

5 结束语

本文提出了一种新的片上真随机数发生器实现方法，并初步完成了方法可行性验证，可供系统芯片、嵌入式系统或其他需要高质量随机数器产品的设计者参考。后续工作包括：按照 FIPS140-1 标准[10]对其进行全面测试；进行更多条件下的测试，确定频率与随机性的具体关系；如果可能，进行流片测试，以便为应用提供指导性的建议。

参 考 文 献

[1] Huang Zhun, Cheng Hongyi. A truly random number generator based on thermal noise. Proceeding of the 4th International Conference on ASIC, Shanghai, 2001: 862 – 864.

[2] Petrie C S, Connelly J A. A noise-based IC random number generator for application in cryptography. *IEEE Trans. on Circuits and Systems I: Fundamental Theory and Applications*, 2000, 47(5): 615 – 621.

[3] Anderson R. Industrial cryptography. *IEE Review*, 1996, 42(3): 118 – 120.

[4] Schneier B. Applied Cryptography. New York: John Wiley & Sons, 1994: 1.

[5] Tsoi K H, Leung K H, Leong P H W. Compact FPGA-based true and pseudo random number generators. 11th IEEE Symposium on Field-Programmable Custom Computing Machines (FCCM 2003), Napa, CA, 2003: 51 – 61.

[6] Petrie C S, Connelly J A. Modeling and simulation of oscillator-based random number generators. IEEE International Symposium on Circuits and Systems, Atlanta, May 1996, vol. 4: 324 – 327.

[7] 王莱，刘松强. 真随机数发生器的设计与实现. 核电子学与探测技术, 1998, 18(6): 452 – 455.

[8] Benjamin Jun, Paul Kocher. The Intel® Random Number Generator. White Paper Prepared for Intel Corporation, April 22, 1999: 4 – 5.

[9] Secure Hash Standard. Federal Information Processing Standards Publication 180-2, August 1, 2002.

[10] The Intel® Random Number Generator, Copyright © Intel Corporation 1999.

周干民： 男，1976年生，博士生，研究方向为多媒体SoC芯片、片上网络芯片设计技术.

杨盛光： 男，1979年生，硕士，研究方向为大规模数模混合集成电路.

蒋召宇： 男，1979年生，博士生，研究方向为模拟集成电路和锁相环设计.

高明伦： 男，1945年生，教授，博士生导师，研究方向为超大规模集成电路设计.