第35卷 第10期 计 算 机 工 程 2009年5月
Vol.35 No.10 Computer Engineering May 2009
·工程应用技术与实现· 文章编号：1000—3428(2009)10—0229—03 文献标识码：A 中图分类号：TP303

应用于网络安全协处理器的真随机数产生器

张晓峰，白国强，陈弘毅
(清华大学微电子学研究所，北京 100084)

摘 要：介绍一款基于环形振荡器的真随机数产生器。电路使用固定频率时钟采样可控频率振荡器的输出，使用级间反馈随机改变可控频率振荡器的振荡频率。设计启动电路来保证环形振荡器快速起振，在使能信号无效时断开振荡电路以节省功耗。电路采用CMOS 0.18 μm标准工艺实现，使用Hspice_RF仿真环形振荡电路的相位抖动以获得最优设计参数。仿真结果表明，电路在输出速率为1 Gb/s时产生的随机序列具有良好的随机性，该设计可用于网络安全协处理器中。

关键词：网络安全协处理器；真随机数产生器；环形振荡器；启动电路

True Random Number Generator for Network Security Co-processor

ZHANG Xiao-feng, BAI Guo-qiang, CHEN Hong-yi
(Institute of Microelectronics, Tsinghua University, Beijing 100084)

【Abstract】This paper introduces a ring oscillator based True Random Number Generator(TRNG) for network security co-processor. To obtain better randomicity, the circuit utilizes a fixed frequency clock to sample the output of a frequency variable high speed ring oscillator. Inter-stage feedback ring is introduced to control the frequency of the high speed ring oscillator to accumulate the phase noise. Start-up circuit is designed not only to make the ring oscillator much easier to oscillate, but also to reduce the power dissipation by introducing enable signal. TRNG is designed under CMOS 0.18 μm standard process. Hspice_RF is used to perform jitter simulation to acquire optimum parameters. Simulation results show that random bit stream can pass statistical test for randomness under 1 Gb/s sampling frequency.

【Key words】network security co-processor; True Random Number Generator(TRNG); ring oscillator; start-up circuit

随着密码算法复杂性的增加及参数长度的加长，采用软件方式已经不能满足网络中数据处理量的需求，采用硬件实现成为一种新趋势。设计专用的网络安全处理芯片，可以保证网络安全运行且不降低处理速度。本文介绍一款网络安全协处理器，给出了随机数产生器的电路原理设计和随机性测试结果。

1 网络安全协处理器

高速网络安全协处理器[1]是一款可以高速处理多种密码算法的安全芯片，一般被用于路由器中来协助网络处理器进行数据加密和认证。它针对网络传输中数据处理量大的特点，根据SSL协议的运算要求优化配置了包括DES, 3DES, AES, ECC, RSA等多种分组密码和公钥密码算法引擎，进行各种加/解密运算，从而实现网络中数据加/解密、数字签名、认证等功能。

协处理器中的真随机数产生器(True Random Number Generator, TRNG)的主要用途是为ECC的k因子、RSA、数字签名和验证提供随机数。加密引擎所使用随机数的随机性直接影响系统的安全性能，因此，TRNG产生的随机比特流必须通过严格的随机性测试才能被使用。由于TRNG须同时为系统中多个模块提供随机数，因此它必须具备较高的随即比特流产生速率。本文设计的TRNG采用如图1所示的方式为系统提供随机序列：随机数产生器输出的串行随机比特流经过移位寄存器转换为64 bit并行数据，缓存在模块的输出FIFO中。若输出FIFO被写满，则模块停止工作。当输出FIFO中的数据被系统中其他模块读出，即输出FIFO进入“非满”状态时，随机数发生器重新启动，将输出FIFO再次填满。采用这种方式，TRNG既可以高效地为系统中各模块提供随机数，又可以在不需要的时候停止工作，降低了系统功耗。

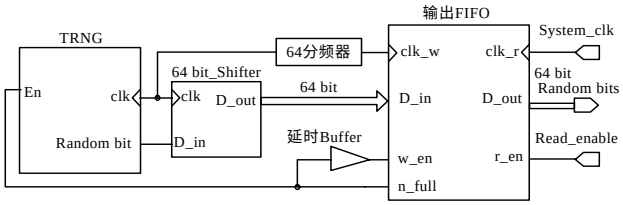

图1 TRNG与协处理器的接口

2 真随机数产生器的电路原理与设计

TRNG的基本电路组成部分包括：可控频率环形振荡电路，低频振荡采样电路，移位异或后处理电路和控制电压产生电路。

2.1 环形振荡器

环形振荡器采用由奇数级的CMOS反相器组成的单端互补CMOS环形振荡器。为了使整体电路有效进入不可预测状态以便能更快、更好地获得随机性，电路中采用改变等效电阻阻值的方法来改变环形振荡器的振荡频率，如图2所示。

基金项目：国家自然科学基金资助项目(60576027, 60544008)；国家“863”计划基金资助项目(2006AA01Z415)
作者简介：张晓峰(1982－)，男，硕士研究生，主研方向：真随机数产生器；白国强，副教授；陈弘毅，教授
收稿日期：2008-10-12 **E-mail：**jlglpk@yahoo.cn

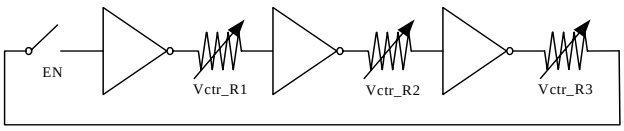

图 2　可控频率环形振荡电路

可变电阻阻值和振荡器的振荡频率之间的关系[2]为

$$f_{OSC}=\frac{G_M}{2NC_G(1+G_MR_V)} \tag{1}$$

其中，G_M 为等效跨导；R_V 为等效电阻；C_G 为寄生电容；N 为反相器级数。

可控频率环形振荡电路原理如图 3 所示。

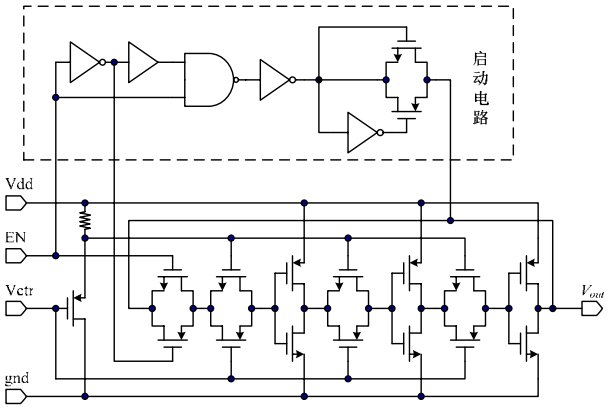

图 3　可控频率环形振荡电路原理

其中，可变电阻由 CMOS 开关来实现，CMOS 开关的 2 个管子均工作在线性区，其等效导通电阻为

$$R_{CMOS\_on,eq}=R_{nmos\_on,eq}\parallel R_{pmos\_on,eq}=\frac{1}{k_n'(\frac{W}{L})_n(ck-V_{in}-V_{Tn})}\parallel\frac{1}{k_p'(\frac{W}{L})_p(V_{in}-\overline{ck}-|V_{Tp}|)} \tag{2}$$

其中，ck 和 $\overline{ck}$ 分别是 CMOS 开关中 NMOS 和 PMOS 管的栅电压；V_{in} 是开关的漏极输入电压。

结合式(1)、式(2)可得出利用控制电压来控制振荡器振荡频率的原理：CMOS 开关的栅电压发生改变→等效导通电阻 R_V 改变→振荡器振荡频率改变。图 3 中控制电压 Vctr 直接控制 PMOS 管栅极，同时经过源极跟随器转换电平后控制 NMOS 管栅极，因此，只要控制电压在一定的范围内变化，开关的栅极电压也将在一定的范围内变化，从而达到通过电压来控制振荡器的振荡频率变化的目的。设计主要考虑以下几点：

(1)振荡器有较高的振荡频率和较大的频率变化范围。

(2)通过仿真设计振荡电路晶体管尺寸，尽量大地获得相位噪声。

(3)保证振荡电路具有较小的传播延时，确保电路有足够驱动能力，能正常起振。

固定频率采样电路的结构与频率可控环形振荡电路相似，区别在于把图 2 中的可变电阻换成了固定电阻。由式(1)可知，通过调整电阻 R_V 的阻值和反相器的级数 N，可以调整固定频率采样电路的振荡频率，进而调整电路的随机比特流输出速率。

如图 4 所示，为了引入更多的相位噪声，在设计中把 2 个不同频率范围的可控频率环形振荡器产生的波形进行异或操作，能有效地把 2 个振荡器产生的相位抖动叠加。用固定频率采样电路进行采样得到未处理的随机比特流，然后输入到后处理电路进行后处理。

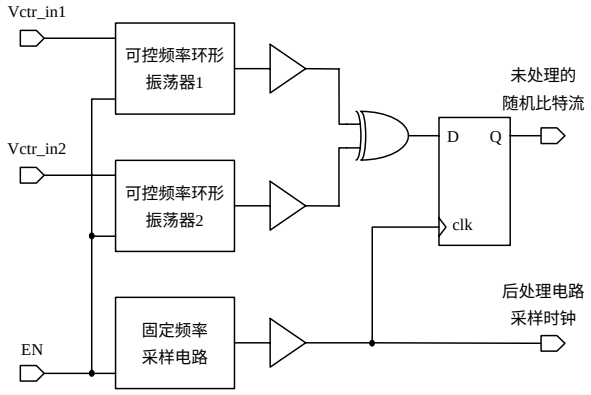

图 4　振荡采样电路

2.2　启动电路

从原理上看，CMOS 反相器是一个电平反向放大电路，如果环形振荡器的初始状态处于中间电平，将导致振荡电路起振速度缓慢，使得 TRNG 在上电后的很长一段时间内不能正常工作，不能得到随机比特流，在最坏情况下电路甚至有可能无法起振。实践表明某些振荡器芯片的确存在起振问题。因此，本文为环形振荡器设计了启动电路来确保振荡器能更快地进入正常工作状态。

启动电路结构如图 3 中虚线框所示，它由组合逻辑组成，其输入端是电路的使能信号 EN。当 EN 为高电平时整体电路正常工作，输出随机比特流；当 EN 为低电平时，振荡环路断开，电路停止工作，节省功耗。启动电路的作用是在 EN 的上升沿产生一个短脉冲信号，该信号输入到振荡器的环路节点中，给振荡器一个明确的高电平起振激励，在脉冲过后，启动电路自动关闭，输出节点悬空，不会对振荡电路内部产生影响。

2.3　后处理电路和控制电压的生成

为使输出序列的“0”和“1”分布更加均匀，设计中引入了如图 5 左边所示的 3 级移位异或后处理电路。其原理[3]表述如下：假设输入比特流中 1 的概率为 p，0 的概率为 1–p。由数学归纳法，序列经过 n 级移位异或后出现 1 的概率为 $P(1)=0.5-2^{n-1}(p-0.5)^n$；出现 0 的概率为 $P(0)=0.5+2^{n-1}(p-0.5)^n$。因此，随着级数 n 的增加，序列趋向于均匀分布，随机性得到提高。级数 n 的确定由电路随机性和电路的功耗、面积来折中考虑。仿真表明，设计中采用 3 级移位异或电路能得到随机性较好的序列。

控制电压由经过后处理的随机序列通过电阻分压产生，如图 5 右边虚线框所示。

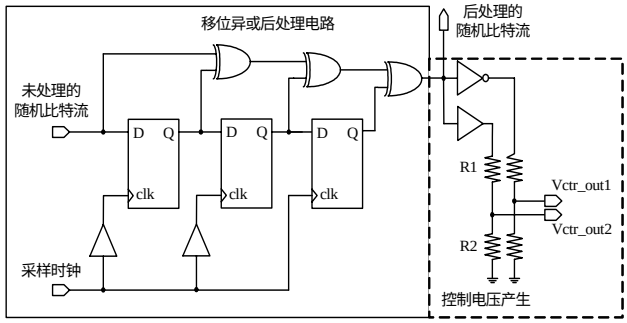

图 5　移位异或后处理电路

利用这组随机电压作为可控频率环形振荡电路的控制电压，可以把随机性通过反馈的形式引回振荡器中，使得可控频率环形振荡电路的振荡频率随机变化。

2.4 3 级反馈环路

图 4 和图 5 拼接后的电路称为单级电路。如果只用单级电路来完成自反馈频率控制，会产生很大的相关性，破坏了生成序列的随机性。基于以上考虑，整体电路的设计采用 3 级结构，形成多级反馈控制环路，利用级间反馈环路来控制可控频率振荡器的振荡频率，从而使电路中的相位噪声被不断地积累放大，噪声产生的抖动和电路的初始状态混合在一起，经过迭代以后电路进入无法预测的状态。TRNG 整体电路结构如图 6 所示。

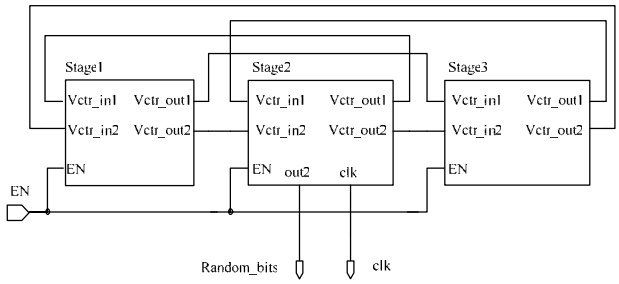

图 6　振荡频率可控的 3 级反馈环路结构

由于同一级电路输出的 2 个控制电压具有相关性，因此本文并不是把本级电路的 2 个控制电压输出端直接连接到同一级电路相应的 2 个控制电压输入端，而是采取了图 5 的连接方式，从而避免相关性的引入。

3 仿真测试结果

3.1 电路仿真结果

电路采用 CMOS 0.18 μm 标准工艺实现，电源电压为 1.8 V。整体电路的平均功耗为 9.57 mW，版图面积约为 300 μm×100 μm。图 5 中分压电阻的阻值设计为 R1:R2=2:5。控制电压的变化范围为 0~1.285 V。固定频率采样电路的振荡频率约为 1 Gb/s。环形振荡器使用 Hspice_RF 进行相位噪声仿真，得到相位抖动和时间的关系，通过仿真来获得最优的设计参数。仿真结果如表 1 所示。

表 1　环形振荡器仿真结果

可控频率环振	控制电压为 0 时的振荡频率/GHz	控制电压为 1.285 V 时的振荡频率/GHz	振荡频率变化最大值/MHz	控制电压为 0，t=500 ns 时的相位抖动/ps	控制电压为 1.285 V，t=500 ns 时的相位抖动/ps
1	1.98	1.53	450	17	66
2	1.76	1.11	650	21	97

3.2 随机性测试结果

在 1 Gb/s 的采样速率时得到 1 个 25 000 bit 的随机序列，其随机性检测结果如表 2 所示，其中，第 3 列为得到的随机序列在对应的检测项目和条件下测量得到的统计平均值，该统计平均值大于显著性水平[4]0.01 即表示序列通过该项检测。从表 2 中可以看出，序列通过了所有检测，表明本文设计的电路能产生具有良好随机性的随机序列。

表 2　随机性检测结果

检测项目	条件	统计平均值
单比特频数检测	—	0.847 8
块内频数检测	m=20	0.203 6
块内频数检测	m=30	0.203 6
块内频数检测	m=50	0.371 0
扑克检测	m=2	0.201 1
扑克检测	m=3	0.989 3
扑克检测	m=4	0.935 8
扑克检测	m=5	0.726 8
扑克检测	m=6	0.635 1
扑克检测	m=7	0.624 4
重叠子序列检测	m=5	0.606 8
重叠子序列检测	m=8	0.577 4
游程总数检测	—	0.786 5
游程分布检测	—	0.335 7
块内最大游程检测	—	0.260 8
二元推导检测	k=1	0.631 8
二元推导检测	k=2	0.293 0
自相关检测	d=1	0.126 3
自相关检测	d=10	0.219 7
自相关检测	d=50	0.646 0
累加和检测	$mode$=0(前向)	0.395 2
累加和检测	$mode$=1(后向)	0.442 1
离散傅立叶检测	—	0.642 0

4 结束语

本文提出一款适用于网络安全协处理器的真随机性产生器电路，它采用振荡采样法实现，具有设计复杂度低、速度快、功耗和面积小、易于集成等特点。输出随机数速率达到 1 Gb/s，测试结果表明生成的序列通过随机性检测，具有良好的随机性。因此，本文提出的真随机数发生器不仅满足笔者所在课题组中的网络安全协处理器的性能要求，同时也适用于各种安全加密场所。

参考文献

[1] Wang Haixin, Yue Yao, Zhang Chunming, et al. A Novel Unified Control Architecture for a High-performance Network Security Accelerator[C]//Proceedings of the International Conference on Security and Management. Las Vegas, USA: [s. n.], 2007.

[2] Retdian N, Takagi S, Fujii N. Voltage Controlled Ring Oscillator with Wide Tuning Range and Fast Voltage Swing[C]//Proc. of IEEE Asia-Pacific Conference. Taipei, China: [s. n.], 2002.

[3] 吴燕雯, 戎蒙恬, 诸　悦, 等. 一种真随机数发生器的 ASIC 设计与实现[J]. 微电子学, 2005, 35(2): 213-216.

[4] Rukhin A, Soto J, Nechvatal J, et al. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications[Z]. (2001-05-15). http://csrc.nist.gov/groups/ST/toolkit/rng/documentation_software.html.

编辑　顾姣健