基于压控振荡器的真随机数发生器设计

汪鹏君[1,2],李 桢[1],李 刚[2],程 旭[3],张会红[1]
(1. 宁波大学信息科学与工程学院,浙江宁波 315211; 2. 温州大学数理与电子信息工程学院,
浙江温州 325035; 3. 复旦大学专用集成电路与系统国家重点实验室,上海 201203)

摘 要: 通过对频率抖动机理的研究,提出一种基于压控振荡器(Voltage-Controlled Oscillator,VCO)的真随机数发生器(True Random Number Generator,TRNG)设计方案. 该方案将电阻热噪声放大后作为VCO的控制信号使其振荡频率在中心频率附近随机抖动. VCO所产生的慢振荡信号对周期固定的快振荡信号采样生成原始随机序列,然后利用后处理电路提高序列均匀性并消除自相关性. 通过热噪声发生器调节VCO的中心频率可实现序列比特率和随机性之间的权衡. 所提电路采用SMIC 55nm CMOS工艺设计,芯片面积0.0124mm^2,比特率10Mbps,平均功率0.81mW. 输出的随机序列通过NIST SP 800-22测试.

关键词: 真随机数发生器; 热噪声; 压控振荡器; 权衡
中图分类号: TN4 **文献标识码:** A **文章编号:** 0372-2112(2019)02-0417-05
电子学报URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2019.02.022

Design of True Random Number Generator Based on VCO

WANG Peng-jun[1,2], LI Zhen[1], LI Gang[2], CHENG Xu[3], ZHANG Hui-hong[1]
(1. *Faculty of Electronic Engineering and Computer Science, Ningbo University, Ningbo, Zhejiang* 315211, *China*;
2. *College of Mathematics, Physics and Electronic Information Engineering, Wenzhou University, Wenzhou, Zhejiang* 325035, *China*;
3. *State Key Laboratory of ASIC and System, Fudan University, Shanghai* 201203, *China*)

Abstract: After studies on the frequency jitter mechanism, a design of true random number generator (TRNG) based on voltage-controlled oscillator (VCO) is proposed. The scheme amplified the thermal noise of resistance and took it as the control signal of VCO. Its oscillation frequency thus randomly jittered around the centre frequency. The slow oscillating signal generated by the VCO generated an raw random sequence by sampling the period-fixed fast oscillating signal, then used the post-processing circuit to improve the uniformity of sequence and to eliminate the autocorrelation. Applying the thermal noise generator to adjust the centre frequency of VCO is able to trade off the bit rate of sequence and the randomness. The proposed circuit is designed in SMIC 55nm CMOS technology with a chip area of 0.0124mm^2, a bit rate of 10Mbps and an average power of 0.81mW. The output of randomly sequence passed the NIST SP 800-22 randomness test.

Key words: true random number generator (TRNG); thermal noise; voltage-controlled oscillator (VCO); trade off

1 引言

随机数发生器是现代电子系统中至关重要的一个组成部分. 相较伪随机数发生器,真随机数发生器TRNG具有独立性和不可预测性. 在诸如密钥生成等场合中随机序列不仅需有优良的统计特性,还要保证足够的安全性. 因此在密码学领域主要采用TRNG以满足对信息安全日益增长的需求[1]. 在典型的TRNG结构中,先从目标熵源提取随机信号,然后对随机信号采样生成数字序列,最后用后处理模块提高序列品质. 熵源主要包括热噪声、核衰变、宇宙辐射等随机物理现象[2]. 众多熵源中应用最广泛的是热噪声. 热噪声是导体中的电子随机运动产生的电压波动[3],基于热噪声的TRNG电路设计方法主要包括:亚稳态采样、热噪声放大和环振抖动三种方法. 亚稳态采样分为两个阶段:第一阶段让双稳态电路稳定在亚稳态;

收稿日期:2018-10-29;修回日期:2018-12-14;责任编辑:马兰英
基金项目:浙江省公益性技术应用研究计划项目(No. 2016C31078);国家自然科学基金(No. 61574041, No. 61874078)

第二阶段电路由亚稳态过渡到稳态. 过渡过程中由热噪声决定输出电平. 该方法具有较高的数据吞吐率[4],但需要占用大量面积. 热噪声放大法利用高增益高带宽差分运算放大器直接放大节点上的热噪声,并将噪声电平与参考电平比较,从而获得高质量的随机序列[5]. 然而热噪声放大法采用的是 sign 量化模式[6],抗干扰能力差. 环振抖动法是将电路热噪声转换为相位抖动,用抖动的低频信号采样高频信号获得随机输出. 其电路结构简单,但随机性差,需要额外电路来增强随机抖动. 文献[6]提出基于抖动采用的具体设计,该方案通过放大电阻热噪声来增强相位抖动,同时利用闭合环路稳定工作点,可有效抵御闪烁噪声,且几乎不受电源与衬底耦合噪声影响. 但其输出速率慢,比特率仅为 4Mbps.

鉴此,提出利用放大的热噪声控制压控振荡器 VCO 使其产生在中心频率附近随机抖动的慢振荡信号. 慢振荡信号对周期确定的快振荡信号采样获得原始序列,经后处理得到随机输出序列. 由于电阻热噪声在热噪声发生器和 VCO 中被分别放大,使得 TRNG 在较高比特率下依旧可以保证足够的随机性. TRNG 比特率由热噪声发生器输出的直流电平决定. 直流电平越高,比特率越高,随机性降低;反之,比特率降低,随机性提高,因此可在随机性和比特率之间权衡.

2 TRNG 电路设计

基于 VCO 的真随机数发生器的电路结构框图如图 1 所示. 热噪声发生器输出的直流电平决定 VCO 的中心频率,其上叠加的电阻热噪声增强 VCO 频率抖动. 压控振荡器所产生的慢振荡信号通过 D 触发器对周期固定的快振荡信号进行采样. 由于慢振荡器的随机抖动范围远远大于快振荡器周期,从而生成原始随机序列. 后处理电路用以消除原始随机序列的不均匀和自相关性,以提高序列的随机性.

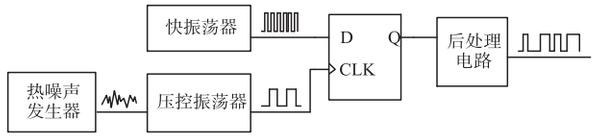

图1 真随机数发生器整体框图

2.1 热噪声发生器

热噪声由导体中载流子的热振动引起,它使沟道电流产生微小波动,从而在导体两端产生波动电压. 其单边谱密度为:

$$S_v(f) = 4kTR, f \geq 0 \qquad (1)$$

式(1)中,$k = 1.38 \times 10^{-23}$ J/K 为玻尔兹曼常数;T 为热力学温度,R 为电阻阻值,f 为频率. 可以发现,热噪声本质上是白噪声,有完美的统计特性,是理想的随机源. 但是其标准差(σ)小,需经放大才能有效提高慢振荡信号频率随机性.

设计中热噪声发生器主要由电阻串型 DAC、运算放大器和外围电阻组成. 其结构如图 2 所示,电阻 $R1$、$R2$ 为热噪声电阻,用以增强运放输入节点的热噪声;运放经 $R3$、$R4$ 负反馈连接,实现 200 倍的闭环增益以放大热噪声;电路输入端 Vref 的直流电压由外部电压源提供. 在运放的共模输入范围内调节 Vref 的电压值以决定输出端 Vout 直流电平进而控制 VCO 的中心频率. DAC 补偿运放的失调电压. 经蒙特卡罗仿真运放的失调电压在 ±12mV,因此 DAC 精度定为 1.5mV,使得补偿既能覆盖失调范围又能防止失调电压被放大造成运放脱离线性工作区.

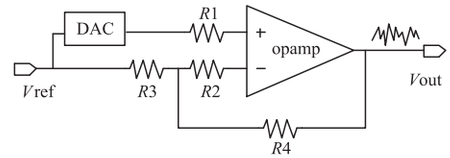

图2 热噪声发生器结构

仿真可得,运放输出端热噪声标准差(σ)为 14.6mV,足以满足需要. 热噪声发生器输出的噪声信号作为 VCO 的输入,以增强慢振荡信号的频率抖动.

2.2 压控振荡器

压控振荡器的结构如图 3 所示. $M3$ 和 $M6$ 作为电流源分别镜像放大 $M2$ 和 $M1$ 的电流. 当振荡器输出低电平时,$M4$ 导通,$M5$ 截止,使得流过 $M3$ 的恒定电流对电容 $C1$ 充电. 当电容 $C1$ 上的电压升高到 V_{SPH}(施密特触发器的正向阈值电压)时,施密特触发器输出变为低电平. 这使得振荡器输出变为高电平,流过 $M6$ 的恒定电流开始对电容 $C1$ 放电. 当电容上的电压放电至 V_{SPL}(施密特触发器的负向阈值电压)时,施密特触发器的输出又变为高电平. 这些输出状态持续进行转换,从而产生方波信号作为输出信号.

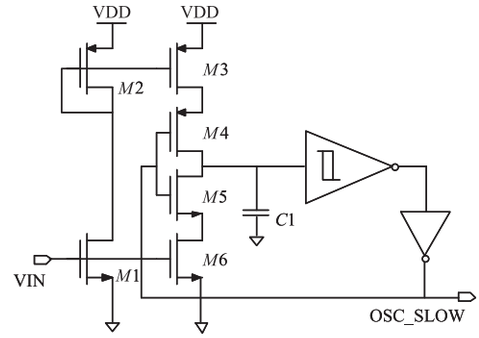

图3 压控振荡器结构

如果把 $M3$ 和 $M6$ 的漏电流分别记作 I_{D3} 和 I_{D6},那么可用下式来估算电容上的电压从 V_{SPL} 充电到 V_{SPH} 所需时间 t_1:

$$t_1 = C1 \cdot \frac{V_{SPH} - V_{SPL}}{I_{D3}} \tag{2}$$

从 V_{SPH} 放电到 V_{SPL} 所需时间 t_2:

$$t_2 = C1 \cdot \frac{V_{SPH} - V_{SPL}}{I_{D6}} \tag{3}$$

其中输入 VIN 的热噪声经 $M1$、$M2$、$M3$ 和 $M6$ 放大并转换为随热噪声电压而独立随机变化的电流,因此 t_1、t_2 也是随机变化的,VIN 通过控制电流的大小决定振荡频率. 振荡周期 $T = t_1 + t_2$,其均值 $E(T)$ 如式(4)所示:

$$E(T) = 2 \cdot C1 \cdot (V_{SPH} - V_{SPL}) \cdot \frac{1}{I_{D0}} \tag{4}$$

I_{D0} 是忽略 VIN 上叠加的热噪声时 I_{D3} 和 I_{D6} 的电流大小. 振荡器相位抖动可定义为输出时钟信号跳变相对于理想位置的偏移,该位置可以超前也可以滞后于时钟跳变的理想位置. 假设振荡器时钟周期的第 n 个周期为 T_n,则每个周期的抖动 J_n 为:

$$J_n = T_n - E(T) \tag{5}$$

相位抖动的均方差 J_{RMS} 为:

$$J_{RMS} = \lim_{N\to\infty} \sqrt{\frac{1}{N}\sum_{n=1}^{N} J_n^2} \tag{6}$$

J_{RMS} 与热噪声幅值呈正相关,通常要求慢振荡器抖动标准方差大约在快振荡器周期的 10 ~ 20 倍之间[7],以提高真随机数发生器抗干扰能力和输出序列随机性.

2.3　后处理电路

为了弥补输出分布的不均匀并消除自相关性,采用 XOR 纠偏法对原始序列进行后处理. 设 X 和 Y 分别为两位随机数,其期望值 $E(X) = E(Y) = u$,p 是它们的相关性,则:

$$E(X \oplus Y) = \frac{1}{2} - 2(u - \frac{1}{2})^2 - 2pu(1-u) \tag{7}$$

当 u 接近 1/2 时,式(7)可表示为:

$$E(X \oplus Y) \approx \frac{1}{2}(1-p) \tag{8}$$

由式(8)可知,若 X 和 Y 是相互独立的(即 $p = 0$),则 $E(X \oplus Y) \approx 1/2$. 若有 n 位彼此独立的随机数进行 XOR,则其期望值为:

$$\frac{1}{2} + (-2)^{n-1}(u - \frac{1}{2})^n = \frac{1}{2}(1 + (-2m)^n) \tag{9}$$

其中 $m = u - 1/2$. 从式(9)可以发现,随着 n 的增大,期望趋近于 1/2. 通常间隔 9 位以上数据彼此间无相关性[8]. 因此,将 40 位 D 触发器组成移位寄存器,选出彼此相邻 10 位数据进行异或消除偏差. XOR 后处理电路结构如图 4 所示.

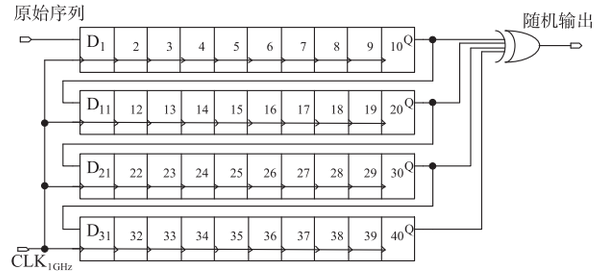

图4　XOR后处理电路

3　计算机仿真结果

电路采用 SMIC 55nm 工艺,核心版图如图 5 所示,采用 Cadence 的 Spectre 仿真器对电路仿真. 在 1.2V 电压、27℃下,Vref = 500mV,输出序列如图 6 所示. 其中,(a)是经采样后 D 触发器输出端的原始序列,(b)为后处理电路输出端序列,可以发现(b)相较(a)更为均匀. (c)为(b)中 40μs 至 56μs 局部放大的序列图,局部连续输出 0 的最长时间为 1.2μs(即 14 个周期),整体无明显偏向性.

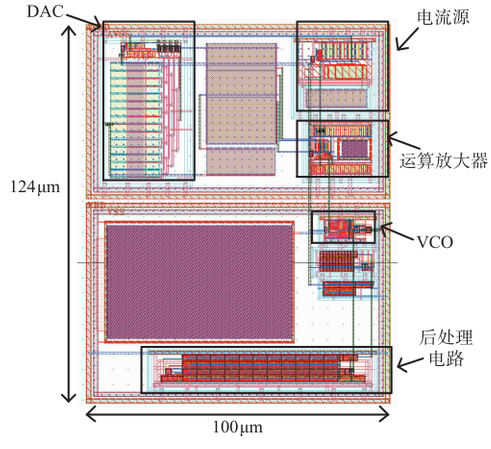

图5　TRNG版图

图 7 以像素点的方式展示了 3025 位随机输出序列(55×55),其中白色代表 1,黑色代表 0. 由图可见,0/1 分布整体均匀,无较大偏差. 将所得序列输入到 Matlab 测试自相关特性,结果如图 8 所示. 由图可知,在 95% 的自信区间内 2000 位连续数据间的自相关性近似为 0.

NIST 随机数测试是由美国国家标准与技术研究所开发的统计包,用于判定可能存在于序列中的各种非随机性. 将仿真获得的 5000 位随机序列分成 10 组,输入到 NIST 测试套件中进行检测. 测试结果如表 1 所示. P 值大于 0.01 则通过随机测试. 从测试结果可以发现,各项 P 值都处在较高水平,随机性优异.

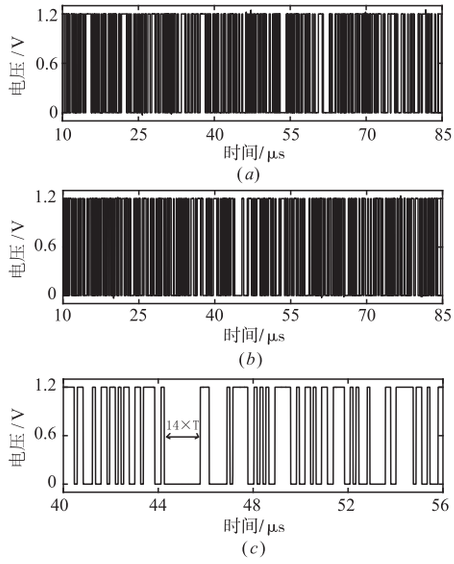

图6 TRNG输出序列

图7 输出序列的阵列展示

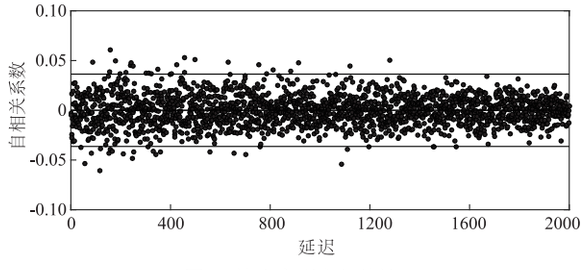

图8 输出序列自相关性

表1 NIST测试结果

NIST测试	*P*值	通过率(%)
频率检测	0.9114	100
块内频率检验	0.5341	100
累加和检验	0.5341	100
游程检验	0.3504	100
最长游程检验	0.3505	100
离散傅里叶变换检验	0.0668	100
非重叠模块匹配检验	0.6153	100
近似熵检验	0.9115	100
序列检验	0.3505	100

图9是电路在慢振荡信号频率为10MHz时的直方图.可以发现信号抖动呈高斯分布,平均值为9.08ns(约为快振荡信号周期的10倍),满足设计要求.对电路在不同工作频率下进行仿真,从图10可以发现,慢振荡信号抖动的标准差随着频率的升高而降低,因此序列随机性与比特率成负相关.而在固定工作频率下,序列随机性与温度成负相关.

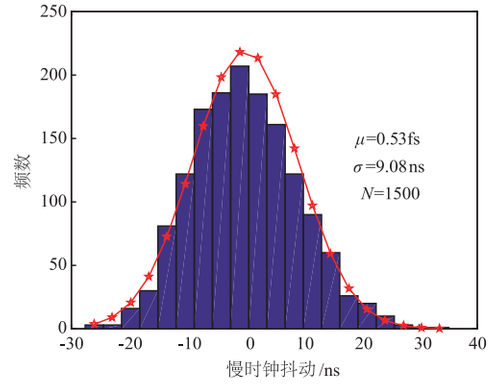

图9 慢时钟抖动频数直方图

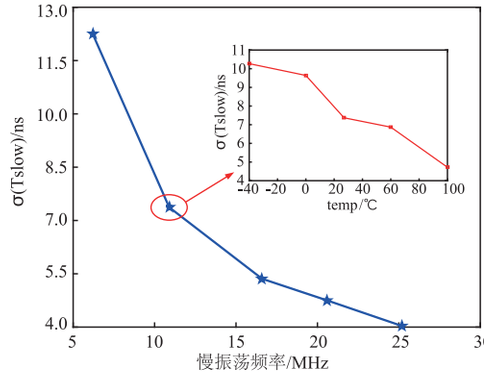

图10 慢时钟抖动vs振荡频率和温度

表2是所设计TRNG与其他文献对比.通过开环结构提高热噪声增益从而加快比特率,10Mb/s的比特率相较文献[6]和[10]提高约2.5倍,相较文献[9]提高10倍.但与文献[9]和[10]相比电路功耗较大,后期可以针对运放进行低功耗设计以降低能耗.

表2 相关文献对比结果

	工艺/nm	熵源	比特率/(Mb/s)	功率/μW	面积/(mm^2)
本设计	55	热噪声和环振抖动	10	810	0.0124
文献[6]	250	热噪声和环振抖动	4	4150	0.09
文献[9]	180	环振抖动	1	28	0.003
文献[10]	28	热噪声和环振抖动	4.6	388	0.025

4 结论

本设计首先利用热噪声提高 VCO 所产生慢振荡信号的相位抖动;然后通过慢振荡信号对周期固定的快振荡信号采样生成原始序列;最后用后处理电路消除序列自相关并增强其均匀性获得随机输出序列. 该电路可通过调节输入电压在序列随机性和比特率之间做出权衡. 所设计 TRNG 电路采用 SMIC 55nm CMOS 工艺实现,输出序列经 NIST 套件测试,具有较高的随机性,可应用于密钥生成和信号加密等领域.

参考文献

[1] Liu Y, Cheung R C C, Wong H. A bias-bounded digital true random number generator architecture[J]. IEEE Transactions on Circuits & Systems I Regular Papers, 2017, 64(1): 133 – 144.

[2] Wieczorek P Z. Lightweight TRNG based on multiphase timing of bistables[J]. IEEE Transactions on Circuits & Systems I Regular Papers, 2016, 63(7): 1043 – 1054.

[3] Srinivasan S, Mathew S, Erraguntla V, et al. A 4Gbps 0.57pJ/bit process-voltage-temperature variation tolerant all-digital true random number generator in 45nm CMOS [A]. International Conference on VLSI Design[C]. New Delhi: IEEE, 2009. 301 – 306.

[4] Mathew S K, Srinivasan S, Anders M A, et al. 2.4 Gbps, 7 mW all-digital PVT-variation tolerant true random number generator for 45nm CMOS high-performance microprocessors[J]. IEEE Journal of Solid-State Circuits, 2012, 47(11): 2807 – 2821.

[5] Brederlow R, Prakash R, Paulus C, et al. A low-power true random number generator using random telegraph noise of single oxide-traps[A]. International Solid State Circuits Conference-Digest of Technical Papers[C]. San Francisco: IEEE, 2006. 1666 – 1675.

[6] 邓焕,金荣华,陈俊,等. 基于振荡器的高性能真随机数发生器[J]. 固体电子学研究与进展, 2007, 27(3): 391 – 396.
Deng Huan, Jin Ronghua, Chen Jun, et al. Oscillator-based high performance truly random number generator[J]. Research & Progress of SSE Solid State Electronics, 2007, 27(3): 391 – 396. (in Chinese)

[7] Jun B, Kocher P. The Intel random number generator[S]. Cryptography Research Inc, white paper prepared for Inter Corp, 1999.

[8] Mathew S, Johnston D, Newman P, et al. μRNG: A 300μ950mV 323Gbps/W all-digital full-entropy true random number generator in 14nm FinFET CMOS[A]. European Solid-State Circuits Conference[C]. Graz: IEEE, 2015. 1 – 10.

[9] 童成盛,郎伟,万培元,常云峰,金银姬,林平分. 一种应用于智能卡的真随机数产生器的研究与设计[J]. 科技信息, 2013(05): 100 – 101.
Tong Chengsheng, Lang Wei, Wan Peiyuan, Chang Yunfeng, Jin Yinji, Lin Pingfen. Research and design of a true random number generator for smart cards[J]. Science & Technology Information, 2013(05): 100 – 101. (in Chinese)

[10] 魏子魁,符令,王雪,何洋,金鑫,谭浪,胡毅,唐晓柯,张海峰,赵东艳. 一种基于热噪声振荡器的高速真随机数设计[J]. 电子技术应用, 2018, 44(10): 29 – 31 + 36.
Wei Zikui, Fu Ling, Wang Xue, He Yang, Jin Xin, Tan Lang, Hu Yi, Tang Xiaoke, Zhang Haifeng, Zhao Dongyan. A high speed truly random number generator based on thermal noise oscillator[J]. Application of Electronic Technique, 2018, 44(10): 29 – 31 + 36. (in Chinese)

作者简介

汪鹏君(通信作者)　男,1966 年出生于浙江奉化,博士,教授,博士生导师,中国电子学会高级会员,中国计算机学会高级会员,中国电子学会电路与系统专业委员会委员,中国人工智能学会理事,目前主要从事低功耗、高信息密度集成电路理论和设计、安全芯片理论和设计、人工智能等相关理论和应用方面研究工作.
E-mail: wangpengjun@nbu.edu.cn

李　桢　男,1994 年出生于安徽铜陵,宁波大学信息科学与工程学院硕士研究生,主要研究方向为真随机数发生器设计.
E-mail: lizhengrys008@163.com