DOI: 10.13382/j.jemi.B2205684

基于可配置异步反馈环形振荡器的真随机数发生器*

鲁迎春 韩 倩 刘新颖 姚 亮
(合肥工业大学电子科学与应用物理学院 合肥 230009)

摘 要:作为现代加密系统不可或缺的一部分,真随机数发生器(TRNG)在信息安全中具有非常重要的作用。本文提出了一种可配置、轻量级、高吞吐量的真随机数发生器。该结构利用与非门和异或门构成了可配置的异步反馈环形振荡器,通过在短时间内增加相位噪声,来扩大时间抖动范围,从而改善了熵源的随机性。该结构在 Xilinx Kintex-7 进行了多次测试验证,实验结果表明,在不同温度(0℃~80℃)和不同输出电压(0.8~1.2 V)的环境变化下,所提出的 TRNG 具有较强的鲁棒性,在硬件资源上仅消耗了 43 个 LUTs 和 6 个 DFFs,并且获得高达 300 Mb/s 的吞吐量。同时,生成的随机比特流能够以较高的 P 值通过 NIST SP800-22 和 NIST SP800-90B 测试。

关键词: 真随机数发生器;可配置异步反馈环形振荡器;轻量级;高吞吐量
中图分类号: TN47 **文献标识码**: A **国家标准学科分类代码**: 510.3040

True random number generator based on configurable asynchronous feedback ring oscillator generator

Lu Yingchun Han Qian Liu Xinying Yao Liang
(School of Electronic Science and Applied Physics, Hefei University of Technology, Hefei 230009, China)

Abstract: As an indispensable part of modern encryption system, true random number generator (TRNG) plays a very important role in information security. A configurable, lightweight and high throughput true random number generator is presented. The structure uses NAND gates and XOR gates to form a configurable asynchronous feedback ring oscillator. By increasing the phase noise in a short time, the time jitter range is expanded, so as to improve the randomness of entropy source. The structure is tested and verified on Xilinx Kintex-7 for many times. The experimental results show that the proposed TRNG has strong robustness under the environmental changes of different temperatures (0 ℃ ~ 80 ℃) and different output voltages (0.8 ~ 1.2 V), and only consumes 43 LUTS and 6 DFFs in hardware resources, and obtains a throughput of up to 300 Mb/s. At the same time, the generated random bit stream can pass the NIST SP800-22 and NIST SP800-90B tests with high P values.

Keywords: true random number generator; configurable asynchronous feedback ring oscillator; lightweight; high throughput

0 引 言

随着云计算和物联网设备的兴起,信息安全问题受到了人们的广泛关注。用于创建随机密钥、质询响应协议中的参数、填充值和初始化向量的随机数对安全性至关重要[1-2]。伪随机数(pseudo random number, PRN)由于确定性算法在输出序列上具有一定的周期性和可预测性,降低了攻击复杂性。在高度可靠的加密系统中,使用不确定的物理源产生的真随机数发生器(true random number generator, TRNG)成为人们的首选。根据物理源的不同,TRNG 可以分为模拟 TRNG 和数字 TRNG。模拟 TRNG 的熵源来源于热噪声[3]、光电效应[4]和磁隧道结[5]等,将模拟器件产生的连续值通过比较器或混沌机制[6]量化成随机比特流,然而受到设备和工艺的限制,这一过程非常复杂且成本较高。数字 TRNG 的熵源主要来源于抖动[7-20](通常由电噪声引起)和亚稳态(通常由于输入信号和时钟信号违反建立和保持时间)[21-22],通过

收稿日期: 2022-07-14 Received Date: 2022-07-14
*基金项目:青年教师科研创新启动专项 A 项目(JZ2022HGQA0233)、国家自然科学基金重大科研仪器研制项目(62027815)资助

采样电路提取并量化熵源的随机性,得到原始比特流。若原始比特流的随机性不好,则需要冯诺依曼处理器或哈希函数等后处理过程。作为半定制电路的现场可编程门阵列(field programmable gate array,FPGA),由于其低成本和易于实现性,逐渐成为 TRNG 设计的主流平台。

基于 FPGA 的 TRNG 的熵源结构主要有锁相环(phase locked loop,PLL)[7-8]、数字时钟管理器(digital clock manager,DCM)[9]、自定时环(self-timed loop,STR)[10-13]和环形振荡器(ring oscillator,RO)[14-20]。基于 PLL 和 DCM 的 TRNG 虽然结构简单,易于实现,但是需要不断地手动调整参数或者通过复杂的算法才能找到合适的参数配置,达到随机数的安全性和高吞吐量[7-9],且该设计移植性较差。Martin 等[10]提出的基于 STR 的 TRNG,能够实现自动化布局布线,从而具有较高的移植性,但是该设计在 FPGA 实现较为复杂且吞吐量只有 32 Mb/s。相对于基于 PLL、DCM 或 STR 的 TRNG,RO 具有较易在 FPGA 中实现的特性,备受研究者的青睐。基于 RO 的 TRNG 利用时钟抖动作为熵源,但是由于时钟抖动的范围非常小,容易采集到确定的值,使输出值不具备随机性。为解决这个问题,最经典的结构是 Sunar 等[14]提出的将多个环形振荡器并行来增加抖动范围。然而,该方法消耗了太多的硬件资源,且吞吐量也不高。为了进一步提高吞吐量,文献[15]将快速进位链配置为延迟线,进行高精度采样时钟抖动,由于严格的路径延迟要求需要手动布局布线,实现过程较为繁琐。文献[17]通过相关采样的方式来获得较高的采样分辨率,从而采集到尽可能多的抖动,此结构可以通过算法自动匹配好 RO 的频率,无需手动布局布线,但是用到的算法较为复杂且资源消耗仍然过大。文献[18]中采用可配置延迟线的方式来产生较大的振荡变化,该设计虽然较文献[15]在资源开销上有所降低,但是其吞吐量也局限于 48 Mb/s。

为了解决 TRNG 的低硬件资源开销和高吞吐量之间不能兼容的问题,本文中提出了一种可配置的异步反馈环形振荡器(configurable asynchronous feedback ring oscillator,CAFRO)结构。通过异步反馈结构,在短时间内迅速增加了相位噪声,扩大时间抖动范围。不仅能够以较低的资源开销得到较高的吞吐量,还可以通过配置异或门的输入端为“1”或“0”,来决定反馈电路中的反相器位置,具有较强的可配置性,缩短了设计周期。本文的贡献如下:

1)提出的 CAFRO TRNG 通过异步反馈结构获得抖动累积,以较低的硬件资源开销得到 300 Mb/s 的高吞吐量。

2)提出的 CAFRO TRNG 由于异或门的可配置性,可以决定反相器和缓冲门的位置,从而产生不同的反馈结构,以较低的成本和较短的设计周期得到不同的 TRNG 设计电路。

3)提出的 CAFRO TRNG 仅使用了查找表资源,易于在不同设备之间进行移植。同时,在电压和温度变化范围内表现出良好的鲁棒性,生成的随机序列以较高的 P-value 值通过 NIST 随机性测试。

1　真随机数发生器相关设计

在 FPGA 平台上,RO 是创建 TRNG 较为简单有效的方法,一个简单的 RO 是由奇数量的反相器构成。如图 1 所示,在理想情况下,任何一个反相器的输出端都将是方波,严格满足 $Q(t+T)=Q(t)$ 关系,其中 $T=2nT_{\text{delay}}$,n 为反相器的个数,T_{delay} 为单个反相器的延迟时间,T 则为环形振荡器的周期。然而,由于电噪声(主要为散粒噪声和热噪声)的存在,波形的上升沿和下降沿都会提前或延迟,形成不可避免的抖动。Sunar 等[14]指出抖动近似服从正态分布 $N(\mu,\sigma^2)$,其中 μ 为理想的上升沿和下降沿位置,σ 为抖动的标准差。研究表明,在一次抖动中存在至少为 0.8 bit 的熵,通过概率统计学可以算出单次抖动的宽度 w 为 1.398σ。如果抖动的宽度被限制在环形振荡器周期的 1/2(即 $T/2$),则抖动的熵源 P_s 为式(1)所示:

$$P_s\left\{w \leqslant \frac{T}{2}\right\}=\int_{\mu-\frac{T}{4}}^{\mu+\frac{T}{4}}\frac{1}{\sqrt{2\pi}\sigma}\mathrm{e}^{-\frac{(x-\mu)^2}{2\sigma^2}}\mathrm{d}x \tag{1}$$

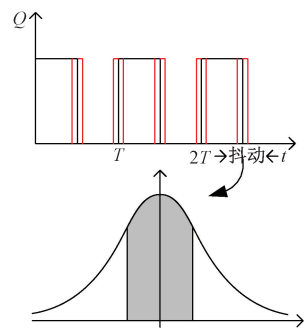


图 1　波形抖动图

Fig. 1　Waveform jitter diagram

从式(1)中可以得出,时间抖动的宽度越大,则获得的抖动熵源越大。然而,仅对一个环形振荡器进行采样,时间抖动宽度有限,容易采集到确定的值,大大降低随机数的质量。如图 2 所示,文献[23]中提出的经典 TRNG 结构,即将多个自由运行的环形振荡器(图 2 中简化为一个反相器、一个延迟 τ 和一个反馈回路)经过 D 触发器采样后,送入异或树(多输入异或单元)得到随机数。这种方法虽然扩大了边沿的不确定性,提高了随机数的质量,能够达到 100 Mb/s 的高吞吐量,但是硬件资源消耗仍然过大。在一些研究中,也有通过牺牲吞吐量来降低

硬件资源[24-25]，但是对于目前需求越来越高的高吞吐量TRNG设计的安全加密系统是不可取的。为了解决上述问题，本文提出的CAFRO TRNG既能以较低的硬件资源开销达到300 Mb/s的高吞吐量，也具有一定的可配置性，缩短TRNG的设计周期。所提出的CAFRO TRNG将在下节作出详细介绍。

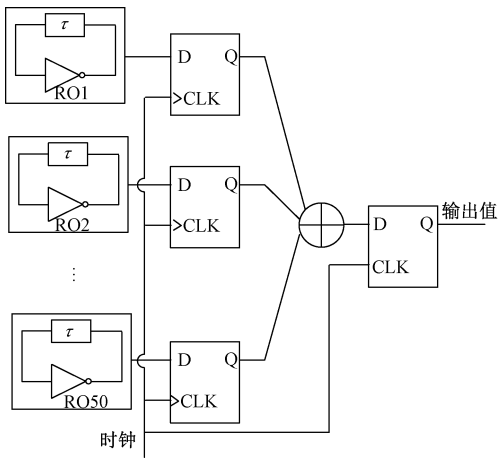


图2　基于多组RO的TRNG

Fig. 2　TRNG based multi-RO

2　CAFRO TRNG设计原理

2.1　RO中相位噪声与频率的关系

在传统的RO设计上，硬件资源开销与吞吐量之间很难做到兼容。文献[26]指出RO的输出频率与RO的阶数之间的关系表达式为：

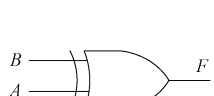
$$f_0 = \frac{1}{2Nt_D} \tag{2}$$

其中，N为反相器的个数，t_D为单个反相器延迟时间。从式(2)中可以看到，随着反相器个数的增加，RO的输出频率f_0会减小。而相位噪声表达式如式(3)所示，其中，k为波尔兹曼常数，T是绝对温度，P是RO的功耗，f是偏移频率，V_{DD}、V_{char}、R_L、I_{tail}、η是特定于RO噪声源的系数。可以看出，随着反相器阶数N的增加，相位噪声会得到优化，但伴随而来的是输出频率f_0的减小，导致吞吐量的降低。为了解决以上矛盾，本文通过异步反馈结构，在增加N的同时，由于反馈结构的频率累积，得到的振荡频率也不会降低，从而得到一个优质的熵源结构。

$$L_{\min}(f) = \frac{8}{3\eta}N\frac{KT}{P}\left(\frac{V_{DD}}{V_{char}} + \frac{V_{DD}}{R_L I_{tail}}\right)\frac{f_0^2}{f^2} \tag{3}$$

2.2　CAFRO结构

异或门的示意图和真值表如图3所示，若将输入端A作为配置端，当A配置为“0”时，则输出端$F=B$，此时异或门配置为缓冲门；当A配置为“1”时，则输出端$F=B^*$(本文中用$*$代表取反)，此时异或门被配置为反相器。



A	B	F
0	0	0
0	1	1
1	0	1
1	1	0

图3　可配置的异或门及其真值表

Fig. 3　Configurable XOR gate and its truth table

本文中提出的可配置异步反馈环形振荡器(CAFRO)如图4所示，基本结构是奇数个与非门串接而成，第1个与非门X_0作为使能端。可配置异步反馈结构由异或门组成，分为前向通道和反馈通道。在设计中，将前向通道的输入端$X_{2n-1,1}$置为1或将反馈通道的输入端$X_{2n-1,2}$置为1，即异或门在该位置被配置为反相器，促使数据状态发生翻转。否则，电路将不会振荡。

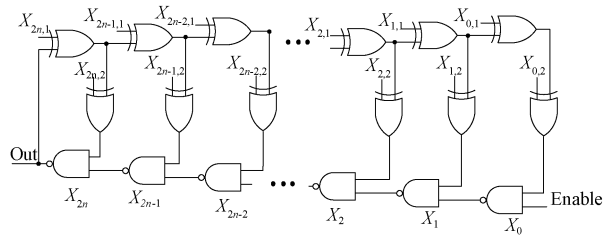


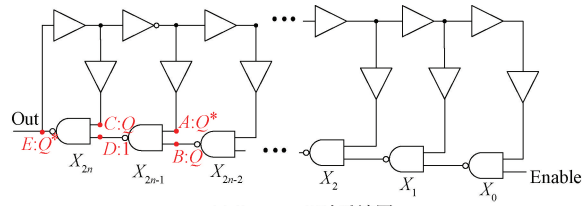
图4　CAFRO原理图

Fig. 4　CAFRO schematic diagram

在第$2n-1$级反馈通路中，将$X_{2n-1,1}$置为“1”，其他异或门的输入端配置为“0”，得到如图5(a)所示的结构示意图。当E结点的上一个状态为Q时，通过反相器的作用，可以得到A结点的值为Q^*；接着通过奇数个异步反馈结构和与非门的共同作用，可以得到B结点的值为Q；A、B两个结点共同作为与非门X_{2n-1}的输入端，通过逻辑代数中的互补律，得到D结点的值为1，由于C结点是由E结点通过2个缓冲门得到，所以和E结点的值保持一致。至此，可以得到E结点的当前状态为Q^*。当E结点为Q^*时，通过计算分别得到A、B、C、D的下一个状态分别为Q、Q^*、Q^*、1，通过X_{2n}这个与非门对C、D两个输入的计算可得E结点下一个状态为Q。

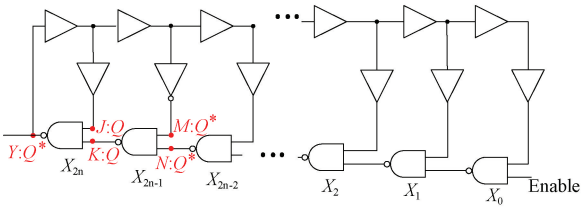
同理，如图5(b)所示，将$X_{2n-1,2}$置为“1”，当Y结点的上一个状态为Q时，通过与非门和缓冲门的作用可以得到N结点的当前状态值分别为Q^*，由于经过了反相器，得到M结点为Q^*。M和N作为X_{2n-1}的输入，经过逻辑代数中的重叠律，可以得到K结点的当前状态为Q，由于J结点为Q，所以可以得到Y结点的当前状态为Q^*；至此，可以算出M、N、J、K、Y下一个状态值分别为

Q、Q、Q^*、Q^*、Q。



(a) “$X_{2n-1,\ 1}$=1”时反馈图

(a) “$X_{2n-1,\ 1}$=1”feedback diagram



(b) “$X_{2n-1,\ 2}$=1”时反馈图

(b) “$X_{2n-1,\ 2}$=1” feedback diagram

图 5　第 $2n-1$ 阶反馈图

Fig. 5　$2n-1$ order feedback diagram

如此循环往复下去,在理想情况下,输出应该为方波,但由于抖动的存在,使输出不再为标准方波。CAFRO 的输出端表达式如下所示:

$$\begin{cases} Q^{n+1} = f(x)\,Q^n \\ f(x) = (1 + x + x^2 + \cdots + x^{2n+1})\,h(x) \end{cases} \tag{4}$$

其中,$f(x)$为异步反馈系数,$h(x)$为异步反馈开关。当 $X_{2n-1,1}=1$ 或 $X_{2n-1,2}=1$ 时,$h(x)=1$,开关打开,异步反馈有效;当 $h(x)=0$ 时,整个电路异步反馈无效,停止振荡。由于异步反馈结构的存在,一方面相当于在短时间内增加环形振荡器的阶数,提高抖动的范围,增加了不确定值的概率;另一方面有效地缩短了环形振荡器的周期,通过异步反馈结构形成频率累积,提高了环形振荡器的振荡频率,有效地解决了不能同时增加环形振荡器阶数和频率的矛盾。

2.3　CAFRO TRNG 框架

如图 6 所示,本文所提出的 CAFRO TRNG 结构在 Xilinx Kintex-7 和 Xilinx Virtex-6 开发板上实现,该结构由 CAFRO、异或树、D 触发器、数字时钟管理器、寄存器以及软核组成。通过数字时钟管理器对板卡上的晶振(差分时钟)进行分频,得到 3 路时钟。其中第 1 路时钟用作 D 触发器的时钟信号输入,此部分用来采样 CAFRO 组成的熵源,得到随机数。第 2 路时钟作为 FIFO 的时钟输入,此部分用来对产生的随机数进行缓存。第 3 路时钟为软核提供工作时钟,此部分一方面用来控制 CAFRO 中的使能信号,使环形振荡器能够持续振荡;另一方面将暂存在 FIFO 中的随机数通过串口发送到 PC 端。本文将 PC 上得到的随机数经过随机数质量评估,包括随机性测试、偏移度测试、自相关测试和鲁棒性测试。值得注意的是,由于电噪声引起的时间抖动范围很小,对一个 CAFRO 的输出信号的上升沿进行采样,很容易采集到确定值,这将极大地减少熵源的积累,降低随机数的质量。因此,本文采用经典的累积法,对 6 个并行的 CAFRO 进行采样量化,得到最终高质量的随机数。

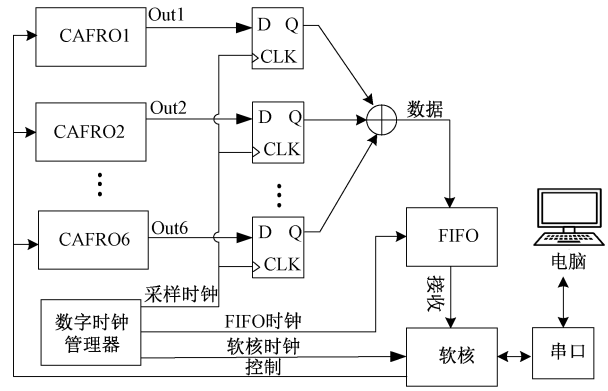


图 6　CAFRO TRNG 整体架构

Fig. 6　CAFRO TRNG genral architecture

3　实验结果与分析

随机数的本质属性是不可预测性,表现为非周期性、独立性和均匀分布性。在本部分中,通过对随机数经过 NIST 测试、偏移度测试和自相关测试,旨在检验本文结构产生随机数的不可预测性。最后在不同的环境下同的电压和较宽的温度范围内),评估 CAFRO TRNG 的鲁棒性。为了表明本文提出的 CAFRO TRNG 结构具有良好的移植性,以上测试均在两种类型的板卡。实现其正常工作电压和温度分别为 1.0 V 和 20 ℃,每次实验均连续采样 100 万比特序列来进行随机性测试。

3.1　NIST 测试

1) NIST SP 800-22 测试

NIST SP 800-22 是 NIST 公布的随机数测试标准,通过同时计算多个比特数据,优化统计测试公式和降低计算复杂度等方法,来简单有效地评估熵源。本次使用的 NIST 测试版本为 sts-2.1.2,共有 15 个随机测试项。该测试主要验证所提出的 TRNG 在正常工作电压和温度下生成的随机序列的随机性。为了避免单块开发板测试数据的偶然性,所提出的结构在两块不同的 Kintex-7 开发板和两块不同的 Virtex-6 开发板上进行连续 100 组的随机序列测试。其中 P-value 值为序列随机数的指标(当 P-value 值大于 0.01 时,表明熵源具有良好的随机性),Prop. 为 100 组测试的通过率。如表 1 所示,所有测试项均以较大的 P-value 值通过 NIST SP 800-22 测试,表明该 TRNG 结构生成的随机序列具有较好的随机性。

表1　Kintex-7和Virtex-6上NIST SP800-22测试结果(温度20 ℃,电压1.0 V)

Table 1　NIST SP800-22 test results on Kintex-7 and Virtex-6(temperature 20 ℃, voltage 1.0 V)

NIST SP 800-22	Kintex-7 FPGAs				Virtex-6 FPGAs			
随机性测试	Chip1		Chip2		Chip1		Chip2	
	P-value	Prop.	P-value	Prop.	P-value	Prop.	P-value	Prop.
频率检验	0.437 27	100%	0.555 94	100%	0.416 22	99%	0.418 06	99%
累加和检验	0.699 31	99%	0.516 12	99%	0.595 55	100%	0.518 74	100%
块内频数检验	0.626 95	100%	0.313 10	100%	0.226 50	100%	0.455 94	99%
游程检验	0.798 14	100%	0.637 12	99%	0.534 15	100%	0.554 42	100%
块内最长游程检测	0.236 81	100%	0.484 77	100%	0.304 13	97%	0.574 90	97%
二元矩阵秩检验	0.108 79	100%	0.224 82	98%	0.779 19	99%	0.494 39	100%
离散傅里叶变换检验	0.739 92	99%	0.437 27	97%	0.416 98	100%	0.401 20	100%
非重叠模块匹配检测	0.457 17	99%	0.447 65	99%	0.504 81	98%	0.400 21	99%
重叠模块匹配检验	0.475 19	100%	0.485 48	99%	0.851 38	99%	0.236 81	100%
通用统计检验	0.224 82	99%	0.565 89	99%	0.719 75	97%	0.637 12	98%
近似熵检验	0.153 76	99%	0.504 44	98%	0.616 31	100%	0.262 25	100%
随机游动检验	0.435 01	100%	0.166 47	98%	0.522 40	99%	0.442 58	99%
随机游动状态频数检验	0.430 85	99%	0.410 14	99%	0.578 16	100%	0.383 41	99%
序列检验	0.355 90	99%	0.136 24	98%	0.264 76	99%	0.108 25	100%
线性复杂度检验	0.383 24	100%	0.477 21	97%	0.637 12	100%	0.202 27	100%

注:对于每组测试,进行了100次实验,P-value是100次实验的平均值。对于累加和检验,非重叠模快匹配检验,随机游动状态检验,随机游动检验和序列检验,表中P-value是对应测试项所有子测试P-value的平均值

2)NIST SP 800-90B测试

NIST SP 800-90B测试是NIST提出的另一种统计测试套件。该测试方法使用了更为严格的方法来估计随机序列的统计分布和最小熵估计。数据之间不具有相关性是序列随机的一个表征。此项测试分为独立同分布测试(IID测试)和非独立同分布测试(非IID测试),若数据能通过IID测试,则可以认为数据独立同分布。IID测试包括排列测试、卡方测试、最长重复子串长度测试(LRS)和重启测试,其中IID最主要的是排列测试,该测试包含11项测试。将原始序列排列10 000次得到的统计值 T 与原始序列的统计值 T_i 进行比较,若 T 大于 T_i,则计数器 $C_{i,1}$ 加1;若 T_i 等于 T,则计数器 $C_{i,0}$ 加1,此时认为排列之后的数据与原始数据的统计值相似,即原始输入序列是独立同分布的。如表2所示,本文提出的TRNG结构在Kintex-7和Virtex-6开发板上分别以最小熵为0.996 188和0.995 535通过了NIST SP 800-90B的IID测试,证明序列的随机性。

3.2　偏移度和自相关测试

本文在两块Xilinx Kintex-7 FPGA和两块Xilinx Virtex-6上进行了实验,对产生的随机序列进行了偏移度测试和自相关性测试。图7是偏移度测试的图,其中黑白像素分别代表序列中的"0"和"1",若一个序列无偏移,则黑白图像均匀;若序列有较大的偏移,则图像会显示大片黑色图像或大片白色图像。从图中可以看到黑白图像分布均匀,可认为该序列无偏移度。序列的自相关性测试在MATLAB平台上实现,通过皮尔逊相关系数可知,当系数小于0.3时,可认定序列不相关。如图8所示,将滞后值设置为100,通过计算当前的输出值与100个滞后变量的相关系数,可以看到纵坐标的自相关系数均小于3×10^{-3},接近于0,表明该序列无相关性。通过两项测试,进一步表明本文提出的TRNG结构能够产生真随机数,不易受到攻击。

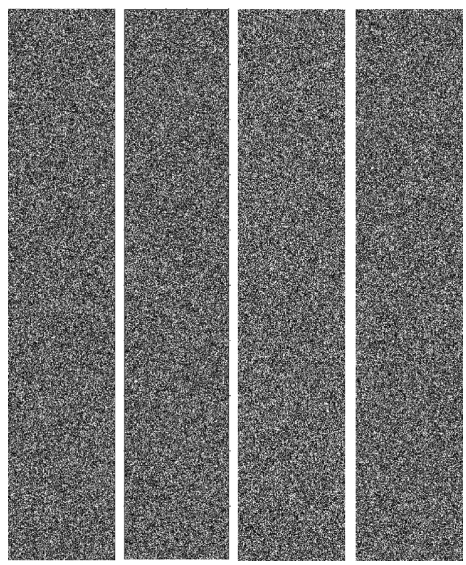


图7　4组偏移度测试图

Fig. 7　Four groups of bitstream test images

表 2　Kintex-7 和 Virtex-6 上 NIST SP800-90B 测试结果

Table 2　NIST SP800-90B test results on Kintex-7 and Virtex-6

NIST SP800-90B			Kintex-7 FPGA			Virtex-6 FPGA		
随机性测试			$C_{i,0}$	$C_{i,1}$	结果	$C_{i,0}$	$C_{i,1}$	结果
排列测试	偏移检验		8 065	0	pass	4 000	0	pass
	定向运行数量检验		7 938	17	pass	1 565	16	pass
	定向运行长度检验		2 519	3 996	pass	2 623	3 862	pass
	增加减少数量检验		1 533	28	pass	8 656	25	pass
	中位数数量检验		1 250	4	pass	4 471	8	pass
	中位数长度检验		2 117	1 677	pass	3 724	2 424	pass
	平均碰撞检验		4 220	6	pass	7 745	2	pass
	最大碰撞检验		8 493	683	pass	2 834	767	pass
	周期性检验	周期(1)	522	7	pass	7 850	14	pass
		周期(2)	9 523	6	pass	9 712	2	pass
		周期(8)	2 945	29	pass	2 239	16	pass
		周期(16)	2 310	22	pass	9 426	8	pass
		周期(32)	869	15	pass	5 422	33	pass
	协方差检验	协方差(1)	4 944	3	pass	6 872	2	pass
		协方差(2)	7 875	5	pass	6 501	7	pass
		协方差(8)	4 188	5	pass	4 461	5	pass
		协方差(16)	9 244	2	pass	7 364	4	pass
		协方差(32)	9 004	79	pass	2 893	7	pass
	压缩检验		3 497	79	pass	8 389	50	pass
卡方测试	卡方独立性检验			pass			pass	
	卡方拟合优度检验			pass			pass	
LRS 测试				pass			pass	
重启测试				pass			pass	
最小熵				0.996 188			0.995 535	

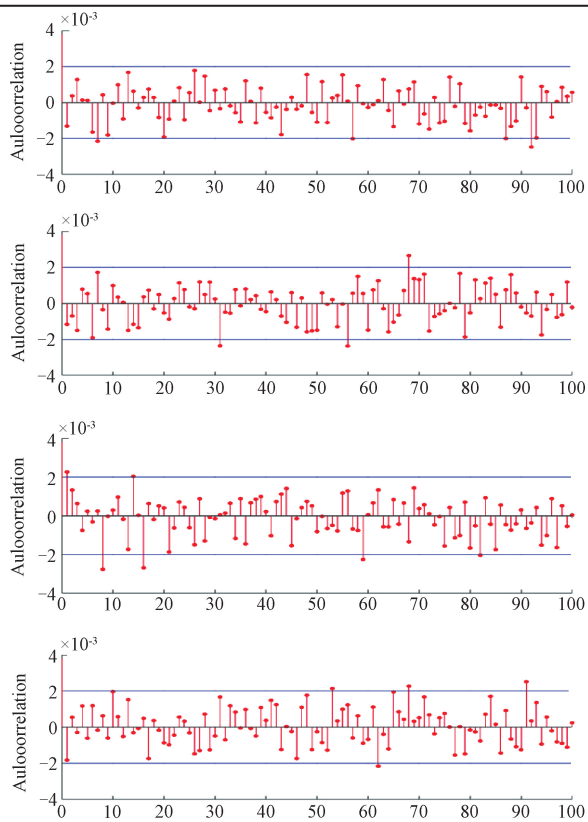


图 8　4 组自相关测试图

Fig. 8　Four groups of autocorrelation test images

3.3　鲁棒性测试

优良的 TRNG 在恶劣的环境变化下仍能产生高质量的随机序列。本文使用 Xilinx Kintex-7 FPGA 开发板在不同温度(0 ℃~80 ℃,20 ℃为步长)、不同的电压(0.8~1.2 V,0.2 V 为步长)进行了多次实验,实验结果如图 9 所示,雷达图中轴坐标表示不同的温度,不同颜色表示相应的电压,轴坐标上的数字表示在不同的工作条件下通过 NIST SP 800-22 的比例平均值。经分析,在正常的工作条件(1.0 V、20 ℃)下,通过率最高。随着电压和温度的改变,通过率会下降,但是仍然能够通过 NIST SP 800-22 测试。实验表明,该 TRNG 设计能够在不同的环境下稳定地产生随机数,具有良好的鲁棒性。

3.4　与相关的 TRNG 性能比较

通过 ISE 中的 XPower 功耗分析工具可得,本文提出的 CAFRO TRNG 结构总的逻辑块功耗为 1.36 mW。在资源消耗和吞吐量方面也和其他的 TRNG 结构进行了比较,结果如表 3 所示。以下 TRNG 设计均是在 FPGA 上实现的数字 TRNG,经对比,文献[14-15]硬件资源开销较大,且吞吐量也不高;在文献[16]中,虽然吞吐量有了质的提高,但是仍然牺牲了较高的硬件资源。后续提出的 STR[10-13]也存在同样的问题,不能同时达到资源开销小且吞吐量高的要求。本文提出的基于 CAFRO 的

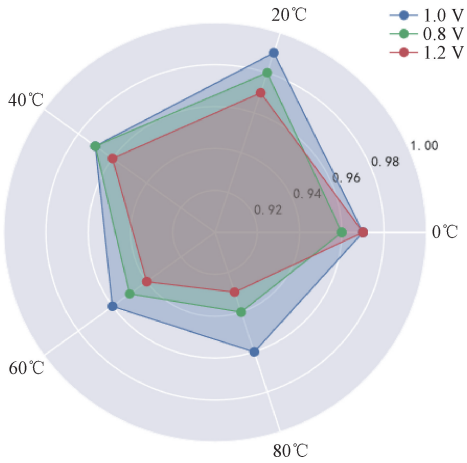


图9　鲁棒性测试

Fig. 9　Robustness test

TRNG结构从总体上看,在硬件资源仅消耗43个LUTs和6个D触发器的条件下,吞吐量能高达300 Mb/s,能够较好的平衡低资源开销与高吞吐量之间的矛盾。

表3　相关TRNG的比较

Table 3　Comparison of related TRNGs

TRNG结构	熵源	实验平台	资源消耗	吞吐量/(Mb·s^{-1})
[10]	STR	Vitex-5/6、Spartan-3E	32LUTs 48DFFs	32
[11]	STR	Vitex-5	320LUTs 320DFFs	200
[12]	STR	Zynq-7	/	100
[13]	STR	Vitex-6、Spartan-6	56LUTs 19DFFs	100
[14]	RO	Vitex-2 pro	565 slices	2.5
[15]	RO	Spartan-6	67 slices	14.3
[16]	RO	Artix-7	75LUTs 419DFFs	120
本文	CAFRO	Kintex-7、Virtex-6	43LUTs 6DFFs	300

4　结　论

本文提出了基于CAFRO的新颖TRNG结构,该结构使用6个并行的CAFRO作为熵源,通过D触发器进行采样量化生成随机序列,整个设计结构简单,便于实现,且易于移植;同时,通过对异或门的输入端进行配置,来决定不同的反馈电路,具有较强的可配置性,缩短了TRNG的设计周期。所提结构在Xilinx的Kintex-7和Virtex-6两种系列开发板上进行了验证,产生的随机数达到了300 Mb/s的高吞吐量,其硬件资源消耗仅为43个LUTs和6个D触发器。另外,实验表明,该结构在温度和电压变化的情况下仍然能够通过NIST SP 800-22测试,具有较好的鲁棒性。

参考文献

[1] WU X F, LI S G. A new digital true random number generator based on delay chain feedback loop[C]. IEEE International Symposium on Circuits and Systems (ISCAS), Baltimore, MD, USA, May 2017: 1-4.

[2] 刘清源,刘瑞佳,王健,等. 基于边缘计算的泛在电力物联网群组密钥管理算法研究[J]. 电测与仪表,2022,59(7):48-56.
LIU Q Y, LIU R J, WANG J, et al. Research on group key management algorithm of ubiquitous power Internet of things based on edge computing [J]. Electrical Measurement & Instrumentation, 2022,59(7):48-56.

[3] 汪鹏君,李桢,李刚,等. 基于压控振荡器的真随机数发生器设计[J]. 电子学报,2019,47(2):417-421.
WANG P J, LI ZH, LI G, et al. Design of true random number generator based on VCO[J]. Acta Electronica Sinca, 2019,47(2):417-421.

[4] UCHIDA A, HONJO T, AMANO K, et al. Fast physical random bit generator based on chaotic semiconductor lasers: Application to quantum cryptography [C]. CLEO/Europe-EQEC 2009-European Conference on Lasers and Electro-Optics and the European Quantum Electronics Conference, Munich, Germany, 2009.

[5] VATAJELU E I, NATALE G D. High-entropy STT-MTJ-based TRNG [J]. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2019, 27(2): 491-495.

[6] 应杰攀,宋贺伦,罗晓朋. 基于GaAs/AlGaAs超晶格受激混沌振荡的随机数发生器设计与实现[J]. 电子测量技术,2021,44(9):1-5.
PANG Y J, SONG H L, LUO X P, et al. Design and implementation of random number generator based on stimulated chaotic oscillation of GaAs/AIGaAs superlattice [J]. Electronic Measurement Technology, 2021,44(9):1-5.

[7] PETURA O, MUREDDU U, BOCHARD N, et al. Optimization of the PLL based TRNG design using the genetic algorithm [C]. 2017 IEEE International Symposium on Circuits and Systems (ISCAS), Baltimore, USA, 2017: 1-4.

[8] ALLINI E N, PETURA O, FISCHER V, et al. Optimization of the PLL configuration in a PLL-based TRNG design[C]. 2018 Design, Automation & Test in Europe Conference & Exhibition (DATE), Dresden, Germany, 2018: 1265-1270.

[9] JOHNSON A P, CHAKRABORTY R S, MUKHOPADYAY D. An improved DCM-based tunable true random number generator for Xilinx FPGA [J]. IEEE Transactions on Circuits and Systems II: Express Briefs, 2017, 64(4): 452-456.

[10] MARTIN H, PERIS-LOPEZ P, TAPIADOR J E, et al. A new TRNG based on coherent sampling with self-timed rings [J]. IEEE Transactions on Industrial Informatics, 2016, 12(1): 91-100.

[11] CHERKAOUI A, FISCHER V, FESQUET L, et al. A

very high speed true random number generator with entropy assessment[C]. 15th International Workshop on Cryptographic Hardware and Embedded Systems (CHES), Santa Barbara, USA, 2013: 179-196.

[12] LIU Y, CHEUNG R C C, WONG H. A bias-bounded digital true random number generator architecture [J]. IEEE Transactions on Circuits and Systems I: Regular Papers, 2017, 64(1): 133-144.

[13] WANG X, LIANG H, WANG Y, et al. High-throughput portable true random number generator based on jitter-latch structure [J]. IEEE Transactions on Circuits and Systems I: Regular Papers, 2021, 68(2): 741-750.

[14] SUNAR B, MARTIN W J, STINSON D R. A provably secure true random number generator with built-in tolerance to active attacks [J]. IEEE Transactions on Computers, 2007, 56(1): 109-119.

[15] ROZIC V, YANG B, DEHAENE W, et al. Highly efficient entropy extraction for true random number generators on FPGAs [C]. 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), San Francisco, USA, 2015: 1-6.

[16] WANG Y G, HUI C, LIU C, et al. Theory and implementation of a very high throughput true random number generator in field programmable gate array [J]. Review of Scientific Instruments, 2016, 87(4):044704.

[17] PEETERMANS A, ROZIC V, VERBAUWHEDE I. A highly-portable true random number generator based on coherent sampling [C]. 2019 29th International Conference on Field Programmable Logic and Applications (FPL), Barcelona, Spain, 2019: 218-224.

[18] ANANDAKUMAR N N, SANADHYA S K, HASHMI M S. FPGA-based true random number generation using programmable delays in oscillator-rings [J]. IEEE Transactions on Circuits and Systems II: Express Briefs, 2020, 67(3): 570-574.

[19] 罗芳,欧庆于,周学广,等. 故障扰动下振荡环型真随机数发生器安全特性及度量方法研究[J]. 电子与信息学报, 2022, 44(6): 2093-2100.
LUO F, OU Q Y, ZHOU X G, et al. Research on the security characteristic and metric method for ring oscillatro-based true random number generator under fault disturbance [J]. Journal of Electronics & Information Technology, 2022, 44(6): 2093-2100.

[20] 鲁迎春, 梁华国, 王鑫宇, 等. 一种基于环形振荡器的轻量级高效率的真随机数发生器 [J]. 电子测量与仪器学报, 2021, 35(3): 115-122.
LU Y CH, LIANG H G, WANG X Y, et al. Lightweight efficient ring oscillator-based true random number generator [J]. Journal of Electronic Measurement and Instrumentation, 2021, 35(3): 115-122.

[21] MAJZOOBI M, KOUSHANFAR F, DEVADAS S. FPGA-based true random number generation using circuit metastability with adaptive feedback control [C]. 13th International Workshop on Cryptographic Hardware and Embedded Systems (CHES 2011), Nara, Japan, 2011:17-32.

[22] STANCHIERI G D, DE MARCELLIS A, PALANGE E, et al. A true random number generator architecture based on a reduced number of FPGA primitives [J]. Aeu-International Journal of Electronics and Communications, 2019, 105: 15-23.

[23] WOLD K, TAN C H. Analysis and enhancement of random number generator in FPGA based on oscillator rings [C]. 2008 International Conference on Reconfigurable Computing and FPGAs, Cancun, Mexico, 2008: 385-390.

[24] PETURA O, MUREDDU U, BOCHARD N, et al. A survey of AIS-20/31 Compliant TRNG cores suitable for FPGA devices [C]. 26th International Conference on Field-Programmable Logic and Applications (FPL), Lausanne, Switzerland, 2016: 1-10.

[25] KAYSICI H I, ERGUN S. Duty cycle correction circuit and its application for high speed random number generation [C]. IEEE International Symposium on Circuits and Systems (IEEE ISCAS), Daegu, Korea, 2021: 1-5.

[26] HAJIMIRI A, LIMOTYRAKIS S, LEE T H. Jitter and phase noise in ring oscillators [J]. IEEE Journal of Solid-State Circuits, 1999, 34(6): 790-804.

作者简介

鲁迎春,于 2002 年获得合肥工业大学学士学位,2005 年获得合肥工业大学硕士学位,2021 获得合肥工业大学博士学位。现任合肥工业大学微电子学院副教授,主要研究方向为硬件安全和 FPGA 应用设计。
E-mail: luyingchun@ hfut. edu. cn

Lu Yingchun received his B. Sc. degree from Hefei University of Technology in 2002, M. Sc. degree from Hefei University of Technology in 2005 and Ph. D. degree from Hefei University of Technology in 2021, respectively. Now he is an associate professor at School of Microelectronics of Hefei University of Technology. His main research interests include hardware security and FPGA application design.

姚亮(通信作者),于 2016 年获得安徽工程大学学士学位,现为合肥工业大学博士研究生,主要研究方向为硬件安全和 FPGA 应用程序设计。
E-mail: 1462786438@ qq. com

Yao Liang (Corresponding author) received his B. Sc. degree from Anhui University of Engineering in 2016. Now he is a Ph. D. candidate in Hefei University of Technology. His main research interests include hardware security and FPGA application design.