DOI: 10.13382/j.jemi.B2003280

一种基于环形振荡器的轻量级高效率的真随机数发生器*

鲁迎春[1] 梁华国[1] 王鑫宇[1] 姚 亮[1] 倪天明[2] 易茂祥[1] 戚昊琛[1] 黄正峰[1]
(1. 合肥工业大学 电子科学与应用物理学院 合肥 230009; 2. 安徽工程大学 电气工程学院 芜湖 241000)

摘 要:真随机数发生器(TRNG)作为芯片中重要的安全组件,在现代加密系统中扮演着越来越重要的角色。对于 TRNG 的设计,关键是需要熵提取器可以在恶劣的环境变化(如工艺波动、电压和温度(PVT))下稳定地生成熵值。基于 Xilinx FPGA 平台提出了一种基于环形振荡器的低成本,高效率真随机数发生器。TRNG 一方面通过快速进位逻辑来提高熵提取的效率,另一方面通过优化电路结构和延迟,在以相对较低的资源开销情况下实现可观的吞吐量和随机性。TRNG 分别在多块 Xilinx Virtex6 FPGAs 和 Xilinx Spartan6 FPGAs 上进行验证,实验数据测试结果表明,所提出的 TRNG 能够在广泛的 PVT 范围内表现出良好的鲁棒性,且生成的随机比特流不仅以相当高 P 值通过 NIST SP800-22 统计测试套件,而且可以通过最新的 NIST SP800-90B 测试。

关键词: 真随机数发生器;快速进位链逻辑;低成本;高鲁棒性
中图分类号: TN47 **文献标识码**: A **国家标准学科分类代码**: 510.3040

Lightweight efficient ring oscillator-based true random number generator

Lu Yingchun[1] Liang Huaguo[1] Wang Xinyu[1] Yao Liang[1]
Ni Tianming[2] Yi Maoxiang[1] Qi Haochen[1] Huang Zhengfeng[1]
(1. School of Electronic Science and Applied Physics, Hefei University of Technology, Hefei 230009, China;
2. College of Electrical Engineering, Anhui Polytechnic University, Wuhu 241000, China)

Abstract: As an important security component in the chip, true random number generator (TRNG) plays an increasingly important role in modern encryption systems. For the design of TRNG, the key is to require an entropy extractor to stably generate entropy under severe environmental changes (such as process fluctuations, voltage and temperature (PVT)). Based on the Xilinx FPGA platform, a low-cost, high-efficiency true random number generator based on ring oscillator was proposed in this paper. The proposed TRNG improves the efficiency of entropy extraction through fast carry logic on the one hand, and optimizes the circuit structure and delay on the other hand to achieve considerable throughput and randomness with relatively low resource overhead. The TRNG proposed was verified on multiple Xilinx Virtex6 FPGAs and Xilinx Spartan6 FPGAs. Experimental data test results show that the proposed TRNG can exhibit good robustness in a wide range of PVT and generate random bit streams. Random bits only passed the NIST SP800-22 statistical test suite with a fairly high P value, but also passed the latest NIST SP800-90B test.

Keywords: true random number generator; fast carry chain logic; low cost; high robustness

0 引 言

随着互联网的快速发展,物联网和云计算等新兴技术已经渗入到人们的生活中,这些技术带来巨大便利的同时,但也给个人隐私带来极大威胁[1-2]。数据的安全和保护越来越受到人们的重视,加/解密算法和协议因此获得了广泛的应用,而在现代加/解密码系统中,随机数在密钥,初始化向量或填充值中起着关键作用[3-5]。由于确定性算法生成的伪随机数发生器(PRNG)的脆弱性,伪

收稿日期: 2020-06-29 Received Date: 2020-06-29
*基金项目:国家自然科学基金(61674048,61904001,61874156,61834006)、安徽省自然科学基金 (1908085QF272)项目资助

随机数不能满足高可靠性信息加密的要求。取而代之的是,利用非确定性随机过程(如电噪声或者量子现象)作为高度可靠的熵源的真随机数发生器(TRNG)引起了越来越多的关注。在很多情况下,真随机数发生器要求必须在生成过程中具有高吞吐量,具有在工艺波动、电压和温度(PVT)影响下稳定地工作的能力,占用硬件资源开销低。半定制集成电路现场可编程门阵列(FPGA)作为TRNG 的设计平台正变得越来越流行。

由于各种轻量级安全系统对 TRNG 的资源开销低和吞吐量的要求,先前有许多工作已经对其进行了大量研究。为了获得高吞吐量的 TRNG,Cherkaoui 等[6]提出了一种基于自定时环(STR)振荡器的 TRNG 结构。该设计虽然实现了 100 MB/s 的吞吐量,但该结构需要 511 级的 STR 振荡器,消耗了大量的 FPGA 资源。为了减少硬件开销,Honorio 等[7]基于 STR 的原理实现仅需要 32 个查找表(LUT)和 48 个寄存器的 TRNG,但其吞吐量仅为 4 MB/s 。国内也对 TRNG 的低开销和高效率进行了大量的研究,Zhang 等[8]提出利用 FPGA 内部资源快速进位链进行高精度采样的 STR 型 TRNG,该设计虽然在吞吐量上有了很大的提高,但是其消耗了大量的 LUT 资源。

结合国内外对于 TRNG 的研究现状可以看出,大部分的研究不能在 TRNG 的吞吐量和资源开销上做到兼优。本文提出的新型 TRNG 通过提高 Xilinx FPGA 上单个环形振荡器的采样精度来有效的从电路抖动中提取熵,不仅产生了高质量的随机比特流,且以非常低的硬件开销实现了高吞吐量。本文利用 FPGA 上的快速进位链配置为延迟线,可以以较高的高精度采样时序[9-10]。该设计通过一种新颖的设计策略通过选择最佳的 LUT 和路由来优化环形振荡器的延迟,以减少快速进位链的资源开销。本文的主要贡献如下:1)提出的 TRNG 通过紧凑的布局实现了 100 MB/s 的高吞吐量;2)提出的 TRNG 可以在较宽的温度,电压和工艺变化范围内表现出良好的鲁棒性;3)提出的 TRNG 生成的随机比特流以较高的 P 值通过 NIST 随机性测试。

1　相关工作

TRNG 电路利用不确定的随机过程(通常以电子热噪声的形式)作为随机熵源,利用提取熵源(噪声)的机制获得随机比特流,然后通过后处理进一步提高随机质量。对于熵源,在 FPGA 上设计的 TRNG 主要通过利用抖动和亚稳态的随机性来获得。由于很难获得完全无偏的物理源,因此基于亚稳电路的 TRNG 经常会面临严重的迁移现象(如统计不平衡数为 0 和 1),并且往往会严重损害 TRNG 提取的熵质量。抖动可以定义为与实际周期性信号的真实周期性之间的偏差,并且该偏差可以来自确定或随机的抖动源(如热噪声)。由于环形振荡器(RO)极易在 FPGA 中构造,因此大多数 TRNG 研究都是基于 FPGA 的 RO 结构设计[2,11-13]。如图 1 所示,由于存在热噪声,当 RO[14-15]开始工作时,采样波形的上升沿和下降沿存在不确定性,此不确定部分称为抖动。

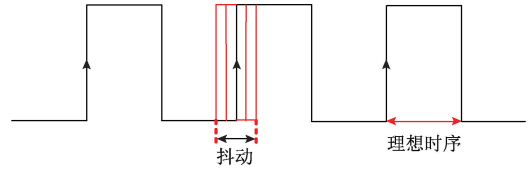


图 1　波形抖动

Fig. 1　Waveform Jitter diagram

根据文献[6]可知,在 FPGA 上提取抖动的随机性方法主要是构建 RO 或者其他形式振荡环。由于抖动区间很小(在 SRAM 型 FPGA 实验中约为几皮秒[16-17]),直接粗粒度采样 RO 抖动将导致非常低的随机性。为了提高 TRNG 的随机性,文献[18]提出如图 2 所示的典型多个并行 RO 抖动采样的 TRNG 结构,以生成高质量的随机比特流。但是,增加了该电路设计的复杂性。为了解决上述问题,本文提出一种具有高质量和低成本的 TRNG 结构。

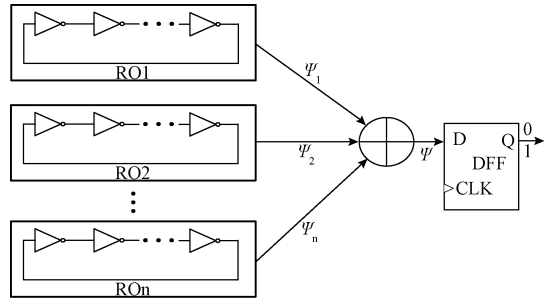


图 2　基于多组 RO 的 TRNG

Fig. 2　Multi-RO based TRNG

2　本文结构

介绍快速进位链的时间-数字转换(TDC)技术及有关熵源提取和延迟线的一般体系结构设计,并提出了一种随机序列的提取机制。

2.1　快速进位链

Nutt 在 1968 年提出 TDC 时钟脉冲测量结构,利用信号传递某些逻辑门的绝对传输时间,早期采用同轴线与集成电路一起实现延迟线[19]。TDC 结构的开发被移植到了 IC 中,并得到了迅速推广。如图 3 所示,整个延迟线由一组延迟单元组成,每个延迟单元都与一个触发器连接。当时钟脉冲结束时,触发器可以记录延迟的时间

单位数,从而实现了将时间转换成数字的测量。由图 3 可知,该测量方法的精确度取决于延迟单元 T1 的延迟时间。德国 ACAM 生产的 TDC-GP21 的精度为 45 ps[20],尽管它可以满足一般的时间测量要求,但对于高精度 TRNG 来说还是远远不够。

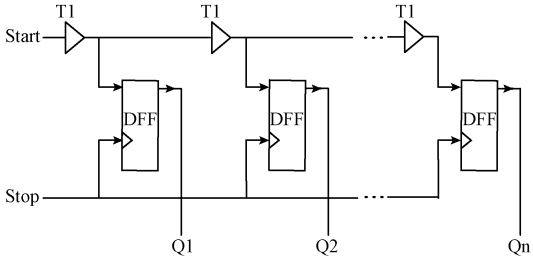


图 3　Nutt 的 TDC 结构

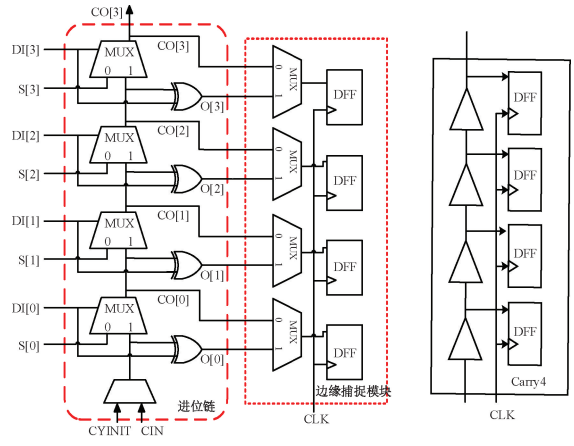
Fig. 3　Nutt's TDC structure

由于吞吐量增益随精度的提高而增加,本文提出的 TRNG 结构对抖动信号高精度采样,相比于传统方法可以提取更多的熵。快速进位链在高精度采样中起着非常重要的作用。在 Xilinx FPGA 上,快速进位逻辑(亦称为 Carry4),称为快速进位链原语,是在可配置逻辑块(CLB)中实现的,可配置逻辑块与查找表(LUT)配合工作以构建加法器和乘法器[9]。为了改善熵提取,快速进位链通常用于实现高精度 TDC 的重要部分。

如图 4(a)所示,快速进位链主要由 4 个选择器和 XOR 门组成,与通过 LUT 实现的延迟相比,其延迟要小的多。CYINIT 和 CIN 以及 S[3:0]作为进位链的输入端口,DI[3:0]是 4 个多路选择器(MUX)的选择端口,CO[3]和 O[3:0]作为输出端口,O[3:0]是 DI[3:0]和 CO[3:0]的 XOR 门的输出。在进行配置过程中,DI[3:0]配置为"1111",以便始终选通 MUX 的输入端口"1",将 CYINIT 值配置为"0",以使输入值始终取决于 CIN 的值。通过 DI 和 CYINIT 的配置,输出端口 CO[3]的值将始终与输入端口 CIN 一致,即实现延迟输入值缓冲区。利用快速进位链具有延时输入缓冲特性,通过 Verilog HDL 代码配置具有 4 个延迟单元的快速延迟链,并通过专用路由路径连接到相邻分片上的快速进位链,以实现更长的延时线。为了将进位链的每个电平的延迟数字化并捕获。图 4(a)的单元通过精确地划分延迟来改善熵提取时间,图 4(b)给出了该单元的简化示意图。

2.2　主要架构

吞吐量增益随着精度的提高而增加。熵源和快速延时线的架构如图 5 所示,熵源由自由运行的 n 级 RO 实现,该 n 级 RO 由一个与非门和多个缓冲器组成。快速延时线由具有 TDC 特性的多个快速进位链连接形成,RO 的波形输出连接到快速延迟线的输入。在时钟上升沿到达后,每个延迟级的输出数据都在 D 触发器中捕获。为



(a) 快速进位链
(a) The fast carry chain

(b) 快速进位链示意图
(b) Schematic of the fast carry chain

图 4　基本快速进位链结构

Fig. 4　Basic the fast carry chain structure

了捕获 RO 振荡器的完整波形,快速延时线的延迟必须大于 RO 的振荡周期,否则快速延迟线将无法捕获抖动的信号沿。

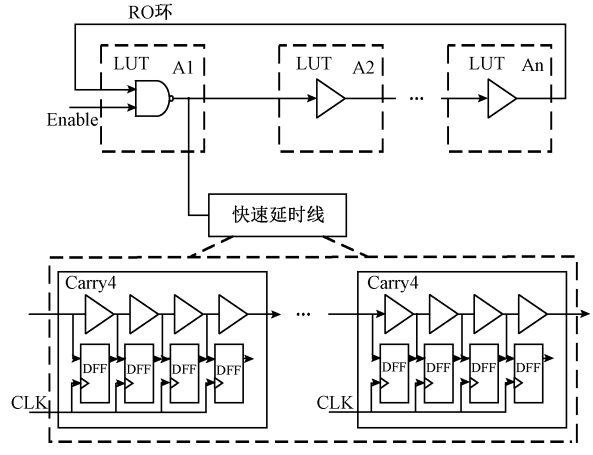


图 5　主要架构

Fig. 5　General architecture

2.3　随机序列提取机制

快速延迟线的延迟必须完全覆盖振荡器周期,但是,实验数据得知快速延迟线的延迟并不完全等于环形振荡器的振荡周期。为了确保捕获抖动信号的完整性并考虑外界环境变化(如温度,电压)对延迟的影响,通常使快速延时线的延时比环形振荡器的振荡周期稍长,但是这将可能导致出现多抖动信号的边缘[21]。另一方面,由于触发器的采样信号可能无法满足触发器建立/保持时间的需要,可能使触发器进入亚稳状态,出现输出不定的情况[22]。上述两种情况的出现,使得输出序列中存在异常翻转的数据位。为了解决这两种问题,本文提出了一种

新颖的随机数提取机制。

首先,本文采用一种简单有效的编码方法来提取随机性。优先编码用于检测由快速延时线采样生成的序列的边缘,原理是奇数位置定义为“0”,偶数位置定义为“1”。在正常情况下,快速延迟线的预期输出是连续的“1”跟随通过运行“0”或连续的“0”跟随运行“1”,信号边沿将在快速延迟线中捕获,如图6(a)所示。如果快速延迟线的输出序列中存在两个边沿,采取只检测到第一个跳变位置,而忽略第二个跳变位置方式。如图6(b)所示,在偶数位置出现第一个“1”跳变为“0”,则输出随机数编码为“1”。对于亚稳态现象引起的异常翻转导致无法确定跳变位置情况,采用滤波异常翻转位方式。如图6(c)所示,序列中的“1”异常被翻转为“0”,通过对此异常翻转位进行滤波,则序列跳变的位置为偶数位置,故随机数编码为“1”。

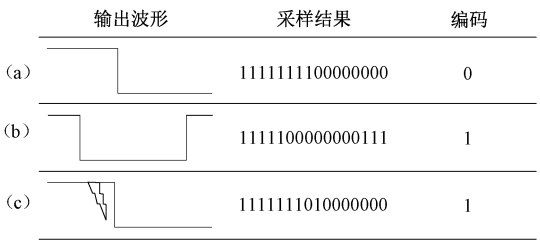


图6　多种情况下随机位生成

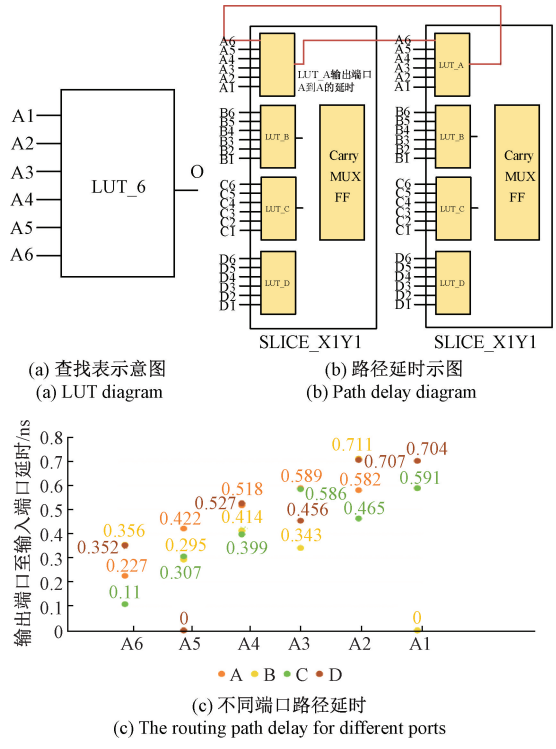
Fig. 6　Random number generation in multiple situations

3　硬件电路实现

本文所提出的TRNG结构在Xilinx Virtex-6 FPGA[9]和Xilinx Spartan-6 FPGA[23]上得以实现。为了获得最低的硬件开销,通过深入研究LUT的结构和路由资源(LUT,SRAM的FPGA中的基本可配置单元)来优化RO的延迟。六输入LUT(LUT_6)示意图如图7(a)所示,每个LUT_6含有6个输入端口(A1,…,A5,A6)和一个输出端口。如图7(b)所示,通过构建RO来测量输入端口到输入端口的延迟,根据Xilinx官方手册[9]可知,Xilinx FPGA中的每行或每列的CLB中LUT相似,故通过连接Slice_X1Y1和Slice_X1Y2来构建RO测量输入端口到输出端口的延迟。先前研究结果[21]如图7(c)所示,对于LUT,A1端口到输出延时最大,而A6端口是输出延时最小的端口。在减少布线延时情况下,选择A6端口作为每级的输入,其中与非门中的Enable端口选择延时其次的A5端口。

4　实验结果

本文通过两种实验对提出的基于RO的TRNG进行



(a) 查找表示意图
(a) LUT diagram

(b) 路径延时示图
(b) Path delay diagram

(c) 不同端口路径延时
(c) The routing path delay for different ports

图7　LUT原理

Fig. 7　Schematic of LUT

性能验证。第1种实验旨在检查提出的TRNG产生的随机比特流的随机性。另一种实验用于评估不同操作环境(温度和电压)下提出的TRNG的稳定性。本文提出的TRNG是在Xilinx Virtex-6 FPGA和Xilinx Spartan-6 FPGA开发板上实现的,其开发板的系统工作频率为100 MHz,正常工作电压为1.0 V,正常工作温度为20 ℃。本文每次实验均提取1 MB原始数据,然后进行NIST SP800-22 RNG测试套件(15个随机测试)[24]测试和NIST SP800-90B Test[25]进行评估。

4.1　NIST测试

1) NIST SP 800-22测试

该测试主要检查本文提出的TRNG在20°C的温度和1.0 V的电压下生成的随机序列的随机性。为了确保实验数据的准确性并避免单个开发板的实验数据偶然性,该实验在3块不同的Virtex-6开发板上进行,每块开发板上重复实验100次,每次实验测试的样本数据为1 MB。测试结果如表1所示,其中*P*-value表示测试结果,*Prop.*表示测试项通过的概率(100次测试中通过测试的概率)。

根据NIST SP800-22测试,对于每个测试结果的*P*-value,大于0.01的值表示被测随机序列的随机性良好。当然,较大的*P*-value表示更好的随机性,作为硬件安全性应用程序更可靠。如表1所示,随机比特流以高*P*-value通过每项的随机性测试。

表 1　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 Virtex-6(temperature 20 °C, voltage 1.0 V)

NIST Pub 800-22,	Chip#1 on V6		Chip#2 on V6		Chip#3 on V6	
Randomness Test	*P*-value	*Prop.*	*P*-value	*Prop.*	*P*-value	*Prop.*
近似熵检验	0.511 011	0.99	0.925 760	0.98	0.489 682	1.00
线性复杂度检验	0.458 373	0.98	0.246 048	0.99	0.645 204	1.00
累加和检验 (1)	0.948 689	0.98	0.987 745	0.99	0.828 697	0.99
累加和检验 (2)	0.911 729	0.98	0.972 916	0.98	0.451 115	0.98
通用统计检验	0.291 896	0.99	0.592 236	1.00	0.541 548	0.99
重叠模块匹配检验	0.110 544	0.98	0.956 764	0.97	0.131 159	0.98
非重叠模块匹配检验	0.439 131	0.99	0.518 914	0.97	0.557 634	0.98
随机游动状态频数检验	0.618 146	0.97	0.332 965	1.00	0.714 818	1.00
随机游动检验	0.553 863	0.97	0.468 866	1.00	0.345 135	0.99
序列检验 (1)	0.205 002	0.99	0.927 355	1.00	0.163 869	0.98
序列检验 (2)	0.221 067	1.00	0.722 709	0.99	0.189 389	0.99
频率检验	0.952 089	1.00	0.959 647	0.99	0.669 447	0.97
块内最长游程检验	0.934 535	1.00	0.566 880	0.99	0.500 842	0.97
块内频数检验	0.164 998	0.99	0.430 228	0.99	0.113 861	0.99
游程检验	0.369 136	0.98	0.597 432	0.99	0.802 504	0.97
离散傅里叶变换检验	0.727 669	0.98	0.222 920	1.00	0.771 671	0.98
二元矩阵秩检验	0.267 678	0.98	0.807 360	1.00	0.499 265	0.98

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;对于非重叠模快匹配检验,随机游动状态检验和随机游动检验,*P*-value 是对应测试项所有子测试 *P*-value 的平均值

本文提出的 TRNG 具有较好移植性,易在其他 FPGA 开发板上实现。为更好的验证所提出的 TRNG 结构的灵活性和适用性,本文在 Xilinx Spartan-6 FPGA 开发板上进行了实验。Xilinx Spartan-6 FPGA 上实验的 NIST 测试结果如图 8 所示,本文提出的 TRNG 生成的随机序列通过所有 NIST 测试项。

2) NIST SP800-90B 测试

NIST 在 2016 年 1 月 27 日发布了 NIST SP800-90B[25]。NIST SP800-90B 比现有的熵估计方法更复杂,更严格。NIST SP800-90B 是对噪声源的统计评估,用于评估随机数发生器。对于该测试中的独立且相同(IID)测试,非 IID 测试并重启测试[25]要求,必须收集 1 M 数据进行测试。Xilinx Spartan-6 开发板上 TRNG 生成的随机比特流的 IID 测试、卡方测试、最长重复子串长度测试(LRS 测试)和重启测试的结果如表 2 所示。可以看出,设计的 TRNG 序列的最小熵为 0.995 860 且通过了 NIST SP800-90B 测试的 IID 测试,即所提出的 TRNG 生成的随机数为随机序列。

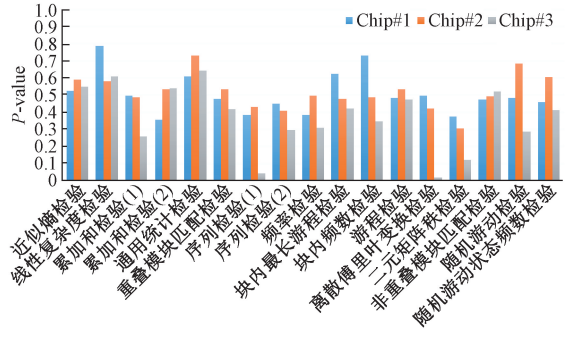


图 8　NIST SP800-22 在 Spartan-6 上的测试结果

Fig. 8　NIST SP800-22 test results on Spartan-6

4.2　PVT 测试

优良的 TRNG 必须能够在恶劣的环境中稳定且有效地产生高质量的随机数序列。为了验证本文提出的 TRNG 可以在不同的环境条件下工作,本文在不同的环境温度(0 ℃ ~ 80 ℃,以 20 ℃ 为步长)和电压(0.9 ~ 1.1 V,以 0.1 V 为步长)下对结构进行了测试。如表 3 所示,比例值是指所有随机测试通过率的平均值。尽管电压和温度的变化会影响所生成的随机比特流的质量,但根据实验结果可以看出所提出的 TRNG 产生的随机比特流均通过了 NIST SP800-22 测试。结果表明,由于通过选择最佳的 LUT 和路由来优化环形振荡器的延迟策略,所提出的 TRNG 可以在环境温度和电压变化的影响下有效稳定地生成高质量的随机数。

4.3　相关 TRNG 比较

本文提出的 TRNG 以 RO 为熵源,通过选择最佳的 LUT 和路由来优化环形振荡器的延迟策略,以高精度采样结构实现高效的随机数生成。当开发板的晶振时钟为 100 MHz 时,提出的 TRNG 达到了 100 MB/s 的吞吐量(单位时间产生的比特数)。另外,本文采用 5 组环形振荡器作为熵源,FPGA 中熵源结构的实现仅需要 5 个 Slices。

表2 针对NIST SP800-90B测试的1 MB TRNG样品的IID测试结果

Table 2 The IID test results of 1 MB TRNG samples against NIST SP800-90B test

测试			结果		
			$C[i][0]$	$C[i][1]$	IID
排列测试		偏移检验	9 598	0	Pass
		定向运行数量检验	9 186	9	Pass
		定向运行长度检验	2 607	3 865	Pass
		增加减少数量检验	2 928	32	Pass
		中位数数量检验	5 871	9	Pass
		中位数长度检验	1 173	989	Pass
		平均碰撞检验	1 372	2	Pass
		最大碰撞检验	1 649	522	Pass
	周期性检验	周期(1)	1 572	16	Pass
		周期(2)	9 321	10	Pass
		周期(8)	9 892	2	Pass
		周期(16)	3 646	35	Pass
		周期(32)	9 033	13	Pass
	协方差检验	协方差(1)	1 766	3	Pass
		协方差(2)	6 984	4	Pass
		协方差(8)	5 558	8	Pass
		协方差(16)	7 731	1	Pass
		协方差(32)	9 711	1	Pass
		压缩检验	1 138	38	Pass
χ测试		χ独立性检验	Pass		
		χ拟合优度检验	Pass		
LRS测试			Pass		
重启测试			Pass		
最小熵			0.995 860		

表3 PVT测试

Table 3 PVT test

	电压/V	温度/℃	比例
NIST Pub 800-22, Randomness Test	0.9	0	0.98
		20	0.98
		40	0.98
		60	0.97
		80	0.97
	1.0	0	0.99
		20	0.98
		40	0.99
		60	0.98
		80	0.99
	1.1	0	0.97
		20	0.98
		40	0.98
		60	0.98
		80	0.97

在Xilinx Virtex-6 FPGA开发板上实现TRNG的硬件开销仅为25个Slices(由于工艺原因,Xilinx Spartan-6 FPGA需要35个Slices)。综上所述,本文提出的TRNG具有资源开销少,吞吐量高和鲁棒性强的特点。从表4看出,与其他现有TRNG结构[6-8,11-12,26-27](其中FF代表D触发器)。文献[6]消耗511个LUT的结构虽然具有与本文相似的吞吐量,但是却牺牲了高昂的硬件开销。与其他相关结构相比,本文提出的TRNG具有更少的资源开销和更高的吞吐量。

表4 相关TRNG性能比较

Table 4 Performance comparison with Related TRNGs

TRNG结构	实验平台	熵源结构	资源消耗	吞吐量/(MB·s^{-1})	PVT测试	是否需要后处理
文献[6]	Cyclone III	STR	>511 LUTs	133	No	No
	Virtex-5	STR	>511 LUTs	100		
文献[7]	Virtex-5/6	STR	32 LUTs	4	No	No
	Spartan-3E	STR				
文献[8]	Virtex-5	STR	47 Slices	150	No	No
文献[11]	Spartan-6	RO	10 LUTs+5FFs	1.15	No	No
	Cyclone V	RO	10 LUTs+6FFs	1.067	No	No
文献[12]	Spartan-3 A	RO	270 slices	6	No	No
文献[26]	Virtex-4	RS Latch	256 gates	6.25	No	No
文献[27]	Kintex-7	PLL	128 gates + 48FFs	4	No	No
本文	Virtex-6	RO	25 slices	100	Yes	No
	Spartan-6	RO	35 slices			

5 结 论

本文针对真随机数发生器的研究和应用需求,提出了一种利用环形振荡器中抖动作为熵源的Xilinx FPGA上实现的新型TRNG。本文通过FPGA中的快速进位链对抖动高精度采样,有效地生成高质量的随机数序列。

由于采用了高精度采样技术,因此本文提出的TRNG能够以较低的硬件开销实现相当高的吞吐率。对于资源开销,在Xilinx Virtex-6 FPGA上仅占用了25个

Slices,在 Spartan-6 FPGA 上占用了 35 个 Slices。在吞吐量方面,提出的 TRNG 具有 100 MB/s 的随机数生成速率。另外,PVT 测试结果表明温度和电压的变化对真正的随机数发生器影响很小,本文所提出的 TRNG 具有良好的鲁棒性。

参考文献

[1] 张旭. 云计算安全综述[J]. 数字化用户数字化用户, 2014,(24):139-139.
ZHANG X. Overview of cloud computing security[J]. Digital User Digital User, 2014,(24):139-139.

[2] WU X, LI S. A new digital true random number generator based on delay chain feedback loop[C]. 2017 IEEE International Symposium on Circuits and Systems (ISCAS),2017, 2130-2133.

[3] 张启星,付敬奇. 基于信道特征提取的物理层安全密钥生成方法[J]. 电子测量与仪器学报,2019,33(1):16-22.
ZHANG Q X, FU J Q. Physical layer security key generation method based on channel feature extraction[J]. Journal of Electronic Measurement and Instrument,2019,33(1):16-22.

[4] 杨睛,刘琪,颜彪,等. 多用户 MIMO 下行链路物理层安全研究[J]. 电子测量与仪器学报,2016,30(09):1306-1312.
YANG J, LIU Q, YAN B, et al. Research on physical layer security of multi-user MIMO downlink[J]. Journal of Electronic Measurement and Instrument, 2016, 30(09):1306-1312.

[5] 李顺,张新豪. 存在主动干扰窃听方时的物理层安全性能分析[J]. 电子测量与仪器学报,2018,32(09):102-107.
LI S, ZHANG X H. Analysis of physical layer security performance when there is active interference with eavesdropping party [J]. Journal of Electronic Measurement and Instrument,2018,32(09):102-107.

[6] CHERKAOUI A, FISCHER V, FESQUET L, et al. A very high speed true random number generator with entropy assessment. cryptographic hardware and embedded systems[J],2013,8086, 179-196.

[7] MARTIN H, PERISLOPEZ 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, 91-100.

[8] ZHANG Y, JIANG J, WANG Q, et al. A self-Timed ring based true random number generator on FPGA. 2018 14th IEEE International Conference on Solid-State and Integrated Circuit Technology (ICSICT), Qingdao, 2018, pp. 1-3.

[9] Xilinx Corporation: Virtex-6 FPGA Configurable Logic Block (UG364), v14.7 (2012). Available: https://www.xilinx.com/support/documentation/user_guides/ug364pdf.

[10] ROZIC V, YANG B, DEHAENE W, VERBAUWHEDE I. Highly efficient entropy extraction for true random number generators on FPGAs[J]. In Proceedings of the 2015 Design Automation Conference (DAC). IEEE, 2015.

[11] YANG B, ROZIC V, GRUJIC M, et al. ES-TRNG: A high-throughput, low-area true random number generator based on edge sampling[J]. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2018, 3, 267-292.

[12] ANANDAKUMAR N, NALLA S, KUMAR S, et al. FPGA-Based true random number generation using programmable delays in Oscillator-Rings[J]. IEEE Transactions on Circuits and Systems II: Express Briefs,2019.

[13] 陈天宇,马原,荆继武,等. 振荡采样型真随机数发生器的健壮性研究[J]. 信息安全学报,2017,2(3):13-22.
CHEN T, MA Y, JING J W, et al. Research on robustness of oscillating sampling true random number generator[J]. Journal of Information Security, 2017, 2(3):13-22.

[14] MARTIN H, MARTINHOLGADO P, MORILLA Y, et al. Total ionizing dose effects on a Delay-Based physical unclonable function implemented in FPGAs [J]. Electronics,2018, 7.

[15] NATHALIE B, FLORENT B, VIKTOR F, et al. True-randomness and pseudo-randomness in ring oscillator-based true random number generators[J]. International Journal of Reconfigurable Computing, 2010, 1-13.

[16] XU X M, LIANG H G, HUANG Z F, et al. A single event transient detector in SRAM-based FPGAs[J]. IEICE Electronics Express, 2017, 14, 20170210-20170210.

[17] MA G L, LIANG H G, YAO L, et al. Efficiency true random number generator on FPGAs[J]. Asian Test Symposium,2018.

[18] 张鸿飞,王坚,罗春丽,等. 基于抖动的高速真随机数发生器的设计和实现[J]. 核技术,2011,34(7):556-560.
ZHANG H F, WANG J, LUO C L, et al. Design and implementation of a high-speed true random number generator based on jitter[J]. Nuclear Technology,2011, 34(7):556-560.

[19] HORSTMANN J U, EICHEL H W, COATES R L. Metastability behavior of CMOS ASIC flip-flops in theory

and test[J]. IEEE Journal of Solid-State Circuits, 2002, 24, 146-157.

[20] AMS: Time-to Digital-Converter preliminary Datasheet. Available: https://ams.com/documents/20143/36005/TDCGP21_UG000431_100.pdf /0338dac1-b1e3-fffb-3c85-6c25bc168464

[21] LIANG H G, XU X M, HUANG Z F, et al. A methodology for characterization of SET propagation in SRAM-Based FPGAs[J]. 2016, IEEE Transactions on Nuclear Science, 63(6), 2985-2992.

[22] VAN B, PRINZIE J, LEROUX P. Radiation assessment of a 15.6ps Single-Shot Time-to-Digital Converter in terms of TID[J]. Electronics 2019, 8, 558.

[23] Xilinx Corporation: Spartan-6 FPGA Configurable Logic Block (UG364), v14.7 (2012). Available: https://www.xilinx.com/support/documentation/user_guides/ug384.pdf.

[24] RUKHIN A, SOTO J, NECHVATAL J. A statistical test suite for random and pseudorandom number generators for cryptographic applications[J]. NIST Special Publication 800-22. Andrew Rukhin Juan Soto James Nechvatal Miles Smid Elaine.

[25] TURAN M S,BARKER E, KELSEY J, et al. NIST Special Publication 800-90B: Recommendation for the Entropy Sources Used for Random Bit Generation. U.S. Department of Commerce, National Institute of Standards and Technology: Gaithersburg, MD, USA, 2018.

[26] HATA H, ICHIKAWA S. FPGA implementation of metastability-based true random number Sgenerator[J]. IEICE Trans. Information & Systems, 2012, 95.426-436.

[27] DEAK N, GYORFI T, MARTON K, et al. Highly efficient true random number generator in FPGA devices using phase-locked loops [C]. International Conference on Control Systems & Computer Science. IEEE,2015.

作者简介

鲁迎春,2002年毕业于合肥工业大学微电子学专业获得学士学位,2005年毕业于合肥工业大学微电子学和固体电子学专业获得硕士学位,现为合肥工业大学集成电路与系统专业在读博士研究生。合肥工业大学电子科学与应用物理学院讲师。他的研究兴趣包括硬件安全、IC和FPGA应用设计。

E-mail: luyingchun@hfut.edu.cn

Lu Yingchun received the B.S. degree in microelectronics from Hefei University of Technology, Hefei, China, in 2002, and the M.S. degree in Microelectronics and solid-state electronics from Hefei University of Technology in 2005. He is currently pursuing Ph.D. degree of integrated circuits and systems in Hefei University of Technology. He is currently a lecturer of Electronic Science and technology at Hefei University of Technology. China. His research interests include Hardware Security, IC and FPGA application design.

黄正峰(通讯作者),1978年出生,现为合肥工业大学电子科学与应用物理学院教授、硕士生导师。他的研究兴趣主要包括嵌入式系统的综合与测试、数字系统设计自动化等。

E-mail: huangzhengfeng@139.com

Huang Zhengfeng was born in 1978. He is a full professor and master supervisor at School of Electronic Science & Applied Physics, Hefei University of Technology. His research interests include synthesis and testing of embedded systems, design automation of digital systems and so on.