DOI: 10.13382/j.jemi.B2407788

多熵源动态切换双模式真随机数发生器*

鲁迎春[1] 纪籽言[1] 许恩溥[1] 马利祥[2]
(1. 合肥工业大学微电子学院 合肥 230601;2. 安徽信息工程学院 芜湖 241000)

摘 要:真随机数生成器(TRNG)在信息安全领域中扮演着关键角色。伽罗瓦环形振荡器(GARO)结合 TRNG 是一种经典的应用设计结构,但通常存在固定点或者周期性振荡的问题,为了解决上述问题,提出了一种基于现场可编程门阵列(FPGA)的多熵源双模式振荡环 DMRO-TRNG 结构,其熵源包括时钟抖动,亚稳态,混沌。与传统的 GARO 不同,它是一种动态的 TRNG 架构,通过使用 MUX 在该电路中实现动态转换,使得该电路实现在不同的工作模式之间进行切换,从而产生随机输出序列,并通过 Xilinx 编译器自动布局布线。该结构有效提高了随机数生成的综合性能。在 Xilinx Kintex-7 和 Artix-7 FPGA 上进行的实验表明,所提出的结构生成的随机序列通过了 NIST SP800-22、NIST SP800-90B、TESTU01 等多项标准测试。该结构已经在电压和温度变化下进行了广泛的测试,并显示出优异的鲁棒性。该 TRNG 只需要消耗 36 个逻辑单元(LUT),4 个 D 触发器(DFF)和 16 个 MUXs 就可以达到 750 Mbps 的吞吐率,且仅使用简单的异或后处理电路,硬件开销低。

关键词: FPGA;伽罗瓦环形振荡器;抖动;亚稳态;混沌;双模式
中图分类号: TN47 **文献标识码**: A **国家标准学科分类代码**: 510.3040

Dual-mode true random number generator with dynamic switching of multiple entropy sources

Lu Yingchun[1] Ji Ziyan[1] Xu Enpu[1] Ma Lixiang[2]
(1. School of Microelectronics, Hefei University of Technology, Hefei 230601, China;
2. Anhui University of Information Engineering, Wuhu 241000, China)

Abstract: True random number generators (TRNGs) play a critical role in information security. While the Galois ring oscillator-based TRNG (GARO-TRNG) represents a classical design architecture, it typically suffers from issues of fixed points or periodic oscillations. To address these limitations, this paper proposes a novel FPGA-based DMRO-TRNG structure with multiple entropy sources incorporating clock jitter, metastability, and chaos. Distinct from conventional GARO architectures, this dynamic TRNG design implements mode switching through MUX, enabling transitions between different operational modes to generate random output sequences. The implementation utilizes Xilinx compiler for automatic place-and-route, effectively enhancing comprehensive performance in random number generation. Experimental evaluations on Xilinx Kintex-7 and Artix-7 FPGAs demonstrate that the generated random sequences successfully pass rigorous standard tests including NIST SP800-22, NIST SP800-90B, and TESTU01. The architecture exhibits exceptional robustness under varying voltage and temperature conditions through extensive testing. With low hardware overhead, this TRNG achieves a throughput of 750 Mbps while consuming only 36 LUTs, 4 DFFs, and 16 MUXs, requiring merely a simple XOR-based post-processing circuit.

Keywords: FPGA; Galois ring oscillator; jitter; metastabilit; chaos; dual mode

收稿日期:2025-08-27 Received Date: 2025-08-27
*基金项目:国家自然科学基金项目(62027815,62174048,62274052)、安徽省研究生教育教学改革研究重点项目(2022jyjxggyj053)资助

0 引 言

随着物联网、计算机网络和自动驾驶技术的迅速发展,人工智能和智能电子产品市场日益扩大,信息安全问题日益受到关注。因此,需要先进的加密算法或硬件安全加密技术来解决安全问题。随机数发生器(random number generator,RNG)作为安全加密技术的关键组件,其重要性不容忽视。RNG 主要分为伪随机数发生器(pseudo random number generator,PRNG)和随机数发生器(true random number generator,TRNG)。PRNG 基于数学算法构建,它通过初始的种子值(又称起始种子)迭代生成看似随机的数列。尽管它们能够产生大量随机数,但其输出是可以预测的,这限制了它在需要高度随机性和不可预测性的应用中的适用性。TRNG 则追求更高的随机性和不可预测性,其在电子测量领域对测量系统的可靠性与数据完整性也具有关键支撑作用。高精度电子测量设备需在复杂电磁环境中保障信号采集与传输的安全性,TRNG 通过物理熵源产生的不可预测随机序列如热噪声、散粒噪声、时钟抖动[1]、亚稳态[2]、混沌[3]等,可为测量数据加密、随机采样控制及抗干扰协议提供核心熵源。例如,在分布式传感器网络中,TRNG 生成的加密密钥能有效防御重放攻击与数据篡改;在量子计量系统中,真随机时序控制可提升系统抗相干噪声能力。通常使用 D 触发器(DFF)进行采样,并且采样的原始随机数通常需要额外的后处理电路来改善其统计特性,以便通过随机性测试[4]。并且 TRNG 的实现复杂度较低,特别是数字 TRNG,它们无需全自定义电路设计,其能够在可编程门阵列(field programmable gate array,FPGA)中高效实现,从而在保证随机性和安全性的同时,降低成本和复杂性[5]。文献[6]使用交叉耦合 NAND 门和手动布线来产生亚稳态,吞吐率可以达到 30 Mbps,但是,需要额外的校准反馈电路和冯·诺伊曼后处理电路来改善生成数字的随机性。在 TRNG 中,使用锁相环(PLL)或 DCM 作为熵源虽然结构简单,但其随机性和可移植性较差,需要通过复杂的计算来优化参数以提高随机数质量[7]。利用环形振荡器(ring oscillator,RO)中的抖动和 D 锁存器的亚稳态作为熵源的 TRNG 虽然资源消耗很小但吞吐率只有 0.76 Mbps[8]。Sunar 等[9]提出了一种经典架构,通过并行化多个环形振荡器来扩展抖动范围。尽管如此,该方法还是存在显著的硬件资源消耗问题,并且表现出较低的吞吐率性能。文献[10]改进了基于 RO 的 TRNG,在异或之前的每个反相器环之后添加额外的触发器,其性能比文献[9]要好,达到了 100 Mbps 的吞吐率,但还是消耗了大量逻辑资源。参考文献[11]可知,基于 FIGARO 的真随机数发生器在最大吞吐率方面表现得非常出色,达到了 400 Mbps,可无缝集成于实时测量系统,满足高速数据加密需求。然而它所需的硬件资源非常庞大,包括 288 个可配置逻辑单元(LUT)和 190 个 DFF。文献[12]提出的一种 TRNG 其随机性是由振荡的自定时环(STR)产生的,消耗了 56 个 LUTs 和 19 个 DFFs,但它的吞吐率只有 100 Mbps。文献[13]主要讨论了斐波那契环形振荡器(Fibonacci ring oscillator,FIRO)作为真随机数生成器的安全性风险。研究表明,FIRO 可能会周期性振荡,而非混沌振荡,这会导致生成的随机数熵值极低,存在显著的安全隐患。为了解决该问题,文献[14]对伽罗瓦环形振荡器(Galois ring oscillator,GARO)和 FIRO 进行改进提出了一种新型的混沌环形振荡器,该结构获得了 125 Mbps 的吞吐率。文献[15]提出一种 FIRO 和 GARO 组合配置实现的结构,吞吐率为 31.25 Mbps。文献[16]对于 GARO 进行改进,利用一阶振荡环推动三输入异或门的输出连续跳跃。传统的 RO 利用多个 RO 并行来获得随机比特流消耗了大量的硬件资源。传统的 FIRO 和 GARO 都利用高阶环作为熵源和特定多项式来获得高质量的随机数,这也消耗了大量的硬件资源。

为了解决了传统的 GARO 可能存在固定点和周期性振荡的问题,本文提出了一种基于 FPGA 的多熵源双模式振荡环真随机数发生器(dual-mode ring oscillator-TRNG,DMRO-TRNG),该 TRNG 资源开销较小且吞吐率高。

1)利用 MUX 来实现该 TRNG 动态转换的功能,使得该电路在不同的工作模式之间进行切换,用奇数阶 RO 给 GARO 提供随机的初始值,极大程度上延迟了传统的 GARO 进入周期性振荡的时间,同时奇数阶 RO 也可以作为熵源,提高了熵源的随机性。

2)单一熵源的 TRNG 会导致产生具有低随机性的原始序列,本文通过增加 MUX 单元,实现了以时钟抖动和亚稳态以及混沌为熵源的多熵源真随机数产生器,并且进行了仿真分析。

3)通过使用异或后处理消除输出序列 0 和 1 的偏置,然后通过高频采样放大随机性,利用 36 个 LUTs,16 个 MUXs,4 个 DFFs 实现了 750 Mbps 的最高吞吐率。

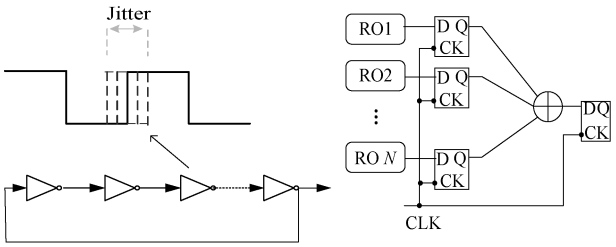
本文在提出建议的熵源组成和工作原理后,对其性能进行了仿真分析。接着,引入采样与后处理电路,构建了一个真随机数发生器。通过了实验和测试,验证了该真随机数发生器的性能。

1 背景和相关工作

1.1 环形振荡器和抖动

传统 RO 结构是由奇数个反相器首尾串联构成,如图 1(a)所示[16]。理想地,RO 的输出信号是周期性方

波,其周期由反相器的数量和反相器的延迟确定,即 $T = 2 \cdot n \cdot \tau$ 并且 $\psi(t) = \psi(t + T)$,其中 T 表示周期,τ 表示单个反相器的延迟。但通常输出的信号是不完美的方波,假设周期以随机方式震动 $T = T + \hat{T}$,其中 $\hat{T}$ 表示随机变量,其取值范围是 $(-T/2, T/2)$ 。在高质量的数字电路中,$\hat{T}$ 的范围与周期相比相当小。时钟信号中的振动,由随机变量 $\hat{T}$ 表示,通常称为抖动。抖动是希望收获的熵的来源[9]。但与逻辑门的固有延迟相比,抖动引起的随机延迟波动是一个微小的参数,因此在单次 RO 采样随机性不足的情况下,需要多个并行的 RO 用于改善生成比特序列的随机性,但这会增加电路的硬件资源,如图 1(b)所示。



(a) 时钟抖动和传统的RO结构　(b)多组并行的RO
(a) Clock jitter and traditional RO structures　(b) Multiple parallel ROs

图 1　时钟抖动和传统的 RO 结构以及多组并行的 RO
Fig. 1　Clock jitter and traditional RO structures and multiple parallel ROs

1.2　亚稳态

D 触发器在时钟上升沿采样其输入信号。如果在采样过程中,器件的建立时间 T_{SU} 或保持时间 T_h 不符合规定,就会使触发器进入亚稳态振荡状态。振荡最终会稳定到‘1’或‘0’的稳定状态。稳定到‘1’的概率是采样时刻与输入信号转换时刻之间的时间差 Δ 的单调函数。该概率可以准确地用高斯累积分布函数(CDF)建模。如果到达信号的延迟差用 Δ 表示,并且 σ 与建立/保持时间窗口的宽度成正比,则输出等于‘1’的概率可以表示为:

$$Prob\{Out = 1\} = Q\left(\frac{\Delta}{\sigma}\right) \tag{1}$$

$$Q(x) = \frac{1}{\sqrt{2\pi}}\int_x^{\infty} \exp\left(\frac{-u^2}{2}\right) \mathrm{d}u \tag{2}$$

在亚稳态情况下,当 Δ→为 0 时,$Q(X) = 0.5$,$P(Q = 1) = P(Q = 0) = 0.5$ 时。也就是说,数据和采样变化边缘之间的差异越小,输出 0 和 1 的概率就越接近 0.5。

1.3　数字混沌(digital chaos)

数字混沌是一个涉及复杂性、随机性和确定性系统的概念,通常与混沌理论相关联。混沌理论主要研究非线性动态系统的行为,这些系统对初始条件非常敏感,即使是微小的变化也可能导致系统行为的巨大差异[17]。系统虽然是确定性的,但其表现却是不可预测的。经典的数字混沌模型有 Lorenz 方程、Rossle 系统、Logistic 映射等。它可以作为生成伪随机数的方法,这些随机数可以用于加密和安全通信。

2　DMRO-TRNG 的设计

2.1　DMRO 单元

本文将选择器引入传统的 GARO 单元如图 2 所示。选择器用作开关,其控制信号(control signal)决定 DMRO 处于何种模式。根据控制信号的不同,有两种情况:当控制信号为逻辑低电平时,异或门从反馈回路中断开,每个反相器的输出连接到下一个反相器的输入形成传统的 RO;当控制信号为逻辑高电平时,异或门连接到反馈回路中,将上述结构转换为传统的 GARO。使用特定资源 PLL 分频出的 CLK(250 MHz)用作选择器的选择信号,使得系统在两种模式之间动态切换。系统的初始状态可以决定其是否进入一个固定点或开始周期性振荡,当 DMRO 处于 RO 模式时,线路中的抖动累积为下一时刻的 GARO 提供了随机的初始值,同时也可以作为输出,使得 GARO 处于固定点或者周期性振荡的概率大大降低。伽罗瓦环形振荡器作为一种基于反馈环结构的真随机数生成器,其随机性源于反相器链路的非线性相位竞争效应。根据理论模型,奇数阶环形结构可通过自激振荡产生非确定性信号,而偶数阶结构因逻辑电平的快速稳定化无法形成持续振荡。本文通过 FPGA 平台实现不同阶数(3 阶、5 阶、7 阶、9 阶)的以 GARO 为基础的 DMRO,生成随机序列样本,采用 NIST SP 800-22 随机性测试套件进行严格评估。实验表明,3 阶 DMRO 虽可产生振荡信号,但其相位竞争动力学受限于过短的环路延时。统计测试结果表明,其输出的序列在频率单调性(p-value = 0.001 2)和长周期重复模式(FFT 检验失败率 82%)上显著偏离随机性假设,无法通过 NIST 标准。当阶数提升至 5 阶时,环路延时增加至亚稳态敏感区间,热噪声扰动被有效放大。5 阶 DMRO 输出的随机序列在 NIST SP 800-22 测试中通过率超过 98%。进一步增加阶数(7 阶、9 阶)可提升抗外部干扰能力,但需权衡面积开销与功耗效率。所以本文选择以 5 阶 GARO 为基础的 DMRO。为验证 MUX 选择信号周期对随机性的影响,实验在 Artix-7 FPGA 平台上测试了 5 阶 DMRO 在 MUX 选择信号频率为 200、250、300 MHz 下的性能。其余条件不变,当频率为 250 MHz 时,NIST SP 800-22 测试通过率最高(15/15 项),且熵值达到 0.995 以上。进一步提高频率至 300 MHz 时熵值下降至 0.89;而降低频率至 200 MHz 时,时钟抖动占比降低,随机性质量亦有所退化(通过率 14/15 项)。

所以选择特定资源 PLL 分频出的 CLK(250 MHz)用作选择器的选择信号。图 3 所示为 HSPICE 软件模拟的传统 5 阶 GARO 输出的波形,可以明显的观察到 300 ns 之后,其波形呈现出周期性的振荡。其生成的随机序列也无法通过 NIST SP 800-22 随机性测试。

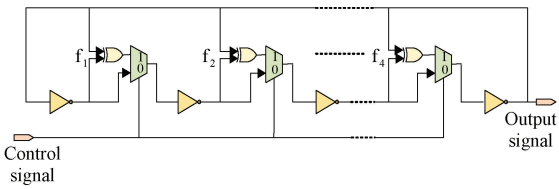


图 2 DMRO 单元

Fig. 2 DMRO cell

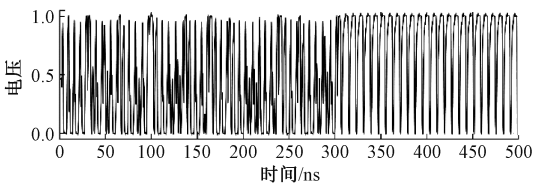


图 3 GARO 输出信号的模拟波形

Fig. 3 Analogue waveforms of GARO output signals

2.2 熵源的随机性分析

运行时序图如图 4 所示,当 MUX 控制信号为 0 时,DMRO-TRNG 为 RO 模式,此时的熵源为抖动,环路中包含 5 个反相器首尾连接,图 5(a)所示是一个 5 阶的 RO,理想情况下会产生周期为 T 的方波:

$$T = 2n\tau \tag{3}$$

式中:n 是反相器的数量;τ 是反相器、线路延迟、MUX 的总和,如式(4)所示。

$$\tau = \tau_{inv} + \tau_{wire} + \tau_{mux} \tag{4}$$

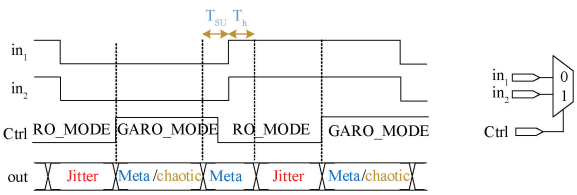


图 4 运行时序图

Fig. 4 Runtime sequence diagram

在实际电路中,由于热噪声、散射噪声、电源波动和环境变化等外部随机物理过程的影响,RO 的上升或下降沿会出现抖动,因此总延迟 τ' 由固定延迟 τ 和抖动干扰延迟 $\Delta\omega$ 共同确定,如式(5)所示。

$$\begin{cases}\tau' = \tau + \Delta\omega \\ \Delta\omega = \Delta\omega_t + \Delta\omega_G + \Delta\omega_D\end{cases} \tag{5}$$

抖动分为两部分,一部分是伪随机性的其中 $\Delta\omega_t$ 和

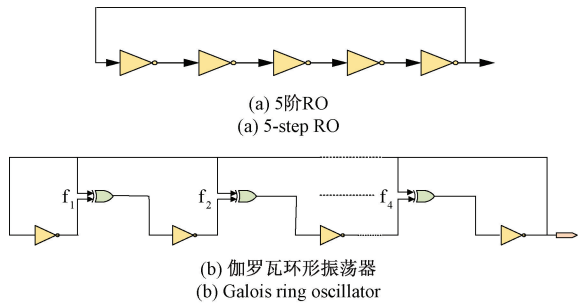


图 5 5 阶 RO 和伽罗瓦环形振荡器

Fig. 5 5-step RO and Galois ring oscillator

$\Delta\omega_D$ 分别表示抖动干扰引起的反相器延迟的积累和确定性的抖动干扰延迟;另一部分是不可预测的,$\Delta\omega_G$ 表示高斯抖动干扰延迟,服从具有无限峰值和无边界值的高斯分布 $N(\mu,\delta^2)$。固定延迟和抖动干扰引起的延迟共同累积,使得 DMRO 单元输出的方波具有可变周期。这种可变周期的信号为系统提供了随机性,从而生成随机熵源。

此时电路中的整体结构为 4 组 5 阶的 RO 异或,RO 的相位噪声可以用式(6)来建模和表示[18]。

$$L(\Delta f)_{min} = \frac{8}{3\eta}N\frac{KT}{P}\left(\frac{V_{DD}}{V}+\frac{V_{DD}}{IR}\right)\left(\frac{f}{\Delta f}\right)^2 \tag{6}$$

式中:K 是玻尔兹曼常数;T 是绝对温度;η、V_{DD}、V、I 和 R 是常数;f、Δf 和 p 分别为环形振荡器的中心频率、频率偏移和功耗;N 是振荡环中使用的反相器数量。上文提到的 τ 是反相器、线路延迟的总和。此时 RO 的频率 $f = \frac{1}{10\tau}$,代入式(5)得到此时的相位噪声,RO 振荡产生的相位噪声,会影响下一阶段的信号转变,使下一阶段的 GARO 的有限状态机的初始状态变得更加随机。

当控制信号在 T_{su} 或 T_h 的间隔内跳跃,不能满足 MUX 建立或保持时间的要求时,它将产生亚稳态现象并输出亚稳态型随机数。

当 MUX 控制信号为 1 时,异或门连接到反馈回路中,此时 DMRO 处于 GARO 模式,如图 5(b)所示。反馈连接由二进制系数 f_i 指定。如果 $f_i = 1$,则相应的开关闭合,如果 $f_i = 0$,则相应的开关断开,在这种情况下对应的 2 输入异或门不存在。反馈系数都可以方便地用称为反馈多项式的二进制多项式来表示 $f(x) = \sum_{i=0}^{r} f_i x^i$,$f_0 = f_r = 1$。虽然这种结构比传统的 RO 结构具有更高的熵,但通常满足不存在固定点的反馈多项式都是高阶的,这消耗了大量的资源。对于长度为 15 的 GARO,有 4 096 个反馈配置,大多数反馈多项式产生大量不同的样本,但一些反馈多项式导致周期振荡或部分混沌振荡变为周期。随着 GARO 长度的增加,可供选择的反馈多项式不断增加,

不同出现样本的数量与反馈多项式的 XOR 连接量之间存在关系。此外,最大化贡献 XOR 抽头的数量可能会维持混沌振荡,并将切换到周期行为的可能性降至最低[19]。考虑到资源消耗,本文选择的反馈多项式为 $f(x)=x^4+x^3+x^2+x+1$。表 1 为不同数目的反向器配置可行的反馈多项式。

表 1　可配置的反馈多项式

Table 1　Configurable feedback polynomials

$F(x)$	多项式
①	$F(x)=x^7+x^5+x+1$
②	$F(x)=x^{10}+x^6+x^5+x^4+x^3+x^2+x+1$
③	$F(x)=x^{11}+x^6+x^5+x^4+x^3+x^2+1$
④	$F(x)=x^{15}+x^{14}+x^7+x^6+x^5+x^4+x^2+1$
⑤	$F(x)=x^{31}+x^{27}+x^{23}+x^{21}+x^{20}+x^{17}+x^{16}+x^{15}+x^{13}+x^{10}+x^9+x^8+x^6+x^5+x^4+x^3+x^1+1$

文献[20]提出通过适当选择反馈多项式,上述 GARO 电路可以是一种混沌电路,混沌电路对初始条件和参数的微小变化非常敏感,这种灵敏性使得混沌电路具有高度的随机性和不可预测性。由表 1 可知,可配置的反馈多项式通常是高阶的,本文提出的 DMRO 无需高阶环作为熵源,通过 RO 对系统进行扰动,提供随机的初始值,使系统进入混沌状态。在 2.1 节中 DMRO 输出信号的模拟波形与经典的混沌模型 Logistic 映射输出的波形十分相似,所以这可以被认为是相对于该时间单位的一种数字混沌。

随机性的主要来源是电路中所有逻辑门的随机延迟和转换时间,由于振荡信号的混沌行为,随着开关频率更高,随机性进一步增加。此外,不规则振荡信号本身可能导致各个逻辑门的随机延迟的较大变化。另一方面,通过式(6)可以看出,相位噪声会随着反相器阶数 N 的增加而增加,但是输出频率 f 会随之减少,吞吐率也会随之降低,而 GARO 电路是一种异步反馈结构,由于反馈结构的频率积累,增加 N 的同时,振荡频率也不会降低,从而得到一个优秀的熵源。

同时其也具有内部亚稳态性,当反馈回路上的所有反相器的输出以及该回路上的第 1 反相器的输入同时达到中间电压值时,具有恒定值,使得反馈信号的变化不维持第 1 反相器的输入信号的变化,因此,与环路上的其他反相器一起保持在中间电压值,从而引起亚稳态性。

2.3　后处理技术

单个 DMRO 单元的输出序列不符合统计要求,所以要进行异或后处理,异或前采集的百万比特序列 0 和 1 的偏差如表 2 所示,为了提高序列的随机性本文进行异或后处理的机制如图 6 所示,其中 p_0 表示一个 DMRO 单元输出 1 的概率,N 表示子结构的数量,n 表示异或门的数量,文献[21]提出可以将体系结构输出 1 的概率表示为 p_{out}:

$$p_{out}(p_0,n)=p_0\sum_{i=0}^{n}(1-2p_0)^i \tag{7}$$

式中:n 表示异或门的数目由于 $p_0\in(0,1)$,可以推导出 $-1\leqslant 1-2p_0\leqslant 1$。因此 p_{out} 可以表示为:

$$p_{out}=p_0\frac{1-(1-2p_0)^{n+1}}{1-(1-2p_0)}=\frac{1-(1-2p_0)^{n+1}}{2} \tag{8}$$

由表 2 可知,$p_0\approx 0.435$,图 7 所示为输出序列中 1 的比率与单元数目的关系。可见当单元数目增加到 4 个时,“0”和“1”的分布足够均匀。

表 2　百万比特序列 0 和 1 的偏差

Table 2　Deviation of the million-bit sequence 0 and 1

组数	1	2	3	4
0 的数量	566 421	562 250	567 723	562 586
1 的数量	433 579	437 750	432 277	437 414
偏差	132 842	126 500	135 446	125 172
p_0	0.43	0.44	0.43	0.44
组数	5	6	7	8
0 的数量	566 182	568 562	562 858	560 390
1 的数量	433 818	431 438	436 142	439 610
偏差	132 364	137 124	127 716	120 780
p_0	0.43	0.43	0.44	0.44

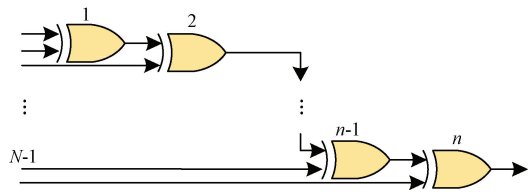


图 6　异或后处理机制

Fig. 6　Hterodyne post-processing mechanism

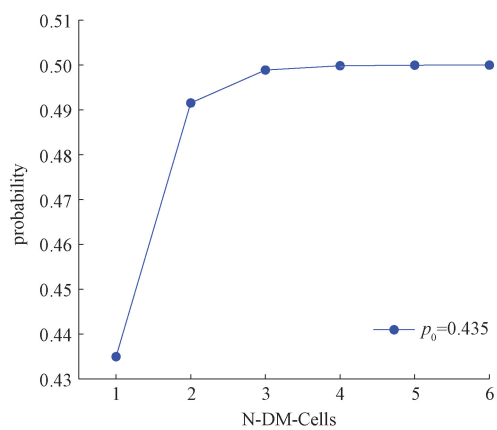


图 7　体系结构输出 1 的概率与子结构数量的关系

Fig. 7　The probability of an architecture outputting 1 as a function of the number of substructures

2.4　DMRO-TRNG 框架

图 8 所示是基于所提出的真随机数生成器的总体架

构。在该方案的实现中,总共使用了 4 个 DMRO 熵源。每个 DMRO 的输出通过 D 触发器捕获,在 Artix-7 和 Kintex-7 上采样频率可配置为高达 750 MHz,然后,通过异或门对在同一时钟边沿采样的所有 4 个熵源的输出数据比特进行异或运算。为了实现所提出的 TRNG,采用 Xilinx ISE 14.7 作为开发平台,实验采用 28 nm 工艺的 Xilinx Kintex-7 XC7K325T 和 Artix-7 XC7A100T FPGA 开发板作为硬件平台。Kintex-7 XC7K325T 提供 326 080 个 LUTs、407 600 个触发器(FFs)、840 个 DSP slices 以及 16.3 Mb 的块 RAM,适用于高性能计算任务;Artix-7 XC7A100T 则提供 101 440 个 LUTs、202 880 个 FFs、240 个 DSP slices 以及 4.86 Mb 的块 RAM,更适合低功耗应用。两类开发板均配备 DDR3 内存接口和 PCIe Gen2 接口。

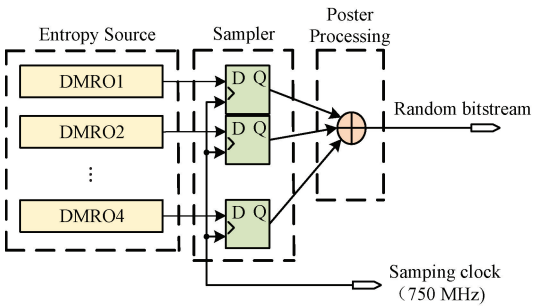


图 8 DMRO-TRNG 的总体架构

Fig. 8 General architecture of DMRO-TRNG

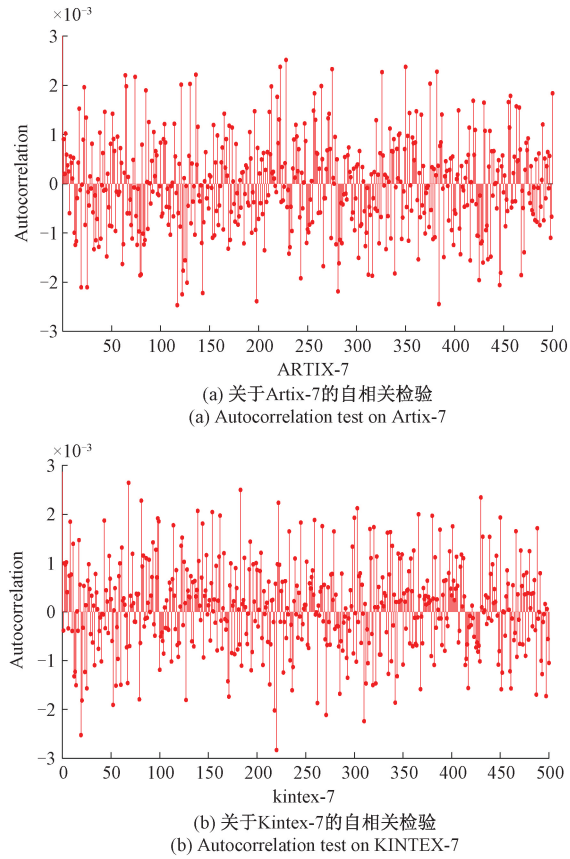


图 9 关于 Artix-7 和 Kintex-7 的自相关检验

Fig. 9 Autocorrelation test on Artix-7 and Kintex-7

3 实验结果与分析

3.1 自相关检验

真随机序列之间没有相关性[22]利用自相关函数(ACF)对 DMRO-TRNG 生成的序列在不同时间段的相关性进行了评估。根据统计标准,当式(9)的相关系数 $\rho<0.3$ 时,可视为不相关。

$$\rho=\frac{\sum_{i=1}^{n-h}(x_i-\bar{u})(x_{i+h}-\bar{u})}{\sum_{i=1}^{n}(x_i-\bar{u})^2} \tag{9}$$

式中:$\bar{u}$ 是完整序列的平均值;h 是滞后值。分别在 Xilinx Artix-7 和 Kintex-7 上生成了 10^6 个比特序列。经 MATLAB 处理后,将滞后值设定为 1~500,并对自相关系数变量进行分析。结果如图 9 所示,表明与自相关值对应的所有自相关系数都<0.03。因此,DMRO-TRNG 生成的随机序列可以被证明不是自相关的。

3.2 偏差检验

偏差检验是真 TRNG 设计中的重大挑战,一个高质量的 TRNG 的偏差应控制在接近零的极小范围内。为进行偏差测试,从两个 TRNG 开发板各收集了 100 组序列,每组含 100 万个二进制位,并计数每组中 0 和 1 的数量。实验结果如图 10(a)、(b)所示,可以看出,在任何生成的随机序列中,0 和 1 的出现概率都非常接近 50%。因此,所提出的真随机数产生器通过了偏差测试。

3.3 电压和温度测试

为了进一步测试应用环境条件波动对 DMRO-TRNG 可靠性的影响,本文利用电压和温度测试对 DMRO-TRNG 进行验证。实验设置了 3 种不同的电源电压和环境温度。利用 Kintex-7 FPGA 分别在不同的电压和温度组合下产生随机序列,并在 NIST SP 800-22 上进行测试,获得统计通过率。如图 11 所示,实验结果表明,在不同的电压和温度下,DMRO-TRNG 产生的随机序列均通过了 NIST SP 800-22 测试。因此,可以得出结论,DMRO-TRNG 具有较高的抗电压和温度波动能力。

3.4 NIST SP800-22 随机性测试

NIST SP 800-22 是用于评估任何随机数序列随机性的最广泛使用的 RNG 测试套件之一[23]。专门用于评估随机数发生器生成的数据序列是否具有足够的随机性和数据分布是否符合随机数测试标准,包含用于评估 TRNG 性能的 15 个测试,每个测试项目完成后将报告相

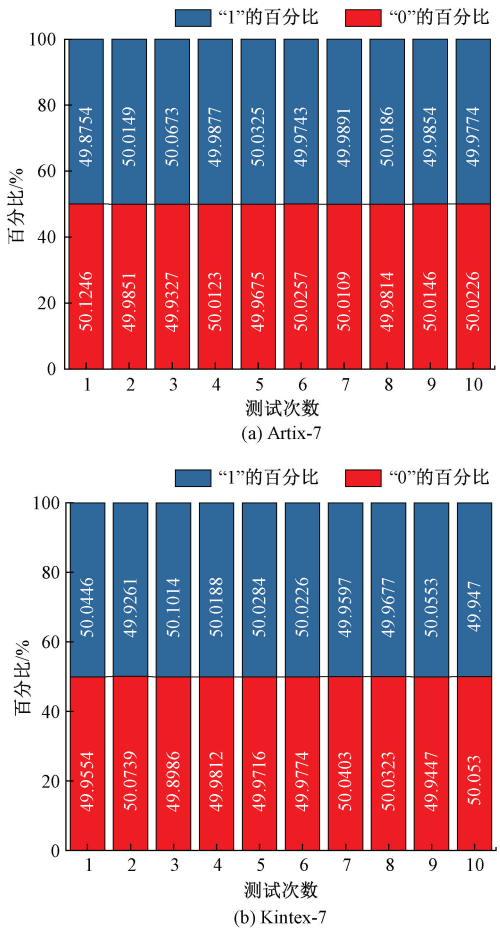


图 10　关于 Artix-7 和 Kintex-7 的偏差测试

Fig. 10　On Artix-7 and Kintex-7 bias testing

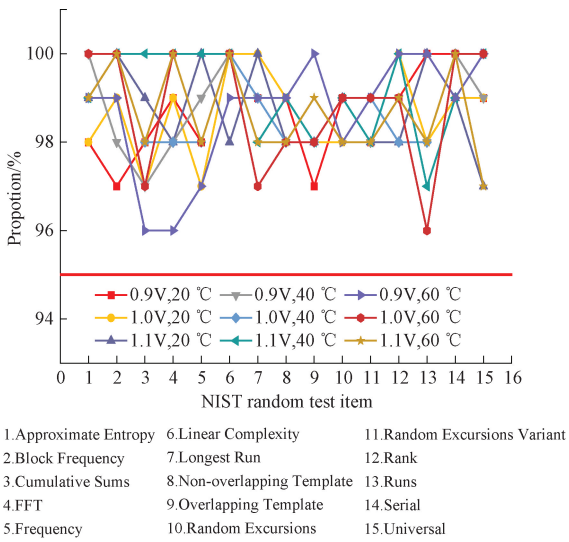


图 11　温度电压测试结果

Fig. 11　Temperature and voltage test results

应的最小 P 值和通过率(prop)。当 P 值大于 0.01 时,认为随机序列通过了该项测试。在不同的两块开发板上生成两组 100 万位随机数序列的测试结果如表 3 所示,几乎所有的随机序列都通过了随机性测试。

表 3　DMRO-TRNG NIST-SP800-22 测试结果

Table 3　DMRO-TRNG NIST-SP800-22 test results

NIST SP 800-22	Kintex-7		Artix-7	
	P-value	Prop	*P*-value	Prop
近似熵检验	0.699 313	99/100	0.816 537	100/100
块内频数检验	0.719 747	99/100	0.514 124	98/100
累加和检验	0.640 795	99/100	0.349 762	99/100
离散傅里叶变换检验	0.867 692	100/100	0.334 538	100/100
频率检验	0.678 686	99/100	0.574 903	99/100
线性复杂度检验	0.935 716	99/100	0.816 537	100/100
块内最长游程检测	0.867 692	100/100	0.924 076	100/100
非重叠模块匹配检测	0.482 919	99/100	0.466 505	99/100
重叠模块匹配检验	0.994 250	99/100	0.514 124	100/100
随机游动检验	0.594 135	99/100	0.501 433	99/100
随机游走频数检验	0.485 761	99/100	0.261 089	99/100
二元矩阵秩检验	0.474 986	98/100	0.383 827	100/100
游程检验	0.366 918	100/100	0.366 918	100/100
序列检验	0.431 122	99/100	0.564 375	99/100
通用统计检验	0.719 747	99/100	0.883 171	99/100

注:*包含多个子测试的测试、P 值和通过率是多个测试的平均值

3.5　NIST SP800-90B 随机性测试

NIST SP800-90B 是用于评估真随机数质量的另一个最重要的测试套件。最终的 SP800-90B 随机性测试结果如表 4 所示。可以发现,两块开发板的输出随机序列都通过了测试,最小熵分别为 0.995 843、0.995 349。根据参考文献[24]定义,通过判断 $C_{i,0}$ 和 $C_{i,1}$ 之和是否小于 9 995,来判定每项测试是否通过。结果显示所有测试项的 $C_{i,0}$ 和 $C_{i,1}$ 之和都远小于 9 995,表明被测随机数据集通过所有 IID 测试项目。

3.6　TESTU01 测试

TESTU01 测试被认为是对随机数序列最严格的测试[25],许多已知的随机数方案不能通过 TESTU01。本文所提出的 DMRO-TRNG 输出通过了所有测试,结果如表 5 所示。

3.7　与现有基于现场可编程门阵列的 TRNG 的比较

将该方案与最新 TRNG 方案进行了比较,结果如表 6 所示。同时,散点图如图 12 所示,以便更直观地比较该方案与其他方案在硬件开销和吞吐率方面的差异。虽然文献[8]的硬件开销低于本文的工作,但其吞吐率仅 0.76 Mbps,并且移植难度很高,需要手动放置和布线。在文献[11]中,熵源电路由两个 10 阶 FIRO 和两个 11 阶 GARO 组成消耗了 288 个 LUTs 和 190 个 DFFs,是本结构开销的 8 倍以上。文献[12]使用 C 单元对 STR 中

表 4 NIST SP_800_90B IID 测试结果

Table 4 NIST-SP800-22 test results

NIST SP 800-90B		Kintex-7		Artix-7	
		$C_{[i][0]}$	$C_{[i][1]}$	$C_{[i][0]}$	$C_{[i][1]}$
偏移检验		2 487	0	4 445	0
定向运行数量检验		9 584	6	8 672	15
定向运行长度检验		6 624	3 104	876	1 873
增加减少数量检验		142	5	1 015	18
中位数数量检验		3 470	5	6 025	11
中位数长度检验		1 211	1 027	8 602	1 192
平均碰撞检验		6 160	2	5 446	5
最大碰撞检验		2 922	818	6 823	995
协方差测试统计(i=11)	周期(1)	430	7	5 013	25
	周期(2)	2 075	16	9 124	13
	周期(8)	638	4	7 695	16
	周期(16)	4 867	28	2 223	30
	周期(32)	1 945	22	3 299	35
	协方差(1)	614	3	2 927	7
	协方差(2)	5 326	7	8 430	3
	协方差(8)	5 951	4	3 512	10
	协方差(16)	2 418	3	2 306	3
	协方差(32)	314	0	203	1
压缩检验		1 856	51	1 608	56
卡方独立性检验		Pass		Pass	
卡方拟合优度检验		Pass		Pass	
LRS 测试		Pass		Pass	
独立性同分布测试		True		True	
最小熵		0.995 843		0.995 349	

表 5 TESTU01 测试结果

Table 5 TESTU01test results

Statistical	*P*-values	P/F
多比特重叠多项分布测试	0.12	Pass
近邻对闭合位匹配测试 t=(2,4)	(0.24,0.07)	Pass
近似稀疏性测试	0.43	Pass
线性复杂度测试	0.23	Pass
莱姆佩尔-齐夫压缩测试	0.5	Pass
傅里叶频谱测试(维度=1)	0.55	Pass
傅里叶频谱测试(维度=3)	0.43	Pass
字符串最长头部游程测试	0.53	Pass
字符串周期性子串测试	0.23	Pass
字符串汉明权重测试	0.32	Pass
字符串汉明相关性测试 L=(32,64,128)	(0.84,0.02,0.03)	Pass
字符串汉明独立性测试 L=(16,32,64)	(0.64,0.45,0.66)	Pass
字符串自相关函数测试 d=(1,2)	(0.65,0.73)	Pass
字符串游程分布测试	0.61	Pass
矩阵秩测试 32×32	0.88	Pass
随机游走测试 (H,M,J,R,C)	(0.84,0.52,0.77,0.69,0.16)	Pass

的独立抖动进行精确量化,有效地提取了熵源的随机性,其资源开销是本文结构的 1.5 倍。文献[26]中的随机源由 31 阶 GARO 提供,多项式选择为表 1 的多项式 5,他们利用 GARO 产生的随机信号对正常 PLL 产生的规则时钟进行采样,资源消耗略大于本文结构,但吞吐率不足本文结构吞吐率的 1/2。文献[27]将亚稳态引入 GARO 和 FIRO,消耗了大量资源却仅有 88 Mbps 的吞吐率。文献[28]提出的矩阵反馈环形振荡器(MFRO)可以在 FIRO,GARO,布尔混沌环形振荡器几种模式来回切换,资源消耗略高于本结构,但吞吐率却远不及本文结构。文献[29]通过利用 RO 中的抖动作为随机性的来源但资源消耗是本文结构的 2 倍以上。虽然文献[30]可以达到 150 Mbps 的吞吐率,但其硬件资源消耗大约是本文结构的 8 倍。

表 6 与其他 TRNG 的比较

Table 6 Comparison with other TRNGs

结构	Entropy Source	Area(LUTs+DFFs)	吞吐率/Mbps	平台
文献[8]	LRO	4LUTs+3DFFs	0.76	Spartan-6
文献[11]	FIGARO	288 LUTs+190DFFs	400	–
文献[12]	STR	56LUTs+19DFFs	100	Virtex-6
文献[26]	GARO	50LUTs+79DFFs	280	Artix-7
文献[27]	Met_FIGARO	1063LUTs	88	EP4CEl5F17C8
文献[28]	MFRO	44 LUTs	125	XC6SLX16
文献[29]	RO	83LUTs+26DFFs	100	Cyclone II
文献[30]	DCFL	298LUTs	150	Cyclone IV
本文	DMRO	36LUTs+16MUXs+4DFFs	750	Artix-7
	DMRO	36LUTs+16MUXs+4DFFs	750	Kintex-7

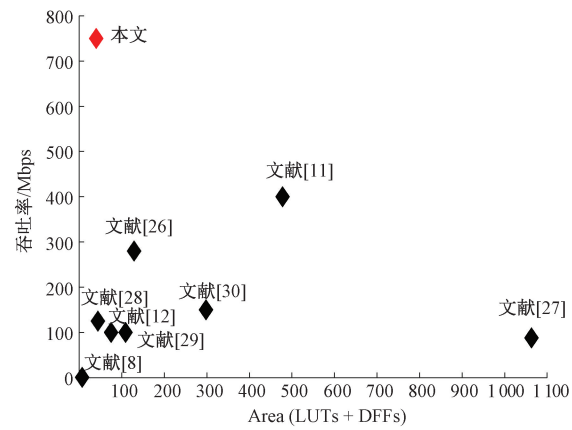


图 12 与近年来报道的其他 TRNG 的直观比较

Fig. 12 Visual comparison with other TRNGs reported in recent years

4 结　论

本文提出了一种多熵源双模式振荡环 DMRO-TRNG 结构。通过结合多熵源采集与双模式动态切换机制,在保证随机性质量的同时显著增加了吞吐率。该结构在 Xilinx Artix-7 和 Kintex-7 FPGAs 上实现,实验结果表明,该真随机数产生器在通过 NIST SP800-22 和 NIST SP800-90B 随机性测试的情况下,仅消耗 36 个 LUTs,4 个 DFFs 和 16 个 MUXs 就可以达到 750 Mbps 的吞吐率。且仅使用简单的异或后处理电路,硬件开销低。因此,该方案将成为信息安全应用领域中一个具有竞争力的候选方案。未来研究将聚焦于抗物理攻击能力的增强、动态熵源自适应选择机制的开发,进一步拓展其在密码学芯片与安全通信系统中的实际应用价值。

参考文献

[1] ANANDAKUMAR N N, SANADHYA S K, HASHMI M S. FPGA-based true random number generation using progr, ammable delays in oscillator-rings [J]. IEEE Transactions on Circuits and Systems II: Express Briefs, 2019,67(3): 570-574.

[2] YAO L, WU X, ZHANG H. DCDRO: A true random number generator based on dynamically configurable dual-output ring oscillator [J]. Integration, 2023, 93: 102053.

[3] 刘正文, 易茂祥, 杨云, 等. 一种高吞吐率自治布尔网络真随机数发生器[J]. 电子测量与仪器学报, 2023, 37(9): 102-109.
LIU ZH W, YI M X, YANG Y, et al. A true random number generator for high throughput autonomous boolean networks [J]. Journal of Electronic Measurement and Instrumentation, 2023, 37(9): 102-109.

[4] NI T, PENG Q, BIAN J, et al. Design of true random number generator based on multi-ring convergence oscillator using short pulse enhanced randomness [J]. IEEE Transactions on Circuits and Systems I: Regular Papers, 2023, 70(12): 5074-5085.

[5] CHOI P, LEE M K, KIM D K. Fast compact true random number generator based on multiple sampling [J]. Electronics Letters, 2017, 53(13): 841-843.

[6] LI C, WANG Q, JIANG J, et al. A metastability-based true random number generator on FPGA[C]. 2017 IEEE 12th International Conference on ASIC (ASICON). IEEE, 2017:738-741.

[7] FUJIEDA N, TAKEDA M, ICHIKAWA S. An analysis of DCM-based true random number generator[J]. IEEE Transactions on Circuits and Systems II: Express Briefs, 2019, 67(6): 1109-1113.

[8] DELLA SALA R, BELLIZIA D, SCOTTI G. A novel ultra-compact FPGA-compatible TRNG architecture exploiting latched ring oscillators[J]. IEEE Transactions on Circuits and Systems II: Express Briefs, 2021, 69(3): 1672-1676.

[9] 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, 2006, 56(1): 109-119.

[10] 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, 2019, 67(3): 570-574.

[11] NANNIPIERI P, DI MATTEO S, BALDANZI L, et al. True random number generator based on Fibonacci-Galois ring oscillators for FPGA[J]. Applied Sciences, 2021, 11(8): 3330.

[12] 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, 2020, 68(2): 741-750.

[13] DICHTL M. Fibonacci ring oscillators as true random number generators-a security risk[J]. Cryptology ePrint Archive, 2015.

[14] YANG Y, JIA S, WANG Y, et al. A reliable true random number generator based on novel chaotic ring oscillator[C]. 2017 IEEE International Symposium on Circuits and Systems (ISCAS). IEEE, 2017: 1-4.

[15] GÜLER Ü, ERGÜN S, DÜNDAR G. A digital IC random number generator with logic gates only[C]. 2010 17th IEEE International Conference on Electronics, Circuits and Systems. IEEE, 2010: 239-242.

[16] LU Y, YANG Y, HU R, et al. High-efficiency TRNG design based on multi-bit dual-ring oscillator[J]. ACM Transactions on Reconfigurable Technology and Systems, 2023, 16(4): 1-23.

[17] 项洪越. 数字混沌映射的动力学特性改进及其在图像加密中的应用研究[D]. 南昌:南昌大学,2021.
XIANG H Y. Improvement of dynamical properties of digital chaotic mapping and its application in image encryption[D]. Nanchang: Nanchang University, 2021.

[18] CUI J, YI M, CAO D, et al. Design of true random number generator based on multi-stage feedback ring oscillator[J]. IEEE Transactions on Circuits and Systems II: Express Briefs, 2021, 69(3): 1752-1756.

[19] SCHRAMM M, DOJEN R, HEIGL M. Experimental

assessment of FIRO-and GARO-based noise sources for digital TRNG designs on FPGAs[C]. 2017 International Conference on Applied Electronics (AE). IEEE, 2017: 1-6.

[20] GOLIC J D. New methods for digital generation and postprocessing of random data[J]. IEEE Transactions on Computers, 2006, 55(10): 1217-1229.

[21] DELLA SALA R, BELLIZIA D, SCOTTI G. High-throughput FPGA-compatible TRNG architecture exploiting multistimuli metastable cells [J]. IEEE Transactions on Circuits and Systems I: Regular Papers, 2022, 69(12): 4886-4897.

[22] CHEN Y, LIANG H, ZHANG L, et al. High throughput dynamic dual entropy source true random number generator based on FPGA[J]. Microelectronics Journal, 2024, 145:106113.

[23] JIN L Y, YI M X, XIAO Y. A dynamically reconfigurable entropy source circuit for high-throughput true random number generator [J]. Microelectronics Journal,2023, 133: 105690.

[24] BARKER E, KELSEY J. Recommendation for the entropy sources used for random bit generation[J]. NIST Special Publication 800-90B, 2012.

[25] YANG S, LIANG H, HU R, et al. Lightweight hybrid entropy source true random number generator based on jitter and metastability [J]. IEEE Transactions on Circuits and Systems II: Express Briefs, 2024,71(7): 3513-3517.

[26] LIN J, WANG Y, ZHAO Z, et al. A new method of true random number generation based on Galois ring oscillator with event sampling architecture in FPGA [C]. 2020 IEEE International Instrumentation and Measurement Technology Conference (I2MTC). IEEE, 2020: 1-6.

[27] FAN L, LONG Y, LUO J, et al. A true random number generator based on meta-stable state [J]. IEICE Electronics Expresss (ISCAS). IEEE, 2017: 1-4.

[28] YANG Y, JIA S, WANG Y, et al. A reliable true random number generator based on novel chaotic ring oscillator[C]. 2017 IEEE International Symposium on Circuits and Systems (ISCAS). IEEE, 2017: 1-4.

[29] WOLD K, TAN C H. Analysis and enhancement of random number generator in FPGA based on oscillator rings [J]. International Journal of Reconfigurable Computing, 2009(1): 501672.

[30] 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). IEEE, 2017: 1-4.

作者简介

鲁迎春,2002 年于合肥工业大学获得学士学位,2005 年于合肥工业大学获得硕士学位,2021 于合肥工业大学获得博士学位,现为合肥工业大学副教授、硕士生导师,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 and M. Sc. supervisor at Hefei University of Technology. His main research interests include Hardware Security and FPGA application design.

马利祥(通信作者),2008 年于山东大学获得学士学位,2013 年于中国科学院大学获得博士学位,现为安徽信息工程学院高级工程师,主要研究方向为智能传感器、雷达信号处理、摩擦电式微纳能源、智慧网联等。

E-mail: lxma@ iflytek. com

Ma Lixiang (Corresponding author) received his B. Sc. degree from Shandong University in 2008, Ph. D. degree from the University of Chinese Academy of Sciences in 2013, respectively. Now he is a senior engineer of Anhui Information Engineering College. His main research interests include intelligent sensor, radar signal processing, triboelectric micro-nano energy, intelligent network connection, etc.