分类号：TN402　　单位代码：10363
密　级：公开　　学　　号：2220330102

基于 FPGA 熵源叠加的高吞吐量 TRNG 研究

RESEARCH ON HIGH-THROUGHPUT TRUE RANDOM NUMBER GENERATOR BASED ONENTROPY SOURCE SUPERPOSITION OF FPGA

学 生 姓 名 ： 俞俊勇

指 导 教 师 ： 倪天明（教授）

学 科 专 业 ： 集成电路科学与工程（0811J3）

研究方向(领域)： 硬件安全

论 文 答 辩 日 期 ： 2025 年 5 月 10 日

二、安徽工程大学学位论文原创性声明

本人郑重声明：本人恪守学术道德，崇尚严谨学风。所呈交的学位论文，是本人在导师的指导下，独立进行研究工作所取得的成果。除文中已明确注明和引用的内容外，本论文不包含任何其他个人或集体已经发表或撰写过的作品及成果的内容。论文为本人亲自撰写，本人对所写的内容负责，并完全意识到本声明的法律后果由本人承担。

学位论文作者签名：俞俊勇

日期：2025年 5月 6 日

三、安徽工程大学学位论文版权使用授权书

学位论文作者完全了解学校有关保留、使用学位论文的规定，同意学校保留并向国家有关部门或机构送交论文的复印件和电子版，允许论文被查阅或借阅。本人授权安徽工程大学可以将本学位论文的全部或部分内容编入有关数据库进行检索，可以采用影印、缩印或扫描等复制手段保存和汇编本学位论文。

保密 □，在 ____ 年解密后适用本版权书。

本学位论文属于

不保密 ☑。

学位论文作者签名：俞俊勇　　指导教师签名：张元叶

日期：2025 年 5 月 16 日　　日期：2025 年 5 月 16 日

基于 FPGA 熵源叠加的高吞吐量 TRNG 研究

摘 要

随着计算机网络技术的发展，诸多信息泄露的危险事件频发，物联网（Internet of Things, IoT）等新兴产业对高可靠加密的需求迫切。作为加密系统的核心组件，基于物理熵源的真随机数发生器（True Random Number Generator, TRNG, TRNG）应用于协议认证、密钥生成、初始化向量等关键领域。现场可编程门阵列（Field Programmable Gate Array, FPGA）具备硬件资源丰富、灵活性高、开发周期短等特点，已成为主流的全数字 TRNG 的开发平台。

当前 FPGA 平台主要采用两类熵源实现方案：基于时钟抖动的环形振荡器（Ring Oscillator, RO）架构和基于时序违规的亚稳态架构。前者通过奇数个反相器链产生时钟抖动，但存在累积速率慢、吞吐量低、硬件开销大等固有缺陷。后者必须对触发器的输入端口和时钟端口的时钟进行精密的延时配置和严格的布局布线，导致可移植性差，且需接入额外的后处理电路来消除偏置。

针对基于抖动的 TRNG 的相关问题，本文提出了一种基于多异或门耦合单元（Coupling Multiple XOR gate cells, CMX-cell）的真随机数发生器，该电路利用了异或门来加快抖动的累积，采用了将反相器链与异或门隔离的方法削弱信号在传输过程产生的短脉冲抑制现象，将不同频率的 RO 中的抖动通过短脉冲信号进行叠加。针对基于亚稳态的 TRNG 的相关问题，本文提出了一种基于亚稳态叠加单元（Metastable Superposition cells, MS-cell）的真随机数发生器，该电路采用反馈设计，将异或门与多路复用器（Multiplexers, MUX）所引导的两类不同的亚稳态在一定的条件下叠加，通过不同级数的 RO 来自由运行，无需对采样时间进行控制。

本文所提出的两种 TRNG 均是基于 Xilinx Vritex-7 FPGA 和 Xilinx Artix-7 FPGA 开发板上进行设计和测试的。测试结果表明，两种 TRNG 均可以通过偏差测试、自相关测试、重启动测试、温度波动测试、电压波动测试、NIST SP800-22 测试和 NIST SP800-90B 测试。其中，基于多异或门耦合单元的 TRNG 以 31 个查找表（Look-Up Tables, LUTs）和 8 个触发器（Flip-Flops, FFs）的硬件开销实现了 500 Mbps 的吞吐量；基于亚稳态叠加单元的 TRNG 以 29 个查找表和 4 个触发器的硬件开销实现了高达 500 Mbps 的吞吐量。本文所提两种 TRNG 均具有良好的随机性与鲁棒性，硬件开销极低。与其他国际上先进的 TRNG 对比结果可知，所提两种 TRNG 具有最高的吞吐量。

关键词：FPGA，真随机数发生器，时钟抖动，亚稳态，吞吐量

RESEARCH ON HIGH-THROUGHPUT TRUE RANDOM NUMBER GENERATOR BASED ON ENTROPY SOURCE SUPERPOSITION OF FPGA

ABSTRACT

With the development of computer network technology, many dangerous incidents of information leakage occur frequently, and emerging industries such as the Internet of Things have an urgent need for high reliable encryption. As the core component of encryption system, True Random Number Generator based on physical entropy source is used in key fields such as protocol authentication, key generation and initialization vector. Field Programmable Gate Array has become the mainstream all-digital TRNG development platform due to its rich hardware resources, high flexibility and short development cycle.

At present, two kinds of entropy source schemes are mainly used in FPGA platform: Ring Oscillator architecture based on clock jitter and metastable architecture based on timing violation. The former generates clock jitter through an odd number of inverter chains, but it has some inherent defects such as slow accumulation rate, low throughput and high hardware overhead. The latter must perform precise delay configuration and strict layout of the clock of the trigger input port and the clock port, resulting in poor portability and additional post-processing circuits to eliminate bias.

To solve the related problems of TRNG based on jitter, a TRNG based on a Coupling Multiple XOR gate cells is proposed in this paper. TRNG based on a coupling multiple XOR gate is used to accelerate jitter accumulation. The method of isolating the inverter chain from the XOR gate is used to weaken the phenomenon of short pulse suppression in the transmission process, and the jitter in different frequency RO is superimposed by short pulse signals. Aiming at the problems related to metastable TRNG, this paper proposes a TRNG based on metastable superposition cells, which adopts feedback design. Two kinds of metastables guided by XOR gate and Multiplexers are superimposed under certain conditions and run freely through different order of RO without controlling the sampling time.

The two TRNGS proposed in this paper are designed and tested on Xilinx Vritex-7 FPGA and Xilinx Artix-7 FPGA development board. The test results show that both TRNGS can pass the deviation test, autocorrelation test, restart test, temperature fluctuation test, voltage fluctuation test, NIST SP800-22 test and NIST

SP800-90B test. Among them, TRNG based on multi-XOR gate coupling unit achieves a throughput of 500 Mbps with the hardware overhead of 31 Look-Up Tables and 8 Flip-Flops. The metastable stack cell based TRNG achieves a throughput of 500 Mbps with the hardware overhead of 29 Look-Up Tables and 4 Flip-Flops. The proposed two TRNGS have good randomness and robustness, low hardware overhead, and the highest throughput compared with other advanced TRNGS in the world.

KEY WORDS： FPGA, true random number generator, clock jitter, metastability, throughput

目 录

插图清单

表格清单

第 1 章 绪论

1.1 研究背景及意义

物联网[1]将各种传感器、处理器等智能设备连接起来，形成一个巨大的网络。这些设备实时产生数据，与周围其他设备交换数据并建立联系。IoT 广泛应用于智能家居、智能电网、智能医疗系统、工业物联网和车联网等领域，预计 2025 年物联网终端设备将激增到 750 亿台[2]。然而物联网技术[3]的应用也带来了层出不穷的安全隐患。例如：2016 年 10 月 21 日，美国东海岸发生世界上瘫痪面积最大、时间量长（6 个多小时）的分布式拒绝服务攻击，“物联网破坏者”劫持网络摄像头，让上百万摄像头同时请求访问互联网，造成网络堵塞瘫痪[4]。2018 年 8 月，台积电遭到勒索病毒入侵，导致台积电在中国台湾省的北、中、南三个重要生产基地停摆几个小时，造成约十几亿美元的营业损失[4]。2022 年 3 月，宏基服务器被勒索软件攻击，要求支付 5000 万美元，后又被爆出服务器受到入侵，窃取了超过 60G 的文件和数据库。2024 年 7 月，宏碁、戴尔、技嘉、英特尔和超微电脑等 5 大设备商的 200 多款机型存在安全启动问题。支撑这些设备安全启动的加密密钥在 2022 年被泄露，几乎所有主要设备制造商的近 300 多种额外设备型号的安全引导完整性都存在严重问题。除此之外，安全设备还存在着诸多非侵入式攻击的威胁，例如：Hayashi 等人[5]对一个符合 ISO/IEC18033 标准的密码模块进行攻击,在不影响密码模块正常工作的情况下获取了密钥信息；Elmohr 等人[6]对基于 ARM 架构和 RISC-V 架构的处理器进行攻击,实现了多条指令的跳过；Majeric 等人[7]详细分析了一个集成了 AES 128 加速电路的片上系统受到电磁故障注入攻击时的行为，观察到在攻击发生时，AES 128 加密过程会出现错误。

上述这些恶性事件都涉及到了物联网设备的硬件安全问题，硬件安全主要体现在固件的安全上，固件作为嵌入式设备的“大脑”，不仅控制设备功能，实现设备协议，还存有敏感信息[8]。固件缺乏加密保护可能导致黑客从设备中提取固件信息并对固件进行分析，从而造成信息泄露[8]。身份验证是安全物联网系统的基本组成部分，用于验证被认证者真实的身份[9]。在基于相互认证协议的物联网设备中，主要的熵生成器是物理不可克隆函数（Physical Unclonable Function, PUF）与真随机数发生器，前者通过利用集成电路制造中不可控制的工艺偏差来生成稳定的唯一标识符[10]，而后者用于创建与电路特征无关的随机无偏比特流[11]。图 1-1 展示了一个 HTTPS 会话流程，其中预主密钥关乎着后续信息的正常交互，增加了系统的安全性。即使有攻击者入侵通信过程，由于预主密钥的存在，难以计算出主密钥和会话密钥，无法窃取数据。TRNG 可提供不可预测的高质量随机数作为预主密钥，进行信息加密，保障数据通信的安全。

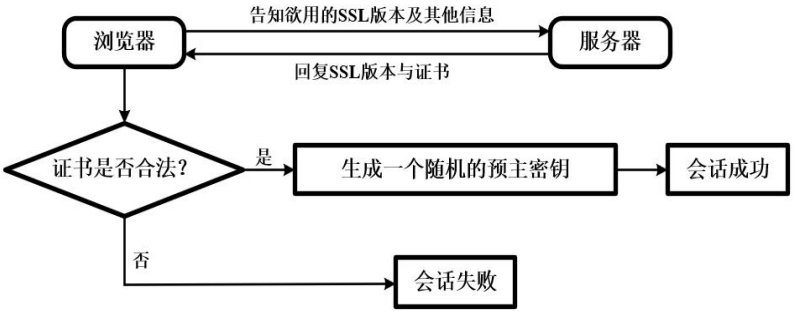

图 1-1 HTTPS 的会话流程

随机数在现代密码技术中具有重要的地位，堪称现代密码技术的基石。随机数的产生依赖于随机数发生器，相比于由种子和迭代算法所生成的、易被破解的伪随 机数发生器，真随机数发生器在安全性上更受高可靠加密系统的青睐。TRNG 的安全性来自于熵源的不可预测性，并选用一些随机的物理现象作为熵源，例如电阻中的放大后的热噪声[12-15]、组合逻辑电路中的亚稳态[16,19,21,25]、锁存器中的亚稳态[17,24]、含抽头延时链的高精度采样电路的亚稳态[18,22,23]、环形振荡器中的相位抖动[26,27,28,29,37]、锁相环中的相位抖动[31]、数字时钟管理器中的相位抖动[32]、自定时环中的相位抖动[36]、基于瞬态效应的环形振荡器中的抖动[33-34]、基于游标技术的高精度量化后的相位抖动[30]、放射性衰变[38]、元胞自动机中的混沌现象[39]、混沌电路中的振荡行为[40-43]等。这些物理现象来源于自然界，以它们作为 TRNG 的熵源安全性更高，所产生的随机序列更加难以预测，更能满足高可靠加密系统对于高质量随机数的需求。图 1-2 展示了真随机数发生器作为密钥生成器在物联网上的加密应用：TRNG 与其他密钥生成算法结合，生成密钥对明文进行加密保护，防止被第三方窃取。

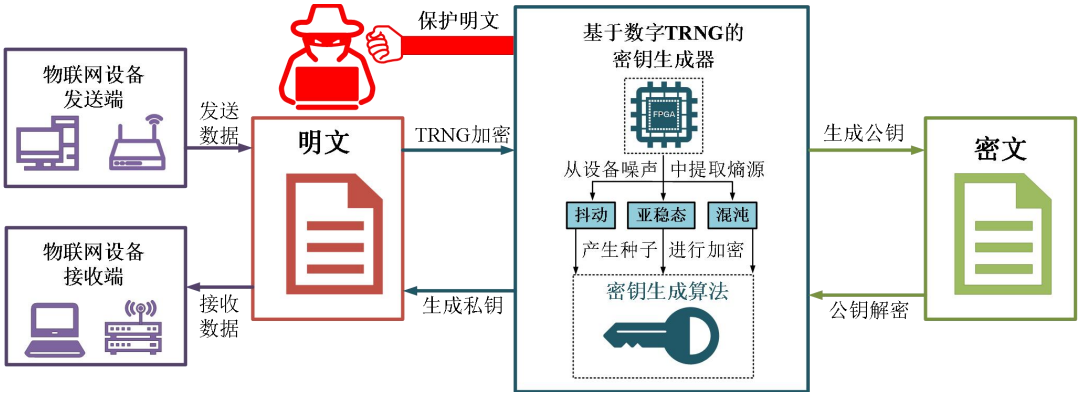

图 1-2 TRNG 的密钥生成器应用

硬件随机数发生器可以由模拟电路实现，也可以由数字电路实现。模拟电路设计 TRNG 存在诸多不变，如速度精度受限、测试验证困难、工艺设计复杂等方面的问题，会给 TRNG 的设计带来很大的研发成本。但基于 FPGA 的全数字 TRNG 可以进行快速开发测试，并且具有良好的可移植性。同时随着数字电路的飞速发展，低速率的 TRNG 难以满足高速密码电路的需求，因此要求 TRNG 具有高吞吐量的特点，来快速产生高质量的随机序列。

1.2 国内外研究现状

人们的生活离不开随机数。早期，人们通过采用抽签、掷骰子、抛硬币等方法产生随机数。随着科学技术的不断发展，高可靠加密系统对随机数的质量、数量和生成速率等指标提出了更高的要求。1946 年冯诺依曼率先创造了伪随机数发生器，即平方取中法。但采用这种方法所生成的随机序列，最终不可避免地会陷入循环中。1949 年，数学家 D.H.Lehmer 利用线性同余生成器（LCG）也实现了随机生成器，但其仍然具有周期性。直到 1951 年，阿兰·图灵在计算机中设置了随机数生成指令，并利用导体中的电子热振荡所产生的热噪声，一次可产生 20 个随机序列。该方案首次将随机的物理事件与计算机相结合，可产生真正的随机数。此后 TRNG 的设计百花齐放，陆续开发出了一系列不同熵源、结构各异、采样方法多样的 TRNG。

随着集成电路产业迅猛发展，FPGA 受到设计真随机数发生器的研究人员的重视。在 FPGA 上实现的数字 TRNG 需要具备良好的熵、吞吐量以及可移植性。时钟抖动和亚稳态现象是 FPGA 平台上应用最广泛的熵源。目前真随机数发生器的国内外研究现状如下：

（1）基于时钟抖动的真随机数发生器：2004 年，乔治梅森大学的 P. Kohlbrenner 团队[44]提出提出使用两个由奇数个反相器组成环形振荡器相互采样的方法来提取 RO 中相位抖动的随机性。2006 年，意大利电信的 Jovan Golić等人[45]在传统 RO 中嵌入异或门来实现反馈结构，提出了斐波那契环形振荡器和如伽罗瓦环形振荡器。采用其相互采样的方式来改善基于 RO 的 TRNG 中存在的耦合降低随机性的问题，同时也大大提升了 TRNG 的吞吐量。2007 年，加大拿滑铁卢大学的 Sunar[46]团队提出将多个 RO 的输出接入异或门再进行采样的方法来提升 TRNG 的吞吐量，但这种做法需要后处理电路。2008 年，挪威科技大学的 K. Wold[47]团队提出对 RO 先进行采样再进行异或的方法，避免了异或门处理高速变化的脉冲。此法大大提升了基于 RO 的 TRNG 的随机性和吞吐量，且无需后处理电路。2010 年，科希策技术大学的 M. Varchola[48]团队提出了如图 1-3 所示的瞬态效应环形振荡器，它是将两个交叉耦合的异或门的一个输入端作为使能，在上电后记录整个电路从开始振荡到振荡停止这段时间内的振荡次数的最低有效位来量化随机性。

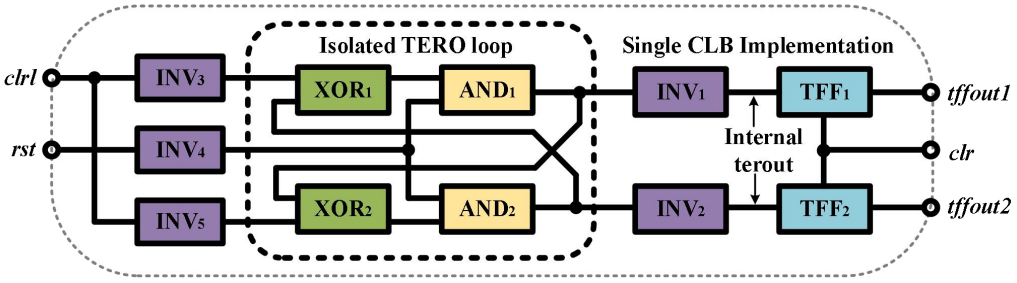

图 1-3 基于 TERO 的 TRNG

2012 年，法国圣艾蒂安大学的 A. Cherkaoui 和 V. Fischer[49]提出用如图 1-4 所示的自定时环作为熵源结构来增强传统 RO 对于恶劣环境变化的鲁棒性。

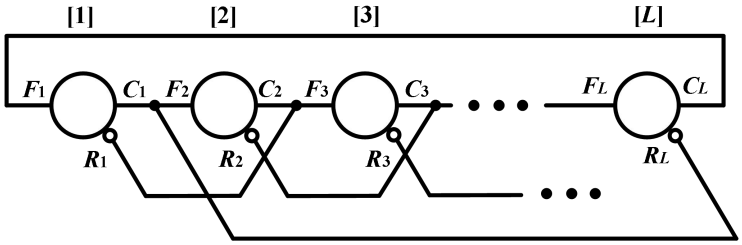

图 1-4 自定时环

2014 年，中国北京信息工程院的马原[50]团队认为基于 RO 的 TRNG 生成的随机序列可能含有伪随机性，由于电路中的扰动的存在会使得其更容易通过统计测试。因此提出了一个随机模型来评估基于振荡器的 TRNG 的熵，然后推导出设计参数（包括采样间隔）的要求，以保证每个随机位有足够的熵，即确保真正的随机性。2016 年，华中科技大学的刘冬生[51]团队提出了如图 1-5 所示的一种基于大抖动的四面体振荡器的 TRNG，具有低成本、低功耗的特点。其环路中包含多个相互嵌套的快环和慢环，导致电路充满线或逻辑和信号竞争，运行逻辑复杂，各种噪声扰动易激发多频率的振荡。

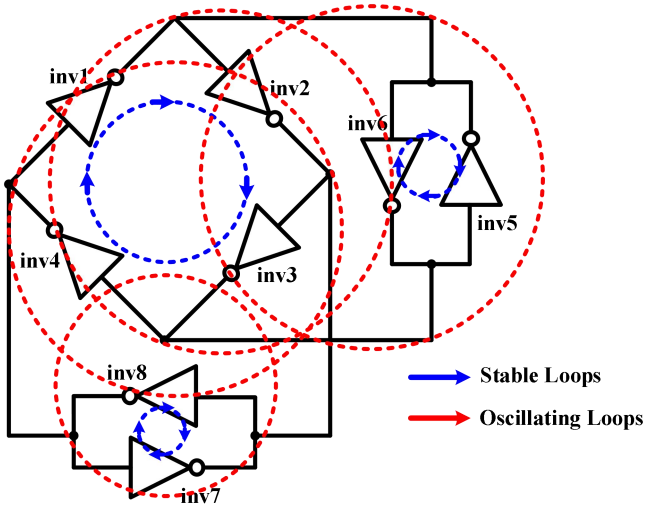

图 1-5 四面体结构的环形振荡器

2018 年，南京航空航天大学刘伟强[52]团队将异或门嵌入到 RO 中，提高了抖动累积的速度。2022 年，合肥工业大学黄正峰[53]团队提出了如图 1-6 所示的多级反馈振荡结构，通过在传统 RO 中引入多级的反馈，以极少的硬件开销实现了 290Mbps 的高吞吐量。2025 年，沙希德·贝赫什蒂大学 Mohammad Hossein Moaiyer[78]团队提出了一种基于亚临界电流区随机磁隧道结开关的可调真随机数发生器，所包含的控制器可用于产生零稳态误差的任意概率，使设计对工艺变化高度稳定。

（2）基于亚稳态的真随机数发生器：2002 年，英国纽尔斯卡大学的 D. J. Kinniment[54]团队提出了利用双稳态电路中的噪声来设计基于亚稳态的模拟

TRNG，并且实现了 100Mbps 的吞吐量。2007 年，法国国家高等电信学院的 Jean-Luc Danger[55]团队首次提出了如图 1-7 所示的基于开环结构的亚稳态 TRNG，其可移植性差，对延迟链的布局布线要求极高。

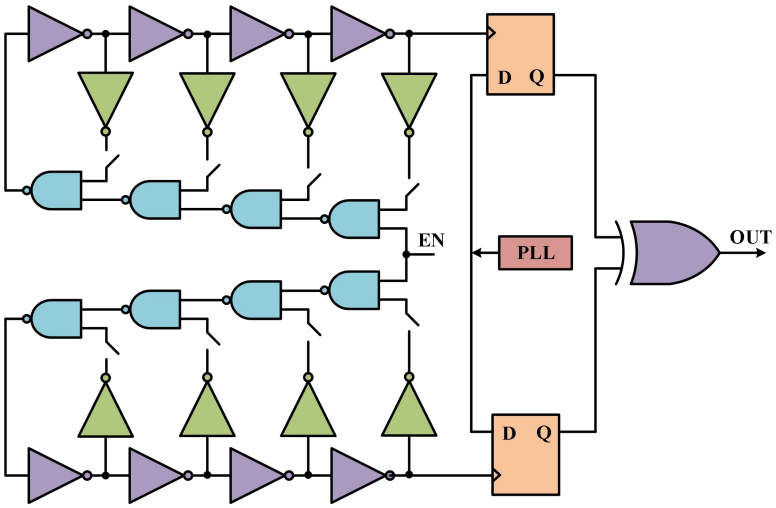

图 1-6 基于多级反馈环形振荡器的 TRNG

2008 年，美国密西根大学的 Trevor Mudge[56]团队提出了一种基于亚稳态的真随机数生成器，通过测量亚稳态分辨率时间来对随机性概率进行分级，可动态控制使系统能够响应确定性噪声，且分级模块允许用户权衡输出比特率和比特流的质量。2011 年，美国莱斯大学的 Mehrdad Majzoobi[57]团队提出了如图 1-8 所示的 TRNG，利用可编程延迟线控制 D 触发器的输出信号和时钟信号的延时差，强制时钟和输入信号几乎同时跳变。

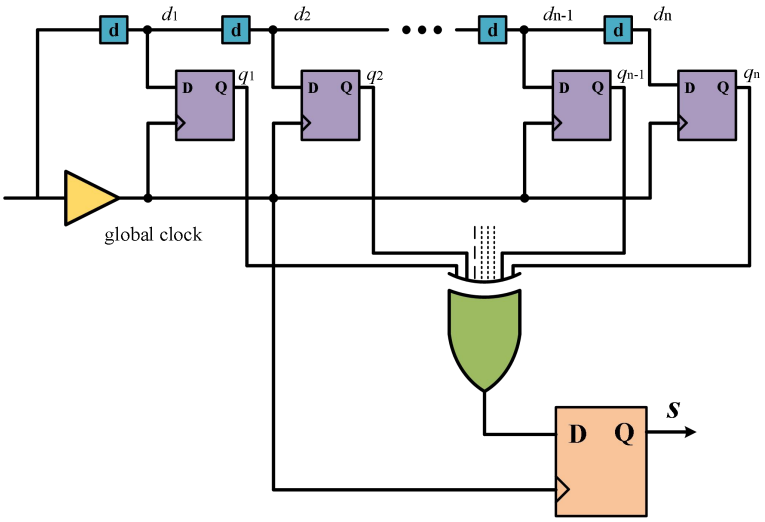

图 1-7 基于开环结构的亚稳态 TRNG

2012 年，丰桥工业大学 Hisashi Hata[58]团队研究了 RS 锁存器在同时使能 R、S 的时候进入亚稳态的现象，提出 RS 锁存器亚稳态 TRNG 结构。2013 年，波兰华沙理工大学的 Piotr Zbigniew Wieczorek[59]团队提出了如图 1-9 所示的利用数字时钟管理器来调节延时来设计基于亚稳态 TRNG 的方法，但需要额外的后处理电路克服随机数的统计弱点。

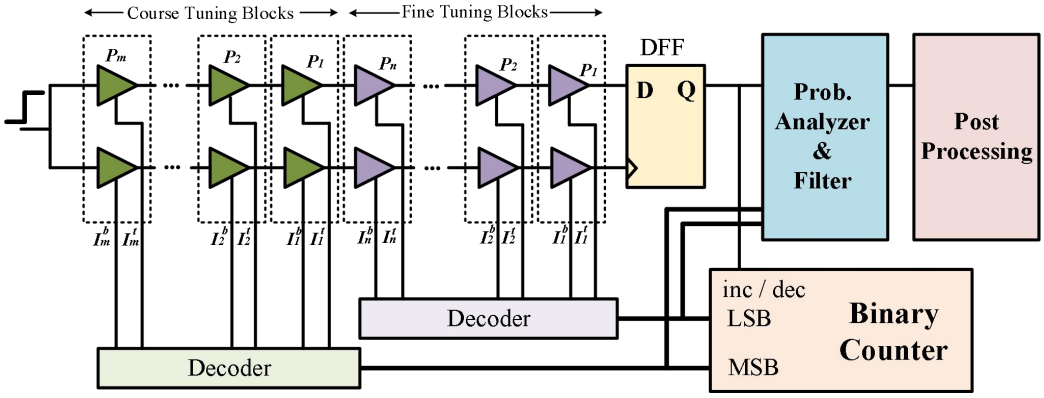

图 1-8 基于可编程延迟线的 TRNG

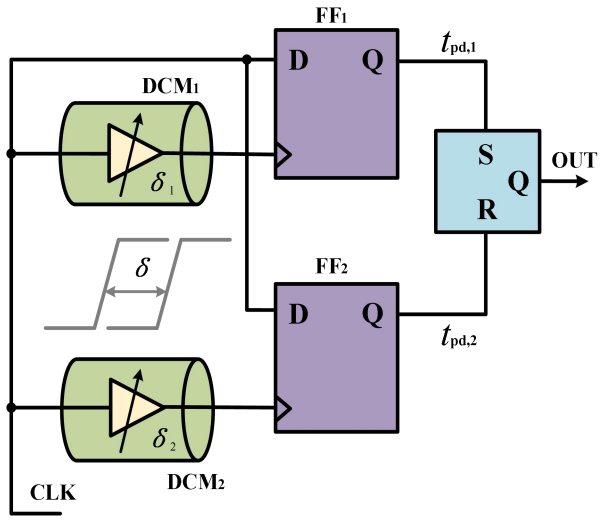

图 1-9 基于数字时钟管理器的 TRNG

2016 年，波兰华沙理工大学的 Piotr Zbigniew Wieczorek[60]团队为克服传统亚稳态需要繁琐路由的缺点，提出了一种基于临近亚稳态的 TRNG 设计。2017 年，上海交通大学王琴[61]团队提出如图 1-10 所示的亚稳态 TRNG，它使用可调节的上升沿周期来对 RS 锁存器的亚稳态信号进行采样，可通过对电路进行手动路由来提高亚稳态事件的数量。

2018 年，杭州电子科技大学的樊凌雁[62]团队提出了一种将亚稳态与斐波那契环形振荡器和伽罗瓦环形振荡器相结合的环形振荡器结构，提升了 TRNG 的随机性和吞吐量。2022 年，意大利罗马大学的 Giuseppe Scotti[63]团队提出了一种利用锁存异或门的真随机数生成器，旨在通过结合锁存器亚稳态和 RO 抖动的影响来提高基于传统 RO-TRNG 的吞吐量。2023 年，合肥工业大学的梁华国[64]团队提出了一种使用具有动态可重构延迟链的环形振荡器的新型熵源电路，所提出 TRNG 结构结合了信号抖动和电路亚稳态两种熵源。2024 年合肥工业大学梁华国[35]团队提出了一种基于抖动和亚稳态的轻量级混合熵源 TRNG 实现方案，该方案使用底层现场可编程门阵列原语语言构建双交叉耦合 XOR 门单元来生成随机输出序列，具有良好的硬件效率。

综上所述，基于抖动的真随机数发生器具有抖动的累积速率较慢、吞吐量较

低、硬件开销极大的缺点。基于亚稳态的真随机数发生器存在可移植性差、吞吐量较低、需要设计出额外的后处理电路来消除偏置的问题。为了解决这些问题并设计出具有高吞吐量的轻量级真随机数发生器，本文分析了不同熵源电路的缺点，结合了相同熵源的随机性叠加，展开了一系列的设计实验工作。

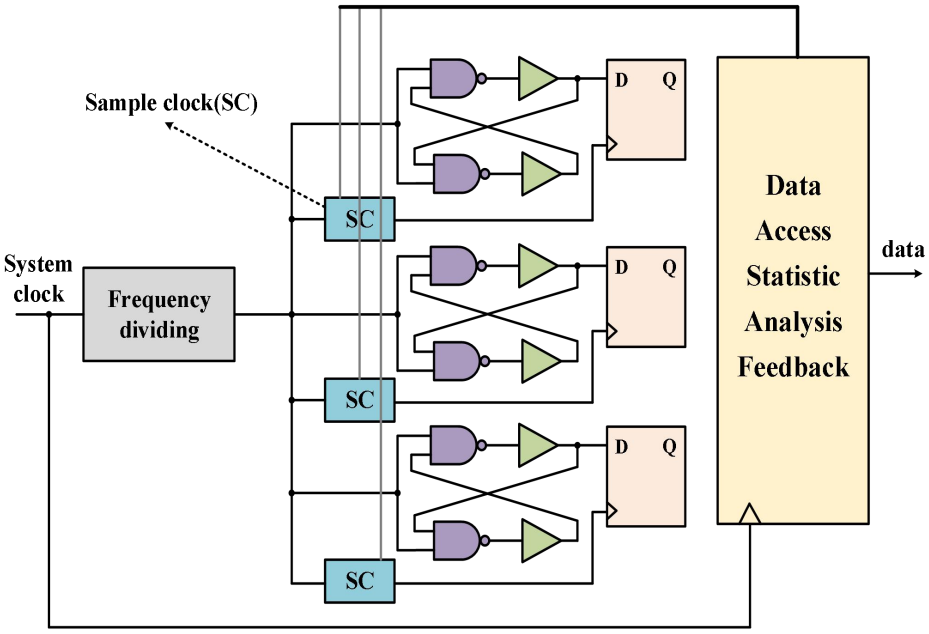

图 1-10 基于 RS 锁存器的亚稳态 TRNG

1.3 论文结构安排

本文共分为 6 个章节，具体安排如下：

第一章：介绍了随机数的研究背景，引导出 TRNG 的设计意义，并以熵源分类的形式对 TRNG 研究现状进行介绍。

第二章：介绍了随机数的定义、性质和随机数发生器的基本概念。详细阐述了 TRNG 的熵源、基本组成和异或组合技术的原理。

第三章：介绍了常见的基于抖动的 TRNG 设计，分析了这些 TRNG 电路的优势和存在的不足。对短脉冲抑制效应进行了详细的介绍，并说明了其危害。根据设计要求，提出了多异或门耦合单元，并结合了异或组合技术来构建完整的 TRNG 电路。

第四章：介绍了常见的基于亚稳态的 TRNG 设计，分析了这些 TRNG 电路的优势和存在的不足。对在组合电路中实现亚稳态 TRNG 进行详细的介绍，并说明了其在可移植性和吞吐量方面的优势。根据设计要求，提出了亚稳态叠加单元，并结合了异或组合技术来构建完整的 TRNG 电路。

第五章：将本文提出的两个 TRNG 电路进行一系列随机性测试，将数据可视化并进行相关讨论。最后将提出的结构与国际上先进的 TRNG 电路进行性能指标上的对比（硬件开销、吞吐率等）并展开分析讨论。

第六章：总结全文和展望。

第 2 章 随机数概念与真随机数发生器原理

2.1 随机数的基本概念

2.1.1 随机数的定义

在与信息安全相关的众多领域，随机数是不可忽略的重要环节，其定义是理解随机现象和进行相关研究的基础。从直观角度看，随机数是在一定范围内无规律出现的数值，但在数学和统计学中有严格定义。从数学角度定义，在一个既定的样本空间内，若一个变量的取值无法预先准确预测，且每个可能取值都有特定的概率与之对应，通过某种随机过程产生的数值，即为随机数。例如，在掷骰子的简单实验中，骰子的点数取值范围是 1 到 6，每次投掷前无法预知结果，且每个点数出现的概率理论上均为 1/6，这里每次投掷产生的点数就是一个随机数。

2.1.2 随机数的性质

随机数主要具有随机性、独立性和均匀性这三个关键性质：

（1）随机性是随机数的最重要的属性。直观而言，随机数没有任何的确定模式和规律，从数学上来讲，一个数列若不被确定，任一数项都不会受其他的数项的影响，即满足不可预测性。例如彩票的抽奖结果，每一次抽奖的结果都不应该受上次结果的影响，号码的抽取都是随机的。如果一种随机序列是可以预测的，那么这种序列在某些对安全性有着高要求的场合是无用的。

（2）随机性与独立性。每个随机数彼此间互不相关，即序列中的任何一个随机数的产生和取值都不依赖其它随机数。例如在硬币抛掷的例子中，每抛掷 1 次的结果（正面或者反面）与抛掷前面每一次结果无关，每抛掷一次得到正面或者反面的概率都为 1/2。应用到实际问题时，独立性确保了模拟的随机数对于复杂系统具有有效性，例如模拟放射性衰变实验中，放射性原子核的衰变时间、衰变粒子类型和衰变数量都是随机的，只有这些指标之间相互独立、互不干扰，模拟的结果才能真实体现放射性衰变的不确定性。

（3）随机数的均匀性体现在随机事件（如古典概型）发生时，在随机数的范围内，每个值出现的概率相同，即同一个样本空间内的任一数随机出现的概率相等。例如，在一副去掉大小王的扑克牌中（52 张），随机抽取一张，抽到黑桃、红桃、方片、梅花的概率是相等的，都为 1/4。在统计学抽样时，均匀性至关重要，它保证了抽样总体样本的代表性，不会由于过量或不充分地抽取某些值而导致结果产生偏差。

2.1.3 随机数发生器

随机数发生器是一种能够按照某种算法连续产生随机数的硬件设备或算法

程序。它的基本目的是产生具随机性、独立性以及均匀性的随机数列。

伪随机数生成器的工作原理是依据固定的算法生成随机数。如图 2-1 所示，PRNG 以一个随机的初始值（即种子）为基础，根据一个特定的算法进行重复迭代计算，得到连续的随机数。常见的随机数生成器的算法有线性同余法、Mersenne Twister 算法和 Weidmann's Algorithm 算法等。PRNG 的优点是生成快速、可重复、易于计算机程序实现；缺点是 PRNG 的迭代算法是已知的，若算法的初始值（种子）被窃取，则生成的随机数序列会被完全预测。因此算法的初始值为 PRNG 的熵源，PRNG 安全性仅取决于种子的保密程度，这极大限制了 PRNG 应用在高可靠加密系统等安全性要求极高的场合。

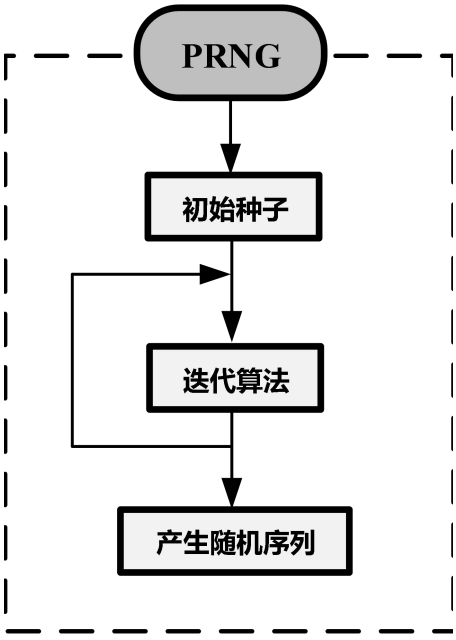

图 2-1 伪随机数发生器的框图

2.2 真随机数发生器原理

2.2.1 真随机数发生器的熵源

真随机数发生器在信息安全、密码学等领域具有不可替代的地位的重要原因之一是 TRNG 的熵源，在基于 FPGA 平台的 TRNG 设计中，使用最为广泛的熵源是时钟抖动和亚稳态。

时钟抖动是指时钟信号在上升沿或下降沿附近产生与理想周期或相位之间的不规律偏差。电子系统中理想的时钟信号应该是其振荡频率、幅度相同，但在实际电路中时钟信号会因热噪声、电源噪声以及自身电路元件固有的特性等因素产生时钟抖动，这种时钟抖动具有随机性，无法被不可预测，且相较于其他熵源易量化提取，是真随机数发生器的一个重要熵源。

一个触发器的输入信号在建立时间和保持时间内发生改变时（即亚稳态窗口），会进入一个不稳定的状态，这个状态称之为亚稳态。此时处于亚稳态的触发器的输出既不是高电位也不是低电位，而是一个中间的不确定状态，并且最终

稳定于哪种状态，输出是高电平还是低电平，是完全随机的，由电路中的噪声、工艺偏差、器件参数的微小差别等多种随机因素决定。

2.2.2 真随机数发生器的基本组成

如图 2-2 所示，真随机数发生器熵源电路、采样电路和后处理电路三部分组成，各个部分之间相辅相成，在整个 TRNG 电路中都起着重要作用。

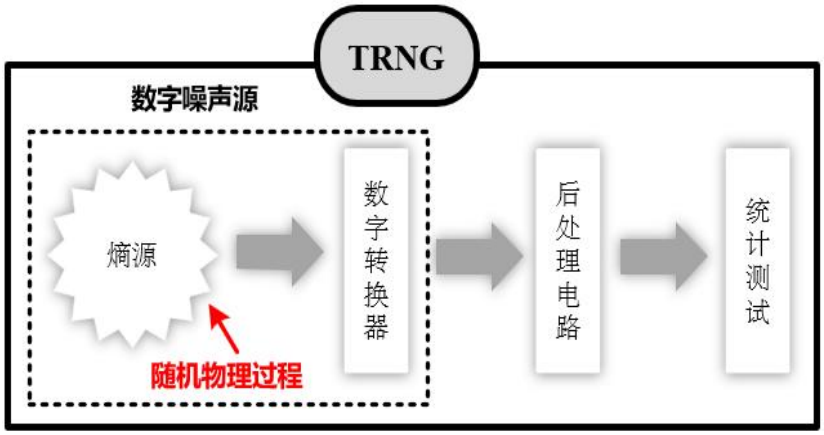

图 2-2 真随机数发生器的电路结构

真随机数发生器的熵源电路是最底层的电路，为真随机数的生成提供真正的随机物理来源。以时钟抖动为例，其幅值和相位都是随机的、不可预知的，并在熵源电路中以连续的电信号形式传播。采样电路是对熵源电路获取的真随机物理过程输出的连续随机信号进行采样的离散化处理，将连续的模拟量量化成一系列的数字量。采样频率的选择决定了该系列的数字信号是否包含熵源的尽可能多的信息，如果过小，有可能产生失真，如果过大，会使 TRNG 的输出呈现相关性。后处理电路相当于对真随机数发生器进行最后的“加工”，因为熵源电路的随机性在被采样电路量化之后存在不同程度的随机性削减，这与采样电路的精度有关。若采样后的输出序列不具备高可靠性，被引入了诸如偏差和相关性等统计弱点，则需要后处理电路对得到的原始真随机数进行调整优化。但后处理电路并非必要的环节，熵源质量高或采样电路精度高的 TRNG 无需后处理电路也能通过统计测试。虽然后处理电路能够消除统计弱点，但会增加 TRNG 的硬件开销，还可能压缩 TRNG 的吞吐量。

2.2.3 异或组合技术

若设计的 TRNG 性能指标较低，可采用异或组合技术来提高 TRNG 的熵[52]，以确保其能够通过统计测试。如图 2-3 所示，多个单一的 TRNG 熵源电路模块被看成一个单元，将多个单元经过相同频率的脉冲采样后，同时进行异或运算，即将采样后的多路输出通过异或树进行数据的处理。显然，这种做法不会压缩 TRNG 的吞吐量，但代价是带来了成倍的硬件开销。这种方法被称为“异或组合技术”并大量应用在具备高吞吐量优势的 TRNG 设计中。

异或组合技术提升香农熵的原理可以通过以下的数学模型验证：

首先给出香农熵的具体公式

$$H = -P_1 \log_2 P_1 - (1-P_1)\log_2(1-P_1) \tag{2-1}$$

其中，P1 表示 TRNG 输出为 1 的概率。

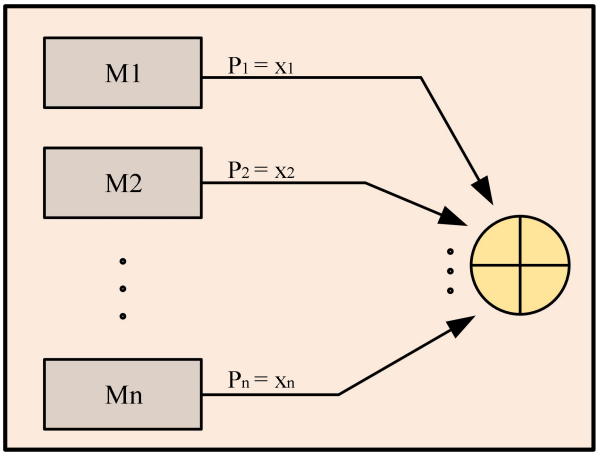

图 2-3 异或组合技术框图

由公式(2-1)易知，若 TRNG 的输出为 1 的概率越接近 0.5，则 TRNG 的香农熵越接近 1。由于异或运算具有“奇校验”的性质，可使用列真值表的方式建立概率模型。为便于表示异或函数，本文采用了与文献[63]类似的方法，假设每个 MS-cell 模块的输出为 1 的概率相同。如图 2-3 所示，把每个模块 M 输出为 1 的概率记作 x，异或之后的输出记为P_R^n，将异或函数记为F_n，n 为异或的模块个数。先考查两模块的异或函数：

$$P_R^2 = F_2(x) = 2x(1-x) \tag{2-2}$$

整理得

$$F_2(x) = 2x - 2x^2 \tag{2-3}$$

再考查 3 个模块的异或函数

$$P_R^3 = F_3(x) = 3x(1-x)(1-x) + x^3 \tag{2-4}$$

整理得

$$F_3(x) = 3x - 2x^2 + 4x^3 \tag{2-5}$$

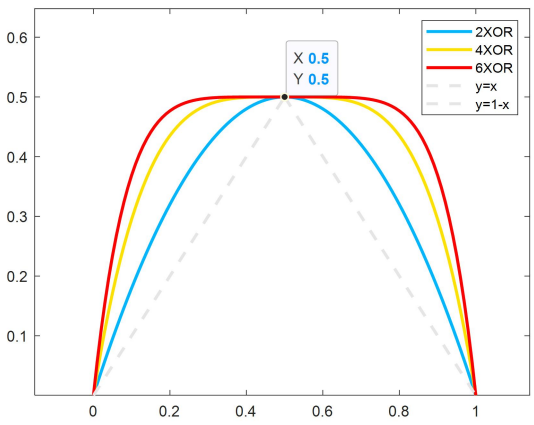

图 2-4 异或函数图像

由“数学归纳法”可推广到 n 元

$$F_n(x)=nx-2C_n^2x^2+4C_n^3x^3-8C_n^4x^4+\cdots \tag{2-6}$$

本文研究了异或数目为 2、4 和 6 的情形，并绘制了如图 2-4 所示的 3 种异或函数的图像。由图可知，三种异或函数的图像均位于虚线$y=x(0<x<0.5)$和虚线$y=1-x(0.5<x<1)$上方，说明进行异或处理与不进行异或处理相比，能够显著提高 TRNG 输出为 1 的概率（更接近 0.5），TRNG 香农熵更容易提升到 1。此外，对于相同的 x 值,异或数目越大，y 值就越接近 0.5。换言之，增大异或数目可以显著提升香农熵。

2.3 本章小结

在本章内容中，首先介绍了随机数定义、性质等基础概念，引导出随机数的产生方法，展开对随机数发生器的分类和组成结构的详细讲解。再将真随机数发生器原理作为重点内容展开，着重剖析真随机数发生器的熵源和基本组成。最后对不压缩 TRNG 吞吐量的异或组合技术进行了详细阐述，并建立数学模型阐明了异或数目与香农熵之间的关系。

第 3 章 基于多异或门耦合单元的 TRNG

3.1 基于抖动的真随机数发生器

振荡器的时钟抖动来源于电路内部的热噪声。在基于 FPGA 的 TRNG 设计中，常由奇数个反相器组成的环形振荡器(RO)的输出中包含的相位抖动作为 TRNG 的熵源。传统的 RO-TRNG 的设计思路是采用如图 3-1 所示的耦合振荡器，即利用低频的 RO 输出信号去采样一个高频的含有抖动的振荡信号[26]，但这种做法的周期匹配极为困难，振荡器内部存在的设计缺陷也会导致信号的漂移，降低 TRNG 的吞吐量。

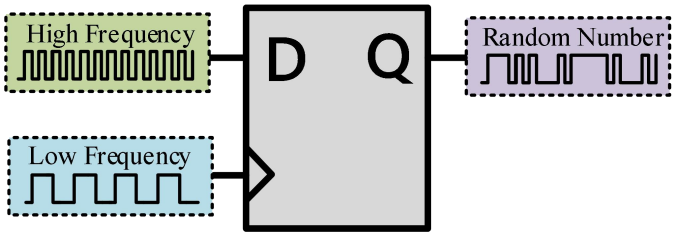

图 3-1 经典耦合振荡器电路结构图

为提高 TRNG 的吞吐量，异或门能加快抖动累积速率的特性被学者们广泛研究。如图 3-2 所示，异或门是一种常见的逻辑门电路，用于实现“异或”运算。由表 3-1 所示的异或门的真值表可以看出，异或运算对脉冲的变化很敏感，即任一输入信号电平发生变化时，输出信号也会随之改变，而振荡器的时钟抖动就发生在脉冲的跳变沿。

表 3-1 异或门的真值表

U1	U2	Y
0	0	0
0	1	1
1	0	1
1	1	0

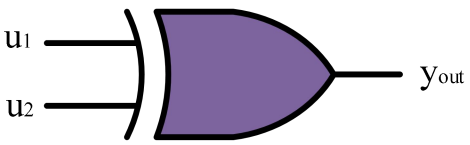

图 3-2 异或门符号

加大拿滑铁卢大学的 Sunar[46]教授团队提出了一种如图 3-3 所示的经典的基于 RO 的 TRNG 设计，即利用异或二叉树来结合多个 RO 的输出，目的是为了

让抖动的过渡区域铺满整个频谱，从而增强随机性。此设计的硬件开销极大，使用 114 个 13 级的 RO 且接入了后处理电路（BCH 码后处理），最终仅实现了 2.5Mbps 的低吞吐量。

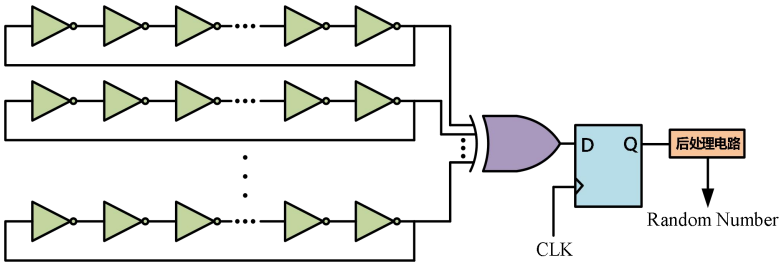

图 3-3 先异或再采样

挪威科技大学的 Wold[47]教授团队对 Sunar 的设计方案进行改良：先利用 D 触发器对 RO 的输出进行采样，使异或树的输入端信号同步，再将采样后的结果进行异或。这种做法可避免大量的异或门输出转换被抑制，将吞吐量提高到 100Mbps（提升了 40 倍），但仍然具有较高的硬件开销（使用了 50 个 3 级 RO）。

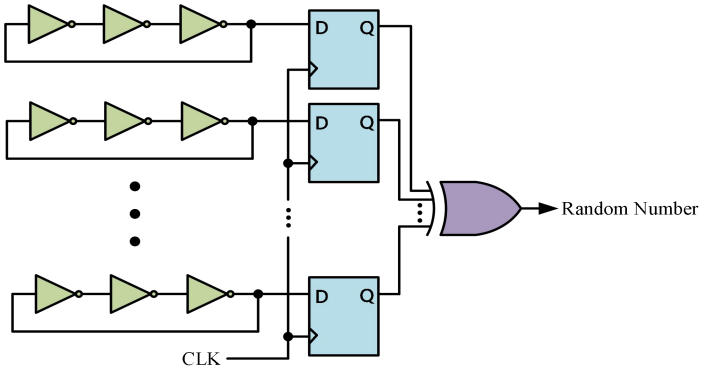

图 3-4 先异或再采样

在文献[45]中，设计出了如图 3-5 和图 3-6 所示的斐波那契环形振荡器（Fibonacci Ring Oscillator, FIRO）和伽罗瓦环形振荡器（Galois Ring Oscillator, GARO）。基于 FIRO 或 GARO 的 TRNG 设计，解决了传统 TRNG 随机性累积效率低下的问题，显著地提升了吞吐量。它的设计思路是利用异或门可以加快抖动的累积速率的特点，在反相器链中嵌入异或门，产生高频且稳定的振荡信号，能在单位时间内产生更多的振荡周期。

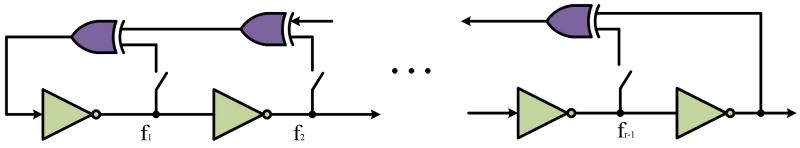

图 3-5 斐波那契环形振荡器

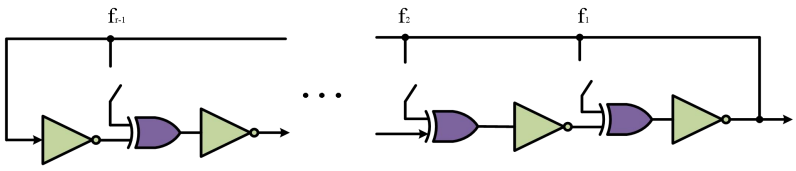

图 3-6 伽罗瓦环形振荡器

在文献[52]中，设计出了如图 3-6 所示的链式振荡环。它具有轻量级且高速率的特点，为 TRNG 在资源与吞吐量之间的权衡问题提供了一个优秀的解决方案。它的设计思路是通过异或门将相邻的 RO 进行连接，扩大 RO 中的抖动范围，实现了混合的多频率振荡信号。

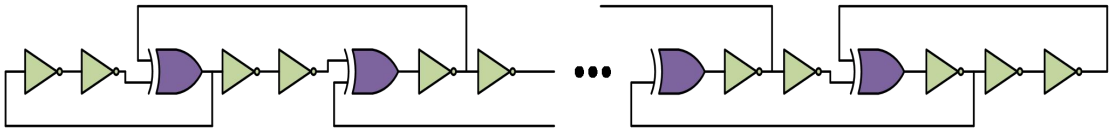

图 3-7 链式振荡环电路图

上述基于异或门的 TRNG 均未能考虑到“短脉冲抑制”的影响，此类 TRNG 设计往往由于其复杂的反馈结构，使得 TRNG 的随机性在电路传递和转换的过程中受到一定程度上的损失，产生具有伪随机性的振荡行为，TRNG 的输出具有周期性。这些周期性的产生与异或门对短脉冲的响应密不可分，本文将在下一节中详细介绍异或门的短脉冲抑制效应及其危害。

3.2 短脉冲抑制效应

3.2.1 异或门的数学模型与短脉冲抑制

文献[10]表明，异或门的数学模型可以建模为公式(3-1)所示的微分方程：

$$\tau \frac{dy_{out}(t)}{dt} = -y_{out}(t) + U_1(t) \oplus U_2(t) \tag{3-1}$$

经过量化之后的电压由公式(2)和公式(3)所表示：

$$Y_{out}(t) = \begin{cases} 1, y_{out}(t) > y_{th} \\ 0, y_{out}(t) < y_{th} \end{cases} \tag{3-2}$$

$$U_i(t) = \begin{cases} 1, u_i(t) > u_{th} \\ 0, u_i(t) < u_{th} \end{cases} \quad i = 1,2 \tag{3-3}$$

其中，τ为异或门响应特性参数，$u_1(t)$、$u_2(t)$为异或门的两个输入信号，$y_{out}(t)$为异或门的输出信号，u_{th}和y_{th}分别对应输入信号与输出信号的量化阈值电压，$U_1(t)$和$U_2(t)$为量化后的输入信号，$Y_{out}(t)$为量化后的输出信号。

基于以上数学模型，图 3-8 展示了异或门面对不同宽度的输入脉冲的输出响应图。如图(a)所示，当$u_1(t)$的输入脉冲足够宽，即高电平持续时间足够长时，异或门的输出信号$y_{out}(t)$可以完全响应为高电平，其中t_{pd}为器件的输入输出响应延迟；当$u_1(t)$的输入脉冲较窄时，异或门的输出信号$y_{out}(t)$不会完全响应为高电平，输出可能会产生“毛刺”；如图(c)所示，当$u_1(t)$的输入脉冲极窄时，即高电平持续时间短于或相当于门延迟t_{pd}，则导致异或门的输出信号$y_{out}(t)$不足以高于量化电压阈值，出现了非正确的响应，$U_1(t)$表现为低电平‘0’，这种现象被称之为“短脉冲抑制”。

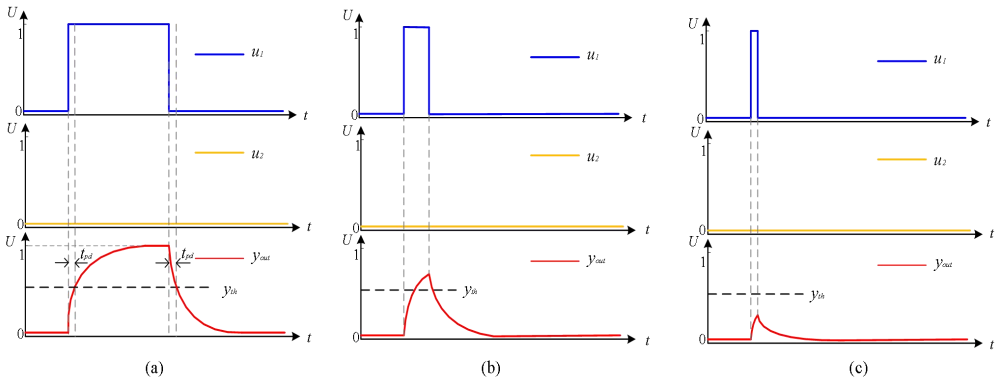

图 3-8 异或门对不同脉冲宽度的响应

3.2.2 短脉冲效应的危害

由于短脉冲抑制效应的存在，加大拿滑铁卢大学的 Sunar 教授团队提出的利用二叉异或树来组合多个振荡器的方案存在着大量的输出转换被抵消，文献[68]针对这一现象进行了 SPICE 仿真，实验结果表明：对测试的所有不同长度的 RO，均有 87%的转换在异或树中丢失。类似的，在文献[69]中，针对如图 3-9 所示的反馈多项式为$f(x) = x^7 + x^4 + x^2 + 1$ 的 FIRO，进行了 HSPICE 仿真实验，结果如图 3-10 所示。

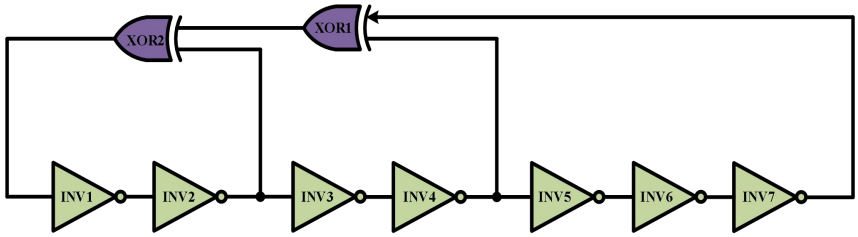

图 3-9 FIRO 电路结构图

由图 3-10 可以看出，异或门对短脉冲的响应在 FIRO 电路中不断地被削弱，直至低于量化阈值电压V_{th}时，短脉冲完全消失，此后的 FIRO 电路输出呈现出周期性（伪随机）的交替振荡。

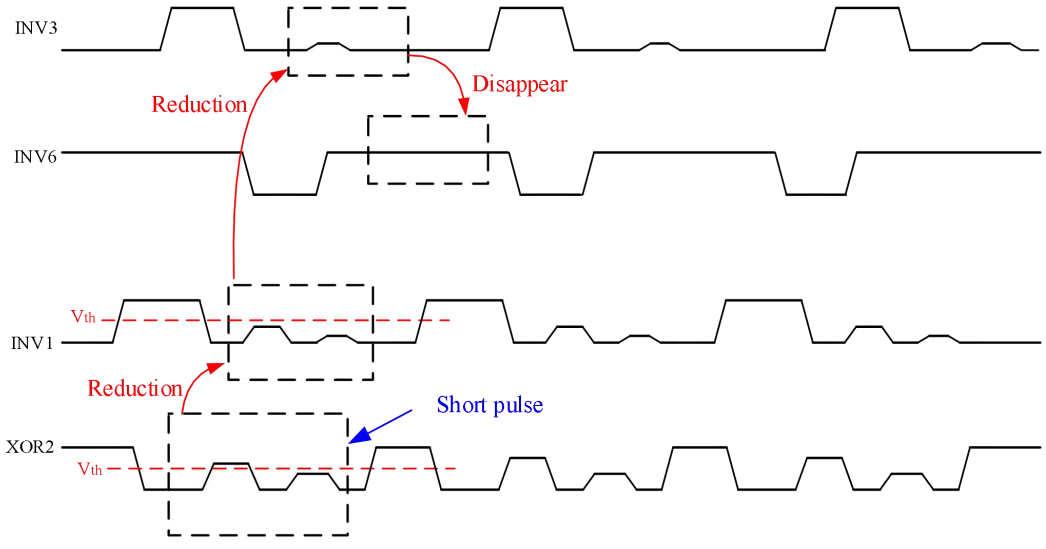

图 3-10 FIRO 电路 HSPICE 仿真图

对于短脉冲本身而言，经过异或门处理后，它是否能完全响应、是否产生毛刺以及是否被抑制，都是不确定的。因为在 TRNG 设计中，异或门处理的脉冲往往都包含了随机的相位抖动。但由于逻辑器件内部含有寄生电容，它的低通滤波特性会导致短脉冲所存在的随机性随着电路的传递逐步丧失，即只要环路足够长，异或门对短脉冲的响应都会被削弱到阈值电压以下。因此，将异或门以反馈的形式嵌入反相器链中的 TRNG 设计，都会降低短脉冲本身所具有的随机性，降低 TRNG 的熵。

3.3 多异或门耦合单元

3.3.1 CMX-cell 的设计思路

全数字 TRNG 通常是基于 FPGA 平台来进行设计的，但由于其资源的限制，使得 TRNG 的吞吐量难以提升，吞吐量和硬件开销之间存在直接矛盾。为解决 TRNG 吞吐量和硬件开销难以权衡的问题，许多学者研究了异或门可以加快抖动累积速率的特性，并由此设计出了很多的 TRNG。此类 TRNG 的设计将异或门嵌入反相器链中，并具有复杂的反馈结构。同时，由于逻辑器件的低通滤波特性，短脉冲经过异或门的输出会逐步被抑制，短脉冲本身的随机性也会随之不断丧失，TRNG 的输出甚至有进入周期振荡的风险。

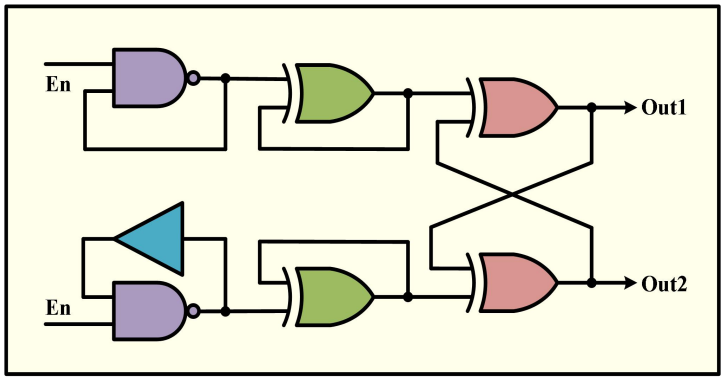

图 3-11 多异或门耦合单元电路图

为了克服短脉冲随机性丧失的问题，本文提出了如图 3-11 所示的多异或门耦合单元（Coupling Multiple XOR gate cells, CMX-cell），旨在将 RO 与异或门分离，杜绝短脉冲在电路传递时被除了异或门之外的逻辑器件滤波，将短脉冲本身的随机性（受抖动影响）尽可能保留下来。同时，该耦合单元中的多个异或门耦合组成了独立的反馈结构（与反相器链隔离），加快抖动的累积速率，进一步提升了 TRNG 的吞吐量，最终的设计以极低的硬件开销代价（31 个查找表和 8 个 D 触发器）在 Xilinx Virtex-7 FPGA 开发板上实现了高达 500Mbps 的吞吐量。

3.3.2 CMX-cell 的工作原理

CMX-cell 由上下两条的路径组成，电路结构的运行可分为三个阶段：

（1）初始抖动累积阶段：上路径是由一个与非门构建的一级 RO，下路径是由与非门和一个缓冲器构建而成。由公式(3-4)和公式(3-5)可知，RO 的级数 N

与其周期 T 成正比、振荡频率 f 成反比。因此，一级 RO 具有最快的振荡频率。其中，t_d为反相器的延迟。

$$T = 2 \cdot N \cdot t_d \tag{3-4}$$

$$f = \frac{1}{T} = \frac{1}{2 \cdot N \cdot t_d} \tag{3-5}$$

公式(3-6)和公式(3-7)展示了上路径 RO 的振荡周期（记为T_1）和下路径 RO 的振荡周期（记为T_2），其中 t_d^{inV} 和 t_d^{Buffer} 分别为反相器延迟和缓冲器延迟。

$$T_1 = 2t_d^{inV} \tag{3-6}$$

$$T_2 = 2(t_d^{inV} + t_d^{Buffer}) \tag{3-7}$$

由公式可知，由于下路径的 RO 比上路径多了一个缓冲器，使得上、下路径的 RO 振荡周期相差了近两倍的缓冲器延迟。因此，当使能端上电之后，上、下路径的 RO 所产生的高速输出脉冲存在着频率上的差异。这种不同振荡频率的 RO 可以避免因“频率互锁”现象而出现输出序列之间相关性，因此无需刻意分散 RO 在 FPGA 开发板上的布局位置。

（2）单异或门抖动增强阶段：前一个阶段，上、下路径 RO 的输出中含有丰富的相位抖动，原因是它们的高频振荡。由第二章所介绍的短脉冲抑制效应可知，短脉冲本身的随机性与异或门的输入脉冲宽度具有直接关系，而脉冲宽度一定程度上又受到了抖动的影响。而在这一阶段，将一级 RO 的输出，连接到独立构成环路的异或门 XOR1 和异或门 XOR2 的输入端口。这种高频的脉冲注入到异或门，更容易和异或门的输出反馈信号之间产生短脉冲。高速的短脉冲信号通过异或门，不仅能够加快抖动的累积速度、扩大抖动区域，还能为异或门的输出提供短脉冲的随机性，增加熵的来源。

（3）双异或门交叉耦合阶段：在此阶段，注入到交叉耦合的异或门内的脉冲，已通过单个独立成环的异或门加强了 RO 抖动的累积，并且所含有的短脉冲尚未被其他逻辑门元件（除异或门之外的逻辑门）削弱。因此，这种具有抖动增强的、短脉冲随机性未丧失的高速信号，注入到双异或门交叉耦合的电路之后，仍然会因异或门短脉冲抑制效应来继续产生随机性，并且异或门 XOR3 和异或门 XOR4 本身仍可以加快抖动的累积速度。与上个阶段类似，短脉冲通过异或门之后的输出电压不会被其他逻辑器件滤波而造成多余的损失。

对于异或门，当某一个输入端为高电平‘1’，其输出与另一端输入的逻辑关系为“取反”，此时异或门表征为反相器；当一个输入端为低电平‘0’，其输出与另一端输入的逻辑关系为“保持”，此时异或门表征为缓冲器。在文献[60]中，提出通过开关元件来改变环路内反相器数量的方法来实现亚稳态。换言之，当 RO 内反相器数目由奇数切换为偶数时，RO 的工作模式由振荡切换为保持，强制 RO 停止振荡。在这一时刻，RO 的输出会出现在“取反”和“保持”之间

的“逻辑冲突”，电位会介于‘0’和‘1’之间。由于内部热噪声的存在，电位最终会随机地稳定为‘0’或‘1’。而当 RO 内反相器数目由偶数切换为奇数时，与上述情况相似，RO 的工作模式由保持切换为振荡，即 RO 起振。接下来本文对双异或门耦合单元进行时序分析，其工作模式如下：

1)当$Y_1 = Y_2 = 1$ 时，此时两个异或门同时表征为反相器，交叉耦合单元相当于一个 SRAM 单元，此时无熵源为 TRNG 提供随机性；

2)当$Y_1 = Y_2 = 0$ 时，此时两个异或门同时表征为缓冲器，交叉耦合单元相当于一根成环的导线，此时无熵源为 TRNG 提供随机性；

3)当$Y_1 = \overline{Y_2}$时，此时两个异或门一个表征为反相器，一个表征为缓冲器，交叉耦合单元相当于一个 1 级 RO，此时熵源为抖动；

4)当$Y_1 = 0$ 且Y_2为上升沿或$Y_2 = 0$ 且Y_1为上升沿时，此时一个异或门表征为缓冲器，另一个异或门由缓冲器切换为反相器，交叉耦合单元相当于 RO 的反相器个数由偶数切换为奇数，RO 起振，此时熵源为亚稳态；

5)当$Y_1 = 0$ 且Y_2为下升沿或$Y_2 = 0$ 且Y_1为下升沿时，此时一个异或门表征为缓冲器，另一个异或门由反相器切换为缓冲器，交叉耦合单元相当于 RO 的反相器个数由奇数切换为偶数，强制 RO 停止振荡，此时熵源为亚稳态；

6)当$Y_1 = 1$ 且Y_2为上升沿或$Y_2 = 1$ 且Y_1为上升沿时，此时一个异或门表征为反相器，另一个异或门由缓冲器切换为反相器，交叉耦合单元相当于 RO 的反相器个数由奇数切换为偶数，强制 RO 停止振荡，此时熵源为亚稳态；

7)当$Y_1 = 1$ 且Y_2为下升沿或$Y_2 = 1$ 且Y_1为下升沿时，此时一个异或门表征为反相器，另一个异或门由反相器切换为缓冲器，交叉耦合单元相当于 RO 的反相器个数由偶数切换为奇数，RO 起振，此时熵源为亚稳态。

综上所述，CMX-cell 利用异或门的特性，将短脉冲作为抖动和亚稳态这两种不同熵源的之间的桥梁，将二者有机地结合起来。具体来说，异或门将高频的 RO 输出中的抖动不断积累，单个独立成环的异或门源源不断地响应高速的短脉冲信号。高速短脉冲信号经过异或门处理后，再作用在交叉耦合的异或门环路内，可在一定条件下触发电路的亚稳态行为，并且累积的抖动也为异或门环路的不同工作模式之间的切换注入了随机性。

3.3.3 CMX-cell 的行为模型

对于单个独立成环的异或门，采用在相关工作中微分方程的数学模型来描述异或门的行为，如公式(8)和公式(9)所示。图 3-12 为对应节点的信号标记图。

$$\tau_1 \frac{dy_1(t)}{dt} = -y_1(t) + I_1(t) \oplus Y_1(t - \tau_{1,1}) \tag{3-8}$$

$$\tau_2 \frac{dy_2(t)}{dt} = -y_2(t) + I_2(t) \oplus Y_2(t - \tau_{2,2}) \tag{3-9}$$

经过量化之后的电压由公式(3-10)和公式(3-11)所表示：

$$Y_i(t)=\begin{cases}1, y_i(t)>y_{th}\\ 0, y_i(t)<y_{th}\end{cases}\ i=1,2 \tag{3-10}$$

$$I_i(t)=\begin{cases}1, i_i(t)>i_{th}\\ 0, i_i(t)<i_{th}\end{cases}\ i=1,2 \tag{3-11}$$

其中，τ_1、τ_2为异或门 XOR1 和异或门 XOR2 的响应特性参数，$\tau_{1,1}$是异或门 XOR1 反馈传输延迟，$\tau_{2,2}$是异或门 XOR2 反馈传输延迟，$i_1(t)$、$i_2(t)$为异或门的 XOR1 和异或门 XOR2 的输入信号，$y_1(t)$、$y_2(t)$为异或门的 XOR1 和异或门 XOR2 的输出信号，i_{th}和y_{th}分别对应输入信号与输出信号的量化阈值电压，$I_1(t)$和$I_2(t)$为量化后异或门 XOR1 和异或门 XOR2 的输入信号，$Y_1(t)$和$Y_2(t)$为量化后异或门 XOR1 和异或门 XOR2 的输出信号。

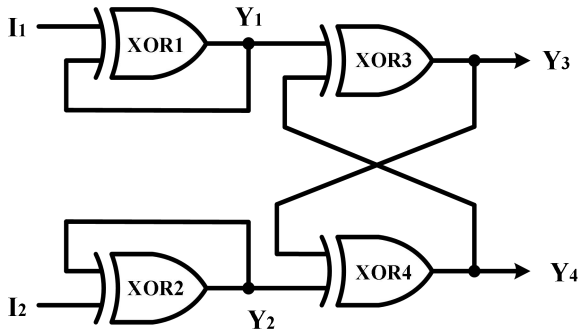

图 3-12 异或门的信号节点标记图

对于双异或门的交叉耦合结构，同理采用在相关工作中微分方程的数学模型来描述异或门的行为，如公式(3-12)和公式(3-13)所示：

$$\tau_3\frac{dy_3(t)}{dt}=-y_3(t)+Y_1(t-\tau_{1,3})\oplus Y_4(t-\tau_{4,3}) \tag{3-12}$$

$$\tau_4\frac{dy_4(t)}{dt}=-y_4(t)+Y_2(t-\tau_{2,4})\oplus Y_3(t-\tau_{3,4}) \tag{3-13}$$

经过量化之后的电压由公式(3-14)表示：

$$Y_i(t)=\begin{cases}1, y_i(t)>y_{th}\\ 0, y_i(t)<y_{th}\end{cases}\ i=1,2,3,4 \tag{3-14}$$

其中，τ_3、τ_4为异或门 XOR3 和异或门 XOR4 的响应特性参数，$\tau_{1,3}$是异或门 XOR1 的输出传递到异或门 XOR3 的传输延迟，$\tau_{2,4}$是异或门 XOR2 的输出传递到异或门 XOR4 的传输延迟，$\tau_{3,4}$是异或门 XOR3 的输出反馈到异或门 XOR4 的输入的传输延迟，$\tau_{4,3}$是异或门 XOR4 的输出反馈到异或门 XOR3 的输入的传输延迟，$y_1(t)$、$y_2(t)$为异或门的 XOR3 和异或门 XOR4 的输入信号，$y_3(t)$、$y_4(t)$为异或门的 XOR3 和异或门 XOR4 的输出信号，y_{th}为对应信号的量化阈值电压，$Y_1(t)$和$Y_2(t)$为量化后异或门 XOR3 和异或门 XOR4 的输入信号，$Y_3(t)$和$Y_4(t)$为量化后异或门 XOR3 和异或门 XOR4 的输出信号。

3.3.4 基于 CMX-cell 的 TRNG 的硬件实现

在实际进行电路设计的过程中，不难发现，单凭一个 CMX-cell 无法通过统计测试，因为它的偏置过大，不能提供足够的熵。传统的处理方法是要采用一些后处理技术，以牺牲吞吐量和硬件开销的代价以确保输出序列通过统计测试。但本文为了克服后处理电路的吞吐量损耗并且让设计的 TRNG 通过统计测试，采用了异或组合技术，将 4 个 CMX-cell 经过采样后进行异或处理。

基于多异或门耦合单元的真随机数发生器的完整结构如图 3-13 所示，具体的电路实现分为熵源电路、采样环节和异或树三个部分。其中熵源电路部分共采用了 4 个 CMX-cell，采样环节分别利用 D 触发器将每个 CMX-cell 的两个输出捕获并采样，采样的时钟频率可配置为 500 MHz，最后利用异或组合技术将采样到的数据进行消除偏置的处理。

本文以 Vivado 作为实验平台，在 A7 和 V7 开发板上均实现了如图 3-13 所示的基于多异或门耦合单元的 TRNG。由图 3-11 可知，每个 CMX-cell 都由 1 个缓冲器、2 个与非门和 4 个异或门组成。通过 Vivado 软件实例化的硬件原语，将所有的逻辑门均采用查找表实现。因此，每个 CMX-cell 都消耗了 7 个查找表。此外，异或二叉树共消耗了 3 个查找表，采样环节共消耗了 8 个触发器。因此，基于多异或门耦合单元的 TRNG 设计共消耗了 31 个 LUTs 和 8 个 FFs，达到了轻量级的 FPGA 实现。

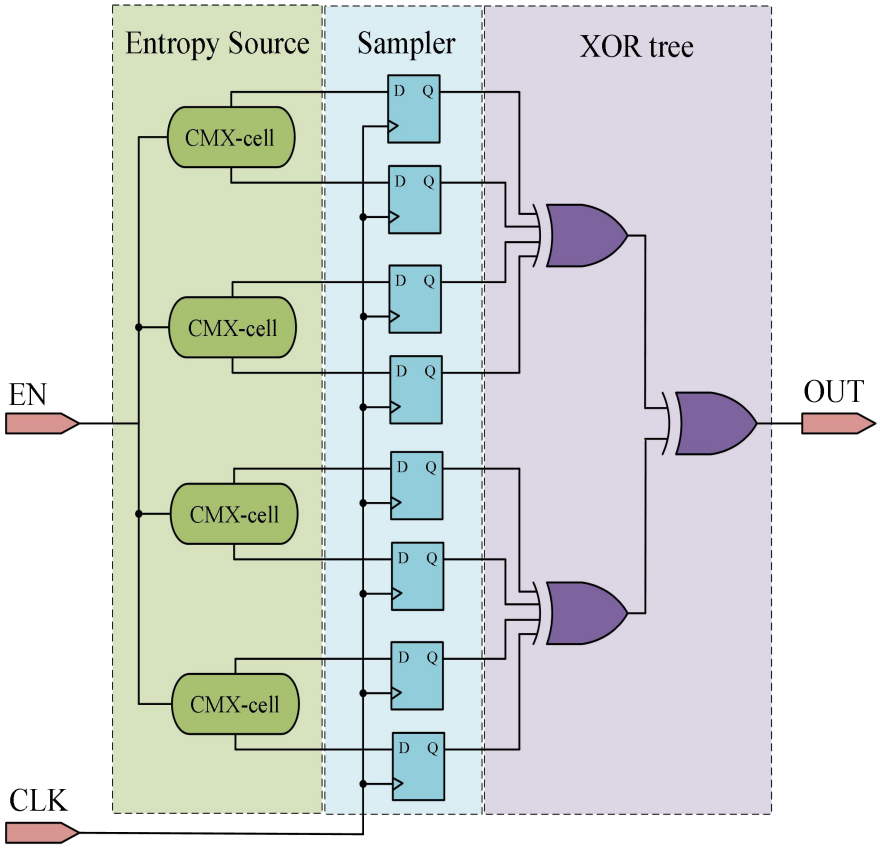

图 3-13 基于多异或门耦合单元的 TRNG 电路图

3.4 本章小结

本章先介绍了常见的基于抖动的 TRNG 设计，引出异或门在提升 TRNG 的吞吐量方面的巨大作用。再深入介绍了两种经典的基于异或门的 TRNG 电路，并指出它们的不足，即没有考虑到短脉冲抑制效应的影响。接着展开了对短脉冲抑制效应的介绍，阐述了异或门的数学模型、短脉冲抑制的形成机理以及它的危害。最后采用将反相器链与异或门分离的方法，提出了多异或门耦合单元，可以最大程度上减弱短脉冲在数字元件的传播中的滤波现象，并且结合了短脉冲本身的随机性来对上下两条路径的使能 RO 中的抖动进行叠加，增强了 TRNG 的熵。此外，本章详细解释了 CMX-cell 的设计思路和工作原理，并且通过异或门的行为模型对 CMX-cell 进行数学建模，再次论证了其结构原理。还描述了基于 CMX-cell 的 TRNG 的硬件实现，采用了异或组合技术来提升 TRNG 的香农熵。最终仅消耗 31 个查找表和 8 个触发器，达到了 500Mbps 的吞吐量，为基于抖动的 TRNG 提供了一种轻量级的高吞吐量 TRNG 的实现方案。

第 4 章 基于亚稳态叠加单元的 TRNG

4.1 基于亚稳态的真随机数发生器

数字电路中的亚稳态现象产生的原因是由于触发器不能在规定的时间窗口内输出一个稳定的状态，即如图 4-1 所示的触发器建立时间和保持时间违规。如果触发器在建立时间和保持时间内进行数据更新（采样脉冲刚好在时间窗口内发生跳变），触发器将会采样到一个介于高电平‘1’和低电平‘0’之间的值，此时触发器内部晶体管尚未处在饱和区对应的高、低电位，而是在一个中间电位之间振荡。由于电路内部热噪声的影响，触发器最终将会输出一个稳定的电平。当一个电路发生亚稳态时，最终稳定电平的高低和亚稳态的持续时间（决断时间）都是不可预测且具备高度随机性的，前者常被用作 TRNG 的熵源。

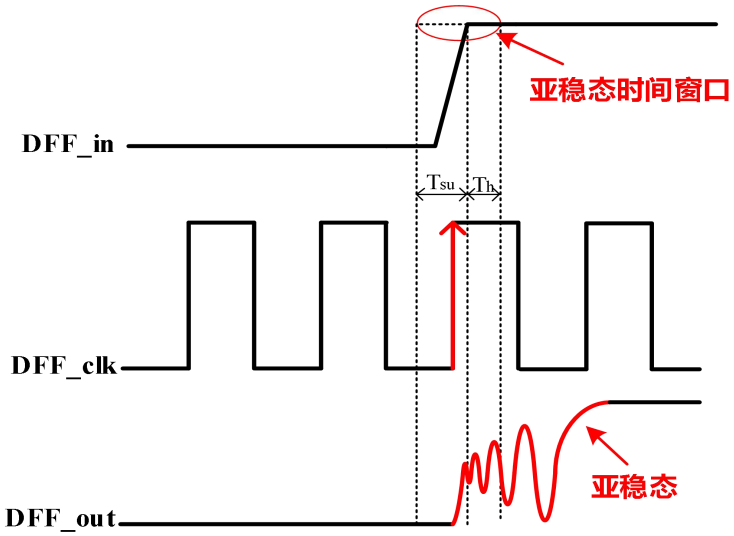

图 4-1 触发器中的亚稳态现象

如何能够精准的控制延时，强制使得 D 触发器的建立时间和保持时间时序行为违规（保证数据输入端和采样脉冲几乎同时发生跳变）是设计基于触发器采样的亚稳态 TRNG 的关键所在。因此，学术界涌现出了许多精准控制延时的方法来设计基于触发器采样的 TRNG，如利用精细延时链[70]、可编程延时线（Programmable Delay Line, PDL）[57]以及数字时钟管理器[71]调节 D 触发器的信号延时。但是这些方法无一例外都需要制定严格的布局布线来抵消电路内部的局部失配，还需要进行复杂的延时校准工作，导致此类 TRNG 的可移植性差。为了解决这一问题，基于临近亚稳态的 TRNG[59]被提出。它不需要繁琐的路由策略，而是在工作在临近亚稳态点，通过仲裁两个相同亚稳态电路的决断时间来量化随机性。但这种做法需要加入复杂的额外电路（后处理电路和熵提取电路），带来了巨大的硬件开销。

4.2 组合逻辑电路中实现亚稳态的方法

4.2.1 经典的亚稳态电路模型

除了触发器的时序违规能产生亚稳态，如图 4-2 所示的双稳态电路模型也可以产生亚稳态。当时钟信号（Clock Sinal, CLK）的上升沿到来之前，开关键 K1 闭合、K2 断开。此时反馈环路尚未形成，数据端 D 输入高电平，经反相器 inv1 作用，U_Q和$U_{\bar{Q}}$均表现为低电平；当 CLK 脉冲的上升沿到来的瞬间，开关键 K1 断开，K2 闭合，此时反馈环路形成，由于反相器 inv2 的作用，U_Q应当为高电平。在这一时刻，Q 的电位会介于高电位和低电位之间，从而进入亚稳态点。幸运的是，由于电路内部的热噪声的存在，亚稳态点将会随机地移动到某一个稳定的状态——逻辑‘0’或逻辑‘1’。基于这一电路模型的理论基础，可以使用多路选择器和异或门作为开关元件来改变 RO 中反相器数量。当 RO 中反相器数目由奇数切换为偶数，这会强制 RO 停止振荡。假设 RO 上一个状态的输出为‘0’，RO 输出应当为上一个状态的取反，即为‘1’。但由于振荡的停止，强制使输出保持为上一个状态的输出‘0’。此时，RO 的输出产生了“逻辑冲突”，即电路进入亚稳态。

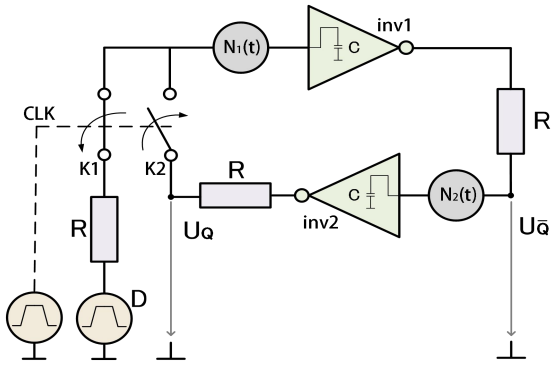

图 4-2 一种经典的双稳态电路模型

4.2.2 基于 MUX 的亚稳态 TRNG

文献[60]使用了两个 MUX 作为开关元件来进行振荡环路的切换。如图 4-3 所示，当 Clear 端表现为低电平，若此时 S 端口为逻辑‘0’，电路表现为两个独立振荡的 1 级 RO；若此时 S 端口为逻辑‘1’，电路表现为一个含有两个反相器的存储单元。因此，在 S 端口输入为上升沿时，强制 RO 停止振荡，电路进入了亚稳态。

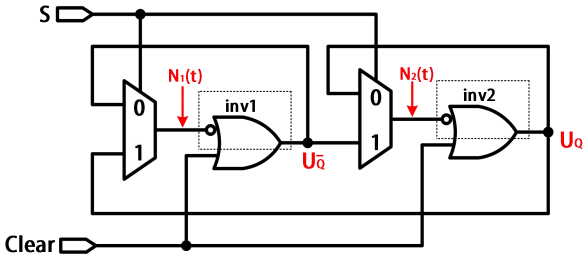

图 4-3 一种基于 MUX 的亚稳态电路

4.2.3 基于异或门的亚稳态 TRNG

如图 4-4 所示，将异或门的其中一个输入端口接入脉冲，当输入脉冲为高电平时，异或门的输出与另一输入端口的逻辑值相反，异或门表征为反相器；当输入脉冲为低电平时，异或门的输出与另一输入端口的逻辑值相同，表征为缓冲器。所以，异或门和 MUX 具有相同的“开关特性”，即通过外部脉冲的控制，不断改变 RO 内所表征的反相器数量。

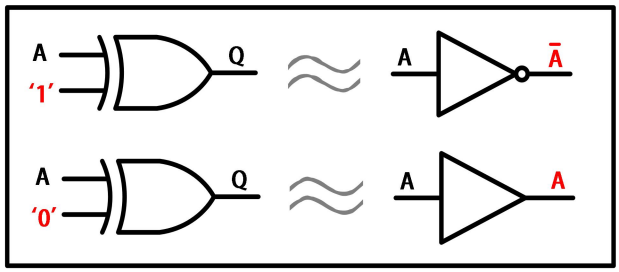

图 4-4 异或门的开关特性

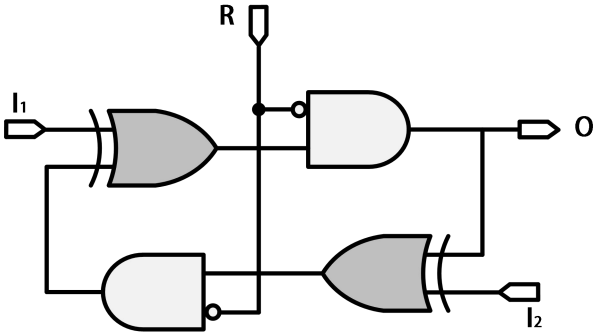

图 4-5 一种基于 MUX 的亚稳态电路

文献[63]使用了两个异或门来改变环路所表征的反相器个数。如图 4-5 所示，当 R 端表现为高电平，若此时 I1 端与 I2 端的输入不匹配，则环路中相当于接入一个反相器，RO 振荡；若此时 I1 端与 I2 端输入匹配，则环路中相当于接入两个（或零个）反相器，表现为存储单元，振荡停止。因此，在 I1 端和 I2 端的输入由不匹配切换为匹配时，电路进入了亚稳态。

综上可以看出，利用异或门和利用 MUX 产生亚稳态的原理上并无区别，它们只是利用切换 RO 内反相器数量的思想来实现亚稳态电路的两种不同的方案。

4.3 亚稳态叠加单元

4.3.1 MS-cell 的设计思路

基于亚稳态的 TRNG 通常对设计的要求很高，设计出的 TRNG 结构的偏置、硬件开销、吞吐量等性能指标，有着不同程度的恶化。利用 D 触发器采样的亚稳态 TRNG 设计需要考虑到繁琐的路由策略，对布局布线的要求十分严格，其吞吐量也会因此受到限制。即便是对路由不敏感的临近亚稳态 TRNG 设计，也需要加入相当复杂的额外电路，如熵提取电路和后处理电路，这也大大增加了面积开销，背离了轻量级设计的初衷。

针对上述存在的问题，本文提出了基于反馈 MUX 的亚稳态叠加的 TRNG 设计，实现了高吞吐量 TRNG 的轻量级实现。该 TRNG 结构基于一种如图 4-6 所示的新型的结构模块——亚稳态叠加单元。MS-cell 具有反馈的电路结构，通过两个级数不同的 RO 来进行环路的切换，能够结合抖动和亚稳态两种熵源。它可以在一定的条件下将 MUX 触发的亚稳态与异或门触发的亚稳态进行叠加，显著提高 TRNG 的吞吐量。

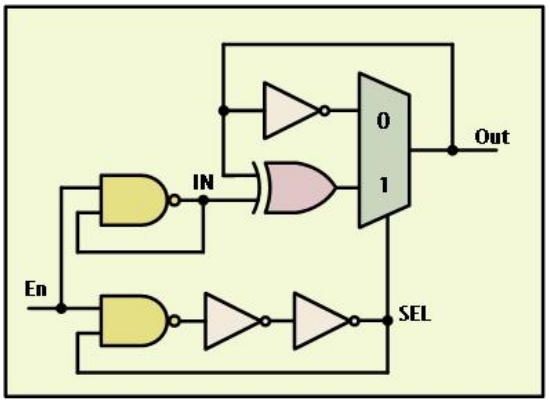

图 4-6 亚稳态叠加单元电路图

4.3.2 MS-cell 的工作原理

MS-cell 是属于自由运行的结构模块，它受到 1 级 RO（脉冲 IN）和 3 级 RO（脉冲 SEL）的控制。从图 4-7 可知，输入脉冲的跳变沿是 MUX 和异或门进入亚稳态的条件，这使得 MS-cell 会由于 RO 输出脉冲的状态（高、低电平或上升、下降沿）从而进入熵源不同的工作模式。因此，需要对 MS-cell 作如下的简单的时序分析：

1)当 SEL 脉冲处于下降沿或低电平时，MUX 选通 IN0 口；此时不论 IN 脉冲是何种状态，MS-cell 表征为由反相器构成的 1 级 RO，熵源为反相器构成 RO 中的抖动。

2)当 SEL 脉冲处于上升沿时，MUX 将选通 IN1 口；若此时 IN 脉冲恰好处于下降沿，异或门将表征为缓冲器，强制将两种由不同器件形成的振荡停止，使得 MS-cell 同时触发了两种亚稳态，熵源为 MUX 和异或门触发的亚稳态的叠加。

3)当 SEL 脉冲处于上升沿时，MUX 将选通 IN1 口；若此时 IN 脉冲处于低电平，异或门已表征为缓冲器。MS-cell 表征为如图 6(a)所示的亚稳态模型，熵源仅源于 MUX 触发的亚稳态。

4)当 SEL 脉冲处于上升沿或高电平时，MUX 选通 IN1 口；若此时 IN 脉冲处于上升沿或高电平，异或门表征为反相器，MS-cell 表征为由异或门构成的 1 级 RO，熵源为异或门构成 RO 中的抖动。

5)当 SEL 脉冲处于高电平时，MUX 已选通 IN1 口；若此时 IN 脉冲处于下降沿，异或门将表征为缓冲器，从而使得振荡停止。MS-cell 表征为图 6(b)所示的亚稳态模型，熵源仅源于异或门触发的亚稳态。

6)当 SEL 脉冲处于高电平时，MUX 已选通 IN1 口；若此时 IN 脉冲处于低电平，异或门已表征为缓冲器。这时的 MS-cell 表征为由一个缓冲器构成的环形电路，无熵源为其提供随机性，仅维持上一个工作模式的电路状态。

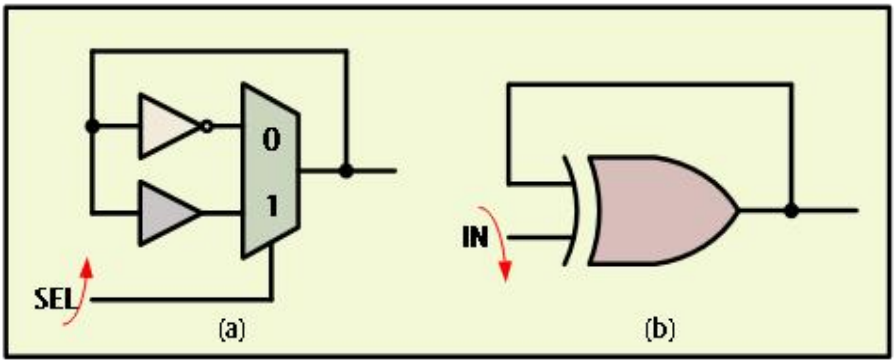

图 4-7 两种数字元件引导的亚稳态

表 4-1 更为详细地枚举出了 SEL 脉冲和 IN 脉冲不同的电路状态对应 MS-cell 的工作模式。不允许被忽视的是，当 SEL=1 且 IN=0 时，MS-cell 处于无熵源的“保持”状态。这对设计出的 TRNG 的威胁极大，因为这会导致输出序列中会含有连续的‘0’或‘1’。为此，MS-cell 设置了 1 级 RO 的输出作为 IN 脉冲，目的是减少“保持”状态的持续时间。由表 4-1 可知，叠加 MUX 和异或门触发的亚稳态的条件近乎严苛。需要在 SEL 脉冲处于上升沿时，IN 脉冲恰好处于下降沿。如果两类脉冲的频率相近，势必要经过很长一段时间才能实现亚稳态的叠加，这也会导致某一工作模式的持续时间过长。因此，需要两类脉冲具有显著的频率上的差距，即一个快速的脉冲不断地追赶一个慢速的脉冲。

表 4-1 MS-cell 的工作模式

SEL 脉冲	IN 脉冲	熵源
↘	×	反相器触发的抖动
0	×	反相器触发的抖动
↗	↘	MUX 与异或门触发的亚稳
↗	0	MUX 触发的亚稳态
↗	↗	异或门触发的抖动
↗	1	异或门触发的抖动
1	↘	异或门触发的亚稳态
1	0	无熵源(保持)
1	↗	异或门触发的抖动
1	1	异或门触发的抖动

因此，为了更加高效地触发 MS-cell 的工作模式的切换，要求 SEL 脉冲的周期要大于 IN 脉冲的周期。环形振荡器的周期 T 如公式(4-1)所示

$$T = 2 \cdot N \cdot \tau \tag{4-1}$$

其中，N 表示为 RO 环中反相器的个数，τ 表示单个反相器的延时。显然，环形振荡器的周期与反相器个数成正比，这意味着提供给 SEL 脉冲的 RO 级数不能比提供给 IN 脉冲的 RO 级数小。同时，为了尽可能的缩减硬件开销，采用 3 级 RO 的输出作为 SEL 脉冲。值得一提的是，由于 MS-cell 的输入脉冲是由 RO 所提供的，而 RO 的输出本身就含有相位抖动，并随着时间不断积累(如图 4-8 所示)，这必然会在 MS-cell 工作模式切换的时候注入不确定性，也在一定程度上也增强了熵。

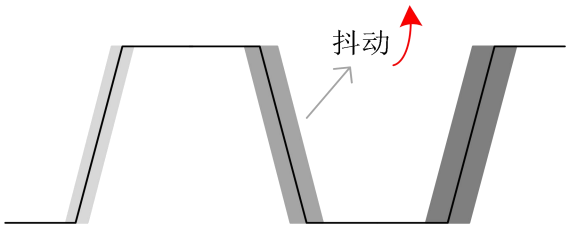

图 4-8 抖动的累积效应

4.3.3 基于 MS-cell 的 TRNG 的硬件实现

事实上，即便完成了上述设计，单个 MS-cell 仍然难以产生足够的熵来通过 NIST 测试。通常情况下，应当采用一些后处理技术，以牺牲吞吐量和增加硬件开销为代价来提高 TRNG 的熵。但本文的初衷是为了设计出高吞吐量的 TRNG，而且许多先进的 TRNG 都没有后处理电路。很多文献表明，异或不但可以提升抖动的累积速度，还能增加 TRNG 的香农熵[52]。为了克服后处理电路的吞吐量损耗并且让设计的 TRNG 通过统计测试，最终采用了异或组合技术，将 4 个 MS-cell 经过采样后进行异或处理。

基于亚稳态叠加单元的真随机数发生器的完整结构如图 4-9 所示，具体的电路实现分为熵源电路、采样环节和异或环节三个部分。其中熵源电路部分共采用了 4 个 MS-cell，采样环节分别利用 D 触发器将每个 MS-cell 的输出捕获并采样，采样的时钟频率可配置为 500 MHz，最后利用异或组合技术将采样到的数据进行消除偏置的处理。

本文以 Vivado 作为实验平台，在 A7 和 V7 开发板上均实现了如图 4-9 所示的基于亚稳态叠加单元的 TRNG。由图 4-6 可知，每个 MS-cell 都由 3 个反相器、2 个与非门、1 个多路复用器和 1 个异或门组成。通过 Vivado 软件实例化的硬件原语，将所有的逻辑门与 MUX 均采用查找表实现。因此，每个 MS-cell 单元都消耗了 7 个查找表。此外，异或环节消耗了 1 个查找表，采样环节共消耗了 4 个触发器。因此，基于多异或门耦合单元的 TRNG 设计共消耗了 29 个 LUTs 和 4 个 FFs，达到了轻量级的 FPGA 实现。

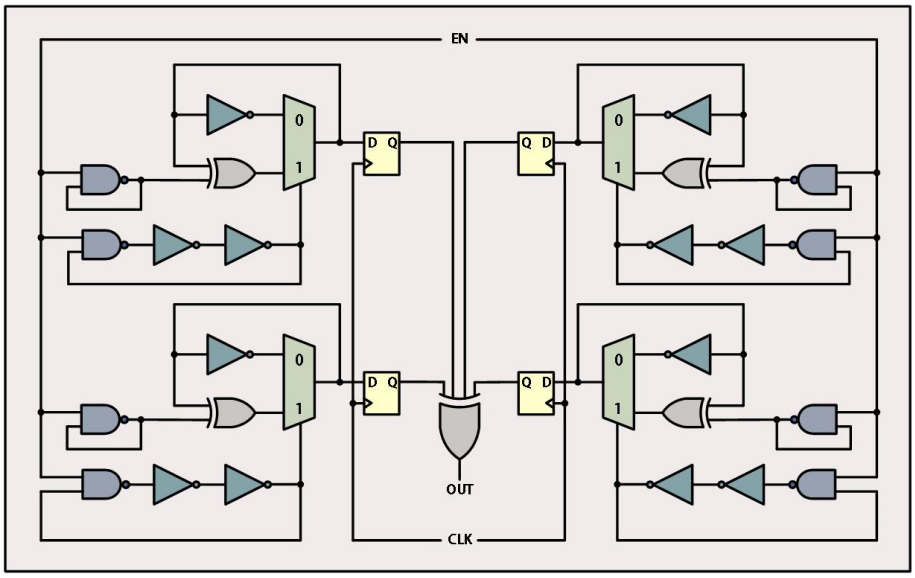

图 4-9 基于亚稳态叠加单元的 TRNG

4.4 本章小结

本章先介绍了基于触发器采样的亚稳态 TRNG 的设计要求，即需要对这类亚稳态电路的延时做到精细的调控以克服内部电路中存在的工艺偏差。接着阐述了采用精细延时链、可编程延时线和数字时钟管理器来对 D 触发器的延时进行调节的不足——均需要进行严格的布局布线且可移植性差，引导出以亚稳态的决断时间为熵源的临近亚稳态 TRNG。但此类亚稳态的吞吐量不高而且需要额外的后处理电路与熵提取电路，硬件开销巨大。

为解决亚稳态 TRNG 需要繁琐的路由、可移植性差的问题，本章深入探究了组合逻辑电路中的亚稳态电路。先介绍了经典的双稳态电路中的亚稳态现象，再分别介绍了基于 MUX 的亚稳态 TRNG 和基于异或门的亚稳态 TRNG。最后通过反馈设计的方法，提出了亚稳态叠加单元。它是将异或门嵌套进入 MUX 的一个输入，组成一个反馈环路，结合外部独立不同级数的 RO 中的抖动，随机地高效触发两类数字元件中的亚稳态，并将其叠加。还能够集成抖动和亚稳态两类熵源，大大提升 TRNG 的吞吐量。

此外，本章详细解释了 MS-cell 的设计思路和工作原理，讨论了反馈环路外部 RO 的级数的设置，低级数的 RO 可提供高频振荡脉冲作为内部反馈环路的使能，高效触发两类亚稳态的叠加，从理论上论证了该 TRNG 具备高吞吐量。还描述了基于 MS-cell 的 TRNG 的硬件实现，采用了异或组合技术来提升 TRNG 的香农熵。最终仅消耗 29 个查找表和 4 个触发器，达到了 500 Mbps 的吞吐量，为基于亚稳态的 TRNG 提供了一种轻量级且高吞吐量 TRNG 的实现方案。

第 5 章 实验方法与结果分析

5.1 实验方法

5.1.1 实验平台

本文以 FPGA 作为实验平台，通过编写特定的代码语言，对器件内部连接进行更改与配置，并设定逻辑单元功能，从而达成特定的设计目标。可配置逻辑模块（Configurable Logic Block，CLB）是 FPGA 中极为关键的硬件资源，它包含了设计 TRNG 所需的触发器、查找表、多路选择器以及进位链等元件。

在进行数字电路设计中，TRNG 的熵源电路往往涉及到组合逻辑电路的实现。设计者通过将各类逻辑门电路的真值表“逆写”（如图 5-1 所示）到查找表中，即可在 FPGA 中实现；再通过代码编程将各个逻辑组件连结起来，便可以完成对 TRNG 熵源电路的设计。TRNG 熵源电路的输出一般为 TRNG 采样电路的输入，TRNG 采样电路的另一输入为时钟输入，显然与时序逻辑电路的实现密不可分。设计者可以直接调用例化的 D 触发器代码（如图 5-2 所示），将 TRNG 采样电路与 TRNG 熵源电路和 TRNG 后处理电路进行相应的连结，即可通过硬件描述语言完成所有的 TRNG 数字电路的设计方案。

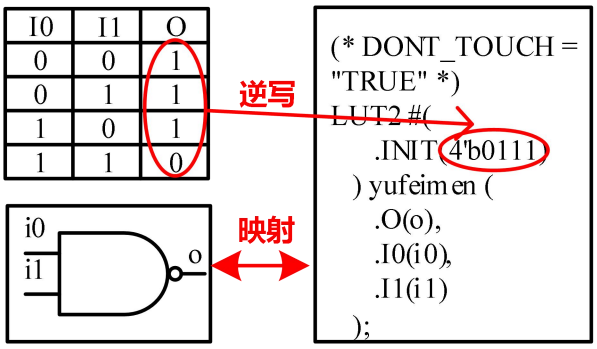

图 5-1 在 FPGA 中实现与非门

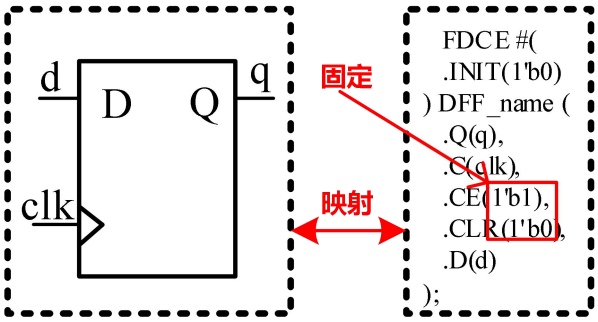

图 5-2 在 FPGA 中实现 D 触发器

本文采用的 FPGA 开发板为 Xilinx Virtex-7（如图 5-3 所示）和 Xilinx Artix-7（如图 5-4 所示），型号分别为 Xilinx xc7vx485tffg1761 和 Xilinx xc7a200tfbg484。

赛灵思 7 系列开发板相较于 6 系列开发板具有更为先进的工艺、更低的功耗、更强的运算能力等优势，并且可以和 Vivado 设计套件协同优化，其性能效果强于 6 系列开发板所依赖的 ISE 设计套件。因此，本文所采用的 FPGA7 系列开发板适用于高性能的数字 TRNG 设计。

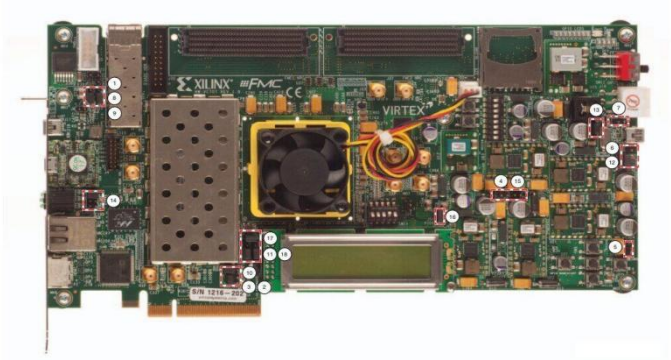

图 5-3 Xilinx Virtex-7 FPGA 外观图

图 5-4 Xilinx Artix-7 FPGA 外观图

本文所使用的是 Xilinx 公司推出的 Vivado 设计软件，并且采用 Verilog HDL 编程语言对 TRNG 进行数字电路描述。使用 Vivado 软件的“Set Up Debug”来对设计的 TRNG 所生成的随机数进行提取，首先将 TRNG 最终的输出信号进行标记抓取，设置采样时钟为其时钟域，设置采样模式和采样深度，再进行综合实现，最后生成比特流文件并烧录到 FPGA 开发板中，就可以进入调试管理界面。在管理界面可手动触发，由于采样深度的限制，一次最多可以采样 13 万多个比特，并以逗号分隔值文件（Comma-Separated Values, CSV）形式保存。显然这是极为不利的，因为后续测试需要 100M 的文本文档。因此需要在管理界面下方输入编写好的脚本文件，自动连续获取保存 800 个逗号分隔符文件，再使用 Python 软件对这些文件进行数据处理。提出的 TRNG 吞吐量与采样时钟保持一致，通过调用 Vivado 中的 IP 核（PLL 或 MMCM）改变采样时钟，就可以对 TRNG 进行吞吐量的测试。

为测试 TRNG 的抗环境变化的能力，需对本文提出的 TRNG 进行温度和电压波动测试。测试时，通过控制温箱的温度，得到在不同温度下设计的 TRNG 所生成的随机数。本文使用德州仪器公司的数字电源控制模块和软件 Fusion Digital Power Designer 对 TRNG 进行电压控制。该软件对 Xilinx Virtex-7 FPGA 开发板的电压、温度监控窗口如图 5-5 所示。

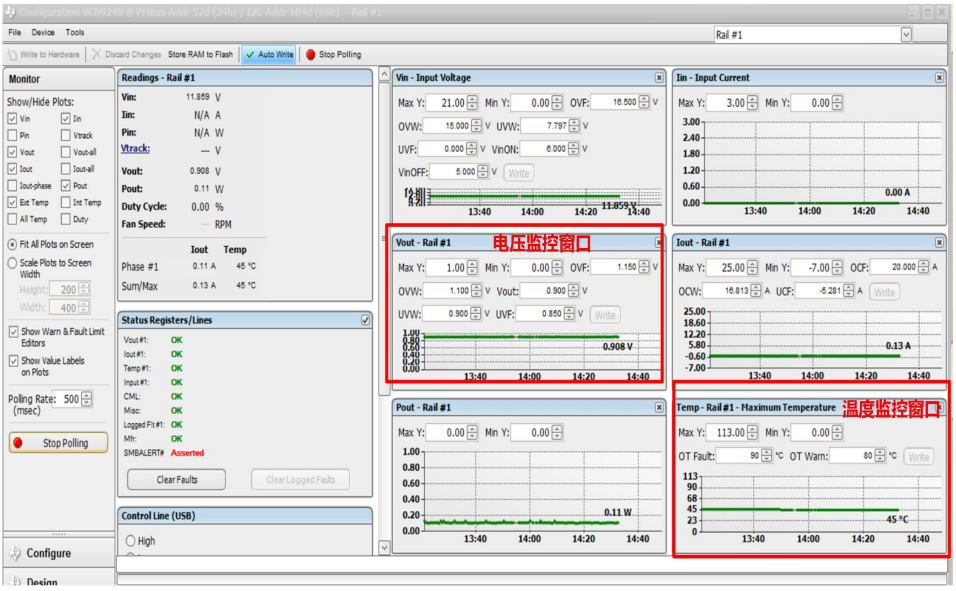

图 5-5 温度和电压测试平台

5.1.2 实验配置

本文提出的 TRNG 分别在 Xilinx Vritex-7 FPGA 和 Xilinx Artix-7 FPGA 开发板上进行实现，FPGA 中的可编程逻辑块的内部资源分布如图 5-6 所示。为完成对于吞吐量的测量，必须使用 PLL 或 MMCM 修改 TRNG 的采样时钟频率，具体的实现方法已经在上一节中详细介绍。

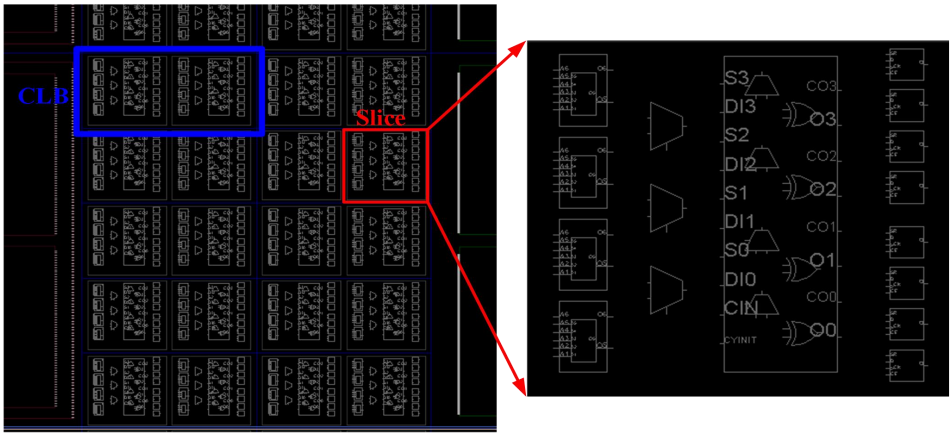

图 5-6 FPGA 的内部资源

本文所设计的两个真随机数发生器所需要用到的逻辑门电路有与非门、异或门、反相器、缓冲器。在上一小节中已经详细介绍过这些逻辑门电路利用其真值表在 FPGA 中通过查找表实现的具体方法，不再赘述。为了便于计算 TRNG 的硬件开销，对于提出的基于亚稳态叠加单元的 TRNG 设计中所涉及到的 MUX 元

件，不直接使用 FPGA 中的实例化原语，统一用查找表实现。将 MUX 的选择端口也作为输入，二选一 MUX 就可以写出一个三输入一输出的真值表，其余操作与实现逻辑门相同。对于采样环节所需要的 D 触发器，直接通过例化内置原语实现。可以看出，本文所提出的两个 TRNG 设计无需其他额外的特定资源，仅仅采用了最为基本的触发器和查找表，电路结构的可移植性较强，便于复现。

本文所设计的两个 TRNG 电路经过上述实现操作，通过 Verilog HDL 硬件描述语言在 Vivado 软件中综合后的 RTL 级模块图如 5-7 所示。本文将设计好的熵源电路（即多异或门耦合单元和亚稳态叠加单元）以模块的形式例化，例化名均为 M1、M2、M3 和 M4，这 4 个模块共同组成 TRNG 的熵源，为其提供随机性。同时模块内部的采样环节构成简单，将熵源电路的输出作为 D 触发器的输入即可。其中，亚稳态叠加单元仅有一个输出，因此需要 4 个 D 触发器构成采样环节，相应的有 4 个输出；而多异或门耦合单元有两个输出，需要 8 个 D 触发器，且有 8 个输出。而对于采样环节的脉冲输入为调用的 PLL 或 MMCM 的 IP 核的输出，可通过配置 IP 核将原始的差分输入的时钟分频为所需要的频率来控制采样速率，进而测试吞吐量。采样环节结束后，提出的两个 TRNG 结构均使用了异或组合技术来提升随机性，将采样环节的输出均接入异或门进行处理。

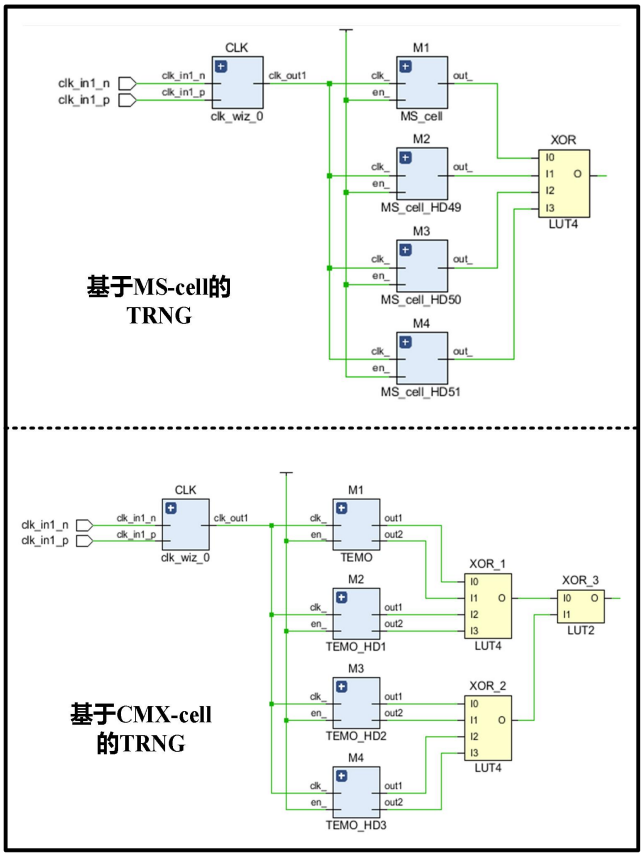

图 5-7 提出的 TRNG 的 RTL 级模块图

为验证本文提出的 TRNG 的抗工艺变化的能力，本文在 Xilinx Artix-7 FPGA 和 Xilinx Vritex-7 FPGA 开发板上均进行了测试（具体测试结果见下一节）。此

外，这种做法不仅可以检验实验是否具有偶然性，还可以对提出的 TRNG 设计的可移植性进行验证。

当完成了对提出的 TRNG 设计的综合实现后，需要对电路内部的查找表与触发器进行布局布线。但本文提出的 TRNG 的设计的初衷之一是为了克服基于亚稳态的 TRNG 需要繁琐路由和严格的布局布线的难点。因此，本文所提出的 TRNG 采用的不是手动路由，而是采用自动布局布线。如果在采用随机的自动布局布线的前提下，提出的 TRNG 电路仍能够通过后续测试，则彻底排除了实验存在的偶然性，说明提出的 TRNG 电路具有良好的可移植性。图 5-8 是 EDA 工具自动产生的电路，即基于亚稳态叠加单元的 TRNG 和基于多异或门耦合单元的 TRNG 布局布线后的电路图。由图可知，基于亚稳态叠加单元的 TRNG 和基于多异或门耦合单元的 TRNG 的布局布线均不对称，可以更有效地测试工艺偏差对 TRNG 生成随机数的影响和 TRNG 的可移植性。

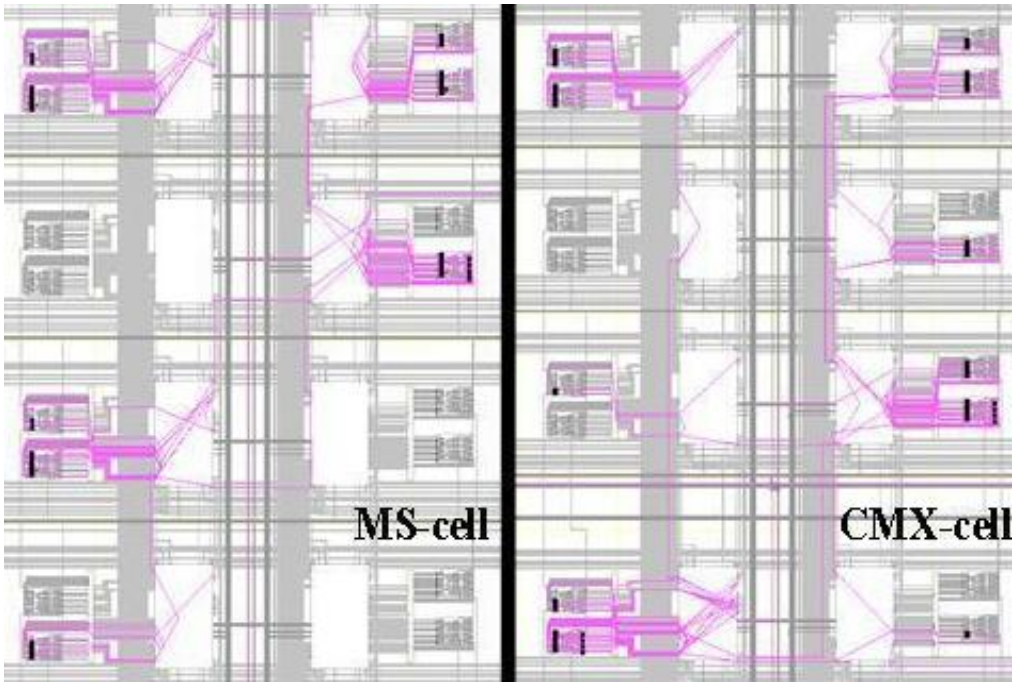

图 5-8 提出的 TRNG 的自动布局布线图

5.2 随机性测试分析

5.2.1 NIST SP 800-22 测试

美国和国际安全界广泛认可的事实标准和权威指南之一是 NIST SP800，它用于评价随机数的质量。其中 NIST SP800-22 测试[72]是专门用来评估任何随机数发生器的统计特性，以验证其随机性的测试统计套件。该套件在密码学领域用于评估加密算法中随机数生成器的安全性；在信息安全领域用于检测随机密钥、随机挑战等的随机性，保障系统安全；在统计模拟等领域确保模拟过程中使用的随机数具有良好的统计特性，使模拟结果更可靠。

该测试套件具体的测试内容如下：

1) 频率测试：又称单比特测试，统计序列中 0 和 1 的个数，检验其是否近似相等，旨在检测序列中 0 和 1 分布的均匀性。

2) 块内频率测试：将序列分块，统计各块内 0 和 1 的频率，查看是否在预期范围内，用于检测局部的 0 和 1 分布均匀性。

3) 游程测试：统计序列中连续 0 或 1 构成的游程数量和长度，检查是否符合随机序列的游程分布特性。

4) 块内最长游程测试：重点关注序列中长度较长的游程，检测是否存在过长或过短的异常游程。

5) 二元矩阵秩测试：将序列构成矩阵，计算矩阵的秩，分析其是否符合随机矩阵的秩分布。

6) 离散傅里叶变换测试：分析经离散傅里叶变换后的随机序列的频谱特性，判定该序列是否存在伪随机行为。

7) 非重叠模块匹配测试：统计某序列中某一特定长度的非重叠模板所出现的次数，并与预期出现的次数进行比较。

8) 重叠模块匹配测试：与非重叠模板匹配测试类似，但允许模板重叠，更全面地检测序列中特定模式的出现情况。

9) Maurer 的通用统计测试：基于序列的压缩性评估随机性，通过计算序列的复杂度来判断其随机性程度。

10) 线性复杂度测试：找到序列生成所需最短线性反馈移位寄存器的长度，以此来衡量序列的线性复杂度，并与原序列长度进行对比。

11) 序列测试：用于判定序列中是否存在连续的相同比特或在特定模式下的连续性是否出现了异常。

12) 近似熵测试：衡量序列中相邻子序列的复杂度和随机性，值越大表明序列随机性越好。

13) 累加和测试：计算序列的累加和，分析其分布特性，检测是否存在趋势或异常波动。

14) 随机偏移测试：将序列视为随机游走的路径，分析随机游走的特性，如是否返回原点等。

15) 随机偏移变量测试：在序列的累计和随机游程中，统计访问特定状态的总次数，并与预期访问次数进行比较。

测试完成之后，每个测试项都会得到 P-value 值和通过率，当每个测试项目的 P 值大于等于 0.01 时，认为序列通过测试[73]。

NIST SP800-22 测试使用到的软件是 Cygwin 和测试工具 STS-2.1.2（如图 5-9 所示）。具体的测试步骤如下：

（1）找到输入 makefile 所在的绝对路径，双击打开测试软件 Cywin64 Terminal。

（2）继续键入：./assess.exe 1000000，再按回车；进入选择测试项目列表，选择 0，再按回车。

（3）此时需要输入测试文件绝对路径，我们可以打开需要测试的 100M 比特的.txt 文件，直接拖进去，就可以自动填充绝对路径，再按回车。

（4）后续依次输入：1，0，100，0；再按回车键，即可测试，测试时间较长，需要耐心等待。

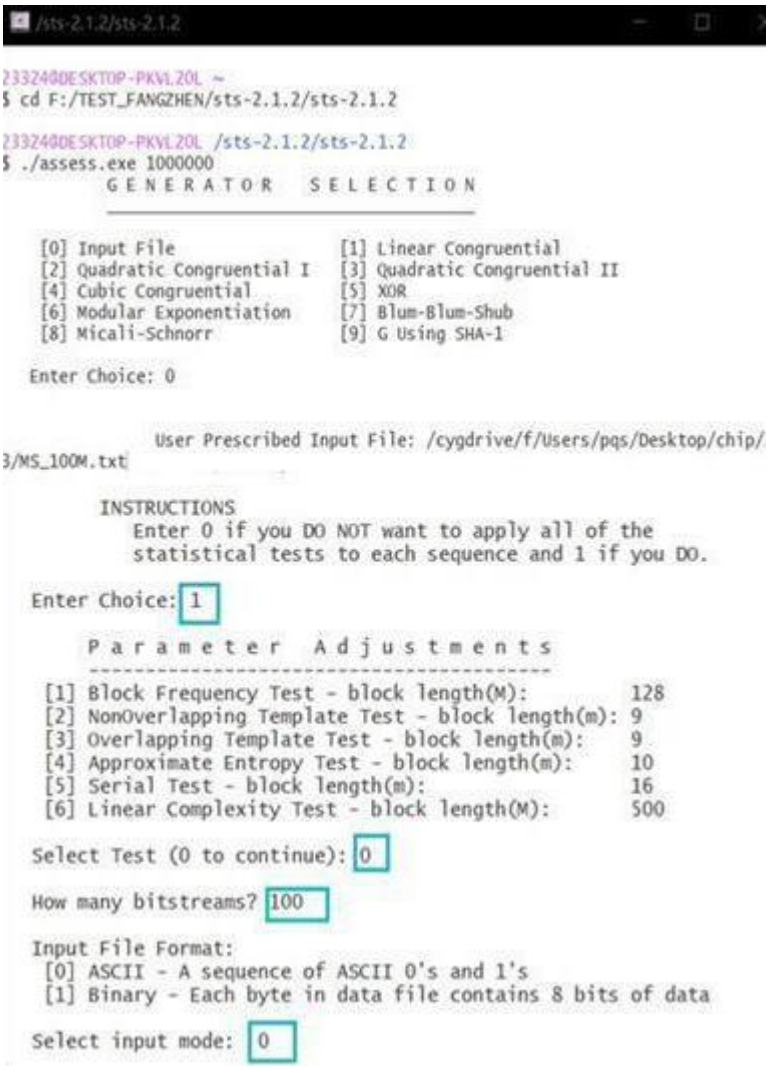

图 5-9 NIST SP800-22 测试流程

在表 5-1 与表 5-2 中，P-value 为各项测试获取的平均 P 值，Pass-rate 指 100 次 NIST 测试的通过比例。依据 NIST SP800-22 测试套件的标准，在每个测试结果中，若 P 值大于 0.01 ，即表明被测随机序列可通过该项测试，且随机性越优，P 值越高。本文将进行的 100 次随机测试的每个测试项目的每次测试结果（即 P 值）记录下来，求和取平均数，得到 P-value。观察表中数据，本文所提 TRNG 于两种不同类型开发板上均成功通过测试，每项测试得出的 P-value 均显著大于 0.01，测试通过率均达 96%以上。实验结果表明，本文设计的 TRNG 随机性良好，可抵御一定程度的工艺变动以生成高质量随机数，具备一定可移植性。

表 5-1 基于 CMX-cell 的 TRNG 的 NIST SP 800-22 测试结果

NIST SP 800-22	Artix-7			Virtex-7		
Randomness Test	P-value	Pass-rate	Result	P-value	Pass-rate	Result
Approximate Entropy	0.4644	98%	PASS	0.4536	99%	PASS
Block Frequency	0.4962	97%	PASS	0.5242	99%	PASS
Cumulative Sums	0.4969	99%	PASS	0.5024	100%	PASS
FFT	0.4510	96%	PASS	0.4489	99%	PASS
Frequency	0.5055	99%	PASS	0.5019	100%	PASS
Linear Complexity	0.4914	100%	PASS	0.5299	100%	PASS
Longest Run	0.4873	99%	PASS	0.5130	100%	PASS
Non-overlapping Temple	0.5003	99%	PASS	0.5013	99%	PASS
Overlapping Template	0.3930	99%	PASS	0.4951	98%	PASS
Random Excursions	0.2667	99%	PASS	0.3048	99%	PASS
Random Excursions Variant	0.2761	99%	PASS	0.2922	99%	PASS
Rank	0.5003	99%	PASS	0.4875	100%	PASS
Runs	0.4740	97%	PASS	0.4911	100%	PASS
Serial	0.4887	99%	PASS	0.5495	99%	PASS
Universal	0.4590	99%	PASS	0.4806	99%	PASS

表 5-2 基于 MS-cell 的 TRNG 的 NIST SP 800-22 测试结果

NIST SP 800-22	Artix-7			Virtex-7		
Randomness Test	P-value	Pass-rate	Result	P-value	Pass-rate	Result
Approximate Entropy	0.5039	99%	PASS	0.5091	98%	PASS
Block Frequency	0.5103	100%	PASS	0.4808	98%	PASS
Cumulative Sums	0.5377	100%	PASS	0.4661	98%	PASS
FFT	0.4542	99%	PASS	0.5221	100%	PASS
Frequency	0.5468	99%	PASS	0.4603	98%	PASS
Linear Complexity	0.4613	99%	PASS	0.4740	98%	PASS
Longest Run	0.5104	100%	PASS	0.5230	99%	PASS
Non-overlapping Temple	0.4957	99%	PASS	0.5006	99%	PASS
Overlapping Template	0.4657	99%	PASS	0.5073	99%	PASS
Random Excursions	0.2718	98%	PASS	0.3105	99%	PASS
Random Excursions Variant	0.2701	99%	PASS	0.3154	98%	PASS
Rank	0.5265	98%	PASS	0.4955	100%	PASS
Runs	0.5507	97%	PASS	0.5541	98%	PASS
Serial	0.4963	97%	PASS	0.5151	100%	PASS
Universal	0.4785	100%	PASS	0.4765	99%	PASS

5.2.2 NIST SP 800-90B 测试

NIST SP800-90B 测试[74-75]为随机数生成器的熵源提供一套科学、统一的评估框架，确保熵源能为随机数生成器提供足够的不可预测性和随机性，从而保障使用这些随机数的信息系统的安全性。具体的测试内容如下：

（1）近似熵测试：量化时间序列复杂度，评估序列不可预测性和非周期性。计算时需定义子序列长度 m 和相似度阈值 r，通过构建子序列、判断相似性、计算平均相似度等步骤得出近似熵值.

（2）最小熵测试：衡量随机变量在最不利情况下的不可预测性，即给出随机数序列中每个元素不确定性的下限估计。若最小熵值高，表明随机数序列抵抗预测攻击的能力强。

（3）碰撞测试：基于哈希函数原理，将随机数序列映射到特定空间，检查是否有过多的碰撞情况。过多碰撞意味着随机数的随机性和唯一性不足。

（4）马尔可夫测试：分析随机数序列是否具有马尔可夫性质，即当前状态只与有限个先前状态有关。若序列不符合马尔可夫性质，则有可能存在长期相关性或具备可预测性。

（5）t-元组测试：统计序列中特定长度 t 的元组实际出现的频率，并与理论上随机序列中 t-元组的预期出现的频率比较，判断序列是否具有随机序列应有的 t-元组分布特性。

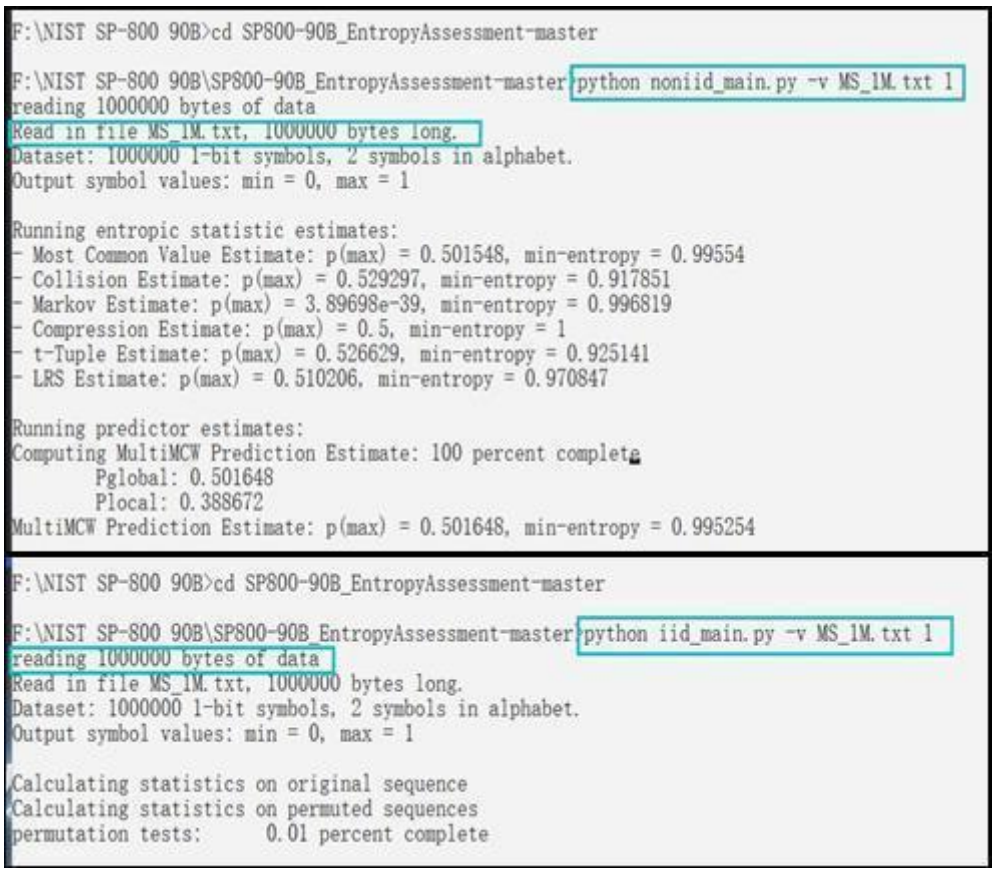

图 5-10 NIST SP800-90B 测试流程

NIST SP800-90B 测试相较于 NIST SP800-22 测试更侧重于对熵源质量、临界测试和统计缺陷等方面的评估，因此本文在 A7 和 V7 开发板上均进行了 NIST 测试中的 IID 测试。由表 5-3 和表 5-4 的测试结果可知，所提 TRNG 生成的随机数均通过了所有测试项目。基于多异或门耦合单元的 TRNG 在 Artix-7 开发板上的最小熵为 0.996237，在 Virtex-7 开发板上的最小熵为 0.994646。基于亚稳态叠加单元的 TRNG 在 Artix-7 开发板上的最小熵为 0.995059，在 Virtex-7 开发板上的最小熵为 0.995120。

表 5-3 基于 CMX-cell 的 TRNG 的 NIST SP 800-90B IID 测试结果

Randomness Test	Artix-7	Virtex-7
IID Permutation	PASS	PASS
Chi-square Independence	PASS	PASS
Chi-square Goodness of fit	PASS	PASS
LRS Test	PASS	PASS
Restart Test	PASS	PASS
Min.Entropy	0.996237	0.994646

表 5-4 基于 MS-cell 的 TRNG 的 NIST SP 800-90B IID 测试结果

Randomness Test	Artix-7	Virtex-7
IID Permutation	PASS	PASS
Chi-square Independence	PASS	PASS
Chi-square Goodness of fit	PASS	PASS
LRS Test	PASS	PASS
Restart Test	PASS	PASS
Min.Entropy	0.995059	0.995120

在实验的过程中，存在某些熵源结构生成的随机数相关性过高，但在独立同分布的假设下，能够侥幸通过 IID 测试的情况发生。为确保本文提出的结构不属于此种特殊情况，本文采用了 Non-IID 测试套件[39]。此种测试套件使用马尔可夫模型、LZ78Y 算法等更为复杂、更为精确的统计模型和算法来测试数据中隐含的相关性信息，更真实地测试其对随机数的影响。因此本文也在 Artix-7 和 Virtex-7 开发板上进行了 NIST SP800-90B 的 Non-IID 测试。根据表 5-5 和表 5-6 的测试结果可知，所提 TRNG 生成的随机数均通过了所有测试项目。基于多异或门耦合单元的 TRNG 在 Artix-7 开发板上的最小熵为 0.922601，在 Virtex-7 开发板上的最小熵为 0.891476；基于亚稳态叠加单元的 TRNG 在 Artix-7 开发板上的最小熵为 0.896712，在 Virtex-7 开发板上的单比特最小熵为 0.891476。

表 5-5 基于 CMX-cell 的 TRNG 的 NIST SP 800-90B Non-IID 测试结果

	Artix-7		Virtex-7	
Randomness Test	p(max)	h-min	p(max)	h-min
MCV	0.501421	0.995906	0.501859	0.994646
Collision	0.519531	0.944718	0.539062	**0.891476**
Markov	3.73292e-39	0.997304	4.39695e-39	0.995459
Compression	0.5	1	0.509277	0.973477
t-Tuple	0.527557	**0.922601**	0.527557	0.922601
LRS	0.510206	0.970847	0.503939	0.988680
Multi-MCW	0.501551	0.995533	0.501692	0.995127
Lag	0.501088	0.996866	0.501234	0.996445
Multi-MMC	0.502067	0.994048	0.501323	0.996188
LZ78Y	0.500500	0.998557	0.501530	0.995593

表 5-6 基于 MS-cell 的 TRNG 的 NIST SP 800-90B Non-IID 测试结果

	Artix-7		Virtex-7	
Randomness Test	p(max)	h-min	p(max)	h-min
MCV	0.501712	0.995069	0.501694	0.995120
Collision	0.537109	**0.896712**	0.539062	**0.891476**
Markov	4.0306e-39	0.996439	4.4813e-39	0.995244
Compression	0.5	1	0.506836	0.980409
t-Tuple	0.526629	0.925141	0.519390	0.945111
LRS	0.502963	0.991475	0.501607	0.995369
Multi-MCW	0.501673	0.995182	0.500678	0.998046
Lag	0.500954	0.997251	0.500901	0.997404
Multi-MMC	0.500685	0.998025	0.501520	0.995621
LZ78Y	0.501425	0.995896	0.500968	0.997211

5.2.3 偏置与自相关测试

在理想情况下，TRNG 所生成的随机数分布不会有明显偏差。然而，这并不意味着 0 和 1 的出现次数必须完全相等，误差应该控制在 0 附近的极小范围内[76]。本节在 A7 和 V7 开发板上采集随机序列，通过 Python 软件将采集到的连续 100 万位的二进制文件进行可视化操作，即将“0”记作黑色像素点，将“1”记作白色像素点，生成黑白位图。从图 5-11 和图 5-12 中可以看到，黑白像素点分布均匀，占比非常接近 50%。

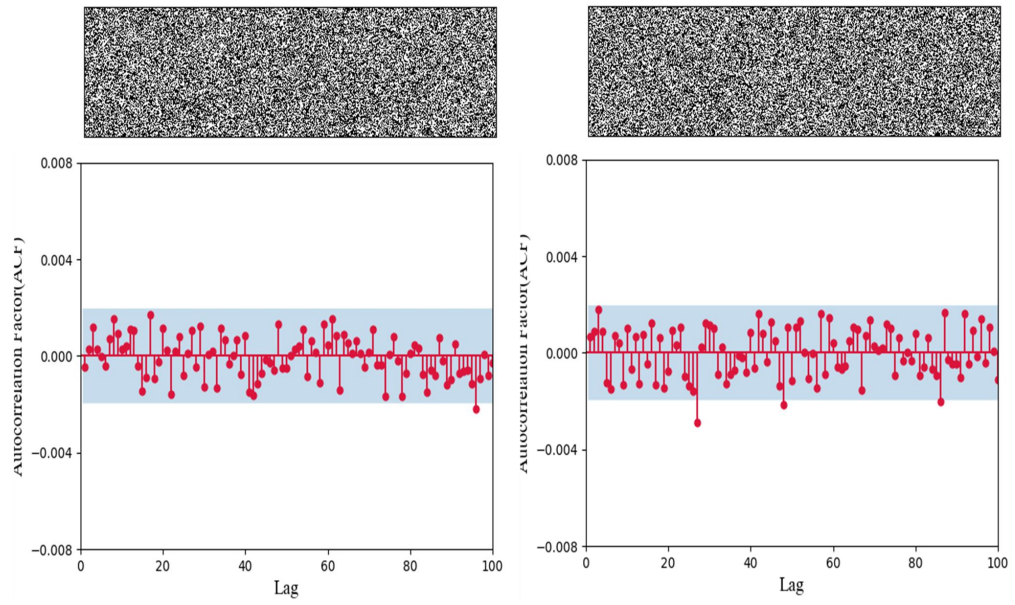

图 5-11 基于多异或门耦合单元的 TRNG 的偏差与自相关测试

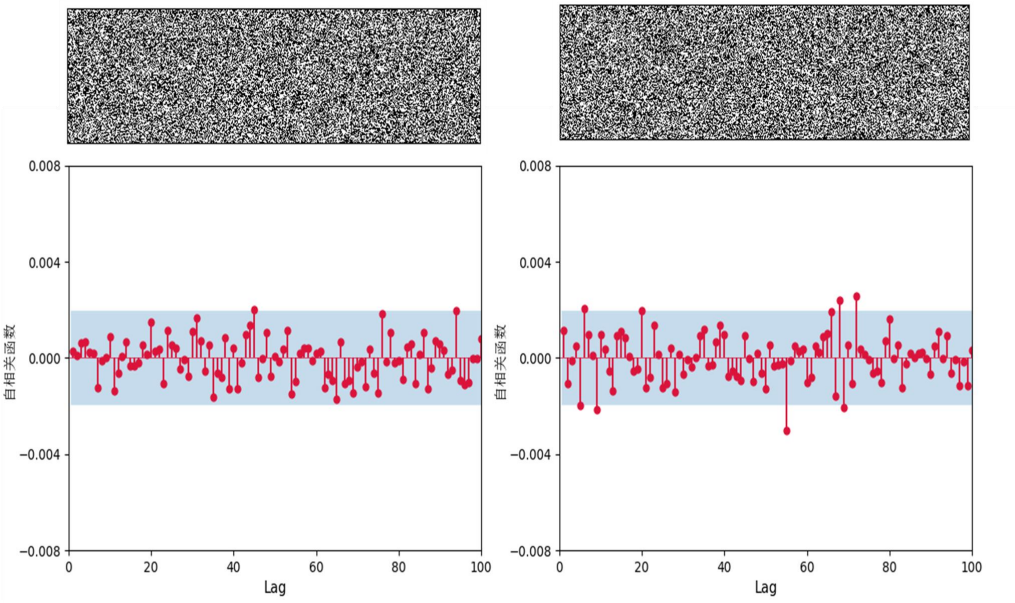

图 5-12 基于亚稳态叠加单元的 TRNG 的偏差与自相关测试

TRNG 生成的随机数之间的相关性必须接近于 0，否则攻击者有可能通过相关性分析破解随机数，窃取隐私信息。自相关性函数[77]（Autocorrelation Function, ACF）是一种可以测试真随机数发生器输出序列相关性程度的统计工具。本文在 A7 和 V7 开发板上得到 6 组 100 万位的测试序列，使用 Python 软件进行自相关测试。如图 5-11 和图 5-12 所示，基于多异或门耦合单元的 TRNG 和基于亚稳态叠加单元的 TRNG 所对应的 ACF 值几乎均在合理的范围内波动。

5.2.4 重启动测试

本文对所提 TRNG 进行了重启动实验，即对 FPGA 开发板重新上电 6 次，每次只记录前 20 位序列。由图 5-13 和图 5-14 可知，每次重启动之后的数据波

形是无序的，不具备任何的规律。说明所提 TRNG 每次上电后产生的初始数据不可预测，是真随机的。

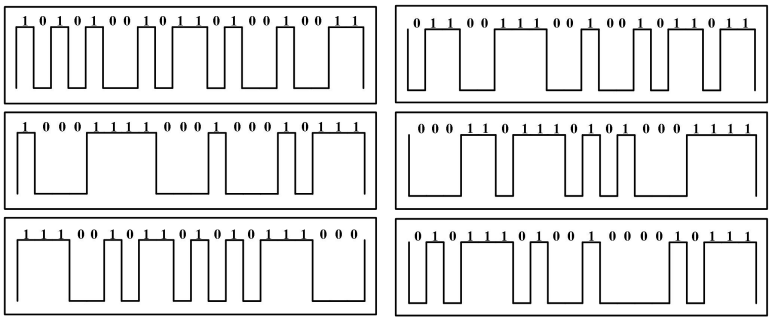

图 5-13 基于多异或门耦合单元的 TRNG 的重启动测试

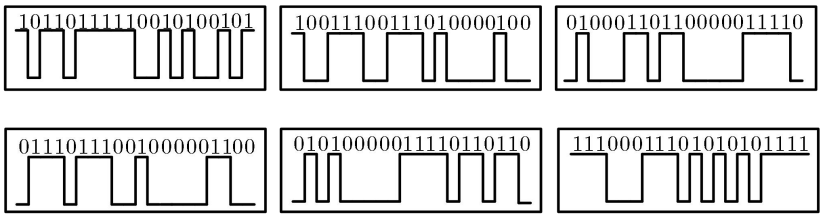

图 5-14 基于亚稳态叠加单元的 TRNG 的重启动测试

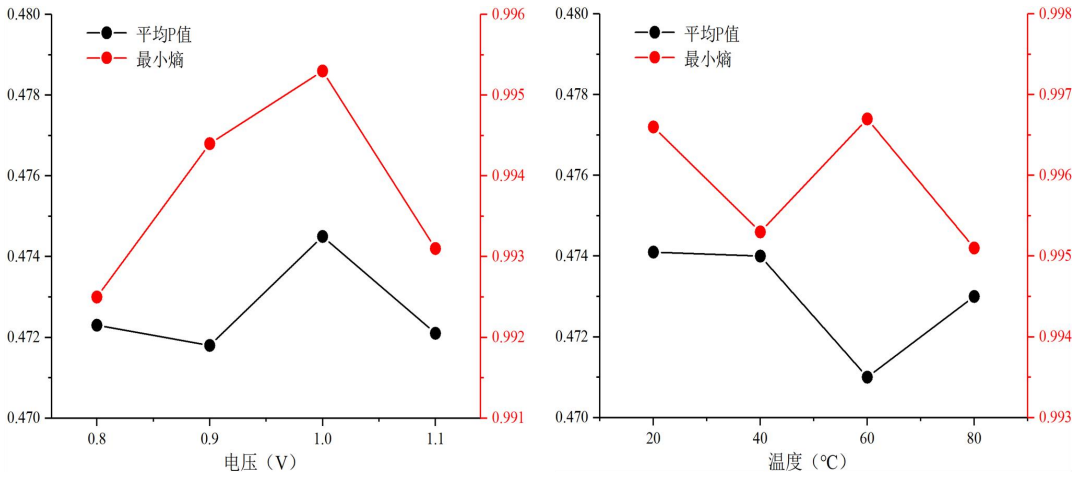

图 5-15 基于多异或门耦合单元的 TRNG 的电压温度测试结果

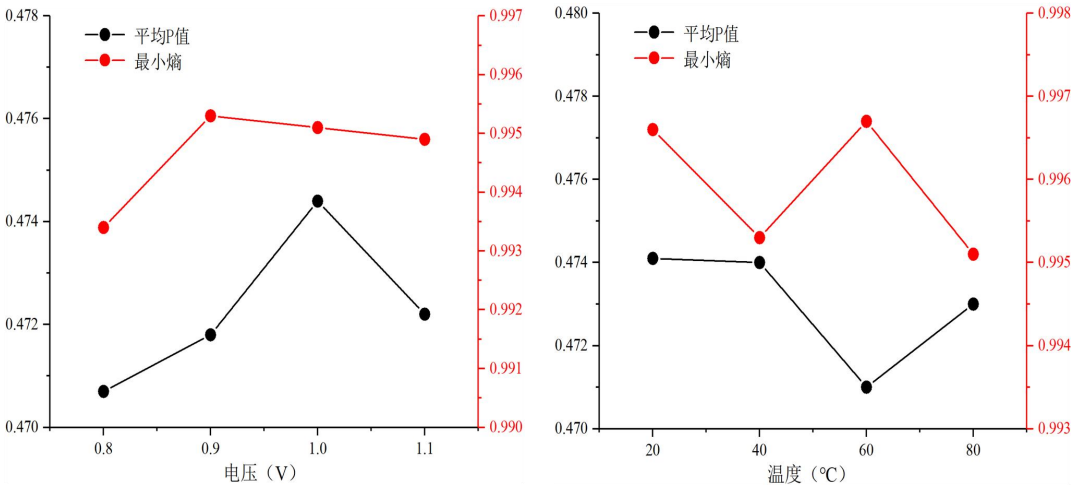

图 5-16 基于亚稳态叠加单元的 TRNG 的电压温度测试结果

5.2.5 电压、温度测试

本文在 0.8 ~ 1.1 V 的范围内，以步长为 0.1 V 进行电压设置，在 20 ~ 80 ℃的范围内，以步长为 20 ℃进行温度设置。基于所使用的 Fusion Digital Power Designer 软件平台，本文进行了多次实验，每次收集 100 万位的随机数。将采集到的随机数经过整合后，进行 NIST 测试，检测被本文提出的 TRNG 在不同的温度和电压下所产生的随机数的质量。并采用 NIST SP800-22 测试中的平均 P 值和 NIST SP800-90B 中的最小熵作为指标，来衡量提出的 TRNG 结构的鲁棒性。测试结果如图 5-15 和图 5-16 所示，由图可知，本文提出的基于多异或门耦合单元的 TRNG 在不同的电压范围内具有不低于 0.471 的平均 P 值和不低于 0.992 的最小熵，在不同的温度范围内具有不低于 0.471 的平均 P 值和不低于 0.995 的最小熵；本文提出的基于亚稳态叠加单元的 TRNG 在不同的电压范围内具有不低于 0.470 的平均 P 值和不低于 0.993 的最小熵，在不同的温度范围内具有不低于 0.470 的平均 P 值和不低于 0.995 的最小熵。此外，本文还补充了温度和电压的交叉实验。在 0.8 ~ 1.1 V 的电压范围和 20 ~ 80 ℃的温度范围内，对任一温度和电压条件下的 TRNG 结构进行测试，并以收集的 100 万位的随机数的偏置作为衡量指标。由图 5-17 可知，本文提出的两个 TRNG 结构即便在最恶劣的环境下（电压为 1.2V 且温度为 80℃）生成随机数的偏置均低于 0.25%。实验结果有力地说明了本文所提 TRNG 在不同的温度电压环境中具备良好的鲁棒性。

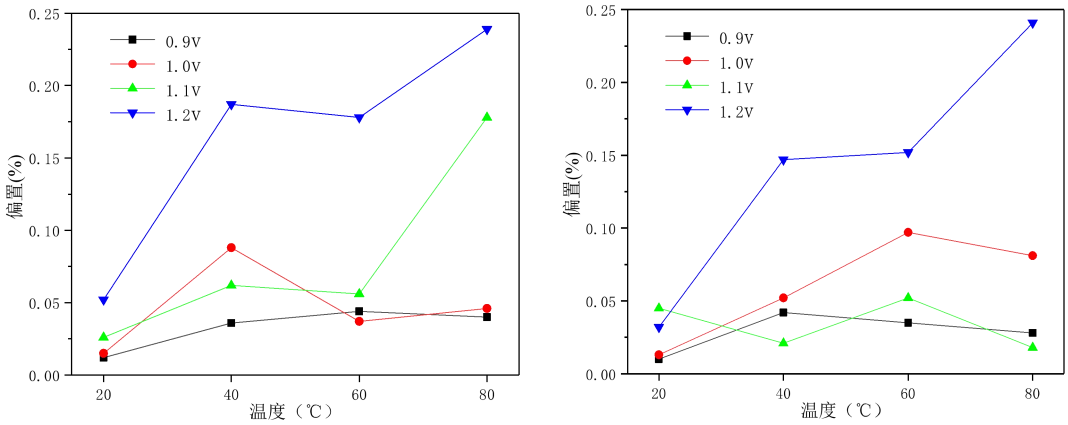

图 5-17 本文所提 TRNG 的电压温度交叉实验结果

5.3 与其他先进 TRNG 的对比

本文提出的基于多异或门耦合单元的 TRNG 和基于亚稳态叠加单元的 TRNG 具有优秀的性能指标，设计的熵源结构有效地提高了 TRNG 的随机性，并采用了异或组合技术进一步提升香农熵，完整的 TRNG 电路结构只需要简单的 D 触发器采样且无需后处理电路，就能够生成高质量的随机序列。设计的 TRNG 均在 Artix-7 FPGA 开发板和 Virtex-7 FPGA 开发板实现，体现出一定的抗工艺变化的能力；通过了温度电压测试，体现出良好的鲁棒性；无需手动布局布线，体现出良好的可移植性。表 5-7 展示了基于多异或门耦合单元的 TRNG 和基

于亚稳态叠加单元的 TRNG 和国际上其他先进的 TRNG 在硬件开销、吞吐量、功耗和有无后处理电路四个方面进行的对比。

表 5-7 与其他先进 TRNG 的对比

Work	FPGA Family	Resource Cost	Throughput [Mbps]	Power [mW]	Post-processing
MEJ'23[25]	Virtex-6	109LUTs + 40FFs	400	-	YES
TCAS-II' 24[35]	Artix-7	12LUTs + 10FFs	150	-	NO
TCAS-I'21[36]	Spartan-6、	56LUTs + 19FFs	100	1.150	YES
DAC'23[37]	Artix-7、Kintex-7	24LUTs + 33FFs	275.8	-	NO
I2MTC'20[38]	Artix-7	50LUTs + 79FFs	280	-	YES
ISVLSI'18[52]	Artix-7	37LUTs + 25FFs	160	-	NO
TCAS-II'22[53]	Virtex-6	24LUTs + 2FFs	290	3703	NO
TCAS-I'22[63]	Spartan-6	36LUTs + 0FFs	12.5	-	NO
TCAD'23[66]	Artix-7	32LUTs + 64FFs	200	-	NO
TCAS-II'23[71]	Zynq XC7Z020	38LUTs + 121FFs	300	119	YES
CMX-cell	**Virtex-7**	**31LUTs + 8FFs**	**500.0**	**171**	**NO**
MS-cell	**Virtex-7**	**29LUTs + 4FFs**	**500.0**	**143**	**NO**

5.3 与其他先进 TRNG 的对比

本文提出的基于多异或门耦合单元的 TRNG 和基于亚稳态叠加单元的 TRNG 具有优秀的性能指标，设计的熵源结构有效地提高了 TRNG 的随机性，并采用了异或组合技术进一步提升香农熵，完整的 TRNG 电路结构只需要简单的 D 触发器采样且无需后处理电路，就能够生成高质量的随机序列。设计的 TRNG 均在 Artix-7 FPGA 开发板和 Virtex-7 FPGA 开发板实现，体现出一定的抗工艺变化的能力；通过了温度电压测试，体现出良好的鲁棒性；无需手动布局布线，体现出良好的可移植性。表 5-7 展示了基于多异或门耦合单元的 TRNG 和基于亚稳态叠加单元的 TRNG 和国际上其他先进的 TRNG 在硬件开销、吞吐量、功耗和有无后处理电路四个方面进行的对比。

由表可知，本文提出的 TRNG 设计与国际上其他先进的 TRNG 相比，具有最高的吞吐量和极低的硬件开销。文献[25]提出的 TRNG 结构新颖，巧妙地将线性反馈移位寄存器与组合逻辑电路中的亚稳态相结合，起振后是多种频率交叠的结果，吞吐量高达 400Mbps。但该结构的电路设计复杂，对后处理电路的需求不可避免，导致其硬件开销（109LUTs + 40DFFs）较大。文献[35]提出了一种基于抖动和亚稳态结合的轻量级混合熵源 TRNG 电路结构，设计了双交叉耦合异或

门单元来生成随机输出序列，虽然其硬件开销仅为 12 个 LUTs 和 10 个 DFFs，但对于吞吐量（150Mbps）的提升有限。文献[36]提出的基于抖动锁存器结构的 TRNG，设计新颖，采用了自定时环的振荡产生随机性。通过利用抖动-锁存器结构精确量化随机性，提高了抖动的采样覆盖率，并增加了结构的输出熵。但需要复杂的后处理电路，导致资源开销较大（56LUTs + 19DFFs），吞吐量仅为 100 Mbps。文献[37]提出了一种利用 D 触发器阵列组成具有 8 个采样点的采样器，来分别对 RO 进行多相位的采样，来精细量化 TRNG 的随机性。该设计所消耗的硬件资源较少（24LUTs + 33DFFs），其吞吐量可达 275.8Mbps。但该设计需要手动布局布线，可移植性不强。文献[38]提出了一种新颖的采样架构，即使用伽罗瓦环振荡器产生的抖动时钟信号对 FPGA 的常规锁相环产生的常规时钟进行采样。并且在常规时钟信号在采样前会先进入一条分接延迟线，形成多相时钟信号，然后再进行异或操作来保证每个采样位都具有最大熵值。与使用时钟采样架构的类似 TRNG 实现相比，可将生成比特率提高 1.33 倍，同时节省了 33%的查找表和 81%的触发器的资源消耗（50LUTs + 79DFFs），吞吐量高达 280Mbps。但与本文提出的结构的指标相比，仍具有相当的差距。文献[52]是十分经典的将异或门嵌入 RO 中的 TRNG 设计，利用异或门来提升抖动的累积速率。其产生的混合振荡显著提升了吞吐量（160Mbps），消耗的硬件资源较少（37LUTs + 25DFFs）。文献[53]在传统环形振荡器的基础上增加了多级反馈结构，扩大了时钟抖动的范围，提高了时钟采样频率和熵源的随机性。具有极低的硬件开销（24LUTs + 2DFFs），比本文提出的 TRNG 要低。虽其吞吐量为 290Mbps，但仍无法与本文高达 500Mbps 的吞吐量相媲美。文献[63]提出的 TRNG 结构将锁存器的不稳定性和环振荡器的抖动相结合，仅仅利用异或门来触发亚稳态行为，以提升随机性（比特熵高达 0.9997）。其消耗的硬件资源不多（36LUTs + 0DFFs），但吞吐量很低（12.5Mbps）。文献[66]基于通用环形发生器架构，采用了面积和时间优化版本的线性反馈移位寄存器，并由多路输出环形振荡器驱动。设计充分利用了单路多路输出 RO 的时序抖动和高速环形发生器架构的优势，但其在吞吐量（200Mbps）和硬件开销（32LUTs + 64DFFs）这两个性能指标上并不出色。文献[71]是基于亚稳态的 TRNG，利用数字时钟管理器来调整两个时钟信号之间的相移，以迫使一个或多个触发器进入可变区，用作随机性源。此设计方案需要复杂的校准，需要手动进行布局布线，可移植性较差。设计的后处理电路有效地提高了吞吐量（300 Mbps），硬件开销高达 38 个 LUTs 和 121 个 DFFs。

综上所述，本文提出的 TRNG 具有最高的吞吐量、不需要后处理电路且无需手动布局布线。在硬件资源消耗方面，只有文献[35]和文献[53]提出的 TRNG 比本文的 TRNG 结构要少，但它们的吞吐量都不能与之相比。其余的 TRNG 结构最多只能在功耗上有优势，但在吞吐量和硬件开销这两个最为重要的性能指标上都是劣势。

5.4 本章小结

在本章内容中，着重针对本文所设计的真随机数发生器展开全面的随机性测试，旨在验证所提 TRNG 是否具备真正的随机性。测试内容涵盖 NIST SP800 - 22 测试和 NIST SP800 - 90B 测试，测试结果充分表明本文设计的 TRNG 符合真随机数的相关标准。此外，为更深入全面地评估 TRNG 的各项性能指标，本章还开展了偏差测试、自相关性测试、重启测试以及温度电压测试等一系列性能测试，测试结果良好。最终，本章将所提的两种 TRNG 设计方案与国际上其他先进的 TRNG 结构，从吞吐率、硬件开销等性能维度进行比较分析。结果显示，本文所提的两种 TRNG 在硬件开销处于极低水平下，仍均可实现最高的 500Mbps 吞吐率，且无需手动布局布线，具有良好的可移植性，从熵源叠加的角度为实现高吞吐量的轻量级 TRNG 提供了两个优秀的解决方案。

由目前的实验结果的对比可知，基于亚稳态叠加单元的 TRNG 相比于基于多异或门耦合单元的 TRNG 在熵、自相关性和硬件开销三个性能指标上有优势，更适用于对安全性要求较高的应用场合，如密钥生成、安全认证以及数字签名等。

第 6 章 总结与展望

6.1 总结全文

随着信息技术的不断更替，在万物互联的时代越来越多的信息安全问题持续频发，设备的安全性和可靠性成为了业内人士研究的重点。真随机数发生器作为一类重要的硬件安全原语，其生成的高质量且可靠的随机数序列可以使得加密算法抵御例如相关性攻击、重放攻击以及暴力破解等攻击手段，保障通信信息数据的安全，是高可靠加密系统中不可缺少的部分。

全数字 TRNG 的设计多数基于 FPGA 平台，按照熵源类型划分 TRNG 主要可以分为基于时钟抖动的 TRNG 和基于亚稳态的 TRNG 两类。传统的基于时钟抖动的 TRNG 因为抖动的累积速率难以提高以及受到采样精度的限制，导致 TRNG 的随机性较差，需要加入额外后处理电路保证其通过统计测试。而传统的基于亚稳态的 TRNG 需要控制 D 触发器的时序违规，因此时钟的频率不能过快；为平衡内部电路的工艺偏差，还需要对 TRNG 严格的手动布局布线，这导致此类 TRNG 的吞吐量低并且可移植性较差。而 TRNG 的共性问题就在于吞吐量与硬件开销之间的矛盾。为此本文针对两类 TRNG，分别设计了基于多异或门耦合的 TRNG 和基于亚稳态叠加单元的 TRNG，均在 A7 和 V7 开发板上实现，且通过了一系列相关性能测试，均实现了 500Mbps 的高吞吐量。其中基于多异或门耦合的 TRNG 的硬件开销分别为 31 个查找表和 8 个 D 触发器，基于亚稳态叠加单元的 TRNG 的硬件开销为 29 个查找表和 4 个 D 触发器。在吞吐量和硬件开销方面，显著优于其他国际上先进的 TRNG。

本文的创新点主要包括以下两个方面：

（1）提出的基于多异或门耦合的 TRNG，采用了将异或门与反相器分离的设计方法，削弱了异或门的短脉冲抑制的对 TRNG 输出的恶化；利用短脉冲将两种频率不同的 RO 中的抖动在交叉耦合的异或门中叠加，提升了 TRNG 的随机性，并建立了数学模型进行验证。

（2）提出的基于亚稳态叠加单元的 TRNG，采用了反馈电路设计，将异或门嵌入 MUX 的反馈环路中，使得由两类数字元件触发的亚稳态可在反馈回路中不断地叠加，增强了 TRNG 随机性，并结合了两类熵源，即不同级数的 RO 中的抖动以及异或门和 MUX 环路中的叠加的亚稳态，提升了 TRNG 的吞吐量，具备良好的可移植性。

6.2 工作展望

本文提出的基于多异或门耦合的 TRNG 和基于亚稳态叠加单元的 TRNG，在吞吐量和硬件开销的权衡方面做了极大的优化，均具备高吞吐量和低硬件开销的特点。所生成的随机数安全可靠，能够通过相关的 NIST 测试、温度电压测试以及一系列的性能测试。受限于硕士期间有限的时间，本文在研究的广度和深度上存在不足，所提 TRNG 电路仍存在下列问题需深入解决：

（1）设计的 TRNG 电路可结合自校准电路或者修改电路设计，对其鲁棒性进行进一步加强，以应对目前工业界对高可靠性加密设备的需求。

（2）目前有许多针对 TRNG 的采样电路的研究，或可加强 TRNG 电路中的采样电路环节，设计更为精密的采样电路来提升采样精度，进而对 TRNG 的性能指标完成更进一步的优化。

（3）提出的 TRNG 缺少实际的应用，后续可以开展协议加密、图像加密和身份验证等相关工作。

（4）后续会对所提的两个 TRNG 进行更深层次的深入实验，研究两者之间的关系，探究其在性能指标上的优劣，分析两者各自更为侧重的应用领域。

（5）后续会提升温度实验的精度，将温度实验的测试范围扩大到工业温度范围（-40℃~85℃），以更精确的数据来反映所提 TRNG 抗温度变化的能力。

参考文献

[1] 李翌昊.区块链技术在物联网信息安全领域应用的分析[J].网络安全技术与应用，2021, 246(06): 17-18.

[2] Chouhan P K, McClean S, Shackleton M. Situation assessment to secure IoT applications[C]//2018 Fifth International Conference on Internet of Things: Systems, Management and Security. IEEE, 2018: 70-77.

[3] 汪秋丽，任志宇，吴翔宇等.基于区块链的物联网可追踪匿名跨域认证方案[J].计算机科学，2025, 2(26): 1-13.

[4] 贾小勇.万物互联，信息安全“芯”守护[J].中国集成电路，2020, 29(09): 18-20.

[5] HAYASHI Y I, HOMMA N, MIZUKI T, et al. Transient IEMI threats for cryptographic devices[J]. IEEE Transactions on Electromagnetic Compatibility, 2013, 55(1): 140-148.

[6] ELMOHR M A, LIAO H, GEBOTYS C H. EM fault injection on ARM and RISC-V[C]//21st International Symposium on Quality Electronic Design (ISQED), 2020: 206-212.

[7] MAJERIC F, BOURBAO E, BOSSUET L. Electromagnetic security tests for SoC[C]//IEEE International Conferenceon Electronics, Circuits and Systems(ICECS), 2016: 265-268.

[8] 温玉耿，卓圣钧，赖怡聪.智慧物联网医疗设备网络安全案例分析[J].物联网技术，2024, 14(07): 58-62.

[9] 罗晓蝶，段威，李一凡等.基于 TRNG 与 PUF 集成结构的安全加密认证系统[J].微电子学与计算机，2023, 40(10): 118-124.

[10] Thirumoorthi M, Jovanovic M, Mirhassani M, et al. Design and Evaluation of a Hybrid Chaotic-Bistable Ring PUF. IEEE Transactions on Very Large Scale Integration Systems, 2021, 29(11): 1912-1921.

[11] LARIMIAN S, MAHMOODI M R, STRUKOV D B. Lightweight integrated design of PUF and TRNG security primitives based on eflash memory in 55-nm CMOS[J]. IEEE Transactions on Electron Devices, 2020, 67(4): 1586-1592.

[12] Petrie C S, Connelly J A. A noise-based IC random number generator for applications in cryptography[J]. IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 2000, 47(5): 615-621.

[13] Bucci M, Germani L, Luzzi R, et al. A high-speed oscillator-based truly random number source for cryptographic applications on a smart card IC[J]. IEEE transactions on computers, 2003, 52(4): 403-409.

[14] Brederlow R, Prakash R, Paulus C, et al. A low-power true random number

generator using random telegraph noise of single oxide-traps[C]//2006 IEEE International Solid State Circuits Conference-Digest of Technical Papers. IEEE, 2006: 1666-1675.

[15] Matsumoto M, Yasuda S, Ohba R, et al. 1200 μm2 physical random-number generators based on SiN MOSFET for secure smart-card application[C]//2008 IEEE International Solid-State Circuits Conference-Digest of Technical Papers. IEEE, 2008: 414-624.

[16] Wieczorek P Z, Gołofit K. Dual-metastability time-competitive true random number generator[J]. IEEE Transactions on Circuits and Systems I: Regular Papers, 2013, 61(1): 134-145.

[17] 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.

[18] Sivaraman R, Rajagopalan S, Sridevi A, et al. Metastability-induced TRNG architecture on FPGA[J]. Iranian Journal of Science and Technology, Transactions of Electrical Engineering, 2020, 44: 47-57.

[19] Tokunaga C, Blaauw D, Mudge T. True Random Number Generator With a Metastability-Based Quality Control[J]. IEEE Journal of Solid-State Circuits, 2008, 43(1): 78-85.

[20] Cao Y, Liu W Y, Zheng Y, et al. A New Reconfigurable True Random Number Generator and Physical Unclonable Function Unified Chip With On-Chip Auto-Calibration[J]. IEEE Transactions on Circuits and Systems I: Regular Papers, 2023, 70(12): 4900-4913.

[21] Vasyltsov I, Hambardzumyan E, Kim Y S, et al. Fast Digital TRNG Based on Metastable Ring Oscillator[C]//Cryptographic Hardware and Embedded Systems.Springer, Berlin, Heidelberg, 2008.

[22] Lozach F, Ben-Romdhane M, Graba T, et al. FPGA Design of an Open-Loop True Random Number Generator[C]//2013 Euromicro Conference on Digital System Design. IEEE, 2013.

[23] Yang X, Cheung R C C. A complementary architecture for high-speed true random number generator[C]//International Conference on Field-programmable Technology. IEEE, 2015.

[24] Wieczorek P Z. An FPGA Implementation of the Resolve Time-Based True Random Number Generator With Quality Control[J]. IEEE Transactions on Circuits and Systems I: Regular papers, 2014, 61(12): 3450-3459.

[25] Jin L Y, Yi M X, Xiao Y, et al. A dynamically reconfigurable entropy source circuit for high-throughput true random number generator[J]. Microelectron J, 2023, 133: 690-699.

[26] 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(03): 115-122.

[27] Robson S, Leung B, Gong G. Truly random number generator based on a ring oscillator utilizing last passage time[J]. IEEE Transactions on Circuits and Systems II: Express Briefs, 2014, 61(12): 937-941.

[28] Prada-Delgado M A, Martínez-Gómez C, Baturone I. Auto-calibrated ring oscillator TRNG based on jitter accumulation[C]//2020 IEEE International Symposium on Circuits and Systems (ISCAS). IEEE, 2020: 1-4.

[29] Wang Y, Li S. A High-Speed Digital True Random Number Generator Based on Cross Ring Oscillator[J]. IEICE Transactions on Fundamentals of Electronics Communications & Computer Sciences, 2016, E99.A(4): 806-818.

[30] Xu X, Liang H, Zhou K, et al. An All-Digital and Jitter-Quantizing True Random Number Generator in SRAM-Based FPGAs[C]//2018 IEEE 27th Asian Test Symposium (ATS). IEEE, 2018.

[31] Drutarovsky M, Varchola M, Petrvalsky M. Remotely testable setup of soft CPU with cryptographic TRNG coprocessor extension embedded into Altera FPGA[C]//2013 IEEE 23th Conference Radioelecktranika. IEEE, 2013.

[32] 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.

[33] Hata H, Ichikawa S. FPGA Implementation of Metastability-Based True Random Number Generator[J]. IEICE Transactions on Information and Systems, 2012, 95-D(2): 426-436.

[34] Fujieda N. On the Feasibility of TERO-Based True Random Number Generator on Xilinx FPGAs[C]//2020 30th International Conference on Field-Programmable Logic and Applications (FPL), 2020.

[35] Yang S, Liang H, Hu R, et al. Lightweight Hybrid Entropy Source True Random Number Generat or Based on Jitter and Metastability. IEEE Transactions on Circuits and Systems II: Express Briefs, 2024, 71(7): 3513-3517.

[36] 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.

[37] Lu Z, Qidiao H, Chen Q, et al. An FPGA-Compatible TRNG with Ultra-High Throughput and Energy Efficiency[C]//2023 60th ACM/IEEE Design Automation Conference (DAC), 2023: 1-6.

[38] 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.

[39] Luo Y, Wang W, Best S, Wang Y, et al. A High-Performance and Secure TRNG Based on Chaotic Cellular Automata Topology[J]. IEEE Transactions on Circuits and Systems I: Regular Papers, 2020, 67(12): 4970-4983.

[40] Hosokawa Y, Nishio Y. Simple chaotic circuit using CMOS ring oscillators[J]. International Journal of Bifurcation and Chaos, 2004, 14(07): 2513-2524.

[41] Dhanuskodi S N, Vijayakumar A, Kundu S. A chaotic ring oscillator based random number generator[C]//2014 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), IEEE, 2014: 160-165.

[42] Tuna M, Alcin M，Koyuncu I, et al. High speed FPGA-based chaotic oscillator design[J]. Microprocessors and Microsystems, 2019, 66(12): 72-80.

[43] Ramji G, Pandey A, Baghel R K. FPGA implementation of chaos-based high-speed true random number generator[J]. International Journal of Numerical Modelling: Electronic Networks, Devices and Fields, 2019, 32(2): 22-31.

[44] Kohlbrenner P, Gaj K. An Embedded True Random Number Generator for FPGAs[C]//Proceedings of the ACM/SIGDA 12th International Symposium on Field Programmable Gate Arrays FPGA, 2004: 71-78.

[45] Golic J D J. New Methods for Digital Generation and Postprocessing of Random Data[J]. IEEE Transactions on Computers, 2006, 55(10): 1217-1229.

[46] 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.

[47] 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, 2008: 385-390.

[48] Varchola M, Drutarovsky M. New High Entropy Element for FPGA Based True Random Number Generators[C]//Proc. of the 12th Int. Workshop on Cryptographic Hardware and Embedded Systems (CHES), 2010: 351-365.

[49] Cherkaoui A, Fischer V, Aubert A, et al. Comparison of Self-Timed Ring and Inverter Ring Oscillators as entropy sources in FPGAs[C]//2012 Design, Automation & Test in Europe Conference & Exhibition (DATE), 2012: 1325-1330.

[50] Ma Y, Lin J, Chen T, et al. Entropy Evaluation for Oscillator-Based True Random Number Generators[C]//International Workshop on Cryptographic Hardware and Embedded Systems.Springer, Berlin, Heidelberg, 2014.

[51] Liu D, Liu Z, Li L,et al. A Low-Cost Low-Power Ring Oscillator-Based Truly Random Number Generator for Encryption on Smart Cards[J]. IEEE Transactions on Circuits & Systems II: Express Briefs, 2016, 63(3): 608-612.

[52] Mei F, Zhang L, Gu C, Cao Y, et al. A Highly Flexible Lightweight and High Speed True Random Number Generator on FPGA[C]//2018 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), 2018: 399-404.

[53] 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, 2022, 69(3): 1752-1756.

[54] Kinniment D J, Chester E G. Design of an on-chip random number generator using metastability[C]//In Proceedings of the 28th European Solid-State Circuit Conference, 2002.

[55] Danger J L, Guilley S, Hoogvorst P. Fast True Random Generator in FPGAs[C]//2007 IEEE MWSCAS/NEWCAS, 2007: 506-509

[56] Tokunaga C, Blaauw D, Mudge T. True Random Number Generator With a Metastability-Based Quality Control[J]. IEEE Journal of Solid-State Circuits, 2008, 43(1): 78-85.

[57] Majzoobi M, Koushanfar F, Devadas S. FPGA-based true random number generation using circuit metastability with adaptive feedback control[C]//in Proc. Crypt. Hard. Embedded Syst. (CHES), 2011: 17–32.

[58] Hata H, Ichikawa S. FPGA implementation of metastability-based true random number generator[J]. IEICE Transactions, 2012,95-D(2):426-436.

[59] Wieczorek P Z. Dual-metastability FPGA-based true random number generator[J]. Electronics Letters, 2013, 49(12): 744-745.

[60] Wieczorek P Z Lightweight TRNG Based on Multiphase Timing of Bistables. IEEE Transactions on Circuits and Systems I: Regular Paper, 2016, 63(7): 1043-1054.

[61] 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), 2017: 738-741.

[62] Lingyan F, Yongping L, Jianjun L, et al. A True Random Number Generator Based On Meta-stable State[J]. IEICE Electronics Express, 2017, 15(1): 1-8.

[63] 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.

[64] Jin L, Yi M, Xiao Y, et al. A dynamically reconfigurable entropy source circuit fo r high-throughput true random number generator[J]. Microelectronics Journal, 20 23, 133: 690-699.

[65] Tang Q, Kim B, Lao Y, et al. True random number generator circuits based on single- and multi-phase beat frequency detection[C]//in Proc. IEEE Custom Integr. Circuits Conf (CICC), 2014: 1–4.

[66] Rajski J, Trawka M, Tyszer J, et al. A Lightweight True Random Number Generator for Root of Trust Applications[C]//in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2023, 42(9): 2815-2825.

[67] Liu H, Wang Y, Sang L, et al. Physical generation of random numbers using an asymmetrical Boolean network[J]. Chinese Physics B, 2021, 30(11): 110503.

[68] Rozic V, Verbauwhede I. Random numbers generation: Investigation of narrowtransitions suppression on FPGA[C]//2009 International Conference on

Field Programmable Logic and Applications, Prague, Czech Republic, 2009: 699-702.

[69] Ni T M, Peng Q S, Bian J C, 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.

[70] Stanchieri G D P, DE Marcellis A, Palange E, et al. A true random number generator architecture based on a reduced number of FPGA primitives[J]. AEU: Archiv fur Elektronik und Ubertragungstechnik: Electronic and Communication, 2019, 105: 15-23.

[71] Frustaci F, Spagnolo F, Perri S, et al. A High-Speed FPGA-Based True Random Number Generator Using Metastability With Clock Managers[J]. IEEE Transactions on Circuits and Systems II: Express Briefs, 2023, 70(2): 756-760.

[72] Rukhin A, Soto J, Nechvatal J, et al. Statistical test suite for random and pseudorandom number generators for cryptographic applications[J]. NIST special publication, 2010.

[73] Dong S, Wang Y, Xin X, et al. A chaos-based true random number generator based on OTA sharing and non-flipped folded Bernoulli mapping for high-precision ADC calibration[J]. Microelectronics Journal, 2021, 116: 259-268.

[74] McKay K. Users guide to running the draft NIST SP 800-90B entropy estimation suite[J]. NIST, Gaithersburg, MD, USA, Tech. Rep. SP, 2016.

[75] Barker E, Kelsey J. Recommendation for the entropy sources used for random bit generation[J]. NIST Special Publication, 2018.

[76] 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, 2016, 64(1): 133-144.

[77] Cao Y, Zhao X, Zheng W, et al. A new energy-efficient and high throughput two-phase multi-bit per cycle ring oscillator-based true random number generator[J]. IEEE Transactions on Circuits and Systems I: Regular Papers, 2021, 69(1): 272-283.

[78] Bahador A, Moaiyeri M H, Ghaderi R. Algorithmically Enhanced Design of Spintronic-Based Tunable True Random Number Generator for Dependable Stochastic Computing[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2025, 44(3): 961-974.

攻读学位期间参与的学术活动及成果情况

一、发表的学术论文

[1] 倪天明, **俞俊勇**, 彭青松, 聂牧. 基于亚稳态叠加单元的高吞吐量真随机数发生器设计[J]. 电子与信息学报, 2024, 46(5): 2289-2297.

二、参与的科研项目

[1] 基于机器学习的芯片系统性缺陷诊断关键技术研究，国家自然科学基金（面上项目），62174001,2022-2025.

[2] 面向全生周期的 Chiplet 可靠性设计，国家自然科学基金（国合项目），62311540021，2023-2025.

[3] 三维集成电路测试与容错，安徽省自然科学基金（杰青项目），2208085J02，2022-2024.

[4] 高可靠集成电路和新型器件创新团队，安徽省高校优秀科研创新团队，2022AH010059，2022-2024.

[5] 数字集成电路单粒子加固单元设计，安徽省重点研究与开发项目，202104b11020032，2021-2023.

三、获得的学术奖励

[1] 两次校级二等奖学金：2023-2024 学年和 2024-2025 学年.

[2] 李飞，吴昊，张娟，**俞俊勇**，张星，完海，李喆，张宏伟，第十一届“挑战杯·华安证卷”安徽省大学生创业计划竞赛金奖，2024.

[3] 李飞，江文，**俞俊勇**，吴昊，芮旺胜，张娟，李喆，卞景昌，安徽省大学生创新大赛（原互联网＋比赛）高教主赛道银奖，2024.

致 谢

时间像须臾间流逝掉的沙子，三年的回忆总带着潮湿的雾气。在我短暂的学涯中，有过不知去向的迷茫，熬过不辞昼夜的劳苦，嗅过付之一炬的焦土气息，尝过瓜熟蒂落的硕果甘甜。尽管其中总有着不够格的失误，但幸得良师益友帮我铸成苦舟，棹学海而歌。承其恩德，感激不尽。

最需要感谢的就是倪天明老师。从研究方向的选择、文献的检索阅读、论文结构的复现、论文创新点的打磨、论文开题、中期答辩、到最终大论文的定稿，这其中的每一个环节都离不开倪老师的谆谆教诲。在三年来，倪老师渊博的学术知识、严谨的教学理念、磊落的人格品质和对学生的责任感让我不由得敬佩万分。在科研上，倪老师对我认真负责，安排了每周的组会研讨和定期科研进度追踪，在为人处事方面也为我点拨迷津，解开了不少的困惑；在生活中，倪老师对我关怀备至，给予了我非常多生活上的帮助。能拜入倪老师的师门，我感到无比的自豪与幸运，再一次向倪老师表示我最诚挚的敬意和感谢！

然后要感谢聂牧老师、卞景昌师兄和彭青松师兄的指导。他们在我进行科研实验的过程中给予了很大的帮助，教会了我各种实验的方法和细节，让我能够将自己的脑中的所思所想落实，并对我提出的结构进行细致入微的评价与讨论，还给出了非常具有建设性的意见。再一次向聂牧老师、卞景昌师兄和彭青松师兄给予我论文上的指导表示由衷的感谢！

还要感谢实验室李飞同学、许克捷同学、叶新伟同学、江文同学以及学弟学妹们，感谢你们一直以来的陪伴与鼓励！在 IICAS 这个大家庭中，我们休戚与共、团结友爱、一同进步，让我感受到了来自这个大集体的温暖与包容。日常生活里，我们互帮互助。在科研学习这条充满挑战的赛道上，我们并肩拼搏奋斗。面对复杂的实验数据，一起反复研讨分析；遇到棘手的理论难题，共同查阅资料、激烈争辩。无数个日夜，我们朝夕相处，实验室里的每一台仪器、每一张桌椅，都见证了我们的成长与坚持。

在此，我还想特别感谢我的父母、哥哥、姐姐和姐夫，是你们一如既往地支持我的学业，帮我解决生活上后顾之忧，安抚我糟糕的个人情绪，使我能够专心致志地进行科研工作，对此我表示深深的感谢!

最后，向在百忙之中审阅此文并给出宝贵意见的专家、教授致以崇高的敬意和衷心的感谢！