振荡采样型真随机数发生器的健壮性研究

陈天宇[1,2,3], 马 原[1,2], 荆继武[1,2,3], 朱双怡[1,2,3]

[1]中国科学院信息工程研究所信息安全国家重点实验室 北京 中国 100093
[2]中国科学院数据与通信保护研究教育中心 北京 中国 100093
[3]中国科学院大学 北京 中国 100049

摘要 真随机数发生器(True random number generator, TRNG)的安全性对于密码系统至关重要。目前主要的国际和国家标准化组织推荐使用熵的概念来评估 TRNG 的安全性。TRNG 所含的熵只能通过其数学模型从理论上得到, 而无法通过输出序列从统计上计算出。然而, 即便理论上安全的 TRNG 在实际使用中也会面临安全风险, 因为 TRNG 中熵源的质量很容易受到物理条件的影响, 包括芯片的制造差异、供电电压和工作温度。在本文中, 针对最通用的振荡采样型 TRNG, 基于理论上的熵估计模型, 我们研究了这种 TRNG 的健壮性, 测试了不同电压下(0.9 V-1.8 V)、不同温度下(–10℃-40℃)的输出, 并比较了同一批次的多个芯片, 从而也对熵估计理论的适用性进行了验证。我们发现: 物理条件的变化对 TRNG 输出的随机性有很大影响。而且, 在应用熵估计理论时, 芯片制造的个体差异和不同环境条件都会导致安全设计参数的不同。本文的实验结果为振荡采样型 TRNG 的安全性评估提供了大量参考, 研究结论可以指导 TRNG 的设计、使用和检测。

关键词 真随机数发生器; 振荡采样; 熵估计; 健壮性
中图法分类号 TP 309.X DOI 号 10.19363/j.cnki.cn10-1380/tn.2017.07.002

On the Robustness of Oscillator-based True Random Number Generators

CHEN Tianyu[1,2,3], MA Yuan[1,2], JING Jiwu[1,2,3], ZHU Shuangyi[1,2,3]

[1]State Key Laboratory Of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
[2]Data Assurance and Communication Security Research Center, Chinese Academy of Sciences, Beijing 100093, China
[3]University of Chinese Academy of Sciences, Beijing 100049, China

Abstract The security of true random number generator (TRNG) is essential for cryptographic applications. At present, the main international and national organizations for standardization recommend to adopt the entropy to estimate the security of TRNGs. The entropy contained in a TRNG cannot be statistically calculated by its generated sequences except utilizing the stochastic model of the TRNG in theory. However, even though the TRNG is secure theoretically, it will be confronted with some security risks. Because the quality of the entropy resource is impressionable for the variation of physical conditions, such as the manufacture difference of chips, the change of voltage or temperature. In this paper, for the most common oscillator-based TRNG, we study the robustness of this type of TRNGs, which is based on the model for the entropy estimation. The experiments analyze the output of the TRNG in different conditions, including the variation of voltage (0.9 V-1.8 V) and temperature (–10℃-40℃), and compare the test results of several chips with the same batch. The applicability of the method for entropy estimation is also verified. We find that the variations of physical conditions cause a great impact on the entropy of the TRNG. In addition, when we employ the entropy estimation, we also discover that the values of the design parameter for security are not consistent due to the manufacture difference of chips and the variation of environmental conditions. The research achievement provides a large number of reference for the security evaluation of the oscillator-based TRNG. The conclusion obtained can guide the design, use and test of TRNGs.

Key words true random number generator; oscillator-based; entropy estimation; robustness

通讯作者: 马原, 于 2014 年在中国科学院大学获得博士学位。现任中国科学院信息工程研究所助理研究员。研究领域为随机数发生器的设计与检测、密码算法高速实现。Email: mayuan@iie.ac.cn。

本课题得到 973 计划(No.2013CB338001), 国家自然科学基金(No.61602476)和中科院战略先导课题(No. XDA06010702)资助。
收稿日期: 2017-02-20; 修改日期: 2017-03-14; 定稿日期: 2017-05-23

1 背景

随机数发生器(Random number generator, RNG), 是信息安全和密码系统中不可缺少的基础元件之一。它是生成密钥的重要资源, 也是密码计算和协议中必要的安全参数提供者, 其安全性是密码系统安全性的前提。随机数发生器所产生的随机数用途广泛, 常用于密码算法的密钥生成、安全协议的认证过程等。RNG 按产生原理分为两类: 真随机数发生器(True random number generator, TRNG)和伪随机数发生器(Pesudo-random number generator, PRNG)。一般地, PRNG 通过一个确定性函数, 由一段有限长的种子(由 TRNG 产生)持续地产生伪随机序列, 该序列具有良好的统计性质, 而序列的随机性大小完全取决于种子; TRNG 则通过采集含有随机性成分的物理现象中的随机性, 持续地产生具有真随机性(不可预测性/不确定性)的序列。因此, TRNG 的安全性至关重要。如何确保 TRNG 在设计和使用中的安全性, 对保障需要随机数服务的密码系统的安全性具有重大意义。

一个高质量的 TRNG 体现在其输出序列具有完美的不可预测性。为验证 TRNG 输出序列的质量, 传统方法是采用统计检测或实验观察分析来判断序列是否具有良好的统计特性, 例如美国国家标准与技术研究院(National Institute of Standards and Technology, NIST)发布的 SP 800-22 标准[1]和我国密码行业标准《随机性检测规范》[2]。但是, 这种评估方法属于黑盒测试, 它只关注于输出序列的统计性质, 对于序列的均匀性和独立性可以做出判别。而对于输出序列是否完全不可预测是很难通过统计检测断定的。因此, 现代 TRNG 评价理念中普遍采用产生的随机数所含有的信息熵, 作为 TRNG 安全性的评估标准。熵作为刻画不确定性的度量, 可以有效地衡量 TRNG 的真随机性。对此, 国际标准化组织发布的标准 ISO 18031[3]和德国 BSI 发布的信息安全标准 AIS 31[4]中, 均推荐采用熵估计方法来指导 TRNG 的设计与检测。熵估计方法属于对 TRNG 的白盒测试。它是根据特定的 TRNG 结构, 通过建立随机模型对其本质的安全性做出评估。这个随机模型的建立则是基于对该 TRNG 熵源做出的假设, 进而描述 TRNG 的工作原理, 根据 0/1 比特的概率分布, 最终得到熵的理论计算结果。这种通过建模进行熵评估的方法, 相比于传统的统计检测(黑盒测试)而言, 可以从本质上给出 TRNG 的熵值, 对 TRNG 的安全性进行定量的评价。

振荡采样型 TRNG 以其结构通用、易于硬件实现、可建模分析等优点, 已成为广泛使用的一类 TRNG。这类 TRNG 可以方便地用数字电路实现, 如在 FPGA(Field-programmable gate array)或 ASIC (Application-specific integrated circuit)平台上。这种结构的 TRNG 随机性来源于电路噪声产生的抖动。抖动可以理解为: 信号在翻转时间上, 相比于理想位置的微小偏移[5]。目前一些设计都是基于振荡采样结构的[6]。对振荡采样型 TRNG 熵估计的基本思想是: 首先根据熵源结构抽象出随机模型, 然后给出理论上的熵计算过程, 再根据设计和噪声参数估计熵值大小。

事实上, 即便通过随机模型可以保证所设计的 TRNG 在理论上是安全的, 但在实际使用中依然难以确保输出序列的熵是充足的。这是因为 TRNG 在实际使用时, 其熵源会受到内部或外部因素的影响, 导致输出序列的熵值变化, 影响使用的安全性。所以, 为了保证 TRNG 的安全性, 需要在设计、使用和检测时充分地考虑物理条件的影响。

这些物理条件对于 TRNG 健壮性影响主要体现在以下两个方面:

- 一方面是芯片制造个体差异, 会导致不同芯片中噪声特性是不同的。这种现象会经常出现在芯片生产过程中的不同批次甚至同一批次的不同芯片中。不同的噪声特性, 会使得 TRNG 芯片中的抖动大小不尽相同。这就可能导致每个 TRNG 芯片在达到所需的安全性要求时, 对应的采样间隔不尽相同。然而, 芯片中精确的噪声特性只能通过实际测量芯片本身得到, 而在芯片制作前现有的电路仿真软件(如 Synopsys HSPICE)并不能精确地模拟出所制作出来的 TRNG 芯片中噪声演变过程。所以, 芯片制造差异很可能使得所生产的某些 TRNG 芯片并不满足所需安全性要求, 而事先无法得知。
- 另一方面是熵源会受到外部环境变化的侵扰[9-12], 外部环境变化是指供电电压或环境温度的变化等; 而且, 熵源也会受到敌手的恶意攻击[13]。无论是外部环境的改变还是恶意攻击, 都会导致 TRNG 的随机特性产生变化。如果在 TRNG 设计时没有充分考虑这些环境因素的影响, 那么输出序列的熵值可能已不满足安全性要求、甚至可能导致 TRNG 停止工作。

总的来说, 一些物理条件的变化会致使理论熵估计中的参数变化, 进而影响熵估计的准确性、甚至可能导致建立的模型失效。本文中, 我们将结合熵估计理论, 研究物理条件对 TRNG 健壮性的影响, 并研

究熵估计理论的在实际电路中的适用性为 TRNG 的设计和检测提供参考依据。

本文的主要贡献如下:

1. 根据熵估计模型, 设计了一种振荡采样结构, 并给出一种离线测量熵值的方法, 能够由采样间隔得到当前的理论熵值。

2. 搭建了 TRNG 健壮性实验系统, 包含原型芯片、可控电压、温度装置, 其中 TRNG 的采样间隔由熵估计结果推导出, 可通过由外部人为控制。

3. 在实验系统下, 分别从芯片制造差异、供电电压和温度变化三个方面, 研究了物理条件对于 TRNG 安全性的影响, 并对实验结果分析。

本文的组织结构如下。第二章介绍振荡采样型 TRNG 的工作原理、现有的熵估计方法, 以及对 TRNG 健壮性的相关研究。第三章结合熵估计理论的物理假设, 提出一种 EO-TRNG 设计结构。第四章给出实验方案, 分别从芯片制造差异、电压和温度三方面分析环境因素对于 TRNG 安全性的影响。第五章给出实验和分析结果。第六章对本文工作的进行总结和展望。

2 相关工作

本章中, 首先介绍了基本的振荡采样型 TRNG (Elementary oscillator-based true random number generator, EO-TRNG)的基本结构和工作原理。其次, 针对于这一结构, 我们分别从时域和相位角度总结了现有的随机模型和熵计算方法。最后, 给出了当前针对于实际运行时 TRNG 安全性的影响因素的相关研究。

2.1 EO-TRNG 的结构和工作原理

EO-TRNG 的结构如图 1 所示。这类 TRNG 的熵源由两个振荡器组成。一种常见的振荡器实现形式是环形振荡器(简称振荡环), 记图 1 中的两个振荡环分别为 RO_i $(i=1,2)$。振荡环 RO_2 的输出(振荡信号)作为采样信号, 经分频器将频率降为原来的 $1/N$, 分频后的信号作为采样单元(例如 D 触发器)的时钟信号。每当时钟信号到达上升(或下降)沿时, 对振荡环 RO_1 输出的被采样信号进行采样, 由 D 触发器输出比特序列。这种生成随机数方法的随机性来源于电路中由噪声产生的抖动, 它附加在振荡信号上, 使得采样点的位置(处于高电平或低电平)存在不确定性, 因而产生了具有随机性的比特序列。参数 N 是该 TRNG 设计中重要的设计参数, 它表示采样间隔的大小, 决定了每一次采样所能积累的抖动量的大小。在设计或检测过程中, 关键点在于: 给定振荡器参数(振荡频率和抖动大小)的情况下, 多大的采样间隔是能够保证累积的随机量是足够的, 即此时的熵是充足的。

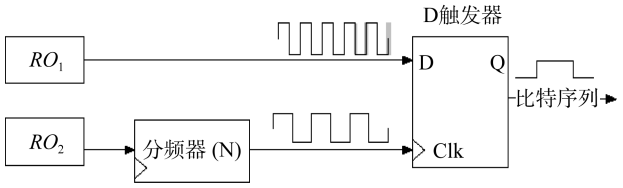

图 1 EO-TRNG 的原理图

2.2 现有振荡采样型 TRNG 的熵估计方法

TRNG 的熵估计方法一般包括两个环节: 建立随机模型和熵计算。具体地, 首先需要从理论上基于噪声模型对 TRNG 的熵源提出假设, 如噪声服从独立的正态分布等。然后根据假设和 TRNG 的工作原理, 用数学语言对噪声转换成随机比特的过程进行详细刻画, 即为建立模型。随后, 从模型出发, 根据噪声参数和设计参数计算输出序列或输出比特的概率分布, 进而计算出 TRNG 的熵。这里的熵的类型可以是最小熵、熵的下界或比特率熵。

对于振荡采样型 TRNG 随机模型的建立, 目前研究工作围绕基于时间演变和基于相位演变两个角度展开。这二者只是衡量角度不同, 本质上是等价的。Killmann 和 Schindler [14] 在 CHES 2008 上, 从时域角度提出了一个通用的随机模型, 可用于评价振荡采样型 TRNG 的安全性, 给出一个熵的下界(lower bound)计算方法。采用类似的建模方法, 马原等人[15]在 CHES 2014 上, 从时间演变的角度建立了随机模型, 并给出了理论熵的精确计算方法。2011 年, Baudet 等人[16]在 Journal of Cryptology 2011 期刊上, 从相位演变的角度建立了随机模型, 同样给出了理论熵的精确计算方法以及熵下界的计算方法, 并且得到了解析表达式。其它类型的振荡器 TRNG 的随机模型在这些文献[8,17-20]中提出。对基于亚稳态或一些复杂熵源结构的 TRNG [21], 由于熵源行为或者随机性提取过程复杂, 目前来看并没有可行的熵估计方法。

特别地, 在文献[15]中, 研究人员都提出将质量因子作为安全参数, 可以从较大程度上反映 TRNG 所含熵值的大小(还有另一变量对熵值有轻微影响)。质量因子越大, TRNG 所含熵值也就越大。在文献[15]中, 作者还给出了一种简单的质量因子测量电路, 能够使用对振荡信号周期计数的方法计算得到质量因子。此外, 在熵阈值规定上, 德国 AIS 31 标准推荐 TRNG 所包含的每比特的熵应不低于 0.997。实验证

实, 这样的熵阈值可以让随机序列通过简单的统计测试[1],[23]。

2.3 目前对 TRNG 健壮性的研究

目前, 很多类型的TRNG在实际使用中, 熵源都容易受到物理条件的影响, 也就是芯片的制造工艺、供电电压和环境温度的变化(Process, Voltage, Temperature - PVT)。在芯片制造方面, 2008 年, Vasyltsov 等人[9]分析了 65 nm 工艺下不同的工艺角(process corner)对于亚稳态型 TRNG 随机性的影响关系。在工艺角仿真实验中, 他们发现在不同的工艺角下, 产生的比特序列均匀性是不同的, 并通过降低采样率的方法来确保他们所设计的 TRNG 输出序列的质量。此外, 在文献[12]中, Rahman 等人对多环结构分析, 指出不同的芯片制作技术会导致 TRNG 所含有的随机性大小不同, 较老的技术节点制作出来的 TRNG 相比较新的具有的随机性少。对此, 他们在相同温度和电压下, 分别在 45 nm、90 nm 和 130 nm 技术节点上做了对比实验, 验证了芯片的制造工艺差异对 TRNG 随机性的这一影响关系。

在 TRNG 工作的环境条件方面, 2009 年, Santoro 等人[10]在多个结构上(多环结构[8]、亚稳态型[9]和复杂熵源结构[21]), 实验探究了温度对于随机性的影响关系, 在实验中温度变量分为器件温度和环境温度, 他们发现环境温度的变化对于随机性的影响较大, 而器件本身温度的变化对于随机性基本影响不大。另外还有一些研究[9,11]也探究了环境温度的变化对于 TRNG 质量的影响。此外, 在 CHES 2009 上, Markettos 等人[13]展示了如何对多环结构的 TRNG 进行主动的频率注入攻击, 受攻击的振荡环会出现频率互锁现象, 使得输出的随机性明显降低。

与以前的研究工作相比, 本文的工作有两个重要的不同点。首先, 本文面向的是一种通用的振荡采样结构 EO-TRNG, 并不是某个特定设计结构, 因为 EO-TRNG 是一种基础架构, 对其的研究结果也可适用于以它为基础的其他结构上。其次, 更重要的是, 因为熵估计目前已经成为公认的对 TRNG 安全性进行评估的方法, 本文研究了目前的熵估计理论在物理条件变化下的适用性, 从一个新的角度来测试 TRNG 的健壮性, 探究理论结果和实验结果的一致性。

3 EO-TRNG 设计

在对 TRNG 建模时, 为了保证模型尽可能简单, 现有熵估计理论[15-16]假设时域抖动或相位增量是独立分布的, 但这在实际中难以保证。由于采样频率较低, 相关噪声的影响对抖动或相位的影响会突显出来。相关噪声的存在会造成对独立抖动的过高估计, 甚至确定性干扰的存在, 都会导致熵估计过高的问题; 为此, 我们首先采用相同结构振荡环来抵消确定性干扰影响; 其次, 基于独立抖动的测量方法, 我们对白噪声影响下的质量因子进行测量, 避免了相关噪声的影响, 从而获得更准确的理论熵估计结果。

图 2 描述了本文所设计的 EO-TRNG 结构。该结构的熵源是一对振荡环(RO_1 和 RO_2), 由 RO_2 输出采样时钟, 在一段时间内(采样间隔)对 RO_1 输出的被采样信号进行采样。两个振荡信号分别由计数器 C_1 和 C_2 对它们的周期计数。当计数器 C_2 中累加了 N 个采样时钟信号的周期后, 发送(一次)计数过程完成指令给控制单元, 控制单元则将清零指令发送到计数器 C_1 中, 执行计数值的清零操作。在每一次清零操作前, 需要将计数结果 *Cnt*(*N*)储存到计数结果保存单元中, 时钟为 *ro_samp*(采样完成信号)。计数结果保存单元的数据经 mod 2 处理后(即最低位)写入到 FIFO 中, 等待接收到外部的读取指令 *read* 后, 输出随机比特。

3.1 熵源结构

由供电电源产生的确定性干扰对振荡信号的影响无法避免, 进而将确定性成分加入到计数结果以及 TRNG 的输出中。这种情况会影响生成比特的安

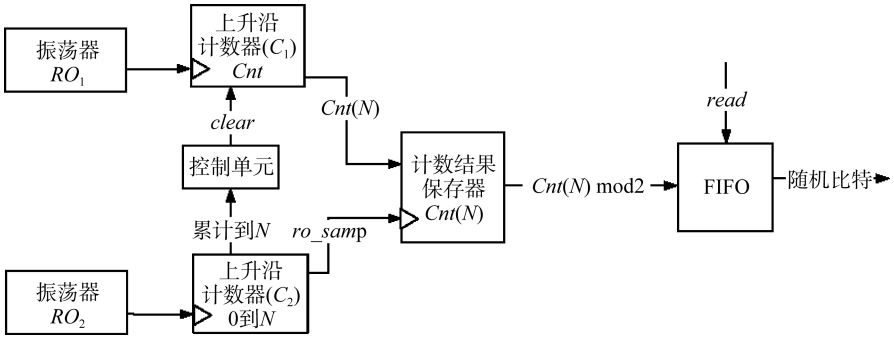

图 2 EO-TRNG 的结构原理

全性, 使得预测的困难度大大降低[15-16]。另外, 文献[13]中指出, 确定性干扰很容易受到敌手的操控。而且, 确定性干扰作用下产生的比特序列, 虽然质量(真随机性)很差, 但会具备较好的统计特性(伪随机性的贡献), 因此依然可以通过黑盒统计测试, 从而造成被测序列具有较好质量的假象, 给密码系统带来严重的安全风险。

确定性干扰几乎无法避免, 所以不能消除其影响。但它可以被抵消: 确定性干扰对芯片上信号的影响是全局的, 在同一位置处的干扰几乎一致。根据这个特点, 我们实现一对振荡环, 而且它们含有相同数量的反相器、具有相同的布线方式、被放置于同一芯片上的相邻位置、被同一电源供电。此时, 这对振荡环所产生的振荡信号会受到几乎一样的确定性干扰的影响, 在采样过程中则可以相互抵消掉干扰对采样序列的影响。

3.2 熵提取方法

在连续采样方式下, 我们采用对振荡信号周期计数的方法收集熵源的随机性。具体流程(如图 3 所示)是: 在一个采样间隔内, 利用一个上升沿计数器 C_1 对被采样信号(RO_1 的输出信号)的周期计数, 计数器存储的数值加 1。其中, 采样间隔大小由采样时钟(RO_2 的输出信号)的 N 个周期决定(N 为采样间隔参数)。每一轮计数过程完成时, 计数结果 $Cnt(N)$则被存储到计数结果保存器(由寄存器实现)中, 并由控制单元发出清零指令 *clear*, 对计数器 C_1 执行清零操作, 然后开始下一轮的计数操作。

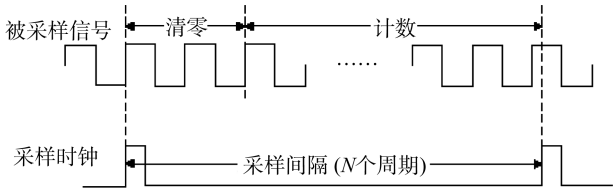

图 3 熵提取过程

3.3 一种离线的熵测量方法

由于 TRNG 随机模型中只考虑了白噪声的影响, 我们需要计算白噪声影响下计算质量因子, 用于估计熵值大小。

在文献[15]给出的熵估计模型中, 作者在独立抖动的假设下, 提出质量因子 q 可以反映 TRNG 熵值。质量因子的表达式为 $q=\dfrac{\sigma\sqrt{v}}{\mu}$, 其中 μ 和 σ 分别为被采样信号的半周期均值和标准差, $v=\dfrac{\Delta t}{\mu}$ 是采样间隔(Δt)下被采样信号半周期的个数。通过表达式, 我们可以直观地看出质量因子 q 的含义是: 在给定的采样间隔内, (独立)抖动的积累量。而文献[16]从相位的角度建模, 给出了等价的质量因子 $Q(=q^2/4)$来反映熵值。因此, 我们可以通过质量因子 q 衡量 TRNG 的熵值。而且, 作者发现当质量因子 $q\geqslant 1$ 时, 在理论上可以保证所产生的随机数的熵值是充足的(不低于 0.9999/每比特)。

事实上, 根据更新过程理论, 质量因子 q 的测量是通过计数结果方差值近似得到的。DATE 2014 中, Haddad 等人[24]针对 EO-TRNG 结构, 给出了一种去除相关噪声影响的周期抖动测量方法。不同于以往测量方法中直接通过计数结果算方差值, 该文章作者采用将相邻的两个计数结果做差, 再计算差值的方差, 然后通过对不同采样间隔下方差值的数据拟合结果, 得到白噪声下的周期抖动。

基于文献[24]中的测量方法, 我们直接测量白噪声影响下的质量因子 q_w, 避免了从周期抖动到质量因子的复杂转换。具体方法为: 首先记录不同采样间隔下相邻计数值差的方差, 利用曲线拟合的方法得到曲线一次项部分, 即为该采样间隔下 q_w 的平方。

此外, 需要说明的是, 相比于使用示波器在芯片外部测量抖动大小的方法, 在我们的内部测试方法中, 由于中间数据(计数结果 $Cnt(N)$)是在发生器内部得到的, 因此可以有效避免从芯片到示波器的传输电路上附加抖动对测量的影响[25], 从而对熵的估计更为精确。

4 健壮性研究的实验方案

这一章中, 我们在 ASIC 芯片上实现该 EO-TRNG 结构, 探究物理条件对其随机性的影响。我们分别针对制造差异、供电电压和环境温度三个影响因素进行实验分析。其中, 制造的差异指的是在同一工艺(本文是中芯国际 SMIC 130 nm)下不同芯片展现出来的偏差, 如振荡环频率、噪声大小等。

4.1 ASIC 芯片的实现

我们在 SMIC 130 nm 工艺下进行了流片, 其中的两个振荡环采用相同的版图。每个振荡环包括一级与门、一级非门和若干延迟单元组成, (在 tt 工艺角下)仿真频率约为 180MHz。正常情况下, 芯片内核的工作电压为 1.2 V, PAD 的供电电压为 3.3V。

该 TRNG 芯片主要包括熵源模块、采样模块和输出模块。为判断物理条件对于 TRNG 随机性的影响关系, 我们将采样间隔这一设计参数设置成可由外部人为进行调节, 从而反映出不同采样间隔下输出随机序列随机性的变化。

4.2 实验平台

图 4 展示了我们的 EO-TRNG 芯片的实验平台。芯片被放置在恒温箱中, 由可调电压源供电。振荡信号频率由示波器观测。芯片的控制和数据管脚都与 FPGA 相连, 进而 FPGA 通过 USB 与 PC 机对接。在运行过程中, PC 机设定采样间隔 N, 然后获取当前采样间隔下的计数结果(用于熵估计)和采样序列(用于统计测试)。表 1-2 分别给出了硬件和软件资源使用情况。

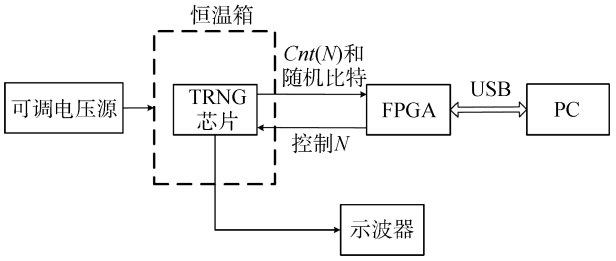

图 4 EO-TRNG 芯片的实验平台

表 1 硬件资源列表

硬件名称	用途描述
PC 机	实验软件集成平台
EO-TRNG 的 ASIC 芯片	EO-TRNG 的集成电路
Virtex-5 FPGA	TRNG 芯片控制
可调电压源	为芯片提供不同电压供电
高低温测试箱	为芯片提供不同环境温度

表 2 软件资源列表

软件名称	用途描述
ISE14.6	硬件语言程序的编写、实现等
自编软件程序	数据接收和离线熵计算
NIST STS 2.1.1 测试包	NIST SP 800-22 随机数统计测试套件

4.3 实验方案

实验的主要目的是探究现有熵估计理论的在不同物理条件下的适用性。为此, 一方面我们通过增大采样间隔 N, 进而测量 q_w, 使得计算出理论熵值大于熵充足条件的阈值; 另一方面, 采集当前熵充足条件下的随机数, 验证其特性是否能够通过严格的统计测试。这里的物理条件包括两部分: 芯片制造的差异和环境(电压、温度)的变化。

4.3.1 实验对象

1) 在芯片制造差异研究的实验中, 实验对象是对于同一批次相同工艺下的不同芯片, 观察在输出比特序列熵充足时, 对应的采样间隔参数的大小关系。

2) 在环境条件变化的实验中, 我们的实验目的是对于同一块或几块芯片, 在不同的供电电压(或环境温度)下, 观察在输出比特序列熵充足时, 对应的采样间隔参数的大小关系。

4.3.2 实验方法

1) 芯片制造差异的实验方法, 实验流程见图 5。

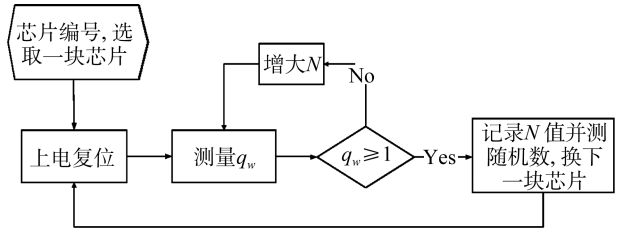

图 5 芯片制造差异实验的流程

具体步骤:

- 第一步: 将同一批次生产的若干个 TRNG 芯片编号, 选取其中一块芯片开始实验。供电电压为 1.2 V, 环境温度是 25℃。
- 第二步: 将芯片上电并复位。
- 第三步: 通过开发板, 测量某一采样间隔参数 N 下得到的 q_w, 判断是否大于等于 1; 若不满足, 则增大参数 N。
- 第四步: 当熵充足条件得以满足并稳定时, 固定参数 N 并记录; 采集此时产生的随机数, 进行统计测试, 记录测试结果。
- 第五步: 换下一块芯片, 继续执行第二步的操作。

2) 环境条件变化的实验方法, 实验流程见图 6。

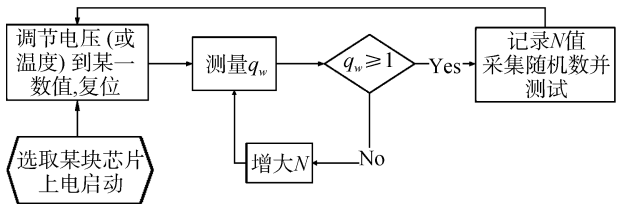

图 6 环境条件变化的实验流程

具体步骤:

➢ 第一步: 将某块 TRNG 芯片上电启动, 初始供电电压为 1.2 V(环境温度为 25℃), 环境温度维持在 25℃(供电电压维持在 1.2 V)。

➢ 第二步: 调节供电电压(环境温度)到某一数值, 将芯片复位。

➢ 第三步: 通过开发板测量某一采样间隔参数 N 下得到的 q_w, 判断是否大于等于 1; 若不满足, 则增大参数 N。

➢ 第四步: 当熵充足条件得以满足并稳定时, 固定参数 N 并记录; 并采集此时产生的随机序列, 进行统计测试, 记录测试结果。然后, 继续执行第二步的操作。

5 实验结果与分析

5.1 制造差异和随机性的关系

我们选取 9 块相同工艺(130 nm)同一批次制造的 TRNG 芯片进行制造差异的测试。实验结果如图 7 所示。其中, 采样间隔参数 N 的取值, 是在熵充足(即 $q_w \geqslant 1$)时得到的。实验时, TRNG 芯片的供电电压保持在 1.2 V, 环境温度保持在 25℃。

从图 7 中看出, 芯片制造差异会影响到每个 TRNG 芯片在实际工作时的随机性大小。具体表现为: 这 9 块芯片在熵充足状态时的采样间隔参数 N 不尽相同, 变化范围在 10240~12800 之间。这里我们每个芯片都做了多次实验, 尽量消除测量随机性带来的影响。这些采样间隔最多差约 25%, 也即是说采样间隔在不同芯片之间最多可能有 25%上下的浮动。需要注意的是, 由于我们测试的是同一批次的芯片, 制造的差异已经尽可能的小, 如果是不同批次的话, 可能还会有更大差别。因此, 这些制造时的差异, 应当充分考虑在设计参数的设定中。

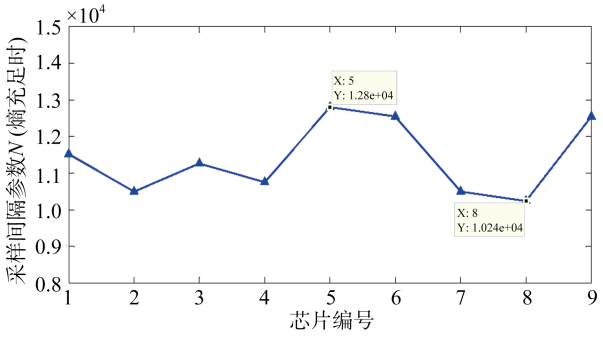

图 7 芯片制造差异和随机性关系

我们任选两块芯片(这里是芯片 1 和芯片 6), 验证表中给出的采样间隔下, TRNG 芯片输出的随机数质量。对输出随机数进行统计检测标准 NIST SP 800-22 的测试。表 3 中展示了 NIST 测试包全部 15 项的测试结果, 被测序列共 1000 组, 每组序列长度为 10^6 比特。检测包括两级检测: 一级检测和二级检测。一级检测关注检测项的通过率, 如果 1000 组中通过某项检测的组数不低于 981, 则说明待测序列达到了该检测项的一级检测要求; 二级检测关注各组序列之间的分布特性是否均匀独立, 如果卡方拟合优度检验结果 $P-value_T \geqslant 0.0001$, 则认为待测序列达到了该项检测的二级检测要求。两级检测都通过, 被测序列则通过了检测。表 3 的测试结果显示, 在所给参数 N 的数值下, 两个 TRNG 芯片产生的随机数均可以顺利通过统计检测。

表 3 NIST 统计检测结果(制造差异)

	芯片 1		芯片 6	
检测项	通过率	$P\text{-}value_T$	通过率	$P\text{-}value_T$
Freq.	991/1000	0.554420	995/1000	0.699313
Block Freq.	993/1000	0.743250	991/1000	0.085587
Cum. Sums	990/1000	0.788728	990/1000	0.534146
Runs	994/1000	0.795017	990/1000	0.657933
Longest Run	993/1000	0.692455	992/1000	0.883171
Rank	995/1000	0.011791	988/1000	0.534146
FFT	992/1000	0.289667	994/1000	0.066882
Overlap. Template (OT)	986/1000	0.299251	991/1000	0.066882
Non-OT	996/1000	0.061517	993/1000	0.213309
Universal	990/1000	0.045675	986/1000	0.015598
Appr. Entropy	991/1000	0.016526	996/1000	0.779188
Random Excursions (RE)	641/643	0.270336	640/643	0.110952
RE Variant	642/643	0.008158	640/643	0.985035
Serial	988/1000	0.278001	989/1000	0.816537
Line. Complexity (LC)	990/1000	0.682134	993/1000	0.851383

5.2 供电电压和随机性的关系

该 TRNG 芯片的正常供电电压是 1.2 V。我们选用一块正常工作的芯片, 将供电电压参数分别设置为 0.6V、0.9 V、1.2 V、1.5 V 和 1.8 V, 观察电压的变化对于随机性的影响, 结果如图 8 所示。实验时, TRNG 芯片的环境温度保持在 25℃。

从图 8 中可以看出, 供电电压的变化(或波动)会影响到 TRNG 芯片在实际工作时的随机性大小。具体表现为: 在供电电压从 0.9 V 渐变到 1.8 V 的过程中, 周期抖动会逐渐减小, 熵充足时对应的采样间隔参数 N 逐渐增大, 也就是说需要更长的时间积累足够多的随机性。而当电压低至 0.6 V, 由于电压过

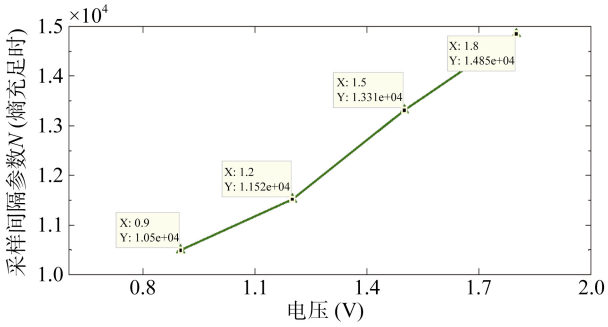

图 8　电压变化和随机性的关系

低导致振荡环无法正常工作。此时, 因电压波动带来的采样间隔变化, 至多会有约 40%。因此, 在设计者实际设计 TRNG 时, 需要考虑到供电电压波动的变化对周期抖动的影响。即便预设的采样间隔可以使得 TRNG 芯片在正常供电电压下, 输出的序列是熵充足, 但在实际运行时, 由于电压波动也会导致熵不足的问题。

我们对不同的电压值下, TRNG 芯片在熵充足时输出的随机数质量进行测试, 结果(如表 4-5 所示)表明在所给参数 N 的数值下, TRNG 芯片产生的随机数均可以顺利通过统计检测。这证实了熵估计理论此时仍然是可用的。

5.3　环境温度和随机性的关系

我们同样选取一块正常工作的 TRNG 芯片, 对其进行环境温度实验。我们将环境温度分别设置在–10℃、0℃、10℃、25℃、40℃, 观察温度的变化对于随机性的影响, 结果如图 9 所示。实验时, TRNG 芯片的供电电压保持在 1.2 V。

表 4　NIST 统计检测结果 1(电压变化)

	0.9 V		1.2 V	
检测项	通过率	$P\text{-}value_T$	通过率	$P\text{-}value_T$
Freq.	987/1000	0.350485	991/1000	0.554420
Block Freq.	994/1000	0.595549	993/1000	0.743250
Cum. Sums	993/1000	0.779188	990/1000	0.788728
Runs	985/1000	0.699313	994/1000	0.795017
Longest Run	996/1000	0.304126	993/1000	0.692455
Rank	992/1000	0.657933	995/1000	0.011791
FFT	990/1000	0.401199	992/1000	0.289667
Overlap. Template (OT)	995/1000	0.616305	986/1000	0.299251
Non-OT	991/1000	0.360851	996/1000	0.061517
Universal	983/1000	0.066882	990/1000	0.045675
Appr. Entropy	998/1000	0.115387	991/1000	0.016526
Random Excursions (RE)	641/643	0.275709	641/643	0.270336
RE Variant	640/643	0.437274	642/643	0.008158
Serial	997/1000	0.304126	988/1000	0.278001
Line. Complexity (LC)	996/1000	0.637119	990/1000	0.682134

表 5　NIST 统计检测结果 2(电压变化)

	1.5 V		1.8 V	
检测项	通过率	$P\text{-}value_T$	通过率	$P\text{-}value_T$
Freq.	993/1000	0.051942	995/1000	0.350485
Block Freq.	990/1000	0.534146	991/1000	0.699313
Cum. Sums	995/1000	0.657933	996/1000	0.213309
Runs	988/1000	0.759756	993/1000	0.971699
Longest Run	995/1000	0.935716	990/1000	0.657933
Rank	992/1000	0.897763	994/1000	0.514124
FFT	997/1000	0.935716	982/1000	0.554420
Overlap. Template (OT)	989/1000	0.122325	993/1000	0.304126
Non-OT	991/1000	0.304126	992/1000	0.224821
Universal	985/1000	0.657933	996/1000	0.719747
Appr. Entropy	991/1000	0.122325	994/1000	0.304126
Random Excursions (RE)	641/643	0.514124	640/643	0.306232
RE Variant	640/1000	0.554420	641/643	0.450564
Serial	983/1000	0.779188	986/1000	0.102526
Line. Complexity (LC)	987/1000	0.834308	991/1000	0.534146

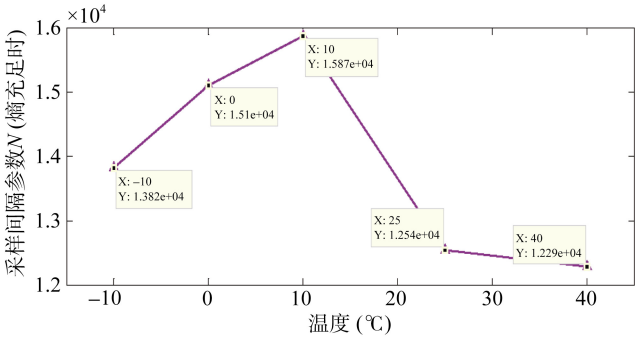

图 9　温度变化和随机性的关系

从图 9 中可以发现, 环境温度的变化会影响到 TRNG 芯片在实际工作时的随机性大小。具体表现为: 在环境温度从–10℃逐步增加到 40℃的过程中, 周期抖动会增大, 但与此同时, 振荡周期也会增大, 因此, 熵充足时对应的采样间隔参数 N 的变化并不是单调的, 而是呈现先增大后减小的趋势。此时, 由于温度变化带来的采样间隔变化, 至多会有约 30%的差距。因此, 在设计者实际设计 TRNG 时, 也要考虑到温度变化对于随机性的影响。因为 TRNG 芯片提供随机数服务可能是一个长期的过程, 运行环境的温度可能会有较大变化(例如一些室外运行的设备)。

为验证模型有效性, 我们对不同的温度下, TRNG 芯片在熵充足时输出的随机数质量进行测试,

结果(如表 6-7 所示)表明在所给参数 N 的数值下, TRNG 芯片产生的随机数均可以顺利通过统计检测。这证实, 在这些温度下熵估计理论仍然可用。

表 6 NIST 统计检测结果 1(温度变化)

	−10℃		0℃	
检测项	通过率	$P\text{-}value_T$	通过率	$P\text{-}value_T$
Freq.	992/1000	0.834308	984/1000	0.739918
Block Freq.	990/1000	0.350485	983/1000	0.637119
Cum. Sums	989/1000	0.739918	986/1000	0.236810
Runs	988/1000	0.437274	993/1000	0.678686
Longest Run	991/1000	0.911413	991/1000	0.759756
Rank	994/1000	0.637119	994/1000	0.834308
FFT	993/1000	0.871321	988/1000	0.262249
Overlap. Template (OT)	990/1000	0.956132	995/1000	0.946308
Non-OT	992/1000	0.437223	992/1000	0.191687
Universal	991/1000	0.873295	986/1000	0.798139
Appr. Entropy	990/1000	0.739238	994/1000	0.012650
Random Excursions (RE)	641/643	0.964295	640/643	0.888137
RE Variant	640/643	0.275709	640/643	0.468595
Serial	985/1000	0.213309	992/1000	0.249284
Line. Complexity (LC)	995/1000	0.931732	993/1000	0.924076

表 7 NIST 统计检测结果 2(温度变化)

	10℃		40℃	
检测项	通过率	$P\text{-}value_T$	通过率	$P\text{-}value_T$
Freq.	994/1000	0.390936	996/1000	0.213309
Block Freq.	991/1000	0.964295	991/1000	0.911413
Cum. Sums	988/1000	0.275709	993/1000	0.350485
Runs	985/1000	0.739918	988/1000	0.804337
Longest Run	986/1000	0.964295	990/1000	0.054199
Rank	992/1000	0.534146	992/1000	0.602458
FFT	990/1000	0.762146	991/1000	0.534146
Overlap. Template (OT)	994/1000	0.213309	994/1000	0.949602
Non-OT	987/1000	0.691468	987/1000	0.739918
Universal	993/1000	0.587163	990/1000	0.816328
Appr. Entropy	995/1000	0.238029	993/1000	0.407091
Random Excursions (RE)	642/643	0.090936	641/643	0.122325
RE Variant	642/643	0.162606	641/643	0.834308
Serial	991/1000	0.637119	992/1000	0.911413
Line. Complexity (LC)	996/1000	0.066882	995/1000	0.043745

6 总结与展望

TRNG 在密码学领域扮演着重要角色, 其中一种常见的类型是振荡采样型 TRNG。然而, 在 TRNG 运行期间, 物理条件的变化会对其安全性产生明显影响, 致使密码系统存在安全风险。为此, 基于熵估计理论, 我们研究了不同的物理条件对振荡采样型 TRNG 所含熵值的影响, 所涉及的物理条件包括: 芯片制造的个体差异、供电电压和环境温度。而且, 我们对熵估计理论的适用性也进行了验证。通过实验我们发现: 这些物理条件的变化会对 TRNG 的随机性产生很大影响。此外, 在验证熵估计理论适用性方面, 我们发现在熵充足的情况下, 由于物理条件的变化, 也会导致 TRNG 的安全设计参数(采样间隔)不同。该研究成果对振荡采样型 TRNG 芯片的设计、使用和检测具有重要参考意义。在设计方面, 设计者需要充分地考虑不同的物理条件对于熵源的影响, 从而确保所设计的 TRNG 芯片在最差条件下是安全的; 在使用方面, 使用者需要熟悉 TRNG 芯片所适用的物理条件范围, 以保障 TRNG 是在适用条件范围内安全运行; 在检测方面, 检测者需要根据受检测 TRNG 芯片的制造水平和工作环境条件, 在不同环境条件下测试 TRNG 芯片的安全性, 并检测制造差异对于 TRNG 芯片的影响是否在可接受范围内。

参考文献

[1] Rukhin, A., Soto, J., Nechvatal, J., et al, “A Statistical Suite for Random and Pseudorandom Number Generators for Cryptographic Applications,” *NIST Special Publication* 800–822, Washington, DC, USA, 2010.

[2] The State Cryptography Administration of China, “GM/T 0005-2012 randomness test standard”.
(国家密码管理局, “GM/T 0005-2012 随机性检测规范”)

[3] ISO/IEC JTC 1/SC 27, “Information technology - Security techniques - Random bit generation,” Berlin, Germany, 2011.

[4] Killmann, W., and Schindler, W., “AIS 31: Functionality Classes and Evaluation Methodology for True (Physical) Random Number Generators. Version 3.1,” T-Systems GEI GmbH and Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn, Germany, 2001.

[5] W. Maichen, “Frontiers in Electronic Testing,” Digital Timing Measurements: From Scopes and Probes to Timing and Jitter. New York, NY, USA: Springer, 2010.

[6] H. Bock, M. Bucci, and R. Luzzi, “An Offset-compensated Oscillator-based Random Bit Source for Security Applications,” in Proc. *Cryptographic Hardware and Embedded Systems (CHES’04)*, pp. 268-281, 2004.

[7] M. Epstein, L. Hars, R. Krasinski, M. Rosner, and H. Zheng, “Design and Implementation of a True Random Number Generator based on Digital Circuit Artifacts,” in Proc. *Cryptographic Hardware and Embedded Systems (CHES’03)*, pp. 152-165, 2003.

[8] B. Sunar, W. J. Martin, and D. R. Stinson, “A Provably Secure

True Random Number Generator with Built-in Tolerance to Active Attacks," *IEEE Trans. Computers*, vol.56, no.1, pp. 109-119, Jan. 2007.

[9] Vasyltsov, I., Hambardzumyan, E., Kim, Y.-S., and Karpinskyy, B., "Fast Digital TRNG Based on Metastable Ring Oscillator," in Proc. *Cryptographic Hardware and Embedded Systems (CHES'08)*, pp. 164-180, 2008.

[10] Santoro, R., Sentieys, O., and Roy, S., "On-the-fly evaluation of fpgabased true random number generator," in Proc. *IEEE Computer Society Annual Symposium on VLSI (ISVLSI'09)*, pp. 55-60, 2009.

[11] Fischer, V., and Lubicz, D., "Embedded Evaluation of Randomness in Oscillator Based Elementary TRNG," in Proc. *Cryptographic Hardware and Embedded Systems (CHES'14)*, pp. 527-543, 2014.

[12] Rahman, M. T., Xiao, K., Forte, D., Zhang, X., Shi, J., and Tehranipoor, M., "TI-TRNG: technology independent true random number generator," in Proc. *Annual Design Automation Conference (DAC'14)*, pp. 179:1-179:6, 2014.

[13] Markettos, A. T., and Moore, S. W., "The Frequency Injection Attack on Ring-Oscillator-Based True Random Number Generators," in Proc. *Cryptographic Hardware and Embedded Systems, (CHES'09)*, pp. 317-331, 2009.

[14] Killmann, W., and Schindler, W., "A Design for a Physical RNG with Robust Entropy Estimators," in Proc. *Cryptographic Hardware and Embedded Systems (CHES'08)*, pp. 146-163, 2008.

[15] Ma, Y., Lin, J., Chen, T., Xu, C., Liu, Z., and Jing, J., "Entropy Evaluation for Oscillator-Based True Random Number Generators," in Proc. *Cryptographic Hardware and Embedded Systems (CHES'14)*, pp. 544-561, 2014.

[16] Baudet, M., Lubicz, D., Micolod, J., and Tassiaux, A., "On the Security of Oscillator-Based Random Number Generators," *J. Cryptology*, vol. 24, no. 2, pp. 398-425, May 2011.

[17] Varchola, M., and Drutarovsky, M., "New High Entropy Element for FPGA Based True Random Number Generators," in Proc. *Cryptographic Hardware and Embedded Systems (CHES'10)*, pp. 351-365, 2010.

[18] Cherkaoui, A., Fischer, V., Fesquet, L., and Aubert, A., "A Very High Speed True Random Number Generator with Entropy Assessment," in Proc. *Cryptographic Hardware and Embedded Systems (CHES'13)*, pp. 179-196, 2013.

[19] Haddad, P., Fischer, V., Bernard, F., and Nicolai, J., "A Physical Approach for Stochastic Modeling of TERO-Based TRNG," in Proc. *Cryptographic Hardware and Embedded Systems (CHES'15)*, pp. 357-372, 2015.

[20] Rozic, V., Yang, B., Dehaene, W., and Verbauwhede, I., "Highly efficient entropy extraction for true random number generators on FPGAs," in Proc. *Annual Design Automation Conference (DAC'15)*, pp. 116:1-116:6, 2015.

[21] Golic, J. D., "New Methods for Digital Generation and Postprocessing of Random Data," *IEEE Trans. Computers*, vol. 55, no. 10, pp. 1217-1229, Dec. 2006.

[22] Wieczorek, P. Z., and Golofit, K., "Dual-Metastability Time-Competitive True Random Number Generator," *IEEE Trans. on Circuits and Systems*, vol. 61-I, no. 1, pp. 134-145, Sep. 2014.

[23] PUB, N. F., "140-2: Security Requirements for Cryptographic Modules". Washington, DC, USA, 2001.

[24] Haddad, P., Teglia, Y., Bernard, F., and Fischer, V., "On the Assumption of Mutual Independence of Jitter Realizations in P-TRNG Stochastic Models," in Proc. *Design, Automation & Test in Europe Conference & Exhibition (DATE'14)*, pp. 1-6, 2014.

[25] Valtchanov, B., Aubert, A., Bernard, F., and Fischer, V., "Modeling and Observing the Jitter in Ring Oscillators Implemented in FPGAs," in Proc. *Design & Diagnostics of Electronic Circuits & Systems (DDECS'08)*, pp. 158-163, 2008.

陈天宇 于 2011 年在北京科技大学信息与计算科学专业获得理学学士学位。现在中国科学院信息工程研究所攻读博士学位。研究领域为随机数发生器的设计与检测。Email: chentianyu@iie.ac.cn

马原 于 2014 年在中国科学院大学获得博士学位。现任中国科学院信息工程研究所助理研究员。研究领域为随机数发生器的设计与检测、密码算法高速实现。Email: mayuan@iie.ac.cn

荆继武 于 2003 年在中国科学院研究生院获得博士学位。现任中国科学院信息工程研究所副所长。研究领域为网络与系统安全。Email: jingjiwu@iie.ac.cn

朱双怡 于 2015 年在中国科技大学获得理学学士学位。现在中国科学院信息工程研究所攻读博士学位。研究领域为随机数检测技术。Email: zhushuangyi@iie. ac.cn