【光电工程 / Optoelectronic Engineering】

基于布尔网络的低功耗物理随机数发生器

杨 芮^{1,2}, 侯二林^{1,2}, 刘海芳^{1,2}, 龚利爽^{1,2}, 王云才^{1,2,3}, 张建国^{1,2}

1) 太原理工大学物理与光电工程学院, 山西太原 030024; 2) 太原理工大学新型传感器与智能控制教育部和山西省重点实验室, 山西太原 030024; 3) 广东工业大学信息工程学院, 广东广州 510006

摘 要: 利用布尔网络设计一种低功耗物理随机数发生器, 熵源部分为 12 个二输入逻辑门相互耦合及 1 个反向器构成的自治布尔网络, 并从时域、频域及计算最大李雅普诺夫指数等方面分析其产生信号的混沌特性. 经过对该混沌信号采样和量化, 生成熵值为 1 bit/sample、实时产生速率为 100 Mbit/s 的随机序列. 整个物理随机数发生器在现场可编程逻辑阵列(field programmable gate array, FPGA)平台上实现, 硬件逻辑资源消耗少. 美国国家标准与技术研究院的随机数测试程序结果表明, 产生的随机数具有良好的随机统计特性. 该设计可应用于高速加密系统、保密通信等信息安全领域.

关键词: 物理电子学; 保密通信; 布尔网络; 混沌; 物理随机数发生器; 现场可编程逻辑阵列

中图分类号: TN918

文献标志码: A

doi: 10.3724/SP.J.1249.2020.01051

Low-power physical random number generator using Boolean networks

YANG Rui^{1,2}, HOU Erlin^{1,2}, LIU Haifang^{1,2}, GONG Lishuang^{1,2},
WANG Yuncai^{1,2,3}, and ZHANG Jianguo^{1,2}

1) College of Physics and Optoelectronics, Taiyuan University of Technology, Taiyuan 030024, Shanxi Province, P. R. China

2) Key Laboratory of Advanced Transducers and Intelligent Control System of Ministry of Education and Shanxi Province, Taiyuan University of Technology, Taiyuan 030024, Shanxi Province, P. R. China

3) School of Information and Engineering, Guangdong University of Technology, Guangzhou 510006, Guangdong Province, P. R. China

Abstract: In order to reduce the power consumption of random number generators (RNGs), a novel physical random number generator (physical-RNG) using Boolean networks is presented. The entropy source is an autonomous Boolean network consisting of 12 two-input logic gates and a inverter, the chaotic characteristics of the generated signal are verified by time domain analysis, frequency domain analysis, and the computation of the maximum Lyapunov exponent. By sampling and quantizing chaotic signals, the physical random number with entropy of 1 bit/sample and real time rate 100 Mbit/s is generated. The physical-RNG is implemented on a field programmable logic array (FPGA) platform with low consumption of hardware logic resources. The NIST SP 800-22 test results indicate that the generated random number has good random characteristics. The design can be applied in the information security fields such as high-speed encryption systems and secure communications.

Received: 2019-02-25; **Accepted:** 2019-04-25

Foundation: National Natural Science Foundation of China (61671316, 61731014, 61775158); Research Project of Shanxi Scholarship Council of China (2017-key-2); Natural Science Foundation of Shanxi Province (201801D121145)

Corresponding author: Professor ZHANG Jianguo. E-mail: zhangjianguo@tyut.edu.cn

Citation: YANG Rui, HOU Erlin, LIU Haifang, et al. Low-power physical random number generator using Boolean networks [J]. Journal of Shenzhen University Science and Engineering, 2020, 37(1): 51-56. (in Chinese)

Key words: physical electronics; secret communication; Boolean networks; chaos; physical random number generator; field programmable gate array

随机数在蒙特卡洛仿真、深度学习、随机建模和密码学等领域具有广泛应用. 密码学的安全算法和加密协议依托随机数生成不可预测的随机数密钥. 因此, 高质量的随机数对保证系统的信息安全尤为重要. 随机数发生器分为伪随机数发生器和物理随机数发生器. 前者主要通过特定算法产生, 但其输出序列具有周期性, 可被预测和还原, 不适于安全保密性要求高的信息安全领域. 物理随机数源于物理熵源, 具有无周期、不可预测及不重复等特点, 满足信息安全系统对随机数不确定性的要求.

激光器的相位噪声^[1]、混沌激光^[2-3]及光的量子效应^[4]等都可以作为产生物理随机数的熵源, 而基于电路的物理随机数发生器具有低功耗、可集成及易于在可编程平台上实现等优点, 得以广泛应用. 利用电路产生物理随机数的方法主要包括: 基于模拟电路结构的直接放大噪声法和离散时间混沌法; 基于数字电路结构的振荡采样法和亚稳态采样法. 直接放大噪声法^[5]通过放大电路中电阻的热噪声, 与阈值比较产生随机序列. 由于电阻噪声中的噪声幅值很小, 需要高增益的运放器进行放大, 而放大器有限的带宽和失调导致随机性变差. 离散时间混沌法^[6]利用混沌电路的不可预测及初值敏感性产生随机数, 但由于电路设计复杂, 很难同时满足高速和低功耗的要求. 振荡器采样法^[7]通过低频信号采样高频信号, 利用时钟抖动作为随机源产生随机序列, 但占空比失谐引起的统计偏差需进行后续处理. 亚稳态是指电路无法在某个规定的时间内达到一个可确认的状态, 当任何数字电路元件一旦进入亚稳状态, 电路的输出将会取决于电路的噪声特性, 而变得具有随机性, 由此输出 0 或 1 的随机序列, 即亚稳态采样法^[8]. 由于电路中亚稳态持续时间较短, 且对温度和电压的变化比较敏感, 产生随机数的速率较慢.

布尔混沌是自治网络中的一种物理现象, 其表现出随机性持续振荡, 且可以产生带宽较高的信号, 因此, 成为随机数发生器的理想熵源. 2013 年, ROSIN 等^[9]提出一种基于自治布尔网络产生物理随机数的方法, 但该方法采用自反馈结构作为物理熵源, 从而引入相关性. 2017 年, DONG 等^[10]对此电路进行改进, 提出每个节点均增添多个反向器的时延自反馈结构. 然而这两种方法均是三输入

结构, 物理随机数发生器的功耗较高.

本研究提出一种基于二输入 12 节点相互耦合及 1 个反向器构成自治布尔网络作为物理随机数发生器 (physical random number generator, physical-RNG) 的熵源, 节点数目的减少使该随机数发生器所占用的逻辑资源降低, 从而降低功耗. 在逻辑元器件的制造过程中, 二输入逻辑门需要的晶体管数量约为三输入的一半, 进一步降低功耗. 该熵源产生带宽为 700 MHz 的混沌信号, 通过 D 触发器采样及量化, 随机序列的香农熵达到 1 bit/sample. 整个物理随机数发生器在可编程逻辑阵列 (field programmable gate array, FPGA) 平台上实现, 逻辑资源消耗极少. 美国国家标准与技术研究院 (National Institute of Standards and Technology, NIST) 随机数测试结果表明, 所产生的随机数具有良好的随机统计特性.

1 熵源模拟

本研究提出的物理随机数发生器结构如图 1, 12 个逻辑运算的节点相互耦合构成网络拓扑结构. 其中, 节点 1 执行三输入异或非 (XNOR) 运算; 2 个输入源于节点 2 和节点 3, 另一个输入来源于反相器; 其余节点均执行二输入异或 (XOR) 运算. 布尔延迟方程^[11] (Boolean delay equation) 可对节点数为 N 的自治布尔网络进行动态分析,

$$x_n(t) = f_n[t, x_1(t - \tau_{n1}), x_2(t - \tau_{n2}), \dots, x_n(t - \tau_{nm})] \quad (1)$$

图 1 物理随机数发生器结构

Fig. 1 Physical random number generator structure

其中, τ_{nm} 为节点 n 到节点 m 的延迟时间; $x_n(t)$ 为节点 n 在 t 时刻的逻辑状态; f_n 为节点 n 执行的逻辑函数。

仿真结果表明, 当 $\tau_{mn} \neq \tau_{nm}$ 时, XNOR 节点输出的信号呈随机混乱状态, 如图 2; 当 $\tau_{mn} = \tau_{nm}$ 时, 网络动态特性无法确定。由于逻辑器件本身的特性, 无法响应转换速度过快的信号, 即所谓的低通滤波效应^[12-13]。布尔网络的振荡频率 f 与节点数目 N 成反比, 当节点数量较小时, 振荡频率较高, 网络无法响应频率过高的信号, 使得该信号被衰减和抑制, 导致振荡停止。随着节点数目的增加, f 逐渐降低, 当 f 低于截止频率时, 网络出现持续性振荡。因此, 需要通过增加节点数目来增加信号的延迟时间, 使网络持续振荡。

图2 布尔网络动态仿真结果

Fig. 2 Dynamic simulation results of Boolean networks

2 熵源实验分析

2.1 混沌熵源电路特性

基于自治布尔网络作为熵源的物理随机数发生器由熵源和熵提取两部分构成。熵源由 12 个节点相互耦合及 1 个反向器构成自治布尔网络, 每个节点均可以产生持续振荡信号。熵提取部分由 1 个三输入 XOR 逻辑门和 3 个 D 触发器组成。3 个 D 触发器分别对节点 1、5 及 9 输出的混沌时序进行采样, 对采样的序列经过 XOR 处理, 进一步降低序列间的相关性和偏差。通过观测 XNOR 节点的电压输出, 分析信号的物理特性。图 3 (a) 为熵源输出信号的时序图, 可见, 该信号呈现复杂且无序的振荡; 图 3 (b) 为熵源输出信号的频谱图, 输出熵源频谱带宽可达 700 MHz (下降 10 dB 带宽); 图 3

(c) 为熵源输出信号的自相关曲线, 结果显示该信号的半高全宽 (full width at half maximum, FWHM) 约为 1 ns。频谱的宽度及较短的自相关时间意味着可以从中提取速率较高的物理随机序列。

(a) 时序图

(b) 频谱图

(c) 自相关曲线

图3 熵源输出信号的时序、频谱及自相关曲线

Fig. 3 Temporal evolution, spectrum and auto-correlation of entropy source output signal

李雅普诺夫指数是混沌动力学特性的一种重要表征方式。最大李雅普诺夫指数为正值即证明该系统为混沌系统^[14]。根据文献[15]的方法, 计算熵源输出信号的最大李雅普诺夫指数 $\lambda_{\max} = 0.36 \text{ ns}^{-1}$, 结果如图 4, 表明输出振荡信号具有混沌特性。其中, d 为轨迹的分离距离。

图 4 熵源信号的最大李雅普诺夫指数

Fig. 4 The maximum Lyapunov exponent of signal generated by entropy source

2.2 熵值分析

熵值可描述信息的不可预测性. 熵值越大, 表示信息的不可预测性越高. 对于长度为 n 的二进制序列 X , 其香农熵为

$$H(X) = - \sum_{i=1}^n p(x_i) \lg p(x_i) \quad (2)$$

其中, $p(x_i)$ 表示 X 的第 i 个元素为 x_i 的概率. 统计由不同数量节点 ($N = 3, 4, \dots, 16$) 构成自治布尔网络的香农熵. 结果如图 5. 可见, 随着 N 的增加, 熵值呈现 3 种不同的状态: ① 当 $N < 4$ 时, 由于低通滤波效应无法产生振荡信号, 此时熵值为 0; ② 当 N 逐渐增大时, 网络中的周期抖动引起小的不确定性, 导致产生低熵; ③ 随着 N 的进一步增大, 受逻辑门退化效应等非理想因素^[9,13] 的影响, 熵值接近于最大值. 需要说明的是, 在经过对节点 1、5 及 9 进行 XOR 处理后, 随机序列的熵值达到了 1 bit/sample, 图 6 为实时速率为 100 Mbit/s 的随机序列. 考虑到随机数发生器的最优功耗, 选择 $N = 12$ 的自治布尔网络作为 physical RNG 的熵源.

图 5 随机序列熵值与节点数目的关系

Fig. 5 The relation between the entropy of random sequence and the number of nodes

图 6 实时速率 100 Mbit/s 的物理随机序列

Fig. 6 Physical random sequence with real-time rate of 100 Mbit/s

3 随机数发生器的硬件实现

该物理随机数发生器 FPGA 部分在可编程逻辑器件 (Altera Cyclone IV, EP4CE10F17C8N) 上实现, 包括熵源及熵提取模块、时钟产生模块、双端口异步先进先出 (first input first output, FIFO) 指令及串口输出, 整体构成如图 7. 在系统时钟的作用下, 熵源模块产生混沌信号, 熵提取模块将信号量化为随机序列. 由于采样时钟和串口时钟是两个不同的时钟, 随机序列需要经过双端口异步 FIFO 对数据进行缓存, 经串口输出模块将数据输出. 由 FPGA 产生的数据经 USB 传输, 上位机接收后, 在 PC 端进行随机性测试. 本研究设计的随机数发生器单个熵源部分仅消耗 13 个逻辑单元 (logic element, LE), 而整个工程所占用的 LE 数量小于整个 FPGA 资源的 1%. 因此, 可根据需要在 FPGA 资源范围内任意添加该 physical-RNG 的路数, 随机数发生器的实时速率可提高至 Tbit/s 级别.

4 随机性测试

对随机数质量的检测通常采用 NIST 发布的随机数测试程序^[16]. 本研究测试了样本容量为 1 Gbit 的随机数. NIST 有 15 个测试项, 设置显著水平值 $\alpha = 0.01$, 测试结果包括 p 值及 proportion, 当 p 值 ≥ 0.01 , proportion > 0.9806 时, 表示通过该项测试. 测试结果如表 1, 可见, 本研究设计的物理随机数发生器产生的 1 Gbit 随机数能够通过所有项的测试, 具备良好的随机性.

图 7 物理随机数发生器的硬件框图
Fig. 7 Hardware of the physical-RNG

表 1 NIST 测试结果
Table 1 NIST test results

测试项	p 值	proportion	测试结果
频率	0.713 801	0.987	通过
块内频率	0.195 557	0.989	通过
累加和	0.718 376	0.991	通过
游程	0.396 862	0.989	通过
块内长游程	0.435 202	0.993	通过
二进制矩阵秩	0.342 361	0.991	通过
离散傅里叶变换	0.968 583	0.985	通过
非重叠模块匹配	0.891 971	0.992	通过
重叠块匹配	0.433 136	0.987	通过
全局通用统计	0.842 073	0.989	通过
近似熵	0.560 970	0.981	通过
随机游动	0.560 970	0.987	通过
随机游动变量	0.903 805	0.993	通过
串行	0.224 293	0.984	通过
线性复杂度	0.466 807	0.989	通过

结 语

本研究通过对自治布尔网络行为的动态仿真模拟，验证其作为物理随机数发生器熵源的可行性。实验分析熵源输出信号的电路特性，结果表明，其

时序呈现复杂无规律的持续振荡，频谱带宽可达 700 MHz，半高全宽约为 1 ns。李雅普诺夫指数的计算结果证明了信号的混沌特性，熵值分析结果表明，当选择以 12 个节点构成的自治布尔网络作为物理熵源时，随机数发生器的功耗及随机序列的质量得以最优化。将通过仿真模拟及实验验证的物理随机数发生器在可编程逻辑器件上实现，提取实时产生速率为 100 Mbit/s 的物理随机数进行 NIST 测试，结果表明，该随机数发生器产生的随机序列具有良好的随机统计特性。本设计仅用 13 个逻辑器件就产生了实时速率为 100 Mbit/s 的物理随机数产生，通过多路复用方式，随机数的产生速率可达 Gbit/s。本设计具有高速、低功耗及易集成等特点，在高速加密系统中具有广泛应用前景。

基金项目：国家自然科学基金资助项目（61671316，61731014，61775158）；山西省回国留学人员科研基金资助项目（2017-重点-2）；山西省自然科学基金资助项目（201801D121145）
作者简介：杨 芮（1992—），太原理工大学硕士研究生。研究方向：宽带混沌的产生及应用。E-mail: 18354255713@163.com
引 文：杨 芮，侯二林，刘海芳，等. 基于布尔网络的低功耗物理随机数发生器[J]. 深圳大学学报理工版，2020，37（1）：51-56.

参考文献 / References:

[1] QI Bing, CHI Y M, LO H K, et al. High-speed quantum random number generation by measuring phase noise of a single-mode laser [J]. Optics Letters, 2010, 35 (3): 312-314.
[2] LI Pu, WANG Yuncui, ZHANG Jianzhong. All-optical fast random number generator [J]. Optics Express, 2010, 18(19): 20360-20369.
[3] WANG Anbang, LI Pu, ZHANG Jianguo, et al. 4.5 Gbps

- high-speed real-time physical random bit generator [J]. Optics Express, 2013, 21(17): 20452-20462.
- [4] KWON O, CHO Y W, KIM Y H. Quantum random number generator using photon-number path entanglement [J]. Applied Optics, 2009, 48(9): 1774-1778.
- [5] PETRIE C S, CONNELLY A. A noise-based IC random number generator for applications in cryptography [J]. IEEE Transactions on Circuits & Systems I: Fundamental Theory & Applications, 2000, 47(5): 615-621.
- [6] GALAJDA M P. Chaos-based true random number generator embedded in a mixed-signal reconfigurable hardware [J]. Journal of Electrical Engineering, 2006, 57(4): 218-225.
- [7] 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.
- [8] WIECZOREK P Z, GOLOFIT K. Dual-metastability time-competitive true random number generator [J]. IEEE Transactions on Circuits and Systems, 2014, 61(1): 134-145.
- [9] ROSIN D P, RONTANI D, GAUTHIER D J. Ultrafast physical generation of random numbers using hybrid Boolean networks [J]. Physical Review E, 2013, 87(4): 040902.
- [10] DONG Lihua, YANG Hui, ZENG Yong. Analysis and improvement of true random number generator based on autonomous Boolean network [C]// The 13th International Conference on Computational Intelligence and Security. Hong Kong, China: IEEE, 2017, 1: 243-247.
- [11] GHIL M, ZALIAPIN I, COLUZZI B. Boolean delay equations: a simple way of looking at complex systems [J]. Physica D: Nonlinear Phenomena, 2008, 237(23): 2967-2986.
- [12] CAVALCANTE H L, GAUTHIER D J, SOCOLAR J E, et al. On the origin of chaos in autonomous Boolean networks [J]. Philosophical Transactions Mathematical Physical & Engineering Sciences, 2009, 368(1911): 495-513.
- [13] ROSIN D P, RONTANI D, GAUTHIER D J, et al. Experiments on autonomous Boolean networks [J]. Chaos, 2013, 23(2): 025102.
- [14] FRAGA L L, TLELO C E. Optimizing the maximum Lyapunov exponent and phase space portraits in multi-scroll chaotic oscillators [J]. Nonlinear Dynamics, 2014, 76(2): 1503-1515.
- [15] ROSENSTEIN M T, COLLINS J J, LUCA C D. A practical method for calculating largest Lyapunov exponents from small data sets [J]. Physica D: Nonlinear Phenomena, 1993, 65(1/2): 117-134.
- [16] RUKHIN A L, SOTO J, NECHVATAL J R, et al. A statistical test suite for random and pseudorandom number generators for cryptographic applications [R/OL]. [2019-02-01]. <https://dl.acm.org/citation.cfm?id=2206233>.

【中文责编：方 圆；英文责编：溯 心】