基于布尔混沌的物理随机数发生器

张琪琪[1,2]，张建国[1,2]，李璞[1,2]，郭龑强[1,2]，王云才[1,2]
（1. 太原理工大学新型传感器与智能控制教育部山西省重点实验室，山西 太原 030024；
2. 太原理工大学物理与光电工程学院，山西 太原 030024）

摘 要：提出了一种利用布尔混沌熵源产生物理随机数的方法。采用二输入逻辑门构建无自反馈自治布尔网络，并详细分析了该网络动力学特性。在此基础上，利用 FPGA 实现了 15 节点无自反馈自治布尔网络，产生出带宽约 680 MHz，最小熵接近于 1 的布尔混沌信号。以该信号为熵源，结合熵提取电路完成了实时速率达 100 Mbit/s 的物理随机数产生。NIST SP800-22 及 DIEHARD 随机数检测结果表明，利用布尔混沌熵源产生的物理随机序列可通过所有测试项，具有良好的随机统计特性。

关键词：布尔混沌；自治布尔网络；物理随机数发生器；现场可编程门阵列
中图分类号：TN918
文献标识码：A
doi: 10.11959/j.issn.1000−436x.2019014

Boolean-chaos-based physical random number generator

ZHANG Qiqi[1,2], ZHANG Jianguo[1,2], LI Pu[1,2], GUO Yanqiang[1,2], WANG Yuncai[1,2]
1. Key Laboratory of Advanced Transducers and Intelligent Control System, Ministry of Education and Shanxi Province, Taiyuan University of Technology, Taiyuan 030024, China
2. College of Physics and Optoelectronics, Taiyuan University of Technology, Taiyuan 030024, China

Abstract: A novel method for generating physical random numbers using Boolean-chaos as the entropy source was proposed. An autonomous Boolean network (ABN) without self-feedback was constructed by using two-input logic gates, and its dynamic characteristics were analyzed. Based on this, a 15-node ABN circuit was implemented to successfully generate Boolean-chaos with a bandwidth of ~680 MHz and a min-entropy around 1. By implementing the entropy source and the entropy extraction circuit on a single FPGA, the physical random number generation with a real-time rate of 100 Mbit/s was finally achieved. The NIST SP800-22 and DIEHARD randomness test results demonstrate that the obtained random sequences by the method successfully pass all tests. This indicates the random numbers has good random statistical characteristics.

Key words: Boolean-chaos, autonomous Boolean network, physical random number generator, field programmable gate array

1 引言

随机数被广泛应用于蒙特卡洛仿真、深度学习、身份认证、密码学等领域[1-4]，尤其在密码学中，不可预测、统计无偏的物理随机数是确保加密信息安全的关键。

目前，很多随机数发生器（RNG，random number generator）是通过计算机或微处理器运行某种确定性的数学算法（如线性同余、线性反馈移位等）来产生伪随机数；但伪随机数具有周期性，存在可被预测的安全隐患，因此伪随机数发生器（PRNG，pseudo-random numbers generator）难以确

收稿日期：2018−05−08；**修回日期**：2018−12−04
通信作者：王云才，wangyc@tyut.edu.cn
基金项目：国家自然科学基金资助项目（No.61731014，No.41604127，No.41704147，No.61505136，No.61475111，No.61775158）
Foundation Item: The National Natural Science Foundation of China (No.61731014, No.41604127, No.41704147, No.61505136, No.61475111, No.61775158)

保加密信息的安全。

与 PRNG 不同，物理随机数发生器（Physical-RNG，physical random number generator）可以产生无周期、不可预测的物理随机数，这对于数据加密技术来说，是真正安全的。目前，Physical-RNG 主要利用不可预测的物理随机过程作为熵源（也称为物理熵源）来产生随机序列，例如电路中的热噪声[5]、振荡器的相位抖动[6]及非线性系统中的混沌[7]等。电路热噪声 Physical-RNG 由于热噪声幅度较小，需要高增益运算放大器进行放大，而放大器不仅功耗大，其有限的带宽和失调还会使 Physical-RNG 的随机特性变差。振荡器 Physical-RNG 利用低频时钟源的随机相位抖动来获取随机数序列，然而该技术存在随机数产生速率较低的不足。混沌是由非线性系统产生的一种类噪声信号，它具有对初值敏感、不可预测等特点[8]，因而在 Physical-RNG 设计中得到了广泛的应用，如利用离散混沌迭代[9]、时空混沌[10]、多混沌系统耦合[11]、无简并高维离散超混沌[12]等方法都可以产生高质量的随机数。然而，上述混沌系统都属于数字混沌系统，存在混沌退化效应[13]，其产生的随机数本质上都是伪随机的[8-13]。

2013 年，一种结构简单的可集成式 Physical-RNG 被报道，该方法利用带有自反馈结构的自治布尔网络作为物理熵源，实现了速率为 100 Mbit/s（单个 Physical-RNG 单元）的物理随机数产生[14]。但是自反馈结构会引入相关性，使得该物理熵源使用了较多、较复杂的节点（16 个三输入逻辑门）以保证产生足够的熵值。

本文提出并实验验证了一种无自反馈结构的自治布尔网络物理熵源，它由多个二输入异或门节点组成。在文中，使用了节点数量为 15 的网络结构，产生了带宽达 680 MHz，最小熵接近于 1 的布尔混沌信号。利用该熵源构建的 Physical-RNG 具有实时速率为 100 Mbit/s（单个 Physical-RNG 单元）的物理随机数产生能力。相比于文献[14]，本方法具有两项突出优势：1) 物理熵源结构更为简单，最少可由 15 个节点组成；2) 所提出的 Physical-RNG 拥有更低的功耗，这是因为在电路制造过程中，二输入逻辑门比三输入逻辑门使用更少的晶体管（约为三输入逻辑门使用数的一半），而较少的晶体管意味着更低的功耗。随机性测试结果表明，本方法产生的物理随机数序列可成功通过 NIST SP800-22 及 DIEHARD 所有测试项，因而具有良好的随机统计特性。

2 布尔混沌物理熵源

2.1 无自反馈结构的自治布尔网络特征

本文提出的无自反馈结构的自治布尔网络由 N 个节点（二输入逻辑门）组成，其结构如图 1 所示，N 个节点以双向耦合连接方式组成环状拓扑结构。在该网络中，N-1 个节点执行异或（xor）运算，一个节点执行异或非（xnor）运算。经数值仿真，发现所设计的自治布尔网络存在 2 种状态：振荡状态与非振荡状态。当自治布尔网络中节点数量是 3 的倍数时（即 N=3n，n 为正整数），该网络进入振荡状态；否则进入非振荡状态，即进入所谓的布尔固定点[15]。

为了验证上述情况，在 FPGA 中搭建了节点个数分别为 N=3,4,5,…,11 的自治布尔网络，并通过观测 xnor 的电压输出来判定网络状态。实验结果如图 2 所示，当 N=5,7,8,10,11 时，xnor 的输出电压保持恒定，表明网络进入了布尔固定点；当 N= 6,9 时，xnor 的输出电压持续变化，表明网络处于振荡状态。但是需要说明的是，实验中当 N = 3 时，网络并未进入振荡状态，与仿真结果不符，其原因是如下。1) FPGA 中的逻辑门并非响应速度无限快的理想器件，无法响应变化速度过快的信号，即存在所谓的低通滤波效应[15-16]。2) 自治布尔网络处于振荡状态时，其振荡频率 f 与节点数量 N 成反比。当 N=3 时，振荡频率 f 较高，高频振荡信号无法被网络中的逻辑门节点响应（即低通滤波效应），因此振荡信号被衰减和抑制，导致振荡停止，如图 2(a)所示；而随着节点数量 N 的增加（如 N = 6,9,…），自治布尔网络的振荡频率 f 逐渐降低，当 f 小于低通滤波效应的截止频率时，自治布尔网络表现出持续振荡，如图 2(d)和图 2(g)所示。

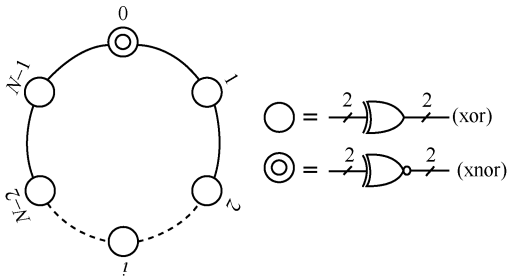

图 1 二输入逻辑门节点组成的自治布尔网络

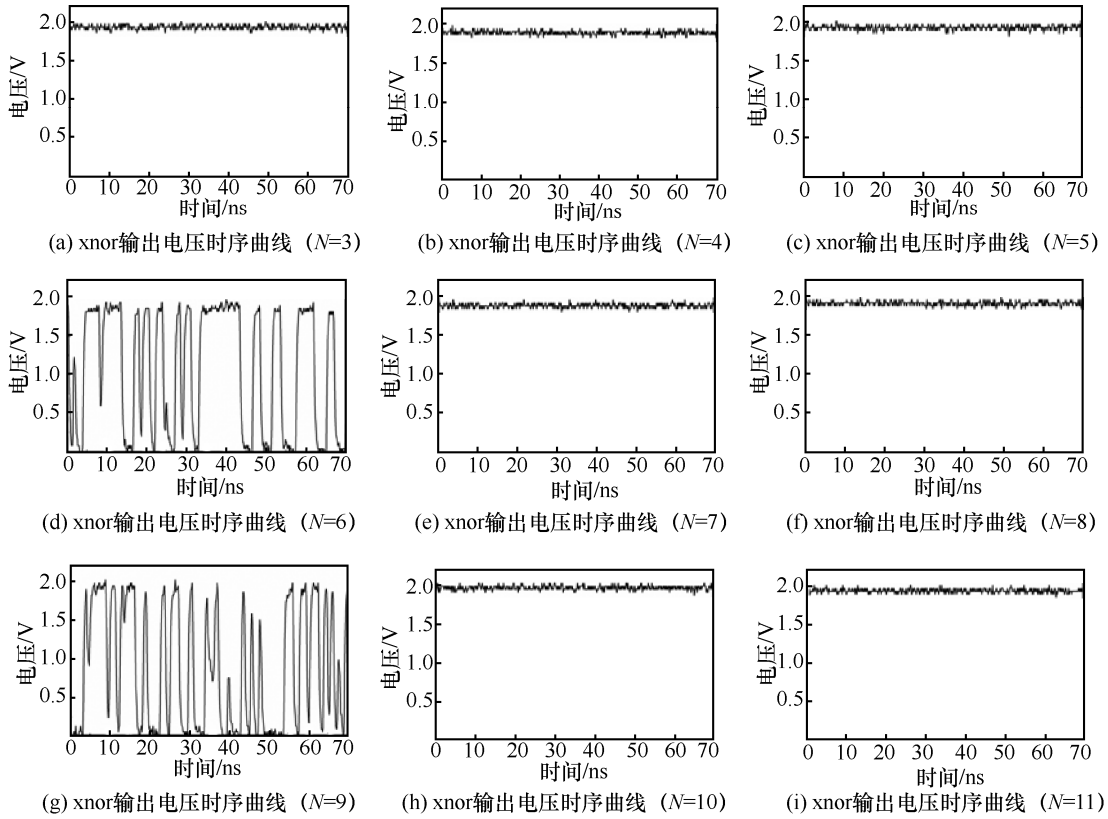

图 2　N 分别为 3~11 时节点自治布尔网络中 xnor 输出电压时序

2.2　布尔混沌的产生及动力学行为

布尔混沌是由自治布尔网络电路产生的一种幅值呈二值变化（逻辑高电平和逻辑低电平），触发时间（相邻 2 个上升沿的时间间隔）呈混沌变化的信号。其产生的动力学原因是自治布尔网络中电子逻辑器件固有的非理想特性，包括低通滤波效应、退化效应等[15-16]。

经 2.1 节分析可知，所设计自治布尔网络要保持振荡状态，其节点个数必须满足 N=3n（n 为大于或等于 2 的正整数）。本部分从最大李雅普诺夫指数与最小熵这 2 个方面进一步分析了振荡状态下自治布尔网络的动力学特性。参照文献[17]，计算了 N≥6 时自治布尔网络输出信号的最大李雅普诺夫指数（λ_{max}）。如图 3 所示，λ_{max} 均大于 0，表明这些网络均产生了布尔混沌信号[18-19]。进一步研究发现，随着节点数量 N 的增加，布尔混沌信号的最大李雅普诺夫指数也随之增大，当 N≥12 时，最大李雅普诺夫指数达到极大值，之后其变化趋势逐渐平稳；因此，为了产生高质量的布尔混沌信号，应选取 N≥12 的自治布尔网络。同时，利用最小熵对所产生布尔混沌的随机特性进行了分析，最小熵接近于 1 则表明布尔混沌信号完全随机且独立同分布，适合作为 Physical-RNG 的物理熵源。实验测量了 N≥6 时布尔混沌信号的最小熵，实验结果如图 3 所示。从图中可观察到，当自治布尔网络的节点数 N≥15 时，所产生的布尔混沌信号的最小熵趋近于 1，之后趋势逐渐平稳，因此，作为 Physical-RNG 的物理熵源，应选取 N≥15 的自治布尔网络。

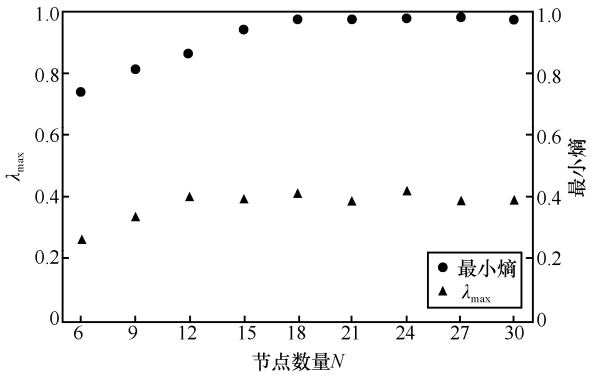

图 3　自治布尔网络（N≥6）的最大李雅普诺夫指数与最小熵

2.3　布尔混沌物理熵源特性

根据 2.2 节分析结果，同时考虑到自治布尔网络的最优功耗，选择 N = 15 的自治布尔网络作为

Physical-RNG 的熵源。熵源产生的布尔混沌信号的时序曲线、频谱曲线和自相关曲线如图 4 所示，从图 4(a)中可以看出，布尔混沌信号的电压呈现大幅度随机起伏（约 2 V）；从图 4(b)中可以看出，布尔混沌信号的频谱平坦且带宽达 680 MHz；从图 4(c)中可以看出，布尔混沌信号的自相关曲线的半高全宽（FWHM，full width at half maximum）约为 1 ns。较宽的频谱与较短的自相关时间表明可以从该物理熵源中提取高速物理随机数序列。

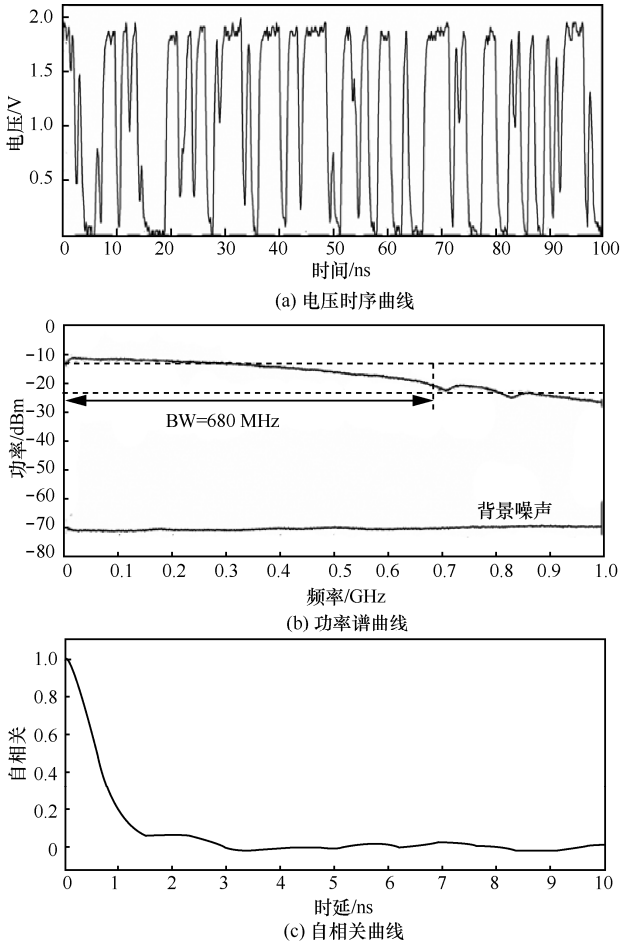

图 4　自治布尔网络（N=15）产生的布尔混沌信号特性

3　物理随机数发生器

本文设计的基于布尔混沌的物理随机数发生器结构如图 5(a)所示，由两部分构成：物理熵源和熵提取电路。物理熵源以节点个数 N=15 的自治布尔网络构成，布尔混沌信号可以由其中任意节点输出。熵提取电路由一个三输入 xor 逻辑门和 3 个 D 触发器构成，其工作原理如下：由 3 个 D 触发器对节点 0、节点 6 和节点 9 输出的混沌序列进行采样，所采样样本再经异或处理以减少物理随机数中的偏差和相关性，最终产生物理随机数序列。

该 Physical-RNG 已在 FPGA（芯片型号：Altera Cyclone IV FPGA，EP4CE10F17C8N）中进行了实验验证，仅需 16 个逻辑单元（LE，logic element）即可实现，消耗资源极少。实验中，利用 FPGA 的 PLL（phase locked loop）单元产生 100 MHz 信号作为 D 触发器的时钟，此时该 Physical-RNG 的随机数实时产生速率为 100 Mbit/s，图 5(b)为实时产生的随机比特序列。值得一提的是，以目前中等规模 FPGA 芯片的容量及规模（如 Cyclone V 的 LE 单元数量为 3×10^5 左右[20]），其内部可以同时构建数万个该 Physical-RNG 结构，此时物理随机数的实时产生速率可至太比特每秒量级，因此，本技术在海量随机数应用领域有着广阔的发展前景。

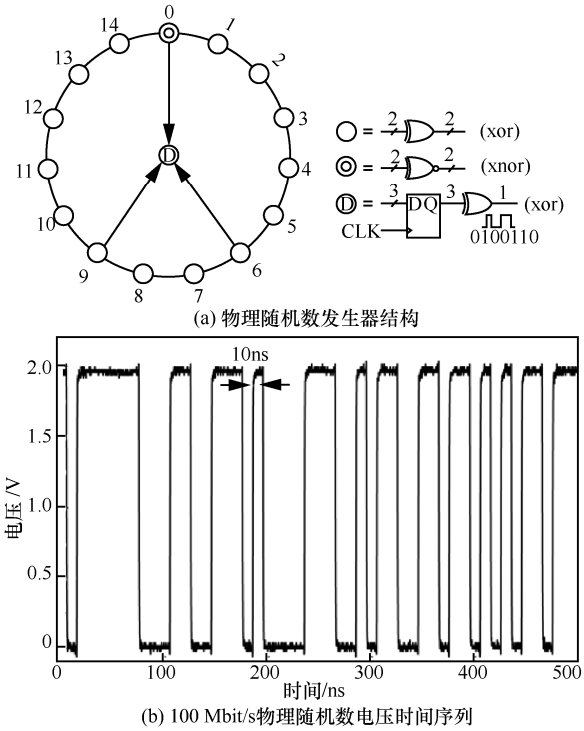

图 5　实时速率为 100 Mbit/s 的物理随机数发生器及产生的信号

4　随机性测试

为了评估基于布尔混沌的 Physical-RNG 产生随机序列的随机性，应用了 2 种国际通用的随机性测试检验标准，分别为 NIST SP800-22[21] 和 DIEHARD[22]，测试的物理随机数样本量均为 1 Gbit。NIST SP800-22 由美国标准局发布，包含 15 项统计测试，每项测试均会针对测试本文数据生成一个 P

值，测试需要 1 000 组数据，每组数据为 1 Mbit。DIEHARD 由 George Marsaglia 发布，包括 18 项测试，其中少数测试重复不同的参数多次测试，每项测试均会生成一个 P 值，如果测试项有多个 P 值，则利用 KS 检验生成一个综合 P 值作为最终测试结果。在 NIST SP800-22 检验标准的 15 项测试中，设置显著水平值为 α=0.01，当 P 值大于 0.000 1，通过 P 值百分比大于 0.980 6 时，则表示通过该项测试。在 DIEHARD 检验标准的 18 项测试中，设置显著水平值为 α=0.01，当每项测试的 P 值大于 0.01 且小于 0.99 时，则表示通过该项测试。2 种检验标准的测试结果分别如表 1 和表 2 所示，所测试的物理随机数序列均通过 NIST SP800-22 及 DIEHARD 所有测试项，这表明该 Physical-RNG 产生的物理随机序列具有良好的随机统计特性。

表 1　NIST SP800-22 检验标准测试结果

统计测试	P 值	proportion	测试结果
频率测试	0.123 038	0.992	通过
块内频率测试	0.715 679	0.985	通过
累加和测试	0.452 173	0.994	通过
游程测试	0.274 341	0.996	通过
块内长游程测试	0.311 542	0.986	通过
二进制矩阵秩测试	0.486 588	0.990	通过
离散傅里叶变换测试	0.101 311	0.983	通过
非重叠模块匹配测试	0.626 709	0.994	通过
重叠块比配测试	0.568 739	0.988	通过
全局通用统计测试	0.823 725	0.988	通过
近似熵测试	0.429 923	0.992	通过
随机游动测试	0.660 048	0.991	通过
随机游动变量测试	0.624 768	0.995	通过
串行测试	0.622 546	0.988	通过
线性复杂度测试	0.304 126	0.994	通过

5　结束语

本文提出并实验验证了一种基于自治布尔网络的宽带物理混沌熵源，并基于该熵源构建了实时速率为 100 Mbit/s 的物理随机数发生器。随机性检测结果表明，物理随机数发生器产生的随机数序列可以通过 NIST SP800-22 检验标准和 DIEHARD 检验标准，具有良好的随机统计特性。

表 2　DIEHARD 检验标准测试结果

统计测试	P 值	测试结果
生日间隔检验	0.742 382	通过(KS)
重叠置换检验	0.931 053	通过
31×31 二元矩阵秩检验	0.743 923	通过
32×32 二元矩阵秩检验	0.924 107	通过
6×8 二元矩阵秩检验	0.595 180	通过(KS)
比特流检验	0.179 66	通过
OPSO 检验	0.942 3	通过
OQSO 检验	0.924 0	通过
DNA 检验	0.173 1	通过
比特 1 计数检验	0.376 065	通过
特定字节比特 1 计数检验	0.952 819	通过
泊车检验	0.189 101	通过(KS)
最小距离检验	0.974 863	通过(KS)
三维圆球检验	0.342 057	通过(KS)
减数检验	0.925 889	通过
重叠累计和检验	0.478 587	通过(KS)
游程检验	0.282 636	通过(KS)
掷骰检验	0.337 318	通过

此外，值得一提的是，基于该熵源设计技术，可以在 FPGA 中构建出速率更高的随机数发生器；这是由于该熵源仅需 16 个 LE 即可实现；因此在 FPGA 中可以大规模部署，达到多熵源并行产生高速随机数的效果。以目前 Altera 公司中低端 FPGA 芯片 Cyclone V 为例，其 LE 单元数量在 3×105 左右，因此可以在芯片内部同时构建数万个本文提出的物理熵源，实现太比特每秒量级的高速物理随机数实时在线产生。未来，本技术在高速随机数发生器应用领域将有着广阔的发展前景。

参考文献：

[1] LI P, WANG Y C, WANG A B, et al. Fast and tunable all-optical physical random number generator based on direct quantization of chaotic self-pulsations in two-section semiconductor lasers[J]. IEEE Journal of Selected Topics in Quantum Electronics, 2013, 19(4): 0600208.

[2] GELENBE E, YIN Y. Deep learning with random neural networks[C]//International Joint Conference on Neural Networks, 2016: 1633-1638.

[3] LI X, MA J, WANG W, et al. A novel smart card and dynamic ID based remote user authentication scheme for multi-server environments[J]. Mathematical & Computer Modelling, 2013, 58(1-2): 85-95.

[4] MATHEW S K, SRINIVASAN S, ANDERS M A, et al. 2.4 Gbps, 7 mW

all-digital pvt-variation tolerant true random number generator for 45 nm cmos high-performance microprocessors[J]. IEEE Journal of Solid-State Circuits, 2012, 47(11):2807-2821.

[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] 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.

[7] CICEK I, PUSANE A E, DUNDAR G. A novel design method for discrete time chaos based true random number generators[J]. Integration the VLSI Journal, 2014, 47(1):38-47.

[8] PARK M, RODGERS J C, LATHROP D P. True random number generation using CMOS Boolean chaotic oscillator[J]. Microelectronics Journal, 2015, 46(12):1364-1370.

[9] WANG X Y, QIN X. A new pseudo-random number generator based on CML and chaotic iteration[J]. Nonlinear Dynamics, 2012, 70(2): 1589-1592.

[10] ZHANG Y Q, WANG X Y. A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice[J]. Information Sciences, 2014, 273(8):329-351.

[11] WANG X Y, YU Q. A block encryption algorithm based on dynamic sequences of multiple chaotic systems[J]. Communications in Nonlinear Science & Numerical Simulation, 2009, 14(2):574-581.

[12] 温贺平, 禹思敏, 吕金虎. 基于hadoop大数据平台和无简并高维离散超混沌系统的加密算法[J].物理学报, 2017,66(23):70-83.
WEN H P, YU S M, LYU J H. Encryption algorithm based on hadoop and non-degenerate high-dimensional discrete hyperchaotic system[J]. Acta Physica Sinica, 2017, 66(23):70-83.

[13] 李孟婷, 赵泽茂. 一种新的混沌伪随机序列生成方法[J]. 计算机应用研究, 2011, 28(1):341-344.
LI M T, ZHAO Z M . New method to generate chaotic pseudo-random sequence[J]. Application Research of Computers, 2011,28(1):341-344.

[14] ROSIN D P, RONTANI D, GAUTHIER D J. Ultrafast physical generation of random numbers using hybrid Boolean networks[J]. Physical review. E, Statistical, Nonlinear, and Soft Matter Physics, 2013, 87(4):040902.

[15] 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.

[16] ROSIN D P, RONTANI D, GAUTHIER D J. Experiments on autonomous Boolean networks[J]. Chaos An Interdisciplinary Journal of Nonlinear Science, 2013, 23(2):025102.

[17] ROSENSTEIN M T, COLLINS J J, LUCA C J D. A practical method for calculating largest Lyapunov exponents from small data sets[J]. Physica D: Nonlinear Phenomena, 1993, 65(1–2):117-134.

[18] YAO T L, LIU H F, XU J L, et al. Estimating the largest Lyapunov exponent and noise level from chaotic time series[J]. Chaos An Interdisciplinary Journal of Nonlinear Science, 2012, 22(3):043103.

[19] FRAGA L G D L, TLELO-CUAUTLE E. Optimizing the maximum Lyapunov exponent and phase space portraits in multi-scroll chaotic oscillators[J]. Nonlinear Dynamics, 2014, 76(2):1503-1515.

[20] INTEL. Cyclone V device overview[EB]. Santa Clara:Integrated Electronics Corporation, 2018.

[21] RUKHIN A, SOTO J, NECHVATAL J, et al. A statistical test suite for random and pseudorandom number generators for cryptographic applications[J]. Andrew Rukhin Juan Soto James Nechvatal Miles Smid Elaine, 2010, 59(4): 2289-2297.

[22] ALANI M M. Testing randomness in ciphertext of block-ciphers using DieHard tests[J]. International Journal of Computer Science and Network Security, 2010, 10(4): 53-57.

[作者简介]

张琪琪（1994− ），男，山西运城人，太原理工大学硕士生，主要研究方向为混沌理论与密码应用。

张建国（1979− ），男，山西太原人，博士，太原理工大学副教授、硕士生导师，主要研究方向为宽带混沌信号的产生及其在信息安全系统中的应用。

李璞（1986− ），男，河北邢台人，博士，太原理工大学副研究员，主要研究方向为保密通信等。

郭龑强（1983− ），男，山西大同人，博士，太原理工大学讲师，主要研究方向为随机数产生，保密通信等。

王云才（1965− ），男，山西运城人，博士，太原理工大学教授、博士生导师，主要研究方向为混沌信号的产生与应用。