DOI: 10.13382/j.jemi.B2306566

一种高吞吐率自治布尔网络真随机数发生器*

刘正文 易茂祥 杨 云 孙立法 鲁迎春 梁华国
(合肥工业大学微电子学院 合肥 230009)

摘 要:真随机数发生器在硬件与信息安全领域具有广泛的应用前景。为提高真随机数发生器的吞吐率与降低硬件开销,以相互耦合的基本逻辑单元构成自治布尔网络做熵源,利用一阶高频振荡环增强网络刷新频率和多级非线性放大,从而获得高熵值混沌信号,结合 DFF 和 XOR 组成的后处理电路,设计构成真随机数发生器并在 FPGA 平台上实现。通过数据的采样和实时提取,然后对数据执行 NIST SP800-22 和 SP800-90B 随机性测试,并对其偏移度、自相关性及最大李雅普诺夫指数等性能进行评估。结果表明,真随机数发生器能够以 600 Mbit/s 的吞吐率产生熵值 0.994 847 bit/sample 的随机数序列,而且具有低的偏移度和自相关性及较低的硬件开销。

关键词: 真随机数发生器;熵源;自治布尔网络;混沌;吞吐率
中图分类号: TN47 **文献标识码**: A **国家标准学科分类代码**: 510.3040

High throughput autonomous boolean network true random number generator

Liu Zhengwen Yi Maoxiang Yang Yun Sun Lifa Lu Yingchun Liang Huaguo
(School of Microelectronics, Hefei University of Technology, Hefei 230009, China)

Abstract: True random number generators have broad application prospects in the fields of hardware and information security. In order to improve the throughput and reduce the hardware overhead of true random number generator, an autonomous Boolean network is constructed with coupled basic logic units as the entropy source. A first-order high-frequency oscillation loop is used to enhance the network refresh frequency and multi-level nonlinear amplification, thereby obtaining a high entropy chaotic signal. Combining a post-processing circuit composed of DFF and XOR, a true random number generator is designed and implemented on an FPGA platform. The sampled output data is extracted using the ChipScope online tool, then NIST SP800-22 and SP800-90B randomness tests are performed on the data, and their performance such as offset, autocorrelation, and maximum Lyapunov exponent are evaluated. The results show that the proposed true random number generator can generate a random number sequence with an entropy value of 0.994 847 bit/sample at a throughput rate of 600 Mbit/s, and is of low offset and no autocorrelation, and low hardware overhead.

Keywords: true random number generator; entropy source; autonomous Boolean network; chaos; throughput

0 引 言

随机数在区块链、密码学、科学仿真和信息安全等领域具有广泛应用,使用随机数作为密钥,可以有效保护系统的信息安全[1]。随机数分为伪随机数和真随机数[2]。伪随机数能够通过特定的数学算法和初值来迭代产生,如线性同余法,但伪随机数序列具有明显周期性,很难保证加密数据的安全性,尤其是在数据安全保密性要求很高的应用领域中[3-4]。而真随机数一般基于物理随机熵源获取,其优点在于不仅具有良好的随机性,而且还具有不可预测性和不可重复性,从而为信息安全领域提供更可靠的解决方案。真随机数发生器成为重要的研究热点之一。

产生真随机数的物理熵源主要有电阻热噪声、电信号相位抖动、电路亚稳态、混沌和量子噪声等[5]。真随机

收稿日期: 2023-05-29 Received Date: 2023-05-29
*基金项目:国家自然科学基金重大科研仪器项目(62027815)资助

数发生器主要应用指标包括高吞吐率和序列随机性,低硬件开销和功耗开销,易于集成和移植等[6]。目前,真随机数发生器的研究与设计主要集中于如何构建一个高效的熵源电路,广泛采用的包括基于模拟电路的噪声放大法[7]和基于数字电路的抖动及亚稳态提取法[8]。直接放大噪声法通过放大电路中电阻的热噪声,并与阈值进行比较,从而产生随机序列,但是由于电阻噪声幅度非常小,必须使用高功率放大器对电阻噪声进行放大,需要滤波电路来降低其对熵源质量的影响,并且造成硬件开销增加和集成困难。数字环形振荡器电路中相位噪声在时域上表现为边沿抖动,可以通过提取振荡器中边沿抖动而获取随机数。但是基于抖动的随机数发生器需要长时间的抖动效应的累积,以形成更多能够提取的相位噪声,这限制了随机数的产生速率[8]。基于电路噪声产生的亚稳态构成的熵源,其量化产生的随机序列中,位值分布不对现象比较严重,需要借助复杂的后处理电路来加以解决。

基于自治布尔网络的混沌系统具有初值敏感性,使得自治布尔网络产生的混沌信号,相比于亚稳态和抖动熵源产生的信号,具有更高的熵,因而获得广泛的研究。文献[9]提出了一种利用自反馈结构来产生物理随机数的真随机数发生器。该方案通过引入了布尔混沌特性,有效提高了熵源信号的熵值[10]。文献[11]对该电路进行了改进设计,提出了延迟自反馈结构,即在每个节点上都增加了多个反向器。文献[12]提出 7 节点布尔网络熵源结构的真随机数发生器,但其声称的高吞吐率实际是由多个熵源并联扩展实现的。文献[13]提出 15 节点的布尔网络熵源结构,实现 100 Mbit/s 的随机数吞吐率。文献[7]提出基于 66 个节点自治布尔网络熵源结构的真随机数发生器,数据采样输出速率达到 156.25 MHz。文献[14]设计了一种 18 节点的布尔网络熵源结构,并研究和优化了熵源数学模型,证明了滤波系数可以抑制和控制混沌信号的产生。

为进一步提高真随机数发生器的吞吐率并降低其硬件开销,本文基于 5 个三输入异或逻辑相互耦合及 10 个反向器,设计构成一个自治布尔网络,作为真随机数发生器物理熵源。该自治布尔网络支持使用更高的采样频率对熵源进行采样,从而显著提高真随机数发生器的吞吐率,并且节点数的减少可以有效降低熵源的硬件开销。论文余下部分在给出建议的熵源构成及工作原理的基础上,对其性能进行仿真分析,然后引入采样与后处理电路,构成真随机数发生器,通过实验和测试,对真随机数发生器的性能进行了验证。

1　建议的熵源结构及其工作原理

1.1　熵源电路构成与数值仿真

建议的真随机数发生器熵源结构如图 1 所示。它是 1 个由 5 个逻辑运算节点相互耦合构成的自治布尔拓扑网络。其中,每个逻辑运算节点均由 1 个三输入异或(exclusive-OR,XOR)逻辑、1 个输出反相器和 1 个反馈输入反相器构成,节点自身可以产生连续的振荡信号。节点输出信号分两路,直接和经反相器连接到相邻节点。反相器输出经 D 触发器采样,结果送入一个异或网络执行后处理,进而生成并输出所需要的真随机数。

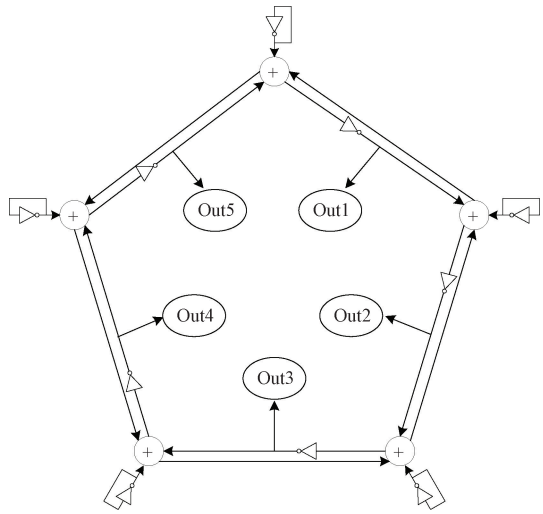


图 1　建议的真随机数发生器熵源结构

Fig. 1　Entropy source of the true random number generator

根据 Ghil 等[15]提出的布尔延迟方程(Boolean delay equation),可对节点为 N 的自治布尔网络进行动态仿真与分析如下:

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

其中,τ_{nm} 为节点 m 到节点 n 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。熵源电路输出信号的基本仿真流程如下:

步骤 1)基于式(1)建立模型;

步骤 2)节点延迟时间、仿真步长等参数设置;

步骤 3)利用 MATLAB 执行电路行为动态仿真。

仿真结果如图 2 所示。当电路节点数为奇数且相邻节点的延迟时间存在的差异,即 $\tau_{mn}\neq\tau_{nm}$ 时,节点输出信号呈随机振荡状态,即所谓的布尔混沌现象。

图 2　熵源节点输出信号的动态仿真结果

Fig. 2　Dynamic simulation results of the entropy source output

1.2　熵源输出信号混沌特性分析

针对本文提出的真随机数发生器熵源结构，使用 MATLAB 工具进一步对熵源输出信号进行频谱特性仿真分析和自相关特性仿真分析。图 3 为熵源输出信号的仿真频谱图。从图中可以看到，输出信号的频谱为连续谱，具有了典型的混沌特征。图 4 为熵源输出信号的自相关特性曲线，从图中可以发现，该信号的半高全宽（full width at half maximum，FWHM）约为 1 ns，短的自相关时间意味着可以以较高采样速率从中提取物理真随机序列[16]。

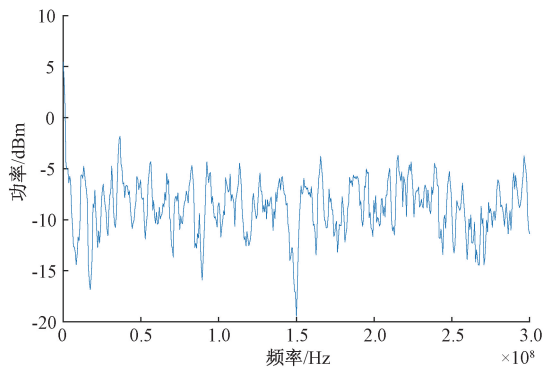


图 3　熵源输出信号的频谱图

Fig. 3　Spectrum diagram of output signal of entropy source

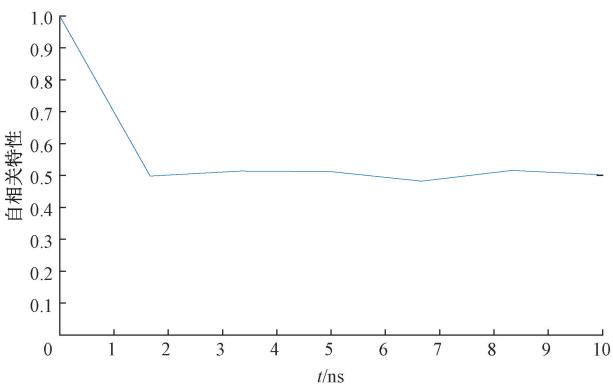


图 4　熵源输出信号的自相关曲线

Fig. 4　Autocorrelation of output signal of entropy source

2　真随机数发生器实现与实验平台

本文设计的真随机数发生器及其测试平台构成如图 5 所示。图中左边的虚框部分为发生器结构，主要由熵源模块、熵源信号采样模块、时钟产生模块和后处理模块构成。熵源模块为图 1 的 5 节点自治布尔网络，采样模块由对应的 5 个 D 触发器构成，由时钟产生模块提供采样时钟，采样结果送入后续的 5 输入异或逻辑网络执行后处理。ChipScope 模块是由基于 Xilinx ISE 的 FPGA 设计软件提供的在线逻辑分析工具 IP 核，例化用于后处理输出信号波形的实时抓取，以实时反映采样频率下所获得的就是最后输出的随机数序列。图 6 所示是通过 ChipScope 抓取获得的一个真随机数发生器输出波形快照。

整体发生器及其输出抓取电路基于 FPGA 器件 Artix-7（XC7A100T）设计实现。实时抓取的结果随机序列通过开发板 USB 接口送到外部的计算机，然后利用 Python 语言将其转换成文本文件，以备接下来的测试与验证实验。用于实验测试的随机序列均为 600 MHz 采样频率下通过所实现的硬件的运行和对输出实时抓取而获得的。

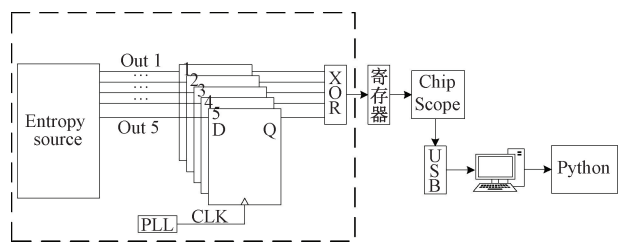


图 5　真随机数发生器及其测试平台

Fig. 5　The true random number generator and its test platform

图 6　输出波形 ChipScope 快照示例

Fig. 6　Example of the output waveform ChipScope snapshot

3　数据测试及结果分析

3.1　NIST SP800-22 随机性测试

通过 NIST 发布的随机数测试程序，对建议的真随机数发生器产生的随机序列进行随机性测试。首先，采用 NIST SP800-22 测试基准，实验选取 −30 ℃ ~ +80 ℃ 3 种温度条件下，分别运行系统总共抓取 100 Mbit 的随机数，并分成 100 组，每组 1 Mbit 的随机数进行实验。共实验 100 次[17]。测试其包括 15 个测试项，每个测试项均设定

了相应的显著性水平值 $\alpha = 0.01$,并将其作为评估指标,最终得出的结果将会反映出随机数的质量。NIST SP800-22 测试结果如表 1 所示。其中 p-Value 远远大于要求的 0.01,而组通过测试比例 proportion 平均大于 0.980 6,这些指标作为随机数的随机性重要评价依据,表明在不同的温度条件下,本文设计的真随机数发生器所产生的随机数具有优异的真随机特性和良好的温度鲁棒性。

表 1　3 种不同温度下 NIST-SP800-22 测试结果

Table 1　NIST-SP800-22 test results at three different temperatures

NIST SP800-22	−30℃		25℃		80℃	
Atrix-7	P-value	Proportion	P-value	Proportion	P-value	Proportion
Approx-Entropy	0.559 656	99/100	0.455 107	99/100	0.543 238	99/100
Block-Freq	0.488 526	100/100	0.466 787	99/100	0.476 152	99/100
Cumsum	0.505 410	99/100	0.516 985	99/100	0.508 857	100/100
FFT	0.482 340	99/100	0.446 498	100/100	0.485 075	99/100
Frequency	0.507 627	99/100	0.482 443	99/100	0.495 872	100/100
Line-Complex	0.463 680	99/100	0.475 824	99/100	0.471 565	99/100
Long-Run	0.524 930	99/100	0.509 380	100/100	0.503 814	99/100
Nonoverlapping	0.500 317	99/100	0.500 077	99/100	0.523 265	99/100
Overlapping	0.510 704	100/100	0.471 377	100/100	0.498 580	99/100
Rand-Excur	0.333 338	68/68	0.275 571	68/68	0.311 846	67/68
Rand-Variant	0.342 183	68/68	0.270 621	67/68	0.298 417	67/68
Rank	0.516 257	98/100	0.578 857	99/100	0.490 383	100/100
Runs	0.490 049	100/100	0.500 707	100/100	0.496 901	99/100
Serial	0.569 362	99/100	0.497 266	100/100	0.494 411	98/100
Universal	0.517 923	100/100	0.532 565	99/100	0.453 949	99/100

3.2　NIST SP_800_90B 测试

SP_800_90B 测试是 NIST 在 2016 年发布的更加严格和复杂的随机数测试方法,其主要目的是为了验证随机数的质量是否能够满足密码学应用的要求。SP_800_90B 测试标准主要包括独立同分布(IID)测试、非独立同分布(Non-IID)测试和最小熵值测试,要求的测试样本数据不少于 1 Mbit,且无需分组[18]。实验采用常温(25 ℃)下生成的随机数集合,测试结果如表 2 所示。其中,计数器 $C_{i,0}$ 和 $C_{i,1}$ 是用于查找原始测试统计信息在排列测试统计信息中的排名。如果数据所测得的计算器出现某些极端值,则表示不能通过 IID 测试,即无法得到准确的结果。此外,还可以通过计算 $C_{i,0}$ 和 $C_{i,1}$ 之和是否小于 9 995,来判定每项测试是否通过。结果显示所有测试项的 $C_{i,0}$ 和 $C_{i,1}$ 之和都远小于 9995,表明被测随机数据集通过所有 IID 测试项目。

表 3 给出的是被测随机数集合 NIST SP_800_90B 的 Non-IID 测试结果,其中 p-max 是观测到最常见样本的概率值,h-min 是可能的最小熵估计值,即最小熵。从表中可以看到,所有测试项的最小熵都接近 1,除了同现有文献类似的 Markov 测试项目例外,测试项 p-max 值均接近 0.5,表明所产生的随机序列的随机性能够满足密码学应用的基本要求。

表 2　NIST SP_800_90B IID 测试结果(25℃)

Table 2　NIST SP_800_90B IID test results(25℃)

Artix-7		Results		
IID Test		$C_{i,0}$	$C_{i,1}$	IID
Excursion		3 826	0	pass
NumDirectionalRuns		3 955	17	pass
LenDirectionalRuns		825	1 794	pass
NumIncreasesDecreases		5 878	33	pass
NumRunsMedian		4 520	9	pass
LenRunsMedian		6 181	2 381	pass
AvgCollision		6 859	9	pass
MaxCollision		6 563	1 043	pass
Periodicity	Peri-1	4 815	24	pass
	Peri-2	6 579	30	pass
	Peri-8	7 502	20	pass
	Peri-16	1 474	17	pass
	Peri-32	6 064	25	pass
Covariance	Cov-1	7 660	6	pass
	Cov-2	6 528	6	pass
	Cov-8	8 923	0	pass
	Cov-16	1 152	0	pass
	Cov-32	6 448	7	pass
Compression		7 081	81	pass
Independence		pass		
Goodness-of-fit		pass		
LRS test		pass		
Restart test		pass		
Min-entropy		0.994 847		

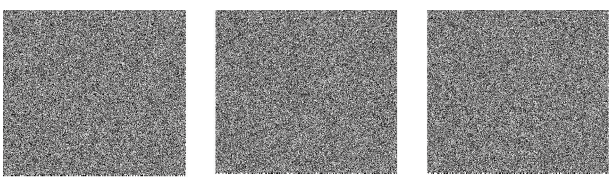
表3　NIST SP_800_90B Non-IID 测试结果(25 ℃)

Table 3　NIST SP_800_90B Non-IID test results(25 ℃)

NIST SP800-90B	Artix-7 FPGA	
Non-IID Test	p-max	h-min
MCV	0.501 789	0.994 847
Collision	0.537 109	0.896 712
Markov	$3.300\ 68\times10^{-39}$	0.998 691
Compression	0.5	1
t-Tuple	0.519 39	0.945 111
LRS	0.510 206	0.970 847
Multi-MCW	0.500 903	0.997 398
Lag	0.500 708	0.997 957
Multi-MMC	0.502 096	0.993 965
LZ78Y	0.501 491	0.995 706

3.3　偏移度测试

随机数序列的偏移度可以在满足要求大小的数据集的条件下,通过序列中二进制数'0'和'1'各自所占的比例来表征[6],理想值为0.5。在本文中真随机数发生器产生的随机比特流是一个大于100万位的二进制文件,数据量较大,无法直观的观察到随机数中'0'和'1'的分布情况。因此通过MATLAB 3种温度条件下得到的随机数文件转化为可视的黑白位图,即将'0'和'1'转化为像素点。如图7(a)、(b)和(c)所示,可以发现位图中黑白像素点分布是十分均匀的,表明建议得真随机数发生器在不同温度下输出的真随机数具有低的偏移度和温度鲁棒性。



(a) 80℃　　(b) -30℃　　(c) 25℃

图7　不同温度下TRNG输出随机数序列位图

Fig. 7　Bitmaps of random number sequences output by TRNG at different temperatures

3.4　自相关性测试

除了偏移度测试之外,自相关性测试也是能评价随机数随机性的一项测试,能够进一步验证所得到随机数是否具有一定的相关性。自相关性是指随机误差项的各期望值之间是否存在着相关关系,对随机序列进行自相关性测试是进一步验证随机序列的随机性其中在自相关性测试中会使用相关系数来表示相关程度的大小[19]。根据卡尔·皮尔逊(Karl Pearson)设计的统计指标,相关系数定义$\boldsymbol{\rho}_{X,Y}$如下:

$$\boldsymbol{\rho}_{X,Y}=\frac{\mathrm{cov}(X,Y)}{\sigma_X\sigma_Y}=\frac{E[(X-\mu_X)(Y-\mu_Y)]}{\sigma_X\sigma_Y} \tag{2}$$

其中,X、Y分别代表测试数据中'0'和'1'的测试集,$cov(X,Y)$表示变量X和Y之间的相关系数,σ_X和σ_Y分别表示变量X和Y的方差,通过MATLAB工具计算得到相关系数的值有正有负,$\boldsymbol{\rho}_{X,Y}$的绝对值越大,则表示该序列的自相关性越强,即所测的$\boldsymbol{\rho}_{X,Y}$越接近于$|\pm1|$,表明相关程度越强;反之$\boldsymbol{\rho}_{X,Y}$越接近于0,表明相关程度越弱。

自相关性程度分级参考以下标准判定,即当$0.8<|\rho_{X,Y}|\leqslant1.0$时为极强自相关,当$0.6<|\rho_{X,Y}|\leqslant0.8$时为强自相关,当$0.4<|\rho_{X,Y}|\leqslant0.6$时为中等自相关,当$0.2<|\rho_{X,Y}|\leqslant0.4$时为弱自相关,而当$0<|\rho_{X,Y}|\leqslant0.2$时,则被判定为极弱自相关或无自相关。一般文献实验设定当$|\rho_{X,Y}|\leqslant0.3$时,认为目标随机数序列的自相关程度极弱,或不存在自相关性[20]。通过MATLAB工具对建议真随机数发生器在3种不同温度条件下生成的随机序列,执行自相关性模拟测试,结果如图8所示。从图8中可以看出,所得随机数据序列的自相关系数的绝对值均小于0.003,近似为没有自相关性。结合前面的NIST测试和偏移度测试,进一步验证了建议真随机数发生器所生成的随机序列的良好随机性。

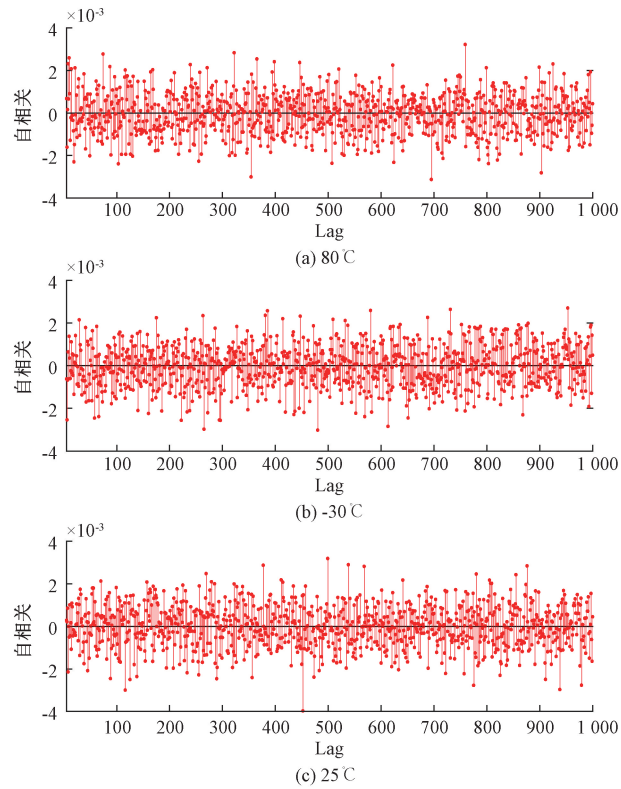


图8　熵源输出信号的三温自相关性图

Fig. 8　Three temperature autocorrelation diagram of entropy source output signal

3.5　最大李雅普诺夫指数分析

最大李雅普诺夫指数(Liapunov expoenent)作为一种相空间相邻轨迹的平均指数发散率的数值表征方法,主要用于刻画一个系统的稳定性,而最大李雅普诺夫指数为正值,则表明目标系统为混沌系统[4,8]。根据文献[8]的方法,本文利用 MATLAB 模拟工具自带的 Lorenz 参考案例数据,调用 Phase Space Reconstruction 函数,重构熵源输出序列'0'和'1'数据集的相空间,结果如图 9 所示。其中,X 轴表示最大李雅普诺夫指数拟合步长,Y 轴表示对相空间的轨迹分离程度进行取对数求平均。MATLAB 模拟表明,图中给出的 2 个 x 坐标点之间的距离为最大李雅普诺夫指数的最佳线性拟合步长,结果显示建议的真随机数发生器输出序列的最大李雅普诺夫指数为 0.377 967 ,表明熵源结构输出振荡信号具有很好的混沌特性。

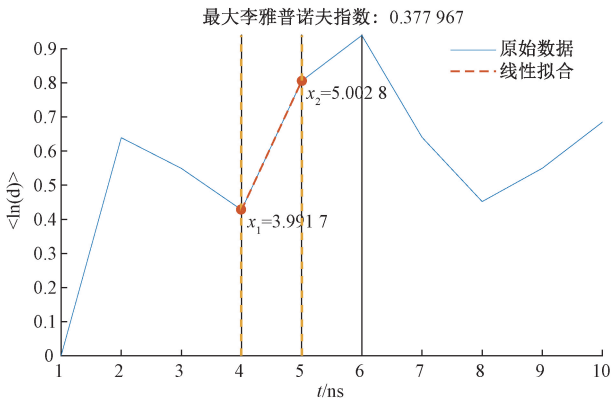


图 9　熵源输出数据线性拟合相空间图

Fig. 9　Linear fitting phase space diagram of entropy source output data

3.6　与相关真随机数发生器的比较

将建议的真随机数发生器与相关的混沌熵源发生器进行性能对比,结果如表 4 所示。本文真随机数发生器可以 600 Mbit/s 采样速率下生成熵值可达 0.994 847 bit/sample 的真随机数,相对于后者有明显提高,熵源仅使用 5 个节点,硬件开销为 16 个 LUTS 和 5 个 DFFS,也具有较大的竞争力。同时,本文建议的正随机数发生器的不同温度条件下的测试结果,也表明其具有良好的温度鲁棒特性和低偏移度与自相关性。

本文还将建议的真随机数发生器与典型非混沌熵源结构的真随机数发生器进行比较,如表 5 所示。其中,文献[19]的开销和吞吐率表现均衡,而文献[20]通过短时间增加相位噪声扩大信号抖动范围,获得较高的随机数吞吐率。比较发现,建议的真随机数发生器的吞吐率具有较明显的优势,且保持较低的硬件开销。

表 4　与基于混沌的真随机数发生器比较

Table 4　Comparison with Chaos Based TRNGs

参数	本文	文献[12]	文献[13]	文献[14]
吞吐率/(Mbit·s^{-1})	600	100	100	100
最小熵	0.994 847	–	1	–
NIST	通过	通过	通过	通过
资源开销	16LUT+5DFF	15LUT	13LUT	18LUT
后处理	是	是	是	是
鲁棒性	通过	–	–	通过

表 5　与非混沌类型真随机数发生器比较

Table 5　Comparison with non-Chaotic TRNGs

参数	本文	文献[18]	文献[19]	文献[20]
吞吐率/(Mbit·s^{-1})	600	14.2	290	300
最小熵	0.994 847	0.992	0.985 281	0.995 535
NIST	通过	通过	通过	通过
资源开销	16LUT+5DFF	60LUT	24LUT	43LUT
后处理	是	否	是	是
鲁棒性	通过	通过	通过	通过

4　结　论

本文建议了一种基于自治布尔网络的真随机数发生器熵源结构,理论与模拟分析表明了熵源的良好混沌特性。结合采样和后处理电路设计,构成真随机数发生器并基于 FPGA 进行了电路实现。3 种工作温度和 600 MHz 采样速率下,执行实际运行并对输出随机数实时抓取,得到真随机数序列集。对随机数序列执行 NIST 标准测试,结果表明,最小熵值平均达到 0.994 847 bit/sample。与相关文献工作结果的比较,显示建议的真随机数发生器在吞吐率、硬件开销和温度稳定性等指标上均具有较明显的优势。

参考文献

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

[2] 马荔,张建国,李璞,等. 基于自治布尔网络的高速物理随机数发生器研究[J]. 中南大学学报(自然科学版), 2018, 49(4):888-892.
MA L, ZHANG J G, LI P, et al. Research on high-speed physical random number generator based on autonomous Boolean network [J]. Journal of Central South University (Natural Science), 2018, 49(4): 888-892.

[3] 蔚艳文. 基于混沌的伪随机数发生器研究[D]. 贵阳: 贵州大学,2021.
WEI Y W. Pseudo random number generator based on chaos study [D]. Guiyang: Guizhou University, 2021.

[4] 许华醒,张平,王昌雷,等. 小型化高速实时量子随机数发生器的设计与实现[J]. 光电子激光, 2022, 33(12): 1255-1262.
XU H X, ZHANG P, WANG CH L, et al. Miniaturization of high-speed real-time quantum random number generator [J]. The Design and Implementation of Photoelectron Laser, 2022, 33 (12): 1255-1262.

[5] 金杰,罗敏,宫月红. 一种基于热噪声的真随机数发生器的设计与实现[J]. 微电子学与计算机, 2015, 32(10):7-11, 16.
JIN J, LUO M, GONG Y H. Design and implementation of a true random number generator based on thermal noise [J]. Microelectronics & Computers, 2015, 32(10):7-11,16.

[6] 马原,陈天宇,吴鑫莹,等. 随机数发生器的设计与检测[J]. 信息安全研究,2019,5(1):39-49.
MA Y, CHEN T Y, WU X Y, et al. Design and detection of random number generator [J]. Information Security Research, 2019,5(1):39-49.

[7] 刘锋. 10 Gbps 物理随机数发生器及其采集存储系统的设计与实现[D]. 太原: 太原理工大学, 2020.
LIU F. Design and implementation of 10 Gbps physical random number generator and its acquisition and storage system [D]. Taiyuan: Taiyuan University of Technology, 2020.

[8] 刘海芳,张建国,龚利爽,等. 基于逻辑器件响应特性的自治布尔网络调控[J]. 物理学报, 2021,70(5): 66-74.
LIU H F, ZHANG J G, GONG L SH, et al. Autonomous Boolean network regulation based on response characteristics of logic devices [J]. Acta Physical Sinica, 2021,70(5):66-74.

[9] ROSIN D P, RONTANI D, GAUTHIER D J, et al. Experiments on autonomous Boolean networks [J]. Chaos, 2013, 23(2): 025102.

[10] ROSIN D P, RONTANI D, GAUTHIER D J. Ultra-fast physical generation of random numbers using hybrid Boolean networks[J]. Physical Review E, 2013,87(4): 040902.

[11] DONG L H, YANG H, ZENG Y. Analysis and improvement of true random number generator based on autonomous Boolean network [C]. The 13th International Conference on Computational Intelligence and Security, IEEE, 2017: 243-247.

[12] 张琪琪,张建国,李璞,等. 基于布尔混沌的物理随机数发生器[J]. 通信学报, 2019,40(1):201-206.
ZHANG Q Q, ZHANG J G, LI P, et al. Physical random number generator based on Boolean chaos [J]. Journal of Communications, 2019,40(1):201-206.

[13] 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.
YANG R, HOU ER L, LIU H F, et al. Low power physical random number generator based on Boolean network [J]. Journal of Shenzhen University (Science & Technology Edition), 2020,37(1):51-56.

[14] 杜海鋆,张建国,刘海芳,等. 异或门自治布尔网络及物理随机数发生器[J]. 深圳大学学报(理工版), 2021,38(1):103-109.
DU H J, ZHANG J G, LIU H F, et al. Xor gate autonomous Boolean networks and physical random number generators [J]. Journal of Shenzhen University (Science and Technology), 2021, 38(1):103-109.

[15] GHIL M, ZALIAPIN I, COLUZZI B. Boolean delay equations: A simple way of looking at complex systems [J]. Physical D: Nonlinear Phenomena, 2008, 237 (23): 2967-2986.

[16] MA L, ZHANG J G, LI P, et al. Research on high-speed physical random number generator based on autonomous boolean network [J]. Journal of Central South University (Science and Technology), 2018, 49(4):888-892.

[17] 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(3):115-122.
LU Y CH, LIANG H G, WANG X Y, et al. A lightweight and efficient true random number generator based on ring oscillator [J]. Chinese Journal of Electronic Measurement and Instrumentation, 2021, 35(3):115-122.

[18] 王浩宇,梁华国,徐秀敏,等. 一种基于 FPGA 的 Latch 结构真随机数发生器[J]. 微电子学, 2018,48 (5): 635-641.
WANG H Y, LIANG H G, XU X M, et al. A Latch structure true random number generator based on FPGA [J]. Journal of Microelectronics, 2018,48 (5) 13:635-641.

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

[20] 鲁迎春,韩倩,刘新颖,等. 基于可配置异步反馈环形

振荡器的真随机数发生器[J]. 电子测量与仪器学报, 2022, 36(11): 126-133.

LU Y CH, HAN Q, LIU X Y, et al. Based on configurable asynchronous feedback ring oscillator of true random number generator [J]. Journal of Electronic Measurement and Instrumentation, 2022, 36(11): 126-133.

作者简介

刘正文,2019 年于阜阳师范大学获得学士学位,现为合肥工业大学硕士研究生,主要研究方向为集成电路工程。

E-mail: 527813608@qq.com

Liu Zhengwen received his B. Sc. degree from Fuyang Normal University in 2019. Now he is a M. Sc. candidate in Hefei University of Technology. His main research interest includes integrated circuit engineering.

易茂祥(通信作者),1986 年于合肥工业大学获得学士学位,1989 年于合肥工业大学获得硕士学位,2010 年于合肥工业大学获得博士学位,现任合肥工业大学微电子学院教授,主要研究方向为 VLSI 测试方法与可测性、可靠性及安全性设计和计算机应用技术与系统。

E-mail: mxyi126@126.com

Yi Maoxiang (Corresponding author) received his B. Sc. degree from Hefei University of Technology in 1986, M. Sc. degree from Hefei University of Technology in 1989 and Ph. D. degree from Hefei University of Technology in 2010, respectively. Now he is a professor at the School of Microelectronics of Hefei University of Technology. His main research interests include VLSI test methods and design of testability, reliability and security and computer application technology and system.