布尔混沌系统的物理随机性分析

龚利爽[1,2]，侯二林[1,2]，刘海芳[1,2]，李凯凯[1,2]，王云才[1,2]
（1. 太原理工大学物理与光电工程学院，山西 太原 030024；
2. 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）

摘 要：为了分析布尔混沌系统的物理随机性，构建了基于自治布尔网络的电路混沌模型，建立了包含相位噪声特性的数学方程，研究了相位噪声对布尔混沌熵增长时间（记忆时间）的影响。研究结果表明，在相位噪声的影响下，布尔混沌输出将在有限的记忆时间（数十纳秒）后达到无法预测，且相位噪声越强，布尔混沌平均记忆时间越短。这证明了相位噪声是布尔混沌物理随机性的来源，且布尔混沌可以作为性能良好的真随机数物理熵源。

关键词：自治布尔网络；布尔混沌；相位噪声；物理随机性
中图分类号：TN91
文献标识码：A
doi: 10.11959/j.issn.1000−436x.2019048

Physical random analysis of Boolean chaos

GONG Lishuang[1,2], HOU Erlin[1,2], LIU Haifang[1,2], LI Kaikai[1,2], WANG Yuncai[1,2]
1. College of Physics and Optoelectronics, Taiyuan University of Technology, Taiyuan 030024, China
2. Key Laboratory of Advanced Transducers and Intelligent Control System, Ministry of Education, Taiyuan 030024, China

Abstract: To analyze the physical randomness of Boolean chaos, the model for chaotic circuit system based on autonomous Boolean network was established. In addition, the equations of the Boolean network with phase noise were deduced. By considering the phase noise, the time for the growth of entropy for an ensemble of trajectories, called the memory time, was analyzed. It was demonstrated that Boolean chaos would be unpredictable after tens of nanoseconds, and less average memory time was required as the phase noise strength increased. It is shown that Boolean chaos has physical randomness because of phase noise and it also lays the theoretical foundation for the entropy source of true random number generator based on chaotic Boolean network.

Key words: autonomous Boolean network, Boolean chaos, phase noise, physical random

1 引言

真随机数是确保信息加密安全的关键[1]。传统的真随机数发生器（TRNG, the random number generator）主要利用热噪声、量子噪声、振荡器抖动、电子器件的亚稳态等不可预测的物理随机过程（物理熵源）来产生真随机数[1-6]。但是，受限于物理熵源带宽，上述真随机数发生器的速率普遍为数十兆比特每秒，难以适用于高速信息的加密需求。在安全通信领域，香农（Shannon）提出的“一次一密”被证明是一种绝对安全的保密通信机制，而该机制实现的前提之一是需要有大量实时产生的加密密钥（真随机数），且这些密钥加密不能重复使用，因此，高速真随机数发生器的研究成为解决安全通信问题的关键技术之一[4, 7]。

近年来，随着宽带混沌技术的出现，基于电路混沌的随机数发生器逐渐成为研究热点[8]。2006 年，Pareschi 等[9]利用马尔可夫混沌映射作为物理熵源，

收稿日期：2018−05−25；**修回日期**：2018−08−01
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）
Foundation Item: The National Natural Science Foundation of China (No.61731014）

实现了 40 Mbit/s 的随机数发生器；2010 年，该课题组进一步修正混沌映射，实现了 100 Mbit/s 的混沌随机数发生器[10]；2013 年，Rosin 等[11]利用布尔混沌作为物理熵源，完成了 12.8 Gbit/s 的随机数发生器的研制；2015 年，Park 等[12]研制了基于布尔混沌的随机数发生器芯片，速率可达 300 Mbit/s。混沌随机数发生器的迅速发展使其有望解决“一次一密”高速保密通信中海量真随机数的实时产生难题。

然而，目前的混沌高速随机数发生器的研究仍面临一个“原则性”问题，即确定性的非线性系统中能否真正产生不可预测的“真随机数”，对此多数研究文献缺乏相关理论分析与证明[13]。为了更好地将电路混沌随机数发生器应用于保密通信中，本文以布尔混沌系统为例，仿真研究了该系统产生的混沌序列在有相位噪声和无相位噪声条件下随机特性（不可预测性）的变化，研究了不同强度相位噪声对布尔混沌熵增长时间（记忆时间）的影响。研究发现，在相位噪声强度下，布尔混沌序列由可预测逐步转变为不可预测，且相位噪声越强，布尔混沌平均记忆时间越短，在相位噪声强度达到时延的 1%~5%时，布尔混沌输出将在有限的记忆时间（数十纳秒）后变得无法预测，该研究结果为基于布尔混沌物理熵源的真随机数发生器提供了理论依据，对其他混沌真随机数发生器研究也提供了有益的借鉴。

2　布尔混沌模型

图 1 是研究所用的三节点自治布尔网络结构，图中“◎”代表 XNOR 逻辑门，“○”代表 XOR 逻辑门。该网络共包含 3 个节点，分别是一个执行异或非（XNOR）运算的节点和 2 个执行异或（XOR）运算的节点。每个节点分别和相邻的 2 个节点连接，构成一个双向反馈的环形自治布尔网络。τ_{ij}（i=1, 2, 3, j=1, 2, 3）是节点 j 到节点 i 的传输时延，通过控制自治布尔网络相邻节点的传输时延，可以使网络输出混沌信号。XOR 逻辑门和 XNOR 逻辑门的输入输出真值如表 1 所示。

电路中的逻辑器件响应并非无限快，无法响应变化速度无限快的信号，即低通滤波效应，考虑低通滤波效应的自治布尔网络方程如式(1)所示。

$$\begin{cases}\tau_{\mathrm{LP}}\dot{x}_1(t)=-x_1(t)+X_2(t-\tau_{12})\oplus X_3(t-\tau_{13})\oplus 1\\ \tau_{\mathrm{LP}}\dot{x}_2(t)=-x_2(t)+X_1(t-\tau_{21})\oplus X_3(t-\tau_{23})\\ \tau_{\mathrm{LP}}\dot{x}_3(t)=-x_3(t)+X_1(t-\tau_{31})\oplus X_2(t-\tau_{32})\end{cases}\tag{1}$$

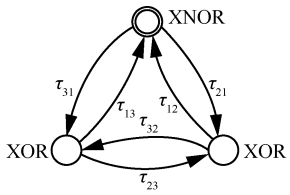


图 1　三节点自治布尔网络结构

表 1　XOR 和 XNOR 逻辑门的输入输出值

输入	XOR 输出	XNOR 输出
00	0	1
01	1	0
10	1	0
11	0	1

其中，⊕是 XOR 运算符，$x_i\in A$=[0,1], i=1, 2, 3。每个布尔变量的值都依赖于运行时刻 t、传输时延及相邻布尔节点上一时刻的逻辑值，其中

$$X_i(t)=\begin{cases}1, & x_i(t)>x_{\mathrm{th}}\\ 0, & x_i(t)\leqslant x_{\mathrm{th}}\end{cases}\tag{2}$$

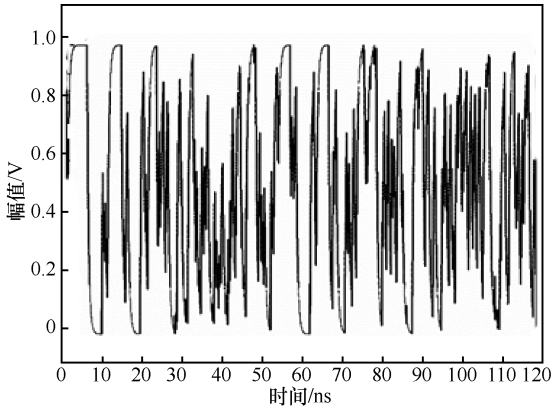
其中，“1”和“0”分别表示布尔网络的高电平和低电平，x_{th}为布尔网络输出为“0”或“1”的阈值，本文取阈值 x_{th}=0.5。

当传输时延 $\tau_{ij}\neq\tau_{ji}$ 时，自治布尔网络 XNOR 节点可以输出复杂信号。图 2(a)和图 2(b)是自治布尔网络输出信号的时序波形和频谱图，图 2(c)是根据 Ghil、Bockman 和 Zhang 等[14-16]提出的计算分段线性微分方程的动力系统的方法得出的网络输出时序的 Lyapunov 指数。图 2 结果表明，当传输时延 $\tau_{ij}\neq\tau_{ji}$ 时，自治布尔网络可以输出带宽达 362 MHz 的复杂信号，网络输出时序的最大 Lyapunov 指数为 0.41 ns^{-1}，代表此布尔网络动力系统是混沌系统。

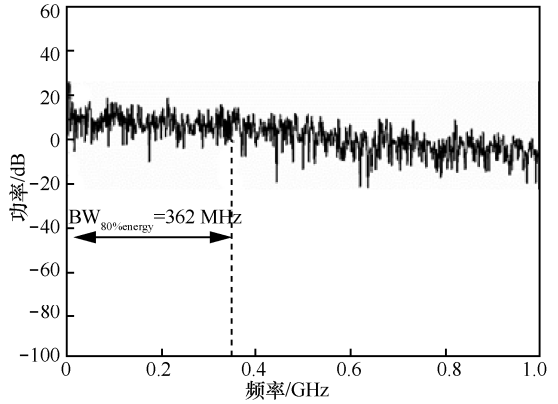
除低通滤波效应外，自治布尔网络电路系统中还存在幅值噪声和相位噪声[17-18]，这 2 种噪声会对传输时延和网络输出的幅值产生影响。考虑到自治布尔网络的幅值限制机理，本文仅分析相位噪声对布尔混沌的影响，建立相位噪声的自治布尔网络模型，如式(3)所示。

$$\begin{cases}\tau_{\mathrm{LP}}\dot{x}_1(t)=-x_1(t)+X_2[t-(\tau_{12}+\tau_{R12})]\oplus\\ X_3[t-(\tau_{13}+\tau_{R13})]\oplus 1\\ \tau_{\mathrm{LP}}\dot{x}_2(t)=-x_2(t)+X_1[t-(\tau_{21}+\tau_{R21})]\oplus\\ X_3[t-(\tau_{23}+\tau_{R23})]\\ \tau_{\mathrm{LP}}\dot{x}_3(t)=-x_3(t)+X_1[t-(\tau_{31}+\tau_{R31})]\oplus\\ X_2[t-(\tau_{32}+\tau_{R32})]\end{cases}\tag{3}$$

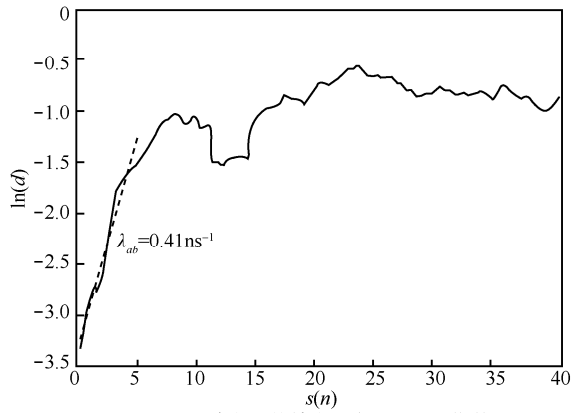
其中，τ_{Rij} 为相位噪声引起的时延抖动。实际电路中热噪声引起的时延抖动服从高斯分布[17]。



(a) 布尔网络输出时序



(b) 布尔网络输出时序频谱



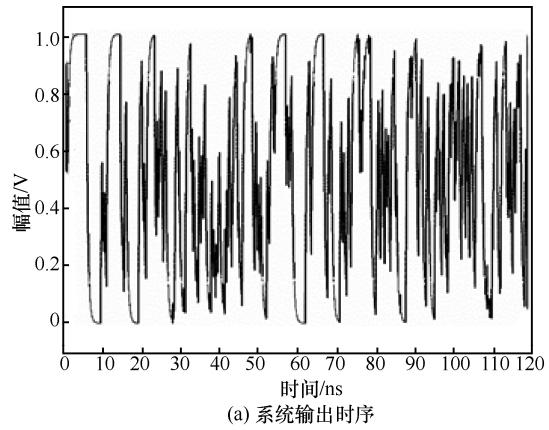
(c) 布尔网络输出最大Lyapunov指数

图 2　自治布尔网络的输出特性

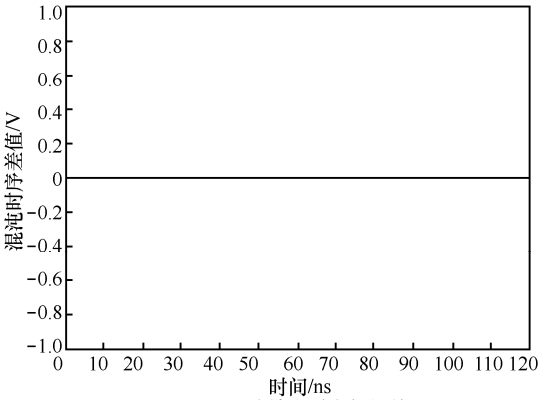
3　相位噪声对布尔混沌系统随机性影响

3.1　相位噪声对混沌动态的影响

基于上述布尔混沌模型，分析了无相位噪声和有相位噪声这 2 种情况下布尔混沌系统的输出特性。图 3 为理想的布尔混沌系统（即系统中没有噪声）XNOR 节点的输出结果；图 4 为在 t=0 时刻

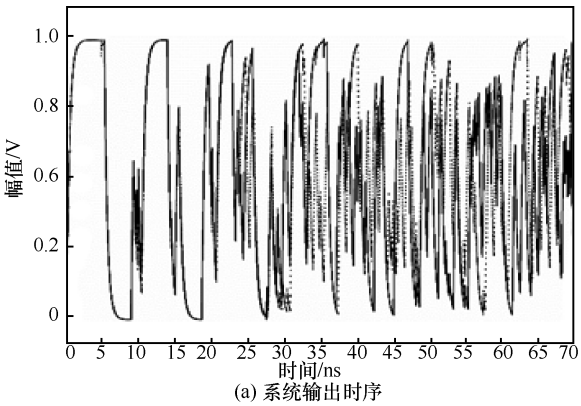


(a) 系统输出时序

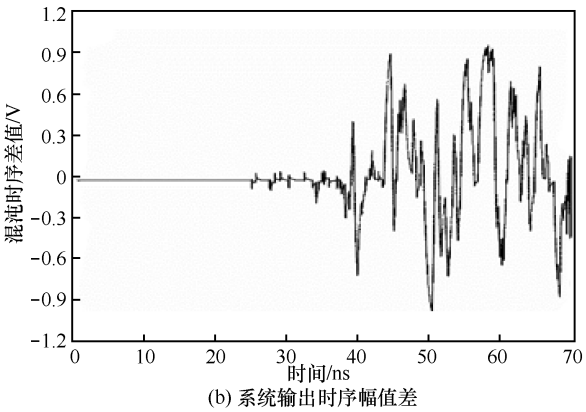


(b) 系统输出时序幅值差

图 3　理想布尔混沌系统 XNOR 节点的输出结果



(a) 系统输出时序



(b) 系统输出时序幅值差

图 4　引入相位噪声后布尔混沌系统 XNOR 节点的输出结果

引入相位噪声后，布尔混沌系统 XNOR 节点的输出结果，其中相位抖动为时延的 0.2%。由图 3 可知，无噪声时布尔混沌系统在重启 2 次的情况下输出的时序相同，这意味着在理想情况下，布尔混沌输出是可以预测的。图 4 显示，布尔混沌系统在最初一段时间内，重启 2 次情况下输出时序基本相同；但由于相位噪声的影响，一段时间后，2 条布尔混沌输出时序轨迹开始分离。在图 4 中，2 条轨迹开始分离的时间是 35~40 ns。

进一步分析相同相位噪声强度的混沌自治布尔网络输出的变化，相位噪声强度相同是指相位抖动的标准差相同。图 5 是布尔混沌电路系统在初始值为 0、相位噪声强度相同时系统运行 1 000 次，系统在 0 ns、10 ns、25 ns 和 95 ns 时输出幅值的概率密度直方图。由图 5(a)可知，在 t=0 时刻（刚加入相位噪声时），布尔混沌运行 1 000 次的输出电压幅值都相同，此时输出某一电压幅值的概率为 1，意味着此时布尔混沌的输出是可以预测的。随着相位噪声在布尔网络中作用时间的增加，布尔混沌系统的输出开始出现不确定值，且随着时间的增加，不确定性逐渐增大，如图 5(b)~图 5(d)所示。

3.2　相位噪声对混沌输出不可预测性的影响

Shannon 熵是对序列随机性的一种有效统计度量，它从概率角度评价输出比特独立性和不确定性[19]。通过计算不同相位噪声强度下布尔混沌输出布尔值在 t 时刻的 Shannon 熵，本文分析了相位噪声对布尔混沌输出不可预测性的影响。

Shannon 熵公式如式(4)所示。

$$H(t)=-\sum_{k=0}^{1}P_k(t)\mathrm{lb}P_k(t) \tag{4}$$

其中，$P_k(t)$是自治布尔网络添加不同相位噪声序列时，自治布尔网络混沌电路系统在 t 时刻输出 0 或者 1 的概率。由式(4)可得，当 $P_k(t)$=0.5 时，所对应 t 时刻的自治布尔网络输出布尔序列的熵最大（即熵等于 1）。这意味着，此时布尔网络的输出不可预测。

图 6 为相同噪声布尔混沌系统多次运行后每一时刻的熵值随时间的变化曲线。这里，图 6(a)和图 6(b)系统初值分别为 0 和 0.15，并各运行 1 000 次。由图 6 可知，加入相位噪声后，布尔混沌的熵值从 0 增长为 1，表明相位噪声使布尔混沌输出由可预测逐渐转变为不可预测。定义熵值从 0 增长为 1 的时间为混沌记忆时间。对比图 6(a)和图 6(b)可知，布尔混沌记忆时间与自治布尔网络初始值有关。

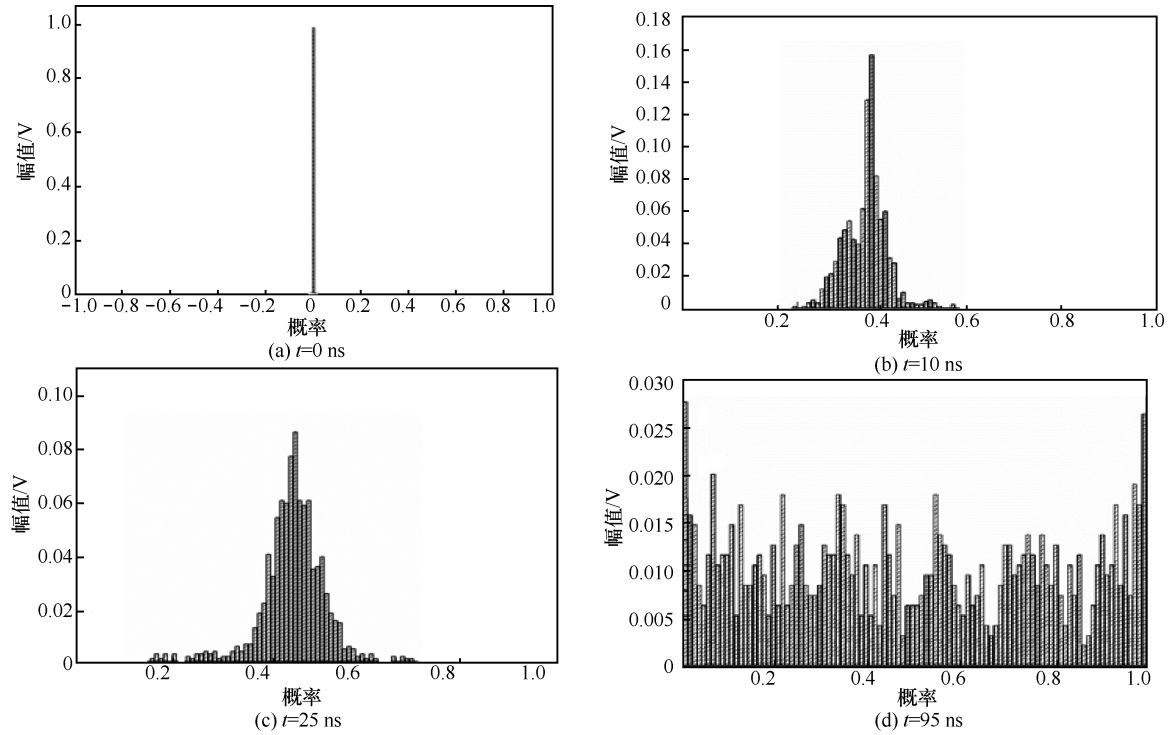


图 5　有相位噪声时混沌布尔网络 XNOR 节点不同时刻的输出概率直方图

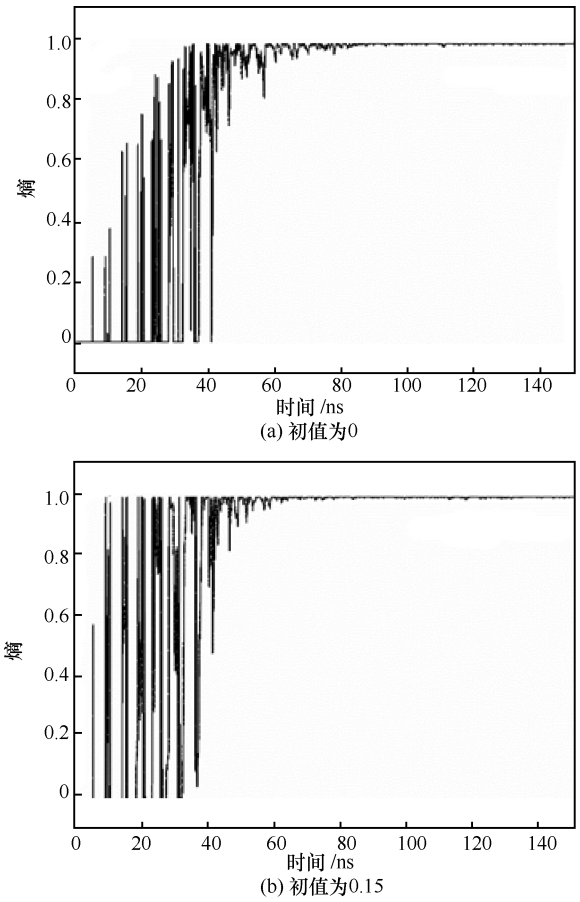


图 6　添加相位噪声后混沌布尔网络熵值随时间的变化

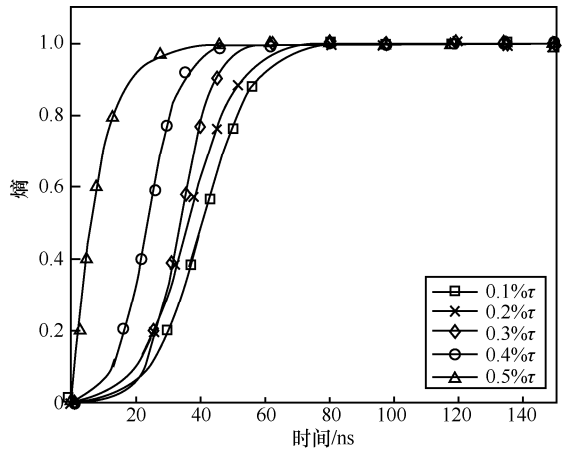


图 7　不同相位噪声强度下布尔混沌熵值随时间的变化

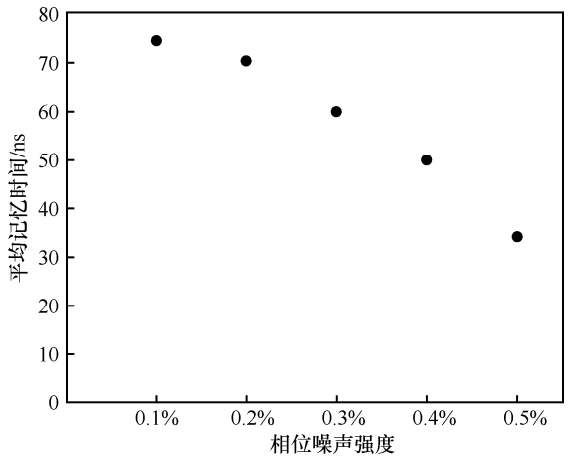


图 8　布尔混沌平均记忆时间和相位噪声强度的关系

进一步分析相同噪声强度、不同网络初值的布尔混沌熵随时间变化的平均值。图 7 是 5 种相位噪声强度的布尔混沌熵值随时间变化的平均结果。图 7 中，5 种相位噪声强度分别为时延的 0.1%、0.2%、0.3%、0.4%和 0.5%，每种相位噪声强度的布尔混沌初值随机变化 1 000 次。由图 7 可知，相同相位噪声强度的布尔混沌熵值随时间的平均变化基本为一条平滑的曲线；不同相位噪声强度的布尔混沌熵值到达 1.0 的时间不同。图 8 是相位噪声强度分别为 0.1%、0.2%、0.3%、0.4%和 0.5%时对应的布尔混沌平均记忆时间结果，它表明相位噪声越强，布尔混沌记忆时间越短，布尔混沌能更快地达到不可预测。

4　结束语

本文通过研究相位噪声对布尔混沌输出的不可预测性影响分析了布尔混沌系统的物理随机性，具体研究了相同噪声布尔混沌系统多次运行后每一时刻的熵值随时间的变化。研究结果表明，电路中存在的固有相位噪声使布尔混沌输出变得不可预测。然后分析了布尔混沌记忆时间和相位噪声强度的关系。由结果可知，相位噪声强度为时延的 0.1%~0.5%时，布尔混沌输出将在有限的记忆时间后（数十纳秒）达到不可预测。相位噪声越强，布尔混沌输出的平均记忆时间越短。本文的研究结果表明相位噪声是混沌布尔网络的物理随机性的原因。该研究结果为基于布尔混沌物理熵源的真随机数发生器提供了理论依据，对其他混沌真随机数发生器研究也提供了有益的借鉴。

参考文献：

[1] WIECZOREK P Z, GOLOFIT K. Dual-metastability time- competitive true random number generator[J]. IEEE Transactions on Circuits and Systems I-Regular Papers, 2014, 61(1): 134-145.

[2] CHEN X, WANG L, LI B, et al. Modeling random telegraph noise as a randomness source and its application in true random number generation[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2016, 35(9): 1435-1448.

[3] GABRIEL C, WITTMANN C, SYCH D, et al. A generator for unique quantum random numbers based on vacuum states[J]. Nature Photon-

ics, 2010, 4(10): 711-715.

[4] 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.

[5] MATHEW S K, JOHNSTON D, SATPATHY S, et al. RNG: a 300–950 mV, 323 Gbps/W all-digital full-entropy true random number generator in 14 nm FinFET CMOS[J]. IEEE Journal of Solid-State Circuits, 2016, 51(7): 1695-1704.

[6] LUBICZ D, BOCHARD N. Towards an oscillator based TRNG with a certified entropy rate[J]. IEEE Transactions on Computers, 2015, 64(4): 1191-1200.

[7] 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 and Systems Ⅱ-Express Briefs, 2016, 63(6): 608-612.

[8] ERGUN S, GULER U, ASADA K. A high speed ic truly random number generator based on chaotic sampling of regular waveform[J]. IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences, 2011, E94A(1): 180-190.

[9] PARESCHI F, SETTI G, ROVATTI R. A fast chaos-based true random number generator for cryptographic applications[C]//The Solid-State Circuits Conference. 2006: 130-133.

[10] PARESCHI F, SETTI G, ROVATTI R. Implementation and testing of high-speed CMOS true random number generators based on chaotic systems[J]. IEEE Transactions on Circuits and Systems I-Regular Papers, 2010, 57(12): 3124-3137.

[11] 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.

[12] 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.

[13] 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.

[14] GHIL M, MULLHAUPT A. Boolean delay equations. II. Periodic and aperiodic solutions[J]. Journal of Statistical Physics, 1985, 41(1-2): 125-173.

[15] BOCKMAN S F. Lyapunov exponents for systems described by differential equations with discontinuous right-hand sides[C]//The American Control Conference. 1991: 1673-1678.

[16] ZHANG R, CAVALCANTE H L D D S, GAO Z, et al. Boolean chaos[J]. Physical Review E, 2009, 80(4): 045202(R).

[17] HAJIMIRI A, LIMOTYRAKIS S, LEE T H. Jitter and phase noise in ring oscillators[J]. IEEE Journal of Solid-State Circuits, 2002, 34(6): 790-804.

[18] DEMIR A, SANGIOVANNIVINCENTELLI A. Analysis and simulation of noise in nonlinear electronic circuits and systems[M]. Germany: Springer-Verlag, 1998.

[19] SUNADA S, HARAYAMA T, DAVIS P, et al. Noise amplification by chaotic dynamics in a delayed feedback laser system and its application to nondeterministic random bit generation[J]. Chaos, 2012, 22(4) : 047513.

[作者简介]

龚利爽（1991− ），女，河南漯河人，太原理工大学博士生，主要研究方向为混沌理论与混沌密码。

侯二林（1992− ），男，河南漯河人，太原理工大学硕士生，主要研究方向为物理随机数发生器技术。

刘海芳（1989− ），女，山西晋中人，太原理工大学博士生，主要研究方向为混沌理论与混沌密码。

李凯凯（1994− ），男，山西晋城人，太原理工大学硕士生，主要研究方向为物理随机数发生器技术。

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。