

文章编号:1001-9081(2010)07-1802-03

计算机迭代下混沌序列的周期研究

盛利元,全俊斌

(中南大学 物理科学与技术学院,长沙 410083)

(binbinquan@gmail.com)

摘要:研究了计算机迭代下基于浮点格式的混沌序列周期及其分布规律。通过构造与标准浮点格式匹配的非标准浮点格式,统计测算了六种常见混沌系统在不同浮点精度下退化的混沌序列周期及其分布,采用线性拟合方法获得了混沌序列周期随计算精度变化的分布关系,纠正了多年来基于定点格式的相应分布关系,为后续的混沌抗退化机制研究提供了一个合理的可用于实验测试的参考标准,也表明对于混沌序列而言,基于定点格式的结论不能简单随意推广到浮点格式。

关键词:混沌;浮点;有限精度效应;周期

中图分类号: TP309 **文献标志码:** A

Research on periods of chaotic sequences under computer iteration

SHENG Li-yuan, QUAN Jun-bin

(School of Physics Science and Technology, Central South University, Changsha Hunan 410083, China)

Abstract: Both the periods of chaotic sequences when iterating on computer and their distribution based on floating point formats have been studied in this paper. By constructing non-standard floating point formats matched with the IEEE standard ones, the periods of six common chaotic systems under different floating point precisions were measured. Using a linear fitting method, the distribution relationship between the periods of chaotic sequence and numerical precisions was obtained, which corrected the distribution relationship based on fixed point formats and gave an experimental criterion for the study of chaotic anti-degradation. This paper also shows that for the chaotic sequence, conclusions based on fixed point formats can not be simply extended to floating point formats.

Key words: chaos; floating point; finite-precision effect; period

0 引言

计算机或其他数字系统计算混沌系统时,有限的精度所带来的截断误差必定会使混沌序列退化为周期序列^[1-2],即所谓有限精度效应。密码学界普遍怀疑混沌密码算法存在因混沌退化而引起的安全性隐患^[3],短周期意味着弱密钥^[4]。人们为改善有限精度效应的负面作用相继提出了利用多个混沌系统迭代、迭代过程中加入扰动等方法^[4],但这些方法都是以牺牲系统运行速度或增加系统资源为代价的,即使如此,仍然不能从理论上证明混沌密码算法不存在由于混沌退化引起的安全性隐患。一种新的解决方案是,如果能够找到一种安全混沌^[5],它具有一定强度的抗退化能力,在可及的空间和可及的时间内不会因为混沌退化而出现周期轨道,根据密码分析学原理,由这样的混沌系统构造的密码算法对于混沌退化而言是安全的。混沌抗退化机制研究可能是解决混沌密码算法因混沌退化而引起的安全性问题的有效理论途径。本文研究基于浮点格式的混沌序列周期及其分布规律,作为混沌抗退化机制的重要内容之一,为混沌抗退化机制研究寻找一个合理的可用于实验测试的参考标准。在理论预期下,一个具有抗退化能力的混沌系统的平均序列周期必定远大于纯退化混沌系统的平均序列周期。

Cernak^[6]测得一维混沌序列的周期分布范围 $[0, 2^{p-\varepsilon}]$,其中 p 为比特位表示的计算精度, $\varepsilon = 0.68 \pm 0.05$; Beck等

人^[7]观察到类似结果,一维混沌序列的平均周期正比于 $(\frac{1}{N})^{-\eta}$,其中 $\frac{1}{N}$ 为计算精度, η 与 ε 相当。这些结论都是基于定点格式的,虽然沿用至今^[8],却只有定性意义,实际意义有限,特别是要作为混沌抗退化机制研究的定量评估标准,理论依据不充分。因为定点数定义在部分实数域上,当计算对象中存在一个或多个变量(包括中间变量)超出了定点数的定义域时,定点格式计算失效。另外,在给定精度下,定点格式的最小单元是常数,浮点格式的最小单元是数的指数函数,必然要影响计算对象,两者功能上存在显著差别^[9]。作为混沌系统抗退化能力的检验标准,需要在浮点格式下重新研究数字混沌序列周期及其分布规律。本文统计测算研究了6种定义于 $[0, 1]$ 上的离散混沌系统,较之Cernak等人的研究,结果表明,就混沌序列而言,定点格式的结论不能简单随意推广到浮点格式。

1 混沌序列周期搜索算法

设混沌系统迭代方程为:

$$x_{n+1} = f(x_n); n = 0, 1, 2, \dots \quad (1)$$

任意给定初始值 x_0 ,经一段瞬态演化后混沌系统将进入周期为 T 的循环状态,如图1所示, x_0 至 x_{t-1} 称为过渡态。搜索算法的目标是找出周期 T 的值。

对应图1,一种快速搜索算法如图2所示,步骤如下:

收稿日期:2010-01-10;修回日期:2010-03-01。 基金项目:国家自然科学基金资助项目(60672041)。

作者简介:盛利元(1956-),男,湖南益阳人,教授,主要研究方向:非线性系统、混沌加密; 全俊斌(1984-),男,广东湛江人,硕士研究生,主要研究方向:混沌加密。

混沌序列的周期,它们分别是:

1) Logistic 映射,由式(3)给出。

2) Tent 映射:

$$x_{n+1} = \begin{cases} \mu x_n, & 0 < x_n < 0.5 \\ \mu(1 - x_n), & 0.5 \leq x_n < 1 \end{cases} \quad (4)$$

其中 μ 为系统参数。

3) 指数映射:

$$x_{n+1} = a^{x_n} \pmod{1}; a > 1, 0 < x_n < 1 \quad (5)$$

其中 a 为系统参数。

4) PWLCM:

$$x_{n+1} = f(x_n) = \begin{cases} x_n/p, & 0 < x_n < p \\ (x_n - p)/(0.5 - p), & p \leq x_n < 0.5 \\ f(1 - x_n), & 0.5 \leq x_n < 1 \end{cases} \quad (6)$$

其中 p 为系统参数。

5) PWNLCM:

$$x_{n+1} = \begin{cases} \frac{a^2 \left(\frac{x_n}{p} \right)}{1 + (a^2 - 1) \left(\frac{x_n}{p} \right)}, & 0 < x_n \leq p \\ \frac{a^2 \left(\frac{x_n - p}{1 - p} \right)}{1 + (a^2 - 1) \left(\frac{x_n - p}{1 - p} \right)}, & p < x_n < 1 \end{cases} \quad (7)$$

其中 a 和 p 为系统参数。

6) 二维 Cat 映射:

$$\begin{cases} x_{n+1} = x_n + y_n \pmod{1} \\ y_{n+1} = x_n + 2y_n \pmod{1} \end{cases} \quad (8)$$

式(8)中无系统参数。

测算方法如下:对于一固定系统参数值,迭代初始值在 $(0,1)$ 区间上以间隔 0.001(二维 Cat 混沌系统以间隔 0.01)均匀取值,得到 999(二维 Cat 混沌系统为 99^2)个周期值,统计出最小值、最大值和平均值。测算程序用 VC++ 6.0 编写。

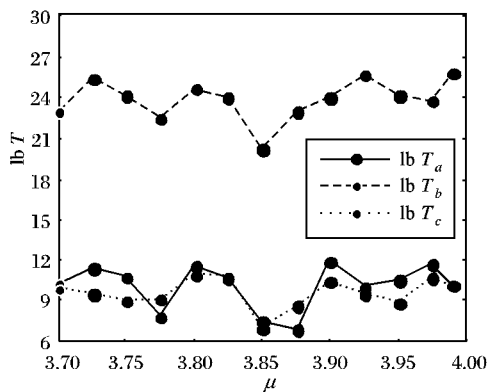


图5 三种数值表示方法下 Logistic 平均周期的对数分布图

3.2 测算结果及分析

图 6 给出了 Logistic 映射在不同计算精度 P 的非标准与标准浮点格式测算下的混沌序列周期分布规律,针对每一种计算精度,分别测算了最长周期 T_{\max} 、最短周期 T_{\min} 以及平均周期 \bar{T} 。由此可见,混沌序列的平均周期 \bar{T} 和最长周期 T_{\max} 与计算精度服从关系:

$$\text{lb } T = kP + b \quad (9)$$

其中 k 与 b 为最小二乘法给出线性拟合系数。其他 5 种混沌序列也具有相同的分布规律,各混沌序列的拟合系数由表 3 给出。

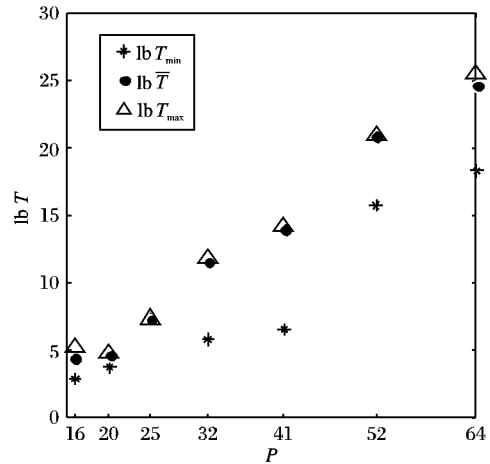


图6 Logistic 混沌系统周期分布图

表3 混沌系统平均周期的分布

混沌系统	系统参数	\bar{k}	\bar{b}	k_{\max}	b_{\max}
Logistic	3.8	0.45	-3.43	0.45	-3.37
	3.9	0.41	-1.91	0.41	-1.69
Tent	1.3	0.46	-4.64	0.46	-4.43
	1.7	0.42	-1.88	0.44	-1.92
指数映射	5	0.44	-1.67	0.44	-1.60
	8	0.41	-1.65	0.41	-1.34
PWLCM	0.1	0.46	-3.61	0.47	-3.78
	0.4	0.48	-4.35	0.48	-3.65
PWNLCM	0.1, 0.5	0.44	-2.03	0.44	-1.65
二维 Cat	—	0.81	-4.84	0.81	-4.60

由图 6 及表 3 给出的多种混沌系统的测算数据,再考虑到测算样本的有限性,若用 D 表示混沌系统的维度,则可归纳出在浮点格式下混沌序列周期的分布规律:

$$T \in [0, 2^{(0.45 \pm 0.05)PD}] \quad (10)$$

分布区间远小于定点格式下的 $[0, 2^{(0.68 \pm 0.05)P}]$ 。

同理,平均周期服从:

$$\bar{T} \sim 2^{(0.45 \pm 0.05)PD} \quad (11)$$

因此,对于一维混沌系统, double 型浮点格式下的混沌序列平均周期约为 64 bit 定点格式下的 $1/30\,000$ 。可见,用计算机研究混沌系统时,采用定点格式或浮点格式,所得结论不能轻易互相引用。

式(10)和式(11)给出了浮点格式下混沌序列周期的分布规律,为评估混沌系统的抗退化强度提供了一个参考标准。若混沌系统存在很强的抗退化能力,其序列周期的分布将出现异常而远远超出式(10)的范围。

4 结语

本文提出了一种混沌序列周期快速搜索算法和一种与标准浮点格式匹配的非标准浮点格式构造与实现方法,以此为基础,分别测算了计算机迭代下基于浮点格式的 6 种混沌序列的周期分布及其平均周期。结果表明:混沌序列的平均周期和最大周期随计算精度呈指数增长;在浮点格式下的混沌序列平均周期远小于定点格式下的平均周期;对于混沌系统

(下转第 1808 页)

计算花销主要是指所需的指数运算数、对运算数等。本协议与协议 ID-TT^[4]、ID-BD^[13]、ID-CMM^[6]、CPK-DDL^[7] 的比较结果如表 1 所示。

表 1 几个组群密钥交换协议效率的对比

协议	轮数	消息数	指数运算数	对运算数
ID-TT	$\lceil \log_3 n \rceil$	$5(n-1)$	$9(n-1)$	$5n\lceil \log_3 n \rceil + 3$
ID-BD	2	$2n$	$n(n+8)$	$4n$
ID-CMM	2	$2n$	$2n(n+1)$	$2n$
CPK-DDL	2	$2n$	$O(n^2)$	0
本协议	2	$2n$	$O(n^2)$	0

从表 1 中易知:协议 ID-TT 通信轮数与通信方数 n 有关,而剩下四个协议是常数轮的,但协议 ID-BD 不能抵抗共谋攻击^[14]。本协议能高效支持成员加入/离开操作,但协议 ID-CMM、CPK-DDL 不支持此操作并且协议 ID-CMM 需要双线性对运算。此外协议 ID-CMM 和 CPK-DDL 均不能抵抗临时密钥泄露攻击,但本协议提供了强安全性保证。综合各方面的考虑,本协议在安全性和效率方面都具有优势。此外,本协议还提供组群密钥交换协议的完全健壮性。协议执行过程中丢失的用户只会使其他用户接收不到该用户选择的部分密钥 k_i ,但剩余用户仍可以正确计算剩余用户之间共享的组群会话密钥 $k = H_1(k_{i_1} + \dots + k_{i_t})$,其中 U_{i_1}, \dots, U_{i_t} 为剩余用户。丢失用户可以通过加入组群操作继续参与组群安全通信。

6 结语

基于高效 CPK 体制,本文提出了一个两轮的强安全组群密钥交换协议。本协议提供显式密钥认证和完全的健壮性,高效支持多成员动态加入或者离开,并且成员加入或者离开操作能确保前向保密性和后向保密性。它能一直保持会话密钥的秘密性,除非某一方的会话临时私钥和长期私钥同时泄露。它也能抵抗密钥泄露伪装攻击和临时密钥泄露攻击,提供完美的前向安全性。此外,本协议相当于提供了一个设计常数轮强安全组群密钥交换协议的方法,且大部分的秘密共享体制均可直接应用于本协议。

(上接第 1804 页)

研究而言,定点格式下与浮点格式下所得的研究结果不能轻易相互引用。本文给出的混沌序列周期随浮点计算精度变化的分布关系,对于混沌加密理论而言具有重要意义,为寻找混沌系统的抗退化机制提供了一个检测的参考标准。

参考文献:

- [1] LI SHUJUN, CHEN GUANRONG, MOU XUANQIN. On the dynamical degradation of digital piecewise linear chaotic maps[J]. International Journal of Bifurcation and Chaos, 2005, 15(10): 3119-3151.
- [2] GREBOGI C, OTT E, YORKE J A. Roudoff-induced periodicity and the correlation dimension of chaotic attractors[J]. Physical Review A, 1988, 38(7): 3688-3692.
- [3] CURIAC D I, IERCAN D, DRANGA O, et al. Chaos-based cryptography: end of the road? [C] // Proceedings of the International Conference on Emerging Security Information, Systems, and Technologies. Washington, DC: IEEE Computer Society, 2007: 71-76.
- [4] LI S J, MOU X Q, CAI Y L, et al. On the security of a chaotic en-

参考文献:

- [1] AL-RIYAMI S, PATERSON K. Certificateless public key cryptography [C] // Proceedings of Asiacrypt'03. Berlin: Springer-Verlag, 2003: 205-217.
- [2] JOSEPH K L, MAN H A, WILLY S. Self-generated-certificate public key cryptography and certificateless signature/encryption scheme in the standard model [C] // Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security. New York: ACM, 2007: 273-283.
- [3] 唐文, 南湘浩, 陈钟. 基于椭圆曲线密码系统的组合公钥技术 [J]. 计算机工程与应用, 2003, 39(21): 1-3.
- [4] BARUA R, DUTTA R, SARKAR P. Extending Joux's protocol to multi-party key exchange [C] // Proceedings of Indocrypt'03. Berlin: Springer-Verlag, 2003: 205-217.
- [5] 宋震, 周贤伟, 奚文华. 一种基于身份标识的 MANET 组密钥协商协议 [J]. 电子学报, 2008, 36(10): 11-18.
- [6] CAO C J, MA J F, MOON S J. Provable efficient certificateless group key exchange protocol [J]. Wuhan University Journal of Natural Sciences, 2007, 12(1): 041-045.
- [7] 邓少峰, 邓帆, 李益发. 基于 CPK 的可证安全组群密钥交换协议 [J]. 信息安全与通信保密, 2009(8): 316-319.
- [8] KRAWCZYK H. HMQV: A high-performance secure Diffie-Hellman protocol [C] // Proceedings of CRYPTO 2005. Berlin: Springer-Verlag, 2005: 546-566.
- [9] LAMACCHIA K, LAUTER K, MITYAGIN A. Stronger security of authenticated key exchange [C] // Proceedings of ProvSec 2007. Berlin: Springer-Verlag, 2007: 1-16.
- [10] BRESSEN E, MANULIS M. Securing group key exchange against strong corruptions [C] // Proceedings of ASIACCS'08. New York: ACM, 2008: 249-260.
- [11] 南湘浩, 陈华平. 组合公钥 (CPK) 体制标准 V2.1 [J]. 计算机安全, 2008(9): 1-2.
- [12] BRESSON E, CHEVASSUT O, POINTCHEVAL D, et al. Provably authenticated group Diffie-Hellman key exchange [C] // Proceedings of ACM CCS'01. New York: ACM, 2001: 255-264.
- [13] CHOI K, HWANG J, LEE D. Efficient ID-based group key exchange with bilinear maps [C] // Proceedings of PKC'04. Berlin: Springer-Verlag, 2004: 130-144.
- [14] ZHANG F, CHEN X. Attack on an ID-based authenticated group key exchange scheme from PKC 2004 [J]. Information Processing Letters, 2004, 91(4): 191-193.

crypton scheme: Problems with computerized chaos in finite computing precision [J]. Computer Physics Communications, 2003, 153(1): 52-58.

- [5] 盛利元, 闻姜, 曹莉凌, 等. TD-ERCS 混沌系统的差分分析 [J]. 物理学报, 2007, 56(1): 78-83.
- [6] CERNAK J. Digital generators of chaos [J]. Physica Letters A, 1996, 214(3/4): 151-160.
- [7] BECK C, ROEPSTORFF G. Effects of phase space discretization on the long-time behavior of dynamical systems [J]. Physica D, 1987, 25(1/3): 173-180.
- [8] MAO YAOBIN, CAO LIU, LIU WENBO. Design and FPGA implementation of a pseudo-random bit sequence generator using spatio-temporal chaos [EB/OL]. [2009-10-05]. <http://citeseerx.ist.psu.edu/viewdoc/download%3Fdoi%3D10.1.1.113.9525>.
- [9] DAVID G. What every computer scientist should know about floating-point arithmetic [J]. ACM Computer Surveys, 1991, 23(1): 5-48.
- [10] IEEE Std 754-2008. IEEE standard for floating-point arithmetic [S], 2008.