基于扰动时空混沌系统的动态S盒设计

赵 耿[1],马英杰[1],陈 磊[2],董有恒[2],侯艳丽[3]
(1. 北京电子科技学院,北京 100070; 2. 北京邮电大学,北京 100876; 3. 西安电子科技大学,陕西西安 710071)

摘 要: 传统时空混沌系统的分布比较集中,其生成序列的均匀性较差,本文基于初等元胞自动机构造了新型扰动单向耦合映像网络时空混沌系统,系统的分布图和相图数值仿真结果表明了扰动系统能够改善原系统的均匀性,提高系统的动力学复杂性. 采用均匀化的扰动时空混沌系统设计了动态S盒生成算法,根据动态更新策略生成动态S盒,对该算法产生的S盒进行非线性度、严格雪崩准则和差分均匀性的统计分析,结果表明均匀化扰动时空混沌系统产生的动态S盒安全性更高.

关键词: 时空混沌; 初等元胞自动机; 扰动; 动态S盒; 安全性分析
中图分类号: TP393 **文献标识码:** A **文章编号:** 0372-2112(2022)08-2037-06
电子学报URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20210200

Design of Dynamic S-Box Based on Perturbed Spatiotemporal Chaotic System

ZHAO Geng[1], MA Ying-jie[1], CHEN Lei[2], DONG You-heng[2], HOU Yan-li[3]
(1. *Beijing Electronic Science and Technology Institute*, *Beijing* 100070, *China*;
2. *Beijing University of Posts and Telecommunications*, *Beijing* 100876, *China*;
3. *Xidian University*, *Xi'an*, *Shaanxi* 710071, *China*)

Abstract: The distribution of traditional spatiotemporal chaotic system is relatively concentrated, and the uniformity of its generating sequence is poor. In this paper, a new spatiotemporal chaotic system with perturbed one-way coupled map lattice is constructed based on elementary cellular automata. The numerical simulation results of the distribution diagram and phase diagram of the system show that the perturbed system can improve the uniformity of the original system and increase the dynamic complexity of the system. A dynamic S-box generation algorithm is designed based on the homogenized disturbed spatiotemporal chaotic system, and the dynamic S-box is generated according to the dynamic update strategy. The statistical analysis of nonlinearity, strict avalanche criterion and differential uniformity of the S-box generated by the algorithm is carried out. The results show that the dynamic S-box generated by the homogenized disturbed spatiotemporal chaotic system is more secure.

Key words: spatiotemporal chaos; elementary cellular automata; disturbance; dynamic S-box; safety analysis

1 引言

现代分组密码中,置换和替换网络是不可或缺的,如AES(Advanced Encryption Standard)算法. 其中S盒作为分组密码中唯一的非线性部件,主要作用就是实现替换运算[1],构造动态S盒的方法有很多,利用混沌系统良好的伪随机性质来构造动态S盒已经成为构造S盒的一个重要方法[2]. 唐国坪等提出一种基于Logistic映射的两步构造S盒的方法,尽管这种设计方法很有效、实用,但还是存在着随机性和不可以测性不够强的缺点[3,4]. 陈果等用三维的Baker映射设计了一种S盒克服了这些缺点[5]. 王永[6]等和Ozkaynak[7]等分别提出了利用帐篷映射和连续时间的Lorenz混沌系统来构造S盒. 佟晓筠提出了一种新的超混沌系统,并将其用于生成置换和替代图像像素的密钥流,使用动态S盒设计加密算法[8]. 闵乐泉设计了基于分段非线性鲁棒混沌映射的伪随机数发生器,提出了批量生成S盒的算法[9]. Akram Belazi提出了一种基于正弦映射的S盒构造的有

收稿日期:2021-02-02;修回日期:2021-06-17;责任编辑:梅志强
基金项目:国家自然科学基金(No.61772047);北京高校"高精尖"学科建设项目(No.3201017)

效方法[10]. Majid Khan 提出基于混沌布尔函数构造 S 盒,并将其用于图像加密[11]. 这些构造方法为得到抵抗差分密码分析和线性密码分析能力好的 S 盒提供了思路. 朱虹宏等基于多混沌系统及复合思想,引入 Arnold 映射置乱算法构造了一种混沌 S 盒[12]. Islam 等构造了四维四翼超混沌系统,并以此设计了一种混沌 S 盒[13]. 然而上述方法所涉及到的混沌映射均在相空间或者回归映射中存在固定结构的吸引子,极易受到相空间重构[14]或者回归映射分析[15]的攻击,而且当混沌系统在有限精度的计算机中运行时会出现退化显现[16],出现周期现象,严重威胁到混沌密码系统的安全性. 基于上述原因,Peizhao Zhou 等人提出了一种基于 PWLCM (Piece Wise Linear Chaotic Map)-sin 映射的耦合映射格子的时空混沌系统[17],并用其生成了 S 盒,分析表明该系统生成的 S 盒具有良好的非线性,然而,每个格子生成的序列在回归映射中依然具有明显的固定帐篷形状,依然易受到回归映射分析攻击. 王永[18]等人为了解决时空混沌系统中存在的概率分布不均以及回归映射中形态结构固定的弱点,向基于分段 Logistic 映射的二维耦合映像格子模型添加了偏移量,使得结果更加均匀,然而该文仅仅对该系统的性能进行了分析并未涉及到模型的应用.

为了改进上述缺点,本文提出基于初等元胞自动机(Elementary Cellular Automata,ECA)的新型扰动单向耦合映像网络时空混沌系统,并进行了分布图、分岔图和相图的数值仿真,结果表明扰动系统能够改善原系统的均匀性,提高系统的动力学复杂性. 采用均匀化的扰动时空混沌系统设计了动态 S 盒生成算法,并进行了非线性度、严格雪崩准则和差分均匀性的统计分析,结果表明均匀化扰动时空混沌系统产生的动态 S 盒具有更高的安全性.

2 基于初等元胞自动机扰动的时空混沌系统构造

2.1 单向耦合映像网络时空混沌系统及其数值仿真

单向耦合映像网络是一类时空混沌系统,具有易于产生、支持并行计算等优点,其定义为

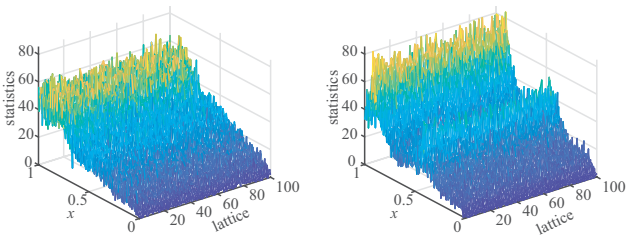
$$x_{n+1}(i)=(1-\varepsilon)f(x_n(i))+\varepsilon f(x_n(i+1)) \tag{1}$$

式中 $n=0,1,2,\cdots$ 和 $i=1,2,3,\cdots,L$ 分别代表时间维度(迭代次数)和空间维度(格点索引),$x_n(i)$ 表示在时刻 n 时,第 i 个格点的状态值,L 表示格点的总数,$\varepsilon(\varepsilon\in(0,1))$ 代表耦合强度. 该系统的边界条件可以表示为 $x_n(i-1)=x_n(L)$,底层映射 f 为 Logistic 映射,即

$$f\left(x_n(i)\right)=ux_n(i)\left(1-x_n(i)\right) \tag{2}$$

当参数 $\varepsilon=0.625$,$u=4$,$L=100$ 时,式(1)所示单向耦合映像网络的分布图如图 1(a)所示,当参数 $\varepsilon=0.875$,$u=4$,$L=100$ 时,单向耦合映像网络的分布图如图 1(b)所示. 从图 1 可以看出,参数 ε 的取值能够影响单向耦合映像网络时空混沌系统的分布情况,该系统存在均匀性较差的缺点.

当参数 $u=4$,改变参数 ε 的取值,式(1)所示系统的相图如图 2 所示. 从图 2 可以看出,参数 ε 的取值能够影响单向耦合映像网络时空混沌系统的相图,该系统存在动力学特性不够复杂的缺点.



(a) ε=0.625,u=4,L=100 分布图 (b) ε=0.875,u=4,L=100 分布图

图 1 单向耦合映像网络的分布图

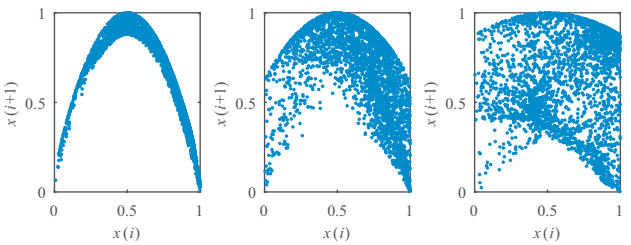


图 2 相图 $u=4$($\varepsilon=0.125$, $\varepsilon=0.625$, $\varepsilon=875$)

2.2 初等元胞自动机

元胞自动机是由数学家 Stanislaw M Ulam 和 John von Neumann 于 1948 年提出的[19,20]. 初等元胞自动机是一种特殊的一维元胞自动机. 初等元胞自动机的构成如图 3 所示.

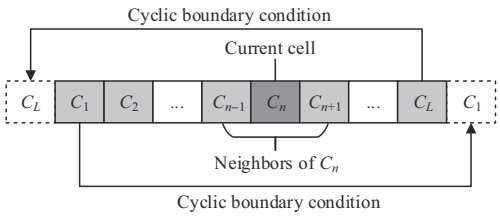


图 3 初等元胞自动机

图 3 中元胞 C_{n-1} 和 C_{n+1} 是元胞 C_n 的邻居,其中 C_1 和 C_L 互为邻居. 在 ECA 中,每次迭代的当前元胞状态值由当前元胞和其邻居的前次状态值决定,如式(3)所示

$$S_i^{t+1}=f(S_{i-1}^t,S_i^t,S_{i+1}^t) \tag{3}$$

其中 S_i^t 代表了元胞 C_i 在 t 时刻的状态值,t 代表时间维

度,即迭代次数,i代表空间维度,即元胞编号. 此处f为布尔函数并由局部转换规则决定,其本质上是一个由集合{000,001,010,011,…,111}到集合{0,1}的映射. 显然对于初等元胞自动机,共有256个转换规则. 其中以第105号转换规则为例,其转换表如表1所示.

根据W Li等人的研究[21],具有不同转换规则的ECA,其在迭代过程中所表现出的动态特性也互不相同. 任意一个具有全局混沌规则的ECA均能够用来构建本文所提出的时空混沌系统. 这些全局混沌规则已在表2中给出. 其中具有110号转换规则的ECA,我们简称为110号ECA,以此类推.

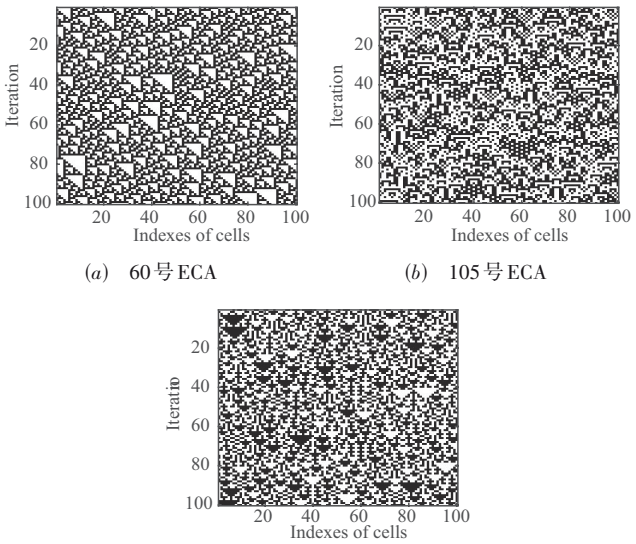
表1　第105号ECA转换规则

$S_{i-1}^t, S_i^t, S_{i+1}^t$	111	110	101	100	011	010	001	000
S_i^{t+1}	0	1	1	0	1	0	0	1

表2　全局混沌规则

Class	Rule number
Global chaotic	18(183), 22(151), 30(86, 135, 149), 45(75, 89, 101), 60(102, 153, 195), 90(165), 105, 106(120, 169, 225), 129(126), 137 (110, 124, 193), 146(182), 150, 161(122)

为了进一步说明具有这些混沌规则的ECA在迭代过程中所表现的伪随机性. 我们在图4中展示了60号,105号以及150号的迭代结果.



(a)　60号ECA　　(b)　105号ECA

(c)　150号ECA

图4　全局混沌的ECA迭代结果

图4中黑色(白色)的方格代表本方格上的元胞其状态值为“1”(“0”),纵坐标代表迭代次数,由上至下递增,横坐标代表元胞索引. 显然,三种ECA均显示出伪随机性. 本文选择105号ECA用来构造时空混沌系统.

2.3　基于初等元胞自动机扰动的时空混沌系统构造及其数值仿真

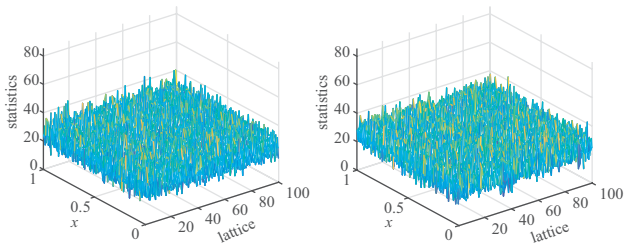
针对式(1)所示传统单向耦合映像网络时空混沌系统存在均匀性较差以及动力学特性不够复杂的问题,本文基于初等元胞自动机构造了新型扰动单向耦合映像网络时空混沌系统,即

$$x_{n+1}(i)=[(1-\varepsilon)f(x_n(i))+\varepsilon f(x_n(i+1)) +0.5\times p(S^n)\times\delta(s_i^n)]\bmod 1 \tag{4}$$

式中,S^n为初等元胞自动机的迭代结果,S_i^n为初等元胞自动机第i个元胞的迭代结果,其中$p(S^n)=\dfrac{\text{bin 2dec}[S^n(b_{35}b_{36}\cdots b_{66})]}{2^{32}-1}$,$\delta(s_i^n)=\begin{cases}1, s_i^n=1\\ -1, s_i^n=0\end{cases}$.

当参数ε=0.625,u=4,L=100时,式(4)所示扰动时空混沌系统的分布图如图5(a)所示,当参数ε=0.875,u=4,L=100时,扰动时空混沌系统的分布图如图5(b)所示.

从图1、图5的对比可以看出,提出的基于初等元胞自动机构造的新型扰动单向耦合映像网络时空混沌系统均匀性明显优于传统时空混沌系统.



(a)　ε=0.625,u=4,L=100分布图　　(b)　ε=0.875,u=4,L=100分布图

图5　扰动时空混沌系统的分布图

当参数u=4,改变参数ε的取值,式(4)所示系统的相图如图6所示.

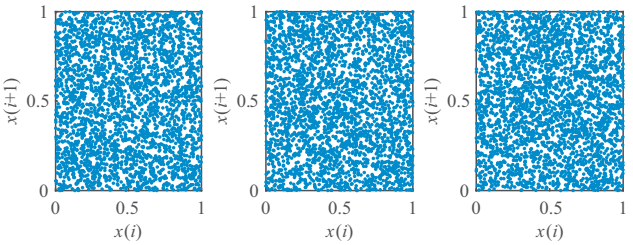


图6　相图u=4(ε=0.125, ε=0.625, ε=0.875)

从图2、图6的对比可以看出,提出的基于初等元胞自动机构造的新型扰动单向耦合映像网络时空混沌系统的动力学复杂性明显优于传统时空混沌系统.

3 基于扰动时空混沌系统的动态S盒设计

3.1 扰动时空混沌系统产生序列

处理函数：$\boldsymbol{M}_{\text{seq}}$=chaosGenFun($\boldsymbol{K}$,$n_0$,$n$)

输入：密钥$\boldsymbol{K}$,输出长度n_0,n.

描述：①密钥$\boldsymbol{K}$由8个长度相等的子密钥构成，可表示为($K(0)$,$K(1)$,$K(2)$,…,$K(7)$). ②n_0为要舍去的混沌系统初始迭代次数，n是后续的迭代次数.

输出：扰动时空混沌序列$\boldsymbol{M}_{\text{seq}}$.

描述：$\boldsymbol{M}_{\text{seq}}$是一个矩阵，大小为$n$×8，生成的混沌序列中的元素以64位双精度浮点数型进行储存.

3.2 生成密钥流

处理函数：[$\boldsymbol{K}_{\text{S}}$]=ksGenFun($\boldsymbol{M}_{\text{seq}}$,$n_{\text{ks}}$)

输入：$\boldsymbol{M}_{\text{seq}}$,输出长度$n_{\text{ks}}$.

描述：n_{ks}为后续步骤中所需密钥流的总长度.

输出：密钥流$\boldsymbol{K}_{\text{S}}$.

描述：$\boldsymbol{K}_{\text{S}}$是一个长度为$n_{\text{ks}}$的向量.

3.3 生成动态S盒

处理函数：[$\boldsymbol{S}_1$,$\boldsymbol{S}_2$]=SboxGenFun($\boldsymbol{K}_{\text{S}}$)

输入：$\boldsymbol{K}_{\text{S}}$.

描述：$\boldsymbol{K}_{\text{S}}$由上一个处理函数产生，要求其长度$8n\geqslant 512+n_{\text{ks}}$.

输出：S盒$\boldsymbol{S}_1$,$\boldsymbol{S}_2$.

描述：双S盒$\boldsymbol{S}_1$,$\boldsymbol{S}_2$均是大小为16×16的替换表，且满足双射条件. S盒和密钥流是由所生成$\boldsymbol{K}_{\text{S}}$的不同部分构成.

(1) 初始化S盒$\boldsymbol{S}_1$和$\boldsymbol{S}_2$. 按顺序赋值为0~255：

$$\boldsymbol{S}_1=\begin{bmatrix}0 & 1 & \cdots & 15\\ 16 & 17 & \cdots & 31\\ \vdots & \vdots & \vdots & \vdots\\ 240 & 241 & \cdots & 255\end{bmatrix};\ \boldsymbol{S}_2=\boldsymbol{S}_1 \tag{5}$$

(2) 构造两个16×16的随机矩阵$\boldsymbol{R}_1$,$\boldsymbol{R}_2$. 分别取$\boldsymbol{K}_{\text{S}}$的256个元素，$RV1$=$\boldsymbol{K}_{\text{S}}$($n_{\text{ks}}$,$n_{\text{ks}}$+255)，$RV2$=$\boldsymbol{K}_{\text{S}}$($n_{\text{ks}}$+256,$n_{\text{ks}}$+511)，然后逐行将$RV1$和$RV2$分别转换为两个随机矩阵$\boldsymbol{R}_1$,$\boldsymbol{R}_2$，大小为16×16.

(3) 利用$\boldsymbol{R}_1$,$\boldsymbol{R}_2$，对S盒$\boldsymbol{S}_1$和$\boldsymbol{S}_2$进行随机化处理. 对$\boldsymbol{S}_1$,$\boldsymbol{S}_2$的元素进行如下操作：

$$\text{swap}_{\boldsymbol{S}_1}(\boldsymbol{R}_1(i,j))=\begin{cases}k=(\boldsymbol{R}_1(i,j))_{\text{MSB}}\\ l=(\boldsymbol{R}_1(i,j))_{\text{LSB}}\\ \text{tmp}=\boldsymbol{S}_1(i,j)\\ \boldsymbol{S}_1(i,j)=\boldsymbol{S}_1(k,l)\\ \boldsymbol{S}_1(k,l)=\text{tmp}\end{cases} \tag{6}$$

其中，i,j=0,2,3,…,15代表$\boldsymbol{S}_1$中元素的索引，分别表示行和列. 函数$(x)_{\text{MSB}}$和$(x)_{\text{LSB}}$分别代表取x的最高四位和最低四位. $\text{swap}_{\boldsymbol{S}_1}(\boldsymbol{R}_1(i,j))$的作用就是根据$\boldsymbol{R}_1(i,j)$的值，得到与$\boldsymbol{S}_1$中位置$(i,j)$上的元素进行交换的元素索引$(k,l)$，并将两元素进行交换. 按顺序将$\boldsymbol{S}_1$中的所有元素即位置(1,1)至(16,16)按照式(6)进行交换乱序后得到随机化后的$\boldsymbol{S}_1$盒. 具体过程如图7所示. 同理，利用随机矩阵$\boldsymbol{R}_2$对$\boldsymbol{S}_2$盒进行上述乱序操作.

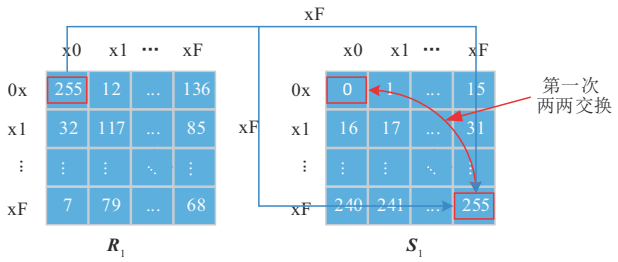


图7 构造S盒$\boldsymbol{S}_1$的示意图

4 动态S盒的安全性分析

4.1 非线性度

本文S盒的非线性度如表3所示，其平均值为105.75，略优于文献[4,11,12]的非线性度，说明该S盒抵抗线性分析的能力更强.

表3 S盒非线性度对比

S-box	Zhu[11]		Liu[12]		Chen[4]		Our approach	
NF	104	106	106	104	100	102	106	106
	108	106	100	106	103	104	104	106
	106	106	102	100	106	106	106	106
	100	108	106	108	106	108	104	108
Average	105.5		104		104.375		105.75	

4.2 严格雪崩准则

严格雪崩准则是指若某个输入比特发生改变，那么对应的输出比特发生改变的概率为1/2. 通过计算，该S盒的数据如表4所示.

表4 S盒严格雪崩准则对比

S-box	Ave-SAC	Difference with 0.500 0
Our approach	0.502 5	0.002 5
Zhu[11]	0.497 2	0.002 8
Liu[12]	0.507 8	0.007 8
Chen[4]	0.498 9	0.001 1

表4中列出了平均值与理论值0.5的差距. 根据表4可以得出，由本文算法得出的S盒仅与理论值0.5相差0.002 5，优于文献[11]和文献[12]，仅次于文献[4]提出的算法，可见该S盒能较好满足严格雪崩准则.

4.3 差分均匀性

通过计算可以得出本文S盒的差分均匀度与其他文献的S盒的差分均匀度的对比如表5所示，根据表5可以看出本文S盒的差分均匀度为10与文献[12]的相同，同样优于另外两个文献的数据. 由此说明本文S盒

针对差分线性分析的抵抗能力较强.

表5　S盒差分均匀性对比

S-box	Zhu[11]	Liu[12]	Chen[4]	Our approach
Max-DP	11	10	12	10

4　总结

本文基于初等元胞自动机构造了新型扰动单向耦合映像网络时空混沌系统,并进行了分布图、分岔图和相图的数值仿真,结果表明扰动系统能够改善原系统的均匀性,提高系统的动力学复杂性. 采用均匀化的扰动时空混沌系统设计了动态S盒生成算法,并进行了非线性度、严格雪崩准则和差分均匀性的统计分析,结果表明均匀化扰动时空混沌系统产生的动态S盒具有更高的安全性. 故本文方案可产生大量性能优秀的S盒,在分组密码设计等方面拥有良好的应用前景.

参考文献

[1] LI C, ZHANG Y, XIE E Y. When an attacker meets a cipher-image in 2018: A year in review[J]. Journal of Information Security and Applications, 2019, 48: 102361.

[2] 臧鸿雁, 黄慧芳. 基于均匀化混沌系统生成S盒的算法研究[J]. 电子与信息学报, 2017, 39(3): 575-581.
ZANG Hong-yan, HUANG Hui-fang. Research on the algorithm of generating S-box based on homogenization chaotic system[J]. Journal of Electronics & Information Technology, 2017, 39(3): 575-581. (in Chinese)

[3] TANG G P, LIAO X F, CHEN Y. A novel method for designing S-boxes based on chaotic maps[J]. Chaos, Solitons and Fractals, 2005(23): 413-419.

[4] 唐国坪. 混沌分组密码及其应用研究[D]. 重庆: 重庆大学, 2005.
TANG Guo-ping. Chaotic Block Cipher and Its Application Research[D]. Chongqing: Chongqing University, 2005. (in Chinese)

[5] CHEN G, CHEN Y, LIAO X F. An extended method for obtaining S-boxes based on three-dimensional chaotic Baker maps[J]. Chaos, Solitons and Fractals, 2017, (31): 571-579.

[6] WANG Y, WONG K W, LIAO X, et al. A block cipher with dynamic S-boxes based on tent map[J]. Communications in Nonlinear Science and Numerical Simulation, 2009, 14(7): 3089-3099.

[7] Özkaynaka Fatih, Ahmet Bedri Özerb. A method for designing strong S-Boxes based on chaotic Lorenz system[J]. Physics Letters A, 2010 (374): 3733-3738.

[8] LIU Yang, TONG Xiaojun, MA Jing. Image encryption algorithm based on hyper-chaotic system and dynamic S-box [J]. Multimedia Tools and Applications, 2016, 75(13): 7739-7759.

[9] 韩丹丹, 闵乐泉, 赵耿, 张丽姣, 闫世杰. 一维鲁棒混沌映射及S盒的设计[J]. 电子学报, 2015, 43(9): 1770-1775.
HAN Dan-dan, MIN Le-quan, ZHAO Geng, ZHANG Li-jiao, YAN Shi-jie. One-dimensional robust chaotic mapping and the design of S-box[J]. Acta Electronica Sinica, 2015, 43(9): 1770-1775. (in Chinese)

[10] Belazi Akram, Ahmed A Abd El-Latif. A simple yet efficient S-box method based on chaotic sine map[J]. Optik, 2017, 130: 1438-1444.

[11] Khan Majid, Shah Tariq, Syeda Iram Batool. Construction of S-box based on chaotic boolean functions and its application in image encryption[J]. Neural Computing and Applications, 2016, 27(3): 677-685.

[12] 朱虹宏, 佟晓筠, 张淼, 等. 基于动态复合混沌系统的S盒设计[J]. 南京大学学报(自然科学), 2018, 54 (240): 61-65.
ZHU Hong-hong, TONG Xiao-jun, ZHANG Miao, et al. S-box design based on dynamic compound chaotic system [J]. Journal of Nanjing University(Natural Sciences), 2018, 54 (240): 61-65. (in Chinese)

[13] ISLAM F U , LIU G J . Designing S-Box based on 4D-4wing hyperchaotic system[J]. 3D Research, 2017, 8(1): 1-9.

[14] ZHANG A, XU Z. Chaotic time series prediction using phase space reconstruction based conceptor network[J]. Cognitive Neurodynamics, 2020, 14(6): 849-857.

[15] PENG Y, SUN K, HE S. An improved return maps method for parameter estimation of chaotic systems[J]. International Journal of Bifurcation and Chaos, 2020, 30(4): 2050058

[16] LI S J, CHEN G R, MOU X Q. On the dynamical degradation of digital piecewise linear chaotic maps[J]. International Journal of Bifurcation and Chaos, 2005, 15(10): 3119-3151.

[17] ZHOU P, DU J, ZHOU K, et al. 2D mixed pseudo-random coupling PS map lattice and its application in S-box generation[J]. Nonlinear Dynamics, 2021, 103(1): 1151-1166.

[18] 王永, 赵毅, Gao Jerry, 等. 基于分段Logistic映射的二维耦合映像格子模型的密码学相关特性分析[J]. 电子学报, 2019, 47(3): 657-663.
WANG Yong, ZHAO Yi, GAO Jerry, et al. Analysis of cryptographic characteristics of two-dimensional coupled

map lattice model based on piecewise Logistic mapping [J]. Acta Electronica Sinica, 2019, 47(3): 657-663. (in Chinese)

[19] NEUMANN J, Burks A W, Theory of self-reproducing automata[J]. Mathematics of Computation, 1967, 21 (100): 745.

[20] Stephen Wolfram. Cellular automata as models of complexity[J]. Nature, 1984, 311(5985): 419-424.

[21] LI W, PACKARD N. The Structure of the elementary cellular automata rule space[J]. Complex Systems, 1990, 4 (3): 281-297.

作者简介

赵 耿 男,1964出生,四川苍溪人,博士,教授,主要研究领域为混沌密码理论及应用.
E-mail: zg@besti.edu.cn

马英杰 女,1979出生,吉林通化人,博士,副教授,主要研究领域为混沌保密通信.
E-mail: dmzm12@163.com

陈 磊 男,1991出生,博士,主要研究领域为密码通信.
E-mail: chenlei510@foxmail.com

董有恒 男,1995出生,山东济宁人,博士生,主要研究领域为混沌密码学.
E-mail: Dyh_231@bupt.edu.cn

侯艳丽 女,1995出生,河南洛阳人,硕士生,主要研究领域为混沌保密通信.
E-mail: yl_hou@163.com