2000 年 9 月
第 2 卷第 9 期

中国工程科学
Engineering Science

Sept.2000
Vol.2 No.9

学术论文

基于混沌的分组密码置换网络的设计

孙 枫，秦红磊，徐耀群，郝燕玲
（哈尔滨工程大学，哈尔滨 150001）

[摘要] 文章利用混沌序列的遍历性，给出了一种分组密码置换网络的设计，并对混沌序列的遍历性和置换网络的时间复杂度做了分析。计算机模拟结果显示，混沌分组密码置换网络具有复杂性高、抗破译性强的优点，可以增强信息系统的安全性。

[关键词] 混沌序列；置换网络；遍历性；时间复杂度

1 引言

现代科学技术发展日新月异，武器系统和作战指挥自动化、数字化的要求使计算机和信息系统在军事上得到了广泛的应用。武器系统和作战指挥在极大提高作战能力的同时，也增加了对计算机和信息系统的依赖性，计算机对抗这一新的对抗形式在现代和未来的信息战场中发挥重要作用。加密是增强计算机对抗性能的有效手段。

分组密码中的置换网络将明文和密文进行双射变换，它在分组密码学中起着中心作用，它的好坏直接影响到分组密码的抗破译性。置换网络的研究涉及开关函数理论和密码学等各个领域。分组密码的置换网络要满足以下要求[1]：a. 分组长度要足够大，防止明文穷举攻击；b. 密钥量要足够大，尽可能消除弱密钥并使所有密钥同等的好；c. 由密钥确定的置换网络算法要足够复杂，充分实现明文与密钥的扩散与混淆。

混沌现象是非线性动力系统中一种确定性的、类随机过程，混沌信号具有对初始值的高度敏感性、不可预测性，并具有遍历性[2,3]。因此，特别适合于混沌保密通信。本文将混沌序列引入分组密码置换网络，利用混沌映射产生的轨道点的遍历性，产生置换网络的双射变换，并对混沌序列的遍历性和置换网络的时间复杂度做了分析。通过计算机模拟，表明这种混沌分组密码置换网络具有复杂性高、保密性好等优点。

2 Logistic 映射性能分析

2.1 Logistic 映射的遍历性分析

混沌映射可用确定性的非线性差分方程来描述，不包含任何随机因素，其轨迹却有可能是完全随机的。而且，它在状态空间上具有遍历性。混沌的遍历理论认为[4]：任一个没有稳定周期轨道的 S 单峰映像 f 必有一个绝对连续不变测度的混沌轨道，因为它有一个测度，它必是混沌的。它由 Collet 和 Echmann 证明[5]给出。所谓映射 $f\{x\}$ 的遍历性是指：对于每个绝对可积函数 $\varphi(x)$ 和几乎所有的初始值 x_0 都有：

$$\lim_{n\to\infty}\frac{1}{N}\sum_{n=0}^{N}\varphi[f^{(n)}(x_0)]=\int\rho(x)\varphi(x)\mathrm{d}x \quad (1)$$

其中 $\rho(x)$ 是轨道的分布密度，$f^{(n)}$ 表示 $f(x)$ 的 n 重复合，由上式可以看出映射 $f(x)$ 对时间的平均等于对象空间状态的平均。混沌运动轨道点集 $\{x_n\}$ 的概率分布密度函数的定义为：

$$\rho(x)=\lim_{n\to\infty}\frac{1}{N}\sum_{n=1}^{N}\delta(x-x_n) \quad (2)$$

Logistic 映射是研究最多的混沌映射，由下式表示：

$$x_{n-1}=\mu x_n(1-x_n)\quad 0<\mu\leqslant 4\quad 0<x<1 \quad (3)$$

本文关心的是满映射，$\mu=4$ 的情况，Logistic 映射的输入和输出都分布在（0，1）上，当式（2）的

[收稿日期] 2000－05－25；修回日期 2000－08－01

[作者简介] 孙 枫（1944－），男，黑龙江桦川县人，哈尔滨工程大学教授

$N\to\infty$时，Logistic映射序列的概率分布密度函数$\rho(x)$如下式所示：

$$\rho(x)=\begin{cases}\dfrac{1}{\pi\sqrt{x(1-x)}} & 0<x<1\\ 0 & \text{其它}\end{cases} \tag{4}$$

式(4)表明式(3)所确定的序列具有遍历性，并且它产生的序列的概率密度分布函数与初始值无关。这就为混沌序列作为分组密码置换网络的映射函数提供了理论支持。

2.2 混沌遍历性时间复杂度分析

对于Logistic映射，其概率分布密度函数如式(4)所示，从式中可以看出混沌序列是遍历的，所以用它可以实现置换网络。这里设n为分组明文长度，将(0，1)区间n等分，m为Logistic混沌序列遍历这n个区间的迭代次数。如果迭代的次数$m>>n$，则会因为置换网络实现的时间复杂度过高，而没有实际意义，下面对m和n的关系进行分析。

为了使Logistic混沌序列对n个区间进行遍历，迭代次数m需满足下式：

$$m\int_{\frac{k}{n}}^{\frac{k+1}{n}}\rho(x)\mathrm{d}x\geqslant 1\Rightarrow m\geqslant 1/\int_{\frac{k}{n}}^{\frac{k+1}{n}}\rho(x)\mathrm{d}x$$

$$0\leqslant k<n \tag{5}$$

其中$\rho(x)$由式(4)确定，由定积分中值定理得到：

$$m\geqslant\frac{n}{\rho(\xi)}\quad\frac{k}{n}\leqslant\xi\leqslant\frac{k+1}{n} \tag{6}$$

由$\min(\rho(x))=\rho(0.5)=2/\pi$，得：

$$m\geqslant n\pi/2 \tag{7}$$

由上式可以看出，为了使混沌序列对n个区间进行遍历，迭代次数m需满足式(7)。但是，由于式(4)是在大量迭代的基础上得到的，还不能作为根本依据。下面分别对n取不同值，$x_0=i/1\,000$，$0<i<1\,000$时，对$m\leqslant kn$中的k进行统计分析，得出实用k值。

表1中max(m)为遍历n个区间的m的最大值，ave(m)为的m平均值，i'为满足$m\leqslant 30n$时遍历n个区间的x_0的个数。从表1中可以看出$\max(k)=\max(m)/n\approx 20$，$\bar{k}\approx\mathrm{lb}n$，不能遍历$n$个区间的$x_0$的个数有$999-i'=3$，这3个点为0.25、0.5、0.75，即周期点和收敛点。由此得到产生混沌置换网络的时间复杂度大约为混沌序列迭代$n\mathrm{lb}\,n$次的时间，可以满足实际应用。

表1 $\bar{k}$值统计分析表

Table 1 $\bar{k}$ statistics table

n	max(m)	ave(m)	i'	$\bar{k}$
32	435	161	996	5.0
64	895	400	996	6.3
128	2 166	952	996	7.4
256	5 243	2 160	996	8.4
512	9 063	4 798	996	9.4
1 024	19 403	10 744	996	10.5
2 048	47 174	23 422	996	11.4

3 用Logistic映射产生置换网络

置换网络是输入集A到输出C上的双射变换

$$f_k:A\xrightarrow{k}C \tag{8}$$

式中k为控制输入的变量，密码学中则为密钥。这里A是输入的n个明文量，C是n个输出的密文量，k为密钥矢量。双射变换要求在给定的k下可以从密文中唯一地恢复出明文。

本文利用混沌序列来实现置换网络的坐标变换，即将明文向量$A=(a_0,a_1,\cdots,a_{n-1})$的各个分量进行置换，得到密文向量$C=(c_0,c_1,\cdots,c_{n-1})$，其置换坐标由混沌序列在给定初始值下迭代产生的序列$\{x_0,x_1,\cdots,x_{n-1}\}$来得到，这里$x_0$即为密钥。置换过程如图1所示。其中：标志数组Flag[k]为遍历标志，当Flag[k]=FALSE时表示$(k/n,(k+1)/n)$区间未遍历到，i为已遍历区间的个数，j为Loigistic映射已经迭代的次数。为了使由于初值取得不好时置换过程能够结束，根据表1得出的结论，这里取当迭代次数$j>30\,n$时，重新选取初值。实际应用中要考虑有限精度对混沌序列的影响，使序列不脱离混沌态，一般混沌序列的精度应大于32位。

4 仿真试验及其结果分析

本文用Logistic映射产生分组长度为128的置换网络，用混沌序列的前7位作为置换网络的映射参数，精度为64位。混沌分组密码置换网络的置换和反置换过程如下：

a. 未置换前的明文“In recent years, some authors have tried to utilize the properties of chaos to implement a secure communication system in papers.”

b. 置换后的密文“snsiotteh eaf ushm e io Iertveeezom . ereoteptsa ccmaosciiiatntch ylstte enp shesei cmsrdnrmumoeitnora t u reo, p rroiuyppnaal”

c. 反置换后的明文“In recent years, some authors have tried to utilize the properties of chaos to implement a secure communication system in papers.”

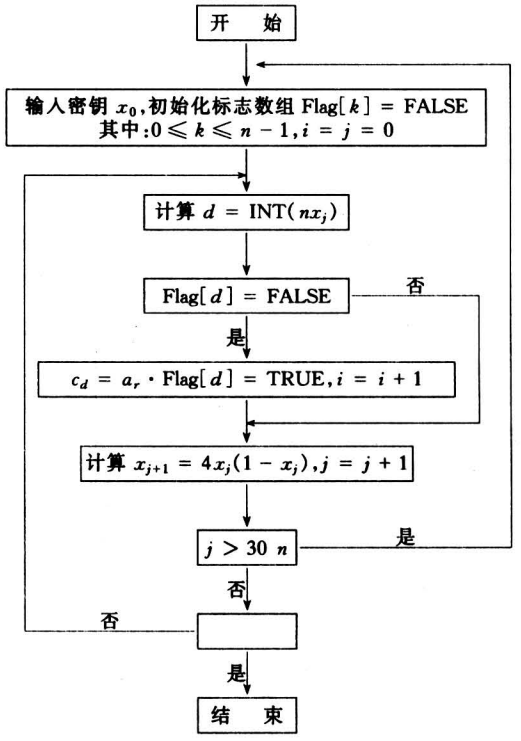

图 1　置换过程流程图

Fig.1　The flow diagram of permutation process

d. 密钥略有不同时置换出的明文“eeo. naumn h sseem philtriro, ioscahzioorotnma spo yvdeccraimamcp saeatu sute tr r tifsetspsee ne citoIh itteyreonreemtlpen”

虽然，混沌信号具有对初始值的高度敏感性、不可预测性，但由于初始值相差较小时，产生的前几个混沌序列取整后得到的序列相同，本文用多重迭代来解决这个问题。这里采用两个初始值 $x_{01}=0.2$ 和 $x_{02}=0.3$ 产生的混沌序列的两重迭代来产生置换网络，解密时初值取 $x_{01}=0.2000000000\ 01$ 和 $x_{02}=0.3000000000\ 001$ 的反置换结果如图 2.d 所示，可以看出，当用来产生加密和解密的混沌序列初始值相差很小时，也无法置换出正确的明文。如果用穷举搜索法对此加密方法进行破译时，计算机计算的时间复杂度为 $2^{2\times64}$，当用来产生置换网络的混沌序列的迭代次数增加，其破译将更加困难。

5　结论

以上的分析和模拟结果表明，利用混沌序列的遍历性来产生分组密码置换网络，克服了以往用简单的移位、取模、线性变换等实现置换网络的缺点，如：分组长度不能太大、置换简单等。它满足了分组密码置换网络的分组长度要求足够长、密钥量要足够大、密钥确定的置换网络算法要足够复杂等要求，充分实现了明文与密钥的扩散与混淆，是一种高抗破译性的算法。通过分析算法的时间复杂度，说明这种算法是实际可行的。将本文的研究成果用于对军事指挥和控制信息系统中，可以提高信息系统的安全性。

参考文献

[1] 王育民，刘建伟．通信网的安全、理论与技术[M]．西安：西安电子科技大学出版社，1999

[2] Hao B L. Elementary symbolic dynamics and chaos in dissipative systems [M]. Singapore: World Scientific Publishing Co Ltd, 1989

[3] Sakai H, Tokumaru H. Auto correlation of a certain chaos [J]. IEEE Trans ASSP, 1980, 289 (5): 588～590

[4] 陈式刚．映像与混沌[M]．北京：国防工业出版社，1992

[5] Collet P, Eckmann J P. Iterated maps on the interval as dynamical system [M]. Boston: Birkhauser, 1980

Design of Block Cipher Substitution Network on Chaos

Sun Feng, Qin Honglei, Xu Yiaoqun, Hao Yianling

(*Harbin Engineering University*, *Harbin* 150001, *China*)

[**Abstract**] In this paper, a design of block cipher substitution network is presented by use of the ergodic theory of chaos. The ergodic theory of chaos and the time complexity of substitution network is analyzed. The computer simulation result shows that the block cipher substitution network of chaos is highly complex and strong in anti-decipher .

[**Key words**] chaos sequence; permutation network; ergodic theory; time complexity