一维时空混沌密码系统及安全性分析

罗 轶

（湖南师范大学 物理与信息科学学院，湖南 长沙 410081）

摘 要：介绍了一维时空混沌密码系统的基本原理，构造了采用改进型Logistic映射的一维时空混沌密码系统模型，并用频数检验、序列检验、扑克检验、自相关检验和误差函数分析法等方法对系统的安全性进行了计算机仿真分析，证明该一维时空混沌密码系统具有较高的实用性和安全性。

关键词：一维时空混沌；密码系统；安全性

中图分类号：TP309.7 **文献标志码**：A **文章编号**：1673-9833(2010)05-0050-04

One-Dimension Spatio-Temporal Chaotic Cryptography and Its Security Analysis

Luo Yi

（School of Physics and Information Science, Hunan Normal University, Changsha 410081，China）

Abstract: The basic principle of one-dimension spatio-temporal chaotic cryptography is introduced, an one-dimension spatio-temporal chaotic cryptography model by utilizing modified Logistic-Map is setup, and the security of cryptography is analysed through the computer simulation, by frequency test, sequence test, playing card test, auto correlation test and error function analysis which proves the cryptography has better practicability and security.

Keywords: one-dimension spatio-temporal chaos; cryptography; security

现有混沌密码系统在安全性方面存在缺陷，笔者通过对混沌密码系统进行研究，发现混沌同步对控制参数的变化不敏感是造成混沌密码系统保密性低的主要原因[1-2]。由于时空混沌同步对控制参数的变化非常敏感，因此，有学者结合混沌同步和序列密码算法提出了一种安全性较高的一维时空混沌密码系统。本文对该一维时空混沌密码系统进行了部分改进，并对改进系统产生的密钥序列进行了随机性检验和安全性能分析，以验证改进系统应用的可行性和安全性。

1 一维时空混沌密码系统基本原理

王亥、匡锦瑜、胡岗、王建明和李吉忠等人在文献[3-6]中提出了一个一维时空混沌密码系统，该系统结构如图1所示。图中编码端和解码端各有1个单向耦合映射格子（one-way coupled map lattice，OCML）系统，分别用作产生加密密钥和解密密钥。

编码端OCML系统的方程为：

$$\begin{cases} x_i(n+1)=(1-\varepsilon_i)f(x_1(n))+\varepsilon_i f(D_n) \quad (i=1), \\ x_i(n+1)=(1-\varepsilon_i)f(x_i(n))+\varepsilon_i f(x_{i-1}(n)) \\ \qquad\qquad (i=2,3,\cdots,L), \\ D_i=c_n/2^{32}. \end{cases} \tag{1}$$

式中：n 代表离散时间；

i 代表空间位置；

L 代表OCML系统的长度；

c_n 为密文；

D_n 为两端OCML系统的驱动信号；

ε_i 为OCML系统的耦合参数，一般取 $\varepsilon_i \in [0.9,1]$，系

收稿日期：2010-06-04

基金项目：湖南师范大学青年科学基金资助项目（10706）

通信作者：罗 轶（1980-），男，广西陆川人，湖南师范大学讲师，博士生，主要研究方向为个人通信和保密通信，

E-mail：km_luoyi@sina.com

统前 w 个格点的耦合参数 $\varepsilon_i(i=1,2,\cdots,w$，$w$ 为系统主密钥个数)为系统的主密钥，后 $L-w$ 个格点的耦合参数 ε_i ($i=w+1,w+2,\cdots,L$)公开；

函数 $f(\cdot)$ 的形式为 $f(x)=4x(1-x)$。

解码端 OCML 系统的方程为式（1）的逆过程，即将式（1）中的输入信号 x 替换为相应输出信号 y 即可。

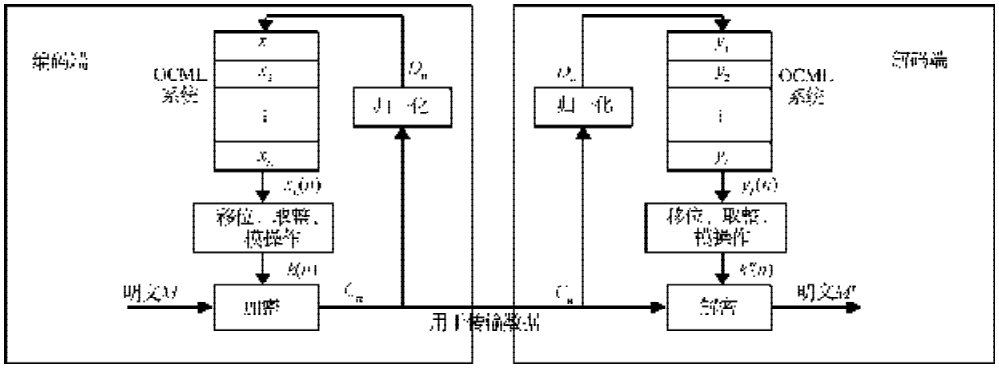


图 1　一维时空混沌密码系统框图

Fig. 1　Block diagram of one-dimension spatio-temporal chaotic cryptography

本文对函数 $f(\cdot)$ 的形式进行了修改，采用改进型 Logistic 映射，即 $f(x)=1-2x^2$，根据文献[3]的分析可知，改进型 Logistic 映射相对于标准型 Logistic 映射具有更为理想的自相关性、互相关性和伪随机性。

在加密通信方案中，编码端 OCML 系统的输入信号 $x_L(n)$ 经过变换（移位、取整和模操作）后获得 32 位的加密密钥，变换方程为：

$$k(n)=\mathrm{INT}\left(x_L(n)\times 2^l\right)\bmod 2^{32}, \tag{2}$$

同样，解码端 OCML 系统的输出信号 $y_L(n)$ 经过同样的变换后获得 32 位解密密钥，变换方程为：

$$k'(n)=\mathrm{INT}\left(y_L(n)\times 2^l\right)\bmod 2^{32}, \tag{3}$$

式（2）和（3）中：l 定义为放大倍数（整数），$l\in[32,52]$。

在图 1 所示的方案中，加密和解密可采用多种传统算法，本文采用相加取模算法。

设明文 $M=\{m_0,m_1,\cdots\}$ 的每个数据 m 和密文 $C=\{c_0,c_1,\cdots\}$ 对应的数据 c 均为 p 位(p=32)，k 为加密密钥，k' 为解密密钥，$M'=\{m_0',m_1',\cdots\}$ 为还原的明文数据，加密变换为：

$$c=(m+k)\bmod 2^{32}, \tag{4}$$

解密变换为：

$$m'=(c-k')\bmod 2^{32}, \tag{5}$$

式（4）和（5）中：k 和 k' 分别取自式（2）和（3）。

当编码端 OCML 系统与解码端 OCML 系统达到同步时，加密密钥 k 与解密密钥 k' 相同，则 m 与 m' 相同，即可以无失真的还原出明文数据。

2　系统安全性能分析

在自同步时空混沌密码系统中，密文信号充当两个角色，它既是明文信息的载体，也是解码系统的驱动信号。针对密文信号所充当的角色不同，攻击者可以采用不同的攻击方法对密码系统进行攻击。本文将从系统产生的密钥序列的随机性检验和抗误差函数分析法攻击这两个方面来分析系统的安全性能。

2.1　密钥序列的随机性检验

密文信号作为明文信息的载体，攻击者可以研究密文信号的统计特性，从而破解出产生该信号的行为特性。在数字实现方式下，由于存在有限精度效应，得到的密钥序列并非完全随机的，是伪随机序列，一般采用几种随机性测试方法，如检验的显著性水平不大于 0.05，则序列可通过检验。本文采用文献[7-8]中介绍的 4 种随机性检验方法对一维时空混沌密码系统所产生的二进制密钥序列进行以下 4 种检验，设系统参数为：$w=1$，$L=25$，$l=50$，$\varepsilon_1\sim\varepsilon_{25}$ 分别取值为 0.92, 0.91, 0.915, 0.93, 0.932, 0.936, 0.941, 0.947, 0.935, 0.941, 0.945, 0.923, 0.915, 0.929, 0.944, 0.951, 0.957, 0.955, 0.959, 0.967, 0.971, 0.978, 0.988, 0.991, 0.971。

1）频数检验　它是用来测试序列中是否有大致相同数量的 0 或 1。设序列中 0 的个数 n_0，1 的个数为 n_1，$n=n_0+n_1$，计算检测统计量

$$\chi^2=(n_0-n_1)^2/n, \tag{6}$$

将计算值与 $\chi_1^2(0.05)=3.841$ 相比，如小则通过检验。

2）序列检验　序列检验的目的是检验序列中出现相同和不同相邻元素的概率是否大致相等。设 n_{00} 表示 00 数量，n_{01} 表示 01 数量，n_{10} 表示 10 数量，n_{11} 表示 11 数量，计算检测统计量

$$\chi^2=\frac{4}{n-1}\sum_{i=0}^{1}\sum_{j=0}^{1}\left(n_{ij}\right)^2-\frac{2}{n}\sum_{i=0}^{1}\left(n_i\right)^2+1, \tag{7}$$

检验结果小于 $\chi_2^2(0.05)=5.991$ 时，则通过检验。

3）扑克检验　将序列分成元素个数为 a 的分组，则每组可能出现 2^a 种排列方式，扑克检验用来检测不同组合出现的次数是否均匀以及各自的频数。本检测中 a=4，并设各种组合的频数为：$f_0, f_1, \cdots, f_{16}$，计算检验统计量

$$\chi^2 = \frac{2^a}{F}\sum_{i=0}^{2^a-1}(f_i)^2 - \sum_{i=0}^{2^a-1} f_i, \qquad (8)$$

检验结果小于 $\chi^2_{15}(0.05) = 24.996$，则通过检验。

经多次检测后，检验测量结果平均值如表 1 所示。

表 1　随机性检验结果

Table 1　Test of randomness

校验方法	对应显著水平 5% 的检验值	实测平均值
频数检验	3.841	0.778
序列检验	5.991	2.242
扑克检验	24.996	14.532

4）自相关检验　明文信号 M 和密文信号 C 的归一化自相关函数为：

$$C_m(m) = \sum_{n=1}^{N-m} x(n)x(n+m) \Big/ \sum_{n=1}^{N} x^2(n) \quad (m << N)。(9)$$

明文信号 M 的归一化自相关特性如图 2 所示，密文信号 C 的归一化自相关特性如图 3 所示。比较图 1 和图 2，可看出自相关性差的明文信号经过密钥序列加密后，产生的密文信号具有良好的自相关特性及更小的旁瓣值。

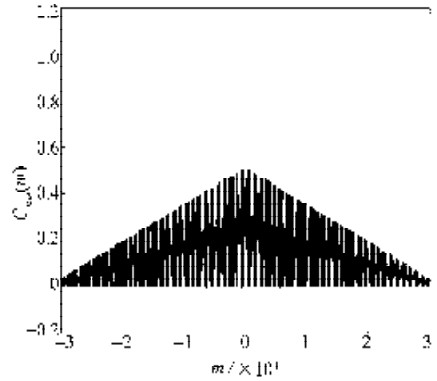


图 2　明文信号 M 的归一化自相关特性

Fig. 2　Normalized autocorrelation of clear text signal M

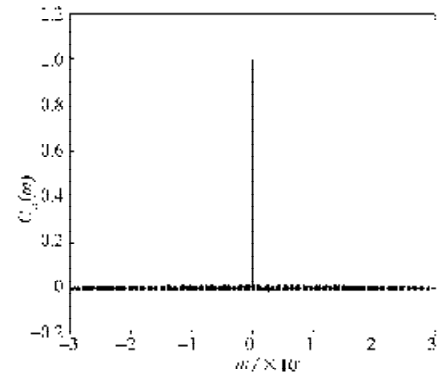


图 3　密文信号 C 的归一化自相关特性

Fig. 3　Normalized autocorrelation of secret text signal C

从以上 4 种检验结果可知，一维时空混沌密码系统产生的二进制密钥序列完全通过了随机性检验。

2.2　密钥序列的安全性能分析

由于系统中密文充当解码系统的驱动信号，所以对系统最有效的攻击方法是误差函数分析法（EFA，error function analysis），它是一种针对解码端系统的攻击方式。攻击者可以自己构造 1 个与合法接收者结构相同的解码端系统，并以测试密钥值代替系统真实的密钥值进行攻击[4,6]。假设系统主密钥只有 1 个(w=1)，即 ε_1，攻击者测试密钥为 ε_1'。设 $\Delta\varepsilon_1 = \varepsilon_1 - \varepsilon_1'$，定义时间 T 内混沌密码系统的误差函数为：

$$e(\Delta\varepsilon_1) = \frac{1}{T}\sum_{n=1}^{T}\left|k'(n) - k(n)\right|/2^r, \qquad (10)$$

式（10）中：$\{k(n)\}$ 为攻击者已知的密钥序列；

$\{k'(n)\}$ 为攻击者利用测试密钥在测试系统中运算后得到的密钥序列。

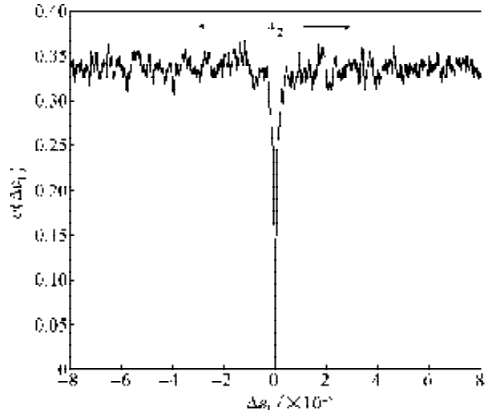
只有在测试密钥 ε_1' 与 ε_1 在一定精度内相等且测试系统与编码端系统达到同步的条件下，密钥序列 $\{k(n)\}$ 和 $\{k'(n)\}$ 相同时 $e(\Delta\varepsilon_1)$ 才会为 0，此时攻击者所使用的测试密钥就是真正的密钥。不断改变 ε_1' 的值，当 $\{k'(n)\}$ 取得最小值时，$e(\Delta\varepsilon_1) \approx 0$，即 $\varepsilon_1 \approx \varepsilon_1'$，此时攻击者就找到了正确的主密钥，从而解密出所有明文。

下面使用文献[6]中采用的误差函数分析法，仿真分析本文构造的一维时空密码系统模型的安全性能。图 4 给出了 T 为 500 次迭代时间，w=1，OCML 系统长度 L 和放大倍数 l 取不同值时，误差函数 $e(\Delta\varepsilon_1)$ 随 $\Delta\varepsilon_1$ 而变化的曲线。观察图 4 中的 a）图、b）图和 c）图可知，在远离密钥区域，误差函数是一条水平有起伏的曲线，$e(\Delta\varepsilon_1) \approx 1/3$；而接近密钥的区域，误差函数曲线大致形成一个喇叭口，且喇叭口宽度非常小，而且，随着系统长度的增大，喇叭口的宽度越来越窄，这也就说明误差函数对密钥的失配越来越敏感。当 L=2，l=50 时，误差函数对密钥失配的灵敏度约为 10^{-5}；而当 L=25，l=50 时，误差函数对密钥失配的灵敏度达到 10^{-10} 数量级。在远离密钥的区域，误差函数值在 $e(\Delta\varepsilon_1) \approx 1/3$ 附近上下摆动，且毫无规则，因此密码系统抵御误差函数攻击的性能主要由喇叭口范围的大小决定。用 W_L 表示系统长度为 L 时喇叭口的宽度，攻击者找到正确密钥的概率与 W_L 成正比。除系统长度 L 会影响混沌同步的灵敏度外，放大倍数 l 的选择也会对其造成影响，图 4 中的 d）图显示了 L = 25，l = 40 时误差函数的变化曲线，对比 c）图可发现，放大倍数 l 减小后，密码系统同步对密钥失配的灵敏度降低了，即攻击者找到正确密钥的概率增加了。与文献[6]中分析的结果进行比较，笔者发现，采用改进型 Logistic 映射的一维时空混沌密码系统较采用标准型 Logistic 映射的一维时

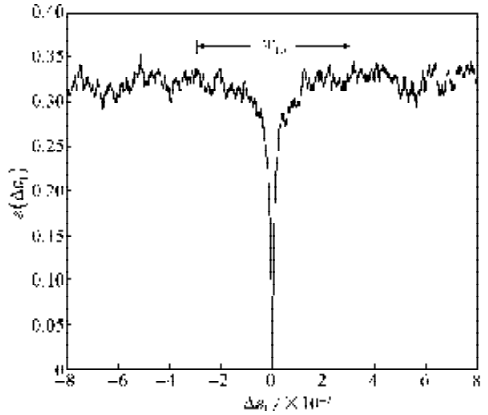
空混沌密码系统具有更好的安全性。

3　结语

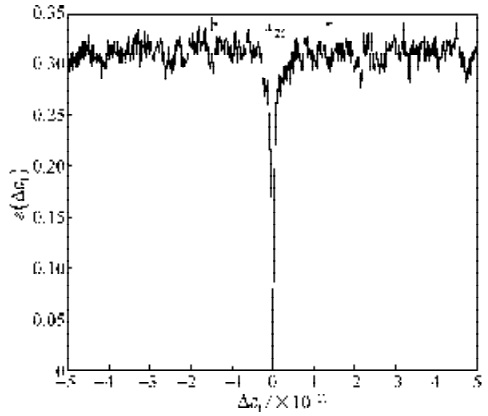
通过以上分析不难看出，采用改进型 Logistic 映射的一维时空混沌密码系统具有较强的安全性，系统产生的密钥序列能够通过随机性检验，能够抵御误差函数分析法的攻击。由于该密码系统结构较为简单，硬件上较容易实现，所以该密码系统也具有较好的实用性。可以预见，该一维时空混沌密码系统将会具有广阔的应用空间。



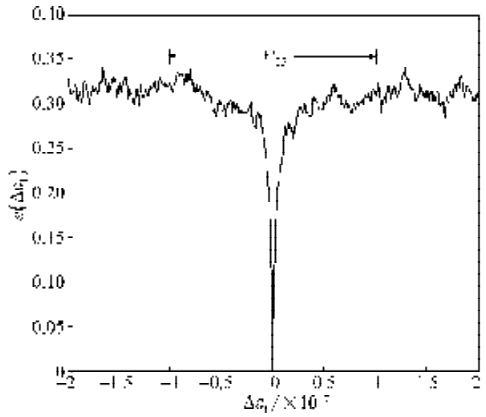
a）$l = 50, L = 2$



b）$l = 50, L = 10$



c）$l = 50, L = 25$



d）$l = 40, L = 25$

图 4　误差函数曲线

Fig. 4　Curve of error function

参考文献:

[1] Palacios A. Cryptography with Cycling Chaos[J]. Phys. Lett., 2002，303：345-351.

[2] Alvarez E. New Approach to Chaotic Encryption[J]. Phys. Lett., 1999，263：373-375.

[3] 王　亥，胡健栋. 改进型 Logistic-Map 混沌扩频序列[J]. 通信学报，1997，18(8)：71-77.
Wang Hai, Hu Jiandong. The Improved Logistic-Map Chaotic Spread-Spectrum Sequences[J]. Journal on Communications, 1997，18(8)：71-77.

[4] 匡锦瑜，邓　昆，黄荣怀. 利用时空混沌同步进行数字加密通信[J]. 物理学报，2001，50(10)：1856-1861.
Kuang Jinyu, Deng Kun, Huang Ronghuai. An Encryption Approach to Digital Communication by Using Spatiotemporal Chaos Synchronization[J]. Acta Physica Sinica, 2001, 50(10)：1856-1861.

[5] 胡　岗，萧井华，郑志刚. 混沌控制[M]. 上海：上海科技教育出版社，2000：181-188.
Hu Gang, Xiao JingHua, Zheng Zhigang. Chaos Control[M]. Shanghai: Shanghai Scientific and Technological Education Publishing House, 2000：181-188.

[6] 李吉忠. 语音压缩及混沌保密系统的 DSP 实现[D]. 北京：北京师范大学，2003.
Li Jizhong. DSP Implementation of Speech Compression and Chaotic Cryptosystem[D]. Beijing：Beijing Normal University, 2003.

[7] 冯国登. 密码分析学[M]. 北京：清华大学出版社，2002：55-62.
Feng Guodeng. Cryptanalysis[M]. Beijing：Tsinghua University Press, 2002：55-62.

[8] 邓　浩，华一满，倪皖荪. 混沌伪随机序列和数字语音保密通信[J]. 通信学报，1999，20(4)：29-35.
Deng Hao, Hua Yiman, Ni Wansun. Chaos Pseudo-Random Sequence and Digital Speech Secure Communication[J]. Journal on Communications, 1999, 20(4)：29-35.

（责任编辑：李玉珍）