一类数字混沌加密系统的安全性分析 [1]

胡国杰 冯正进

(上海交通大学机械工程学院 上海 200030)

摘 要 在 Kirchhoff 准则下，从选择密文攻击出发，探讨数字混沌加密系统的安全性能，并指出基于数字滤波器的数字混沌加密系统不具有很高的安全性，在选择密文攻击下，可以获得加密系统的密钥.

关键词 混沌，Kirchhoff 准则，选择密文攻击

中图号 TN918

1 引 言

自从混沌理论进入密码学应用领域以来，混沌加密方法得到了越来越多的重视. 由于混沌系统良好的统计学和拓扑学特性，它已经开始成为密码研究的重要前沿，但是由于大部分混沌加密系统都采用自然的混沌系统，它们不一定能提供具有严格密码学意义下的保密性. 为了提高混沌加密的保密性，人们的注意力转向数字加密. Chua 和 Lin[1,2] 指出数字滤波器具有混沌特性，当实现精度足够高时，数字滤波器与无限精度混沌系统在实际上无法区分. 在数字域进行数字混沌编码，克服了模拟混沌电路中加密器和解密器参数无法完全匹配的固有缺陷.

在 Chua 和 Lin 对数字滤波器混沌现象研究的基础上，Frey[3] 提出了利用一类非稳定的有限字长数字滤波器对数字信号进行加密的方案. Frey 的研究引起了学术界的广泛关注. Aislam 等人 [4] 在脉冲幅度调制通信链路中使用 Frey 的混沌加密 / 解密器，并估算了它的 BER，PDF 等指标，发现在信噪比较高的情况下，Frey 的加密 / 解密器性能表现良好. Werter[5] 对 Frey 提出的混沌加密 / 解密器进行了改进，改进后的结构实际上是一个数字随机数发生器.

但是，Frey 提出的基于数字滤波器的加密器由于结构简单，并不能提供很高的安全性能，Werter 指出 Frey 的加密器具有明显的重构特征. Frey 采用的加入混沌或随机信号扰动的方法虽然能提高加密性能，但是系统将同时失去自同步，所以不适用于实时信号保密传输. 文献 [6] 中 Chambers 对 Frey 提出的加密方案进行了分析，分析结果表明这种加密方案不具有很高的安全性.

为了进一步提高混沌加密系统的安全性，Götz[7] 提出了一类离散时间连续数值的加密系统，这类系统的输出具有均匀分布特性和良好的相关性能，完全满足密码序列的特性要求. 此外，周黎晖等 [8] 使用一类迭代的分段线性混沌映射构造出一种新型的数字混沌保密系统，该系统结合 n 阶延迟信号的组合来产生数字密码序列. 该密码序列特性决定于加密系统本身的动力学特性，且具有有限脉冲响应，故适用于实时数字信号加密 / 解密系统.

对于混沌保密系统而言，要保证系统的安全性，则系统必须通过现代密码学的分析方法的分析. 现代密码学认为：保密体制的保密性不是由其结构的保密性决定，衡量保密系统的保密性应在保密体制或者算法已知的条件下，考察其密钥的保密性 (Kirchhoff 加密准则)[9] . 对于保密通信系统而言，要保证系统的安全性，就必须保证整个系统 (加密器，解密器) 都是安全的. 本文在 Kirchhoff 准则下，从选择密文攻击出发，考察了文献 [7] 和文献 [8] 中混沌保密通信的解密器的安全性能，从而考察数字混沌加密系统的安全性能.

[1] 2002-05-24 收到，2002-10-14 改回

2 离散时间混沌加密系统安全性分析

Götz 在文献 [7] 中提出了一类离散时间连续数值的混沌加密系统，这种加密系统产生的序列具有均匀分布特性和良好的相关性能，完全满足密码序列的特性要求。

加密器为

$$s(t) = \mathrm{mod}\left[i(t) + \sum_{j=1}^{n} c_j s(t-j)\right] \tag{1}$$

解密器为加密器的逆系统，其表达式为

$$i^*(t) = \mathrm{mod}\left[r(t) - \sum_{j=1}^{n} c_j r(t-j)\right] \tag{2}$$

其中 $i(t)$ 为信息信号，$s(t)$ 为加密信号，$c_1 - c_n$ 为加密器、解密器的系数，$r(t)$ 为解密器接收信号，$i^*(t)$ 为恢复的信息信号，它们的取值范围均为 $[-1,1]$，$\mathrm{mod}(\cdot)$ 为取模函数：

$$\mathrm{mod}(x) = x - 2\lfloor (x+1)/2 \rfloor \tag{3}$$

当系数 $c_1 - c_n$ 满足 $c_n \in Z$, $|c_n| > 1$ 以及 $c_i \neq 0$, $i = 0, 1, \cdots, n-1$ 时，$s(t)$ 在 $[-1,1]$ 上是遍历且具有 n 维均匀分布的特性。

在这个加密系统中，由于加密器中存在反馈，对其进行选择明文攻击时，很难得到其确切的明文-密文对，此时不便对加密器进行分析；但是对于解密器而言，只有前馈环节，没有反馈环节，在选择密文攻击下，通过控制解密器的输入，可以得到确切的明文 - 密文对，因此解密器很容易被攻击。

对于 n 阶系统，若解密器的输入为 $e(n-1)$, $e(n-2)$, $e(n-3)$, $\cdots$, $e(0)$ 。此时，解密器的输出 $i(n)$ 等于 $\mathrm{mod}\left(\sum_{j=1}^{n} c_j e(n-j)\right)$, $e(\cdot)$ 已知。若 $-1 < \sum_{j=1}^{n} c_j e(n-j) < 1$, $\mathrm{mod}\left(\sum_{j=1}^{n} c_j e(n-j)\right) = \sum_{j=1}^{n} c_j e(n-j)$，所以很容易分析参数 $c_1 - c_n$ 。

例 设加密器的阶数为 $n = 2, c_1 = -1.5, c_2 = 3.0$。在选择密文攻击下，为了求出 c_1，设输入 $e_1 = \delta, \delta = 10^{-6}, e_2 = 0$，此时输出 $\mathrm{mod}(c_1e_1 + c_2e_2) = \mathrm{mod}(c_1e_1) = \mathrm{mod}(-1.5\times10^{-6}) = c_1e_1 = -1.5\times10^{-6}$，在知道输入、输出的情况下，我们可以求出 $c_1 = -1.5$。同样我们设 $e_1 = 0, e_2 = \delta$, $\delta = 10^{-6}$，此时输出 $\mathrm{mod}(c_1e_1 + c_2e_2) = \mathrm{mod}(c_2e_2) = \mathrm{mod}(3.0\times10^{-6}) = c_2e_2 = 3.0\times10^{-6}$，在知道输入、输出的情况下，我们可以求出 $c_2 = 3.0$。

所以，这种混沌加密系统的安全性不很高。在选择密文攻击下，我们容易得到其解密器的密钥 $c_1 - c_n$ 。

3 数字混沌加密系统 [8]

在文献 [7] 的基础上，周黎晖等 [8] 使用一类迭代的分段线性混沌映射构造出一种新型的数字混沌加密系统，该系统结合 n 阶延迟信号的组合来产生数字密码序列。该密码序列特性决定于迭代的分段线性混沌映射的动力学特性，且具有有限脉冲响应，故适用于实时数字加密 / 解密系统。图 1 为混沌加密系统加密器的结构图。

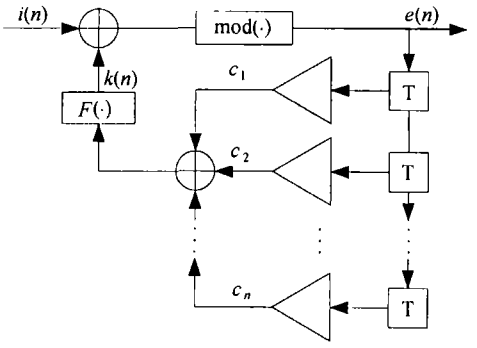

图 1 加密器

加密器为

$$k(t) = F\left(\sum_{i=1}^{n} c_i e(t-i)\right) \tag{4}$$

$$e(t) = \mathrm{mod}(i(t) + k(t)) \tag{5}$$

解密器为加密器的逆系统，其表达式为

$$k(t) = F\left(\sum_{i=1}^{n} c_i e(t-i)\right) \tag{6}$$

$$i(t) = \mathrm{mod}(e(t) - k(t)) \tag{7}$$

其中 $i(t)$ 为信息信号， $e(t)$ 为密文信号， $k(t)$ 为混沌系统产生的密钥信号， $c_1 - c_n$ 为加密器、解密器的系数，它们的取值范围均为 $[0,1]$， $\mathrm{mod}(\cdot)$ 与 (3) 式相同.

$f(\cdot)$ 为定义在区间 $I = [0,1]$ 上的混沌映射：

$$f(x(t)) = \begin{cases} x(t)/p, & x(t) \in (0,p) \\ (1-x(t))/(0.5-p), & x(t) \in (p,0.5) \\ f(1-x(t)), & \text{其它} \end{cases} \tag{8}$$

由于 $f(\cdot)$ 是充分扩展的分段线性 Markov 映射，系统具有均匀不变分布的特性[10]， $F(\cdot) = f^m(\cdot)$, $m > 1$.

4 混沌加密系统[8]安全性分析

4.1 安全性分析

对于 Markov 映射而言，其具有“分段线性”特性，即整个混沌映射分成若干线段. 在这些线段中，我们只要知道任意两点，就可以得到该线段上其他点的信息. 在这个加密系统中，由于加密器中存在反馈，对其进行选择明文攻击时，很难得到其确切的明文 - 密文对，此时不便对加密器进行分析；但是对于解密器而言，只有前馈环节，没有反馈环节，在选择密文攻击下，通过控制解密器的输入，可以得到确切的明文 - 密文对，因此解密器很容易被攻击.

对于 n 阶系统，若解密器的输入为 $e(n-1), e(n-2), e(n-3), \cdots, e(0)$. 此时，解密器的输出 $i(n)$ 等于 $e(n) - F\left(\sum_{j=1}^{n} c_j e(n-j)\right)$, $e(\cdot)$ 已知. 因为 $F(\cdot)$ 为“逐段线性”映射，当 $\sum_{j=1}^{n} c_j e(n-j) \to 0$， $e(n) - F\left(\sum_{j=1}^{n} c_j e(n-j)\right) = e(n) - k\sum_{j=1}^{n} c_j e(n-j)$ ，所以很容易分析参数 $c_1 - c_n$.

为了便于理解，我们在 $x = 0$ 的邻域进行分析，因为对于 Markov 映射而言， $x = 0$ 为固定点，即 $f(0) = 0$. 假设解密器的输入 δ 足够小，在 $x = 0$ 的邻域，则有

$$\left.\begin{aligned} F(\delta c_1 + 2\delta c_2) &= k \times (\delta c_1 + 2\delta c_2) = i_1 \\ F(2\delta c_1 + \delta c_2) &= k \times (2\delta c_1 + \delta c_2) = i_2 \\ F(\delta c_1 + \delta c_2) &= k \times (\delta c_1 + \delta c_2) = i_3 \end{aligned}\right\} \tag{9}$$

其中 k 为 $x=0$ 的邻域中直线段的斜率。因为 δ, i_1, i_2, i_3 已知，所以可以求出 c_1, c_2，同样可以求出 $c_3, c_4, \cdots, c_n$。

4.2 Markov 映射安全性分析

在求出 $c_1, c_2, \cdots, c_n$ 的基础上，我们可以对 Markov 映射进行安全性分析。由于充分扩展的 Markov 映射为分段线性，具有一定几何特征，如图 2 所示。在驱动信号 $u(t)$ 及其对应流密码 $k(t)$ 已知的情况下，若在 Markov 的同一线性分段上存在两个 (或更多)$k(t)$ 与 $u(t)$ 对应，则很容易求出混沌映射参数 p[11]：

$$p=(k_1-k_2)/(u_1-u_2) \tag{10}$$

当混沌函数进行多次迭代，有 $k(t)=f^m(u(t))$, $m>1$。此时 $f^m(\cdot)$ 映射具有 4^m 个线性分段区间，线性分段区间大小：

$$L=p^i(0.5-p)^{m-i},\quad i\in[0,m] \tag{11}$$

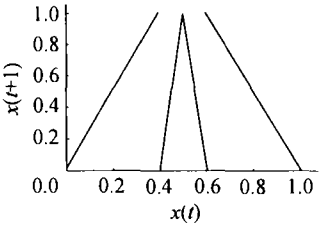

图 2　Markov 映射

此时，混沌映射 (8) 式上最大线性分段区间的大小为 $L_{\max}=(\max(p,0.5-p))^m$，最小线性分段区间的大小为 $L_{\min}=(\min(p,0.5-p))^m$，且有 $L_{\min}\le 2^{-2m}\le L_{\max}\le 2^{-m}$。

若迭代次数 $m\to\infty$，则 $L_{\max}\to 0$。对于任一个随机获取的明文 u_1，另一在 $[0,1]$ 上均匀分布的明文 u_2 在 u_1 处于同一线性分段上的概率 prob 为 $L_{\min}\le \text{prob}\le L_{\min}\le 2^{-m}$，显然，对任意指定的微小量 $\varepsilon>0$，总可以找到迭代次数 m，使得这类破译的概率降至足够低，prob$<\varepsilon$，但是对于已设计好的加密器 / 解密器而言，混沌映射的迭代次数是一定的，其破译概率大于一定的数值 λ, prob$>\lambda$。

4.3 举例

设加密系统为四阶系统，其中 $c_1=0.23, c_2=0.34, p=0.4$，即 $k=2.5$。在选择密文攻击下，设 $\delta=10^{-6}$，根据方程组 (9)，(10) 式对解密器进行分析。分析结果见表 1。

表 1　参数 c_1, c_2 和 p 的分析

m	i_1	i_2	i_3	i_1/i_2	i_3/i_2	c_1	c_2	$1/p$
2	$5.6875e-6$	$5e-6$	$7.125e-6$	1.1375	1.425	0.23	0.34	2.5
4	$3.5546875e-5$	$3.125e-5$	$4.453125e-5$	1.1375	1.425	0.23	0.34	2.5
8	0.00138854	0.00122070	0.00173950	1.1375	1.42499	0.23	0.34	2.499

其中 m 为 Markov 映射的迭代次数。同理，我们可以求出 c_3, c_4。所以，文献 [8] 提出的加密算法是不安全的。随着 Markov 映射的迭代次数增加，系统的安全性逐渐提高，但这种安全性的提高是以降低时效性为代价的。

5 结　论

本文在 Kirchhoff 准则下，从选择密文攻击出发，考察了数字混沌加密系统的安全性能。分析结果表明，现有的基于数字滤波器的混沌加密系统不具有很高的安全性，不适合于高加密强度的场合。

参 考 文 献

[1] L. O. Chua, T. Lin, Chaos in digital filters, IEEE Trans. on CAS., 1988, CAS-35(6), 648–658.

[2] T. Lin, L. O. Chua, On chaos of digital filters in the real world, IEEE Trans. on CAS., 1991, CAS-38(10), 557–558.

[3] D. R. Frey, Chaotic digital coding: an approach to secure communication, IEEE Trans. on CAS. II, 1993, CAS-II-41(10), 660–666.

[4] T. Aislam, J. A. Edwards, Secure communications using chaotic digital encoding, Electron. Lett., 1996, 32(3), 190–191.

[5] M. J. Werter, An improved chaotic digital encoder, IEEE Trans. on CAS. II, 1998, CAS-II-45(2), 227–229.

[6] W. G. Chambers, Comments on Chaotic digital encoding: an approach to secure communication, IEEE Trans. on CAS II, 1999, CAS-II-46(11), 1445–1447.

[7] M. Götz, K. Kelber, W. Schwarz, Discrete-time chaotic encryption systems-Part I: Statistical design approach, IEEE Trans. on CAS. I, 1997, CAS-I-44(10), 963–970.

[8] Li-Hui Zhou, Zheng-Jin Feng, A new idea of using one-dimensional PWL map in digital secure communications—Dual-resolution approach, IEEE Trans. on CAS. II, 2000, CAS-II-47(10), 1107–1111.

[9] B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C. New York: Wiley, 1996, 162–163.

[10] A. Baranousky, D. Daems, Design of one-dimensional chaotic maps with prescribed statistical properties, Int'l J. of Bifur. Chaos., 1995, 5(6), 1585–1598.

[11] 周红，凌燮亭，有限精度混沌系统的 m 序列扰动实现，电子学报，1997, 25(7), 95–97.

SECURITY PROPERTY OF A CLASS OF DIGITAL CHAOTIC ENCRYPTION SYSTEM

Hu Guojie Feng Zhengjin

(*School of Mechanical Eng., Shanghai Jiaotong University, Shanghai* 200030, *China*)

Abstract Under Kirchhoff principle, the security property of digital chaotic encryption system is discussed using chosen-ciphertext attacking. The key of the encryption system can be got by chosen-ciphertext attacking. The digital chaotic encryption system based on digital filter does not have high privacy.

Key words Chaos, Kirchhoff principle, Chosen-ciphertext attack

胡国杰： 男，1974 年生，博士生，主要研究方向为混沌保密通信.

冯正进： 男，1938 年生，教授，博士生导师，现从事机电系统控制工程及混沌动力学的应用研究.