一类混沌流密码的分析 [1]

李树钧 牟轩沁 纪 震* 张基宏*

(西安交通大学电子与信息工程学院 西安 710049)
*(深圳大学信息工程学院 深圳 518060)

摘 要 该文指出一类基于数字化逐段线性混沌映射的混沌流密码方案是不够安全的. 在有限数字精度下, 分段线性混沌映射存在可度量的特征退化, 这种退化由控制参数所在的参数空间子集唯一决定. 由此可以推知, 在已知明文的情况下, 整个密钥空间可以分解为强度依次降低的弱密钥子空间. 在此基础上可以导出一类多分辨率攻击方法, 在密钥随机分配的情况下, 该攻击方法从总体上可以把密钥熵降低 2bit . 试验结果表明, 该文提出的多分辨率攻击方法是实际可行的. 该文还讨论了一些可能采取的改进措施及其效果.

关键词 混沌流密码, PLCM, 密码分析, 弱密钥, 多分辨率

中图号 TN918.1

1 引 言

由于混沌系统特性和保密系统的密码学特性之间存在着紧密的联系, 1989 年以来, 混沌密码学分别在物理学、电子工程和密码学等多个领域同时发展起来 [1−9], 相关的密码分析研究也随之兴起 [9−12] . 混沌为密码算法的设计注入了新的思路, 但是相当数量的混沌密码已经被证实是不够安全的.

1996~1998 年间, 周红等人提出了一类基于逐段线性混沌映射 (PLCM, Piecewise Linear Chaotic Map) 的流密码设计方案 [1−4] . 该方案从结构上可以分为两种: 一种基于均匀分布驱动信号下的非线性多次迭代 [1,2]; 一种是基于混沌迭代序列的分区间非线性处理 [3,4]. 1999 年桑涛等人指出 [5]: 由于 PLCM 的逐段线性性, 可能存在 "潜在的 " 攻击方法, 建议采用一类逐段非线性混沌映射代替 PLCM, 但并未给出可能的攻击方案. 到目前为止, 尚未见到对上述混沌密码的密码分析报道.

本文的分析指出: 由于数字化 PLCM 存在可度量的特征退化, 文献 [1, 2] 提出的流密码方案是不够安全的, 在密钥随机分配的情况下, 密钥空间中存在相当数量的弱密钥, 并且弱密钥的强度不随系统实现精度而改变. 在此基础上, 提出了一类多分辨率攻击方法, 其平均攻击复杂度小于直接穷举攻击; 在密钥随机分配的情况下, 该攻击方法可以将密钥熵降低 2 bit . 虽然平均攻击复杂度提高的并不明显, 但对弱密钥的攻击却相当有效: 密钥越弱, 攻击速度越快, 所需明文数量也越少.

本文的内容安排如下: 第 2 节对文献 [1, 2] 中的加密方案作了简要的介绍. 第 3 节介绍数字化 PLCM 的特征退化. 弱密钥分析与多分辨率攻击方案的性能分析在第 4 节中给出. 第 5 节讨论了一些可能的改进方案及其性能. 第 6 节为实验与仿真部分, 结论在最后一节给出.

2 基于 PLCM 的混沌流密码

文献 [1, 2] 的密码基于一类逐 PLCM $F(x,p)$ (p 为控制参数):

$$F(x,p)=\begin{cases} x/p, & x\in[0,p) \\ (x-p)/(1/2-p), & x\in[p,1/2] \\ F(1-x,p), & x\in[1/2,1] \end{cases}, \qquad 0<p<1/2 \tag{1}$$

[1] 2001-12-17 收到, 2002-07-29 改回

上述混沌映射 (1) 式满足下列特性 [13,14]: (1) 系统是混沌的，输出信号满足遍历性、混合性和确定性; (2) 具有唯一的均匀不变分布 $f^*(x)=1$; (3) 输出轨道的自相关函数 $\tau(n)=\delta(n)$ 。

基于上述特点，文献 [1] 使用 n 级 m 序列 $c(t)$ 生成输入驱动信号 $u_0(t)=\sum_{i=1}^{n}2^{-i}\times c(t+i-1)$ ，该信号经过 k 次混沌迭代输出密钥流 $k(t)=u_k(t)=F^k(u_0(t),p)$; 文献 [2] 针对传统混沌逆系统加密方法的缺陷，提出了基于映射 (1) 式的改进方案，其加密过程可表示为 $y(t)=\lfloor u(t)+F^k(y(t-1),p)\rfloor \bmod 1$ (有限精度 $n$bit 下实现，并要求 $k>n$) 。文献 [2] 的加密方案实际上是一种密文反馈式的流密码方案，由于 $y(t)$ 近似满足均匀分布，可以把它看作文献 [1] 方案的一种变形 (文献 [2] 中的 $y(t-1)$ 即相当于文献 [1] 中的 $u_0(t)$) 。

研究表明 [10,15]，有限精度实现的数字化混沌系统的动力学特性相对连续系统而言存在严重的退化，这可能直接影响以上混沌流加密系统的安全性。为了解决这个问题，文献 [1] 采用了文献 [15] 中的方法对数字化混沌系统进行 m 序列扰动实现; 文献 [2] 没有提及这个问题，但这种数字化特性的退化是必须考虑的，我们假设文献 [2] 的方案也应用了文献 [15] 的扰动策略。本文的后续部分将着重针对文献 [1] 展开。文献 [1, 2] 的流密码结构参见图 1 。

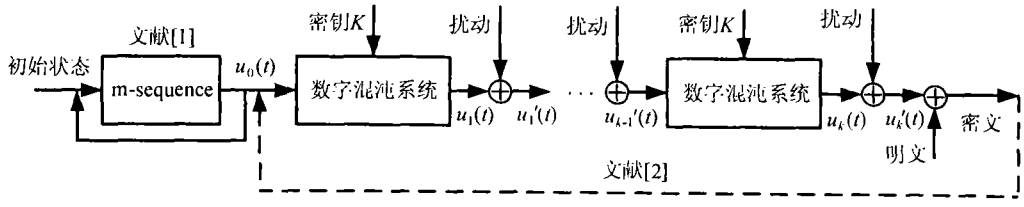


图 1 文献 [1, 2] 流密码结构示意图

根据文献 [10] 可知，数字化 PLCM 存在可度量的统计特征退化，使用文献 [15] 提出的扰动策略，并不能从本质上改变这种退化。本文的分析表明，扰动结构已知时，相应的加密系统对于已知明文攻击是不够安全的，密钥空间中存在相当多的弱密钥。下面我们先来简要介绍一下文献 [10] 中的基本结论。

3 数字化 PLCM 的特征退化

一个混沌映射在连续域具有均匀的不变分布，意味着如下事实: 如果输入信号 $u_0(t)$ 是均匀分布的，则输出信号 $u_1(t)=F(u_0(t),p)$ 也是均匀分布的，这个特性是文献 [1, 2] 密码系统安全性的基础之一。但是当混沌系统在有限计算精度下实现时，上述结论不再成立，系统的动力学特性出现严重的退化。考虑混沌映射 (1) 式在有限精度 $n$bit 下实现，如果输入信号在该精度下满足离散均匀分布，可以严格地证明，一次迭代输出信号在该精度下不满足离散均匀分布; 相对离散均匀分布的偏离有如下表现: 输出信号的最低 i 个比特全为 0 的概率始终大于离散均匀分布下的概率 $1/2^i$ ，当控制参数 p 位于不同的参数子集时，该概率值存在较大的差异。为了便于下文的叙述，下面我们引入一些必要的符号和定义。

定义 1 $S_n=\left\{a\,\middle|\,a=\sum_{i=1}^{n}a_i\cdot 2^{-i},a_i\in\{0,1\}\right\}$ 。S_n 称为分辨率为 n 的数字集合 (digital set) 。$\forall i<j$ ，S_i 称为 S_j 的分辨率为 i 的数字子集 (digital subset) 。特别地，定义 $S_0=\{0\},S_\infty=[0,1)$ 。显然，$\{0\}=S_0\subset S_1\subset\ldots\subset S_i\subset\ldots\subset S_\infty=[0,1)$ 。

定义 2 $V_i=S_i-S_{i-1}(i\geq 1)$ ，$V_0=S_0$ 。$V_i(0\leq i\leq n)$ 称为分辨率为 i 的数字层集 (digital layer) 。显然，$\{V_i\}_{i=0}^{n}$ 构成 S_n 的一个划分，我们称之为 S_n 的完全多分辨率分解，

S_n 的分辨率 n 也称为该数字集合的分解级数。类似地，$\{V_i\}_{i=0}^{\infty}$ 称为 $S_\infty=[0,1)$ 的完全多分辨率分解。$\forall p\in V_i$，i 称为 p 的分辨率，显然，$\forall p\in S_n$，p 的分辨率 i 是唯一的。

定义 3　函数 $G_n: S_\infty\to S_n$ 称为分辨率为 n 的数字近似转换函数 (DATF)，如果 $\forall x\in S_\infty=[0,1)$，$|G_n(x)-x|<1/2^n$。三种最常用的 DATF 如下：(1) $\mathrm{floor}_n(x)=\lfloor x\cdot 2^n\rfloor/2^n$；(2) $\mathrm{ceil}_n(x)=\lceil x\cdot 2^n\rceil/2^n$；(3) $\mathrm{round}_n(x)=\mathrm{round}(x\cdot 2^n)/2^n$。

对于一个定义在区间 $I=S_\infty=[0,1)$ 上的一维混沌映射 $F: I\to I$，实现精度为 $n$bit 的数字化映射可以表示为 $F_n=G_n\circ F: S_n\to S_n$，这里 $G_n(\cdot)$ 是分辨率为 n 的 DATF。任给输入信号 x，定义 $F_n(x,p)$ 的最低 i 个比特均为 0 的概率为 $P_i=P\{F_n(x,p)\in S_{n-i}\}$。对于数字化混沌映射 (1) 式，有如下结论 (参见文献 [10] 的 Theorem 5 和 6 及 Fig.1 和 2)：当控制参数 p 的分辨率不同时，相应的概率值 P_j 也不同，且 P_j 的最大可能值为 $4/2^i$，次大值为 $2/2^i$，二者之间有较大的差异。因此，通过观察 $P_1\sim P_n$，可以得到密钥 p 的分辨率 i。

4 弱密钥分析及多分辨率攻击

对于混沌映射 (1) 式，当流密码实现精度为 n bit 时，密钥空间为 $S'_n=S_n\cap(0,\frac{1}{2})$。定义 $S'_i=S_i\cap(0,\frac{1}{2})$ 及 $V'_i=V_i\cap(0,\frac{1}{2})$，类似节 3 定义 2，可以定义 S'_n 的完全多分辨率分解 $\{V'_i\}_{i=2}^{n}$：$S'_n=\bigcup_{i=2}^{n}V'_i$，$\forall i\neq j, V'_i\cup V'_j=\emptyset$，其分解级数为 $n-1$。

对 S'_n 进行完全多分辨率分解，得到 $S'_n=\bigcup_{i=2}^{n}V'_i$，根据文献 [10] 的 Theorem 6，当密钥 p 属于不同的 V'_i 时，概率值 $P_1\sim P_n$ 是不同的。因此，得到概率值 $P_1\sim P_n$，也就可以得到 p 的分辨率 i，从而可以仅在子密钥空间 $V'_i\subset S'_n$ 内部搜索密钥，降低密钥攻击的整体复杂度。由于 i 越低，子空间 V'_i 就越小，攻击所需的时间也就越短，则相应的密钥 p 就越弱，弱密钥的强度随分辨率的减小按指数速率降低。

怎样才能得到概率值 $P_1\sim P_n$ 呢？文献 [1] 中流密码的设计使得对上述概率值的观察成为可能。令数字化混沌系统中间第 j 轮迭代的直接输出为 $u_j(t)$，扰动后的第 j 轮输出为 $u'_j(t)$，混沌流密码的输出密钥流 $k(t)=u'_k(t)$(参看图 1)。在已知明文攻击条件下，$k(t)$ 已知，由于扰动结构也是已知的，可以去除扰动得到第 k 轮混沌输出 $u_k(t)=F(u'_{k-1}(t),p)$。由于扰动使得 $u'_{k-1}(t)$ 近似满足 S_n 上的离散均匀分布，则概率值 $P_i(1\le i\le n)$ 可以由 $u_k(t)$ 的统计结果估算。当已知明文的数量逐渐增加时，相应的概率 P_i 逐渐趋向于文献 [10] 的 Theorem 5 和 6 中的理论值，由于 P_i 的最大可能取值和次大可能取值之间存在足够大的差异 $(4/2^i-2/2^i=2/2^i)$，p 的分辨率 i 会逐渐显露。

一般来说，确定密钥分辨率的方法如下：同时观察 n 个不同的概率值 $P_j(1\le j\le n)$，如果概率值 P_i 趋向于最大可能取值，而 P_{i-1} 趋向于次大可能取值，则密钥的分辨率为 i，观察所需的明文数量为 2^i 量级。从所需明文的数量上来看，密钥 p 的分辨率 i 越小，则通过概率值 $P_j(1\le j\le n)$ 确定 i 的速度也越快，从而该密钥也越弱。可以看到，当实现精度为 $n$bit 时，整个密钥空间可以分为 $n-1$ 个强度依次递增的子密钥空间 $V'_2\sim V'_n$；提高系统的实现精度到 $n'>n$，将引入 $n'-n$ 个新的子密钥空间 $V'_{n+1}\sim V'_{n'}$，但原精度 n 下的所有弱密钥的强度并不会因为实现精度的提高而改善。

显然，上述分析弱密钥的过程可以看成是一类多分辨率攻击。假设密钥在整个密钥空间 S'_n 内部等概随机分配，我们来分析一下多分辨率攻击的总体性能。

(1) 所需观察明文的平均量级： $N_p = \sum_{i=2}^{n} \frac{2^{i-2}}{2^{n-1}-1} \cdot 2^{i-2} = \frac{2^{2n-1}-1}{3 \cdot (2^{n-1}-1)}$，当 $n \geq 8$，$N_p \approx \frac{2^{n-1}}{3}$；

(2) 搜索子密钥的平均复杂度： $N_k = \sum_{i=2}^{n} \frac{2^{i-2}}{2^{n-1}-1} \cdot 2^{i-3} = \frac{2^{2n-2}-1}{6 \cdot (2^{n-1}-1)}$，当 $n \geq 8$，$N_k \approx \frac{2^{n-2}}{3}$；

(3) 多分辨率攻击下的密钥熵： $H(K) = \sum_{i=2}^{n} \frac{2^{i-2}}{2^{n-1}-1} \cdot (i-2) = \frac{(n-3) \cdot 2^{n-1}+2}{2^{n-1}-1}$，当 $n \geq 8$，$H(K) \approx n-3$，比穷举攻击下的密钥熵 $H(K) = \log_2(\#(S'_n)) \approx n-1$ 减小了 2bit。

观察上述结果，可以看到所需观察明文的数量的平均值较大，总体密钥熵的降低也不是特别的明显；考虑到分辨率较低的弱密钥的存在 (按照最严格的观点，只有分辨率为 n 的密钥才是不弱的，而这样的密钥仅占总数的一半)，多分辨率攻击仍然是较为有效的。

5 可能的改进措施

为了避免弱密钥问题和多分辨率攻击，本节讨论一些可能的改进措施及其优缺点。

(1) 提高系统的数字化有限精度　增大混沌流密码的实现精度 n，可能是提高系统安全性的一个最为简单而方便的方法。上节的分析表明，使用该措施可以从总体上改善混沌流密码抗多分辨率攻击的能力；由上节的分析我们已经知道，把实现精度从 n 提高到 n'，原实现精度下的所有密钥的强度并不会得到提高。因此，我们认为提高实现精度不是一个根本的改进措施。

(2) 掩盖数字化混沌系统的扰动结构　如前所述，只有在扰动结构已知的情况下，我们才能由扰动后的输出流密钥 $k(t) = u'_k(t)$ 得到未经扰动的最后一轮混沌迭代输出 $u_k(t)$，从而估计概率值 $P_i(1 \leq i \leq n)$ 并得到密钥的分辨率 i。如果掩盖算法中的扰动结构，则可能提高系统的安全性。但是根据 Kerckhoffs 原则，密码系统的安全性不应依赖于算法结构的保密性；因此我们必须将扰动 m 序列的特征多项式、初始状态以及扰动位数作为密钥的一部分。但是，攻击者只要设法得到 m 序列部分的子密钥，仍然可以使用多分辨率攻击对混沌子密钥 p 进行攻击，因此，这也不是一个根本的解决方法。

(3) 避免使用弱密钥　另一个较为简单而朴素的想法是避免使用任何弱的密钥。从最为苛刻的要求出发，只有分辨率为 n 的密钥是不弱的。这样就要求有效密钥仅在 V'_n 内随机选取，则系统的密钥熵从近似等于 $n-1$ 降低到 $n-2$。也可以采用一种折衷的方案：即仅仅避免使用那部分“很弱”的密钥 (如避免使用所有分辨率小于 $n/2$ 的密钥)，以保证系统具有一个抗多分辨率攻击的下限。这个方法的缺点是牺牲了一定数量的可用密钥。

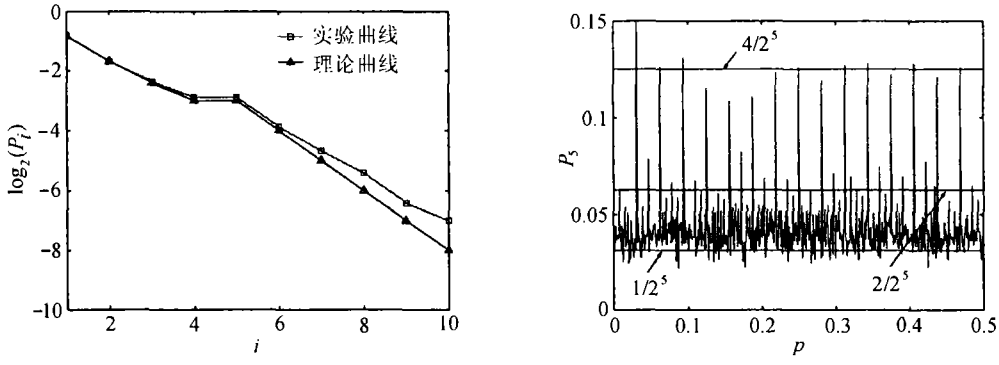
(4) 使用更复杂的混沌映射　本文的多分辨率攻击基于数字化 PLCM 的可度量特征退化，因此改用其他更为复杂的混沌映射也许是一个根本的解决方案。一个可用的替代映射是文献 [5] 中提出的逐段非线性混沌映射。但是逐段非线性混沌映射计算较繁，不得不采用浮点运算，这将严重影响混沌密码系统的加密速度，并提高系统的实现成本，从而影响混沌流密码的易用性和广泛适用性。另外，对于一般的混沌映射而言 (如文献 [5] 中提出的非线性混沌映射)，是否也存在类似的可度量的退化特征，还缺乏深入细致的研究。

6 实验与仿真

针对文献 [1] 中的加密方案，我们对本文提出的多分辨率分析法进行了实验分析，实验结果和前面的理论分析完全是一致的。相关的实验参数为有限精度 $n = 10$，DATF 为 $\mathrm{floor}_n(\cdot)$，混

沌迭代次数 $k=n+1$，产生驱动信号和扰动信号的 m 序列特征多项式分别为 $1+x^3+x^{10}$、$1+x^2+x^3+x^8+x^{10}$，m 序列的初始状态均为 1，扰动方式为按位“异或”，扰动位数 $n_m=5$。

由于 $u'_{k-1}(t)$ 近似满足 S_n 上的均匀离散分布，按照文献 [10] 的 Theorem 5 和 6，根据 $u_k(t)$ 得到的概率估计值应该逐渐收敛到理论值上去，当然由于均匀分布的近似性，二者之间可能有一定的偏离。实验表明，这种偏离是比较小的，不会影响对密钥分辨率的确定。图 2 给出了通过 $u_k(t)$ 得到的概率估计值与理论值的比较。图 2(a)、2(b) 可以分别与文献 [10] 的 Fig.1(a) 和 Fig.2 相对照。可以看到，实验结果基本符合文献 [10] 的 Theorem 5 和 6 的理论结果。图 2(b) 显示，在 P_5 的最大值和次大值之间，确实存在足够的区分度，P_5 虽然有一定的波动，但是并不影响判断 (这是近似离散均匀分布的直接表现，因此在判断时需要引入模糊阈值)。



(a) $p=3/2^5$ 时 $P_1\sim P_n$ 的估计值　　(b) 不同密钥参数下的 P_5 估计值

图 2　通过 $u_k(t)$ 得到的概率估计值与理论值的比较

最后，取密钥 $p=3/2^5\in V'_5$，我们进行了实际攻击测试。$p'=5/2^4\in V'_4$ 与 $p''=7/2^6\in V'_6$ 选为对比参数。观察 P_4 与 P_5 的概率估计值 P[4]、P[5] 随观察明文数量增加的变化，可以看到，经过一个短时间的过渡阶段之后，P[4]、P[5] 逐渐稳定到理论值 $2/2^5$、$4/2^5$ 上下做小的波动。攻击成功所需的明文数量 (即 P[5] 与 P[4] 逐渐稳定进入阈值范围的明文数量) 为 $O(2^5)$。

7 结　论

本文指出文献 [1, 2] 中提出的混沌加密方案是不够安全的。由于它采用的分段线性混沌映射在有限精度实现时存在可度量的特征退化，造成相应的加密方案存在大量的弱密钥；一种多分辨率攻击可用于对该混沌流密码进行攻击，整体密钥熵可以降低 2bit。为了避免这种攻击，原混沌加密方案必须采取一定的改进措施。本文的意义在于：使用混沌系统构造保密系统，仅在连续域证明其优良特性是不够的，还必须充分考虑数字化环境下混沌系统的特性退化对系统安全性的影响。使用混沌系统设计一个真正安全的密码体系，还需要在混沌系统特性研究方面做更多深入的工作。

参　考　文　献

[1] 周红，俞军，凌燮亭，混沌前馈型流密码的设计，电子学报，1998, 26(1), 98–101.

[2] Hong Zhou, Xie-Ting Ling, Problems with the chaotic inverse systems encryption approach, IEEE Trans. on Circuits and Systems-I, 1997, 44(3), 268–271.

[3] 周红，罗杰，凌燮亭，混沌非线性反馈密码序列的理论设计和有限精度实现，电子学报，1997, 25(10), 57–60.

[4] Zhou Hong, Ling Xieting, Generating chaotic secure sequences with desired statistical properties and high security, Int. J. Bifurcation Chaos, 1997, 7(1), 205–213.

[5] 桑涛，王汝笠，严义埙，一类新型混沌反馈密码序列的理论设计，电子学报，1999, 27(7), 47–50.

[6] T. Habutsu, Y. Nishio, I. Sasase, S. Mori, A secret key cryptosystem by iterating a chaotic map, Advances in Cryptology-EuroCrypt'91, Brighton, UK: 1991, Spinger-Verlag, 1991, Lecture Notes in Computer Science vol. 0547, 127–140.

[7] G. Alvarez, F. Monotoya, G. Pastor, M. Romera, Chaotic cryptosystems, in Proc. 33nd Annual 1999 Int. Carnahan Conf. Security Technology, Madrid, Spain 1999, IEEE, 1999, 332–338.

[8] E. Alvarez, A. Fernández, P. García, J. Jiménez, A. Marcano, New approach to chaotic encryption, Physics Letters A, 1999, 263(4-6), 373–375.

[9] Shujun Li, Xuanqin Mou, Yuanlong Cai, Improving security of a chaotic encryption approach, Physics Letters A, 2001, 290(3/4), 127–133.

[10] Shujun Li, Qi Li, Wenmin Li, Xuanqin Mou, Yuanlong Cai, Statistical properties of digital piecewise linear chaotic maps and their roles in cryptography and pseudo-random coding, Cryptography and Coding—8th IMA Int. Conf., Cirencester, UK: 2001, Springer-Verlag, Lecture Notes in Computer Science vol. 2260, 205–221.

[11] Maciej J. Ogorzatek, Hervé Dedieu, Some tools for attacking secure communication systems employing chaotic carriers, Proc. Int. Symp. Circuits and Systems, Monterey, USA: 1998, IEEE, 1998, vol.4, 522–525.

[12] Eli Biham, Cryptoanalysis of the chaotic-map cryptosystem suggested at EuroCrypt'91, Advances in Cryptology-EuroCrypt'91, Brighton, UK: 1991, Spinger-Verlag, 1991, Lecture Notes in Computer Science vol.0547, 532–534.

[13] Andrzej Lasota, Michael C. Mackey, Chaos, Fractals, and Noise-Stochastic Aspects of Dynamics, Second edition, New York: Springer-Verlag, 1997, Chapter 5–6.

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

[15] 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.

CRYPTANALYSIS OF A CLASS OF CHAOTIC STREAM CIPHERS

Li Shujun Mou Xuanqin Ji Zhen* Zhang Jihong*

(*School of Electron. and Info. Eng., Xi'an Jiaotong University, Xi'an* 710049, *China*)

*(*Faculty of Information Engineering, Shenzhen University, Shenzhen* 518060, *China*)

Abstract This paper points out that a class of chaotic stream ciphers proposed recently is not secure enough, which is based on digital Piecewise Linear Chaotic Maps (PLCM). It has been known that digital PLCMs' statistical properties have essential degradation when PLCMs are realized in finite computing precision, and that such degradation is determined by the resolution of the control parameter (i.e., determined by which digital subset the control parameter is in). Hence, for the studied chaotic stream ciphers, the whole key space can be divided into $n-1$ subspaces with incremental weakness degree, and the weakness of any fixed key cannot be improved by using higher precision. Based on the above fact, a kind of multi-resolution cryptanalysis is presented to attack the chaotic ciphers. When secure key is selected randomly, the key entropy will decrease by 2bit as a whole. Experiments show that this cryptanalysis is feasible and efficient.

Key words Chaotic stream cipher, PLCM, Cryptanalysis, Weak key, Multi-resolution

李树钧： 男，1975 年生，博士生，目前研究方向为混沌加密、图像 / 视频加密等.

牟轩沁： 男，1964 年生，副教授，目前研究方向为医学图像处理、三维重建等.

纪 震： 男，1973 年生，副教授，目前研究方向为医学图像处理、数字水印等.

张基宏： 男，1964 年生，教授，目前研究方向为图像编码、矢量量化等.