# 对混沌序列密码的相关密钥攻击

金晨辉 杨 阳 祁传达
(解放军信息工程大学电子技术学院 郑州 450004)

**摘 要** 该文首次提出了对混沌序列密码的相关密钥攻击方法。该方法将线性密码分析的思想与对混沌密码的分割攻击方法相结合，利用多个相关密钥产生的乱数序列对混沌密码实施分割攻击，从而大大提高了分割攻击方法的效率，克服了当混沌密码吻合度分布泄漏的信息较小或密钥规模较大时，分割攻击方法难以将攻击方案的计算复杂性降低在可实现范围内的局限。作为例子，该文实现了对具有64bit密钥的ZLL混沌密码的相关密钥攻击，在主频为2.5GHz的Pentium 4-PC机上，整个攻击时间平均为154s，成功率为0.96。

**关键词** 混沌密码，相关密钥攻击，ZLL混沌密码算法，分割攻击，已知明文攻击
**中图分类号**：TN918.1 **文献标识码**：A **文章编号**：1009-5896(2006)03-0410-05

# A Related-Key Attack on Chaotic Stream Ciphers

Jin Chen-hui Yang Yang Qi Chuan-da
(*Electronic Technology Institute, PLA Information Engineering University, Zhengzhou* 450004, *China*)

**Abstract** In this paper the authors first present a related-key attack on chaotic stream ciphers. Combining the idea of linear cryptanalysis and divide-and-conquer attack on chaotic ciphers, the attack uses the output sequences created by multiple related keys, hence enhances the efficiency of divide-and-conquer attacks. The related-key attack breaks the confinements that it is difficult to reduce the computing complexity of divide-and-conquer attacks to a realizable range when the information amount leaked by the distribution of coincidence degree of a chaotic cipher is small or the size of key is large. As an example, the related-key attack on the ZLL chaotic cipher with 64 bits key on a Pentium 4/2.5GHz personal computer was realized and it took about 154s to recover key at a success rate 0.96.

**Key words** Chaotic cipher, Related-key attack, ZLL chaotic cipher algorithm, Divide-and-conquer attack, Known plain texts attack

## 1 引言

混沌密码是一类新型的密码算法，在数据加密、图像加密和信息隐藏等领域都有应用，因此，研究混沌密码的安全性及安全性分析方法具有重要的意义。文献[1]提出了对混沌密码的多分辨率攻击方法，该方法平均将文献[2]提出的混沌密码的密钥熵降低2bit，但所需的已知明文量和攻击方案的计算复杂性都很大。文献[3]和文献[4]发现了混沌序列初态的低位比特对前若干输出信号的影响不大这个信息泄漏，并利用吻合度[4]的分布规律给出了对该信息泄漏进行定量刻化的一种方法，进而提出了对混沌密码的分割攻击方法，从而利用不长的乱数序列大大降低了对混沌密码攻击的计算复杂性。但是，该攻击方法在应用中具有两个局限性：其一是当混沌密码的吻合度分布泄漏的信息较小时，攻击方法降低的密钥熵不是很大；其二是当密钥规模较大时，尽管该攻击方法可大大降低密钥熵，但仍然难以将攻击方案的计算复杂性降低在可实现的范围之内。如文献[4]的分割攻击方法的平均计算复杂度为$2^{45}$，在单台PC机上至少需要几个月时间才能运行完毕。

为解决这两个局限性，本文将线性密码分析[5]的思想与对混沌密码的分割攻击方法[3,4]相结合，提出了对混沌密码的相关密钥攻击方法。该方法综合利用多个相关密钥产生的乱数序列提供的信息对混沌密码进行攻击，从而大大提高了分割攻击的效率，克服了分割攻击方法的上述局限性。作为例子，本文实现了对具有64bit密钥的ZLL混沌密码[6]的相关密钥攻击，成功率可达到0.96以上，而且在主频为2.5GHz的Pentium 4 PC机上，整个攻击时间平均仅有154s。

## 2 ZLL混沌密码算法及其信息泄漏规律

### 2.1 ZLL混沌密码算法

文献[6]提出的"ZLL序列密码算法"包含两个密码变换，其中一个是混沌映射，另一个是量化函数。

设$p$是自然数，实数$a_0,a_1,\cdots,a_{p+1}$满足$0=a_0<a_1<a_2<\cdots<a_p<a_{p+1}=1$，则ZLL序列密码算法中的混沌映射$f:[-1,1)\to[-1,1)$定义为

$$f(x)=\begin{cases}-1+2(x-a_j)/(a_{j+1}-a_j), & x\in[a_j,a_{j+1}),\ j=0,1,\cdots,p\\ f(-x), & x<0\end{cases}$$

再设$n$是自然数，$I_0,I_1,\cdots,I_{2^n-1}$是$[-1,1)$的$2^n$个连续的左闭右开的等分区间，即$I_i=\left[\frac{i}{2^{n-1}}-1,\frac{i+1}{2^{n-1}}-1\right)$，则ZLL序

2005-01-26收到，2005-08-04改回
河南省杰出青年科学基金(0312001800)资助课题

列密码算法的量化函数 $T:[-1,1)\to\{0,1\}$ 定义为

$$T(x)=\begin{cases}0, & x\in\bigcup_{k=0}^{2^{n-1}-1}I_{2k}\\ 1, & x\in\bigcup_{k=0}^{2^{n-1}-1}I_{2k+1}\end{cases}$$

由文献[4]知 $T(x)=\mathrm{Int}(2^{n-1}x)\bmod 2$，即量化函数 $T$ 将输入的小数点后的第 $n-1$ 比特作为输出值。

设 $x=\sum_{i=1}^{\infty}x_i/2^i$ 是一个非负小数且 $x_i\in\{0,1\}$，则称 $\sum_{i=1}^{m}x_i/2^i$ 是 $x$ 的 $m$ 精度小数。以下总将 $m$ 维二元向量 $(x_1,x_2,\cdots,x_m)$ 与小数 $\sum_{i=1}^{m}x_i/2^i$ 之间相互转换，且称 $(x_1,x_2,\cdots,x_n)$ 为 $x=\sum_{i=1}^{\infty}x_i/2^i$ 的高 $n$ 位比特。

在选定密码算法的参数 $p,n$ 和 $a_0,a_1,\cdots,a_{p+1}$ 之后，就可构造出 ZLL 序列密码算法：

设 $k=(k_1,k_2,\cdots,k_m)$ 是 ZLL 密码算法的密钥，它对应的 $m$ 精度小数记为 $x_0$，则可按递归关系

$$x_i=f(x_{i-1}),\qquad i\ge 1$$

得到一个混沌序列 $\{x_i\}_{i=1}^{\infty}$。ZLL 密码算法根据 $s_i=T(x_i)$ 产生一条二元序列 $\{s_i\}_{i=1}^{\infty}$，称这条序列为乱数序列。将该二元序列与明文序列 $\{m_i\}_{i=1}^{\infty}$ 逐位模 2 加，即得到密文序列。显然当已知明密文对时，即可获得对应的乱数，因此对 ZLL 算法的已知明文攻击就是对该算法的已知乱数攻击。

ZLL 算法也可将参数 $p,n$ 和 $a_0,a_1,\cdots,a_{p+1}$ 都设置为密钥，但为简单起见，本文以下均假设它们都是已知的参数。

### 2.2 ZLL 混沌密码算法的信息泄漏规律

**定义 1**[4]　设 $k$ 和 $k'$ 分别是某序列密码算法的正确密钥和试验密钥，$\{s_i\}_{i=1}^{\infty}$ 和 $\{s'_i\}_{i=1}^{\infty}$ 分别是它们产生的乱数序列，则称 $\max\{n:\forall 1\le i\le n,\text{有}s'_i=s_i\}$ 为 $k'$ 的吻合度。

对于设计较好的序列密码算法，试验密钥 $k'$ 产生的乱数序列应当平衡且与正确密钥产生的乱数序列相互独立，故其吻合度 $\xi$ 应服从几何分布，即 $p(\xi=t)=2^{-t-1},t\ge 0$，因而 $p(\xi\ge t)=2^{-t}$ 且其期望值等于 1。但由于混沌映射多是连续函数或间断连续函数，故其初态低位比特的微小变化将导致前几个状态不大的变化，因而通常对输出乱数的前几个信号影响较小。现用 $k^{(m)}$ 表示将正确密钥 $k$ 的高 $m$ 比特保持不变，其它比特全部置 0 所得的试验密钥，且记 $k^{(m)}$ 的吻合度为 $n_m$，则混沌密码的上述信息泄漏表现为 $k^{(m)}$ 的吻合度偏大，因而与几何分布有很大的差异。当 $p(n_m\ge t)$ 显著大于 $2^{-t}$ 时，就可将 $k^{(m)}$ 与除高 $m$ 比特外全为 0 的其它试验密钥区分开来。

文献[4]用模拟分析方法给出了密钥为 64bit，参数 $n=6,p=2$ 的 ZLL 算法的吻合度分布的统计规律。当参数 $a_1=$ 0xa5df 0369 5dfd 47d1 和 $a_2=$ 0xcde6 dfef 0063 ff00 时，1 万例实验表明 $n_{16}$ 的分布规律如表 1 所示。

一般地，有 $p(n_{16}\ge 5)=0.7309$，$p(n_{32}\ge 14)=0.5928$，$p(n_{48}\ge 22)=0.6623$。据此就可对混沌密码采取先攻击 $k^{(16)}$，再依次攻击 $k^{(32)},k^{(48)},k^{(64)}$ 的方法进行分割攻击[3,4]。例如，可先对 $k^{(16)}$ 的各种可能值进行穷举，并将吻合度 $\ge 5$ 者作为 $k^{(16)}$ 的候选值；然后再将 $k^{(16)}$ 的候选值作为 $k^{(32)}$ 的高 16 位对 $k^{(32)}$ 的每种可能值穷举，并将吻合度 $\ge 14$ 者作为 $k^{(32)}$ 的候选值。类似地对 $k^{(48)},k^{(64)}$ 进行攻击。分割攻击方法的依据是：

**引理 1**[4]　设 $k$ 是序列密码算法的密钥，则在除高 $m$ 比特外全为 0 的所有试验密钥中，吻合度 $\ge t$ 的试验密钥个数的期望为 $2^{m-t}$，且吻合度 $\ge t$ 的试验密钥中包含 $k^{(m)}$ 的概率为 $p(n_m\ge t)$。

引理 1 说明可将吻合度 $\ge t$ 的除高 $m$ 比特外全为 0 的试验密钥都作为 $k^{(m)}$ 的候选密钥[3-4]。为确保整个攻击方案的成功率，应保证 $k^{(m)}$ 的候选密钥中包含正确密钥的概率 $p(n_m\ge t)$ 足够大。但是，该方法有一定的局限性。其一，由于此时错误密钥的吻合度 $\ge t$ 的概率都在 $2^{-t}$ 附近，因而 $k^{(m)}$ 的候选密钥的个数约为 $2^{m-t}$；故当 $k^{(m)}$ 的吻合度的信息泄漏量不足以找到足够大的 $t$ 使得 $p(n_m\ge t)$ 大于预定值时，由于 $k^{(m)}$ 的候选密钥的个数 $2^{m-t}$ 较大，因而上述分割攻击方法就很难将整个攻击方案的计算复杂性降低在可实现的范围内。其二，若将使 $p(n_m\ge t)$ 大于预定值的 $t$ 看作 $m$ 的函数 $t(m)$，则候选密钥个数 $2^{m-t(m)}$ 一般将随着 $m$ 的增长而急剧增长。因此，随着密钥规模的增加，尽管该攻击方法可将密钥熵大幅度降低，但很难将攻击方案的计算复杂性减少在可实现的范围内。例如文献[4]中对 ZLL 混沌密码算法攻击的平均计算复杂度为 $2^{45}$，故尽管该攻击在大型计算机上可以很快完成，但在单台 PC 机上至少需要几个月的时间才能完成。

## 3　对 ZLL 序列密码算法的相关密钥攻击

为克服上述两个局限性，下面将线性密码分析的思想与对混沌密码的分割攻击方法相结合，提出对混沌密码的相关密钥攻击方法，从而同时利用多个相关密钥产生的乱数序列提供的信息对混沌密码进行攻击，大大提高分割攻击的效率。

设 $\alpha_1,\alpha_2,\cdots,\alpha_N$ 已知，且以诸 $k\oplus\alpha_i$ 为密钥产生的乱数序列 $\{d_{ij}\}_{j=1}^{\infty}$ 也已知。显然 $k\oplus\alpha_1,k\oplus\alpha_2,\cdots,k\oplus\alpha_N$ 是 $N$ 个相关密钥。因此在此条件下求解密钥 $k$ 即为对 ZLL 算法的相关密钥攻击。

上述相关密钥攻击的条件在某些情况下是现实可得的。例如，如果通信双方采取下述会话密钥协议，就自动提供了相关密钥攻击的条件：设用户 $A$ 和用户 $B$ 共享的密钥为 $k$，加密算法为 $E_k(m)$。当 $A$ 向 $B$ 传送消息 $m$ 时，$A$ 随机选取一个与 $k$ 等长的随机数 $\alpha$，并将密文 $E_{k\oplus\alpha}(m)$ 和 $\alpha$ 一起明传给 $B$。

表 1　$n_{16}$ 的分布规律

| $n_{16}$ | ≤2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | ≥13 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 个数 | 294 | 665 | 1732 | 2609 | 2116 | 1214 | 672 | 311 | 147 | 85 | 33 | 17 |

### 3.1 对混沌密码算法的相关密钥攻击的基本原理

**引理2** 设 $k=\sum_{i=1}^{\infty}k_i2^{-i},k_i\in\{0,1\}$ 和 $a=\sum_{i=1}^{\infty}a_i2^{-i},a_i\in\{0,1\}$ 分别是 $k$ 和 $a$ 的二进制表示，则有 $(k\oplus a)^{(m)}=k^{(m)}\oplus a^{(m)}$。

对混沌密码的相关密钥攻击基本原理为：设 $p(n_m\geq d)=p$，则以 $(k\oplus\alpha_i)^{(m)}$ 为密钥产生的前 $d$ 个乱数与以 $k\oplus\alpha_i$ 为密钥产生的前 $d$ 个乱数相等的概率为 $p$。由于诸 $\alpha_i$ 已知，故对 $k^{(m)}$ 的每个假设 $k'$，都可求出相应的 $(k'\oplus\alpha_i)^m=k'\oplus\alpha_i^{(m)}$，从而生成以 $(k'\oplus\alpha_i)^m$ 为密钥的乱数序列。由引理2易证 $(k'\oplus\alpha_i)^m=(k\oplus\alpha_i)^m$ 等价于 $k'=k^{(m)}$，故当 $k'=k^{(m)}$ 时，$(k'\oplus\alpha_i)^m$ 的吻合度大于等于 $d$ 的概率是 $p(n_m\geq d)=p$；当 $k'\neq k^{(m)}$ 时，因 $(k'\oplus\alpha_i)^m\neq(k\oplus\alpha_i)^m$，因而 $(k'\oplus\alpha_i)^m$ 的吻合度大于等于 $d$ 的概率都很小，据此就可同时利用 $(k'\oplus\alpha_1)^m,\cdots,(k'\oplus\alpha_N)^m$ 产生的 $N$ 条乱数序列对 $k'$ 进行筛选，并利用下述算法求出正确的 $k^{(m)}$。

**算法1** 对 $k^{(m)}$ 的每个可能值 $k'$，$\forall i:1\leq i\leq N$，检验以 $k'\oplus\alpha_i^{(m)}$ 为密钥产生的前 $d$ 个乱数是否与以 $k\oplus\alpha_i$ 为密钥产生的前 $d$ 个已知乱数全部一致。全部一致时令 $\xi_i(k')=1$，否则令 $\xi_i(k')=0$.记 $T_{k'}=\sum_{i=1}^{N}\xi_i(k')$，将使 $T_{k'}$ 达到最大的那个 $k'$ 判断为正确的 $k^{(m)}$。

**引理3** 设算法1中试验密钥为 $k'$，使 $p_{k'}=p(\xi_i(k')=1)$，$p_{k^{(m)}}=p(\xi_i(k^{(m)})=1)$。又设 $\xi_i(k')$ 相互独立，则算法1的输出是 $k^{(m)}$ 的概率为

$$\sum_{i=1}^{N}\left[C_N^ip_{k^{(m)}}^i\left(1-p_{k^{(m)}}\right)^{N-i}\prod_{k'\in\{0,1\}^m\setminus k^{(m)}}\sum_{j=0}^{i-1}C_N^jp_{k'}^j(1-p_{k'})^{N-j}\right]$$

**证明** $T_{k'}=i$ 等价于在 $\xi_1(k'),\cdots,\xi_N(k')$ 中，有 $i$ 个为1，$N-i$ 个为0，故有

$$p(T_{k'}=i)=C_N^ip_{k'}^i(1-p_{k'})^{N-i}$$

又因算法1求出的 $k'$ 是 $k^{(m)}$ 等价于 $T_{k^{(m)}}>\max_{k':k'\neq k^{(m)}}T_{k'}$，且诸 $T_{k'}$ 相互独立，故由算法1求出的 $k'$ 是 $k^{(m)}$ 的概率为

$$\begin{aligned}&p\left(T_{k^{(m)}}>\max_{k'\in\{0,1\}^m\setminus k^{(m)}}Tk'\right)\\&=\sum_{i=0}^{N}p\left(T_{k^{(m)}}=i\text{且}\forall k'\in\{0,1\}^m\setminus k^{(m)},\text{有}T_{k'}<i\right)\\&=\sum_{i=0}^{N}\left[p\left(T_{k^{(m)}}=i\right)\prod_{k'\in\{0,1\}^m\setminus k^{(m)}}p(T_{k'}<i)\right]\\&=\sum_{i=1}^{N}\left[C_N^ip_{k^{(m)}}^i(1-p_{k^{(m)}})^{N-i}\prod_{k'\in\{0,1\}^m\setminus k^{(m)}}\sum_{j=0}^{i-1}C_N^jp_{k'}^j(1-p_{k'})^{N-j}\right]\end{aligned}$$

由引理3可知算法1中 $d$ 的选择对算法的性能影响巨大。当 $d$ 的选择不当时，算法1的成功率将急剧下降。所以 $d$ 的选取应在保证成功率的条件下尽可能地小，以降低算法的平均计算复杂性。通过大量的试验我们发现，当选取的 $d$ 等于其期望值时，算法的成功率最大。

### 3.2 对ZLL算法的相关密钥攻击

下面给出对具有64bit密钥的ZLL算法的相关密钥攻击算法。攻击的思路是采取算法1依次求出 $k^{(16)}$，$k^{(32)},k^{(48)},k^{(64)}$。具体算法如下：

**算法2**

步骤1 取 $N=80$，$d_{16}=5$，$d_{32}=14$，$d_{48}=22$，$d_{64}=28$ 及 $m_i=16i$，$1\leq i\leq4$，$m_0=0$。初始化 $i=1$。

步骤2 将 $k^{(m_i)}$ 的最高 $m_{i-1}$ 比特块设置为 $k^{(m_{i-1})}$，并穷举 $k^{(m_i)}$ 的低 $m_i-m_{i-1}$ 比特块的每个可能值，设 $k'$ 是如此得到的 $k^{(m_i)}$ 的一个试验密钥，当 $1\leq i\leq3$ 时，$\forall j:1\leq j\leq N$，检验以 $k'\oplus\alpha_j^{(m_i)}$ 为密钥产生的前 $d_{m_i}$ 个乱数是否与以 $k\oplus\alpha_j$ 为密钥产生的前 $d_{m_i}$ 个已知乱数全部一致。全部一致时令 $\xi_j(k')=1$，否则令 $\xi_j(k')=0$。记 $T_{k'}=\sum_{j=1}^{N}\xi_j(k')$，将使 $T_{k'}$ 达到最大的 $k'$ 判断为正确的 $k^{(m_i)}$，并将 $i$ 增1后返回步骤2。当 $i=4$ 时，若 $\forall j:1\leq j\leq N$，以 $k'\oplus\alpha_j^{(m_4)}$ 为密钥产生的前 $d_{m_4}$ 个乱数与以 $k\oplus\alpha_j$ 为密钥产生的前 $d_{m_4}$ 个已知乱数全部一致，则输出 $k^{(m_4)}$，算法终止。否则，当所有可能的 $k^{(m_4)}$ 都检验完毕时，报告算法2失败，否则返回步骤2检验下个可能的 $k^{(m_4)}$。

**定理1** 算法2的平均计算复杂性为计算混沌映射 $1.60\times2^{26}$ 次。

**证明** 算法2的平均计算复杂性是攻击 $k^{(16)}$，$k^{(32)},k^{(48)},k^{(64)}$ 的平均计算复杂性之和。现将计算复杂性考虑为计算混沌映射的次数，则当 $1\leq i\leq3$ 时，攻击 $k^{(16i)}$ 时的平均计算复杂性均近似为 $d_{16i}\times N\times2^{16}/2$，因而攻击 $k^{(16)},k^{(32)},k^{(48)}$ 的平均复杂性分别为 $1.56\times2^{23}$，$1.09\times2^{25}$，$1.72\times2^{25}$。而在攻击 $k^{(64)}$ 时，假定 $k^{(64)}$ 的试验密钥的吻合度大于等于 $d_{48}$，所以当某一试验密钥产生的第 $j$ 条乱数序列的第 $i$ 比特与正确密钥产生的对应比特位不等时，将此试验密钥判断为错误密钥的概率为 $2^{-(j-1)(d_{32}-d_{24})-i}$，则攻击 $k^{(64)}$ 的平均计算复杂度等于

$$\sum_{j=1}^{80}\sum_{i=1}^{d_{64}-d_{48}}[(j-1)d_{64}+d_{48}+i]\times2^{16}\times2^{-(j-1)(d_{64}-d_{48})-i}=1.22\times2^{17}$$

因而算法2的平均计算复杂性为计算混沌映射 $1.60\times2^{26}$ 次。

**定理2** 设 $k=(k_{16},k_{32},k_{48},k_{64})$ 是ZLL算法的正确密钥，$k'=(k'_{16},k'_{32},k'_{48},k'_{64})$ 是算法2的输出，其中 $k_{16i}$ 和 $k'_{16i}$ 都是16bit块。则有

$$\begin{aligned}p(k=k')=&p(k'_{16}=k_{16})\\&\times p(k'_{32}=k_{32}\mid k'_{16}=k_{16})\\&\times p(k'_{48}=k_{48}\mid(k'_{16},k'_{32})=(k_{16},k_{32}))\\&\times p(k'_{64}=k_{64}\mid(k'_{16},k'_{32},k'_{48})=(k_{16},k_{32},k_{48}))\end{aligned}$$

根据定理2和引理2即可求出算法2的成功率。显然，随着试验密钥 $k'$ 与正确密钥全部一致的高位比特数的增加，

$k'$ 与正确密钥的吻合度也将增加。只要对诸 $m$,能得到仅高 $m$ 位与正确密钥全部一致的试验密钥 $k'$ 对应的 $p_{k'}$ 的实验值，就可根据引理 2 和定理 2 近似计算出算法 2 的正确率。

我们在主频为 2.5GHz 的 Pentium 4 PC 机上对 64bit 密钥的 ZLL 算法做了 1000 例攻击实验，每例实验的平均运行时间为 4min52s，求出的 64bit 密钥的正确率为 0.98。

在利用算法 2 所做的 1000 例试验中，当 $N$ =20 时成功率仅为 0.51，当 $N$ =25 时为 0.56，当 $N$ =30 时为 0.65。因此，适当增大 $N$ 可迅速提高算法 2 的成功率。当 $N$ 较小时，可以将算法 2 修改为多候选密钥方案以确保成功率。

**算法3**

步骤1　取 $N=20$，$d_{16}=5$，$d_{32}=14$，$d_{48}=22$，$d_{64}=28$。当 $1\le i\le 4$ 时 $m_i=16i$，$m_0=0$。令 $M_{16}=2$，$M_{32}=2$，$M_{48}=2$。当 $1\le i\le 3$ 时，令 $t_i$ 的初始值等于1。初始化 $i=1$。

步骤 2　攻击 $k^{(m_i)}$。当 $i$=1 时，令 $k'\in\{0,1\}^{16}$ 为 $k^{(16)}$ 的实验密钥，当 $2\le i\le 4$，将 $k^{(m_i)}$ 的最高 $m_{i-1}$ 比特块设置为 $k^{(m_{i-1})}$ 的第 $t_{i-1}$ 候选密钥，并穷举 $k^{(m_i)}$ 的低 $m_i-m_{i-1}$ 比特块的每个可能值,设 $k'$ 是如此得到的 $k^{(m_i)}$ 的一个试验密钥。对 $\forall j$，$1\le j\le N$，以 $k'\oplus\alpha_j^{(m_i)}$ 为密钥产生乱数序列的前 $d_{m_i}$ 个信号。如果该序列与由 $k\oplus\alpha_j$ 产生的已知乱数序列的前 $d_{m_i}$ 个信号全部相同，则记 $\xi_j(k')=1$，否则记 $\zeta_j(k')=0$。令 $T_{k'}=\sum_{j=1}^{N}\xi_j(k')$。如果试验密钥 $k_1',\cdots,k_{M_i}'$ 对任意的 $k'\notin\{k_1',\cdots,k_{M_i}'\}$，都有 $T_{k_1'}\ge T_{k_2'}\ge\cdots\ge T_{k_{M_i}'}\ge T_{k'}$ 成立，则将试验密钥 $k_1',\cdots,k_{M_i}'$ 分别记为 $k^{(m_i)}$ 的第 1，第 2，…，第 $M_i$ 候选密钥。同时将 $i$ 增 1，如果 $i=4$，则执行步骤 3，否则返回步骤 2。

步骤 3　对 $\forall j$，$1\le j\le N$，以 $k'\oplus\alpha_j^{(m_4)}$ 为密钥产生乱数序列的前 $d_{m_4}$ 个信号。如果该序列与由 $k\oplus\alpha_j$ 产生的已知乱数序列的前 $d_{m_4}$ 个信号全部相同，则输出 ZLL 算法的密钥 $k^{(m_4)}$；否则，将 $t_3$ 增加 1，并且在 $t_3\le M_3$ 时返回步骤 2。如果 $t_3=M_3+1$,令 $t_3=1$，$i$=2，同时将 $t_2$ 增 1，并在 $t_2\le M_2$ 时返回步骤 2。如果 $t_2=M_2+1$，令 $t_2=1$，$i$=1，同时将 $t_1$ 增 1，并在 $t_1\le M_1$ 时返回步骤 2。如果 $t_1=M_1+1$，则宣告算法 3 失败，算法结束。

1000 例试验的结果表明算法 3 的成功率为 0.96，平均运行时间为 154s。

在利用算法 1 攻击 $k^{(m)}$ 时，$k^{(m)}$ 的计数值近似为 $Np(n_m\ge d_m)$，错误实验密钥 $k'$ 的计数值近似为 $Np_{k'}$，其中 $p_{k'}=p$( 错误密钥 $k'$ 的吻合度 $\ge d_m$ )。显然，随着 $N$ 的增加，二者差异会逐渐增大，因而可以很大的概率求出 $k^{(m)}$。基于类似的原因，算法 2 和算法 3 能以很大的概率求出其它各密钥块。由此可见，对于密钥更长的混沌密码算法，也能利用上述方法以很小的计算复杂性和很高的成功率求出正确密钥；只要 $p(n_m\ge d_m)$ 与 $p_{k'}$ 有明显的差异，即使 $p(n_m\ge d_m)$ 不大，仍可有效地实施分割攻击。这样就利用相关密钥攻击解决了目前的分割攻击方法的两个局限性。

## 4　利用其它类型的相关密钥的攻击

我们提出的相关密钥攻击方案是基于等式 $(k\oplus\alpha_i)^m=k^{(m)}\oplus\alpha_i^{(m)}$ 确保了由 $k^{(m)}$ 能得到 $(k\oplus\alpha_i)^m$。如果相关密钥具有形式:

$$k+\alpha_1,k+\alpha_2,\cdots,k+\alpha_N$$

其中 + 为模 $2^n$ 加或者逐块模 $2^n$ 加，混沌映射 $f(k+\alpha_i)$ 仍具有输入的低位比特的变化对输出的高位比特影响较小这个特点，因而也表现出由 $k^{(m)}+\alpha_i^{(m)}$ 产生的乱数与由 $k+\alpha_i$ 产生的乱数的前几个比特相等的特性，所以仍然可采用算法 2 和算法 3 的攻击思想和方法对它进行攻击。

假设对 64bit 的 ZLL 算法，上述加法为模 $2^{64}$ 加。则易证 $(k+\alpha_i)^m=(k^{(m)}+\alpha_i^{(m)}+A_m2^{-m})\bmod 1$，其中 $A_m$ 是第 $m$+1 位向第 $m$ 位的进位。因此，当 $A_m=0$，$(k^{(m)}+\alpha_i^{(m)})\bmod 1$ 的吻合度 $\ge d$ 的概率最大；当 $A_m=1$，$(k^{(m)}+2^{-m}+\alpha_i^{(m)})\bmod 1$ 的吻合度 $\ge d$ 的概率最大，但二者非常接近。因此，按前面攻击方法求出的密钥可能是正确的 $k^{(m)}$，也可能是 $(k^{(m)}+2^{-m})\bmod 1$。为减少候选密钥的选取量，可采取将各候选密钥 $k'$ 对应的 $(k'-2^{-m})\bmod 1$ 也作为 $k^{(m)}$ 的候选密钥的技巧。试验表明，在已知相关密钥 $(k+\alpha_1)\bmod 2^{64}$，$(k+\alpha_2)\bmod 2^{64},\cdots,(k+\alpha_N)\bmod 2^{64}$ 对应的乱数序列时，利用修改后的算法 3 攻击 ZLL 算法，在主频为 2.5GHz 的 Pentium 4-PC 机上平均运行时间为 465s，成功率为 0.95。

基于同样的原理，如果函数 $g:\{0,1\}^n\times\{0,1\}^l\to\{0,1\}^n$ 具有输入的低位比特的变化对输出的高位比特的影响较小这个特点，那么就可利用形式为

$$g(k,\alpha_1),g(k,\alpha_2),\cdots,g(k,\alpha_N)$$

的相关密钥对该混沌密码进行相关密钥攻击。因此，在会话密钥协议中，以明传的随机数 $\alpha_i$ 和共享密钥 $k$ 为变量的函数 $g$ 的密码特性对于混沌密码能否抵抗相关密钥攻击十分重要。但归根结底，混沌密码是否安全，还是取决于其吻合度的分布是否合理，取决于该混沌密码是否有明显的信息泄漏。

## 5　结束语

本文将线性密码分析方法的思想与对混沌密码的分割攻击方法相结合，提出了对混沌密码的相关密钥攻击方法。由于该方法同时利用多个相关密钥产生的乱数序列对混沌密码进行攻击，从而大大提高了分割攻击的效率，克服了现有分割攻击方法的局限性。作为例子，本文实现了对具有 64bit 密钥的 ZLL 混沌密码[6]的相关密钥攻击。本文的结论说明，即使混沌密码的吻合度不是很大，仍有将其彻底攻破的可能性，因此，确保吻合度分布的合理性是混沌密码设计中需要考虑的一个重要问题。尽管本文的攻击实例是针对仅以初态为密钥的ZLL算法进行的，但对于将参数也设置为密钥的ZLL算法和其它类似的混沌密码，本文的攻击方法仍然能够适用。

## 参 考 文 献

[1] 李树钧等. 一类混沌流密码的分析[J]. 电子与信息学报, 2003, 25(4): 473-479.

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

[3] 金晨辉. 一个基于混沌的分组密码算法的分析[J]. 中国工程科学, 2001, 3(6): 75-80.

[4] 金晨辉, 高海英. 对两个基于混沌的序列密码算法的分析[J]. 电子学报, 2004, 34(7): 1066-1070.

[5] Matsui M. Linear cryptanalysis method for DES cipher[A]. In: Advance in Cryptology——Eurocrypt'93[C]. LNCS 765. Springer Verlag, 1994: 386-397.

[6] 周红, 罗杰, 凌燮亭. 混沌非线性反馈密码序列的理论和有限精度实现[J]. 电子学报, 1997, 25(10): 57-60.

金晨辉: 男, 1965年生, 教授, 博士生导师, 研究方向为密码学和信息安全.

杨 阳: 女, 1980年生, 硕士生, 研究方向为密码学.

祁传达: 男, 1964年生, 博士生, 研究方向为密码学和应用数学.