学术评论

一个基于混沌的分组密码算法的分析

金晨辉
（解放军信息工程大学 电子技术学院，郑州 450004）

[摘要] “基于混沌的分组密码置换网络的设计”一文提出的一个分组密码算法在已知明文攻击和唯密文攻击下都是很容易被破译的，而且在知道加密变换的条件下，很容易利用分割攻击方法求出该分组密码的密钥。此外，基于 Logistic 映射的混沌序列的相邻值之间的相互制约性，以及该混沌序列的前若干值对初值的低位比特不敏感。

[关键词] 混沌序列；分组密码；移位密码；唯密文攻击；已知明文攻击；分割攻击

1 相关知识

开区间(0,1)中的每个实数 a 都可表示为 $a=\sum_{i=1}^{\infty}a_i2^{-i}$，$a_i\in\{0,1\}$，其中 $\forall t>1$，a_t，a_{t+1}，a_{t+2}，… 不全为 1。称 $\sum_{i=1}^{m}$ 为 a 的 m 精度小数。显然，每个 m 精度小数都与 $\{0,1\}^m$ 中的 m 维二元向量一一对应。为方便起见，称 $(a_1,a_2,\cdots,a_n)$ 为 a 的高 n 位。

文献[1]利用混沌变换 $f(x)=4x(1-x)$，$0<x<1$ 产生的混沌序列构造了一个分组密码算法，并认为该密码算法具有很高的安全性，其具体构造方法如下：

设密钥规模为 m 比特，$x_0=\sum_{i=1}^{m}k_i2^{-i}$ 为密钥 $k=(k_1,k_2,\cdots,k_m)$ 对应的 m 精度小数，$\forall i\geqslant 1$，递归地定义 x_i 为 $4x_{i-1}(1-x_{i-1})$ 的 m 精度小数，这样就得到一条混沌序列 $x_0,x_1,x_2,\cdots$；将该序列中诸元素 x_i 换作 n 精度（$n\leqslant m$）小数 x_i' 后又得到该混沌序列的一条截尾序列 $x_0',x_1',x_2',\cdots$。将序列 $2^nx_0',2^nx_1',2^nx_2',\cdots$ 的前 2^n 个不同的元素依出现的次序分别记为 $p(0),p(1),\cdots,p(2^n-1)$，则由 m 比特的密钥 k 就产生了一个 2^n 元置换 p。在加密时，先将明文每 2^n 个字符分为一组，然后将 $(a_{p(0)},a_{p(1)},\cdots,a_{p(2^n-1)})$ 作为明文分组 $(a_0,a_1,\cdots,a_{2^n-1})$ 对应的密文。当然，也可采取将该加密变换的逆变换作为加密变换的方式。究竟采取哪种加密方式，文献[1]中没有明确交代，但这对分析没有本质的影响。

2 对基于混沌序列的分组密码算法的分析

容易看出，该分组密码算法本质上是利用秘密密钥产生一个古典的移位密码，因而是极其脆弱的。由于移位密码的破译问题早已解决，移位密码既不能抵抗已知明文攻击，也不能抵抗唯密文攻击，因而该文提出的分组密码算法没有安全性可言。

这里做了一例已知明文攻击实验。设密钥规模为 64 比特，密钥为 f0f1 f0f1 f0f1 f0f1（16 进制表示，下同），则它产生的 64 元置换 p 将 0，1，…，63 依次变换为：

60 14 44 54 31 63 0 1 3 45 52 37 61 8 29 7
26 27 62 38 10 34 5 18 53 36 4 17 50 43 55 28
2 9 33 16 49 20 30 48 46 51 40 59 47 15 39 11
25 21 56 13 42 57 24 12 32 6 23 41 58 19 22 35

[收稿日期] 2001-02-09；修回日期 2001-03-27

[作者简介] 金晨辉（1965-），男，河南扶沟县人，解放军信息工程大学教授

取加密变换为 $x_i \to x_{p(i)}$，则明文

a great deal of interest has bee
n shown recently in electronic f
und transfer systems, much of the
attraction of such a system is
that it offers an alternative to
the growing problems of paperba
sed transactions for the more. wi
th careful design an electronic
fund transfer system can offer I
ts users a higher degree of secu
rity than they have hitherto had
available.

在最后添加21个空格后可构成6个分组，其中每两行构成一个明文分组，其加密结果为：

t ndasr o ryc thstcwi oe inefne
tsefhlelcnebgern o ea renliea ta
an soutssa, sy nftfciacsesuteeyct
stm rs nmatdfiotr oeh hh u mr
t oirpasttofmhpevnrglbaobn o r
heatelrnps afw o eifatte egtrai
antsohtsoh genescreir crln finet
c t mtri o .dauefaelc waendsior
ratnfaoy s eeeugufnee cferstisr
cuoemh grns isseaf d drshfret
ha ntt hyah i aoh l avd a
vi rh . ht l bi eteya reet

记 $A_{k,i}$ 是第 k 个密文分组中出现第 k 明文分组中的第 i 个字母（$0 \leqslant i \leqslant 63$）的位置全体构成的集合，$A_i = \bigcap_{k=1}^{t} A_{k,i}$，则当 A_0，A_1，…，A_{63} 都是单点集合时，映射 p 就唯一确定了。实验表明：对于64字符分组的加密算法，只要利用3个分组（即取 $t=3$）就能按上述方法唯一确定出映射 p；对于128字符分组的加密算法，只要利用4个分组（即取 $t=4$）就能按上述方法唯一确定出映射 p。

由于对移位密码的唯密文攻击也有成熟的攻击方法，这里不再多叙。此时，借助明文的内在规律，就可在仅知道密文的条件下对移位密码实现破译。

3 混沌序列的内在规律

下面将要指出：混沌序列的截尾序列 x_0'，x_1'，x_2'，…的相邻信号之间具有很强的相互制约关系，而且初值 x_0 的低位比特对 x_0'，x_1'，x_2'，…的前几个值几乎没有影响，换句话说，x_0'，x_1'，x_2'，…的前几个值只与初值 x_0 的高位比特有关。借助这两个性质，可以减少破译该分组密码所需的已知明文量或已知密文量，并求出产生该移位变换的密钥 k。

例如，对于上面的攻击实验，对于64字符分组的加密算法，只要利用2个密文分组就可确定出 $p(0), p(1), \cdots, p(63)$ 中除

$$p(1), p(7), p(12), p(15), p(19), p(28),$$
$$p(46), p(51), p(53), p(54), p(62)$$

以外的全部值；借助 x_i' 与 x_{i+1}' 的相互制约性可直接假设出 $p(1), p(7), p(12)$，再借助后一个性质，就可利用分割攻击方法求出密钥 k，从而完全确定出移位变换 p。具体攻击方法将在介绍完攻击原理后再给予介绍。以下分别用 $\mathrm{E}(x)$ 和 ceil (x) 表示不大于 x 的最大整数和不小于 x 的最小整数。

定理1 设 x_0，x_1，x_2，… 是利用混沌变换 $f(x)=4x(1-x), 0<x<1$ 由 m 精度的初值 x_0 产生的 m 精度小数序列，x_i' 是 x_i 的 n 精度小数，则在 x_i' 给定时，x_{i+1}' 至多有5种变化，且 $2^n x_{i+1}'$ 的可能取值范围是仅与 x_i' 有关的连续的整数。

证明 设 $x_i = x_i' + a$，则 $0 \leqslant a < 2^{-n}$，且由 x_i 是 m 精度的小数知 $0 \leqslant a \leqslant 2^{-n} - 2^{-m}$，故有 $x_i' \leqslant x_i \leqslant x_i' + 2^{-n} - 2^{-m}$。又由 $f(x) = 1 - (2x-1)^2$ 知 $2^n x_{i+1}' = \mathrm{E}(2^n f(x_i)) = \mathrm{E}(2^n - 2^n(2x_i - 1)^2)$。

现借助 $x_i' \leqslant x_i \leqslant x_i' + 2^{-n} - 2^{-m}$ 这个条件，考查整数 $2^n x_{i+1}'$ 的取值范围。

由于 $\frac{\mathrm{d}}{\mathrm{d}x} f(x) = -4(2x-1)$，故当 $0 < x \leqslant 0.5$ 时，$f(x)$ 为增函数；当 $0.5 \leqslant x < 1$ 时，$f(x)$ 为减函数。下面分两种情况证明。

1）如果 $x_i' < 0.5$，则由 x_i' 是 n 精度小数知 $x_i' \leqslant 0.5 - 2^{-n}$，从而

$$x_i' \leqslant x_i \leqslant x_i' + 2^{-n} - 2^{-m} \leqslant 0.5 - 2^{-m}。$$

再由 $0 < x \leqslant 0.5$ 时 $f(x)$ 为增函数知 $f(x_i') \leqslant f(x_i) \leqslant f(x_i' + 2^{-n} - 2^{-m})$，因而

$$\mathrm{E}(2^n f(x_i')) \leqslant \mathrm{E}(2^n f(x_i)) \leqslant \mathrm{E}(2^n f(x_i' + 2^{-n} - 2^{-m})),$$

即

$$\mathrm{E}(2^n f(x_i')) \leqslant 2^n x_{i+1}' \leqslant \mathrm{E}(2^n f(x_i' + 2^{-n} - 2^{-m}))。$$

由 $n < m$ 知 $2^{2-m} - 2^{2-n} < 0$，令

$$g(x) = 2^n f(x + 2^{-n} - 2^{-m}) - 2^n f(x),$$

则

$$g(x) = 2^n[(2^{2-m} - 2^{2-n})(2x-1) - (2^{1-m} - 2^{1-n})^2]$$

是减函数，因而

$$g(x_i') < g(0) = 2^n[(2^{2-n} - 2^{2-m}) - (2^{1-m} - 2^{1-n})^2] < 4。$$

再记

$$2^n f(x_i' + 2^{-n} - 2^{-m}) = 1\ \mathrm{E}(2^n f(x_i' + 2^{-n} - 2^{-m})) + \alpha,$$

$$2^n f(x_i') = \mathrm{E}(2^n f(x_i')) + \beta,$$

则 $0 \leqslant \alpha, \beta < 1$，因而 $\alpha - \beta < 1$，从而 $2^n x_{i+1}'$ 的可能取值个数为

$$\mathrm{E}(2^n f(x_i' + 2^{-n} - 2^{-m})) - \mathrm{E}(2^n f(x_i')) + 1 = 2^n f(x_i' + 2^{-n} - 2^{-m}) - 2^n f(x_i') + \alpha - \beta + 1 < 5 + \alpha - \beta < 6。$$

2）如果 $x_i' \geqslant 0.5$，则有 $0.5 \leqslant x_i' \leqslant x_i \leqslant x_i' + 2^{-n} - 2^{-m}$。再由 $0 < x \leqslant 0.5$ 时 $f(x)$ 为减函数知 $f(x_i' + 2^{-n} - 2^{-m}) \leqslant f(x_i) \leqslant f(x_i')$，因而

$$\mathrm{E}(2^n) f(x_i' + 2^{-n} - 2^{-m})) \leqslant \mathrm{E}(2^n) f(x_i)) \leqslant \mathrm{E}(2^n f(x_i')),$$

即

$$\mathrm{E}(2^n) f(x_i' + 2^{-n} - 2^{-m})) \leqslant 2^n x_{i+1}' \leqslant \mathrm{E}(2^n f(x_i'))。$$

由 $n < m$ 知 $2^{2-m} - 2^{2-n} < 0$。

令

$$g(x) = 2^n f(x) - 2^n f(x + 2^{-n} - 2^{-m}),$$

则

$$g(x) = 2^n[(2^{2-n} - 2^{2-m})(2x-1) + (2^{1-n} - 2^{1-m})^2]$$

是增函数，故由 $x_i' \leqslant 1 - 2^{-n}$ 知

$$g(x_i') \leqslant g(1 - 2^n) = 4 - 2^{2-n} - (1 - 2^{-m})2^{2+n-m} < 4,$$

从而类似 $x_i' < 0.5$ 的情形可证：

$$\mathrm{E}(2^n f(x_i')) - \mathrm{E}(2^n f(x_i' + 2^{-n} - 2^{-m})) + 1 < 6,$$

这说明 x_{i+1}' 至多有 5 种变化。显然 x_{i+1}' 这些可能的取值都是连续的。

实验结果与定理 1 完全吻合。当定理 1 中的 $m = 64$ 且 $n = 6$ 时，x_i' 的后继 x_{i+1}' 的取值个数是 1,2,3,4,5 的分别有 8,16,16,16 和 8 个。

定理 2　设 $x_0, x_1, x_2, \cdots$ 是利用混沌变换 $f(x) = 4x(1-x), 0 < x < 1$ 由 m 精度的初值 x_0 产生的 m 精度小数序列，x_i' 是 x_i 的 n 精度小数，则在 x_{i+1}' 给定时，如果 $x_{i+1}' = 2^n - 1$，则 x_i' 至多有 $\mathrm{E}(2^{\frac{n}{2}-1}) + \mathrm{ceil}(2^{\frac{n}{2}-1}) + 1$ 种变化，否则 x_i' 至多有 $\mathrm{E}(2^{\frac{n+1}{2}}) - 2^{\frac{n}{2}}) + 4$ 种变化。此外，x_i' 的取值范围是仅与 x_i' 有关的连续的整数。

证明　由 $f(x) = 1 - (2x-1)^2$ 知

$$2^n x_{i+1}' = \mathrm{E}(2^n f(x_i)) = \mathrm{E}(2^n - 2^n(2x_i - 1)^2)。$$

由于 $f(x_i) = 1 - (2x_i - 1)^2$ 是精度为 $2m$ 的小数，故有

$$x_{i+1}' \leqslant 1 - (2x_i - 1)^2 \leqslant x_{i+1}' + 2^{-n} - 2^{-2m},$$

从而

$$2^{2n-2} + 2^{2n-2m-2} - 2^{n-2}(2^n x_{i+1}' + 1) \leqslant (2^n x_i - 2^{n-1})^2 \leqslant 2^{2n-2} - 2^{2n-2} x_{i+1}',$$

故有

$$\frac{1}{2}\sqrt{2^{2n} + 2^{2n-2m} - 2^n(2^n x_{i+1}' + 1)} \leqslant \left|2^n x_i - 2^{n-1}\right| \leqslant \frac{1}{2}\sqrt{2^{2n} - 2^{2n} x_{i+1}'},$$

因而

$$2^{n-1} + \frac{1}{2}\sqrt{2^{2n} + 2^{2n-2m} - 2^n(2^n x_{i+1}' + 1)} \leqslant 2^n x_i \leqslant 2^{n-1} + \frac{1}{2}\sqrt{2^{2n} - 2^{2n} x_{i+1}'},$$

或者

$$2^{n-1} - \frac{1}{2}\sqrt{2^{2n} - 2^{2n} x_{i+1}'} \leqslant 2^n x_i \leqslant 2^{n-1} - \frac{1}{2}\sqrt{2^{2n} + 2^{2n-2m} - 2^n(2^n x_{i+1}' + 1)},$$

故 $2^n x_i'$ 的个数为

$$N = \mathrm{E}\left(2^{n-1} + \frac{1}{2}\sqrt{2^{2n} - 2^{2n} x_{i+1}'}\right) - \mathrm{E}\left(2^{n-1} + \frac{1}{2}\sqrt{2^{2n} + 2^{2n-2m} - 2^n(2^n x_{i+1}' + 1)}\right) + 1 + \mathrm{E}\left(2^{n-1} - \frac{1}{2}\sqrt{2^{2n} + 2^{2n-2m} - 2^n(2^n x_{i+1}' + 1)}\right) - \mathrm{E}\left(2^{n-1} - \frac{1}{2}\sqrt{2^{2n} - 2^{2n} x_{i+1}'}\right) + 1 = \mathrm{E}\left(\frac{1}{2}\sqrt{2^{2n} - 2^{2n} x_{i+1}'}\right) + ceil\left(\frac{1}{2}\sqrt{2^{2n} - 2^{2n} x_{i+1}'}\right) - \mathrm{E}\left(\frac{1}{2}\sqrt{2^{2n} + 2^{2n-2m} - 2^{2n} x_{i+1}' - 2^n}\right) - ceil\left(\frac{1}{2}\sqrt{2^{2n} + 2^{2n-2m} - 2^{2n} x_{i+1}' - 2^n}\right) + 2。$$

当 $2^n x_{i+1}' = 2^n - 1$ 时，

$$N = \mathrm{E}(2^{\frac{n}{2}-1}) + \mathrm{ceil}(2^{\frac{n}{2}-1}) - \mathrm{E}(2^{n-m-1}) - \mathrm{ceil}(2^{n-m-1}) + 2 =$$

$$\mathrm{E}(2^{\frac{n}{2}-1})+\mathrm{ceil}(2^{\frac{n}{2}-1})+1。$$

一般地，令

$$g(x)=\frac{1}{2}\sqrt{2^{2n}-2^{n}x}-\frac{1}{2}\sqrt{2^{2n}+2^{2n-2m}-2^{n}(x+1)},$$

则 $g(x)$是严格增函数，故当 $2^{n}x'_{i+1}\leqslant 2^{n}-2$ 时，有

$$g(2^{n}x'_{i+1})\leqslant g(2^{n}-2)=2^{\frac{n-1}{2}}-\sqrt{2^{2n-2m-2}+2^{n-2}}<2^{\frac{n-1}{2}}-2^{\frac{n}{2}-1}。$$

令

$$\mathrm{E}\left(\frac{1}{2}\sqrt{2^{2n}-2^{n}x'_{i+1}}\right)=\frac{1}{2}\sqrt{2^{2n}-2^{n}x'_{i+1}}-\alpha,$$

$$\mathrm{ceil}\left(\frac{1}{2}\sqrt{2^{2n}-2^{n}x'_{i+1}}\right)=\frac{1}{2}\sqrt{2^{2n}-2^{n}x'_{i+1}}+\alpha',$$

$$\mathrm{E}\left(\frac{1}{2}\sqrt{2^{2n}+2^{2n-2m}-2^{n}x'_{i+1}-2^{n}}\right)=\frac{1}{2}\sqrt{2^{2n}+2^{2n-2m}-2^{n}x'_{i+1}-2^{n}}-\beta,$$

$$\mathrm{ceil}\left(\frac{1}{2}\sqrt{2^{2n}+2^{2n-2m}-2^{n}x'_{i+1}-2^{n}}\right)=\frac{1}{2}\sqrt{2^{2n}+2^{2n-2m}-2^{n}x'_{i+1}-2^{n}}+\beta',$$

则 $0\leqslant\alpha,\alpha',\beta,\beta'<1$，于是 $\alpha'-\alpha<1,\beta-\beta'<1$，故由 $2^{n}x'_{i+1}\leqslant 2^{n}-2$ 知

$$N=\frac{1}{2}\sqrt{2^{2n}-2^{2n}x'_{i+1}}-\alpha+\frac{1}{2}\sqrt{2^{2n}-2^{2n}x'_{i+1}}+\alpha'-\left[\frac{1}{2}\sqrt{2^{2n}+2^{2n-2m}-2^{2n}x'_{i+1}-2^{n}}-\beta\right]-\left[\frac{1}{2}\sqrt{2^{2n}+2^{2n-2m}-2^{2n}x'_{i+1}-2^{n}}+\beta'\right]+2=2g(2^{n}x'_{i+1})+2+(\alpha'-\alpha)+(\beta-\beta')<2g(2^{n}-2)+4=2^{\frac{n+1}{2}}-2^{\frac{n}{2}}+4。$$

故有

$$N\leqslant\mathrm{E}(2g(2^{n}-2)+4)=\mathrm{E}(2^{\frac{n+1}{2}}-2^{\frac{n}{2}})+4。$$

即 $2^{n}x'_{i}$ 至多有 $\mathrm{E}(2^{\frac{n+1}{2}}-2^{\frac{n}{2}})+4$ 种可能值，显然这些可能值都是连续的整数。

例如，如果 $n=6$，则当 $2^{n}x'_{i+1}=63$ 时，$2^{n}x'_{i}$ 至多有

$$N=\mathrm{E}(2^{\frac{6}{2}-1})+\mathrm{ceil}(2^{\frac{6}{2}-1})+1=9$$

种变化；当 $2^{n}x'_{i+1}\leqslant 62$ 时，$2^{n}x'_{i}$ 至多有 $\mathrm{E}(2^{\frac{6+1}{2}}-2^{\frac{6}{2}})+4=7$ 种变化。实际的值比 7 都小，而且基本上都是 2 和 4。

定理 2 再次说明 $3^{n}x'_{i}$ 与 $2^{n}x'_{i+1}$ 之间有很强的相互制约关系。下面指出混沌序列 $x'_0,x'_1,x'_2,\cdots$ 的另一个弱点。

定理 3 设 $f(x)=4x(1-x),0<x<1,0<\varepsilon<1$，则 $|f(x+\varepsilon)-f(x)|\leqslant 4\varepsilon(1+\varepsilon)$。

证明 由 $f(x+\varepsilon)-f(x)=-4\varepsilon(2x+\varepsilon-1)$ 即知 $|f(x+\varepsilon)-f(x)\leqslant 4\varepsilon(1+\varepsilon)$。

推论 设 $\varepsilon_0=\varepsilon$ 为 m 精度小数 $\varepsilon_{k+1}=2^{-m}\mathrm{E}(2^{m}\varepsilon_k(1+\varepsilon_k)),k\geqslant 0$ 又设 x'_k 和 y'_k 分别为初值 x_0 和 y_0 对应的混沌序列的截尾序列的值，且 $y_0-x_0=\varepsilon$，则有

$$|y'_k-x'_k|\leqslant 4^{k}\varepsilon_{k+1}。$$

证明 由于 $f(x)$和 $f(x+\varepsilon)$都是 m 精度的小数，故定理 3 的结论还可进一步精确为

$$|f(x+\varepsilon)-f(x)|\leqslant 2^{2-m}\mathrm{E}(2^{m}\varepsilon(1+\varepsilon)),$$

由此利用归纳法就可证得本推论。

设 $g(x)=x+\delta,0\leqslant x,\delta<1$，则 $g(x)\geqslant 1$ 的概率为 δ，故定理 3 及其推论说明，当 ε 很小时，初值 x_0 中低位比特的变化对混沌序列的截尾序列 $x'_0,x'_1,x'_2,\cdots$ 的开头几个信号几乎没有影响，也就是说 $x'_0,x'_1,x'_2,\cdots$ 的前几个值只与初值 x_0 的高位比特有关。

例如，取 $m=128,n=7,\varepsilon=2^{-64}$，则 $\varepsilon_k\approx 2^{2k-64}$，由于当初值 x_0 的低 64 位变化时，必有 $\varepsilon<2^{-64}$，故此时前 20 个信号都不改变的概率不小于 $1-\prod_{k=1}^{20}(1-2^{2k-64})\approx 1$，即前 20 个信号几乎不会改变，实验也证实了这个结果。

这个特性为利用截尾序列 $x'_0,x'_1,x'_2,\cdots$ 对其初值 x_0 实施分割攻击奠定了基础。

4 对基于混沌序列的分组密码算法的密钥的分割攻击

4.1 分割攻击算法

以 $m=64$ 为例做了一例实验，实际的密钥 k 取为 f0f1 f0f1 f0f1 f0f1。实验密钥 k'的高 16 位至低 16 位依次记为 k_1,k_2,k_3,k_4，采取对 k_1,k_2,k_3,k_4 逐个穷举的方法对正确密钥 k 实施分割攻击。记 $y'_0,y'_1,y'_2,\cdots$为以 y 为初值产生的截尾序列。具体算法如下：

Step 1 记 $n_1=3,n_2=19,n_3=36,n_4=640,m_1=2^{10},m_2=m_3=m_4=2^{16}$。令 $k_1=0,t=1$。

Step 2 执行 $k'\leftarrow x'_0+\sum_{i=1}^{t}k_i2^{-16i}$，并检查以 k'

为初值产生的截尾序列片段 $y'_0, y'_1, \cdots, y'_{n_t}$ 是否与 $x'_0, x'_1, x'_2, \cdots$ 的相应值一致。

如果全部一致，则在 $t=4$ 时将 k' 作为候选密钥输出，算法终止；在 $t<4$ 时将 t 增 1 后，$k_t=1$ 令并返回 Step 2。如果不全一致，则执行 Step 3。

Step 3　将 k_t 增 1 后判断 $k_t=m_t$ 是否成立。当 $k_t \neq m_t$ 时返回执行 Step 2，当 $k_t=m_t$ 时判断 t 是否为 1。如果 $t=1$，则报告算法失败，终止；如果 $t \neq 1$，则令 $k_t=0$，并将 t 减 1 后返回执行 Step 3。

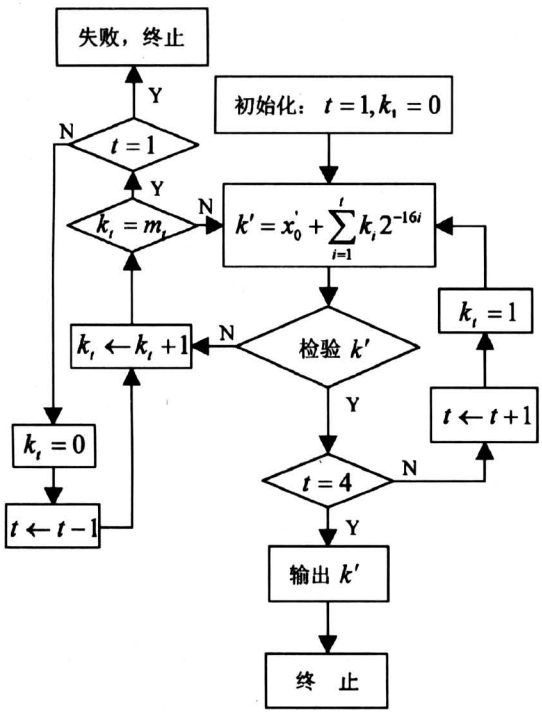

图 1　分割攻击算法流程图

Fig.1　The flow diagram of the algorithm of divide-and-conquer attack

几点说明：

1) 由于 x'_0 就是初值 x_0 的高 6 位比特，因而密钥 $k=x_0$ 的高 6 比特可直接由 x'_0 获得；

2) 实验表明，在上述算法中，如果限定 $t=1$，则通过 Step 2 的 k_1 的范围是从 f0ae 至 f102，共 85 个；如果限定 $t \leqslant 2$，则通过 Step 2 的 (k_1, k_2) 的范围是从 f0f1 f0d4 至 f0f1 f119，共 70 个；如果限定 $t \leqslant 3$，则通过 Step 2 的 (k_1, k_2, k_3) 的范围是从 f0f1 f0f1 f0ed 至 f0f1 f0f1 f0ff，共 19 个；通过全部检验的只有正确密钥。

3) 在不知序列 $x'_0, x'_1, x'_2, \cdots$ 但已知其产生的移位变换 p 的条件下，将上述算法适当修改，仍可求出正确密钥。这时，只需将 Step 2 中“检查 $y'_0, y'_1, \cdots, y'_{n_i}$ 是否与 $x'_0, x'_1, x'_2, \cdots$ 的相应值一致”改为“检查 $y'_0, y'_1, \cdots, y'_{n_i}$ 产生的不同值 $p'(0), p'(1), \cdots, p'(s)$ 是否与 $p(0), p(1), \cdots, p(s)$ 的相应值一致”即可。实验表明，此时仍可唯一求出正确密钥。

4) 即使移位变换 p 的值有几个未知，在对攻击算法做适当改动的条件下，仍可求出正确密钥。实验表明，对于前面提到的对 64 字符分组的分组密码的已知明文攻击，在仅知两个分组的已知明文的条件下，仍然可以唯一求出正确密钥。

4.2　分割攻击算法的进一步完善

上述分割攻击算法中 n_i 的选取需根据大量的实验确定。当 n_i 选取得太小时，会造成 k_i 的候选量太多，因而增加算法的计算复杂性；当 n_i 选取得太大时，又会漏掉正确的 k_i，为此，可利用混沌序列可能初值的分布特性进一步完善对密钥的分割攻击方案。

定理 4　设 $f(x)=4x(1-x)$，则开区间 $(0,1)$ 中使得 $a \leqslant \mathrm{E}(2^n f(z)) \leqslant b$ 的点 z 形成两个分别位于 $(0,0.5]$ 和 $[0.5,1)$ 的闭区间。

证明　由 $\mathrm{E}(x)$ 是增函数，以及 $f(x)$ 在 $(0, 0.5]$ 和 $[0.5,1)$ 内分别递增和递减知 $\mathrm{E}(2^n f(z))$ 在 $(0,0.5]$ 和 $[0.5,1)$ 内连续且分别递增和递减，故由闭区间关于连续的单调函数的逆像仍是闭区间即知本定理成立。

推论 1　设 $x'_0, x'_1, x'_2, \cdots$ 是前面定义的序列，则使得 $x'_i=a_i$ 对 $0 \leqslant i \leqslant k$ 都成立的初值 x_0 对应的 $2^m x_0$ 构成 $[0, 2^m]$ 中的一个连续整数片段。

证明　由定理 4 即知推论 1 在 $k=1$ 时成立。设推论 1 对 $k-1$ 成立，则使 $x'_i=a_i$ 对 $1 \leqslant i \leqslant k$ 都成立的 m 精度小数 x_1 全体形成一个连续片段 $[c, d]$。由定理 4 知，使得 $c \leqslant x_1 \leqslant d$ 成立的 m 精度小数 x_0 在 $(0, 0.5]$ 和 $[0.5, 1)$ 中各形成一个连续片段，因而它们与 $\{x \in (0,1): \mathrm{E}(2^n x)=x'_0\}$ 的交集构成一个 m 精度小数的连续片段。

推论 2　设 $x'_0, x'_1, x'_2, \cdots$ 是前面定义的序列，$p(0), p(1), \cdots, p(k)$ 是由序列 $\{x'_i\}_{i=0}^{\infty}$ 产生的 $Z/(2^n)$ 中的前 $k+1$ 个互不相同数，$k<2^n$，记 $p'(0), p'(1), \cdots, p'(k)$ 是由初值 y_0 产生的序列 $\{y'_i\}_{i=0}^{\infty}$

构造的 $Z/(2^n)$中的前 $k+1$ 的互不相同数，则使得 $p'(i)=p(i)$对 $0\leqslant i\leqslant k$ 都成立的所有初值 y_0 对应的 $2^m y_0$ 构成$[0,2^m]$中的若干个连续的整数片段。

证明 设由 $y'_0, y'_1, y'_2, \cdots, y'_t$ 可造出 $p(0)$, $p(1),\cdots,p(k)$，则混沌序列产生的前 $t+1$ 个 n 精度小数是 $y'_0, y'_1, y'_2, \cdots, y'_t$ 的初值 y_0 全体构成一个连续片段。又因可造出 $p(0),p(1),\cdots,p(k)$ 的 $y'_0, y'_1, y'_2, \cdots, y'_t$ 有多种可能，因而能产生 $p(0)$, $p(1),\cdots,p(k)$的初值全体将形成多个连续片段。

由此可知，搜索混沌序列的初值所得的解一般是连续的。如果记录下通过分割攻击算法第 $i+1$ 步的 k_i 所在连续整数片段的端点及该片段中点的个数，则当因某个 n_i 选取太大而漏掉正确的 k_i 时，就可在 k_i 所在的连续整数片段向外偏移几个点搜索 k_i。一般来说，从个数较少的那些连续整数片段向外偏移来搜索 k_i 时成功率较大。

5 结语

作者分析了“基于混沌的分组密码置换网络的设计”一文设计的分组密码的不安全性，并给出了相应的攻击算法。混沌序列的截尾序列的相邻值之间具有很强的相互制约性，且前若干值主要由初值的高位比特决定。一个安全的分组密码算法不仅要有足够的分组规模和密钥规模，而且还必须满足混乱和扩散等设计标准，所设计的算法必须能够经得住选择明文等攻击方法的考验。在将混沌变换应用于密码领域时，必须设法克服混沌变换的自身弱点。

参考文献

[1] 孙枫，秦红磊，徐耀群，等. 基于混沌的分组密码置换网络的设计[J]. 中国工程科学，2000，2(9)：47～50

[2] 王育民，何大可. 保密学——基础和应用[M]. 西安：西安电子科技大学出版社，1990

[3] Baker W. Cryptanalysis of the single columnar transposition cipher [M]. Aegean Park Press, USA, 1994

Analysis of A Block Cipher Based on Chaos

Jin Chenhui

(*Electronic Technology Institute, Information Engineering University, Zhengzhou* 450004, *China*)

[**Abstract**] In this paper, it is pointed out that the block cipher proposed in "Design of Block Cipher substitution network on chaos" can be broken by attack with known plaintext and attack with ciphertext only, and the key of this cipher can be found by the divide-and-conquer attack with the encipher transformation. Furthermore, the mutual restriction between the successive values of the chaos sequences based on the Logistic mapping, and the property that the frontal values of the chaos sequences are not sensitive to the bits on the lower positions of the initial value are also pointed out.

[**Key words**] chaos sequence; block cipher; transposition cipher; attack with known plaintext; attack with ciphertext only; divide-and-conquer attack

* * * * * *