单圈 T 函数输出序列的稳定性研究

罗小建*①② 胡 斌① 郝珊珊③ 张 翀④
①(信息工程大学电子技术学院 郑州 450004)
②(解放军 69010 部队 乌鲁木齐 830000)
③(铁道警官专科学校 郑州 450003)
④(信息工程大学电子技术学院兰州技术大队 兰州 730000)

摘 要：k-错线性复杂度是衡量序列稳定性的重要指标，该文对单圈 T 函数按位输出序列的 k-错线性复杂度进行了深入研究，利用序列线性复杂度的多项式求解法和 Chan Games 算法，分析得到了当输入规模 n=2^t 时，单圈 T 函数按位输出序列 k-错线性复杂度的分布，并进一步给出了该序列的 k-错线性复杂度曲线。

关键词：密码学；T 函数；线性复杂度；k-错线性复杂度
中图分类号：TN918.1 **文献标识码**：A **文章编号**：1009-5896(2011)10-2328-06
DOI: 10.3724/SP.J.1146.2010.01384

The Stability of Output Sequences of Single Cycle T-function

Luo Xiao-jian①② Hu Bin① Hao Shan-shan③ Zhang Chong④
①(*Electronic Technology Institute, Information Engineering University*, *Zhengzhou* 450004, *China*)
②(*PLA* 69010 *Army*, *Urumqi* 830000, *China*)
③(*Railway Police College*, *zhengzhou* 450003, *China*)
④(*Electronic Technology Institute*, *Information Engineering University*, *Lanzhou Institute of Technology Unit*, *Lanzhou* 730000, *China*)

Abstract: The k-error linear complexity of the output sequences by-bit of single cycle T-function is investigated with the polynomial and the Chan Games algorithm as the main tools. The distribution of k-error linear complexity and k-error linear complexity profile of the output sequences by-bit of single cycle T-function are presented when n=2^t.

Key words: Cryptography; T-functions; Linear complexity; k-error linear complexity

1 引言

2002 年，Klimov 等人[1]首次提出了 T 函数的概念。T 函数由于具有计算速度快、密码学性质良好等特点而得到广泛应用，先后用于构造分组密码、Hash 函数和流密码。文献[1]用单圈 T 函数代替流密码中的线性反馈移位寄存器，因此，单圈 T 函数输出序列的稳定性成为研究的重点。安全强度高的序列不但具有高的线性复杂度，而且必须具有很好的稳定性，而序列的稳定性一般采用 k-错线性复杂度进行刻画，如果序列的安全性好，其 k-错线性复杂度也应较大。

单圈 T 函数输出序列有两种输出方式：按状态输出和按位输出。国内外对单圈 T 函数输出序列线性复杂度的研究较少，2006 年，张文英等人[2]给出了在输入规模 n=2^t 时，单圈 T 函数按状态输出序列的线性复杂度和线性复杂度第 1 下降点，以及该点对应的 k-错线性复杂度取值；2008 年，赵璐等人[3]得到了在输入规模 n=2^t 时，单圈 T 函数按位输出序列的线性复杂度和线性复杂度第 1 下降点，以及该点对应的 k-错线性复杂度取值。

本文对单圈 T 函数按位输出序列的 k-错线性复杂度进行了深入研究，利用序列线性复杂度的多项式求解法和 Chan Games 算法，在输入规模 n=2^t 时，分析得到了单圈 T 函数按位输出序列线性复杂度的所有下降点及其对应位置的 k-错线性复杂度取值，并进一步给出该序列 k-错线性复杂度的分布情况及 k-错线性复杂度曲线。

2 准备知识

符号说明：

(1)记 Z_2^n 是二元域上的 n 维线性空间，$Z/(2^n)$ 为模 2^n 剩余类环。对 $x \in Z/(2^n)$，x 有唯一的二进制表示 $x=\sum_{i=0}^{n-1}2^i[x]_i$，这样可将 x 看成是 Z_2^n 中的

2010-12-16 收到，2011-07-25 改回
*通信作者：罗小建 luojian1232@163.com

向量，即 $x=([x]_{n-1},[x]_{n-2},\cdots,[x]_0)$，下文中将对其不加区分地使用。

(2)“$\oplus$”表示“异或加”。

(3) 若 $x=([x]_{n-1},[x]_{n-2},\cdots,[x]_0)\in Z/(2^n)$，则 $W(x)$ 表示 x 的汉明重量，特别地，对于二元周期序列 S，$W(S)$ 表示 S 在一个周期内的 1 的个数。

线性复杂度：

设 $S=s_0s_1s_2\cdots$ 是 Z_2 上周期为 N 的序列，定义其形式化多项式 $s(x)$ 为

$$s(x)=s_0+s_1x+s_2x^2+\cdots+s_{N-1}x^{N-1} \tag{1}$$

序列 S 的线性复杂度指产生此序列的线性反馈移位寄存器的最小阶数，记为 $\mathrm{LC}(S)$。文献[4]给出了周期序列 S 的线性复杂度的一个代数化描述，即

$$\begin{aligned}\mathrm{LC}(S)&=\deg\left(\frac{1-x^N}{\gcd(1-x^N,s(x))}\right)\\&=N-\deg(\gcd(1-x^N,s(x)))\end{aligned} \tag{2}$$

2.1 基本定义

定义 1[1]　设 $f(x)$ 是 $Z/(2^n)\to Z/(2^n)$ 上的多输出函数，记 $f(x)=([f(x)]_{n-1},\cdots,[f(x)]_1,[f(x)]_0)$，如果其输出的第 i 位 $[f(x)]_i$ 仅与输入的第 0 至第 i 位，即 $([x]_i,\cdots,[x]_0)$ 有关，则称 $f(x)$ 为 T 函数。其中 $[x]_i$，$[f(x)]_i$ 表示 x 和 $f(x)$ 的第 i 路分量，$i=0,1,\cdots,n-1$。

显然，根据 T 函数的定义，可将 T 函数表示为如下形式：

$$\begin{pmatrix}([x]_{n-1},\cdots,[x]_1,[x]_0)\\\downarrow\\(f_{n-1}([x]_{n-1},[x]_{n-2},\cdots,[x]_0),\cdots,f_1([x]_1,[x]_0),f_0([x]_0))\end{pmatrix} \tag{3}$$

其中 $f_i(x)=f_i([x]_i,[x]_{i-1},\cdots,[x]_0)$ 为布尔函数。

定义 2[1]　若可逆 T 函数的状态转移图是单圈的，则称该函数为单圈 T 函数。

定义 3[5]　对一个周期序列 S，每个周期改变小于或等于 k 比特后得到的新序列的最小线性复杂度，称为 k-错线性复杂度，记为 $\mathrm{LC}_k(S)$。

从定义可以看出，计算 $\mathrm{LC}_k(S)$ 的一般方法为构造一个周期与 S 相同的序列 $\underline{e}$，一般称为错误序列，则 $\mathrm{LC}_k(S)=\min\{\mathrm{LC}(S\oplus\underline{e})\,|\,W(\underline{e})\le k\}$。

定义 4[5]　对周期序列 S，定义 $\min\mathrm{error}(S)$ 为使得 $\mathrm{LC}_k(S)<\mathrm{LC}(S)$ 的 k 的最小值。

定义 5[5]　设 S 是 Z_2 上周期为 N 的序列，S 的 k-错复杂度曲线定义为 S 的 k-错复杂度序列，即 $\mathrm{LC}_0(S)=\mathrm{LC}(S),\mathrm{LC}_1(S),\cdots,\mathrm{LC}_{W(S)}(S)$。

2.2 单圈 T 函数输出序列

单圈 T 函数周期达到最大，即为 2^n，设 $s_i=(a_{i,0},a_{i,1},\cdots,a_{i,n-1})$ 为单圈 T 函数输出的第 i 个状态，$1\le i\le n-1$，称 $S(T)=(s_0\,|\,s_1\,|\cdots|\,s_{2^n-1}\cdots)$ 为单圈 T 函数输出序列，其中 $s_i\,|\,s_{i+1}$ 表示状态 s_i 和 s_{i+1} 的级联，即 $s_i\,|\,s_{i+1}=(a_{i,0},\cdots,a_{i,n-1},a_{i+1,0},\cdots,a_{i+1,n-1})$。

引理 1[1]　设 $f(x)$ 是单圈 T 函数，$s_0,s_1,\cdots,s_{2^n-1}$ 表示 $f(x)$ 在一个周期内的所有输出状态，设 $a_i=(a_{0,i},a_{1,i},\cdots,a_{2^n-1,i},\cdots)$ 表示 $f(x)$ 的第 i 分位序列，则

(1) a_i 的周期为 2^{i+1}；

(2) $a_{j,i}\oplus a_{j+2^i,i}=1$ 对 $j\ge 0$ 都成立。

3　单圈 T 函数按位输出序列的 k-错线性复杂度

在序列的线性复杂度较好时，有时还需要进一步考察其稳定性，其稳定性可通过 k-错线性复杂度来刻画。我们主要研究当 $n=2^t$ 时，单圈 T 函数输出序列的 k-错线性复杂度的分布，首先给出几个引理。

引理 2[2]　设 S 是周期为 N 的二元序列，若 $N=2^t$，则 $\min\mathrm{error}(S)=2^{W(N-\mathrm{LC}(S))}$。

引理 3[2]　(Chan Games 算法)　令 $s^m=(s_0,s_1,\cdots,s_{2^m-1})\in Z/(2^{2^m})$，则 $S=(s^m,s^m,s^m,\cdots)$ 是周期为 2^m 的序列。记 $s^m=(L(s^m),R(s^m))$，其中 $L(s^m)=(s_0,\cdots,s_{2^{m-1}-1})$，$R(s^m)=(s_{2^{m-1}},\cdots,s_{2^m-1})$ 分别表示 s^m 的左半部分和右半部分。令 $\mathfrak{D}=L(s^m)\oplus R(s^m)$，则当 $\mathfrak{D}$ 为全零向量时，$\mathrm{LC}(S)=\mathrm{LC}(L(s^m))$，当 $\mathfrak{D}$ 不为全零向量时，$\mathrm{LC}(S)=2^{m-1}+\mathrm{LC}(\mathfrak{D})$。

由 Chan Games 算法知，序列的周期越小，线性复杂度越小。

基于上述几个引理，下面研究当 $n=2^t$ 时，单圈 T 函数按位输出序列 S 的 k-错线性复杂度，首先给出当 $k=2^u\times 2^{n-1}$ 时，S 的 k-错线性复杂度，其中 $0\le u\le t$。

定理 1　设 S 是单圈 T 函数按位输出序列，若输入规模 $n=2^t$，则 S 的 k-错线性复杂度为 $\mathrm{LC}_k(S)=(n-2^u-1)\times 2^n+2^{n-2^u-1}+1$，其中 $k=2^u\times 2^{n-1}$，$0\le u\le t$。

证明　设单圈 T 函数按位输出序列为 $S=(a_{0,0},\cdots,a_{2^n-1,0},a_{0,1},\cdots,a_{2^n-1,1},\cdots,a_{0,n-1},\cdots,a_{2^n-1,n-1},\cdots)$。令 $l_i=(a_{0,i},\cdots,a_{2^n-1,i})$，$i=0,1,\cdots,n-1$。$S$ 在一个周期内的 2^{n+t} 个比特记为 $S^{(n)}=(l_0\,|\,l_1\,|\cdots|\,l_{n-1})$，令 $\underline{e}=(e_0,e_1,\cdots,e_{n-1})$，其中 $e_i=(e_{0,i},\cdots,e_{2^n-1,i})\in\{0,1\}^n$，$i=0,1,\cdots,n-1$，则 $S^{(n)}\oplus\underline{e}=(l_0\oplus e_0,\cdots,l_{n-1}\oplus e_{n-1})$。记 $c_1=L(S^{(n)}\oplus\underline{e})\oplus R(S^{(n)}\oplus\underline{e}),c_2=L(c_1)\oplus R(c_1),\cdots,c_t=L(c_{t-1})\oplus R(c_{t-1})$。

序列 S 在每个周期内改变 $2^u\times 2^{n-1}$ 个比特后的序列记为 S'，由 Chan Games 算法可知，S' 的周期越小，S' 的线性复杂度也越小。若 c_1 为全零，则 S' 的周期整除 2^{n+t-1}，我们首先考察重量为 $2^u\times 2^{n-1}$ 的

$\underline{e}$ 能否使得 c_1 为全零。

由于 $c_1=((l_0\oplus e_0)\oplus(l_{2^{t-1}}\oplus e_{2^{t-1}}),(l_1\oplus e_1)\oplus(l_{2^{t-1}+1}\oplus e_{2^{t-1}+1}),\cdots,(l_{2^{t-1}-1}\oplus e_{2^{t-1}-1})\oplus(l_{2^t-1}\oplus e_{2^t-1}))$，因此，要使得 c_1 为全零，$\underline{e}$ 必须使得下列方程组成立：

$$\left.\begin{aligned} l_0\oplus l_{2^{t-1}}&=e_0\oplus e_{2^{t-1}}\\ l_1\oplus l_{2^{t-1}+1}&=e_1\oplus e_{2^{t-1}+1}\\ &\vdots\\ l_{2^{t-1}-1}\oplus l_{2^t-1}&=e_{2^{t-1}-1}\oplus e_{2^t-1}\end{aligned}\right\}\tag{4}$$

由引理 1 知，$l_i\oplus l_{2^{t-1}+i}$ 中分别含有 2^{n-1} 个 0 和 1，$0\le i\le 2^{t-1}-1$，则 $W(e_i\oplus e_{2^{t-1}+i})=2^{n-1}$，即 $(W(e_i,e_{2^{t-1}+i}))_{\min}=2^{n-1}$。进而有 $W(\underline{e})_{\min}=2^{t-1}\times 2^{n-1}$，假定 u 是 0,1,$\cdots$,t 中一个不定的数，则 $W(\underline{e})=2^u\times 2^{n-1}<2^{t-1}\times 2^{n-1}$，于是 $c_1\ne 0$，因此，$\mathrm{LC}(S+\underline{e})=2^{t-1+n}+\mathrm{LC}(c_1)$。用同样的考察方法发现 $c_2,c_3,\cdots,c_{t-u-1}$ 全不为全零，

$$\mathrm{LC}(S\oplus\underline{e})=2^{t-1+n}+2^{t-2+n}+\cdots+2^{u+1+n}+\mathrm{LC}(c_{t-u-1})\tag{5}$$

下面考察重量为 $2^u\times 2^{n-1}$ 的 $\underline{e}$ 是否可使得 $c_{t-u-1}=0$。

由于 $c_{t-u}=\left(\bigoplus_{i=0}^{2^{t-u}-1}(l_{i\times 2^u}\oplus e_{i\times 2^u}),\bigoplus_{i=0}^{2^{t-u}-1}(l_{i\times 2^u+1}\oplus e_{i\times 2^u+1}),\cdots,\bigoplus_{i=0}^{2^{t-u}-1}(l_{i\times 2^u+2^u-1}\oplus e_{i\times 2^u+2^u-1})\right)$，因此，要使得 c_{t-u} 为全零，$\underline{e}$ 必须满足下列方程组成立：

$$\left.\begin{aligned} \bigoplus_{i=0}^{2^{t-u}-1}l_{i\times 2^u}&=\bigoplus_{i=0}^{2^{t-u}-1}e_{i\times 2^u}\\ \bigoplus_{i=0}^{2^{t-u}-1}l_{i\times 2^u+1}&=\bigoplus_{i=0}^{2^{t-u}-1}e_{i\times 2^u+1}\\ &\vdots\\ \bigoplus_{i=0}^{2^{t-u}-1}l_{i\times 2^u+2^u-1}&=\bigoplus_{i=0}^{2^{t-u}-1}e_{i\times 2^u+2^u-1}\end{aligned}\right\}\tag{6}$$

当 $0\le j\le 2^u-1$ 时，$W\left(\bigoplus_{i=0}^{2^{t-u}-1}e_{i\times 2^u+j}\right)=2^{n-1}$，即 $(W(e_j,e_{2^u+j},\cdots,e_{(2^{t-u}-1)\times 2^u+j}))_{\min}=2^{n-1}$，进而有 $W(\underline{e})_{\min}=2^u\times 2^{n-1}$。若 $W(\underline{e})=2^u\times 2^{n-1}$ 且式(3)成立时，则

$$\mathrm{LC}(S\oplus\underline{e})=2^{t-1+n}+2^{t-2+n}+\cdots+2^{u+1+n}+\mathrm{LC}(L(c_{t-u-1}))\tag{7}$$

其中 $L(c_{t-u-1})=\left(\bigoplus_{i=0}^{2^{t-u-1}-1}(l_{i\times 2^{u+1}}\oplus e_{i\times 2^{u+1}}),\bigoplus_{i=0}^{2^{t-u-1}-1}(l_{i\times 2^{u+1}+1}\oplus e_{i\times 2^{u+1}+1}),\cdots,\bigoplus_{i=0}^{2^{t-u-1}-1}(l_{i\times 2^{u+1}+2^u-1}\oplus e_{i\times 2^{u+1}+2^u-1})\right)$。

下面证明当 $\underline{e}$ 满足式(3)且

$$\left(\bigoplus_{i=0}^{2^{t-u-1}-1}e_{i\times 2^{u+1}},\bigoplus_{i=0}^{2^{t-u-1}-1}e_{i\times 2^{u+1}+1},\cdots,\bigoplus_{i=0}^{2^{t-u-1}-1}e_{i\times 2^{u+1}+2^u-1}\right)$$

为全零，即 $L(c_{t-u-1})=\left(\bigoplus_{i=0}^{2^{t-u-1}-1}l_{i\times 2^{u+1}},\bigoplus_{i=0}^{2^{t-u-1}-1}l_{i\times 2^{u+1}+1},\cdots,\bigoplus_{i=0}^{2^{t-u-1}-1}l_{i\times 2^{u+1}+2^u-1}\right)$ 时，

$\mathrm{LC}(c_{t-u-1})$ 取得最小值 $(2^u-1)\times 2^n+2^{2^t-2^u-1}+1$。

记 $\bigoplus_{i=0}^{2^{t-u-1}-1}l_{i\times 2^{u+1}+j}=l'_{h_j}=(a'_{0,h_j},a'_{1,h_j},\cdots,a'_{2^n-1,h_j})$，$\bigoplus_{i=0}^{2^{t-u-1}-1}e_{i\times 2^{u+1}+j}=e'_{h_j}$，其中 $0\le j\le 2^{u+1}-1$，则 $c_{t-u-1}=(l'_{h_0}\oplus e'_{h_0},l'_{h_1}\oplus e'_{h_1},\cdots,l'_{h_{2^{u+1}-1}}\oplus e'_{h_{2^{u+1}-1}})$。设 $(l'_{h_0},l'_{h_1},\cdots,l'_{h_{2^u-1}})$ 的形式化多项式为 $s'(x)$，则

$$\begin{aligned}s'(x)=&(a'_{0,h_0}+a'_{1,h_0}x+\cdots+a'_{2^n-1,h_0}x^{2^n-1})\\&+x^{2^n}(a'_{0,h_1}+a'_{1,h_1}x+\cdots+a'_{2^n-1,h_1}x^{2^n-1})+\cdots\\&+x^{2^{u-1}\times 2^n}(a'_{0,h_{2^{u-1}}}+a'_{1,h_{2^{u-1}}}x+\cdots\\&+a'_{2^n-1,h_{2^{u-1}}}x^{2^n-1})+\cdots+x^{(2^u-1)2^n}(a'_{0,h_{2^u-1}}\\&+a'_{1,h_{2^u-1}}x+\cdots+a'_{2^n-1,h_{2^u-1}}x^{2^n-1})\end{aligned}$$

由引理 1 可知，当 $0\le i\le 2^u-2$ 时，$a'_{j,h_i}=a'_{2^w+j,h_i}$，其中 $w\ge h_{2^u-1}$。因此，

$$\begin{aligned}&x^{i\times 2^n}(a'_{0,h_i}+a'_{1,h_i}x+\cdots+a'_{2^n-1,h_i}x^{2^n-1})\\&=x^{i\times 2^n}(1+x)^{2^n-2^{h_{2^u-1}}}(a'_{0,h_i}+a'_{1,h_i}x+\cdots\\&\quad+a'_{2^{h_{2^u-1}}-1,h_i}x^{2^{h_{2^u-1}}-1})\end{aligned}$$

又由引理 1 知，$a'_{j,h_{2^u-1}}=a'_{2^{h_{2^u-1}}+j,h_{2^u-1}}\oplus 1$ 且 $a'_{j,h_{2^u-1}}=a'_{2^w+j,h_{2^u-1}}$，其中 $w>h_{2^u-1}$。因此，

$$\begin{aligned}&x^{(2^u-1)2^n}\left(a'_{0,h_{2^u-1}}+a'_{1,h_{2^u-1}}x+\cdots+a'_{2^n-1,h_{2^u-1}}x^{2^n-1}\right)\\&=x^{(2^u-1)2^n}(1+x)^{2^n-2^{h_{2^u-1}}+1}\Big[(1+x)^{2^{h_{2^u-1}}}\left(a'_{0,h_{2^u-1}}\right.\\&\quad\left.+a'_{1,h_{2^u-1}}x+\cdots+a'_{2^{h_{2^u-1}}-1,h_{2^u-1}}x^{2^{h_{2^u-1}}-1}\right)\\&\quad+x^{2^{h_{2^u-1}}}(1+x)^{2^{h_{2^u-1}}-1}\Big]\end{aligned}$$

因此，$s'(x)$ 可进一步化简为

$$s'(x)=(1+x)^{2^n-2^{h_{2^u-1}}-1}\left[(1+x)g(x)+x^{2^{h_{2^u-1}}+(2^u-1)\times 2^n}\right]$$

其中

$$\begin{aligned}g(x)=&\left(a'_{0,h_0}+a'_{1,h_0}x+\cdots+a'_{2^{h_{2^u-1}}-1,h_0}x^{2^{h_{2^u-1}}-1}\right)\\&+x^{2^n}\left(a'_{0,h_1}+a'_{1,h_1}x+\cdots+a'_{2^{h_{2^u-1}}-1,h_1}x^{2^{h_{2^u-1}}-1}\right)\\&+\cdots+x^{(2^u-1)2^n}\\&\left(a'_{0,h_{2^u-1}}+a'_{1,h_{2^u-1}}x+\cdots+a'_{2^{h_{2^u-1}}-1,h_{2^u-1}}x^{2^{h_{2^u-1}}-1}\right)\end{aligned}$$

设 $L(c_{t-u-1})$ 的形式化多项式为 $s'_1(x)$，则

$$s_1^{'}(x)=s'(x)+(e_{0,h_0}^{'}+e_{1,h_0}^{'}x+\cdots+e_{2^n-1,h_0}^{'}x^{2^n-1})+x^{2^n}(e_{0,h_1}^{'}+e_{1,h_1}^{'}x+\cdots+e_{2^n-1,h_1}^{'}x^{2^n-1})+\cdots+x^{(2^u-1)\times 2^n}(e_{0,h_{2^u-1}}^{'}+\cdots+e_{2^n-1,h_{2^u-1}}^{'}x^{2^n-1})$$

由 $\mathrm{LC}(l_{h_0}^{'},l_{h_1}^{'},\cdots,l_{h_{2^u-1}}^{'})=2^u\times 2^n-\gcd(1-x^{2^u\times 2^n},s'(x))$ 可知，若 $\mathrm{LC}(L(c_{t-u-1}))<\mathrm{LC}(l_{h_0}^{'},l_{h_1}^{'},\cdots,l_{h_{2^u-1}}^{'})$，则

$$\gcd(1-x^{2^u\times 2^n},s_1^{'}(x))>\gcd(1-x^{2^u\times 2^n},s'(x)) \quad (8)$$

因此，要使得 $\mathrm{LC}(L(c_{t-u-1}))<\mathrm{LC}(l_{h_0}^{'},l_{h_1}^{'},\cdots,l_{h_{2^u-1}}^{'})$ 成立，则 $s_1^{'}(x)$ 必须具有形式：

$$s_1^{'}(x)=s'(x)+\sum_{r=0}^{2l}x^{i_r\times 2^n+j_r}(1+x)^{2^n-2^{h_{2^u-1}}-1}+g_1(x)(1+x)^{2^n-2^{h_{2^u-1}}} \quad (9)$$

其中 $0\le l\le 2^{u-1},0\le i_r\le 2^u-1,0\le j_r\le 2^{h_{2^u-1}},r=0,1,\cdots,2l$，$i_0,i_1,\cdots,i_{2l}$ 两两不同，$g_1(x)$ 是布尔函数。

从式(9)可知，由于 $s_1^{'}(x)$ 的最简式中存在 $x^{i_0\times 2^n+j_0}(1+x)^{2^n-2^{h_{2^u-1}}-1}$，而 $x^{i_0\times 2^n+j_0}(1+x)^{2^n-2^{h_{2^u-1}}-1}$ 的展开式中共有 2^{n-1} 项，即 $W(e_{h_{i_0}}^{'})=2^{n-1}$，又由于 $W(e_{h_{i_0}}^{'},e_{h_{i_0+2^u}}^{'})=2^{n-1}$，故此时 $e_{h_{i_0+2^u}}^{'}=0$。根据式(3)有，$l_{h_{i_0}}^{'}+e_{h_{i_0}}^{'}=l_{h_{i_0+2^u}}^{'}$，显然，此时 $L(c_{t-u-1})>\mathrm{LC}(l_{h_0}^{'},l_{h_1}^{'},\cdots,l_{h_{2^u-1}}^{'})$，与假设矛盾，故 $\mathrm{LC}(L(c_{t-u-1}))\ge(2^u-1)\times 2^n+2^{2^t-2^u-1}+1$，即当 $W(\underline{e})=2^u\times 2^{n-1}$ 时，序列 $S+\underline{e}$ 的线性复杂度最小值为

$$\begin{aligned}\mathrm{LC}(S\oplus\underline{e})&=2^{t-1+n}+2^{t-2+n}+\cdots+2^{u+1+n}+\mathrm{LC}(L(c_{t-u-1}))_{\min}\\&=(n-2^u-1)\times 2^n+2^{n-2^u-1}+1\end{aligned}$$

故定理成立。　　证毕

设 S 是二元周期序列，记 $\mathrm{err}_1(S)$ 为使得 $\mathrm{LC}_k(S)<\mathrm{LC}(S)$ 成立最小的 k，称 $\mathrm{err}_1(S)$ 为序列 S 线性复杂度的第1下降点，显然 $\mathrm{err}_1(S)=\min\mathrm{error}(S)$；记 $\mathrm{err}_2(S)$ 为使得 $\mathrm{LC}_t(S)<\mathrm{LC}_{k_1}(S)$ 成立最小的 t，其中 $k_1=\mathrm{err}_1(S)$，称 $\mathrm{err}_2(S)$ 为序列 S 线性复杂度的第2下降点。同样可得到第3,…，第 k 下降点的定义。显然 $1\le\mathrm{err}_1(S)<\cdots<\mathrm{err}_k(S)<\cdots$ 且 $\mathrm{LC}(S)>\mathrm{LC}_{\mathrm{err}_1(S)}(S)>\cdots>\mathrm{LC}_{\mathrm{err}_k(S)}(S)>\cdots$。

基于定理1可进一步给出当输入规模 n=2^t 时，单圈T函数按位抽取输出序列 S 的 k-错线性复杂度取值分布。首先给出序列 S 的线性复杂度的第 u 下降点及对应的 k-错线性复杂度，其中 $1\le u\le n$–1。

定理 2　设 S 是单圈T函数按位输出序列，若输入规模 n=2^t，则 S 的线性复杂度第 u 下降点及其对应的 k-错线性复杂度为 $\mathrm{err}_u(S)=u\times 2^{n-1}$ 且 $\mathrm{LC}_k(S)=(n-u-1)\times 2^n+2^{n-u-1}+1$，其中 k=$\mathrm{err}_u(S)$, $1\le u\le n$–1。

证明　设单圈T函数按位输出序列为 S=$(a_{0,0},\cdots,a_{2^n-1,0},a_{0,1},\cdots,a_{2^n-1,1},\cdots,a_{0,n-1},\cdots,a_{2^n-1,n-1},\cdots)$。令 $l_i=(a_{0,i},\cdots,a_{2^n-1,i})$，$i=0,1,\cdots,n-1$。$S$ 在一个周期内的 2^{n+t} 个比特记为 $S^{(n)}=(l_0\,|\,l_1\,|\cdots|\,l_{n-1})$，令错误序列 $\underline{e}=(e_0,e_1,\cdots,e_{n-1})$，其中 $e_i=(e_{0,i},\cdots,e_{2^n-1,i})\in\{0,1\}^n$，$i=0,1,\cdots,n-1$，则 $S^{(n)}\oplus\underline{e}=(l_0\oplus e_0,\cdots,l_{n-1}\oplus e_{n-1})$。记 c_1=$L(S^{(n)}\oplus\underline{e})\oplus R(S^{(n)}\oplus\underline{e})$, c_2=$L(c_1)\oplus R(c_1),\cdots$, $c_t=L(c_{t-1})\oplus R(c_{t-1})$。

下面用数学归纳法对该定理进行证明。

(1)当 $u=1$ 时，由引理2可知，$\min\mathrm{error}(S)=2^{n-1}$，即 $\mathrm{err}_1(u)=2^{n-1}$，由定理1可知 $\mathrm{LC}(S+\underline{e})=2^{t+n}-2^{n+1}+2^{n-2}+1$，故当 $u=1$ 时结论成立。

(2)假设当 $u=h$ 时，结论成立，即 $\mathrm{err}_h(S)=h\times 2^{n-1}$ 且 $\mathrm{LC}_k(S)=(n-h-1)\times 2^n+2^{n-h-1}+1$, $k=\mathrm{err}_h(S)$。

首先构造满足 $\mathrm{LC}_k(S)=(n-h-1)\times 2^n+2^{n-h-1}+1$, $k=\mathrm{err}_h(S)$ 的错误序列 $\underline{e}$，此时 $\mathrm{LC}(S\oplus\underline{e})=\mathrm{LC}_k(S)=(n-h-1)\times 2^n+2^{n-h-1}+1$，通过研究使得序列 $S\oplus\underline{e}$ 线性复杂度的下降点，可进一步确定当 $u=h$+1时，$\mathrm{err}_{h+1}(S)$ 且 $\mathrm{LC}_k(S)$，$k=\mathrm{err}_{h+1}(S)$ 的取值情况。

设 $h=2^{i_r}+2^{i_{r-1}}+\cdots+2^{i_1}$，其中 $0\le i_1<i_2<\cdots<i_r\le t$，并且 $0\le h\le 2^t$。下面根据定理1的证明过程构造错误序列 $\underline{e}$ 使其满足 $W(\underline{e})=h\times 2^{n-1}$ 且 $\mathrm{LC}(S+\underline{e})=(n-h-1)\times 2^n+2^{n-h-1}+1$。总共分成 r 步实现，具体步骤如下：

第1步，由于 $2^{i_r}\le h<2^{i_r+1}$，由定理1可知，改变 $S^{(n)}$ 的 $2^{i_r}\times 2^{n-1}$ 个比特使得其线性复杂度变小。记向量集合 $A_{i_r}=\{e_{j\times 2^{i_r+1}+j_1}\,|\,j=0,1,\cdots,2^{t-i_r-1}-1,\ j_1=0,1,\cdots,2^{i_r}-1\}$。

令 A_{i_r}=0 且 $\bigoplus_{j=0}^{2^{t-i_r-1}-1}e_{j\times 2^{i_r+1}+2^{i_r}}$, $\bigoplus_{j=0}^{2^{t-i_r-1}-1}e_{j\times 2^{i_r+1}+2^{i_r}+1}$, …, $\bigoplus_{j=0}^{2^{t-i_r-1}-1}e_{j\times 2^{i_r+1}+2^{i_r+1}-1}$ 满足下列方程成立：

$$\left.\begin{aligned}\bigoplus_{j=0}^{2^{t-i_r}-1}l_{j\times 2^{i_r}}&=\bigoplus_{j=0}^{2^{t-i_r}-1}e_{j\times 2^{i_r}}\\\bigoplus_{j=0}^{2^{t-i_r}-1}l_{j\times 2^{i_r}+1}&=\bigoplus_{j=0}^{2^{t-i_r}-1}e_{j\times 2^{i_r}+1}\\&\vdots\\\bigoplus_{j=0}^{2^{t-i_r}-1}l_{j\times 2^{i_r}+2^{i_r}-1}&=\bigoplus_{j=0}^{2^{t-i_r}-1}e_{j\times 2^{i_r}+2^{i_r}-1}\end{aligned}\right\} \quad (10)$$

由定理1知，此时，$\mathrm{LC}(S\oplus\underline{e})=2^{t-1+n}+2^{t-2+n}+\cdots+2^{i_r+1+n}+\mathrm{LC}(L(c_{t-i_r-1}))$，且 $L(c_{t-i_r-1})=\left(\bigoplus_{j=0}^{2^{t-i_r-1}-1}l_{j\times 2^{i_r+1}},\bigoplus_{j=0}^{2^{t-i_r-1}-1}l_{j\times 2^{i_r+1}+1},\cdots,\bigoplus_{j=0}^{2^{t-i_r-1}-1}l_{j\times 2^{i_r+1}+2^{i_r}-1}\right)$。

第2步，由于 $2^{i_{r-1}}\le h-2^{i_r}<2^{i_{r-1}+1}$，因此在第1步的基础上继续改变 $S^{(n)}$ 的 $2^{i_{r-1}}\times 2^{n-1}$ 个比特，使得改变后的序列 S' 线性复杂度更小。

记 $C_{i_r}=\left(\bigoplus_{j=0}^{2^{t-i_r-1}-1}(l_{j\times 2^{i_r+1}}\oplus e_{j\times 2^{i_r+1}}),\bigoplus_{j=0}^{2^{t-i_r-1}-1}(l_{j\times 2^{i_r+1}+1}\oplus e_{j\times 2^{i_r+1}+1}),\cdots,\bigoplus_{j=0}^{2^{t-i_r-1}-1}(l_{j\times 2^{i_r+1}+2^{i_r}-1}\oplus e_{j\times 2^{i_r+1}+2^{i_r}-1})\right)$，用 C_{i_r} 代替 $S^{(n)}$。由定理 1 可知，当 C_{i_r} 改变 $2^{i_{r-1}}$ 个比特时，

$$\mathrm{LC}(C_{i_r})=2^n\times(2^{i_r-1}+2^{i_r-2}+\cdots+2^{i_{r-1}+1})+\mathrm{LC}(C_{i_{r-1}})$$

其中 $C_{i_{r-1}}=\left(\bigoplus_{j=0}^{2^{i_r-i_{r-1}-1}-1}C_{i_r,j\times 2^{i_{r-1}+1}},\bigoplus_{j=0}^{2^{i_r-i_{r-1}-1}-1}C_{i_r,j\times 2^{i_{r-1}+1}+1},\cdots,\bigoplus_{j=0}^{2^{i_r-i_{r-1}-1}-1}C_{i_r,j\times 2^{i_{r-1}+1}+2^{i_{r-1}+1}-1}\right)$。

记 $A_{i_{r-1}}=A_{i_r}-\{e_{(2^{i_r-1}-2^{i_{r-1}}+j_1)}\mid j_1=2^{i_{r-1}},2^{i_{r-1}}+1,\cdots,2^{i_{r-1}+1}-1\}$。令 $A_{i_{r-1}}=0$ 且 $e_{(2^{i_r-1}-2^{i_{r-1}}+j_1)}$ 为使得 $\bigoplus_{j=0}^{2^{i_r-i_{r-1}-1}-1}C_{i_r,j\times 2^{i_{r-1}+1}+j_1}=\bigoplus_{j=0}^{2^{i_r-i_{r-1}-1}-1}C_{i_r,j\times 2^{i_{r-1}+1}+2^{i_{r-1}}+j_1}$ 成立的向量，其中 $j_1=2^{i_{r-1}},2^{i_{r-1}}+1,\cdots,2^{i_{r-1}+1}-1$。则

$$\mathrm{LC}(L(c_{t-i_r-1}))=2^n\times(2^{i_r-1}+2^{i_r-2}+\cdots+2^{i_{r-1}+1})+\mathrm{LC}(L(C_{i_{r-1}}))$$

因此，$S^{(n)}$ 在改变 $2^{i_r+i_{r-1}}\times 2^{n-1}$ 个比特时，序列 S 改变后线性复杂度最小可达到

$$\begin{aligned}\mathrm{LC}(S\oplus\underline{e})&=2^{t-1+n}+2^{t-2+n}+\cdots+2^{i_r+1+n}+2^n\\&\quad\times(2^{i_r-1}+2^{i_r-2}+\cdots+2^{i_{r-1}+1})\\&\quad+\mathrm{LC}(L(C_{i_{r-1}}))\\&=2^{t+n}-2^{i_r+n}-2^{i_{r-1}+1+n}+\mathrm{LC}(L(C_{i_{r-1}}))\end{aligned}$$

由于 $e_{(2^{i_r-1}-2^{i_{r-1}}+j_1)}$，$j_1=2^{i_{r-1}},2^{i_{r-1}}+1,\cdots,2^{i_{r-1}+1}-1$ 在第 2 步中发生改变，故需要将第 1 步中的向量集

$$\bigoplus_{j=0}^{2^{t-i_r-1}-1}e_{j\times 2^{i_r+1}+2^{i_r}},\bigoplus_{j=0}^{2^{t-i_r-1}-1}e_{j\times 2^{i_r+1}+2^{i_r}+1},\cdots,\bigoplus_{j=0}^{2^{t-i_r-1}-1}e_{i\times 2^{i_r+1}+2^{i_r+1}-1}$$

进行相应的改变使得式(10)继续成立。

以此类推，继续第 3 步，…，第 r 步，每一步都需要对前一步的向量集进行相应的改变，最终得到错误序列 $\underline{e}$ 满足 $W(\underline{e})=h\times 2^{n-1}$ 且

$$\begin{aligned}\mathrm{LC}(S\oplus\underline{e})&=2^{t+n}-2^{i_r+n}-2^{i_{r-1}+1+n}+(2^{i_{r-1}+n}\\&\quad-2^{i_{r-2}+1+n})+\cdots+(2^{i_2+n}-2^{i_1+1+n})\\&\quad+\mathrm{LC}(L(C_{i_1}))\\&=(2^t-h-1)\times 2^n+2^{2^t-h-1}+1\end{aligned}$$

由引理 2 知，$\min\mathrm{error}(S\oplus\underline{e})=2^{W(h)}\times 2^{n-1}$。从 $u=h$ 时错误序列的构造过程知，要使得序列继续变小，需要在 $L(C_{i_1})$ 中改变若干个比特。从 $S\oplus\underline{e}$ 的线性复杂度计算过程，我们可将 $S\oplus\underline{e}$ 形象地表示为 $(L(C_{i_1}),R(C_{i_1}),R(C_{i_2}),R(C_{i_3}),\cdots,R(C_{i_r}))$，其中 $L(C_{i_j})=R(C_{i_j})$，并且 $(L(C_{i_1}),R(C_{i_1}),R(C_{i_2}),\cdots,R(C_{i_{j-1}}))\in L(C_{i_j})$，$j=2,3,\cdots,r$。若 $L(C_{i_1})$ 改变 2^{n-1} 个比特，则要使得

$$\begin{aligned}\mathrm{LC}(S\oplus\underline{e})&=2^{t+n}-2^{i_r+n}-2^{i_{r-1}+1+n}+(2^{i_{r-1}+n}\\&\quad-2^{i_{r-2}+1+n})+\cdots+(2^{i_2+n}-2^{i_1+1+n})\\&\quad+\mathrm{LC}(L(C_{i_1}))\end{aligned}$$

继续成立，需要相应地对 $R(C_{i_1})$ 改变对应于 $L(C_{i_1})$ 的 2^{n-1} 个比特，$R(C_{i_2})$ 中改变对应于 $L(C_{i_2})$ 的 $2\times 2^{n-1}$ 个比特，如此类推，最后在 $R(C_{i_r})$ 中改变对应于 $L(C_{i_r})$ 的 $2^{r-1}\times 2^{n-1}$ 个比特。总共在每个周期内改变了序列 $S\oplus\underline{e}$ 的 $(1+1+2+2^2+\cdots+2^{r-1})\times 2^{n-1}=2^r\times 2^{n-1}=2^{W(h)}\times 2^{n-1}$ 个比特。因此，在一个周期内改变序列 $S\oplus\underline{e}$ 的 $2^{W(h)}\times 2^{n-1}$ 个比特等价于改变 $L(C_{i_1})$ 的 2^{n-1} 个比特，也即改变序列 S 的 $h\times 2^{n-1}+2^{n-1}=(h+1)\times 2^{n-1}$ 个比特，即 $\min\mathrm{error}(S\oplus\underline{e})=2^{W(h)}\times 2^{n-1}$ 等价于 $\mathrm{err}_{h+1}(S)=(h+1)\times 2^{n-1}$，且

$$\mathrm{LC}_k(S)=2^{t+n}-h\times 2^n-2^{i_1+n}+\mathrm{LC}_{k'}(L(C_{i_1}))$$

其中 $k=\mathrm{err}_{h+1}(S),k'=2^{n-1}$。

下面计算 $\mathrm{LC}_{k'}(L(C_{i_1}))$，$k'=2^{n-1}$ 的值。

$$L(C_{i_1})=\left(\bigoplus_{(j_{r-1},\cdots,j_1,j_0)=(0,\cdots,0,0)}^{(2^{i_2-i_1-1}-1,\cdots,2^{i_r-i_{r-1}-1}-1,2^{t-i_r-1}-1)}l_{j_0 2^{i_r+1}+\cdots+j_{r-1}2^{i_1+1}+0},\cdots,\bigoplus_{(j_{r-1},\cdots,j_1,j_0)=(0,\cdots,0,0)}^{(2^{i_2-i_1-1}-1,\cdots,2^{i_r-i_{r-1}-1}-1,2^{t-i_r-1}-1)}l_{j_0 2^{i_r+1}+\cdots+j_{r-1}2^{i_1+1}+2^{i_1}-1}\right)$$

因此，$\mathrm{LC}_{k'}(L(C_{i_1}))=\mathrm{LC}_{k'}(l_{2^t-h-2^{i_1}},l_{2^t-h-2^{i_1}+1},\cdots,l_{2^t-h-1})=(2^{i_1}-2)\times 2^n+2^{2^t-h-2}+1$，其中 $k'=2^{n-1}$。于是有

$$\begin{aligned}\mathrm{LC}_k(S)&=2^{t+n}-h\times 2^n-2^{i_1+n}+\mathrm{LC}_{k'}(L(C_{i_1}))\\&=(2^t-(h+1)-1)\times 2^n+2^{2^t-(h+1)-1}+1\end{aligned}$$

故当 $u=h+1$ 时，结论也成立。

综上(1), (2)所述，定理成立。 证毕

定理 2 给出了当输入规模 n=2^t 时，单圈 T 函数按位抽取输出序列 S 的第 1,2,…,n–1 下降点及对应的 k-错线性复杂度。进一步地，可给出 S 的第 n 下降点及其对应的 k-错线性复杂度。

定理 3 设 S 是单圈 T 函数按位输出序列，若输入规模 n=2^t，则序列 S 线性复杂度的第 n 下降点及 k-错线性复杂度为 $\mathrm{err}_n(S)=n\times 2^{n-1}$ 且 $\mathrm{LC}_k(S)=0$，其中 $k=\mathrm{err}_n(S)$。

证明 一方面，由定理 2 的证明过程可知，当 $\mathrm{err}_{n-1}(S)=(n-1)\times 2^{n-1}$ 且 $\mathrm{LC}_k(S)=2^{k_0}+1$，$k=\mathrm{err}_{n-1}(S)$ 时，$\mathrm{err}_n(S)=n\times 2^{n-1}$；另一方面，由于 $W(S)=n\times 2^{n-1}$，故 $\mathrm{LC}_k(S)=0$，其中 $k=\mathrm{err}_n(S)$。

故定理成立。 证毕

基于定理 2 和定理 3，可给出当输入规模 n=2^t 时，单圈 T 函数按位输出序列的 k-错线性复杂度分布。

定理 4 设 S 是单圈 T 函数按位输出序列，当输入规模 $n=2^t$ 时，序列 S 的 k-线性复杂度分布为

$$\mathrm{LC}_k(S)=\begin{cases}(n-1)\times 2^n+2^{n-1}+1, & 0\le k<2^{n-1}\\ (n-2)\times 2^n+2^{n-2}+1, & 2^{n-1}\le k<2\times 2^{n-1}\\ \quad\vdots & \\ (n-u-1)\times 2^n+2^{n-u-1}+1, & \\ \qquad\qquad u\times 2^{n-1}\le k<(u+1)\times 2^{n-1} & \\ \quad\vdots & \\ 2^0+1, & (n-1)\times 2^{n-1}\le k<n\times 2^{n-1}\\ 0, & k=n\times 2^{n-1}\end{cases}$$

定理 4 的证明可直接由 $\mathrm{LC}_k(S)$ 的定义，定理 2 和定理 3 得到，在此不再进行证明。

基于上述讨论可以得到当输入规模 n=2^t 时，单圈 T 函数按位输出序列的 k-错线性复杂曲线，如图 1 所示。

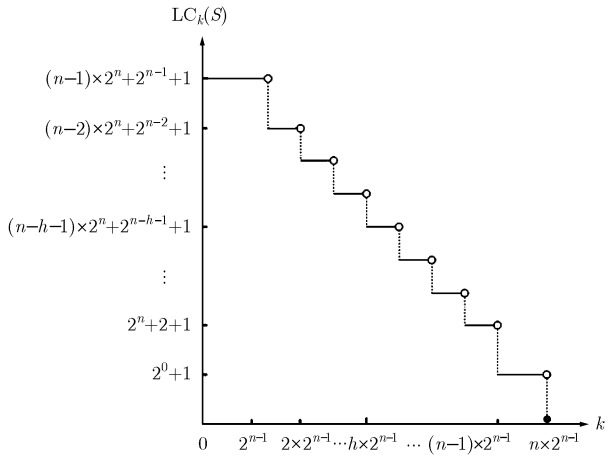

图 1 单圈 T 函数按位输出序列 k-错线性复杂度曲线

图 1 形象地描述了当输入规模 n=2^t 时，单圈 T 函数按位输出序列的 k-错线性复杂的变化情况，图中横坐标 k 表示序列 S 在一个周期内改变了 k 比特，纵坐标 $\mathrm{LC}_k(S)$ 表示序列 S 的 k-错线性复杂度取值。

4　结束语

本文分析了当输入规模 n=2^t 时单圈 T 函数按位输出序列的 k-错线性复杂度分布情况及 k-错线性复杂度曲线。对于单圈 T 函数按位输出序列来说，在输入规模为任意取值时，单圈 T 函数按位输出序列的 k-错线性复杂度的分布和 k-错线性复杂度曲线都是非常有意义的问题，值得进一步研究。

参 考 文 献

[1] Klimov A and Shamir A. A new class of invertible mappings . Workshop of CHES 2002, 2003, LNCS 2523: 470–483.

[2] Zhang W Y and Wu C K. The algebraic normal form, linearcomplexity and k-error linear complexity of single-cycle T-function. Proceedings of SETA 2006, 2006, LNCS 4086: 391–401.

[3] 赵璐, 温巧燕. 单圈T函数输出序列的线性复杂度及稳定性. 北京邮电大学学报, 2008, 31(4): 62–65.
Zhao Lu and Wen Qiao-yan. Linear complexity and stability of output sequences of single cycle T-function. *Journal of Beijing University of Posts and Telecommunications*, 2008, 31(4): 62–65.

[4] Cusick T, Ding C, and Renvall A. Stream Ciphers and Number Theory. North-Holland Elsevier, 1998: 1.

[5] Ding C, Xiao G, and Shan W. The Stability Theoery of Stream Ciphers. Springer Verlag Press, 1991, LNCS 561: 1.

[6] Kurosawa K and Sato F. A relationship between linear complexity and k-error linear complexity. *IEEE Transactions on Information Theory*, 2000, 46(2): 694–698.

[7] Games R A and Chan A H. A fast algorithm for determining the complexity of a binary sequence with period 2^n . *IEEE Transactions on Information Theory*, 1983, 29(4): 144–146.

[8] Massey J, Costeuo D, and Juotesen J. Polynomial weights and code constructions. *IEEE Transactions on Information Theory*, 1973, IT–19(1): 101–110.

[9] 周旋, 瞿成勤, 李斌. 单圈T函数输出序列性质研究. 电子技术学院学报, 2009, 21(6): 13–16.
Zhou Xuan, Qu Cheng-qin, and Li Bin. Research on properties of output sequences of single cycle T-function. *Journal of Institure of Electronic Technology*, 2009, 21(6): 13–16.

[10] 王菊香. 周期序列的k-错线性复杂度分析和研究.[硕士论文], 合肥工业大学, 2009.
Wang Ju-xiang. Analyse and research of the k-error linear complexity of periodic sequences. [Master dissertation], Hefei University of Technology, 2009.

[11] 郝年朋, 岳勤. 二元周期序列线性复杂度的2位置错误谱. 计算机工程, 2010, 36(02): 158–160.
Hao Nian-peng and Yue Qin. 2-position error spectrum of linear complexity for binary periodic sequence. *Computer Enginerring*, 2010, 36(2): 158–160.

[12] Xu Li-qing. On GF(P)-linear complexities of binary sequences. *The Journal of China Universities of Posts and Telecommunications*, 2009, 16(4): 112–115.

罗小建：　男，1985 年生，硕士生，研究方向为密码学与信息安全.
胡　斌：　男，1971 年生，博士，教授，硕士生导师，研究方向为密码学与信息安全.
郝珊珊：　女，1973 年生，在职研究生，讲师，研究方向为网络信息安全.
张　翀：　男，1985 年生，助教，研究方向为信息安全.