第33卷第7期　　电 子 与 信 息 学 报　　Vol.33No.7
2011年7月　　Journal of Electronics & Information Technology　　Jul. 2011

单圈 T 函数输出序列 k-错线性复杂度研究

罗小建*　　胡　斌
(解放军信息工程大学电子技术学院　郑州　450004)

摘　要：该文对单圈 T 函数输出序列的 k-错线性复杂度进行了深入研究，利用多项式理论和 Chan Games 算法，分析得到了当 $n=2^t$ 时，单圈 T 函数输出序列线性复杂度的 n 个下降点及其对应位置的 k-错线性复杂度，并给出了 k-错线性复杂度的分布和 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　　**文献标识码**：A　　**文章编号**：1009-5896(2011)07-1765-05
DOI: 10.3724/SP.J.1146.2010.00853

k-error Linear Complexity of Output Sequences of Single Cycle T-function

Luo Xiao-jian　　Hu Bin
(*Electronic Technology Institute*, *Information Engineering University*, *Zhengzhou* 450004, *China*)

Abstract: The k-error linear complexity of the output sequences of single cycle T-function is investigated with the polynomial theory and the Chan Games algorithm as the main tools. All of the linear complexity drop points and the k-error linear complexity on the drop position of the output sequences are given when $n=2^t$. The distribution of k-error linear complexity and k-error linear complexity profile of the output sequences of single cycle T-function are given.

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

1　引言

2002 年，文献[1]提出了 T 函数的概念，并对其进行了系列研究。T 函数是非线性的甚至是非代数的，并能在软件上快速实现，T 函数先后用于分组密码，Hash 函数和流密码的构造。

如果可逆 T 函数所决定的状态转移图的周期为 2^n，则称该 T 函数为单圈 T 函数。文献[1]提出用单圈 T 函数代替线性移位寄存器作为密钥发生器的驱动源的思想，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-错线性复杂度表征。

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，文献[2]给出了单圈 T 函数输出序列的线性复杂度和 k-错线性复杂度；2008 年，文献[3]得到了单圈 T 函数按位输出的序列的线性复杂度以及 k-错线性复杂度。本文对单圈 T 函数输出序列的 k-错线性复杂度进行了深入研究，利用多项式理论和 Chan Games 算法，在输入规模 $n=2^t$ 时，分析得到了单圈 T 函数输出序列的线性复杂度的所有下降点，及其相应位置的 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

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

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

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

2010-08-12 收到，2011-05-11 改回
*通信作者：罗小建　luojian1232@163.com

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：

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

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 $S(T)=(s_0\,|\,s_1\,|\cdots|\,s_{2^n-1}\cdots\cdots)$ 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 函数输出序列 k-错线性复杂度研究

下面研究当 $n=2^t$ 时，单圈 T 函数输出序列的 k-错线性复杂度的分布情况及 k-错线性复杂度曲线。首先给出几个引理。

引理 2[6] 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[7] 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 $\boldsymbol{d}=L(s^m)\oplus R(s^m)$，则当 $\boldsymbol{d}$ 为全零向量时，$\mathrm{LC}(S)=\mathrm{LC}(L(s^m))$，当 $\boldsymbol{d}$ 不为全零向量时，$\mathrm{LC}(S)=2^{m-1}+\mathrm{LC}(\boldsymbol{d})$。

由引理 3 可知，序列的周期越小，线性复杂度越小。

引理 4[8] 设 $k,t\in Z,\ k<2^t$，则 $(1+x)^{k-1}$ 的项数为 $2^{W(k-1)}$。

引理 5 设 S 是单圈 T 函数输出序列，记单圈 T 函数的第 i 分位序列为 a_i，a_i 改变若干比特后的序列记为 b_i，其周期为 $p(b_i)$，则对任意整数 j，$0\le j\le i$，可在 S 的每个周期内通过改变 a_i 的 2^{n-1} 个比特得到 b_i，使得 $p(b_i)=2^j$ 成立，其中 $0\le i\le n-1$。

证明 设单圈 T 函数输出序列为 $S=(a_{0,0},a_{0,1},\cdots,a_{0,n-1},a_{1,0},a_{1,1},\cdots,a_{1,n-1},\cdots,a_{2^n-1,0},a_{2^n-1,1},\cdots,a_{2^n-1,n-1},\cdots)$，显然 S 的周期 $p(S)=n\times 2^n$。设单圈 T 函数输出序列的第 i 分位序列 $a_i=(a_{0,i},a_{1,i},\cdots,a_{2^{i+1},i},\cdots)$，显然 S 的一个周期内第 i 分位序列的长度为 2^n，记为 $a_i^{(2^n)}$，由引理 1 知，$p(a_i^{(2^n)})=2^{i+1}$。

设 $b_i=(b_{0,i},b_{1,i},\cdots,b_{2^j-1,i},\cdots)$ 是周期为 2^j 的任一序列，$0\le j\le i$，并记 $b_i^{(t)}$ 表示 b_i 的前 t 个比特，下面证明将 $a_i^{(2^n)}$ 变成 $b_i^{(2^n)}$ 需要改变 2^{n-1} 个比特。

由于 $p(b_i)=2^j\,|\,2^i$，显然，$b_i^{(2^{i+1})}=(b_i^{(2^i)},b_i^{(2^i)})$。不妨设将 $(a_{0,i},a_{1,i},\cdots,a_{2^i-1,i})$ 变成 $b_i^{(2^i)}$ 需要改变 x 个比特，$0\le x\le 2^i$，即 $(a_{0,i},a_{1,i},\cdots,a_{2^i-1,i})$ 和 $b_i^{(2^i)}$ 有 x 个比特不同，2^i-x 个比特相同。再由引理 1 知，$a_{j,i}\oplus a_{j+2^i,i}=1$，因此，$(a_{2^i,i},a_{2^i+1,i},\cdots,a_{2^{i+1}-1,i})$ 和 $b_i^{(2^i)}$ 有 x 个比特相同，2^i-x 个比特不同，进而要将 $(a_{2^i,i},a_{2^i+1,i},\cdots,a_{2^{i+1}-1,i})$ 变成 $b_i^{(2^i)}$ 需要改变 2^i-x 个比特。因此，要将 $(a_{0,i},a_{1,i},\cdots,a_{2^{i+1},i})$ 变成 $b_i^{(2^{i+1})}$ 一共需要改变 $x+(2^i-x)=2^i$ 个比特。又因为 $p(a_i^{(2^n)})=2^{i+1}\,|\,2^n$，$a_i^{(2^n)}$ 由 2^{n-1-i} 个 $(a_{0,i},a_{1,i},\cdots,a_{2^{i+1},i})$ 组成，故将 $a_i^{(2^n)}$ 变成 $b_i^{(2^n)}$ 需要改变 $2^{n-1-i}\times 2^i=2^{n-1}$ 个比特。

证毕

由引理 5 及其证明过程可知，对任意满足 $j<i+1$ 的非负整数 j，在单圈 T 函数输出序列的一个周期内，改变分位序列 a_i 的 2^{n-1} 个比特，可使得改变后的序列 b_i 为周期整除 2^i 的任意序列。

定理 1 设 S 是单圈 T 函数输出序列，当 $n=2^t$ 时，对任意的整数 $u,1\le u\le n-1$，令 $k=u\times 2^{n-1}$，S 的 k-错线性复杂度为 $\mathrm{LC}_k(S)=n-u+n\times 2^{n-u-1}$。

证明 设单圈 T 函数输出序列为 $S=(a_{0,0},a_{0,1},\cdots,a_{0,n-1},a_{1,0},a_{1,1},\cdots,a_{1,n-1},\cdots,a_{2^n-1,0},a_{2^n-1,1},\cdots,a_{2^n-1,n-1},$

$\cdots$)，显然S的周期为$n\times 2^n$。

设$a_i=(a_{0,i},a_{1,i},\cdots,a_{2^n-1,i},\cdots)$为输出序列的第$i$分位序列，$0\le i\le n-1$。由引理3可知，要将序列$S$的线性复杂度降低，在$S$的一个周期内改变相同比特数的前提下，改变后序列的周期越小，其线性复杂度越小。进一步地，根据序列S的特性和引理5可知，当S在每个周期内改变$u\times 2^{n-1}$个比特时，其周期最小可以达到$n\times 2^{n-u}$，即将$a_{n-u},\cdots,a_{n-1}$这u个分位序列分别改变2^{n-1}个比特，使得改变后的分位序列周期整除2^{n-u}。

设$(1+x)^u=1+c_1x+\cdots+c_ux^u$，其中$c_1,\cdots,c_u\in Z_2$。对任意整数$i$ $(1\le i\le u)$，若$c_i=0$，将分位序列$a_{n-1-(u-i)}$在每周期内改变2^{n-1}个比特使其变成全零序列；若$c_i=1$，将$a_{n-1-(u-i)}$在每周期内改变2^{n-1}个比特使其变成a_{n-u-1}。

因此，根据c_i的取值，存在序列$b_{n-1-(u-i)}=(b_{0,n-1-(u-i)},b_{1,n-1-(u-i)},\cdots,b_{2^n-1,n-1-(u-i)},\cdots)$，满足周期为$2^n$且$W(b_{n-1-(u-i)})=2^{n-1}$，使得$a_{n-1-(u-i)}\oplus b_{n-1-(u-i)}=c_ia_{n-u-1},\ i=1,2,\cdots,u$。令错误序列为$\underline{e}=(0\cdots 0b_{0,n-u}\cdots\ b_{0,n-1},0\cdots 0b_{1,n-u}\cdots b_{1,n-1},\ \cdots,0\cdots 0\cdot b_{2^n-1,n-u}\cdots b_{2^n-1,n-1},\cdots)$，其中$(0\cdots 0b_{i,n-u}\cdots b_{i,n-1})$中含有$n$个比特，$i=0,1,\cdots,2^n-1$，则$W(\underline{e})=u\times 2^{(n-1)}$，$S\oplus\underline{e}$的周期为$n\times 2^{n-u}$。设$S\oplus\underline{e}$的形式化多项式为$s'(x)$，即

$$\begin{aligned}s'(x)=&a_{0,0}+a_{0,1}x+\cdots+a_{0,n-u-1}x^{n-u-1}+(a_{0,n-u}\\&\oplus b_{0,n-u})x^{n-u}+\cdots+(a_{0,n-1}\oplus b_{0,n-1})x^{n-1}\\&+x^n(a_{1,0}+a_{1,1}x+\cdots+a_{1,n-u-1}x^{n-u-1}\\&+(a_{1,n-u}\oplus b_{1,n-u})x^{n-u}+\cdots+(a_{1,n-1}\oplus b_{1,n-1})\\&\cdot x^{n-1})+\cdots+x^{(2^{n-u}-1)n}(\ (a_{2^{n-u}-1,0}+a_{2^{n-u}-1-1,1}x\\&+\cdots+a_{2^{n-u}-1-1,n-u-1}x^{n-u-1})+(a_{2^{n-u}-1,n-u}\\&\oplus b_{2^{n-u}-1,n-u})x^{n-u}+\cdots+(a_{2^{n-u}-1,n-1}\\&\oplus b_{2^{n-u}-1-1,n-1})x^{n-1}\ )\end{aligned}$$

由引理1知，当$0\le i<n-u-1,\ 0\le j\le 2^{n-u-1}-1$时，$a_{j,i}\oplus a_{j+2^{n-u-1},i}=0$且$a_{j,n-u-1}\oplus a_{j+2^{n-u-1},n-u-1}=1$，则

$$\begin{aligned}s'(x)=&(1+x^n)^{2^{n-u-1}}g(x)+x^{2^{n-u-1}}(1+x^n)^{2^{n-u-1}-1}\\&\cdot(1+c_1x+c_2x^2+\cdots+c_ux^u)\end{aligned}\qquad(4)$$

其中

$$\begin{aligned}g(x)=&a_{0,0}+a_{0,1}x+\cdots+a_{0,n-u-1}x^{n-u-1}+x^n(a_{1,0}\\&+a_{1,1}x+\cdots+a_{1,n-u-1}x^{n-u-1})+\cdots+x^{(2^{n-u-1}-1)n}\\&\cdot(a_{2^{n-u-1}-1,0}+a_{2^{n-u-1}-1,1}x+\cdots\\&+a_{2^{n-u-1}-1,n-u-1}x^{n-u-1})\end{aligned}$$

则

$$\begin{aligned}s'(x)=&(1+x^n)^{2^{n-u-1}-1}[(1+x^n)g(x)+x^{2^{n-u-1}}\\&\cdot(1+c_1x+c_2x^2+\cdots+c_ux^u)]\\=&(1+x)^{(2^{n-u-1}-1)n+u}[(1+x)^{n-u}g(x)+x^{2^{n-u-1}}]\end{aligned}$$

因此，$\gcd(1-x^{n\times 2^{n-u}},s'(x))=(1+x)^{(2^{n-u-1}-1)n+u}$。

进而有：$\mathrm{LC}(S\oplus\underline{e})=n\times 2^{n-u}-\deg(\gcd(1-x^{n\times 2^{n-u}},s'(x)))=n\times 2^{n-u-1}+n-u$。

由引理4可以保证$\deg(\gcd(1-x^{n\times 2^{n-u}},s'(x)))$的最大性，进而当改变$u\times 2^{n-1}$个比特时，序列的线性复杂度最小值为$n\times 2^{n-u-1}+n-u$，即$\mathrm{LC}_k(S)=n-u+n\times 2^{n-u-1}$，其中$k=u\times 2^{n-1}$。 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,$\cdots$，第$k$下降点的定义。显然$1\le\mathrm{err}_1(S)<\cdots<\mathrm{err}_k(S)<\cdots$且$\mathrm{LC}(S)>\mathrm{LC}_{\mathrm{err}_1(S)}(S)>\cdots>\mathrm{LC}_{\mathrm{err}_k(S)}(S)>\cdots$。

下面给出当$n=2^t$时，单圈T函数输出序列线性复杂度的第u下降点$\mathrm{err}_u(S)$及当$k=\mathrm{err}_u$时，$\mathrm{LC}_k(S)$取值。

定理2 设S是单圈T函数输出序列，当$n=2^t$时，对任意整数$u,1\le u\le n-1,$ S的线性复杂度的第u下降点$\mathrm{err}_u(S)=u\times 2^{n-1}$，且$\mathrm{LC}_k(S)=n-u+n\times 2^{n-u-1}$，其中$k=\mathrm{err}_u(S)$。

证明 当$u=1$时，$\mathrm{err}_1(S)=\min\mathrm{error}(S)=2^{W(n\times 2^{n-1}-n\times 2^{n-1}-n)}=2^{n-1}$，由引理5可知，$\mathrm{LC}_k(S)=n-1+n\times 2^{n-2}$，其中$k=\mathrm{err}_1(S)$，故此时结论成立；

假设当$u=h$时，$\mathrm{err}_h(S)=2^{h\times(n-1)}$且$\mathrm{LC}_k(S)=n-h+n\times 2^{n-h-1}$，其中$k=\mathrm{err}_h(S)$，由定义可知，存在错误序列$\underline{e}$满足周期为$n\times 2^n$且$W(\underline{e})=h\times 2^{n-1}$，使得$\mathrm{LC}(S\oplus\underline{e})=n-h+n\times 2^{n-h-1}$。

下面按照定理1中的证明过程构造满足条件的错误序列$\underline{e}$。设$(1+x)^h=1+c_1x+\cdots+c_hx^h$，其中$c_1,\cdots,c_h\in Z_2$，根据$c_i$的取值，存在序列$b_{n-1-(u-i)}=(b_{0,n-1-(u-i)},b_{1,n-1-(u-i)},\cdots,b_{2^n-1,n-1-(u-i)},\cdots)$满足$W(b_{m-1-(u-i)})=2^{n-1}$，使得$a_{n-1-(u-i)}\oplus b_{n-1-(u-i)}=c_ia_{n-u-1},\ i=1,2,\cdots,u$。

令$\underline{e}=(0\cdots 0b_{0,n-u}\cdots b_{0,n-1},0\cdots 0b_{1,n-u}\cdots b_{1,n-1},\cdots,0\cdots 0b_{2^n-1,n-u}\cdots b_{2^n-1,n-1},\cdots)$，其中$(0\cdots 0b_{i,n-u}\cdots b_{i,n-1})$中一共含有$n$个比特，$0\le i\le 2^n-1$，错误序列$\underline{e}$使得$S$的$h$个分位序列$a_{n-1},\cdots,a_{n-h}$在每周期内分别改

变了 2^{n-1} 个比特，使得这 h 个分位序列都变成了周期整除 2^{n-h} 的序列，则 $S\oplus \underline{e}$ 的周期为 $n\times 2^{n-h}$，且由定理 1 知，$\mathrm{LC}(S\oplus \underline{e})=n-h+n\times 2^{n-h-1}$。

由定理 1 可知，影响 $\mathrm{LC}(S\oplus \underline{e})$ 取值的是周期为 2^{n-h} 的分位序列，这些分位序列都由 $c_i=1$ 决定，即由 $(1+x)^h$ 的非零系数所决定。由引理 4 可知，$(1+x)^h$ 的项数为 $2^{W(h)}$，即 $\#\{c_i=1\mid i=1,2,\cdots,h\}=2^{W(h)}-1$，这就说明错误序列 $\underline{e}$ 将 $a_{n-1},\cdots,a_{n-h}$ 中的 $2^{W(h)}-1$ 个分位序列变成 a_{n-h-1}，不妨设这 $2^{W(h)}-1$ 个分位序列为 $a_{n-i_1},a_{n-i_2},\cdots,a_{n-i_{2^{W(h)}-1}}$，$1\le i_1<i_2<\cdots<i_{2^{W(h)}-1}\le h$；还将 $\{a_{n-1},\cdots,a_{n-h}\}-\{a_{n-i_1},a_{n-i_2},\cdots,a_{n-i_{2^{W(h)}-1}}\}$ 这 $h-2^{W(h)}+1$ 个分位序列变成全零序列。

因此，当 $u=h+1$ 时，要使得 $\mathrm{LC}_k(S)<n-h+n\times 2^{n-h-1}$，需将 S 中的 $a_{n-i_1},a_{n-i_2},\cdots,a_{n-i_{2^{W(h)}-1}}$，$a_{n-h-1}$ 这 $2^{W(h)}$ 个分位序列在每个周期内分别改变 2^{n-1} 个比特使得其变成周期整除 2^{n-h-1} 的序列，另外还需将 $\{a_{n-1},\cdots,a_{n-h}\}-\{a_{n-i_1},a_{n-i_2},\cdots,a_{n-i_{2^{W(h)}-1}}\}$ 这 $h-2^{W(h)}+1$ 个分位序列变成全零序列。因此，当 $u=h+1$ 时，需要在 S 的每个周期内改变 $(2^{W(h)}+h-2^{W(h)}+1)\times 2^{n-1}=(h+1)\times 2^{n-1}$ 个比特使得 S 改变后的序列线性复杂度小于 $n-h+n\times 2^{n-h-1}$。故当 $u=h+1$ 时，$\mathrm{err}_{h+1}(S)=2^{(h+1)\times(n-1)}$，由定理 1 可知，$\mathrm{LC}_k(S)=n-h-1+n\times 2^{n-h-2}$，其中 $k=\mathrm{err}_{h+1}(S)$； 证毕

推论 设 S 是单圈 T 函数状态输出序列，当 $n=2^t$ 时，S 的线性复杂度的第 n 下降点为 $\mathrm{err}_n(S)=u\times 2^{n-1}$，且 $\mathrm{LC}_k(S)=0$，其中 $k=\mathrm{err}_n(S)$。

证明 从定理 2 的证明过程中 $u=h$ 到 $u=h+1$ 的推导过程可知，当 $\mathrm{err}_{n-1}(S)=(n-1)\times 2^{n-1}$，且 $\mathrm{LC}_k(S)=1+n\times 2^{k_0}$，其中 $k=\mathrm{err}_{n-1}(S)$ 时，$\mathrm{err}_n(S)=n\times 2^{n-1}$。又由于 $W(S)=n\times 2^{n-1}$，故当序列 S 改变 $n\times 2^{n-1}$ 个比特时，$\mathrm{LC}_k(S)=0$，其中 $k=\mathrm{err}_n(S)$。 证毕

由定理 2 及其推论，定理 3 将给出 $n=2^t$ 时，单圈 T 函数输出序列 k-错线性复杂度的分布情况。

定理 3 设 S 是单圈 T 函数状态输出序列，当 $n=2^t$ 时，序列 S 的 k-错线性复杂度分布如下：

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

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

基于上述讨论，可以得到当 $n=2^t$ 时，单圈 T 函数输出序列的 k-错线性复杂曲线，如图 1 所示：

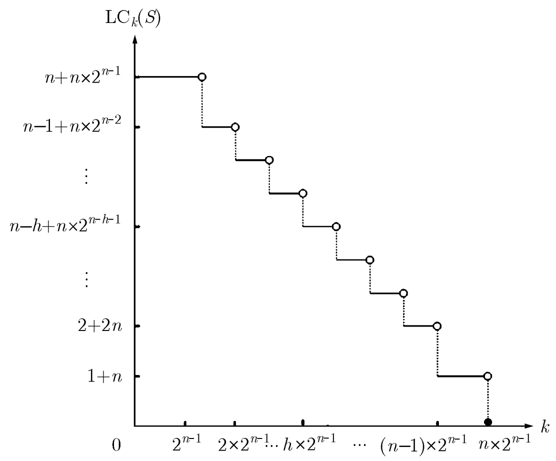

图 1 单圈 T 函数输出序列 k-错线性复杂度曲线

图 1 形象地描述了当 $n=2^t$ 时，单圈 T 函数输出序列的 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 个比特，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 $n=2^t$ 时，单圈 T 函数输出序列的 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 函数输出序列来说，在输入规模为任意取值时，单圈 T 函数输出序列的 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, Springer Verlag, 2003, LNCS 2523: 470–483.

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

[5] Ding C, Xiao G, and Shan W. The stability theoery of stream ciphers. Springer-Verlag, Heidelberg, LNCS 561, 1991: 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(2): 158–160.
Hao Nian-peng and Yue Qin. 2-position error spectrum of linear complexity for binary periodic sequence. *Computer Engineering*, 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，副教授，硕士生导师，研究方向为密码学与信息安全.