2^n-周期二元序列的 3-错误序列分布

周建钦*①② 刘 军①
①(杭州电子科技大学通信工程学院 杭州 310018)
②(安徽工业大学计算机学院 马鞍山 243032)

摘 要：线性复杂度和 k- 错线性复杂度是度量密钥流序列密码强度的重要指标。为了更好地研究序列的随机性，该文通过将序列的 k- 错线性复杂度的计算转化为求 Hamming 重量最小的错误序列的方法，讨论了序列不同 k- 错线性复杂度条件下对应的 k- 错误序列的分布情况。基于 Games-Chan 算法，该文给出了线性复杂度为 2^n 的 2^n -周期二元序列的 3 错误序列的计数公式，计算机编程验证了该文方法的正确性。

关键词：序列密码；线性复杂度；k- 错线性复杂度；k- 错误序列
中图分类号：TN918.1 **文献标识码**：A **文章编号**：1009-5896(2012)08-1923-05
DOI: 10.3724/SP.J.1146.2011.01315

On the 3 error Sequence Distribution of 2^n- periodic Binary Sequences

Zhou Jian-qin①② Liu Jun①
①(*Telecommunication School*, *Hangzhou Dianzi University*, *Hangzhou* 310018, *China*)
②(*Computer Science School*, *Anhui University of Technology*, *Ma'anshan* 243032, *China*)

Abstract: The linear complexity and the k- error linear complexity of a sequence are used as important measures of keystream strength. By studying linear complexity of binary sequences with period 2^n, it is proposed that the computation of k- error linear complexity can be converted to finding error sequences with minimal Hamming weight. In order to study sequence randomness, the k- error sequences distribution that corresponds with the k- error linear complexity of sequence is discussed. Based on Games-Chan algorithm, for $k=3$, the counting functions on the k- error sequences of 2^n- periodic binary sequences with linear complexity 2^n- are derived and the effectiveness is proved with computer programming.

Key words: Stream cipher; Linear complexity; k- error linear complexity; k- error sequences

1 引言

为了抵抗 Berlekamp-Massey(B-M)算法的攻击，作为密钥流序列的密码强度的重要指标，序列的线性复杂度和 k- 错线性复杂度都应该保证要足够大。因为仅考虑序列具有较高线性复杂度是不够的，还希望在改变序列少量的比特时，其线性复杂度不会急剧下降。为此，文献[1]提出了序列的稳定性理论及序列的球形复杂度，随后文献[2]也引入了类似‘球体复杂度’的线性复杂度稳定性度量指标：k- 错线性复杂度。文献[3]给出 2^n- 周期二元序列 s 的 k- 错线性复杂度严格小于线性复杂度 $L(s)$ 的最小值为：$k_{\min}=2^{W_H(2^n-L(s))}$，其中 $W_H(b)$ 表示整数 b 在二进制表示下的 Hamming 重量。文献[4]给出有限域 F_q 上 $2p^n$- 周期序列的 k-错线性复杂度严格小于其线性复杂度的最小 k- 值；文献[5]给出有限域 F_q 上 $q^m p^n$- 周期序列的 k- 错线性复杂度严格小于其线性复杂度的最小 k- 值的上下界。

文献[3]提出了错误序列的概念，文献[6]在此基础上引出了 k- 错误序列，认为一条安全性强的序列不仅要有较高的线性复杂度和 k- 错线性复杂度，而且对数值较小的 k- 值，还要有较少的 k-错误序列，并给出了相应的 k- 错误序列 $(k=1,2)$ 的计数公式。本文根据文献[7]提出的将 k- 错线性复杂度的计算转化为求 Hamming 重量最小的错误序列的方法，对 $k=3$，基于 Games-Chan 算法，给出了线性复杂度为 2^n 的 2^n- 周期二元序列的 k- 错误序列的计数公式 $M_k(s)$。同时给出若干实例，并通过计算机编程进行验证。

2 预备知识与引理

设周期为 N 的二元序列 s，s^N 是它的第一周

2011-12-12 收到，2012-04-20 改回
浙江省自然科学基金(Y1100318)和安徽省自然科学基金(1208085MF106)资助课题
*通信作者：周建钦 zhou9@yahoo.com

期， $s^N=\{s_0,s_1,s_2,\cdots,s_{N-1}\}$，其生成函数定义为 $s^N(x)=s_0+s_1x+s_2x^2+\cdots+s_{N-1}x^{N-1}$。则序列 s 的生成函数 $s(x)$ 可以表示为

$$s(x)=s^N(x)\left(1+x^N+x^{2N}+\cdots\right)=\frac{s^N(x)}{1-x^N}$$
$$=\frac{s^N(x)\Big/\gcd\left(s^N(x),1-x^N\right)}{1-x^N\Big/\gcd\left(s^N(x),1-x^N\right)}=\frac{g_s(x)}{f_s(x)} \quad (1)$$

显然，$\gcd(g_s(x),f_s(x))=1$，$f_s(x)$ 是 $s^{(n)}$ 的极小多项式，且 $f_s(x)$ 的次数是序列 $s^{(n)}$ 的线性复杂度，记作 $\mathrm{LC}(s)$。

定义 1[2] 设 $s=(s_0,s_1,\cdots,s_{N-1})^N$ 是 N- 周期序列，其 k-错线性复杂度 $\mathrm{LC}_k(s)$ 定义为

$$\mathrm{LC}_k(s)=\min_{W_H(e)\le k}\mathrm{LC}(s+e) \quad (2)$$

其中 $e=(e_0,e_1,\cdots,e_{N-1})^N$，$W_H(e)$ 表示序列 e 在一个周期 N 内的 Hamming 重量。

随后，文献[3]提出了错误序列的概念，文献[6]认为错误序列的多少与密钥序列的安全强度有很大的关系，故在此基础上给出了 k-错误序列的定义。

定义 2[6] 设 N- 周期序列 s 的 k-错线性复杂度为 $\mathrm{LC}_k(s)$，若 N- 周期序列 e 满足 $\mathrm{LC}(s+e)=\mathrm{LC}_k(s)$ 且 $1\le W_H(e)\le k$，则称 e 为 s 的 k-错误序列。记序列 s 的 k-错误序列 e 的总数为 $M_k(s)$。

本文以下将 2^n- 周期二元序列 s 表示成 $s^{(n)}$。下面给出了 10 个引理，引理 1，引理 2，引理 3 可参考文献[7]。

引理 1 设 $N=2^n$ 的周期二元序列 $s^{(n)}$，其线性复杂度 $\mathrm{LC}(s^{(n)})=2^n$，当且仅当该序列的一个周期的 Hamming 重量为奇数。

引理 2 设 $N=2^n$ 的周期二元序列 $s_1^{(n)}$ 和 $s_2^{(n)}$。如果 $\mathrm{LC}(s_1^{(n)})\ne\mathrm{LC}(s_2^{(n)})$，则有 $\mathrm{LC}(s_1^{(n)}+s_2^{(n)})=\max\{\mathrm{LC}(s_1^{(n)}),\mathrm{LC}(s_2^{(n)})\}$，如果 $\mathrm{LC}(s_1^{(n)})=\mathrm{LC}(s_2^{(n)})$，则有 $\mathrm{LC}(s_1^{(n)}+s_2^{(n)})<\mathrm{LC}(s_1^{(n)})$。

引理 3 设 E_i 是周期为 $N=2^n$ 的二元序列，它的第一周期只在第 i 位置元素是 1，其他位置元素全为 $0,0\le i<N$。若 $j-i=2^r(1+2a),\ a\ge 0$，$0\le i<j<N$，$r\ge 0$，则 $\mathrm{LC}(E_i+E_j)=2^n-2^r$。

引理 4[3] 设 $s^{(n)}$ 是周期为 $N=2^n$ 的二元序列，则 $\mathrm{merr}(s^{(n)})=2^{W_H(2^n-\mathrm{LC}(s^{(n)}))}$，其中 $\mathrm{merr}(s^{(n)})$ 为满足不等式 $\mathrm{LC}_k(s^{(n)})<\mathrm{LC}(s^{(n)})$ 的最小正整数 k，$W_H(a)$ 是整数 a 的二进制表示中的 Hamming 重量。

3 2^n- 周期序列的 3-错误序列

对于 2^n- 周期二元序列 $s^{(n)}$，当 $\mathrm{LC}(s^{(n)})<2^n$，文献[6]已给出 $M_2(s^{(n)})$ 的计算公式。通过引理 1 可知，$W_H(s^{(n)})$ 为偶数，$\mathrm{LC}_3(s^{(n)})=\mathrm{LC}_2(s^{(n)})$，即有 $M_3(s^{(n)})=M_2(s^{(n)})$。下面将给出 $\mathrm{LC}(s^{(n)})=2^n$ 时的 $s^{(n)}$ 的 3-错误序列个数的计数公式 $M_3(s^{(n)})$。

引理 5[8] 设 $s^{(n)}=\{s_0,s_1,s_2,\cdots,s_{2^n-1}\}$ 是二元序列 s 的第一周期，$n\ge 1$，根据 Games-Chan 算法，定义映射 φ_n 从 $F_2^{2^n}$ 到 $F_2^{2^{n-1}}$，$\varphi_n(s^{(n)})=\varphi_n(s_0^{(n)},s_1^{(n)},\cdots,s_{2^n-1}^{(n)})=(s_0^{(n)}+s_{2^{n-1}}^{(n)},s_1^{(n)}+s_{2^{n-1}+1}^{(n)},\cdots,s_{2^{n-1}-1}^{(n)}+s_{2^n-1}^{(n)})$。

那么，映射 φ_n 满足下面的性质：

(1) $W_H\left(\varphi_n\left(s^{(n)}\right)\right)\le W_H\left(s^{(n)}\right)$；

(2) $W_H\left(\varphi_n\left(s^{(n)}\right)\right),W_H\left(s^{(n)}\right)$ 的奇偶性相同；

(3) 集合 $\varphi_{n+1}^{-1}\left(s^{(n)}\right)=\left\{v\in F_2^{2^{n+1}}\mid\varphi_{n+1}(v)=s^{(n)}\right\}$ 的大小为 2^{2^n}。

引理 6 设 $s^{(n)}$ 是 2^n- 周期二元序列，且 $\mathrm{LC}(s^{(n)})=2^n,n\ge 4$，则 $\mathrm{LC}_3(s^{(n)})$ 为 $0,2^n-7$ 或者 $2^n-2^{r+1}+c,\ 3\le r\le n-1,\ 1\le c\le 2^r-1$。

证明 若 $W_H(s^{(n)})=1$ 或 3，则 $\mathrm{LC}_3(s^{(n)})=0$。

若 $W_H(s^{(n)})>3$，根据引理 5，每步对折后，$W_H(s^{(k)})$ 都是奇数，$0\le k\le n-1$。

(1) 如果在第 $(n-t)$ 步后 $W_H(s^{(t)})=3$，$2\le t\le n-1$，则一定存在一个正整数 $r,\ t\le r\le n-1$，使得 $W_H(s^{(r)})=3$，$W_H(s^{(r+1)})>3$。根据 Games-Chan 算法，通过改变 $s^{(r+1)}$ 中的 3 bit 而得到的新 $s^{(r+1)}$ 满足 $\mathrm{Left}(s^{(r+1)})=\mathrm{Right}(s^{(r+1)}),\ \mathrm{LC}(s^{(r+1)})=\mathrm{LC}(\mathrm{Left}\cdot(s^{(r+1)}))=c$，故 $\mathrm{LC}_3(s^{(n)})=2^n-2^{r+1}+c$，$1\le c\le 2^r-1$。而 $r=2$ 时，c 只能取 1。例如 $s^{(3)}=(1110\ 1001)$，错误序列 $e^{(3)}$ 只能是 $(0001\ 0110)$。

(2) 如果在第 $(n-t)$ 步后不存在 $W_H(s^{(t)})=3$，$2\le t\le n-1$，但一定存在 $W_H(s^{(t)})=1$，$W_H(s^{(t+1)})=2a+1,a\ge 2$，即存在一正整数 $r,t\le r\le n-1$，使得 $W_H(s^{(r)})=1$。

(a)若此时改变原 $s^{(r+1)}$ 的 1 bit，而使得所得到的新 $s^{(r+1)}$ 的线性复杂度等于 2^r-2^m，根据引理 4，对原 $s^{(r+1)}$，$\mathrm{merr}(s^{(r+1)})=4$，此时可改变 3 bit 而使得所得到的新 $s^{(r+1)}$ 满足 $\mathrm{LC}(s^{(r+1)})<2^r-2^m$。故有 $\mathrm{LC}_3(s^{(n)})=2^n-2^{r+1}+\mathrm{LC}_3(s^{(r+1)})=2^n-2^{r+1}+c,\ c\ne 2^r-2^m,\ 1\le c\le 2^r-3$。在 $r=2$ 时，c 只能为 1。例如 $s^{(3)}=(1010\ 1110)$，则 $e^{(3)}=(0101\ 0001)$。

(b)若改变原 $s^{(r+1)}$ 的 1 bit 而得到的新 $s^{(r+1)}$ 满足 $\mathrm{Left}(s^{(r+1)})=\mathrm{Right}(s^{(r+1)})$，且 $\mathrm{LC}(s^{(r+1)})=\mathrm{LC}(\mathrm{Left}\cdot(s^{(r+1)}))=c\ne 2^r-2^m$。根据引理 4，无法通过改变 3 bit 而使得新 $s^{(r+1)}$ 的线性复杂度小于 c，故 $\mathrm{LC}_3(s^{(n)})=2^n-2^{r+1}+\mathrm{LC}_1(s^{(r+1)})=2^n-2^{r+1}+c,\ 1\le c\le 2^r-3,c\ne 2^r-2^m,\ 0\le m\le r-1$。同样，在 $r=2$ 时，$c=1$。例如 $s^{(3)}=(1111\ 0111)$，则

$e^{(3)}=(0000\ 1000)$。　　证毕

引理 7　设 $s^{(n)}$ 是 2^n-周期二元序列，且 $\mathrm{LC}(s^{(n)})=2^n, \mathrm{LC}_3(s^{(n)})=c, 1\le c\le 2^{n-2}$，则 $M_3(s^{(n)})=1$。

证明　设有两个不同的序列 $p^{(n)}$ 和 $q^{(n)}$，且 $\mathrm{LC}(p^{(n)})=\mathrm{LC}(q^{(n)})=c, 1\le c\le 2^{n-2}$，另设两个不同的二元序列 $u^{(n)}$ 和 $v^{(n)}$, $W_H(u^{(n)})=1$ 或 3, $W_H(v^{(n)})=1$ 或 3。

假设 $p^{(n)}+u^{(n)}$ 和 $q^{(n)}+v^{(n)}$ 是相同的，也即 $p^{(n)}+q^{(n)}$ 与 $u^{(n)}+v^{(n)}$ 相同。根据引理 2, $\mathrm{LC}(p^{(n)}+q^{(n)})<c\le 2^{n-2}$。根据 Games-Chan 算法，则 $p^{(n)}+q^{(n)}$ 和 $u^{(n)}+v^{(n)}$ 均呈 4 等分分布。故只能取 $W_H(u^{(n)}+v^{(n)})=4, \mathrm{LC}(u^{(n)}+v^{(n)})=2^{n-2}$，与 $\mathrm{LC}(p^{(n)}+q^{(n)})<2^{n-2}$ 矛盾，故 $p^{(n)}+u^{(n)}\ne q^{(n)}+v^{(n)}$。所以，线性复杂度为 2^n 的序列 $s^{(n)}=p^{(n)}+u^{(n)}$，它的 3-错误序列只有 $u^{(n)}$ 本身，即 $M_3(s^{(n)})=1$。　　证毕

通过计算机编程进行了验证，取 $n=4$，对所有 $\mathrm{LC}(s^{(n)})=2^n$, $\mathrm{LC}_3(s^{(n)})=c, 1\le c\le 4$ 的序列 $s^{(n)}$, $M_3(s^{(n)})=1$。如 $\mathrm{LC}_3(s^{(n)})=4$ 的 $s^{(n)}=(1001\ 0111\ 0001\ 0001)$，其 3-错误序列是 $e^{(4)}=(1000\ 0110\ 0000\ 0000)$。

引理 8　设 $s^{(n)}$ 是 2^n-周期二元序列，$\mathrm{LC}(s^{(n)})=2^n$, $\mathrm{LC}_3(s^{(n)})=2^{n-1}-2^m+x$, $n\ge 4$, $2\le m\le n-2$, $0<x<2^{m-1}$，则 $M_3(s^{(n)})=1, 2, 4$ 或 2^{n-m-1}。

证明　令 $s^{(n)}=p^{(n)}+u^{(n)}$，其中 $\mathrm{LC}(p^{(n)})=2^{n-1}-2^m+x$, $2\le m\le n-2$, $0<x<2^{m-1}$。$\mathrm{LC}(u^{(n)})=2^n$，且 $W_H(u^{(n)})=1$ 或 3。根据引理 4，若要使得 $\mathrm{LC}_3(p^{(n)})<\mathrm{LC}(p^{(n)})$，需满足 $\mathrm{merr}(s^{(n)})\ge 8$。故有 $\mathrm{LC}_3(s^{(n)})=\mathrm{LC}_3(p^{(n)}+u^{(n)})=\mathrm{LC}(s^{(n)})=2^{n-1}-2^m+x$。

(1)当 $W_H(u^{(n)})=1$ 时，存在序列 $v^{(n)}$，$W_H(v^{(n)})=3$，且 $\mathrm{LC}(u^{(n)}+v^{(n)})=2^{n-1}-2^r, m\le r\le n-2$，这样的 $v^{(n)}$ 有 $2^{n-1}/2^m-1=2^{n-m-1}-1$ 个(即保证 $u^{(n)}+v^{(n)}$ 的半个周期中的两非零元素之间的距离是 2^m 的整数倍)，或者 $v^{(n)}=u^{(n)}$，从而使得 $\mathrm{LC}_3(p^{(n)}+u^{(n)})=\mathrm{LC}(p^{(n)})$。故 $M_3(s^{(n)})=2^{n-m-1}$。

(2)当 $W_H(u^{(n)})=3$ 时，先将 $u^{(n)}$ 分成 2^m 个子序列，子序列中的每个元素之间的位置满足：$\{i, i+2^m, \cdots, i+(2^{n-m}-2)\cdot 2^m, i+(2^{n-m}-1)\cdot 2^m | 0\le i\le 2^m-1\}$。

(a)若 $u^{(n)}$ 中的 3 个非零元素属于同一子序列，且有 2 个非零元素之间的距离为 2^{n-1}，存在 $1+(2^{n-1}/2^m-2)=2^{n-m-1}-1$ 个不同的 $v_i^{(n)}$，$1\le i\le 2^{n-m-1}-1, W_H(v_i^{(n)})=1$ 或 3，使得 $\mathrm{LC}(u^{(n)}+v_i^{(n)})=2^{n-1}-2^r$，$m\le r\le n-2$；或者 $v^{(n)}=u^{(n)}$。故 $M_3(s^{(n)})=2^{n-m-1}$。

若 $u^{(n)}$ 中的 3 个非零元素属于同一子序列，但不存在 2 个非零元素之间的距离为 2^{n-1}，则存在 3 个不同的序列 $v_i^{(n)}, 1\le i\le 3$，$W_H(v_i^{(n)})=3$，使得 $\mathrm{LC}(u^{(n)}+v_i^{(n)})=2^{n-1}-2^r$，$m\le r\le n-2$；或者 $v^{(n)}=u^{(n)}$。故 $M_3(s^{(n)})=4$。

(b)若 $u^{(n)}$ 中只有 2 个非零元素属于同一子序列，且它们之间的距离为 2^{n-1}，则存在 $2^{n-m-1}-1$ 个不同的 $v_i^{(n)}, W_H(v_i^{(n)})=3, 1\le i\le 2^{n-m-1}-1$，使得 $\mathrm{LC}(u^{(n)}+v_i^{(n)})=2^{n-1}-2^r$，$m\le r\le n-2$；或者 $v^{(n)}=u^{(n)}$。故 $M_3(s^{(n)})=2^{n-m-1}$。

此时，若不存在 2 个非零元素之间的距离为 2^{n-1}，则恰好存在 1 个序列 $v^{(n)}, W_H(v^{(n)})=3$，使得 $\mathrm{LC}(u^{(n)}+v^{(n)})=2^{n-1}-2^r$，$m\le r\le n-2$；或者 $v^{(n)}=u^{(n)}$。故 $M_3(s^{(n)})=2$。

(c)若 3 个非零元素分别属于 3 个不同的子序列，则不存在序列 $v^{(n)}, W_H(v^{(n)})=1$ 或 3，使得 $\mathrm{LC}(u^{(n)}+v^{(n)})=2^{n-1}-2^r, m\le r\le n-2$，即只能 $v^{(n)}=u^{(n)}$，故 $M_3(s^{(n)})=1$。　　证毕

经验证，取 $n=4, m=2$ 时，对所有 $\mathrm{LC}(s^{(n)})=2^n, \mathrm{LC}_3(s^{(n)})=5$ 的序列 $s^{(n)}$，它的 3-错误序列为 1 或 2 个。如 $s^{(n)}=(0000\ 0010\ 1000\ 0111)$，其 3-错误序列有 $e^{(4)}=(1000\ 0101\ 0000\ 0000)$；再如 $s^{(n)}=(0000\ 0011\ 0100\ 0011)$，其 3-错误序列 $e^{(4)}$ 有 $(0100\ 1000\ 0000\ 1000)$ 和 $(1100\ 0000\ 1000\ 0000)$。

引理 9　设 $s^{(n)}$ 是 2^n-周期二元序列，$\mathrm{LC}(s^{(n)})=2^n, \mathrm{LC}_3(s^{(n)})=2^{n-1}-2^m, n\ge 4, 0\le m\le n-3$，则 $M_3(s^{(n)})=1, 2$ 或 4。

证明　令 $s^{(n)}=p^{(n)}+u^{(n)}$，其中 $\mathrm{LC}(p^{(n)})=2^{n-1}-2^m$，根据引理 4，对所有 $W_H(u^{(n)})=1$ 序列 $u^{(n)}$，均有 $\mathrm{LC}_3(s^{(n)})=\mathrm{LC}_3(p^{(n)}+u^{(n)})<2^{n-1}-2^m$。

对 $W_H(u^{(n)})=3$ 的序列 $u^{(n)}$，先将 $u^{(n)}$ 分成 2^m 个子序列，子序列中的每个元素之间的位置满足：$\{i, i+2^m, \cdots, i+(2^{n-m}-2)\cdot 2^m, i+(2^{n-m}-1)\cdot 2^m | 0\le i\le 2^m-1\}$。

(1)若 $u^{(n)}$ 中只有 2 个非零元素属于同一子序列，且不存在 2 个非零元素之间的距离为 $2^m(1+2a)$, $a\ge 0$ 或 2^{n-1}，则存在 1 个序列 $v^{(n)}, W_H(v^{(n)})=3$，使得 $\mathrm{LC}(u^{(n)}+v^{(n)})=2^{n-1}-2^r, m+1\le r\le n-2$。根据引理 2, $\mathrm{LC}_3(s^{(n)})=2^{n-1}-2^m$；或者 $v^{(n)}=u^{(n)}$。故 $M_3(s^{(n)})=2$。

(2)若 $u^{(n)}$ 中 3 个非零元素同属于一个子序列，但不存在两个非零元素之间的距离为 $2^m(1+2a)$, $a\ge 0$ 或 2^{n-1}，则存在 3 个 $W_H(v^{(n)})=3$ 的不同 $v^{(n)}$，使得 $\mathrm{LC}(u^{(n)}+v^{(n)})=2^{n-1}-2^r, m+1\le r\le n-2$，即 $\mathrm{LC}_3(s^{(n)})=2^{n-1}-2^m$；或者 $v^{(n)}=u^{(n)}$。故 $M_3(s^{(n)})=4$。

(3)若 $u^{(n)}$ 中 3 个非零元素分别属于 3 个不同的子序列，则不存在一个不同于 $u^{(n)}$ 的序列 $v^{(n)}$，$W_H(v^{(n)})=1$ 或 3，使得 $\mathrm{LC}_3(s^{(n)})=\mathrm{LC}_3(p^{(n)}+u^{(n)})=2^{n-1}-2^m$。此时 $s^{(n)}=p^{(n)}+u^{(n)}$ 的 3-错误序列即为 $u^{(n)}$，故有 $M_3(s^{(n)})=1$。 证毕

经验证，当 $n=4$ 时，对所有 $\mathrm{LC}(s^{(n)})=2^n$，$\mathrm{LC}_3(s^{(n)})=6$ 的序列 $s^{(n)}$，$M_3(s^{(n)})=2$，如 $s^{(n)}=(0000\ 0110\ 0011\ 0111)$，$e^{(4)}$ 分别是 (0010 0001 0001 0000) 和 (0011 0000 0000 0001)；对 $\mathrm{LC}_3(s^{(n)})=7$ 的所有序列 $s^{(n)}$，其 3-错误序列有 4 个。

引理 7，引理 8，引理 9 都是引理 5 中 $r=n-1$ 的情况，接下来讨论 r 的一般情况。

引理 10 设 $n\ge 4$，$\mathrm{LC}(r,c)=2^n-2^3+1$ 或 $2^n-2^{r+1}+c$, $3\le r\le n-2$,$1\le c\le 2^r-1$。$M_3(s^{(n)})$ 表示周期为 2^n，线性复杂度为 2^n 的序列 $s^{(n)}$，其 3-错线性复杂度为 $\mathrm{LC}(r,c)$ 的 3-错误序列的个数，则

$$M_3\left(s^{(n)}\right)=\begin{cases}2^{n-r-1}\left(2^{2n-r-3}-2^{2n-2r-4}+1\right)\\ \quad \text{其中 } \mathrm{LC}_3\left(s^{(n)}\right)=2^n-2^{r+1}+c,\ 2\le r\le n-2,\ 1\le c\le 2^{r-1},\ W_H\left(e^{(n)}\right)=1 \text{ 或 } 3\\ 2^{3n-3r-3}\\ \quad \text{其中 } \mathrm{LC}_3\left(s^{(n)}\right)=2^n-2^{r+1}+c,\ 2\le r\le n-2,\ 1\le c\le 2^{r-1},\ W_H\left(e^{(n)}\right)=3\\ 2^{n-r-1}+2^{3n-2r-4}+2^{3n-2r-m-3}-5\times 2^{3n-3r-5}\\ \quad \text{其中 } \mathrm{LC}_3\left(s^{(n)}\right)=2^n-2^r-2^m+c,\ 2\le m\le r-1,\ 0<c<2^{m-1},\ W_H\left(e^{(n)}\right)=1 \text{ 或 } 3\\ 2^{3n-3r-3},\ 2^{3n-3r-2},\ 2^{3n-3r-1} \text{ 或 } 2^{3n-2r-m-3}\\ \quad \text{其中 } \mathrm{LC}_3\left(s^{(n)}\right)=2^n-2^r-2^m+c,\ 2\le m\le r-1,\ 0<c<2^{m-1},\ W_H\left(e^{(n)}\right)=3\\ 2^{3n-3r-3},\ 2^{3n-3r-2} \text{ 或 } 2^{3n-3r-1}\\ \quad \text{其中 } \mathrm{LC}_3\left(s^{(n)}\right)=2^n-2^r-2^m,\ 0\le m\le r-2,\ W_H\left(e^{(n)}\right)=3\end{cases}$$

其中 $W_H(e^{(n)})$ 表示序列 $s^{(n)}$ 的 3-错误序列 $e^{(n)}$ 的汉明重量。

证明 对于一般形式 $\mathrm{LC}_3(s^{(n)})=2^n-2^{r+1}+c$，根据 Games-Chan 算法，对 $\mathrm{LC}(s^{(n)})=2^n$，改变 $s^{(r+1)}$ 中的 1 bit 或 3 bit 而使得 $s_L^{(r+1)}=s_R^{(r+1)}$，改变后得到的新序列 $s^{(r+1)}$ 满足 $\mathrm{LC}(s^{(r+1)})=c$,$1\le c\le 2^r-1$。

(1)根据引理 7，当 $1\le \mathrm{LC}_3(s^{(r+1)})\le 2^{r-1}$ 时，对原 $s^{(r+1)}$，有 $M_3(s^{(r+1)})=1$。其中，当 $W_H(e^{(r+1)})=1$ 时，通过 Games-Chan 算法的一步逆过程可以得到，在 $e^{(r+2)}$ 中，$W_H(e^{(r+2)})$ 的值可以等于 1，但同样也可以等于 3。例如 $e^{(r+1)}=(0100\ 0000)$，$e^{(r+2)}$ 可以是 (0100 0000 0000 0000)，也可以是 (1100 0000 1000 0000)。从 $\mathrm{LC}_3(s^{(r+1)})$ 到 $\mathrm{LC}_3(s^{(n)})$，故 $M_3(s^{(n)})=2^{n-r-1}+2^{n-r-1}\times(2^{r+1}-1)\times(2^2)^{n-r-2}=2^{n-r-1}(2^{2n-r-3}-2^{2n-2r-4}+1)$；当 $W_H(e^{(r+1)})=3$ 时，得到的相应原 $s^{(n)}$ 的 3-错误序列个数为 $M_3(s^{(n)})=(2^3)^{n-r-1}=2^{3n-3r-3}$。

根据引理 6，若 $r=2$，$\mathrm{LC}_3(s^{(r+1)})=1$，则对应 3-错误序列 $e^{(r+1)}$ 唯一。若 $W_H(e^{(r+1)})=1$，有 $M_3(s^{(n)})=2^{n-r-1}(2^{2n-r-3}-2^{2n-2r-4}+1)=2^{3n-8}-2^{3n-11}+2^{n-3}$；若 $W_H(e^{(r+1)})=3$，有 $M_3(s^{(n)})=2^{3n-3r-3}=2^{3n-9}$。

(2)根据引理 8，当 $\mathrm{LC}_3(s^{(r+1)})=2^r-2^m+c$，$2\le m\le r-1$，$0<c<2^{m-1}$，$3\le r\le n-2$，有 $M_3(s^{(r+1)})=1,\ 2,\ 4$ 或 2^{r-m}。经过 Games-Chan 算法的 $(n-r-1)$ 步逆过程，$\mathrm{LC}_3(s^{(n)})=2^{n-1}+\cdots+2^{r+1}+(2^r-2^m+c)=2^n-2^r-2^m+c$。

当 $M_3(s^{(r+1)})=2^{r-m}$ 时，如果 $W_H(e^{(r+1)})=1$ 或 3，那么 $M_3(s^{(n)})=2^{n-r-1}(2^{2n-r-3}-2^{2n-2r-4}+1)+(2^{r-m}-1)\times(2^3)^{n-r-1}=2^{n-r-1}+2^{3n-2r-4}+2^{3n-2r-m-3}-5\times 2^{3n-3r-5}$；如果 $W_H(e^{(r+1)})=3$，则 $M_3(s^{(n)})=2^{r-m}\times 2^{3n-3r-3}=2^{3n-2r-m-3}$。

当 $M_3(s^{(r+1)})=1,2$ 或 4 时，$W_H(e^{(r+1)})=3$，故有 $M_3(s^{(n)})=2^{3n-3r-3}$，$2^{3n-3r-2}$ 或 $2^{3n-3r-1}$。

(3)当 $\mathrm{LC}_3(s^{(r+1)})=2^r-2^m$，$0\le m\le r-2$，对 $\mathrm{LC}_3(s^{(n)})=2^{n-1}+\cdots+2^{r+1}+(2^r-2^m)=2^n-2^r-2^m$ 时，根据引理 9，只能取 $W_H(e^{(r+1)})=3$，且 $M_3(s^{(r+1)})=1,\ 2$ 或 4，故 $M_3\left(s^{(n)}\right)=2^{3n-3r-3}$，$2^{3n-3r-2}$ 或 $2^{3n-3r-1}$。 证毕

经验证，当取 $n=4$ 时，对所有 $\mathrm{LC}(s^{(n)})=2^n$，只能取 $r=2$，$\mathrm{LC}_3(s^{(n)})=9$ 时的序列 $s^{(n)}$，它的 3-错误序列为 8 或者 16 个。例如 $s^{(n)}=(0000\ 1111\ 1101\ 0101)$，它的 3-错误序列有 8 个；$s^{(n)}=(0000\ 1111\ 1110\ 0000)$，它的 3-错误序列有 16 个。

引理 7，引理 8，引理 10 已给出了所有线性复杂度为 2^n 的 2^n- 周期二元序列 3-错误序列的分布，即下面的定理。

定理 1 设 $n\ge 4$，$\mathrm{LC}(r,c)=2^n-2^{r+1}+c$ 或 2^n-2^3+1, $3\le r\le n-1$，$1\le c\le 2^r-1$。$M_3(s^{(n)})$ 表示周期为 2^n，线性复杂度为 2^n 的序列 $s^{(n)}$，其 3-错线性复杂度为 $\mathrm{LC}(r,c)$ 的 3-错误序列的个数，则

$$M_3\left(s^{(n)}\right)=\begin{cases}1\\ \quad 其中\mathrm{LC}_3\left(s^{(n)}\right)=c,\ r=n-1,\ 1\le c\le 2^{n-2}\\ 2^{3n-3r-3},\ 2^{n-r-1}\left(2^{2n-r-3}-2^{2n-2r-4}+1\right)\\ \quad 其中\mathrm{LC}_3\left(s^{(n)}\right)=2^n-2^{r+1}+c,\ 2\le r\le n-2,\ 1\le c\le 2^{r-1}\\ 2^{n-m-1}\\ \quad 其中\mathrm{LC}_3\left(s^{(n)}\right)=2^{n-1}-2^m+c,\ r=n-1,\ 2\le m\le n-2,\ 0<c<2^{m-1}\\ 2^{3n-3r-3},\ 2^{3n-3r-2},\ 2^{3n-3r-1},\ 2^{3n-2r-m-3}\\ \text{或 } 2^{n-r-1}+2^{3n-2r-4}+2^{3n-2r-m-3}-5\times 2^{3n-3r-5}\\ \quad 其中\mathrm{LC}_3\left(s^{(n)}\right)=2^n-2^r-2^m+c,\ 3\le r\le n-2,\ 2\le m\le r-1,\ 0<c<2^{m-1}\\ 2^{3n-3r-3},\ 2^{3n-3r-2}\text{ 或 }2^{3n-3r-1}\\ \quad 其中\mathrm{LC}_3\left(s^{(n)}\right)=2^n-2^r-2^m,\ 3\le r\le n-1,\ 0\le m\le r-2\end{cases}$$

4　结束语

本文讨论了线性复杂度为 2^n 的序列的 3-错线性复杂度的分布情况，并对其相应的 3-错误序列进行了逐步分析，确定了 2^n-周期序列 $s^{(n)}$ 的 3-错误序列的计数公式 $M_k(s^{(n)})$。

对于 2^n-周期序列 $s^{(n)}$，如果 $\mathrm{LC}(s^{(n)})=2^n$，则 $\mathrm{LC}_4(s^{(n)})=\mathrm{LC}_3(s^{(n)})$，故 $M_4(s^{(n)})=M_3(s^{(n)})$，对 $\mathrm{LC}(s^{(n)})<2^n$ 的 $s^{(n)}$ 的 $M_4(s^{(n)})$ 尚待研究。此外，文献[9]研究了关于随机周期序列的线性复杂度和 k-错线性复杂度统计性质(期望、方差的界)的一些估计。文献[6]给出了 2^n-周期序列的 1-错误序列个数的期望值。对 $k\ge 2$，通过研究 $\mathrm{LC}(s^{(n)})=2^n$ 或 $\mathrm{LC}(s^{(n)})<2^n$ 条件下 2^n-周期二元序列 k-错误序列个数的统计特性，拓宽对序列的随机性检测方式。

参 考 文 献

[1] Ding C S, Xiao G Z, and Shan W J. The Stability Theory of Stream Ciphers[M]. Berlin: Springer-Verlag, 1991, Chapter 5.

[2] Stamp M and Martin C F. An algorithm for the k-error linear complexity of binary sequences with period 2^n [J]. *IEEE Transactions on Information Theory*, 1993, 39(4): 1398–1401.

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

[4] Zhou J Q. On the k-error linear complexity of sequences with period $2p^n$ over GF(q)[J]. *Designs, Codes and Cryptography*, 2011, 58(3): 279–296.

[5] 皮飞, 戚文峰. F_q 上 q^np^n-周期序列的线性复杂度与 k-错线性复杂度[J]. 信息工程大学学报, 2011, 12(1): 1–6.
Pi F and Qi W F. Linear complexity and k-error linear complexity of q^np^n-periodic sequences over F_q[J]. *Journal of Information Engineering University*, 2011, 12(1): 1–6.

[6] 谭林, 戚文峰. F_2 上 2^n-周期序列的 k-错误序列[J]. 电子与信息学报, 2008, 30(11): 2592–2595.
Tan L and Qi W F. On the k-error sequences of 2^n -periodic binary sequences[J]. *Journal of Electronics & Information Technology*, 2008, 30(11): 2592–2595.

[7] 周建钦. 具有 2^n 线性复杂度的 2^n-周期二元序列的 3-错线性复杂度[J]. 应用数学学报, 2012, 35(3).
Zhou J Q. On the 3- error linear complexity of 2^n-periodic binary sequences with linear complexity 2^n[J]. *Acta Mathematicae Applicatae Sinica*, 2012, 35(3).

[8] Meidl W. On the stability of 2^n-periodic binary sequences[J]. *IEEE Transactions on Information Theory*, 2005, 51(3): 1151–1155.

[9] Fu F, Niederreiter H, and Su M. The characterization of 2^n-periodic binary sequences with fixed 1-error linear complexity[C]. 4th International Conference on Sequences and Their Applications Beijing, 2006: 88–103.

周建钦：　男，1963 年生，教授，研究领域为通信、密码学与理论计算机科学.

刘　军：　男，1988 年生，硕士生，研究方向为密码学.