# $F_2$ 上 $2^n$-周期序列的 $k$-错误序列

谭　林　　戚文峰
(郑州信息工程大学信息工程学院应用数学系　郑州　450002)

**摘　要**：为了更好地刻画和研究序列的随机性，该文提出了序列的 $k$-错误序列的概念，并对 $k=1,2$，确定了 $F_2$ 上 $2^n$-周期序列的 $k$-错误序列的计数，还给出了 $F_2$ 上 $2^n$-周期序列的 1-错误序列个数的均值。

**关键词**：序列密码；线性复杂度；$k$-错误线性复杂度；$k$-错误序列
**中图分类号**：TN918.1　　**文献标识码**：A　　**文章编号**：1009-5896(2008)11-2592-04

# On the $k$-error Sequences of $2^n$-Periodic Binary Sequences

Tan Lin　　Qi Wen-feng
(*Department of Applied Mathematics, Zhengzhou Informativon Engineering University, Zhengzhou* 450002, *China*)

**Abstract**: In order to depict and study randomicity of sequences better, this correspondence gives the concept of $k$-error sequences of keystream, and for $k=1,2$, the counting function, i.e., the number of $k$-error sequences of $2^n$-periodic binary sequence, and the expected value of the number of 1-error sequences of $2^n$-periodic binary sequences are provided.

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

## 1　引言

设 $\underline{s}=(s_0,s_1,\cdots,s_{N-1})^\infty$ 为 $N$-周期的二元序列，其线性复杂度 $LC(\underline{s})$ 是指使得 $s_i+d_1s_{i-1}+\cdots+d_Ls_{L-1}+0$ 成立的最小非负整数 $L$，其中 $d_i\in F_2$，$i\geq L$，也就是指能生成该序列的最短线性反馈移位寄存器的长度。特别地，当 $\underline{s}$ 为 0 序列时，$LC(\underline{s})=0$。我们定义 $s(x)$ 为 $s(x)=s_0+s_1x+\cdots+s_{N-1}x^{N-1}$，则有

$$LC(\underline{s})=N-\deg\left(\gcd(x^N+1,s(x))\right) \tag{1}$$

线性复杂度是密钥流序列随机性检验的一个重要指标。为了抵抗 B-M 算法的攻击，密钥流序列的线性复杂度应该足够大。但仅仅线性复杂度高是不够的，还希望对序列改变少量的比特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体复杂度，文献[2]在文献[1]的基础上提出了序列的 $k$-错误线性复杂度。

**定义 1**[2]　设 $\underline{s}=(s_0,s_1,\cdots,s_{N-1})^\infty$ 是 $N$-周期的序列，其 $k$-错误线性复杂度 $LC_k(\underline{s})$ 定义为

$$LC_k(\underline{s})=\min_{W_N(\underline{e})\leq k}LC(\underline{s}+\underline{e}) \tag{2}$$

其中 $\underline{e}=(e_0,e_1,\cdots,e_{N-1})^\infty$，$W_N(\underline{e})$ 表示序列 $\underline{e}$ 一个 $N$-周期中非零元的个数。

记 $\mathrm{merr}(\underline{s})$ 为满足不等式 $LC_k(\underline{s})<LC(\underline{s})$ 的最小整数 $k$。文献[3]提出了错误序列的概念，我们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 $k$-错误序列的定义。

**定义 2**　设 $N$-周期序列 $\underline{s}$ 的 $k$-错误线性复杂度为 $LC_k(\underline{s})$，若 $N$-周期序列 $\underline{e}$ 满足 $LC(\underline{s}+\underline{e})=LC_k(\underline{s})$ 且 $1\leq W_N(\underline{e})\leq k$，则称 $\underline{e}$ 为 $\underline{s}$ 的 $k$-错误序列。记序列 $\underline{s}$ 的 $k$-错误序列的总数为 $M_k(\underline{s})$。

序列的线性复杂度稳定性的研究背景就是用一个线性复杂度较低的序列来逼近密钥序列，从而寻求近似解密，如果对某个正整数 $k$，密钥序列的 $k$-错误序列个数越多，则可供攻击者选择的序列就越多。所以我们认为一条安全性强的序列不仅要有高的线性复杂度和 $k$-错误线性复杂度，而且对数值较小的 $k$，还要有少的 $k$-错误序列。本文对 $k=1,2$，确定了 $F_2$ 上 $2^n$-周期序列 $\underline{s}$ 的 $k$-错误序列的计数 $M_k(\underline{s})$，并给出了 $F_2$ 上 $2^n$-周期序列的 1-错误序列个数的均值。本文所讨论的序列都是 $F_2$ 上的，在下文中我们不再重复说明了。

## 2　预备知识

**引理 1**[3]　设 $\underline{s}$ 是非零的 $2^n$-周期二元序列，则 $\mathrm{merr}(\underline{s})=2^{W_H(2^n-LC(\underline{s}))}$，这里 $W_H(j)$ 是 $j$ 的二进制表示中的汉明重量，$0\leq j\leq 2^n-1$。

由式(1)和引理1，不难得到下面的引理2。

**引理 2**　设 $\underline{s}$ 是 $2^n$-周期序列，$W_H(\underline{s})$ 表示 $\underline{s}$ 的汉明重量，若 $W_H(\underline{s})$ 为偶数，则 $LC_1(\underline{s})=LC(\underline{s})<2^n$；若 $W_H(\underline{s})$ 为奇数，则 $LC_1(\underline{s})<LC(\underline{s})=2^n$ 且 $LC_{2k}(\underline{s})=LC_{2k-1}(\underline{s})$，这里 $k$ 是任意的正整数。

2007-05-14 收到，2007-09-26 改回
国家自然科学基金(60673081)和国家“863”计划项目(2006AA01Z417)资助课题

**引理 3**[4]　设 $\underline{s}$ 是 $2^n$ -周期序列，且 $LC(\underline{s})=2^n$，则 $LC_1(\underline{s})$ 为 0 或者形为 $2^n-2^{r+1}+c$，$0\le r\le n-1$，$1\le c\le 2^r-1$。

**引理 4**[4]　设 $L_{r,c}=2^n-2^{r+1}+c$，$0\le r\le n-1$，$1\le c\le 2^r-1$。记 $N_1(L_{r,c})$ 表示线性复杂度为 $2^n$ 且 1-错误线性复杂度为 $L_{r,c}$ 的 $2^n$ -周期二元序列的个数，则 $N_1(0)=2^n$，$N_1(L_{r,c})=2^{L_{r,c}+r}$。

**引理 5**[5]　设 $N(L)$ 表示线性复杂度为 $L$ 的 $2^n$ -周期序列的个数，$0\le L\le 2^n$，则

$$N(0)=1,\quad N(L)=2^{L-1},\quad 1\le L\le 2^n$$

## 3　主要结果

**定理 1**　设 $\underline{s}$ 是 $2^n$ -周期序列，若 $LC_k(\underline{s})=LC_{k-1}(\underline{s})<LC_{k-2}(\underline{s})$，$k\ge 2$，则 $M_k(\underline{s})=M_{k-1}(\underline{s})$。

**证明**　因为 $LC_k(\underline{s})=LC_{k-1}(\underline{s})$，由 $k$-错误序列和 $M_k(\underline{s})$ 的定义，易知 $M_k(\underline{s})\ge M_{k-1}(\underline{s})$。又因为 $LC_{k-1}(\underline{s})<LC_{k-2}(\underline{s})$，所以 $W_H(\underline{s})+k-1$ 为偶数，并且 $LC_k(\underline{s})=LC_{k-1}(\underline{s})<2^n$。设 $\underline{e}$ 是任意汉明重量为 $k$ 的 $2^n$ -周期序列，则 $W_H(\underline{s}+\underline{e})$ 是奇数，$LC(\underline{s}+\underline{e})=2^n\ne LC_k(\underline{s})$，所以 $M_k(\underline{s})=M_{k-1}(\underline{s})$。

证毕

**推论 1**　设 $\underline{s}$ 是 $2^n$ -周期序列，若 $W_H(\underline{s})$ 为奇数，则 $M_{2k}(\underline{s})=M_{2k-1}(\underline{s})$，$k\ge 1$；若 $W_H(\underline{s})$ 为偶数，则 $M_1(\underline{s})=0$。

**证明**　若 $W_H(\underline{s})$ 为奇数，则 $LC_1(\underline{s})<LC(\underline{s})=2^n$，$LC_{2k}(\underline{s})=LC_{2k-1}(\underline{s})$，所以 $LC_{2k}(\underline{s})<2^n$。设 $\underline{e}$ 是任意汉明重量为 $2k$ 的 $2^n$ -周期序列，则 $W_H(\underline{s}+\underline{e})$ 是奇数，$LC(\underline{s}+\underline{e})=2^n\ne LC_{2k}(\underline{s})$，所以 $M_{2k}(\underline{s})=M_{2k-1}(\underline{s})$；若 $W_H(\underline{s})$ 为偶数，则 $LC(\underline{s})<2^n$，$LC_1(\underline{s})=LC(\underline{s})$。不存在汉明重量为 1 的 $2^n$ -周期序列 $\underline{e}$ 使得 $LC(\underline{s}+\underline{e})=LC(\underline{s})$，所以 $M_1(\underline{s})=0$。

证毕

设 $\underline{e}_i$ 表示汉明重量为 1 的 $2^n$ -周期序列，且 1 的位置在第 $i$ 位上，$0\le i\le 2^n-1$。

**引理 6**　设 $\underline{s}$ 是 $2^n$ -周期序列，$LC(\underline{s})=2^n$ 且 $2^n-2^{r+1}<LC_1(\underline{s})<2^n-2^r$，$1\le r\le n-1$，若 $LC_1(\underline{s})=LC(\underline{s}+\underline{e}_i)$，则 $LC(\underline{s}+\underline{e}_j)=LC_1(\underline{s})$ 当且仅当 $i\equiv j \bmod 2^{r+1}$，其中 $0\le i,j\le 2^n-1$。

**证明**　充分性：设 $\underline{s}$ 对应的函数为 $s(x)$，因为 $LC_1(\underline{s})=LC(\underline{s}+\underline{e}_i)$，所以 $\underline{s}+\underline{e}_i$ 对应的函数为 $s(x)+x^i=(1-x)^{2^n-LC_1(\underline{s})}a(x)$，$a(1)\ne 0$，则 $\underline{s}+\underline{e}_j$ 对应的函数为

$$s(x)+x^j=(1-x)^{2^n-LC_1(\underline{s})}a(x)+x^i(1-x^{j-i}) \tag{3}$$

因为 $2^n-LC_1(\underline{s})<2^{r+1}$，而 $j-i\ge 2^{r+1}$，所以，由式(1)可得 $LC(\underline{s}+\underline{e}_j)=LC(\underline{s}+\underline{e}_i)=LC_1(\underline{s})$。

必要性：$LC(\underline{s}+\underline{e}_j)=LC(\underline{s}+\underline{e}_i)=LC_1(\underline{s})$，设 $s(x)+x^j=(1-x)^{2^n-LC_1(\underline{s})}b(x)$，$b(1)\ne 0$，则

$$x^i+x^j=x^i(1-x^{j-i})=(1-x)^{2^n-LC_1(\underline{s})}(a(x)+b(x)) \tag{4}$$

又因为 $2^n-LC_1(\underline{s})>2^r$，所以

$$\begin{aligned}\deg(\gcd((1-x)^{2^n},x^i+x^j))&=\deg(\gcd((1-x)^{2^n},1-x^{j-i}))\\&=\gcd(2^n,j-i)>2^r\end{aligned}$$

从而可知 $2^{r+1}$ 整除 $j-i$，故 $i\equiv j \bmod 2^{r+1}$。　　证毕

**定理 2**　设 $\underline{s}$ 是 $2^n$ -周期序列，$LC(\underline{s})=2^n$，则 $M_2(\underline{s})=M_1(\underline{s})$。进一步，如果 $2^n-2^{r+1}<LC_1(\underline{s})<2^n-2^r$，$1\le r\le n-1$，则 $M_2(\underline{s})=M_1(\underline{s})=2^{n-r-1}$；如果 $LC_1(\underline{s})=0$，则 $M_k(\underline{s})=1$，$k\ge 1$。

**证明**　若 $LC(\underline{s})=2^n$，则 $W_H(\underline{s})$ 为奇数，由推论 1，取 $k=1$ 即有 $M_2(\underline{s})=M_1(\underline{s})$。再根据引理6可知，$LC(\underline{s}+\underline{e}_j)=LC(\underline{s}+\underline{e}_i)=LC_1(\underline{s})$ 当且仅当 $i\equiv j \bmod 2^{r+1}$。而 $0\le i,j\le 2^n-1$，所以 $M_2(\underline{s})=M_1(\underline{s})=2^{n-r-1}$；若 $LC_1(\underline{s})=0$，显然错误序列就是 $\underline{s}$，故 $M_k(\underline{s})=1$，$k\ge 1$。　　证毕

由引理 5 可知，线性复杂度为 $2^n$ 的 $2^n$ -周期二元序列有 $2^{2^n-1}$ 条，再由引理 4 和定理 2 容易得到定理 3。

**定理 3**　线性复杂度为 $2^n$ 的 $2^n$ -周期序列的 1-错误序列个数的均值 $E_{1,2^n}$ 为

$$E_{1,2^n}=2^{n+1}\sum_{r=1}^{n-1}2^{-2^{r+1}}(2^{2^r-1}-1)+2^{-2^n+n+1} \tag{5}$$

Meidl 在文献[4]中指出，若 $2^n$ -周期序列 $\underline{s}$ 的 $LC(\underline{s})=2^n$，则 $LC_1(\underline{s})=LC_2(\underline{s})$，引理 4 中的计数对 $k=1,2$ 都成立，由定理 2 又知道 $M_2(\underline{s})=M_1(\underline{s})$，所以定理 3 的结果实际上是对 $k=1,2$ 时，线性复杂度为 $2^n$ 的 $2^n$ -周期序列的 $k$-错误序列个数的均值。由推论 2 可知线性复杂度小于 $2^n$ 的 $2^n$ -周期序列的 1-错误序列个数为零，所以容易得到推论 2。

**推论 2**　$2^n$ -周期序列的 1-错误序列个数的均值为

$$E_1=2^n\sum_{r=1}^{n-1}2^{-2^{r+1}}(2^{2^r-1}-1)+2^{-2^n+n} \tag{6}$$

接下来讨论线性复杂度小于 $2^n$ 时序列 $\underline{s}$ 的 $M_2(\underline{s})$。记 $\underline{s}_{i,j}=\underline{s}+\underline{e}_i+\underline{e}_j$，其中 $\underline{e}_i$，$\underline{e}_j$ 是重量为 1 的 $2^n$ -周期二元序列，$i\ne j$。

**引理 7**[6]　若 $1\le L\le 2^{n-1}$，$2^n$ -周期序列 $\underline{s}_1$，$\underline{s}_2$ 的线性复杂度都为 $L$，则 $\underline{s}_1$ 与 $\underline{s}_2$ 的汉明距离：

$$d_H(\underline{s}_1,\underline{s}_2)\ge 4 \tag{7}$$

**引理 8**[6]　设 $\underline{s}$ 是 $2^n$ -周期序列，$2^n-2^{r+1}<LC(\underline{s})<2^n-2^r$，$1\le r\le n-2$，则对任意的 $0\le i\le 2^n-1$，正好有 $2^{n-r-1}-1$ 个 $\underline{s}_{i,j}$ 满足 $LC(\underline{s}_{i,j})=LC(\underline{s})$，$0\le j\le 2^n-1$。

**定理 4** 设 $\underline{s}$ 是 $2^n$ -周期序列，若 $1 \le LC(\underline{s}) < 2^{n-1}$，则 $M_2(\underline{s}) = 0$；若 $2^n - 2^{r+1} < LC(\underline{s}) < 2^n - 2^r$，$1 \le r \le n-2$，则 $M_2(\underline{s}) = 2^{2n-r-2} - 2^{n-1}$。

**证明** 若 $1 \le LC(\underline{s}) < 2^{n-1}$，则 $\mathrm{merr}(\underline{s}) > 2$，故 $LC_2(\underline{s}) = LC(\underline{s})$，由引理 7 可知，不存在 $2^n$ -周期序列 $\underline{e}$，$1 \le W_H(\underline{e}) \le 2$，使得 $LC(\underline{s}+\underline{e}) = LC_2(\underline{s}) = LC(\underline{s})$，所以 $M_2(\underline{s}) = 0$；若 $2^n - 2^{r+1} < LC(\underline{s}) < 2^n - 2^r$，$1 \le r \le n-2$，则 $\mathrm{merr}(\underline{s}) > 2$，$LC_2(\underline{s}) = LC(\underline{s})$，由引理 8 可知，对任意的 $0 \le i \le 2^n - 1$，正好有 $2^{n-r-1} - 1$ 个 $\underline{s}_{i,j}$ 满足 $LC(\underline{s}_{i,j}) = LC_2(\underline{s})$，再由 $i$ 和 $j$ 的对称性知：$M_2(\underline{s}) = 2^n(2^{n-r-1} - 1)/2 = 2^{2n-r-2} - 2^{n-1}$。 证毕

**引理 9** 设 $\underline{s}$ 是 $2^n$ -周期序列，若 $LC(\underline{s}) = 2^n - 2^r$，$0 \le r \le n-1$，则对任意的 $0 \le i \le 2^n - 1$，正好有 $2^{n-r-1}$ 个 $\underline{s}_{i,j}$ 满足 $LC(\underline{s}_{i,j}) < LC(\underline{s})$，$0 \le j \le 2^n - 1$，从而总共存在 $2^{2n-r-2}$ 个 $\underline{s}_{i,j}$ 使得 $LC(\underline{s}_{i,j}) < LC(\underline{s})$。

**证明** 因为 $LC(\underline{s}) = 2^n - 2^r$，由引理 1 可知 $\mathrm{merr}(\underline{s}) = 2$，$LC_2(\underline{s}) < LC(\underline{s})$。设 $\underline{s}$ 对应的函数为 $s(x) = (1-x)^{2^r} a(x)$，$a(1) \ne 0$，则 $\underline{s}_{i,j}$ 对应的函数为

$$\underline{s}_{i,j}(x) = s(x) + x^i + x^j = (1-x)^{2^r} a(x) + x^i(1 - x^{j-i}) \quad (8)$$

故 $LC(\underline{s}_{i,j}) < LC(\underline{s}) \Leftrightarrow \deg(\gcd((1-x)^{2^n}, 1-x^{j-i})) = \cdot\gcd(2^n, j-i) = 2^r \Leftrightarrow j = i + t2^r \bmod 2^n$，$1 \le t \le 2^{n-r} - 1$ 且 $t$ 为奇数。

对任意的 $0 \le i \le 2^n - 1$，这样的 $j$ 正好有 $2^{n-r-1}$ 个，而 $i$ 和 $j$ 是对称的，所以使得 $LC(\underline{s}_{i,j}) < LC(\underline{s})$ 的 $\underline{s}_{i,j}$ 总共有 $2^n 2^{n-r-1}/2 = 2^{2n-r-2}$ 个。 证毕

**引理 10** 设 $\underline{s}$ 是 $2^n$ -周期序列，若 $LC(\underline{s}) = 2^n - 2^r$，$0 \le r \le n-1$，则 $LC_2(\underline{s}) = 0$ 或为如下两种形式：

$$LC_2(\underline{s}) = \begin{cases} 2^n - 2^{t+1} + c, & r+1 \le t \le n-1, 1 \le c \le 2^t - 1 \\ 2^n - 2^r - 2^{t+1} + c, & 1 \le t \le r-1, 1 \le c \le 2^t - 1 \end{cases}$$

**证明** 如果 $W_H(\underline{s}) = 2$，则 $LC_2(\underline{s}) = 0$；若 $W_H(\underline{s}) \ne 2$，则因为 $LC(\underline{s}) = 2^n - 2^r$，所以按照 Games–Chan 算法，在第 $n-r$ 步后 $\underline{s}^{(2^r)} = 0$，即 $\underline{s}_L^{(2^{r+1})} = \underline{s}_R^{(2^{r+1})}$。因为 $W_H(\underline{s})$ 为偶数，所以每步对折后 $\underline{s}^{(2^i)}$ 的汉明重量都是偶数，$r \le i \le n-1$。若 $W_H\left(\underline{s}^{(2^{r+1})}\right) = 2$，则一定能找到一正整数 $t$，$r+1 \le t \le n-1$，使得 $W_H\left(\underline{s}^{(2^t)}\right) = 2$，$W_H\left(\underline{s}^{(2^{t+1})}\right) > 2$，那么就有 $\underline{s}_L^{(2^{t+1})} = \underline{s}_R^{(2^{t+1})} + \underline{e}_{ij}$，其中 $\underline{e}_{ij}$ 的周期为 $2^t$，汉明重量为 2。根据 Stamp-Martin 算法可以改变 $\underline{s}^{(2^{t+1})}$ 的两比特使得 $\underline{s}_L^{(2^{t+1})} = \underline{s}_R^{(2^{t+1})}$，故 $LC_2(\underline{s}) = 2^n - 2^{t+1} + c$，其中 $1 \le c \le 2^t - 1$。若 $W_H\left(\underline{s}^{(2^{r+1})}\right) \ne 2$，则 $W_H\left(\underline{s}_L^{(2^{r+1})}\right)$ 一定为大于 1 的奇数，否则，则 $LC\left(\underline{s}_L^{(2^{r+1})}\right) < 2^r$，从而 $LC(\underline{s}) = 2^n - 2^{r+1} + LC\left(\underline{s}_L^{(2^{r+1})}\right) < 2^n - 2^r$，这与条件矛盾。于是有 $LC\left(\underline{s}_L^{(2^{r+1})}\right) = LC\left(\underline{s}_R^{(2^{r+1})}\right) = 2^r$，那么 $LC_2(\underline{s}) = 2^n - 2^{r+1} + LC_1\left(\underline{s}_L^{(2^{r+1})}\right)$，再由引理 3 可知 $LC_1\left(\underline{s}_L^{(2^{r+1})}\right) = 2^r - 2^{t+1} + c$，$1 \le t \le r-1$，$1 \le c \le 2^t - 1$，故 $LC_2(\underline{s}) = 2^n - 2^r - 2^{t+1} + c$。 证毕

**定理 5** 设 $\underline{s}$ 是 $2^n$ -周期序列，$LC(\underline{s}) = 2^n - 2^r$，$0 \le r \le n-1$，有

(1)若 $LC_2(\underline{s}) = 0$，则 $M_2(\underline{s}) = 1$；

(2) 若 $LC_2(\underline{s}) = 2^n - 2^r - 2^{t+1} + c$，$1 \le t \le r-1$，$1 \le c \le 2^t - 1$，则 $M_2(\underline{s}) = 2^{2n-r-t-3}$；

(3)若 $LC_2(\underline{s}) = 2^n - 2^{t+1} + c$，$r+1 \le t \le n-1$，则

(a)如果 $1 \le c \le 2^{t-1} - 1$，则 $M_2(\underline{s}) = 2^{2n-2t-2}$。

(b) 如果 $2^{t-1} \le c \le 2^t - 1$ 则 $M_2(\underline{s}) = 2^{2n-2t-2}$ 或者 $2^{2n-2t-1}$。

**证明** (1) 若 $LC_2(\underline{s}) = 0$ 则 $W_H(\underline{s}) = 2$，显然有 $M_2(\underline{s}) = 1$；

(2)若 $LC_2(\underline{s}) = 2^n - 2^r - 2^{t+1} + c$，由引理 10 的证明过程可知 $\underline{s}_L^{(2^{r+1})} = \underline{s}_R^{(2^{r+1})}$，且 $LC\left(\underline{s}_L^{(2^{r+1})}\right) = LC\left(\underline{s}_R^{(2^{r+1})}\right) = 2^r$，根据 Stamp-Martin 算法，$LC_2(\underline{s}) = 2^n - 2^{r+1} + LC_1\left(\underline{s}_L^{(2^{r+1})}\right)$，对 $\underline{s}^{(2^{r+1})}$ 改变的 2 比特即：对 $\underline{s}_L^{(2^{r+1})}$ 和 $\underline{s}_R^{(2^{r+1})}$ 作相同的 1 比特改变，使得

$$LC\left(\underline{s}_L^{(2^{r+1})} + \underline{e}_i\right) = LC_1\left(\underline{s}_L^{(2^{r+1})}\right) = 2^r - 2^{t+1} + c,$$
$$1 \le t \le r-1,\ 1 \le c \le 2^t - 1。$$

其中 $\underline{e}_i$ 是重量为 1 的 $2^r$ 长的序列，且 1 在第 $i$ 个位置上，$0 \le i \le 2^r - 1$。根据定理 2 可知，这样的 $\underline{e}_i$ 有 $2^{r-t-1}$ 个。从原序列 $\underline{s}$ 来看，错误位置应该为 $\left(i + m_1 2^{r+1}, j + m_2 2^{r+1}\right)$，其中 $j = i + 2^r$，$m_1, m_2 = 0, 1, \cdots, 2^{n-r-1} - 1$。从而就可得到 $M_2(\underline{s}) = 2^{r-t-1}(2^{n-r-1})^2 = 2^{2n-r-t-3}$。

(3)若 $LC_2(\underline{s}) = 2^n - 2^{t+1} + c$，由引理 10 的证明过程知：一定能找到一正整数 $t$，$r+1 \le t \le n-1$，使得 $W_H\left(\underline{s}^{(2^t)}\right) = 2$，$W_H\left(\underline{s}^{(2^{t+1})}\right) > 2$，$\underline{s}_L^{(2^{t+1})} = \underline{s}_R^{(2^{t+1})} + \underline{e}_{ij}$，其中 $\underline{e}_{ij}$ 的周期为 $2^t$，汉明重量为 2。Stamp-Martin 算法的思想就是改变 $\underline{s}^{(2^{t+1})}$ 的两比特使得 $\underline{s}_L^{(2^{t+1})_r} = \underline{s}_R^{(2^{t+1})_r}$，因为 $LC_2(\underline{s}) = 2^n - 2^{t+1} + c$，故可知 $LC\left(\underline{s}_L^{(2^{t+1})_r}\right) = c$ 且 $LC\left(\underline{s}_L^{(2^{t+1})}\right) \ge c$，$LC\left(\underline{s}_R^{(2^{t+1})}\right) \ge c$。若 $LC\left(\underline{s}_R^{(2^{t+1})}\right) = c$，则对 $\underline{s}^{(2^{t+1})}$ 的改变为位置 $(i, j)$；若 $LC\left(\underline{s}_L^{(2^{t+1})}\right) = c$，则对 $\underline{s}^{(2^{t+1})}$ 的改变为位置 $(2^t + i, 2^t + j)$。若 $LC\left(\underline{s}_L^{(2^{t+1})}\right) = LC\left(\underline{s}_R^{(2^{t+1})}\right) = c$，则对 $\underline{s}^{(2^{t+1})}$ 的改变为 $(i, j)$ 和 $(2^t + i, 2^t + j)$ 两种。若 $LC\left(\underline{s}_L^{(2^{t+1})}\right) > c$ 且

$LC\left(\underline{s}_R^{(2^{t+1})}\right)>c$，则对$\underline{s}^{(2^{t+1})}$的改变可能为位置$(i,2^t+j)$或$(j,2^t+i)$。

如果$1\le c\le 2^{t-1}-1$，由引理7可知$LC\left(\underline{s}_L^{(2^{t+1})}\right)$和$LC\left(\underline{s}_R^{(2^{t+1})}\right)$不可能同时为$c$，$LC(\underline{s}_L^{(2^{t+1})}+\underline{e}_i)$和$LC\left(\underline{s}_L^{(2^{t+1})}+\underline{e}_j\right)$也不可能同时为$c$，故此时对$\underline{s}^{(2^{t+1})}$的改变位置只能为$(i,j)$，$(2^t+i,2^t+j)$，$(i,2^t+j)$和$(j,2^t+i)$中的一种，即对$\underline{s}^{(2^{t+1})}$的改变是唯一的，若记为$(i',j')$，则从原序列$\underline{s}$来看，改变的错误位置应该为$(i'+m_1 2^{t+1},j'+m_2 2^{t+1})$，其中$m_1$，$m_2=0,1,\cdots,2^{n-t-1}-1$。所以$M_2(\underline{s})=(2^{n-t-1})^2=2^{2n-2t-2}$。

如果$2^{t-1}\le c\le 2^t-1$，当$LC\left(\underline{s}_L^{(2^{t+1})}\right)=LC\left(\underline{s}_R^{(2^{t+1})}\right)$时，对$\underline{s}^{(2^{t+1})}$的改变为$(i,j)$和$(2^t+i,2^t+j)$两种；当$LC\left(\underline{s}_L^{(2^{t+1})}\right)>c$且$LC\left(\underline{s}_R^{(2^{t+1})}\right)>c$时，若$LC\left(\underline{s}_L^{(2^{t+1})}+\underline{e}_i\right)=LC\left(\underline{s}_L^{(2^{t+1})}+\underline{e}_j\right)=c$，则对$\underline{s}^{(2^{t+1})}$的改变也有两种：$(i,2^r+j)$和$(j,2^r+i)$，此两种情形时，$M_2(\underline{s})=2(2^{n-t-1})^2=2^{2n-2t-1}$；而其他情形时，对$\underline{s}^{(2^{t+1})}$的改变都只有一种，即$M_2(\underline{s})=2^{2n-2t-2}$。　　证毕

## 4　结束语

本文从序列密码安全性的角度提出了序列的$k$-错误序列的概念，并对$k=1,2$，确定了$F_2$上$2^n$-周期序列$\underline{s}$的$k$-错误序列的计数$M_k(\underline{s})$，还给出了$F_2$上$2^n$-周期序列的1-错误序列个数的均值。对$k>2$，确定$2^n$-周期序列的$k$-错误序列的计数和均值，以及确定一般周期序列的$k$-错误序列的计数和均值或者给出其有效的界，仍是我们尚待研究的问题。

## 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 Trans. on information Theory*, 1993, 39(4): 1398–1401.

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

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

[5] Rueppel R A. Analysis and Design of Stream Ciphers[M]. Berlin: Springer-Verlag, 1986, chapter 4.

[6] Fu Fangwei, Niederreiter Harald, and Su Ming. The characterization of $2^n$-periodic binary sequences with fixed 1-error linear complexity[C]. Sequences and Their Applictions. Beijing, 2006: 88–103.

[7] Games R A and Chan A H. A fast algorithm for determining the complexity of a pseudo random sequence with period $2^n$[J]. *IEEE Trans. on Information Theory*, 1983, 29(1): 144–146.

[8] Zhu Fengxiang and Qi Wengfeng. The 2-error linear complexity of $2^n$-periodic binary sequences with linear complexity $2^n-1$[J]. *Journal of Electronics*(China), 2007, 24(3): 390–395.



谭　林：　男，1983年生，硕士生，研究方向为密码学.

戚文峰：　男，1963年生，教授，博士生导师，研究领域包括密码学与信息安全.