

线性复杂度为 $2^n - 2^m - 1$ 的 2^n -周期二元序列 的 k -错线性复杂度 *

朱士信, 梁 静

(合肥工业大学 数学学院, 合肥 230009)

摘 要: 线性复杂度和 k -错线性复杂度是研究流密码稳定性的两个重要概念。当改变序列某几位时不会使得序列的线性复杂度急剧减少, 说明该序列的稳定性良好。运用 Chan-Games 给出了当 $k=4$ 或 5 时, F_2 上固定线性复杂度为 $2^n - 2^m - 1$ 的 2^n -周期二元序列的 k -错线性复杂度所有可能值, $LC_k(\underline{s}) = 0$ 或 $LC_k(\underline{s}) = 2^n - 2^m - 2^{r+1} + c$, $LC_k(\underline{s}) = 2^n - 2^{r+1} + c$ 。这一结果对流密码稳定性的研究有重要的应用价值。

关键词: 线性复杂度; k -错线性复杂度; Chan-Games 算法; 二元周期序列; 流密码

中图分类号: TN918.4

文献标志码: A

文章编号: 1001-3695(2012)03-1104-03

doi:10.3969/j.issn.1001-3695.2012.03.083

k -error linear complexity of 2^n -periodic binary sequences with linear complexity $2^n - 2^m - 1$

ZHU Shi-xin, LIANG Jing

(School of Mathematics, Hefei University of Technology, Hefei 230009, China)

Abstract: Linear complexity and k -error linear complexity are two important concepts to study the stability of the stream cipher. When a sequences changed some bit don't lead to the linear complexity sharply reduce, so the sequences more stability. For a 2^n -periodic binary sequence with linear complexity $2^n - 2^m - 1$ on F_2 , and $k=4$ or 5 , this paper obtained all the possible values of the k -error linear complexity using Chan-Games algorithm, $LC_k(s) = 0$ or $LC_k(s) = 2^n - 2^m - 2^{r+1} + c$, $LC_k(s) = 2^n - 2^{r+1} + c$. The result has an important application value for study the stability of stream cipher.

Key words: linear complexity; k -error linear complexity; Chan-Games algorithm; periodic binary sequences; stream ciphers

0 引言

设 $\underline{s} = (s_0, s_1, \dots, s_{N-1})^\infty$ 为 N -周期二元序列, 定义 s 的汉明重量为 $\underline{s}$ 的一个周期中非零元的个数, 记为 $W(s)$ 。类似地定义 $\underline{s}^N$ 的汉明重量为 $\underline{s}^N$ 中非零元的个数, 记为 $W(s^N)$ 。显然对于周期序列 $\underline{s}$, 若 $\underline{s}^N$ 是其一个周期, 则有 $W(s) = W(s^N)$ 。 s 的线性复杂度记为 $LC(\underline{s})$, 是使得等式 $s_i + d_1 s_{i-1} + \dots + d_L s_{i-L} = 0$ 成立的最小正整数 L , 其中 $d_i \in F_2 (i \geq L)$ 。特殊地, 当 s 为 0 序列时, 其线性复杂度为 0, 即 $LC(s) = 0$ 。定义 N -周期二元序列 s^N 的连接多项式为 $s^N(x) = s_0 + s_1 x + \dots + s_{N-1} x^{N-1}$, 则其线性复杂度为 $LC(s) = N - \deg(\gcd(s^N(x), 1 - x^N))$ 。

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。但仅仅线性复杂度足够大还不够, 还希望即使序列在改变少量的比特时也不会使得序列的线性复杂度急剧下降。于是文献[1]提出了球体复杂度, 文献[2]在文献[1]的基础上提出了序列的 k -错线性复杂度。

定义 1^[2] 设 s^N 是 F_2 上 N -周期二元序列, 对整数 $k(0 \leq k \leq N)$, 改变 s^N 中至多 k 位后得到的最小线性复杂度称为 s^N 的

k -错线性复杂度, 记为 $LC_k(s)$, 则有 $LC_k(s^N) = \min_{0 \leq W(e^N) \leq k} LC(s^N + e^N)$ 。其中 $e = (e_0, e_1, \dots, e_{N-1})^\infty$, $W_H(e)$ 表示序列 e 一个 N -周期中非零元的个数。

文献[3]给出了序列的线性复杂度严格小于 k -错线性复杂度的 k 的表示形式。在文献[4]中, Meidl 给出了 2^n -周期二元序列 1-错线性复杂度的具体形式及期望, 并讨论了 k -错 ($k \geq 2$) 线性复杂度期望的界。文献[5]对固定线性复杂度 $2^n - 1$ 的 2-错线性复杂度进行讨论, 给出了 2-错线性复杂度的具体形式及期望。文献[6]给出了线性复杂度为 $2^n - 2^m$ 的 2-错线性复杂度的具体形式及其错误序列的个数。本文通过运用 Chan-Games^[7], 给出了线性复杂度为 $2^n - 2^m - 1$ 的 2^n -周期二元序列的 k -错线性复杂度的具体形式及特定重量下的计数。

本文主要讨论 $N = 2^n$ 的情形。为了方便叙述, 下面给出一些简记形式。因为序列 $s^N = (s_0, s_1, \dots, s_{N-1})^\infty$ 是序列 $\underline{s} = (s_0, s_1, \dots, s_{N-1})^\infty$ 的前 N 周期, 所以有 $LC(\underline{s}^N) = LC(\underline{s})$ 。当 $N = 2^n$ 时用 $\underline{s}^{(n)}$ 代替 $\underline{s}^{2^n}$ 。

1 预备知识

引理 1^[3] 设 $\underline{s}$ 是非零 2^n -周期二元序列, 则 $\min \text{error}(\underline{s}) =$

收稿日期: 2011-08-01; 修回日期: 2011-09-03 基金项目: 国家自然科学基金资助项目(60973125); 高校博士点基金资助项目(20080359003); 东南大学移动通信国家重点实验室开放课题资助项目

作者简介: 朱士信(1962-), 男, 教授, 博导, 国家级教学名师, 主要研究方向为序列密码和纠错码理论; 梁静(1986-), 女, 安徽蒙城人, 硕士研究生, 主要研究方向为序列密码和纠错码(beaulj8607@163.com)。

$2^{W_H(2^n - LC(\underline{s}))}$, 此处 $W_H(j)$ 是 j 的二进制表示中的汉明重量, $0 \leq j \leq 2^n - 1$ 。

引理 2^[8] 设 $\underline{s}$ 是 2^n -周期二元序列, 则 $LC(\underline{s}) = 2^n \Leftrightarrow W(\underline{s})$ 为奇数。

引理 3^[5] 设 $\underline{s}^{(n)} = (s_0, s_1, \dots, s_{2^n-1})$ 是 2^n -周期二元序列, 则 $\underline{s}^{(n)}$ 的线性复杂度满足 $LC(\underline{s}^{(n)}) \leq 2^n - 2 \Leftrightarrow s_0 + s_2 + \dots + s_{2^n-2} = s_1 + s_3 + \dots + s_{2^n-1} = 0$ 。

引理 4^[5] 设 $\underline{s}^{(n)} = (s_0, s_1, \dots, s_{2^n-1})$ 是线性复杂度为 $2^n - 1$ 的 2^n -周期二元序列, $N_{2|LC(\underline{s})=2^n-1}(L_{r,c})$ 表示 $LC(\underline{s}) = 2^n - 1$ 且 $LC_{2^n,2}(\underline{s}) = L_{r,c}$ 的 2^n -周期二元序列的条数。如果 $L_{r,c}$ 满足 $L_{r,c} = 2^n - 2^{r+1} + c, 2 \leq r \leq n-1, 1 \leq c \leq 2^r - 2$, 则 $N_{2|LC(\underline{s})=2^n-1}(L_{r,c}) = 2^{2^n-2^{r+1}+c+2r-1}$, 且 $N_{2|LC(\underline{s})=2^n-1}(0) = 2^{2^n-2}$ 。对于不等于 $L_{r,c}$ 的正整数 L , 不存在 $LC(\underline{s}) = 2^n - 1$ 且 $LC_{2^n,2}(\underline{s}) = L$ 的 2^n -周期二元序列。

因为本文的主要工具是 Chan-Games 算法, 下面就简要地介绍一下该算法。

设 $\underline{s}^{(t)} = (s_0, s_1, \dots, s_{2^t-1})$, 事实上 Chan-Games 算法是一个递归过程, 每一步将向量 $\underline{s}^{(t)}$ ($1 \leq t \leq n$) 分成左右两部分: $L(\underline{s}^{(t)}) = (s_0, s_1, \dots, s_{2^{t-1}-1}), R(\underline{s}^{(t)}) = (s_{2^{t-1}}, s_{2^{t-1}+1}, \dots, s_{2^t-1})$ 。

如果 $L(\underline{s}^{(t)}) = R(\underline{s}^{(t)}), LC(\underline{s}) = LC(L(\underline{s}^{(t)}))$, 否则 $LC(\underline{s}) = 2^{t-1} + LC(b)$, 其中 $b = L(\underline{s}^{(t)}) + R(\underline{s}^{(t)})$ 。从该算法可以看出, 当且仅当 $L(\underline{s}^{(t)}) \neq R(\underline{s}^{(t)})$ 时线性复杂度才会增加。由 Chan-Games 算法的思想, 可以定义一个 $F_2^{2^t}$ 到 $F_2^{2^{t-1}}$ 的映射 φ_t :

$$\varphi_t(s_0, s_1, \dots, s_{2^t-1}) = (s_0 + s_{2^{t-1}}, s_1 + s_{2^{t-1}+1}, \dots, s_{2^{t-1}-1} + s_{2^t-1})$$

满足下面三个性质:

$$P1: W(\varphi_t(\underline{s}^{(t)})) \leq W(\underline{s}^{(t)});$$

$$P2: \text{当 } t \geq 2 \text{ 时, } W(\varphi_t(\underline{s}^{(t)})) \text{ 和 } W(\underline{s}^{(t)}) \text{ 同偶};$$

$$P3: \underline{s}^{(t)} \text{ 的原像集合 } \varphi_{t+1}^{-1}(\underline{s}^{(t)}) = \{\underline{v} \in F_2^{2^{t+1}} \mid \varphi_{t+1}(\underline{v}) = \underline{s}^{(t)}\}$$

中元素的个数为 2^{2^t} 。

2 主要结果

设 2^n -周期二元序列 $\underline{s}$ 的线性复杂度为 $2^n - 2^m - 1$ ($0 \leq m \leq n-1$)。由引理 1 的 $\min \text{ error } 2^{W_H(2^n - LC(\underline{s}))} = 4$, 则该序列的线性复杂度下降当且仅当 $k \geq 4$ 。由引理 2 知, $W_{2^n}(s)$ 为偶数, 若每个周期相同位置改变恰好 5 bit, 则 $W_{2^n}(s)$ 变成奇数, 序列的线性复杂度变成了 2^n , 故 $LC_{2^n,4}(s) = LC_{2^n,5}(s)$ 。下面只考虑序列 $\underline{s}$ 的 4-错线性复杂度。

定理 1 设 $\underline{s}$ 是线性复杂度为 $2^n - 2^m - 1, 0 \leq m \leq n-1, 2^n$ -周期二元序列, $LC_{2^n,4}(\underline{s}) = 0$, 或为如下两种形式:

$$LC_{2^n,4}(\underline{s}) = \begin{cases} 2^n - 2^m - 2^{r+1} + c, 2 \leq r \leq m-1, 1 \leq c \leq 2^r - 2 \\ 2^n - 2^{r+1} + c, m+1 \leq r \leq n-1, 1 \leq c \leq 2^r - 2, c \neq 2^r - 2^m - 1 \end{cases}$$

证明 设 $\underline{s}^{(n)} = (s_0, s_1, \dots, s_{2^n-1})$ 是序列 $\underline{s}$ 一个 2^n -周期所对应的向量。 $\underline{s}^{(t)} = \varphi_{t+1} \cdots \varphi_n(\underline{s}^{(n)}) = (s_0^{(t)}, s_1^{(t)}, \dots, s_{2^t-1}^{(t)})$, 其中 $m \leq t \leq n-1$ 。根据 Chan-Games 算法, 序列 $\underline{s}$ 必满足

$$L(\underline{s}^{(t)}) \neq R(\underline{s}^{(t)}), m+2 \leq t \leq n, L(\underline{s}^{(m+1)}) = R(\underline{s}^{(m+1)}) \quad (1)$$

且 $LC(L(\underline{s}^{(m+1)})) = 2^m - 1$, 显然 $\underline{s}^{(m)} = 0$ 。

由映射 φ_t 的性质 $P1$ 和 $P2, W(\underline{s}^{(t)})$ 为偶数, 且 $W(\underline{s}^{(t)}) \leq$

$$W(\underline{s}^{(n)}), m \leq t \leq n。$$

下面根据 $\underline{s}^{(n)}$ 和 $\underline{s}^{(m+1)}$ 的汉明重量来分情况讨论。

情形 1 $W_{2^n}(\underline{s}) = W(\underline{s}^{(n)}), W(\underline{s}^{(n)}) \leq 4$

显然 $LC_{2^n,4}(\underline{s}) = 0$ 。

情形 2 $W_{2^n}(\underline{s}) = W(\underline{s}^{(n)}) > 4$, 且 $W(\underline{s}^{(m+1)}) > 4$

当 $j > m$ 时有 $W(\underline{s}^{(j)}) > 4$, 而且 $L(\underline{s}^{(m+1)}) = R(\underline{s}^{(m+1)})$, 则 $LC_{2^n,4}(s) = 2^{n-1} + 2^{n-2} + \dots + 2^{m+1} + K, K < 2^m$ 。而由 $L(\underline{s}^{(m+1)}) = R(\underline{s}^{(m+1)})$ 可知, 要使 $L(\underline{s}^{(m+1)})$ 中两个比特发生改变, 需要改变 $\underline{s}^{(n)}$ 中的四个比特, 从而 $k = LC_{2^n,2}(L(\underline{s}^{(m+1)}))$ 。由引理 2 知 $W(\underline{s}^{(n)})$ 为偶数, 又 $W(\underline{s}^{(n)}) > 4, W(\underline{s}^{(m+1)}) > 4$, 故 $W(L(\underline{s}^{(m+1)})) > 2$; 另一方面 $LC(L(\underline{s}^{(m+1)})) = 2^m - 1$, 由引理 4 知 $K = 2^m - 2^{r+1} + c, 2 \leq r \leq m-1, 1 \leq c \leq 2^r - 2$ 。

根据 Chan-Games 算法的递归过程可知, $\underline{s}^{(n)}$ 的 4-错线性复杂度为 $2^{n-1} + 2^{n-2} + \dots + 2^{m+1} + 2^m - 2^{r+1} + c = 2^n - 2^m - 2^{r+1} + c (2 \leq r \leq m-1, 1 \leq c \leq 2^r - 2)$ 。

情形 3 $W_{2^n}(\underline{s}) = W(\underline{s}^{(n)}) > 4$ 且 $W(\underline{s}^{(m+1)}) \leq 4$

设 r 是使得 $W(\underline{s}^{(r)}), m+1 \leq r \leq n-1$, 至多为 4 的最大整数, 由 $W(\underline{s}^{(m+1)}) \leq 4$ 知这样的 r 是存在的。令 $W(\underline{s}^{(r)}) = b$, 由 φ_n 的性质 $P3$ 知 $b = 4$ 或 2 。设 $a^{(n)}$ 是由 $\underline{s}^{(n)}$ 改变 b bit 得到的向量, 类似 $\underline{s}^{(t)}$, 定义 $a^{(t)} = (a_0^{(t)}, a_1^{(t)}, \dots, a_{2^t-1}^{(t)}), m+1 \leq t \leq n$, 则向量 $a^{(t)}$ 和 $\underline{s}^{(t)}$ 至多相差 b bit, 且对于整数 $j, r < j < n$, 都有 $L(a^{(j+1)}) \neq R(a^{(j+1)})$, 则 $LC_{2^n,4} > 2^{n-1} + 2^{n-2} + \dots + 2^{r+1}$ 。

如果改变 $\underline{s}^{(n)}$ 中至多 b bit 使得 $\underline{s}^{(r)}$ 变成 0 , 即 $L(a^{(r+1)}) = R(a^{(r+1)})$, 则 $a^{(n)}$ 的线性复杂度形式如下: $L'_{r,c} = 2^{n-1} + 2^{n-2} + \dots + 2^{r+1} + c, 0 \leq c \leq 2^r$, 其中 $c = LC(L(a^{(r+1)}))$ 。

如果 $L(a^{(r+1)}) \neq R(a^{(r+1)})$, 即 $a^{(r)}$ 是非零向量, 则 $a^{(n)}$ 的线性复杂度 LC' 满足 $LC' > 2^{n-1} + 2^{n-2} + \dots + 2^{r+1} + 2^r \geq L'_{r,c}$, 而 $LC_{2^n,4}(s)$ 是 $\underline{s}^{(n)}$ 中改变 b bit 所得到的最小的线性复杂度, 因此 $LC_{2^n,4}(s) = L'_{r,c}$ 。其中 c 是由 $\underline{s}^{(n)}$ 改变后得到的最小的线性复杂度。不妨设 $a^{(n)}$ 是由 $\underline{s}^{(n)}$ 改变 b bit 后所得到的线性复杂度最小的向量。

下面证明 $c \leq 2^r - 2, c \neq 2^r - 2^m - 1$ 。

设 $\underline{s}^{(r)} = (0, \dots, \underbrace{1}_{u_1}, \dots, \underbrace{1}_{u_2}, \dots, \underbrace{1}_{u_b}, \dots, 0)$, 即 $s_{u_1}^{(r)} = s_{u_2}^{(r)} = \dots = s_{u_b}^{(r)} = 1, 0 \leq u_1 \leq u_2 \leq \dots \leq u_b \leq 2^r - 1$, 且 $s_j^{(r)} = 0, 0 \leq j \leq 2^r - 1, j \neq u_1, u_2, \dots, u_b$ 。

由 $\underline{s}^{(r)} = \varphi_{r+1}(\underline{s}^{(r+1)})$, 有

$$\begin{cases} s_{u_1}^{(r+1)} + s_{u_1+2^r}^{(r+1)} = 1 \\ \dots \\ s_{u_b}^{(r+1)} + s_{u_b+2^r}^{(r+1)} = 1 \end{cases} \quad (2)$$

$$s_j^{(r+1)} = s_{j+2^r}^{(r+1)}, 0 \leq j \leq 2^r - 1, j \neq u_1, u_2, \dots, u_b。$$

可以适当改变 $s_{u_1}^{(r+1)}, s_{u_2}^{(r+1)}, \dots, s_{u_b}^{(r+1)}, s_{u_1+2^r}^{(r+1)}, s_{u_2+2^r}^{(r+1)}, \dots, s_{u_b+2^r}^{(r+1)}$ 中的 b bit 来保证式 (2) 中的 b 个等式变成 0, 同时使得 $a_0^{(r+1)} + a_2^{(r+1)} + \dots + a_{2^r-2}^{(r+1)} = 0, a_1^{(r+1)} + a_3^{(r+1)} + \dots + a_{2^r-1}^{(r+1)} = 0$ 。由引理 3 可知, $c = LC(L(\underline{a}^{(r+1)})) \leq 2^r - 2$ 。

假设 $c = LC(L(\underline{a}^{(r+1)})) = 2^r - 2^m - 1$, 对 $L(\underline{a}^{(r+1)})$ 执行 Chan-Games 算法来计算其线性复杂度。设 $\underline{b}^{(r)} = L(\underline{a}^{(r+1)}), b_t = \varphi_{t+1} \cdots \varphi_r(\underline{b}^{(r)}), m+1 \leq t \leq r-1$, 且 $\underline{b}^{(m+1)} = (b_0^{(m+1)}, b_1^{(m+1)}, \dots,$

$b_{2m+1-1}^{(m+1)}$ 。则 $L(\underline{b}^{(t)}) \neq R(\underline{b}^{(t)}), m+2 \leq t \leq r-1, L(\underline{b}^{(m+1)}) = R(\underline{b}^{(m+1)})$, 且 $LC(L(\underline{b}^{(m+1)})) = 2^m - 1$ 。

由于 $\underline{b}^{(r)}$ 是 $L(\underline{a}^{(r+1)})$ 在位置 $u_1, u_2, \dots, u_b$ 改变得到的。此时 $R(\underline{s}^{(r+1)})$ 作相应的变化可使得 $\underline{s}^{(r)}$ 变成 0。当 $b=4$ 时, 因为 $W(\underline{s}^{(i)}) = 4, m+1 \leq i \leq r$, 且 $\underline{s}^{(m)} = \varphi_{m+1} \cdots \varphi_r(\underline{s}^{(r)}) = 0$, 则 $u_1 \equiv u_3 + 2^m \bmod 2^{m+1}, u_2 \equiv u_4 + 2^m \bmod 2^{m+1}$ (当然还有其他的表示形式, 此处只列出这一种形式, 其他形式结果相同)。

$b_{u_1 \bmod 2^{m+1}}^{(m+1)}, b_{u_2 \bmod 2^{m+1}}^{(m+1)}$ 与 $b_{u_3 \bmod 2^{m+1}}^{(m+1)}, b_{u_4 \bmod 2^{m+1}}^{(m+1)}$ 分别属于 $L(\underline{b}^{(m+1)})$ 与 $R(\underline{b}^{(m+1)})$ 。因此适当改变 $b_{u_1 \bmod 2^{m+1}}^{(m+1)}, b_{u_2 \bmod 2^{m+1}}^{(m+1)}, b_{u_3 \bmod 2^{m+1}}^{(m+1)}, b_{u_4 \bmod 2^{m+1}}^{(m+1)}$ 来保证

$$\begin{cases} b_{u_1 \bmod 2^{m+1}}^{(m+1)} + b_{u_3 \bmod 2^{m+1}}^{(m+1)} = 0 \\ b_{u_2 \bmod 2^{m+1}}^{(m+1)} + b_{u_4 \bmod 2^{m+1}}^{(m+1)} = 0 \end{cases}, \text{同时使}$$

得 $\begin{cases} b_0^{(m+1)} + b_2^{(m+1)} + \cdots + b_{2^m-2}^{(m+1)} = 0 \\ b_1^{(m+1)} + b_3^{(m+1)} + \cdots + b_{2^m-1}^{(m+1)} = 0 \end{cases}$, 由引理 3 可知 $LC(L(\underline{b}^{(m+1)})) \leq 2^m - 2$ 与 $LC(L(\underline{b}^{(m+1)})) = 2^m - 1$ 矛盾, 故 $c \neq 2^r - 2^m - 1$ 。当 $b=2$ 时, 类似讨论也有 $c \neq 2^r - 2^m - 1$ 。

综上: 当 $W_{2n}(\underline{s}) = W(\underline{s}^{(n)}) > 4, W(\underline{s}^{(m+1)}) \leq 4$ 时, $LC_{2n,4}(\underline{s})$ 形如 $L'_{r,c} = 2^{n-1} + 2^{n-2} + \cdots + 2^{r+1} + c = 2^n - 2^{r+1} + c, 1 \leq c \leq 2^r - 2, c \neq 2^r - 2^m - 1$ 。

定理 2 设 $\underline{s} = (s_0, s_1, \dots, s_{2n-1})$, 则满足线性复杂度为 $2^n - 2^m - 1$, 且 $W_{2n}(\underline{s}) = W(\underline{s}^{(n)}) > 4, W(\underline{s}^{(m+1)}) > 4$ 的 2^n -周期二元序列的条数为 $2^{2n-2m-2r+1+c+2r-1}$, 其中 $2 \leq r \leq m-1, 1 \leq c \leq 2^r - 2$ 。

证明 由定理 1 情形 2 的证明过程可知, $LC(L(\underline{s}^{(m+1)})) = 2^m - 1, LC_{2n,2}(L(\underline{s}^{(m+1)})) = 2^m - 2^{r+1} + c, 2 \leq r \leq m-1, 1 \leq c \leq 2^r - 2$, 由引理 4 可知满足该条件的序列的个数为 $2^{2m-2r+1+c+2r-1}$ 。再由映射 φ_n 的性质 P3, 满足 $LC(\underline{s}) = 2^n - 2^m - 1$ 且 $W_{2n}(\underline{s}) = W(\underline{s}^{(n)}) > 4, W(\underline{s}^{(m+1)}) > 4$ 的 2^n -周期二元序列的条数为 $2^{2n-1+2n-2+\cdots+2m+1+2m-2r+1+c+2r-1} = 2^{2n-2m-2r+1+c+2r-1}, 2 \leq r \leq m-1, 1 \leq c \leq 2^r - 2$ 。

例 1 设 $n=4, m=2$, 求线性复杂度为 $2^n - 2^m - 1 = 11$ 的 2^n -周期二元序列 $s = (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$ 的

4-错线性复杂度。

因 $W(\underline{s}) = W(\underline{s}^{(4)}) = 8 > 4$ 且 $W(\underline{s}^{(2)}) = 4$, 利用定理 1 情形 3 的结论知 $1 \leq LC_4(\underline{s}) \leq 6, LC_4(\underline{s}) \neq 3$ 。计算得 $LC_4(\underline{s}) = 6$, 与情形 3 的结论相符合。

3 结束语

本文给出了 F_2 上线性复杂度为 $2^n - 2^m - 1$ 的 2^n -周期二元序列 $\underline{s}$ 的 4-错或 5-错线性复杂度的表示形式, 并在此基础上给出了特定重量下序列的条数。序列的期望和方差对流密码稳定性也起到了重要的作用, 有待于进一步研究。

参考文献:

- [1] DING Cun-sheng, XIAO Guo-zhen. The stability theory of stream ciphers [M]. Berlin: Springer-Verlag, 1991.
- [2] STAMP M, 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, SAKATA T, et al. A relationship between linear complexity and k -error linear complexity [J]. IEEE Trans on Information Theory, 2000, 46(2): 694-698.
- [4] MEIDL W. On the stability of 2^n -periodic binary sequences [J]. IEEE Trans on Information Theory, 2005, 51(3): 1151-1155.
- [5] ZHU Feng-xiang, QI Wen-feng. The 2-error linear complexity of 2^n -periodic binary sequences with linear complexity $2^n - 1$ [J]. Journal of Electronics, 2007, 24(3): 390-395.
- [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.
- [7] GAMES R A, CHAN A H. A fast algorithm for determining the complexity of a binary sequence with period 2^n [J]. IEEE Trans on Information Theory, 1983, 29(1): 144-146.
- [8] FU Fang-wei, NIEDERREITER H, SU Ming. The characterization of 2^n -periodic binary sequences with fixed 1-error linear complexity [C]//Proc of SETA. Berlin: Springer, 2006: 88-103.

(上接第 1103 页)

4 结束语

本文的网络安全评估方法能定期地对网络系统进行安全扫描, 分析扫描结果, 帮助系统管理员更有效地管理整个网络系统。实验结果表明, 该方法能够直观地给出漏洞、主机和整个网络系统三个层次的脆弱性指数评估值, 使管理员及时地了解系统安全动态, 查找安全变化的原因, 调整安全策略, 从而保证系统的安全。而且该方法具有很好的扩展性, 可以适应对国家级公共基础网络或者运营商网络等大规模复杂网络脆弱性综合分析的需要。

参考文献:

- [1] SWILER L P, PHILLIPS C, ELLIS D, et al. Computer-attack graph generation tool [C]//Proc of DARPA Information Survivability Conference and Exposition. [S. l.]: IEEE Computer Society, 2001: 1307-1321.
- [2] SWILER L P, PHILLIPS C, GAYLOR T. A graph-based network-

vulnerability analysis system, SAND97-3010/1 [R]. California: Sandia National Laboratories, 1998.

- [3] JAJODIA S, NOEL S. Topological vulnerability analysis: a powerful new approach for network attack prevention, detection, and response [M]//Algorithm, Architectures and Information Systems Security. New Jersey: World Scientific, 2009: 285-305.
- [4] OU Xin-ming. A logic-programming approach to network security analysis [D]. Princeton: Princeton University, 2005.
- [5] LIPPMANN R P, INGOLS K W, SCOTT C, et al. Evaluating and strengthening enterprise network security using attack graphs, ESC-TR-2005-064 [R]. [S. l.]: Lincoln Laboratory, MIT, 2005.
- [6] 张海霞, 连一峰, 苏璞睿, 等. 基于安全状态域的网络评估模型 [J]. 软件学报, 2009, 20(2): 451-461.
- [7] CHAMBERS J T, THOMPSON J W. The common vulnerability scoring system: final report and recommendations by the council [R]. [S. l.]: National Infrastructure Advisory Council, 2004.
- [8] MELL P. The common vulnerability scoring system (CVSS) and its applicability to federal agency systems [R]. [S. l.]: NIST, 2007.