

多重周期二元序列的联合 k 错 2-adic 复杂度

董丽华 胡予濮 曾 勇

(西安电子科技大学计算机网络与信息安全国家教育部重点实验室 西安 710071)

摘 要 具有较强密码学性质的序列应该具有较大的 2-adic 复杂度,以抗击已知的带进位操作反馈移位寄存器综合算法,同时改变较少的几项也不应引起序列的 2-adic 复杂度的急剧减小,即 k 错 2-adic 复杂度也应尽可能地大. 近来,向量化流密码的设计逐渐成为国内外密码学界关注的一个重要方向. 对这种类型的流密码的安全性分析需要研究多重序列-有限多个序列的并行流的复杂度. 目前对多重序列的复杂度研究多集中于线性复杂度. 基于此,文中首先给出了多重二元序列的联合 k 错 2-adic 复杂度的定义. 随后,借助数论中的中国剩余定理等相关理论给出了联合 k 错 2-adic 复杂度的下界,并讨论了具有最大联合 2-adic 复杂度以及较大联合 k 错 2-adic 复杂度的 N 周期序列的存在性及具有此种性质的序列的数目下界. 以此种周期序列作为密钥流序列可以有效抵抗穷举攻击.

关键词 密码学;流密码;FCSR;联合 2-adic 复杂度; k 错 2-adic 复杂度

中图法分类号 TP309 **DOI 号**: 10.3724/SP.J.1016.2009.01134

Joint k -Error 2-Adic Complexity for Binary Periodic Multi-Sequences

DONG Li-Hua HU Yu-Pu ZENG Yong

(Key Laboratory of Computer Networks and Information Security of Ministry of Education, Xidian University, Xi'an 710071)

Abstract Cryptographically strong sequences should have a large 2-adic complexity to thwart the known feedback with carry shift register synthesis algorithms. At the same time the change of a few terms should not cause a significant decrease of the 2-adic complexity, that is, the k -error 2-adic complexity should also be large. Recent developments in stream ciphers point towards an interest in word-based stream ciphers, which require the study of the complexity of multi-sequences. This paper introduces joint k -error 2-adic complexity measures for multi-sequences. Several results on the existence and lower bounds on the number of multi-sequences with maximal joint 2-adic complexity and large joint k -error 2-adic complexity are proved. The existence of many such sequences thwarts attacks against the keystreams by exhaustive search.

Keywords cryptography; stream cipher; FCSR; joint 2-adic complexity; k -error 2-adic complexity

1 引 言

在新一代的移动通信系统中,巨大的信息吞吐量需要安全快速的信息加密体制,如流密码和分组

密码. 传统的基于线性反馈移位寄存器 (LFSR) 的序列密码易受攻击,近年来出现了一些新型的序列密码设计部件,诸如 T 函数、NLFSR,带进位操作的反馈移位寄存器(FCSR)等等. 其中 FCSR 自 Klapper 与 Goresky 于文献[1]中引入之后已引起密码学界

的广泛关注. FCSR 序列与 LFSR 序列平行的一些基本性质包括周期、有理表达式、指数表达式和有理近似算法等^[2-5]得到了广泛的讨论.

最近几年,国内外学者纷纷注意到序列的线性复杂度在极小的扰动下也可能是极不稳定的,因而相继引入了球体复杂度、 k 错线性复杂度等概念,并作了大量的相关研究工作. 特别的文献[6-8]对具有最大线性复杂度以及接近周期的 k 错线性复杂度的周期序列的存在性进行了研究,给出了此种周期序列的数目下界. 在对 FCSR 序列的研究过程中,文献[9]的作者指出了序列的 2-adic 复杂度测度具有同样的不稳定性,例如, N 周期序列 $\mathbf{S} = (1, 0, \dots, 0)^\infty$ 或 $(0, 1, \dots, 1)^\infty$ 具有最大的 2-adic 复杂度 $\log_2(2^N - 1)$; 然而,若序列 \mathbf{S} 的每个周期改变一个比特,其 2-adic 复杂度将退化为 0. 进而只要知道有限个比特就可以有效地重构初始序列. 基于此,文献[9]的作者首先给出了 k 错 2-adic 复杂度的概念. 随后,胡红刚^[10]等学者给出了周期序列的 k 错 2-adic 复杂度以及 k 错对称 2-adic 复杂度的一个下界. 在文献[11]中我们给出了计算周期为 2^n 的二元序列的 2-adic 复杂度综合算法,并以该算法为基础,给出了一个计算周期为 2^n 的二元序列的 k 错 2-adic 复杂度综合算法. 在文献[12]中我们证明了具有最大 2-adic 复杂度以及较大 k 错 2-adic 复杂度的 N 周期序列的存在性,给出了具有这种性质的周期序列的数目的下界.

当前,向量化流密码的设计已逐渐成为国内外密码学界关注的一个重要方向. 对这种类型的流密码的安全性分析需要研究多重序列-有限多个序列的并行流的复杂度. 在文献[13]中,Meidl 与 Niederreiter 首先建立了多重序列的 k 错线性复杂度理论,随后, Niederreiter 与 Venkateswarlu^[14]进一步讨论了具有较大 k 错线性复杂度的多重序列的存在性以及具有此性质的序列的个数的下界. 胡红刚等学者则首先确定了二元周期多重序列的联合 2-adic 复杂度的期望值并给出了二元周期多重序列的联合对称 2-adic 复杂度的期望值的一个下界^[15].

目前对多重周期序列的 k 错 2-adic 复杂度的研究尚未见公开报导,本文将首先给出多重周期二元序列的联合 k 错 2-adic 复杂度的一个定义,随后使用数论中的相关理论给出了联合 k 错 2-adic 复杂度的下界,并讨论了具有最大联合 2-adic 复杂度以及较大联合 k 错 2-adic 复杂度的 N 周期序列的存在性及具有此种性质的序列的数目下界. 文中的结果

对对称密码学^[16]中 FCSR 理论的发展将起到极大的促进作用. 这里的代数运算不再是逐比特加而是有限比特串的 2-adic 加法. 由于 $2^j + 2^j = 2^{j+1}$, 2-adic 加法将溢出比特进位到高阶项.

2 基本概念

任意给定一个二元序列 $\mathbf{S} = s_0, s_1, s_2, \dots$ 在 2-adic 整数环 \mathbb{Z}_2 中总可以找到与之相匹配的 2-adic 数 $\alpha = s_0 + s_1 2 + \dots + s_{N-1} 2^{N-1} + \dots$ ^[3]. 特别地,若序列 \mathbf{S} 是具有最小周期 N 的严格周期序列,则

$$\alpha = -\frac{\sum_{i=0}^{N-1} s_i 2^i}{2^N - 1} = -\frac{\mathbf{S}^N(2)}{2^N - 1} \quad (1)$$

通过约减,可得到 α 的最简分数为 $-p/q$, 其中 q 是正整数且 $0 \leq p \leq q$. 同时可知序列 \mathbf{S} 的周期是使得 $2^t \equiv 1 \pmod{q}$ 成立的最小正整数 t , 而 q 则为生成该二元序列 \mathbf{S} 的最小 FCSR 的联结整数^[2].

定义 1^[2]. 若记与周期二元序列 $\mathbf{S} = s_0, s_1, s_2, \dots$ 相对应的 2-adic 数的最简分数为 $-p/q$, 则序列 \mathbf{S} 的 2-adic 复杂度 $\lambda_2(\mathbf{S})$ 为实数 $\log_2(\max(p, q))$.

结论 1^[2]. 若序列 \mathbf{S} 是全零序列, 则令 $\lambda_2(\mathbf{S}) = 0$.

结论 2^[2]. 若序列 \mathbf{S} 是最小周期为 $N \geq 2$ 的严格周期序列, 则

$$\lambda_2(\mathbf{S}) = \log_2 q = \log_2((2^N - 1) / \gcd(\mathbf{S}^N(2), 2^N - 1)) \quad (2)$$

序列的 k 错 2-adic 复杂度可以简要定义如下.

定义 2. N 周期二元序列 \mathbf{S} 的 k 错 2-adic 复杂度定义为

$$\lambda_{N,k}(\mathbf{S}) = \min_{\{per(\mathbf{T})=N, d(\mathbf{S}, \mathbf{T}) \leq k\}} \lambda(\mathbf{T}).$$

k 错 2-adic 复杂度的定义类似于 k 错线性复杂度. 其中函数 $per(\mathbf{T}) = N$ 表示序列 \mathbf{T} 的最小周期为 N , 而函数 $d(\mathbf{S}, \mathbf{T}) \leq k$ 则表示向量 $(t_0, t_1, \dots, t_{N-1})$ 与 $(s_0, s_1, \dots, s_{N-1})$ 的汉明距离至多为 k . 因而 k 错 2-adic 复杂度 $\lambda_{N,k}(\mathbf{S})$ 是所有 N 周期序列 \mathbf{T} 的 2-adic 复杂度的最小值, 而这些 N 周期序列是由序列 \mathbf{S} 在每个周期中改变至多 k 项得到的.

设 $\mathbf{S} = (S_1, S_2, \dots, S_m)$ 为 $\text{GF}(2)$ 上的一个 m 重序列, 其分量序列 $S_u = (s_{u,0}, s_{u,1}, \dots, s_{u,N-1})^\infty$ 为 $\text{GF}(2)$ 上的 N 周期序列, $u = 1, 2, \dots, m$. 这里我们需要注意的是 N 周期指的是序列的一个周期长度为 N , 但没有必要是最小周期长度. 由文献[14]知道序列 \mathbf{S} 的联合 2-adic 复杂度为 $\log_2(\text{lcm}(q_1, q_2, \dots,$

$q_m))$, 这里 $-p_1/q_1, -p_2/q_2, \dots, -p_m/q_m$ 分别是其分量序列 S_1, S_2, \dots, S_m 的最简分式. 另外, 我们知道 $q = \text{lcm}(q_1, q_2, \dots, q_m)$

$$\begin{aligned} &= \text{lcm}\left(\frac{2^N-1}{\text{gcd}(2^N-1, S_1^N(2))}, \dots, \frac{2^N-1}{\text{gcd}(2^N-1, S_m^N(2))}\right) \\ &= \frac{2^N-1}{\text{gcd}(2^N-1, S_1^N(2), \dots, S_m^N(2))}. \end{aligned}$$

因而

$$\begin{aligned} \lambda_2(S_1, S_2, \dots, S_m) &= \log_2(\text{lcm}(q_1, q_2, \dots, q_m)) \\ &= \log_2(2^N-1) - \\ &\quad \log_2(\text{gcd}(2^N-1, S_1^N(2), \dots, S_m^N(2))). \end{aligned}$$

在下文中, m 重周期序列 S 的一项指的是其某个分量序列 $S_j (1 \leq j \leq m)$ 的一项.

定义 3. 设 $S = (S_1, S_2, \dots, S_m)$ 与 $T = (T_1, T_2, \dots, T_m)$ 为 $\text{GF}(2)$ 上的两个有限长度的 m 重序列, 我们定义序列 S 与 T 的项距 $d_T(S, T)$ 为序列 S 与序列 T 中对应项不相同的个数.

定义 4. 设 $S = (S_1, S_2, \dots, S_m)$ 为 $\text{GF}(2)$ 上的 m 重 N 周期二元序列, 则对于某整数 $k, 0 \leq k \leq mN$, 序列 S 的联合 k 错 2-adic 复杂度 $\lambda_{N,k}(S)$ 是对序列 S 的每个周期的 N 项改变至多 k 项后得到的所有 N 周期序列 T 的联合 2-adic 复杂度的最小值, 即

$$\lambda_{N,k}(S) = \min_{\{per(T)=N, d_T(S,T) \leq k\}} \lambda_2(T).$$

3 具有较大联合 k 错 2-adic 复杂度的多重周期序列

接下来的叙述中, 称单序列 S 的一个周期中由第 t 个比特开始的“0”游程的长度为 r 是指由“ $s_t s_{t+1} \dots s_{t+r-2} s_{t+r-1}$ ”所对应的比特串为“00...01”, 另设 2^N-1 有如下分解

$$2^N-1 = \prod_{i=1}^h p_i^{m_i}, \quad p_1 < p_2 < \dots < p_h.$$

定理 1. 对于任意的 m 重 N 周期二元序列 $S = (S_1, S_2, \dots, S_m)$ 及任意的满足 $1 \leq k \leq mN$ 的 k , 我们有

$$\lambda_{N,k}(S) \leq \min\{N - \lceil \log_2(W) \rceil, \lambda_2(S)\},$$

这里

$$\begin{aligned} W = \max \Big\{ & Q = \prod_{i=1}^h p_i^{k_i} : 0 \leq k_i \leq m_i, \\ & \sum_{u=1}^m r_u + m \lceil \log_2(Q) \rceil \leq k \Big\}, \end{aligned}$$

其中, r_u 是序列 S_u 的一个在周期中由第 $\lceil \log_2(Q) \rceil$ 个

比特开始的“0”游程的长度.

证明. 对于任意的 N 周期单序列 $S_u = (s_{u,0}, s_{u,1}, \dots, s_{u,N-1})^\infty$, 在 2-adic 整数环 Z_2 中总可以找到与之相对应的 2-adic 数 α , 即

$$\begin{aligned} \alpha &= s_{u,0} + s_{u,1} \cdot 2 + \dots + s_{u,N-1} \cdot 2^{N-1} + s_{u,N} \cdot 2^N + \dots \\ &= -\frac{\sum_{i=0}^{N-1} s_{u,i} \cdot 2^i}{2^N-1} = -\frac{S_u^N(2)}{2^N-1}. \end{aligned}$$

进而可以找到某个小于 Q 的整数 w_u , 使得

$$S_u^N(2) \equiv w_u \pmod{Q}, \text{ 这里 } Q = \prod_{i=1}^h p_i^{k_i} \text{ 而 } 0 \leq k_i \leq m_i, 1 \leq u \leq m. \text{ 而 } w_u \text{ 的 2-adic 展开式中非零项的数目应不大于 } \lceil \log_2(Q) \rceil, 1 \leq u \leq m.$$

对于 $1 \leq u \leq m$, 设对某整数 l 有

$$T_u^N(2) := S_u^N(2) - w_u = lQ,$$

那么在 2-adic 整数环 Z_2 中可以找到某个序列 $T_u := (t_{u,0}, t_{u,1}, \dots, t_{u,N-1})^\infty$, 使得

$$\begin{aligned} \beta &= t_{u,0} + t_{u,1} \cdot 2 + \dots + t_{u,N-1} \cdot 2^{N-1} + t_{u,N} \cdot 2^N + \dots \\ &= -\frac{\sum_{i=0}^{N-1} t_{u,i} \cdot 2^i}{2^N-1} = -\frac{T_u^N(2)}{2^N-1}. \end{aligned}$$

那么显然可以通过改变序列 S_u 中至多 $r_u + \lceil \log_2(Q) \rceil$ 个比特而得到序列 T_u , 这里 r_u 是序列 S_u 的一个周期中由第 $\lceil \log_2(Q) \rceil$ 个比特开始的“0”游程的长度, $1 \leq u \leq m$. 同时 m 重 N 周期二元序列 T 与 S 的每个周期中至多有 $\sum_{u=1}^m r_u + m \lceil \log_2(Q) \rceil \leq k$ 个不同项, 即 $d_T(S, T) \leq k$.

再者, 对于 $1 \leq u \leq m$ 有 $T_u^N(2)$ 被 Q 整除, 因而 $\text{gcd}(T_1^N(2), \dots, T_m^N(2), 2^N-1) \geq Q$.

进而 m 重 N 周期二元序列 T 的 2-adic 复杂度满足

$$\begin{aligned} \lambda_2(T) &= \log_2((2^N-1)/\text{gcd}(T_1^N(2), \dots, T_m^N(2), \\ &\quad 2^N-1)) \leq N - \lceil \log_2(Q) \rceil. \end{aligned}$$

由于 $d_T(S, T) \leq k$, 通过最大化 Q , 可以得到 m 重 N 周期二元序列 S 的联合 k 错 2-adic 复杂度 $\lambda_{N,k}(S)$ 满足

$$\lambda_{N,k}(S) \leq \min\{N - \lceil \log_2(W) \rceil, \lambda_2(S)\}. \quad \text{证毕.}$$

对于每个 $1 \leq u \leq m$, 考虑如下同余方程组

$$S_u^N(2) \equiv s_i^{(u)}(2) \pmod{p_i^{m_i}}, \quad 1 \leq i \leq h \quad (3)$$

这里 $s_i^{(u)}(2)$ 是给定的整数. 对于任意选定的 $s_i^{(u)}(2), 1 \leq i \leq h$, 由中国剩余定理可以得到唯一的一个满足式 (3) 的整数 $S_u^N(2)$, 使得 $\log_2(S_u^N(2)) < N$.

设 $s_i(2) = (s_i^1(2), \dots, s_i^m(2))$, 利用式 (3), 我们

有 $\mathbf{S}^{(N)}(2) \equiv \mathbf{s}_i(2) \pmod{p_i^{m_i}}, 1 \leq i \leq h$.

这里同余式是逐分量成立的. 因而 m 重 N 周期二元序列 \mathbf{S} 与其向量组 $\mathbf{s}_i(2) (1 \leq i \leq h)$ 一一对应. 下面我们总是假设两个向量之间的同余关系是逐分量成立的.

定理 2. 与 2-adic 展开式中非零项的数目不大于 k 的 m 重 N 周期二元序列相对应的所有整数向量 \mathbf{f} 构成的集合为 $P(N, k)$, 且设 $M = |P(N, k)|$. 那么满足 $\lambda_2(\mathbf{S}) = \log_2(2^N - 1)$ 且 $\lambda_{N,k}(\mathbf{S}) \geq \log_2\left((2^N - 1) \prod_{i=1}^h p_i^{k_i}\right)$ 的 m 重 N 周期二元序列 \mathbf{S} 的数目至少为

$$\prod_{\substack{i=1 \\ l_i \neq m_i}}^h p_i^{m(m_i - l_i - 1)} (p_i^{m(l_i + 1)} - (l_i + 1)^m - M) \times \prod_{\substack{i=1 \\ l_i = m_i}}^h p_i^{m(m_i - 1)} (p_i - 1)^m.$$

证明. 令 \mathbf{V}_i^l 为分量小于 p_i^{l+1} 的 m 维向量构成的集合, 则该集合中对 p_i 取模之后不为零的向量的数目为 $p_i^{m(l+1)} - (l+1)^m$.

如果存在某个整数 $0 \leq l_i < m_i$ 使得 $M < p_i^{m(l_i + 1)} - (l_i + 1)^m$, 则在集合 \mathbf{V}_i^l 中我们可以找到满足如下条件的整数向量 \mathbf{g}_i :

$\mathbf{g}_i \not\equiv \mathbf{0} \pmod{p_i}$ 同时对于所有的 $\mathbf{f} \in P(N, k)$, 有

$$\mathbf{g}_i \not\equiv \mathbf{f} \pmod{p_i^{l_i + 1}},$$

其中 $0 \leq i \leq h$.

如果 $l_i = m_i$, 则我们必定可以找到一个满足条件 $\mathbf{g}_i \not\equiv \mathbf{0} \pmod{p_i}$ 的整数向量.

令 $\mathbf{s}_i(2) = \mathbf{g}_i$, 则利用中国剩余定理求解同余方程组 $\mathbf{S}^{(N)}(2) \equiv \mathbf{s}_i(2) \pmod{p_i^{m_i}}, 1 \leq i \leq h$, 可以得到唯一的一个 m 重 N 周期二元序列 \mathbf{S} . 由于对于所有的 $i (0 \leq i \leq h)$, 有 $\mathbf{S}^N(2) \not\equiv \mathbf{0} \pmod{p_i}$, 因而 m 重 N 周期二元序列 \mathbf{S} 的联合 2-adic 复杂度为 $\log_2(2^N - 1)$.

设 \mathbf{T} 为任意的一个满足 $d_T(\mathbf{S}, \mathbf{T}) \leq k$ 的 m 重 N 周期二元序列, 则存在某个向量 $\mathbf{f} \in P(N, k)$, 使得 $\mathbf{T}^N(2) = \mathbf{S}^N(2) - \mathbf{f}$. 如果存在某个整数 i 使得 $0 \leq l_i < m_i$, 则有

$$\mathbf{T}^N(2) = \mathbf{S}^N(2) - \mathbf{f} \not\equiv \mathbf{0} \pmod{p_i^{l_i + 1}}.$$

否则 $\mathbf{s}_i(2) \equiv \mathbf{f} \pmod{p_i^{l_i + 1}}$. 这与 $\mathbf{s}_i(2)$ 的选择标准相矛盾. 进而表明

$$\gcd(T_1^N(2), \dots, T_m^N(2), 2^N - 1) \leq \prod_{i=1}^h p_i^{l_i}.$$

故有 $\lambda_2(\mathbf{T}) \geq \log_2\left((2^N - 1) \prod_{i=1}^h p_i^{l_i}\right)$, 即

$$\lambda_{N,k}(\mathbf{S}) \geq \log_2\left((2^N - 1) \prod_{i=1}^h p_i^{l_i}\right).$$

接下来我们计算一下满足条件的 $\mathbf{s}_i(2) (0 \leq i \leq h)$ 的数目. 对于任意的对应于 m 重 N 周期二元序列 \mathbf{S} 的整数向量 $\mathbf{S}^{(N)}(2)$, 有同余方程组

$$\mathbf{S}^{(N)}(2) \equiv \mathbf{s}_i(2) \pmod{p_i^{m_i}}, 1 \leq i \leq h,$$

这里 $\mathbf{s}_i(2)$ 的分量是小于 $p_i^{m_i}$ 的整数.

如果 $l_i = m_i$, 则可以令 $\mathbf{s}_i(2) = \mathbf{g}_i + p_i \mathbf{e}_i$, 这里 \mathbf{e}_i 是分量小于 $p_i^{m_i - 1}$ 的整数向量. 在这种情形下, $\mathbf{s}_i(2)$ 有 $p_i^{m(m_i - 1)} (p_i - 1)^m$ 种选择.

否则, 即若 $l_i \neq m_i$, 则可以令 $\mathbf{s}_i(2) = \mathbf{g}_i + p_i^{l_i + 1} \mathbf{e}_i$, 这里 \mathbf{e}_i 是分量小于 $p_i^{m_i - l_i - 1}$ 的整数向量. 在这种情形下, $\mathbf{s}_i(2)$ 有 $p_i^{m(m_i - l_i - 1)} (p_i^{m(l_i + 1)} - (l_i + 1)^m - M)$ 种选择.

因而满足条件的 $\mathbf{s}_i(2) (0 \leq i \leq h)$ 的数目至少为

$$\prod_{\substack{i=1 \\ l_i \neq m_i}}^h p_i^{m(m_i - l_i - 1)} (p_i^{m(l_i + 1)} - (l_i + 1)^m - M) \times \prod_{\substack{i=1 \\ l_i = m_i}}^h p_i^{m(m_i - 1)} (p_i - 1)^m.$$

因而结论成立.

证毕.

4 结 论

文中给出了 m 重 N 周期二元序列 \mathbf{S} 的联合 k 错 2-adic 复杂度的定义, 联合 k 错 2-adic 复杂度的下界, 并讨论了具有最大联合 2-adic 复杂度以及较大联合 k 错 2-adic 复杂度的 N 周期序列的存在性及具有此种性质的序列的数目下界. 由定理 3 的证明过程知道确实可以构造大量具有最大联合 2-adic 复杂度以及较大联合 k 错 2-adic 复杂度的 m 重 N 周期二元序列, 因而在流密码中使用具有这种性质的周期序列可以有效抗击对密钥流序列的穷举攻击.

参 考 文 献

- [1] Klapper A, Goresky M. 2-adic shift registers//Proceedings of the Fast Software Encryption, Cambridge Security Workshop. LNCS 809. Cambridge, UK: Springer-Verlag, 1994: 174-178

- [2] Klapper A, Goresky M. Feedback shift registers, 2-adic span, and combiners with memory. *Journal of Cryptology*, 1997, 10(2): 111-147
- [3] Klapper A. A survey of feedback with carry shift registers// *Sequences and Their Applications*, SETA 2004. LNCS 3486. Berlin: Springer-Verlag, 2005: 56-71
- [4] Arnault François, Berger Thierry P, Nacer Abdelkadar. Feedback with carry shift registers synthesis with the Euclidean algorithm. *IEEE Transactions on Information Theory*, 2004, 50(5): 910-917
- [5] Klapper A, Xu Jingzhong. Register synthesis for algebraic feedback shift registers based on non-primes. *Designs, Codes and Cryptography*, 2004, 31(3): 227-250
- [6] Niederreiter H. Periodic sequences with large k -error linear complexity. *IEEE Transactions on Information Theory*, 2003, 49(2): 501-505
- [7] Meidl W, Niederreiter H. Periodic sequences with maximal linear complexity and large k -error linear complexity. *Applicable Algebra in Engineering, Communication and Computing*, 2003, 14(4): 273-286
- [8] Niederreiter Harald, Shparlinski Igor E. Periodic sequences with maximal linear complexity and almost maximal k -error linear complexity//*Proceedings of the Cryptography and Coding*, 2003, 2898: 183-189
- [9] Wang Lei, Cai Mian, Xiao Guo-Zhen. On stability of 2-adic complexity of periodic sequence. *Journal of Xidian University*, 2000, 27(3): 348-350(in Chinese)
(王磊, 蔡勉, 肖国镇. 周期序列 2-adic 复杂度的稳定性. 西安电子科技大学学报, 2000, 27(3): 348-350)
- [10] Hu Hong-Gang, Feng Deng-Guo. On the 2-adic complexity and the k -error 2-adic complexity of periodic binary sequences//*Sequence and Its Application*, SETA 2004. LNCS 3486. Berlin: Springer-Verlag, 2005: 185-196
- [11] Dong Li-Hua, Hu Yu-Pu, Zeng Yong. k -error 2-adic complexity algorithm for the binary sequences with period 2^n . *Chinese Journal of Computers*, 2006, 29(9): 1590-1595(in Chinese)
(董丽华, 胡予濮, 曾勇. 周期为 2^n 的二元序列 k 错 2-adic 复杂度算法. 计算机学报, 2006, 29(9): 1590-1595)
- [12] Dong Li-Hua, Hu Yu-Pu, Zeng Yong. Periodic sequences with large 2-adic and k -error 2-adic complexities. *Journal of South China University of Technology*, 2007, 35(5): 86-89 (in Chinese)
(董丽华, 胡予濮, 曾勇. 具有大 2-adic 与 k 错 2-adic 复杂度的周期序列. 华南理工大学学报, 2007, 35(5): 86-89)
- [13] Meidl W, Niederreiter H, Venkateswarlu A. Error linear complexity measures for multi-sequences. *Journal of Complexity*, 2007, 23(2): 169-192
- [14] Niederreiter H, Venkateswarlu A. Periodic multi-sequences with large error linear complexity. *Designs, Codes and Cryptography*, 2008, 49(1-3): 33-45
- [15] Hu Hong-Gang, Hu Lei, Feng Deng-Guo. On the expected value of the joint 2-adic complexity of periodic binary multi-sequences//*Sequence and Its Application*, SETA 2006. LNCS 4086. Berlin: Springer-Verlag, 2006: 199-208
- [16] Rueppel R. *Analysis and Design of Stream Ciphers*. New York: Springer-Verlag, 1986



DONG Li-Hua, born in 1977, Ph.D., lecturer. Her research interests include the design and analysis of stream cipher and pseudorandom sequences.

HU Yu-Pu, born in 1955, professor, Ph.D. supervisor. His research interests include cryptography, computer network and information security.

ZENG Yong, born in 1978, Ph.D.. His research interests focus on wireless network security, network survivability.

Background

This work is supported by a grant from the Major State Basic Research Development Program (973 Program) of China (No. 2007CB311201), by the National Natural Science Foundation of China (Nos. 60473029, 60673072), and by the National Science Fund for Distinguished Young Scholars (No. 60503010). The projects mainly focus on the theory of stream cipher. This research group has published a lot of papers.

In the study of the theory of stream cipher, much atten-

tion has been paid on the stability theory of stream cipher. This theory suggests that good keystream sequences must not only have a large linear complexity, but also a change of a few terms must not cause a significant drop of the linear complexity. This requirement leads to the theory of the k -error linear complexity of keystream sequences of Niederreiter's [2003]. In the study of the Klapper's FCSR sequences, the following fact has also been found. Let $\mathbf{S} = (1, 0, \dots, 0)^\infty$ or $(0, 1, 1, \dots, 1)^\infty$ with period N . Then the 2-adic complexity is

$\log_2(2^N - 1)$. However, after changing 1 bit within every period, the 2-adic complexity becomes 0. For this case, knowledge of the first few bits can allow the efficient generation of a sequence, which closely approximates the original sequence. This observation motivates the study of the k -error 2-adic complexity of sequences. The area of k -error 2-adic complexity was first formally studied by Wang Lei [2000]. Then a lower bound of the k -error 2-adic complexity was given by Hu Hong-Gang [2005].

To respond efficiently considerations, recent developments in stream ciphers point towards an interest in word-based stream ciphers (e. g. , RC4, SNOW and the ECRYPT stream cipher project, etc). The theory of such stream ciphers requires a study of the complexity of multi-sequences, i. e. , of parallel streams of finitely many sequences. In 2007 Meidl and Niederreiter develop a theory of the k -error linear

complexity for multi-sequences. And in 2008 Niederreiter and Venkateswarlu discussed the existence and lower bounds on the number of multi-sequences with large k -error linear complexity. while in 2006, Hu determined the expected value of the joint 2-adic complexity of periodic binary multi-sequences and gave a nontrivial lower bound for the expected value of the joint symmetric 2-adic complexity of periodic binary multi-sequences.

In this paper, the authors introduce joint k -error 2-adic complexity measures for multi-sequences. Several results on the existence and lower bounds on the number of multi-sequences with maximal joint 2-adic complexity and large joint k -error 2-adic complexity are proved. The existence of many such sequences thwarts attacks against the keystreams by exhaustive search.