两类最优跳频序列集的线性复杂度

高军涛[1,2]，胡予濮[1]，李雪莲[3]，向上荣[4]

(1. 西安电子科技大学 计算机网络与信息安全教育部重点实验室，陕西 西安 710071；
2. 中国科学院 软件研究所 信息安全国家重点实验室，北京 100190；
3. 西安电子科技大学 应用数学系，陕西 西安 710071；4. 西安电子科技大学 计算机学院，陕西 西安 710071)

摘 要：利用有限域中的一类不同于幂置换的置换多项式，将两类具有低线性复杂度的跳频序列集变换为具有高线性复杂度的最优跳频序列集。通过理论证明给出了变换以后序列线性复杂度的精确值。所得到的两类新的跳频序列集不仅具有最优的 Hamming 相关值，而且相对于变换前的序列集具有大的线性复杂度，可以抵抗 Berlekamp-Massey 算法的攻击。

关键词：跳频序列；线性复杂度；置换多项式；Hamming 相关

中图分类号：TN918.1 **文献标识码**：A **文章编号**：1000-436X(2012)02-0175-07

Linear complexity of two classes of optimal sets frequency-hopping sequences

GAO Jun-tao[1,2], HU Yu-pu[1], LI Xue-lian[3], XIANG Shang-rong[4]

(1.Key Lab. of Computer Networks and Information Security, Ministry of Education, Xidian University, Xi'an 710071, China;
2. State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing 100190, China;
3. Department of Applied Mathematics, Xidian University, Xi'an 710071, China;
4. School of Computer and Technology, Xidian University, Xi'an 710071, China)

Abstract: By using a type of permutation polynomials which were different from power permutations, the two classes of frequency-hopping sequence sets with low linear complexity was transformed into the ones with high linear complexity. The exact values of linear complexity of these sequences were given by applying the theoretical proof. The results show that the two new classes of frequency-hopping sequences sets not only have optimal Hamming correlation, but also have larger linear span and can resist the Berlekamp-Massey attack compared with the two primary classes of frequency-hopping sequence sets.

Key words: frequency-hopping sequence; linear complexity; permutation polynomial; Hamming correlation

1 引言

跳频(FH)序列在扩频通信和码分多址(CDMA)通信系统中都有广泛的应用。跳频码分多址系统(FH-CDMA)被广泛地应用于蓝牙、雷达系统等方面。在这些系统中，信号接收者面临的主要问题就是信号之间的相互干扰。针对这种情况，人们一般采用具有低 Hamming 相关的跳频序列集来降低干扰，提高系

收稿日期：2010-08-23；**修回日期**：2010-11-14

基金项目：国家自然科学基金重点资助项目（60833008）；国家重点基础研究发展计划（"973"计划）基金资助项目（2007CB311201）；111 计划（B08038）；中央高校基本科研业务费专项基金资助项目（K50511010007）

Foundation Items: The National Natural Science Foundation of China (60833008); The National Basic Research Program of China (973 Program) (2007CB311201); 111 Project (B08038); The Fundamental Research Funds for the Central Universities (K50511010007)

统的性能。除此之外，在实际应用中，特别是在军用系统中，人们不希望自己传送的信息被怀有敌意的人获得或者蓄意干扰。为了抵抗干扰和增加保密性，跳频序列除了应该具有低的 Hamming 相关以外，还应该具有较大的线性复杂度[1]。线性复杂度是衡量序列安全性的一个重要指标。如果一个序列的线性复杂度很低，即使它有大的周期，也很容易受到 Berlekamp-Massey 算法的攻击，因而序列的使用者就没有秘密可言。另一方面，为了降低通信收发双方的实现复杂度，跳频序列的实现应该尽量简单。因此设计实现简单，低 Hamming 相关且高线性复杂度的跳频序列集就具有重要的意义。

当前有许多种类的最优跳频序列集[2~11]，这些跳频序列集有的是用代数方法设计的[2~6]，有的则是用组合数学方法设计的[7~11]。所有这些集合中序列间的 Hamming 相关满足 Lempel-Greenberger 界[12]或 Peng-Fan 界[13]。在这些序列集中有些序列的线性复杂度很小[2~4]，有些序列的线性复杂度仍然没有结论[7~11]，使得这些跳频序列不能应用于保密通信中[14]。虽然当前存在具有高线性复杂度的最优跳频序列集[5,6]，但这些序列集是通过广义 Bent 函数或者多项式环构造的，实现相对比较困难。因此如何将低线性复杂度的最优跳频序列集变换为具有高线性复杂度的最优序列集，同时保证序列实现简单，就成为一个亟待解决的问题。

为了提高跳频序列的线性复杂度，Ding 和 Yin[2]指出人们可以使用有限域中的幂置换[15]将一个具有低线性复杂度的跳频序列集变换为一个具有较高线性复杂度的跳频序列集。在文献[16]中，Wang 研究了三类最优跳频序列集在幂置换下的线性复杂度，指出这三类序列集中序列的线性复杂度在幂置换下可以大幅增加。Wang 同时指出：“除了幂置换以外，其他类型的置换多项式也有可能增加序列的线性复杂度，但计算这些序列线性复杂度的精确值并不容易”。

本文利用有限域中另一类置换多项式$\delta(x)$来提高序列的线性复杂度，通过理论证明给出了置换以后得到的序列线性复杂度的精确值。结果表明，这类置换多项式可以使变换后序列的 Hamming 相关保持最优，而且还大幅度地增加了序列的线性复杂度。因此证明了 Wang 提出的命题，即其他类型的置换多项式也可以提高序列的线性复杂度，得到序列线性复杂度的精确值。本文得到的新型跳频序列集的工程实现是比较简单的，同时具有高的线性复杂度。与现有的具有大线性复杂度的跳频序列集[5,6,16]相比，本文的序列具有如下的优点：①相比于文献[5,6]中最优跳频序列集，我们这类序列集的实现更为简单。②与文献[16]中幂置换后的最优跳频序列集相比，本文给出的新型最优跳频序列集的实现复杂度与幂置换后序列的实现复杂度相当，而线性复杂度比大部分幂置换给出的序列的线性复杂度要更高，比少数幂置换给出的序列线性复杂度低。详细的对比情况参见本文第 4 节。

2 基础知识

2.1 最优跳频序列

设 l 是一个正整数，一个有限集合 F 定义为 $F=\{f_0, f_1, \cdots, f_{l-1}\}$。令长度为 n 的序列 $X=x_0\, x_1 \cdots\ x_{n-1}$，其中 $x_i \in F$。长度为 n 的所有跳频序列组成的集合记为 $S=\{X \mid X=x_0\, x_1 \cdots x_{n-1}$，其中 $x_i \in F\}$。$\forall X, Y \in S$，它们之间的 Hamming 相关定义如下：

$$H_{X,Y}(t)=\sum_{i=0}^{n-1} h[x_i, y_{i+t}], \quad 0 \leqslant t < n \tag{1}$$

其中，如果 $x_i=y_{i+t}$，则 $h[x_i, y_{i+t}]=1$；否则 $h[x_i, y_{i+t}]=0$。由式(1)集合 S 中的 Hamming 相关可以定义如下[1]：

$$H(X)=\max_{1 \leqslant t < n}\{H_{X,X}(t)\} \tag{2}$$

$$H(X,Y)=\max_{1 \leqslant t < n}\{H_{X,Y}(t)\} \tag{3}$$

$$M(X,Y)=\max\{H(X), H(Y), H(X,Y)\} \tag{4}$$

一个跳频序列的Hamming相关如果满足式(5)，称其满足 Lempel-Greenberger 界。

引理 1[12] 对于 F 上的每一个长度为 n 的跳频序列 X，其 Hamming 相关满足

$$H(X) \geqslant \left\lceil \frac{(n-\varepsilon)(n-\varepsilon-l)}{l(n-1)} \right\rceil \tag{5}$$

其中，ε是 n 模 l 的最小非负剩余，即$\varepsilon \equiv n \bmod l$。

满足 Lempel-Greenberger 界的单个序列称为最优跳频序列。

为了判断一个跳频序列集是否达到最优，还需要用到引理 2。

引理 2[13] 设 S 是包含 N 个长度为 n 的跳频序列组成的集合，跳频序列中分量取自集合 F。定义 $I=\lfloor nN/l \rfloor$，则

$$M(S) \geqslant \left\lceil \frac{(nN-l)n}{(nN-1)l} \right\rceil \tag{6}$$

并且

$$M(S)\geqslant\left\lceil\frac{2InN-(I+1)Il}{(nN-1)N}\right\rceil \tag{7}$$

其中，$M(S)=\max\{\max_{X\in S}H(X),\max_{X,Y\in S,X\neq Y}H(X,Y)\}$。

一个跳频序列集的 Hamming 相关值如果满足式(6)或者式(7)，则称这类序列集满足 Peng-Fan 界。满足 Peng-Fan 界的跳频序列集称为最优跳频序列集。

2.2　序列的线性复杂度

设 GF(q)表示含有元素个数为 q 的有限域，GF(q)*表示 GF(q)中所有的非零元，这里 $q=p^r$，p 是一个素数，$r\geqslant1$ 是一个正整数。对于一个元素取自 GF(q)上的序列 $s=s_0s_1\cdots$，其线性复杂度可以定义为产生该序列最短的线性反馈移位寄存器(LFSR)的长度。设序列 s 由一个 LFSR 生成，并满足递归关系式：$s_{n+l}=c_{l-1}s_{n+l-1}+c_{l-2}s_{n+l-2}+\cdots+c_0s_n$，$n\geqslant0$。多项式 $c(x)=c_lx^l+c_{l-1}x^{l-1}+\cdots+c_1x+c_0$ 称为序列 s 的特征多项式。显然满足上述递归关系的特征多项式有很多，其中具有最低次数 L 的特征多项式称为序列 s 的最小多项式。序列 s 的线性复杂度还可以定义为其最小多项式的次数，记为 LS(s)=L。

线性复杂度是衡量序列安全性的一个重要指标。如果一个序列具有较低的线性复杂度，那么序列可以由较短的 LFSR 来生成，攻击者利用 Berlekamp-Massey 算法可以很容易得到生成该序列最短的 LFSR 长度和它的反馈逻辑，因此，高线性复杂度是序列安全的一个必要条件。从工程角度来说，线性复杂度可以认为是利用 LFSR 生成序列的困难程度。

3　主要结果

对于一个最优跳频序列或者最优跳频序列集来说，线性复杂度是一个重要的指标。当前存在具有较高线性复杂度的跳频序列集[5,6]，但这些跳频序列是通过广义 bent 函数或者多项式环设计的，在实际应用中实现并不简单。在文献[16]中，Wang 利用有限域 GF(q)上的幂置换：$x\to x^\sigma$，这里 $x\in$GF(q)，gcd(σ, $q-1$)=1，提高几类序列的线性复杂度。Wang 同时指出“或许”可以利用其他类型的置换多项式来提高序列的线性复杂度，但计算线性复杂度并不像幂置换那么容易。本文利用下面的置换研究两类最优跳频序列的线性复杂度。

引理 3[15]　当 q 为奇数时，多项式 $x^{(q+1)/2}+bx\in$GF(q)[x]是 GF(q)上的一个置换多项式当且仅当 $b=(c^2+1)(c^2-1)^{-1}$，这里 $c\in$GF(q)，$c\neq0$，$c^2\neq1$。

上述引理中的置换多项式和幂置换显然是不同的。因此给出的具有高线性复杂度的最优跳频序列集是一类新的跳频序列集。

3.1　第一类跳频序列集

设 p 是个奇素数，$q=p^r$，r 是一个正整数，$m\geqslant3$ 是一个奇数。假设 α 是 GF(q^m)*的生成元，$n=(q^m-1)/2$，d 是一个整数满足 gcd(d, q^m-1)=1。令 $\beta=\alpha^{2d}$，$\forall a\in$GF(q^m)，定义一个序列 s_a 如下：

$$s_a=(\mathrm{Tr}(a),\mathrm{Tr}(a\beta),\cdots,\mathrm{Tr}(a\beta^{n-1})) \tag{8}$$

其中，$\mathrm{Tr}(x)=x+x^q+\cdots+x^{q^{m-1}}$ 是 GF(q^m)→GF(q)上的迹函数。文献[3]已经证明：s_a 是一个(((q^m-1)/2, ($q^{m-1}-1$)/2; q)最优跳频序列。{s_a, $s_{a'}$}是一个((q^m-1)/2, 2, ($q^{m-1}-1$)/2; q) 最优跳频序列集，这里 a 是 GF(q^m)*中某个元素的平方，而 a'不能表示为 GF(q^m)*中某个元素的平方。文献[16]证明了这些序列的线性复杂度等于 m。相比于序列的周期(q^m-1)/2 来说，该序列的线性复杂度非常低，下面证明可以利用置换多项式来得到具有大线性复杂度的跳频序列集。

引理 4[17]

$$\left(\sum_{j=1}^{N}a_j\right)^n=\sum_{k_1+k_2+\cdots+k_N=n}\frac{n!}{k_1!k_2!\cdots k_N!}a_1^{k_1}a_2^{k_2}\cdots a_N^{k_N}$$

引理 5[18]　设 $f(x)\in$GF(q)[x]，$f(x)$在其分裂域上的全部根记为 α_1，α_2，$\cdots$，α_n。序列 $a=a_0a_1\cdots$以 $f(x)$为特征多项式当且仅当存在一组元素 λ_1，λ_2，$\cdots$，λ_n，使得

$$a_k=\lambda_1\alpha_1{}^k+\lambda_2\alpha_2{}^k+\cdots+\lambda_n\alpha_n{}^k,\quad k=0,1,\cdots$$

序列 a 的线性复杂度等于上式中不等于 0 的那些 λ_i 的个数。

该引理表明一个序列中的元素可以由序列特征多项式的根来表示，并且序列的线性复杂度也可以由序列根表示的数目确定。

引理 6[19]　设 $f(x)\in$GF(q)[x]，$f(x)$在其分裂域上无重根。则 $f(x)$可以表示为 $f(x)=f_1(x)f_2(x)\cdots f_k(x)$，$k>0$，$f_i(x)$，$i=1,2,\cdots k$，是 GF($q$)上不同的不可约多项式。设序列 s 是以 $f(x)$为极小多项式生成的序列，则序列 s 可以表示为 $s=s^{(1)}+s^{(2)}+\cdots+s^{(k)}$，其中 $s^{(i)}$是以 $f_i(x)$为极小多项式生成的序列。

定理 1　设序列 s_a 由式(8)给出，$b=(c^2+1)(c^2-1)^{-1}$，这里 $c\in$GF(q)，$c\neq0$，$c^2\neq1$。设 $\delta(x)=x^{(q+1)/2}+bx$，定义

$$\delta(s_a(t))=\mathrm{Tr}(a\beta^t)^{(q+1)/2}+b\mathrm{Tr}(a\beta^t)$$

$0 \leqslant t \leqslant (q^m-1)/2-1$ 则

1) $(\delta(s_a), \delta(s_{a'}))$组成一个$((q^m-1)/2, 2, (q^{m-1}-1)/2; q)$ 最优跳频序列集。

2) $\delta(s_a)$的线性复杂度为

$$\binom{m+(p+1)/2-1}{(p+1)/2}\binom{m+(p-1)/2-1}{(p-1)/2}^{r-1}+m$$

证明

定理 1 中的 1)是显然成立的。因为$\delta(x)$: GF(q)→GF(q)是 GF(q)上的置换多项式，所以序列$\delta(s_a)$是序列 s_a 的置换序列。根据式(1)中 Hamming 相关的定义，$\delta(s_a)$满足引理 1 中的最优界。下面证明定理 1 中的 2)部分。

因为 $q=p^r$，$(q+1)/2$ 可以表示为

$$(q+1)/2=\sum_{i=0}^{r-1}\eta_i p^i \quad , \quad 0 \leqslant \eta_i < p$$

所以

$$\mathrm{Tr}(a\beta^t)^{(q+1)/2}=\left(\sum_{j=0}^{m-1}(a\beta^t)^{q^j}\right)^{(q+1)/2}$$

$$=\prod_{i=0}^{r-1}\left(\sum_{j=0}^{m-1}(a^{p^i}\beta^{p^i t})^{q^j}\right)^{\eta_i}$$

根据引理 4，

$$\left(\sum_{j=0}^{m-1}(a^{p^i}\beta^{p^i t})^{q^j}\right)^{\eta_i}$$

$$=\sum_{\lambda_{i,0}+\lambda_{i,1}+\cdots+\lambda_{i,m-1}=\eta_i}\frac{\eta_i!}{\lambda_{i,0}!\lambda_{i,1}!\cdots\lambda_{i,m-1}!}\left(a^{p^i}\beta^{p^i t}\right)^{\sum_{j=0}^{m-1}q^j\lambda_{i,j}}$$

所以

$$\mathrm{Tr}(a\beta^t)^{(q+1)/2}$$

$$=\prod_{i=0}^{r-1}\sum_{\lambda_{i,0}+\lambda_{i,1}+\cdots+\lambda_{i,m-1}=\eta_i}\frac{\eta_i!}{\lambda_{i,0}!\lambda_{i,1}!\cdots\lambda_{i,m-1}!}\left(a^{p^i}\beta^{p^i t}\right)^{\sum_{j=0}^{m-1}q^j\lambda_{i,j}}$$

$$=\sum_{\sum_{j=0}^{m-1}\lambda_{0,j}=\eta_0}\cdots\sum_{\sum_{j=0}^{m-1}\lambda_{r-1,j}=\eta_{r-1}}\prod_{i=0}^{r-1}\left(\frac{\eta_i!}{\lambda_{i,0}!\lambda_{i,1}!\cdots\lambda_{i,m-1}!}\cdot a^{\sum_{j=0}^{m-1}q^j\sum_{i=0}^{r-1}\lambda_{i,j}p^i}\beta^{(\sum_{j=0}^{m-1}q^j\sum_{i=0}^{r-1}\lambda_{i,j}p^i)t}\right) \quad (9)$$

根据引理 5，需要给出式(9)中β的系数模 q^m-1 有多少是互不相同的。对于不同的$\lambda_{i,j}$，$\lambda'_{i,j}$考虑式(10)：

$$\sum_{j=0}^{m-1}q^j\sum_{i=0}^{r-1}\lambda_{i,j}p^i \equiv \sum_{j=0}^{m-1}q^j\sum_{i=0}^{r-1}\lambda'_{i,j}p^i \bmod(q^m-1) \quad (10)$$

因为 $\lambda_{i,j} \leqslant \eta_i$， $\lambda'_{i,j} \leqslant \eta_i$ 并且当 $q>3$ 时有：

$$0<(q+1)/2=\sum_{i=0}^{r-1}\eta_i p^i < q-1$$

所以 $\sum_{j=0}^{m-1}q^j\sum_{i=0}^{r-1}\lambda_{i,j}p^i$ 和 $\sum_{j=0}^{m-1}q^j\sum_{i=0}^{r-1}\lambda'_{i,j}p^i$ 都小于 q^m-1。因此，式(10)中的 mod(q^m-1)可以省去。

由式(10)可知，

$$q^0(\lambda_{0,0}+\lambda_{1,0}p+\cdots+\lambda_{r-1,0}p^{r-1})+\cdots+$$

$$q^{m-1}(\lambda_{0,m-1}+\lambda_{1,m-1}p+\cdots+\lambda_{r-1,m-1}p^{r-1})$$

$$=q^0(\lambda'_{0,0}+\lambda'_{1,0}p+\cdots+\lambda'_{r-1,0}p^{r-1})+\cdots+$$

$$q^{m-1}(\lambda'_{0,m-1}+\lambda'_{1,m-1}p+\cdots+\lambda'_{r-1,m-1}p^{r-1}) \quad (11)$$

对于上式把等号两边模 q 得到：

$$\lambda_{0,0}+\lambda_{1,0}p+\cdots+\lambda_{r-1,0}p^{r-1}$$

$$=\lambda'_{0,0}+\lambda'_{1,0}p+\cdots+\lambda'_{r-1,0}p^{r-1} \bmod q \quad (12)$$

显然，式(12)等号两边的值都是小于 q 的，所以 mod q 可以省去。得到$\lambda_{0,0}=\lambda'_{0,0}$, $\lambda_{1,0}=\lambda'_{1,0}$, …, $\lambda_{r-1,0}=\lambda'_{r-1,0}$。同理，对式(11)两端同时模 q^k, k=2, 3, …, $m-1$, 可以得到 $\forall i, j$, $\lambda_{i,j}=\lambda'_{i,j}$，这与$\lambda_{i,j} \neq \lambda'_{i,j}$矛盾。因此证明了式(9)中$\beta$的次数是互不相同的。

下面证明序列 $b\,\mathrm{Tr}(a\beta^t)$ 中的β的次数与式(9)中β的次数是互不相同的。因为

$$b\mathrm{Tr}(a\beta^t)=b\sum_{k=0}^{m-1}(a\beta^t)^{q^k}$$

所以，$\mathrm{Tr}(a\beta^t)$ 中β的次数形式为 q^kt。假设存在$\lambda_{i,j}$使下式成立：

$$q^0(\lambda_{0,0}+\lambda_{1,0}p+\cdots+\lambda_{r-1,0}p^{r-1})+\cdots+$$

$$q^{m-1}(\lambda_{0,m-1}+\lambda_{1,m-1}p+\cdots+\lambda_{r-1,m-1}p^{r-1})$$

$$=q^k \bmod(q^m-1)$$

显然上式左边和 q^k 都是小于 q^m-1 的，所以 mod(q^m-1)可以省略。因为所有的 $0 \leqslant \lambda_{i,j} \leqslant \eta_i$，要使得上式成立，必须有$\lambda_{0\,k}=1$ 且其余的$\lambda_{i,j}=0$，这就意味着$\eta_0=1$，$\eta_i=0$， $i=1, 2, \cdots, r-1$，即$(q+1)/2=1$。这与 p 是奇素数，q 是 p 的幂次矛盾。因此 $\mathrm{Tr}(a\beta^t)^{(q+1)/2}$ 与 $b\mathrm{Tr}(a\beta^t)$ 中β的次数都互不相同。

为了计算$\delta(s_a)$的线性复杂度，根据引理 5 必须给出$\delta(s_a)$的表示中系数不为 0 的β的个数。因为

$$\eta_i=\sum_{j=0}^{m-1}\lambda_{i,j} \quad , \quad 0 \leqslant \lambda_{i,j} \leqslant \eta_i \, ,$$

根据组合数公式[17]，共有：

$$\binom{m+\eta_i-1}{\eta_i}$$

个方式将η_i表示为满足条件的$\lambda_{i,j}$的和。

因此，$\mathrm{Tr}(a\beta^t)^{(q+1)/2}$中共含有以下数目的项：

$$\prod_{i=0}^{r-1}\binom{m+\eta_i-1}{\eta_i}$$

又因为$b\mathrm{Tr}(a\beta^t)$中β的幂次与$\mathrm{Tr}(a\beta^t)^{(q+1)/2}$中的完全不同，由引理 6 序列$\delta(s_a)$的线性复杂度为

$$\prod_{i=0}^{r-1}\binom{m+\eta_i-1}{\eta_i}+m \tag{13}$$

从式(13)可以看出，线性复杂度的提高依赖于$(q+1)/2$的分解。因为$q=p^r$，所以

$$p^r+1=2\sum_{i=0}^{r-1}\eta_i p^i=2\eta_0+\sum_{i=1}^{r-1}2\eta_i p^i$$

即 $p^r=2\eta_0-1+\sum_{i=1}^{r-1}2\eta_i p^i$。根据正整数的 p 元表示，当$0\leqslant\eta_i<p-1$时，

$$p^r-1=(p-1)(1+p+\cdots+p^{r-1})$$

因此可以确定

$\eta_0=(p+1)/2$，$\eta_i=(p-1)/2$，i=1, 2, …, r−1

当 p、r、m 3 个参数固定时，$\delta(s_a)$的线性复杂度是固定的，即

$$\binom{m+(p+1)/2-1}{(p+1)/2}\binom{m+(p-1)/2-1}{(p-1)/2}^{r-1}+m$$

显然，相比于原来的线性复杂度，置换以后的序列线性复杂度有明显的提高。证毕。

3.2　第二类跳频序列集

设 p 是一个素数，$q=p^r$，r 是一个正整数。设 m 和 d 是 2 个正整数，满足 $d\mid q^m-1$，并且 $\gcd((q^m-1)/(q-1), d)=1$。假设α是 $\mathrm{GF}(q^m)^*$的生成元，$\beta=\alpha^{\mu d}$，μ是一个正整数满足 $\gcd(q^m-1, \mu)=1$，设 $n=(q^m-1)/d$，对于每一个 $0\leqslant i\leqslant d-1$，可以定义下面的序列：

$$s_i(t)=\mathrm{Tr}(\alpha^i\beta^t),\ 0\leqslant t\leqslant n-1 \tag{14}$$

文献[2]已经证明了由序列

$$s_i=(\mathrm{Tr}(\alpha^i),\mathrm{Tr}(\alpha^i\beta),\cdots,\mathrm{Tr}(\alpha^i\beta^{n-1}))$$

组成的序列族 $S=\{s_i\mid 0\leqslant i\leqslant d-1\}$是一个$((q^m-1)/d, d, (q^{m-1}-1)/d; q)$最优跳频序列集。

由参数β，α，d，μ的定义可以看出，式(14)中的序列是式(8)中序列的一种广义描述。第二类跳频序列集中要求 $\gcd(q^m-1, \mu)=1$，$d\mid q^m-1$；而第一类跳频序列集中 $\gcd(q^m-1, d)=1$，$2\mid q^m-1$；第一类序列可以看作是第二类序列中 d=2 时的一个特例，因此第二类跳频序列集可以看作是第一类跳频序列集的推广。文献[16]证明这些序列的线性复杂度等于 m。相比于序列的周期来说，该线性复杂度显然是非常低的。利用的置换多项式$\delta(x)$和第一类序列集同样的方法，可以改进第二类序列集的线性复杂度，所以有定理 2。

定理 2　设序列 s_i 由式(14)给出，$b=(c^2+1)(c^2-1)^{-1}$，这里 $c\in\mathrm{GF}(q)$，$c\neq 0$，$c^2\neq 1$。设 $\delta(x)=x^{(q+1)/2}+bx$，定义

$$\delta(s_i(t))=\mathrm{Tr}(\alpha^i\beta^t)^{(q+1)/2}+b\mathrm{Tr}(\alpha^i\beta^t)$$

则

1) 如果 $\gcd(d, \sum_{i=0}^{m-1}q^i)=1$，序列集$\{\delta(s_i)\mid 0\leqslant i\leqslant d-1\}$构成一个$((q^m-1)/d, d, (q^{m-1}-1)/d; q)$最优跳频序列集。

2) $\delta(s_a)$的线性复杂度为

$$\binom{m+(p+1)/2-1}{(p+1)/2}\binom{m+(p-1)/2-1}{(p-1)/2}^{r-1}+m$$

定理 2 的证明与定理 1 类似，略去。

可以看出，利用置换多项式$\delta(x)$可以将低线性复杂度的最优跳频序列集转化为高线性复杂度的最优跳频序列集。例如：当 p=7，$q=7^3$，m=5，在原序列集中线性复杂度仅为 5，而经过 $\delta(x)=x^{(q+1)/2}+bx$ 置换以后得到的新跳频序列集的线性复杂度等于 85 755，显然大幅度增加了序列的线性复杂度。

4　比较和实现

本节主要将本文给出的最优跳频序列集与现有的具有高线性复杂度的最优跳频序列集[5,6,16]从线性复杂度和工程实现 2 个角度进行对比，说明本文给出的跳频序列集具有的优势。

由式(8)和式(14)可以看出，置换前的两类跳频序列集都可以通过迹函数来实现。众所周知，当迹函数中只包含一个元素的幂次时，其工程实现是非常简单的。但由于这两类跳频序列集的线性复杂度太低，因此只能限制在保密要求很低的环境中使用。本文置换以后的跳频序列集，是在原序列集上增加了一个$(q+1)/2$ 乘幂次运算(即增加的乘法次数约为 $\log((q+1)/2)$次)，而后与原序列输出相加。这

种改变仅仅增加了一个简单的乘法电路和一次加法运算，其中加法运算由于运算量非常小是可以忽略不计的，可见置换以后跳频序列的工程实现仍然是非常简单的，以增加非常少量的实现复杂度来获得较高的线性复杂度是非常值得的。

文献[5]利用广义 bent 序列和广义 bent 函数构造了两类具有高线性复杂度的最优跳频序列集。其中第一类最优跳频序列集的线性复杂度并不是太高(当周期为 p 的幂次时，线性复杂度仅为 p)，第二类最优跳频序列集的线性复杂度相比于第一类较高。然而因为这两类序列集都是基于广义 bent 函数或者广义 bent 序列构造的，所以实现是比较复杂的[20]。

文献[6]的目的也是构造具有高线性复杂度的最优跳频序列集，这种构造主要是基于代数中的多项式环理论，相比于文献[2,3]中利用有限域构造的最优跳频序列集来说，这种基于环构造的最优跳频序列本身更加的复杂，并且实现也不简单，但这种构造可以获得较高的线性复杂度，在保密性要求较高的环境中可以使用该类跳频序列集。

文献[16]是利用幂置换将具有低线性复杂度的最优跳频序列集置换为具有高线性复杂度的最优跳频序列集，其工程实现也相对简单，仅仅是在原序列上增加一个 σ (满足 $\gcd(\sigma, q-1)=1$) 的幂次运算，增加的乘法次数约为 $\log \sigma$次。而本文给出的新型最优跳频序列的实现大约需要增加 $\log ((q+1)/2)$ 次乘法和一次加法运算。因此本文序列的实现复杂度与文献[16]中序列的实现复杂度大致相当。在线性复杂度方面，由文献[16]中的结论，置换后序列线性复杂度的值取决于 σ 的 p 元表示，而且当 $\sigma=p^r-p^j-1$ 时，序列的线性复杂度取到最大。本文利用置换多项式 $\delta(x)$得到置换后跳频序列线性复杂度的值依赖于 $(q+1)/2$ 的 p 元表示，因此有限域给定时，置换后序列的线性复杂度就是给定的。由本文定理 1、定理 2 和文献[16]中定理 5、推论 6、定理 9、推论 10 中的结论可以看出：本文给出的新型最优跳频序列的线性复杂度要小于幂置换 $\sigma=p^r-p^j-1$ 时序列的线性复杂度，但要大于大多数使用其他幂置换得到的最优跳频序列的线性复杂度。

综上所述，利用 $\delta(x)$可以将两类低线性复杂度的最优跳频序列集变换为具有高线性复杂度的最优跳频序列集，与现有的具有高线性复杂度的最优跳频序列集相比，增加了非常少的实现复杂度，获得了较高的线性复杂度。

5 结束语

本文主要证明了 Wang 给出的命题[16]，即除幂置换以外，其他类型的置换多项式也可以给出具有大线性复杂度，实现相对简单的最优跳频序列集，并且可以给出置换后序列线性复杂度的精确值。由定理 1 和定理 2 的结论可以看出，利用置换多项式 $\delta(x)= x^{(q+1)/2}+bx$ 可以将低线性复杂度的最优跳频序列集转化为具有高线性复杂度，实现简单的最优跳频序列集。通过计算序列表示中 α不同幂次的数目，给出了这些序列线性复杂度的精确值。本文利用的置换 $\delta(x)$与文献[16]中使用的幂置换显然是不同的，因此得到的是新型的最优跳频序列集。

参考文献：

[1] SIMON M K, OMURA J K, SCHOLZ R A, *et al*. Spread Spectrum Communications Handbook[M]. New York: McGraw-Hill, 2002.

[2] DING C, YIN J. Sets of optimal frequency-hopping sequences[J]. IEEE Transactions on Information Theory, 2008, 54(8): 3741-3745.

[3] DING C, MOISIO M J, YUAN J. Algebraic constructions of optimal frequency-hopping sequences[J]. IEEE Transactions on Information Theory, 2007, 53(7): 2606-2610.

[4] DING C, FUJI-HARA R, FUJIWARAY *et al*. Sets of frequency hopping sequences: bounds and optimal constructions[J]. IEEE Transactions on Information Theory,2009, 55(7):3297-3304.

[5] KUMAR P V. Frequency-hopping code sequence designs having large linear span[J]. IEEE Transactions on Information Theory, 1988, 34(1): 146-151.

[6] UDAYA P, SIDDIQI M U. Optimal large linear complexity frequency hopping patterns derived from polynomial residue class rings[J]. IEEE Transactions on Information Theory, 1998, 44(4): 1492-1503.

[7] CAO Z, GE G, MIAO Y. Combinatorial characterizations of one-coincidence frequency- hopping sequences[J]. Design Codes and Cryptography, 2006, 41(2): 177-184.

[8] CHU W, COLBOURN C J. Optimal frequency-hopping sequences via cyclotomy[J]. IEEE Transactions on Information Theory, 2005, 51(3): 1139-1141.

[9] GE G, FUJI-HARA R, MIAO Y. Further combinatorial constructions for optimal frequency hopping sequences[J]. Journal of Combinatorial Theory Ser A, 2006, 113: 1699-1718.

[10] GE G, MIAO Y, YAO Z. Optimal frequency hopping sequences: auto- and cross-correlation properties[J]. IEEE Transactions on Information

Theory, 2009, 55(2): 867- 879.

[11] FUJI-HARA R, MIAO Y, MISHMA M. Optimal frequency hopping sequences: a combinatorial approach[J]. IEEE Transactions on Information Theory, 2004, 50(10): 2408- 2420.

[12] LEMPEL A, GREENBERGER H. Families of sequences with optimal Hamming correlation properties[J]. IEEE Transactions on Information Theory, 1974, 20(1): 90-94.

[13] PENG D, FAN P. Lower bounds on the Hamming auto- and cross-correlations of frequency-hopping sequences[J]. IEEE Transactions on Information Theory, 2004, 50(9): 2149-2154.

[14] BERLEKAMP E. Algebraic Coding Theory[M]. New York: McGraw-Hill, 1968.

[15] LIDL R, NIEDERRERTER H. Finite Fields[M]. London: Addison-Wesley, 1983.

[16] WANG Q. Optimal sets of frequency hopping sequences with large linear spans[J]. IEEE Transactions on Information Theory, 2010, 56(4): 1729-1736.

[17] BOGRART K, STEIN C, DRYSDALE R L. Discrete Mathematics for Computer Science[M]. College Publishing, 2005.

[18] 李超, 屈龙江. 密码学讲义[M]. 科学出版社, 2010.

CHAO L, QU L J. Lectures on Cryptology[M]. Science Press, 2010.

[19] GOLOMB S W, GUANG G. Signal design for Good Correlation, for Wireless Communication, Cryptography, and Radar[M]. Cambridge Univ Press, 2005.

[20] 胡予濮, 张玉清, 肖国镇. 对称密码学[M]. 北京：机械工业出版社, 2002.

HU Y P, ZHANG Y Q, XIAO G Z. Symmetric Key Cryptography[M]. Beijing: China Machine Press, 2002.

作者简介：

高军涛（1979-），男，河北临城人，博士，西安电子科技大学副教授，主要研究方向为伪随机序列、流密码。

胡予濮（1955-），男，河南濮阳人，博士，西安电子科技大学教授、博士生导师，主要研究方向为密码学、信息安全与网络安全。

李雪莲（1979-），女，吉林公主岭人，博士，西安电子科技大学讲师，主要研究方向为密码函数、流密码。

向上荣（1988-），女，陕西西安人，西安电子科技大学本科生，主要研究方向为计算机科学与技术。