Control and Cybernetics

vol. **42** (2012) No. 2

Improved linear complexities of the frequency hopping sequences in two optimal sets[*][†]

by

Juntao Gao[1,2], Xuelian Li[3] and Yongzhuang Wei[4]

[1]State Key Laboratory of ISN, Xidian University, Xi'an, 710071, China
[2]State Key Laboratory of Information Security,
Graduate University of Chinese Academy of Sciences, Beijing, 100049, China
[3] Department of Applied Mathematics,
Xidian University, Xi'an, 710071, China
[4] Guangxi Key Laboratory of Wireless Wideband Communication
and Signal Processing, Guilin University of Electronic Technology,
Guilin, 541004, China
e-mail: jtgao@mail.xidian.edu.cn, walker_wyz@guet.edu.cn

Abstract: For the anti-jamming purpose, high linear complexity is desired for each frequency hopping sequence in an optimal set. Using a proper power permutation, Wang has shown that an optimal set of frequency hopping sequences with small linear complexity can be transformed into a new optimal set of frequency hopping sequences with large linear complexity.

This paper conains two results. First, we extend the result of Wang. A power permutation is only suitable for a special construction of optimal set of frequency hopping sequences, see Wang (2011). However, the power permutation chosen in this paper applies to the general construction of optimal set of frequency hopping sequences. Second, by using a binomial permutation polynomial $P(x)$, which is different from those permutations used before, we obtain a novel optimal set of frequency hopping sequences with high linear complexity from an optimal set of frequency hopping sequences with small linear complexity. By counting the number of different roots in the sequence representation, we determine the linear complexities of the frequency hopping sequences in two optimal sets transformed by the power permutation or binomial permutation.

Keywords: frequency hopping sequence, linear complexity, permutation polynomial, optimal set.

[*]Submitted: November 2011; Accepted: April 2012

[†]This paper is the full version of the paper in the proceedings of INCoS 2011.

1. Introduction

In modern communication systems, the frequency hopping technique is widely applied in code division multiple access and Bluetooth technology. An optimal set of frequency hopping sequences (Section 2.1) plays an important role in the frequency hopping communication. The construction of the optimal set of frequency hopping sequences has been extensively investigated in the related literatures, see Chu and Colbourn (2005), Ding et al. (2007), Wang (2011), Ding et al. (2009), Udaya and Siddiqi (1998), Fujihara et al. (2004), Ge et al. (2006), Zhou and Tang (2009), Wang (2010), Kumar (1988), Ding and Yin (2008), Ge et al. (2009). In secure communication, the frequency hopping sequences have to be strong enough to resist some common cryptanalytic techniques, such as the Berlekamp-Massey algorithm, so that it is infeasible to reconstract them from some short segments of the sequences, see Golomb and Gong (2005). Therefore, besides long period, uniform symbol distribution, good Hamming correlation, and computational practicality, the frequency hopping sequences in the optimal set have to possess high complexity to prevent an eavesdropper from obtaining all the frequency hopping patterns, and further stealing the secret information. Linear complexity is the most important and most necessary security indicator. For the frequency hopping sequences with small linear complexity, the eavesdropper can obtain all of the frequency hopping patterns by combining some short sequence samples with the Berlekamp-Massey algorithm. So, high linear complexity is desired for the frequency hopping sequences in order to resist the eavesdropper in secure communication.

Ding and Yin mentioned that a new optimal set of frequency hopping sequences with large linear complexity could be obtained from an optimal set of frequency hopping sequences with small linear complexity by using a proper power permutation over the finite field F_q, see Ding and Yin (2008). The new optimal set of frequency hopping sequences shares several parameters with the original optimal set, such as the sequence length in the set, the number of the sequences in the set, and the Hamming correlation, but each frequency hopping sequence in the new optimal set has higher linear complexity than in the original optimal set.

Ding et al. (2009) gave a general construction of optimal set and a special case of the general construction. All of the frequency hopping sequences in the two constructions have small linear complexity. Wang (2011) transformed the special construction of optimal set (Example 2) into a new optimal set of frequency hopping sequences with higher linear complexity by applying a power permutation and determined the linear complexity of the frequency hopping sequences in the transformed optimal set. However, it may be difficult to derive the linear complexity of the transformed frequency hopping sequences in the general construction by a power permutation. *Furthermore*, other types of permutation polynomials over F_q may be employed in improving the linear complexity of the frequency hopping sequences in an optimal set, but calculating the linear complexity of the transformed frequency hopping sequences may not be easy, see Wang (2010).

This paper gives two contributions. Firstly, we transform the general construction of optimal set into a novel optimal set of frequency hopping sequences with high linear complexity by applying a properly chosen power permutation. We derive the linear complexity of frequency hopping sequences in the transformed general construction of the optimal set. Secondly, by using a binomial permutation $P(x)$, which is different from the power permutation, we transform the special construction of optimal set of frequency hopping sequences into a new optimal set, and we give the exact value of the linear complexity of the transformed frequency hopping sequences. The linear complexities of the transformed frequency hopping sequences in two new optimal sets are very high compared to their lengths. This paper is organized as follows. In Section 2, we recall some definitions and properties of the optimal set of frequency hopping sequences and linear complexity. In Section 3, we determine the linear complexity of the transformed frequency hopping sequences in the general construction by a power permutation. Section 4 gives the linear complexity of the transformed frequency hopping sequences in the special construction by the binomial permutation $P(x)$, Section 5 gives an implementation of the optimal set of frequency hopping sequences. Concluding remarks and comparisons are given in Section 6.

2. Preliminaries

2.1. Optimal set of frequency hopping sequences

Let $F = \{f_0, f_1, \ldots, f_{\gamma-1}\}$ be a set of available frequencies with alphabet size γ. Let $\mathcal{F}$ be a set of all frequency sequences of length L over F. For any two sequences $X, Y \in \mathcal{F}$, where $X = (X(0), X(1), \ldots, X(L-1))$, $Y = (Y(0), Y(1), \ldots, Y(L-1))$, we can define their Hamming correlations $H_{X,Y}$ as follows

$$H_{X,Y}(\tau) = \sum_{i=0}^{L-1} h[X(i), Y(i+\tau)], \qquad 0 \leq \tau < L \tag{1}$$

where $h[X(i), Y(i+\tau)] = 1$ if $X(i) = Y(i+\tau)$, and 0 otherwise, and the addition operations are performed modulo L. If $X = Y$, $H_{X,X}(\cdot)$ is called the *autocorrelation function* of the sequence X. $H_{X,Y}(\cdot)$ is the *crosscorrelation function* of X and Y if $X \neq Y$. For any distinct $X, Y \in \mathcal{F}$, we define

$$H(X) = max_{1 \leq \tau < L}\{H_{X,X}(\tau)\}$$

$$H(X,Y) = max_{0 \leq \tau < L}\{H_{X,Y}(\tau)\}$$

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

In a frequency hopping spread spectrum system, the interference occurs if two distinct transmitters use the same frequency simultaneously. To reduce the interference and maximize the throughput in the system, we hope to design the set $\mathcal{F}$ with good Hamming correlation and a large number of the sequences. Lempel and Greenberger (1974) developed the following lower bound for a single frequency hopping sequence to determine whether it is good.

Lemma 1 *For every frequency hopping sequence of length L over an alphabet F of size γ, we have*

$$H(X) \geq \left\lceil \frac{(L-\varepsilon)(L+\varepsilon-\gamma)}{\gamma(L-1)} \right\rceil \tag{2}$$

where ε is the least nonnegative residue of L modulo γ.

Let $\mathcal{F}$ be a set containing N frequency hopping sequences. The maximum nontrivial Hamming correlation of the frequency hopping sequence set $\mathcal{F}$ is defined by

$$M(\mathcal{F}) = max\left\{ max_{X\in\mathcal{F}} H(X), max_{X,Y\in\mathcal{F},X\neq Y} H(X,Y) \right\}.$$

In this paper, we denote by $(L, N, \lambda; \gamma)$ the set $\mathcal{F}$ of N frequency hopping sequences of length L over an alphabet F, where $\lambda = M(\mathcal{F})$. To measure the quality of a set of frequency hopping sequence, Peng and Fan (2004) described the following bounds on $M(\mathcal{F})$.

Lemma 2 *Let $\mathcal{F}$ be a set containing N frequency hopping sequences of length L over an alphabet of size γ. Define $I = \lfloor LN/\gamma \rfloor$, Then*

$$M(\mathcal{F}) \geq \left\lceil \frac{(LN-\gamma)L}{(LN-1)\gamma} \right\rceil \tag{3}$$

and

$$M(\mathcal{F}) \geq \left\lceil \frac{2ILN-(I+1)I\gamma}{(LN-1)N} \right\rceil. \tag{4}$$

From Lemmas 1 and 2, we define an optimal sequence or an optimal set of frequency hopping sequences as follows,

1. A sequence $X \in \mathcal{F}$ is called optimal if the Lempel-Greenberger bound in Lemma 1 is met.
2. A set $\mathcal{F}$ is an optimal set if one of the bounds in Lemma 2 is met.

Relatively, it is easier to construct a single optimal frequency hopping sequence than an optimal set of frequency hopping sequences. In general, there exist two main methods to construct the optimal set of frequency hopping sequences, the algebraic method and the combinatoric method.

2.2. Linear complexity of a sequence

From the engineering point of view, the linear complexity of a sequence is the length of the shortest linear feedback shift register (LFSR) which can produce the sequence. Let $S = (s_0, s_1, \cdots)$ be a sequence produced by the LFSR satisfying the following linear recurrence relation

$$s_{n+l} = c_1 s_{n+l-1} + c_2 s_{n+l-2} + \cdots + c_l s_n$$

where $n \geq 0$. $c(x) = c_l x^l + c_{l-1} x^{l-1} + \cdots + c_1 x + 1 \in F_q[x]$ is called the connection polynomial of the LFSR or a connection polynomial of sequence S. The connection polynomial of S with the least degree is called the minimal polynomial of S. The linear complexity of a sequence S is defined as the degree of the minimal polynomial of S, and can be derived by finding the root representation, or the trace representation of the sequence S, see Golomb and Gong (2005). Currently, there exist several optimal sets of frequency hopping sequences with large linear complexity, see Kumar (1988), Udaya and Siddiqi (1998), Wang (2010, 2011).

High linear complexity is not a sufficient condition for the security of a sequence, but a necessary one. For a sequence with small linear complexity it can be easily reconstructed by combining some sequence segments and using the Berlekamp-Massey algorithm. So, an optimal set of frequency hopping sequences with small linear complexity can not be used in the secure communication, otherwise, these sequences will easily be attacked by the Berlekamp-Massey algorithm.

3. Linear complexity of the transformed frequency hopping sequences in the general construction by a power permutation

We begin this section by introducing some notations which will be used throughout this paper.

- p is an odd prime, and $q = p^s$ is a power of p.
- m is a positive integer. N is a positive divisor of $q^m - 1$, and $nN = q^m - 1$.
- F_{q^m} is a finite field with q^m elements, which is an extension of F_q, and $F_{q^m}^* = F_{q^m} - \{0\}$.
- α is a generator of $F_{q^m}^*$, and $\beta = \alpha^N$.
- $Tr_1^m(\cdot)$ denotes the trace function from F_{q^m} to F_q, that is, $Tr_1^m(x) = \sum_{i=0}^{m-1} x^{q^i}$ for $x \in F_{q^m}$.
- $\#A$ denotes the cardinality of the set A.

The linear complexity of a periodic sequence over F_q can be calculated by its root representation, see Golomb and Gong (2005). Every sequence $S = s_0 s_1 s_2 \ldots$ over F_q of period $q^m - 1$ can be uniquely expressed as

$$s_t = \sum_{i=0}^{q^m-2} c_i \alpha^{it}, \quad for\ all\ 0 \leq t \leq q^m - 2 \tag{5}$$

where $c_i \in F_{q^m}$ for $0 \leq i \leq q^m - 2$ and α is a generator of $F_{q^m}^*$. Let $I = \{i | c_i \neq 0,\ 0 \leq i \leq q^m - 2\}$, then the linear complexity of S is equal to $\#I$. The minimal polynomial of S is defined as

$$m(x) = \prod_{i \in I} (x - \alpha^i).$$

For each $0 \leq i \leq N - 1$, the sequence S_i is defined by

$$S_i(t) = Tr_1^m(\alpha^i \beta^t), 0 \leq t \leq n - 1. \tag{6}$$

Obviously, S_i is a sequence of length n over the finite field F_q. The set of frequency hopping sequences is defined as

$$\mathcal{S} = \{S_i : 0 \leq i \leq N - 1\}. \tag{7}$$

Ding et al. (2009) showed that the sequence set $\mathcal{S}$ is an optimal set of frequency hopping sequences, as noted in by Theorem 1 in this paper.

THEOREM 1 *If N is even, $gcd(n, N)$=1, $gcd((q^m - 1)/(q - 1) mod N, N)$=2 and $q - 1 \equiv N/2 \ mod N$, the set $\mathcal{S}$ of (3) consists of an optimal set of frequency hopping sequences with parameters $((q^m - 1)/N,\ N,\ (q^m - 1 - q + (q - 1)\sqrt{q^m})/(qN); q)$. Furthermore, if $N > (q - 1)\sqrt{q^m}/q$, the set $\mathcal{S}$ is optimal with respect to the Peng-Fan bound.*

The optimal set in Theorem 1 is called the general construction of the optimal set. Furthermore, Ding et al. (2009) gave a special case of the general construction as follows,

LEMMA 3 *Let $q \equiv 1 mod\ 4$, $m = 2$ and $N = 2(q - 1)$. The set $\mathcal{S}$ of (7) is a $((q+1)/2, 2(q-1), 1; q)$ set of frequency hopping sequences over F_q, meeting the bound of (4).*

Wang was the first to show that the linear complexity of the frequency hopping sequences in the optimal set $\mathcal{S}$ of Lemma 3 is equal to 2. Furthermore, Wang improved the linear complexity by a proper power permutation over F_q in the following Theorem 2, see Wang (2011).

THEOREM 2 *Let $q \equiv 1 (mod\ 4)$, $m = 2$, $N = 2(q - 1)$ and $n = (q + 1)/2$. Let $\sigma = \sum_{j=1}^{w} \sigma_j p^{e_j}$ be a positive integer with $0 < \sigma < q - 1$ such that $gcd(\sigma, q - 1) = 1$, where $0 < \sigma_j \leq p - 1$, and $0 \leq e_1 < e_2 \ldots < e_w < s$. Define $\mathcal{S}^\sigma = \{S_i^\sigma : 0 \leq i \leq N - 1\}$, where S_i is defined by (6). Then*

(1) *$\mathcal{S}^\sigma$ is $((q + 1)/2, 2(q - 1), 1; q)$ optimal set of frequency hopping sequences, meeting the bound of (4).*

(2) *The linear complexity of the transformed frequency hopping sequences could be large compared to their length $n = (q + 1)/2$. In particular, if $w < s$ or* *there is at least one $\sigma_j < (p-1)/2$ for $1 \leq j \leq w$, the linear complexity of the transformed frequency hopping sequences is*

$$\prod_{j=1}^{w}(\sigma_j + 1).$$

Obviously, Theorem 2 is only suitable for the special construction of the optimal set in Lemma 3. For the general construction in Theorem 1, Theorem 2 does not work. In the following, we generalize the results of Theorem 2. We improve the linear complexity of the frequency hopping sequences in the general construction of the optimal set by choosing a proper power permutation. Our method is suitable for all frequency hopping sequences in Theorem 1 with a large prime p.

Theorem 3 *Let N be even, $gcd(n, N)=1$, $gcd((q^m-1)/(q-1) mod N, N)=2$ and $q-1 \equiv N/2 \ mod N$. Let $\sigma = \sum_{j=1}^{w} \sigma_j p^{e_j}$ be a positive integer with $0 < \sigma < q-1$ such that $gcd(\sigma, q-1) = 1$, where $0 < \sigma_j \leq [\frac{p-1}{N}]$, and $0 \leq e_1 < e_2 \ldots < e_w < s$. Define $\mathcal{S}^\sigma = \{S_i^\sigma : 0 \leq i \leq N-1\}$, where S_i is defined by (6). Then*

(1) *$\mathcal{S}^\sigma$ is $((q^m-1)/N,\ N,\ (q^m-1-q+(q-1)\sqrt{q^m})/(qN);\ q)$ optimal set of frequency hopping sequences, meeting the bound of (4).*

(2) *The linear complexity of the transformed frequency hopping sequences can be high compared to their length $L = (q^m-1)/N$, that is, the linear complexity of the transformed frequency hopping sequences is equal to*

$$\prod_{j=1}^{w}\binom{m+\sigma_j-1}{\sigma_j}.$$

Proof:

(1) Since $\gcd(\sigma, q-1)$=1, we know that S_i^σ is a permutation sequence of S_i. The Hamming correlations in $\mathcal{S}^\sigma$ are still optimal. $\mathcal{S}^\sigma$ is also $((q^m-1)/N$, N, $(q^m-1-q+(q-1)\sqrt{q^m})/(qN); q)$ optimal set of frequency hopping sequences.

(2) According to the definition of S_i, we have

$$S_i^\sigma(t) = \left(Tr_1^m(\alpha^i\beta^t)\right)^\sigma$$

Since $\sigma = \sum_{j=1}^{w}\sigma_j p^{e_j}$, we have

$$S_i^\sigma(t) = \prod_{j=1}^{w}\left(Tr_1^m(\alpha^{ip^{e_j}}\beta^{tp^{e_j}})\right)^{\sigma_j}.$$

Using the multinomial formula, see Bogart et al. (2005)

$$(g_0 + g_1 + \ldots + g_{m-1})^{\sigma_j} = \sum_{\eta_{j,0}+\eta_{j,1}+\ldots+\eta_{j,m-1}=\sigma_j}\binom{\sigma_j}{\eta_{j,0},\eta_{j,1},\ldots,\eta_{j,m-1}} g_0^{\eta_{j,0}} g_1^{\eta_{j,1}} \ldots g_{m-1}^{\eta_{j,m-1}}$$

where

$$\binom{\sigma_j}{\eta_{j,0},\eta_{j,1},\ldots,\eta_{j,m-1}}=\frac{\sigma_j!}{\eta_{j,0}!\eta_{j,1}!\ldots\eta_{j,m-1}!}$$

we can obtain that

$$\begin{aligned}&\Big(Tr_1^m(\alpha^{ip^{e_j}}\beta^{tp^{e_j}})\Big)^{\sigma_j}\\ &=\Big(\textstyle\sum_{k=0}^{m-1}(\alpha^{ip^{e_j}}\beta^{tp^{e_j}})^{q^k}\Big)^{\sigma_j}\\ &=\textstyle\sum_{\eta_{j,0}+\ldots+\eta_{j,m-1}=\sigma_j}\binom{\sigma_j}{\eta_{j,0},\eta_{j,1},\ldots,\eta_{j,m-1}}(\alpha^{ip^{e_j}}\beta^{tp^{e_j}})^{\sum_{k=0}^{m-1}q^k\eta_{j,k}}\end{aligned}$$

and then

$$\begin{aligned}S_i^\sigma(t)&=\prod_{j=1}^{w}\sum_{\eta_{j,0}+\ldots+\eta_{j,m-1}=\sigma_j}\binom{\sigma_j}{\eta_{j,0},\eta_{j,1},\ldots,\eta_{j,m-1}}(\alpha^{ip^{e_j}}\beta^{tp^{e_j}})^{\sum_{k=0}^{m-1}q^k\eta_{j,k}}\\ &=\sum_{\sum_{k=0}^{m-1}\eta_{1,k}=\sigma_1}\cdots\sum_{\sum_{k=0}^{m-1}\eta_{w,k}=\sigma_w}\prod_{j=1}^{w}\binom{\sigma_j}{\eta_{j,0},\eta_{j,1},\ldots,\eta_{j,m-1}}b\beta^{g(\eta,e)t}.\end{aligned}$$

where

$$g(\eta,e)=\sum_{k=0}^{m-1}q^k\sum_{j=1}^{w}\eta_{j,k}p^{e_j},\quad b=\alpha^{ig(\eta,e)}.$$

We firstly show that all the exponents of β are pairwise distinct mod q^m-1, then we show that the exponents of α in S_i^σ are pairwise distinct mod q^m-1 if we choose some proper σ. Let

$$g(\eta,e)\equiv g(\eta',e)(\ mod\ q^m-1)$$

where η and η' denote two different vectors. Since $\sigma=\sum_{j=1}^{w}\sigma_j p^{e_j}$, $0<\sigma<q-1$, and $0\le\eta_{j,k}\le\sigma_j$, $0\le\eta'_{j,k}\le\sigma_j$, for $j=1,2,\ldots,w$, $k=0,1,\ldots,m-1$, $g(\eta,e)$ is less than q^m-1 and the modulo operation can be omitted:

$$\begin{aligned}&q^0(\eta_{1,0}p^{e_1}+\eta_{2,0}p^{e_2}+\ldots+\eta_{w,0}p^{e_w})\\ &+q^1(\eta_{1,1}p^{e_1}+\eta_{2,1}p^{e_2}+\ldots+\eta_{w,1}p^{e_w})\\ &\vdots\\ &q^{m-1}(\eta_{1,m-1}p^{e_1}+\eta_{2,m-1}p^{e_2}+\ldots+\eta_{w,m-1}p^{e_w})\\ &=q^0(\eta'_{1,0}p^{e_1}+\eta'_{2,0}p^{e_2}+\ldots+\eta'_{w,0}p^{e_w})\\ &+q^1(\eta'_{1,1}p^{e_1}+\eta'_{2,1}p^{e_2}+\ldots+\eta'_{w,1}p^{e_w})\\ &\vdots\\ &q^{m-1}(\eta'_{1,m-1}p^{e_1}+\eta'_{2,m-1}p^{e_2}+\ldots+\eta'_{w,m-1}p^{e_w}).\end{aligned}$$

We consecutively reduce the above equation modulo q^k for $k=0,1,\ldots,m-1$, and we have $\eta_{j,k}=\eta'_{j,k}$ for $j\in\{1,2,\ldots,w\}$ and $k\in\{0,1,\ldots,m-1\}$. Therefore, we obtain that all of the exponents of β in $S_i^\sigma(t)$

are pairwise distinct. In the following, we show that the exponents of α in S_i^σ are pairwise distinct mod $q^m - 1$ under some conditions.
Since $\beta = \alpha^N$, we suppose that there exist $g(\eta, e)$ and $g(\eta', e)$ such that $\sigma \leq g(\eta, e) < g(\eta', e) \leq \sigma q^{m-1}$ and

$$\alpha^{Ng(\eta,e)} = \alpha^{Ng(\eta',e)}.$$

As the order of α is equal to $q^m - 1$, it follows that

$$q^m - 1 | N(g(\eta', e) - g(\eta, e)) \tag{8}$$

that is,

$$\frac{q^m - 1}{N} |(g(\eta', e) - g(\eta, e)).$$

Note that

$$g(\eta', e) - g(\eta, e) = \sum_{k=0}^{m-1} q^k \sum_{j=1}^{w} (\eta_{j,k} - \eta'_{j,k}) p^{e_j}$$

and $0 < \sigma_j \leq [\frac{p-1}{N}]$, $0 \leq \eta_{j,k}, \eta'_{j,k} \leq \sigma_j$ for $j=1,2,\ldots,w$, $k=0,1,\ldots,m-1$. Therefore, we have

$$g(\eta', e) - g(\eta, e) < \frac{q^m - 1}{N}$$

so that $q^m - 1$ does not divide $N(g(\eta', e) - g(\eta, e))$, which contradicts (8). Therefore, the exponents of α are pairwise distinct.
The linear complexity of S_i^σ can be computed as follows. Note that there are

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

possibilities to represent σ_j as

$$\sigma_j = \sum_{k=0}^{m-1} \eta_{j,k}, \; for \; 0 \leq \eta_{j,k} \leq \sigma$$

and by applying this result to all σ_j's, the linear complexity is equal to

$$\prod_{j=1}^{w} \binom{m + \sigma_j - 1}{\sigma_j}$$

as desired.

Example 1 *Let $p = 4r(2t+1)+1$ be a prime, where $t \geq 1$ is a positive integer, and r is an odd with $gcd(r, 2t+1) = 1$. Let $q = p$, and $N = 8r$. It is obvious that $p-1 \; \equiv N/2 \; mod \; N$. If $m = 2$, then $n = (p-1)(p+1)/N = \frac{(p+1)}{2}\frac{(p-1)}{4r}$. Since $gcd(\frac{(p+1)}{2}, \frac{(p-1)}{2}) = 1$, we have $gcd(n, N) = 1$. $gcd((p^2-1)/(p-1) mod N, N) =$*

$gcd((p+1)modN, N) = gcd(4r+2, 8r) = 2$. Therefore, $\mathcal{S}$ is a $((p^2-1)/8r$, $8r$, $(2p^2-2p-1)/(8pr); p)$ optimal set of frequency hopping sequences, meeting the bound of (4). Now, we choose a $\sigma \leq [\frac{p-1}{8r}] = t$ with $gcd(\sigma, p-1) = 1$, and construct the transformed set $\mathcal{S}^\sigma$, then by theorem 3, the sequences in $\mathcal{S}^\sigma$ have much larger linear complexity than the ones in $\mathcal{S}$.

REMARK 1 *In Theorem 3, the power permutations meeting the $0 < \sigma_j \leq [\frac{p-1}{N}]$ can be employed in improving the linear complexity of the frequency hopping sequences in the general construction. Therefore, our method applies to the general construction of the optimal set with relatively large prime p, but the chosen power permutation can significantly improve the linear complexity of the frequency hopping sequences in the general construction when a large prime p is used.*

4. The linear complexity of the frequency hopping sequences transformed by binomial permutation

In this section, we improve the linear complexity of the frequency hopping sequences from Lemma 3 by using a binomial permutation $P(x)$, see Laigle-Chapuy (2007). The linear complexity of the transformed sequences could be higher than that of the sequences in Theorem 2.

LEMMA 4 *Let l and d be two positive integers. Let k be the order of p in Z/dZ. Take $q = p^{kld}$, and r a positive integer coprime with $q-1$. If $a \in F_{p^{kl}}$, then the binomial*

$$P(x) = x^r(x^{\frac{q-1}{d}} + a)$$

is a permutation polynomial over F_q if and only if $(-a)^d \neq 1$.

Both $x^{r+\frac{q-1}{d}}$ and ax^r in $P(x)$ are power permutations, since two exponents are coprime with $q-1$ as shown in the following lemma, Laigle-Chapuy (2007).

LEMMA 5 *Let l,k be two positive integers. Let d be a divisor of p^k-1 and r be coprime with $p^{kld}-1$. Then*

$$gcd(p^{kld}-1, \frac{p^{kld}-1}{d} + r) = 1.$$

We transform the optimal set of frequency hopping sequences from Lemma 3 into a novel optimal set by employing the binomial permutation $P(x)$, and give the exact value of the linear complexity of the transformed frequency hopping sequences in the novel optimal set.

THEOREM 4 *Let l and d be two positive integers. Let k be the order of p in Z/dZ. Take $q = p^{kld} \equiv 1(mod\ 4)$, $m = 2$, $N = 2(q-1)$ and $n = (q+1)/2$. Let $r = \sum_{j=1}^{w} r_j p^{e_j}$, $r + \frac{q-1}{d} \equiv \sum_{j=1}^{w} \theta_j p^{e_j}$ mod $(q-1)$ be two positive integers with*

$0 < r < q-1$ such that $gcd(r, q-1) = 1$, where $0 \leq r_j \leq p-1$, $0 \leq \theta_j \leq p-1$, and $0 \leq e_1 < e_2 \ldots < e_w < kld$. Define $P(\mathcal{S}) = \{P(S_i) : 0 \leq i \leq N-1\}$, where S_i is defined by (6). Then

(1) *$P(\mathcal{S})$ is $((q+1)/2, 2(q-1), 1; q)$ optimal set of frequency hopping sequences, meeting the bound of (4).*

(2) *The linear complexity of the transformed frequency hopping sequences can be high compared to their length $n = (q+1)/2$. In particular, if $\theta_j + r_j < (p-1)/2$ for $j = 1, 2, \ldots, w$ and there is at least one $\theta_j - r_j \neq 2(l_j - k_j)$ for $j = 1, 2, \ldots, w$, then the linear complexity of the transformed frequency hopping sequences is equal to*

$$\prod_{j=1}^{w}(\theta_j + 1) + \prod_{j=1}^{w}(r_j + 1).$$

Proof:

(1) Since $P(x) = x^r(x^{\frac{q-1}{d}} + a)$ is a binomial permutation over F_q, we know that $P(S_i)$ is a permutation sequence of S_i. The Hamming correlations in $P(\mathcal{S})$ are still optimal. $P(\mathcal{S})$ is also a $((q+1)/2, 2(q-1), 1; q)$ optimal set of frequency hopping sequences.

(2) Note that $S_i(t) = Tr_1^2(\alpha^i\beta^t) = \alpha^i\beta^t + (\alpha^i\beta^t)^q$. Then

$$\begin{aligned}
P(S_i) \quad &= (Tr_1^2(\alpha^i\beta^t))^{r+\frac{q-1}{d}} + a(Tr_1^2(\alpha^i\beta^t))^r \\
&= (\alpha^i\beta^t + (\alpha^i\beta^t)^q)^{r+\frac{q-1}{d}} + a(\alpha^i\beta^t + (\alpha^i\beta^t)^q)^r \\
&= (\alpha^i\beta^t + (\alpha^i\beta^t)^q)^{\sum_{j=1}^{w}\theta_j p^{e_j}} + a(\alpha^i\beta^t + (\alpha^i\beta^t)^q)^{\sum_{j=1}^{w} r_j p^{e_j}}. \\
&= \prod_{j=1}^{w}(\alpha^{ip^{e_j}}\beta^{tp^{e_j}} + (\alpha^{ip^{e_j}}\beta^{tp^{e_j}})^q)^{\theta_j} + a\prod_{j=1}^{w}(\alpha^{ip^{e_j}}\beta^{tp^{e_j}} + (\alpha^{ip^{e_j}}\beta^{tp^{e_j}})^q)^{r_j}
\end{aligned}$$

Here, we define

$$S_i^{\theta} = \prod_{j=1}^{w}(\alpha^{ip^{e_j}}\beta^{tp^{e_j}} + (\alpha^{ip^{e_j}}\beta^{tp^{e_j}})^q)^{\theta_j}$$

and

$$S_i^{r} = \prod_{j=1}^{w}(\alpha^{ip^{e_j}}\beta^{tp^{e_j}} + (\alpha^{ip^{e_j}}\beta^{tp^{e_j}})^q)^{r_j}.$$

Therefore, $P(S_i) = S_i^{\theta} + S_i^{r}$. We first consider the exponents of α in S_i^r. Using the binomial formula,

$$(x+y)^n = \sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k}$$

where we take $\binom{0}{k} = 1$, then

$$\begin{aligned}&\prod_{j=1}^{w}(\alpha^{ip^{e_j}}\beta^{tp^{e_j}} + (\alpha^{ip^{e_j}}\beta^{tp^{e_j}})^q)^{r_j}\\ &= \prod_{j=1}^{w}\sum_{k_j=0}^{r_j}\binom{r_j}{k_j}(\alpha^{ip^{e_j}}\beta^{tp^{e_j}})^{k_j+q(r_j-k_j)}\\ &= \sum_{k_1=0}^{r_1}\sum_{k_2=0}^{r_2}\cdots\sum_{k_w=0}^{r_w}\prod_{j=1}^{w}\binom{r_j}{k_j}\alpha^{ig(k,e)}\alpha^{Ntg(k,e)}\end{aligned}$$

where

$$g(k,e) = \sum_{j=1}^{w}k_jp^{e_j} + q\sum_{j=1}^{w}(r_j - k_j)p^{e_j},\ k = (k_1, k_2, \ldots, k_w),\ e = (e_1, e_2, \ldots, e_w). \tag{9}$$

We show that all the exponents $g(k,e)$ of α in S_i^r are pairwise distinct modulo $q^2 - 1$. Assume that two different parameters k and k' generate the same exponent of α modulo $q^2 - 1$, that is,

$$Ng(k,e) \equiv Ng(k',e)\ mod\ (q^2 - 1).$$

Since $N = 2(q-1)$, we obtain

$$g(k,e) \equiv g(k',e)\ mod\ (\frac{q+1}{2}). \tag{10}$$

With the equations (9) and (10), we obtain that

$$\sum_{j=1}^{w}k_jp^{e_j} + q\sum_{j=1}^{w}(r_j - k_j)p^{e_j} \equiv \sum_{j=1}^{w}k'_jp^{e_j} + q\sum_{j=1}^{w}(r_j - k'_j)p^{e_j}\ mod\ (\frac{q+1}{2}).$$

Note that $q \equiv -1\ mod\ (\frac{q+1}{2})$, and then it follows that

$$\sum_{j=1}^{w}2(k_j - k'_j)p^{e_j} \equiv 0\ mod\ (\frac{q+1}{2}).$$

Since $q \equiv 1\ mod\ 4$, we have $gcd(2, \frac{q+1}{2}) = 1$. It follows that

$$\sum_{j=1}^{w}(k_j - k'_j)p^{e_j} \equiv 0\ mod\ (\frac{q+1}{2}). \tag{11}$$

Note that $0 \leq k_j \leq r_j \leq \frac{p-1}{2}$, $0 \leq k'_j \leq r_j \leq \frac{p-1}{2}$ for $j = 1, 2, \ldots, w$. This implies that $-\frac{p-1}{2} \leq k_j - k'_j \leq \frac{p-1}{2}$ for $j = 1, 2, \ldots, w$. Since

$$\frac{q+1}{2} = \frac{p-1}{2}(p + p^2 + \cdots + p^{s-1}) + \frac{p+1}{2}$$

and $0 \leq r_j \leq \frac{p-1}{2}$, we have that the equation (11) can not be satisfied unless $k_j - k'_j = 0$ for $j = 1, 2, \ldots, w$, which implies that the exponents of α in S_i^r are pairwise distinct modulo $q^2 - 1$. Similarly, we can show that the exponents of α in S_i^θ are pairwise distinct modulo $q^2 - 1$.

In the following, we show that the exponents of α in S_i^θ are pairwise distinct with those of α in S_i^r. Note that

$$\begin{aligned} S_i^\theta &= \prod_{j=1}^{w} (\alpha^{ip^{e_j}} \beta^{tp^{e_j}} + (\alpha^{ip^{e_j}} \beta^{tp^{e_j}})^q)^{\theta_j} \\ &= \prod_{j=1}^{w} \sum_{l_j=0}^{\theta_j} \binom{\theta_j}{l_j} (\alpha^{ip^{e_j}} \beta^{tp^{e_j}})^{l_j + q(\theta_j - l_j)} \\ &= \sum_{l_1=0}^{\theta_1} \sum_{l_2=0}^{\theta_2} \cdots \sum_{l_w=0}^{\theta_w} \prod_{j=1}^{w} \binom{\theta_j}{l_j} \alpha^{ig(l,e)} \alpha^{Ntg(l,e)} \end{aligned}$$

where

$$g(l,e) = \sum_{j=1}^{w} l_j p^{e_j} + q \sum_{j=1}^{w} (\theta_j - l_j) p^{e_j},\ l = (l_1, l_2, \ldots, l_w),\ e = (e_1, e_2, \ldots, e_w). \tag{12}$$

Assume that k and l generate the same exponents of α, that is,

$$Ng(l,e) \equiv Ng(k,e)\ mod\ (q^2 - 1). \tag{13}$$

Similarly, we have

$$\sum_{j=1}^{w} l_j p^{e_j} + q \sum_{j=1}^{w} (\theta_j - l_j) p^{e_j} \equiv \sum_{j=1}^{w} k_j p^{e_j} + q \sum_{j=1}^{w} (r_j - k_j) p^{e_j}\ mod\ (\frac{q+1}{2}). \tag{14}$$

Note that $q \equiv -1\ mod\ (\frac{q+1}{2})$, and so we have

$$\sum_{j=1}^{w} ((\theta_j - l_j) - (r_j - k_j) + k_j - l_j) p^{e_j} \equiv 0\ mod\ (\frac{q+1}{2}). \tag{15}$$

Since $0 \leq k_j \leq r_j$ and $0 \leq l_j \leq \theta_j$ for $j = 1, 2, \ldots, w$, we have

$$-(\theta_j + r_j) \leq (\theta_j - l_j) - (r_j - k_j) + k_j - l_j \leq \theta_j + r_j,\ for\ j = 1, 2, \ldots, w.$$

If $\theta_j + r_j \leq \frac{p-1}{2}$ for $j = 1, 2, \ldots, w$, then the equation (15) can not be satisfied unless $\theta_j - r_j = 2(l_j - k_j)$ for $j = 1, 2, \ldots, w$. Therefore, if $\theta_j + r_j \leq \frac{p-1}{2}$ for $j = 1, 2, \ldots, w$ and there is at least one $\theta_j - r_j \neq 2(l_j - k_j)$ for $j = 1, 2, \ldots, w$, then all the exponents of α in the representations of S_i^θ and S_i^r are pairwise distinct modulo $q^2 - 1$. By counting the number of the roots in the sequence representation, we can know that the linear complexity of the frequency hopping sequences in $P(\mathcal{S})$ is equal to

$$\prod_{j=1}^{w}(\theta_j + 1) + \prod_{j=1}^{w}(r_j + 1).$$

5. Implementations

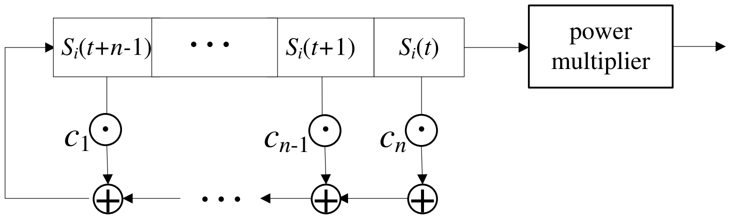

Figure 1. Implementation of the transformed frequency hopping sequences

The transformed frequency hopping sequences with large linear complexity can be easily implemented, as illustrated in Fig. 1. Symbol $\boxed{S_i(t)}$ in Fig. 1 denotes a storage element which holds one symbol in the field F_q. $\boxed{S_i(t)}$ holds its symbol until a clock signal is applied. In Fig. 1, all of these $\boxed{S_i(t)}$ storages are clocked simultaneously. The box containing the 'Power multiplier' denotes an implementation of the permutation polynomial by multiplications. The original frequency hopping sequences are constructed by trace functions, which can be implemented by linear feedback shift register, see Lidl and Harald (1983). Since the transformed frequency hopping sequences are constructed by using a permutation polynomial over the original sequences, we can implement the transformed frequency hopping sequences by appending a permutation polynomial to the linear feedback shift register, and the permutation polynomial can be implemented by some simple power multiplications and additions. Therefore, at a low cost (only adding a permutation polynomial), we obtain two optimal sets of frequency hopping sequences with larger linear complexities than the original optimal set.

6. Comparisons and conclusions

We have determined the linear complexities of the frequency hopping sequences in two new optimal sets, which are transformed by power permutation and binomial permutation, respectively. Table 1 describes the parameters and their linear complexities of the frequency hopping sequences in the related optimal sets. From Table 1, we see that the frequency hopping sequences in two original optimal sets have small linear complexities, however, the frequency hopping sequences in two new optimal sets have higher linear complexities than the original frequency hopping sequences. Our results have the advantages over the existing results as follows:

1) The original power permutation, see Wang (2011) is only suitable for the optimal set of frequency hopping sequences of Lemma 3, which is an optimal set with special parameters. Our permutation from Theorem 3 is suitable for the optimal set of a general construction. Observing the sixth row in Table 1, we see that the linear complexity of the transformed frequency hopping sequences in the general construction can be high compared to the sequence length. We have proven that some chosen power permutations apply to the optimal set of the general construction in Theorem 1 for improving the linear complexity.

2) Wang noted that besides the power permutation, other types of permutation polynomials could also be used for improving the linear complexity of the frequency hopping sequences in the optimal set, but it could be difficult to obtain the value of linear complexity, see Wang (2010). Here, we use the binomial permutation $P(x)$ to improve the linear complexity, and obtain the exact value of the linear complexity of the transformed frequency hopping sequences. Observing the third row and the fourth row in Table 1, we see that the linear complexity of the frequency hopping sequences transformed by binomial permutation can be higher than that transformed by some chosen power permutations.

3) From Theorems 3 and 4, we know that both of the transformed optimal sets of frequency hopping sequences are novel optimal sets. They are different from the existing optimal sets. The frequency hopping sequences in the transformed optimal sets (the fourth and the sixth row in Table 1) have higher linear complexities than the frequency hopping sequences in the original optimal sets (the second and the fifth row in Table 1). They are stronger to resist the Berlekamp-Massey algorithm than the original sequences.

The methodology used for calculating the linear complexity is to count the number of the roots in the sequence representation. It is a traditional and efficient technique to derive the linear complexity of the sequence constructed by trace function, see Golomb and Gong (2005). Our contributions focus on two aspects. The first one is that we generalize one of the Wang's conclusions and find some power permutations which are suitable for the optimal set of the

Table 1. Comparisons of several optimal sets

The Optimal Set	Linear Complexity
$((q+1)/2, 2(q-1), 1; q)$, see Wang (2011).	2
$((q+1)/2, 2(q-1), 1; q)$ transformed by power permutation, see Wang (2011).	$\prod_{j=1}^{w}(\sigma_j+1)$
$((q+1)/2, 2(q-1), 1; q)$ transformed by binomial permutation. This paper, Theorem 4.	$\prod_{j=1}^{w}(\theta_j+1)+\prod_{j=1}^{w}(r_j+1)$
$((q^m-1)/N,\ N,\ (q^m-1-q$ $+(q-1)\sqrt{q^m})/(qN);\ q)$, see Wang (2011)	m
$((q^m-1)/N,\ N,\ (q^m-1-q$ $+(q-1)\sqrt{q^m})/(qN);\ q)$ transformed by power permutation. This paper, Theorem 3.	$\prod_{j=1}^{w}\binom{m+\sigma_i-1}{\sigma_i}$.

general construction with a large prime p. The second one is that we employ the binomial permutation in improving the linear complexity of the frequency hopping sequences in an optimal set. The transformed optimal set is a novel optimal set, which is different from the existing ones. All of the values of the linear complexities of the transformed frequency hopping sequences in Theorem 3 or 4 depend on the chosen permutations, and may be high compared to the sequence length if the permutations are properly chosen. In addition, the binomial permutation can be suitable for other optimal sets of frequency hopping sequences, but it could be complicated to obtain the exact value of the linear complexity.

We have given two optimal sets of frequency hopping sequences with higher linear complexity than the original optimal sets. The two optimal sets have better ability to resist the Berlekamp-Massey algorithm than the original optimal sets, however, large linear complexity does not imply that these sequences can resist various cryptanalytic methods, such as correlation attack, see Meier and Staffelbach (1998), algebraic attack, see Courtois and Meier (2003), etc., in that large linear complexity is only a necessary condition to resist the Berlekamp-Massey algorithm. Our future work will focus on the ability of these transformed frequency hopping sequences to resist some definite cryptanalytic methods.

Acknowledgment

The research reported in this paper was supported by the Natural Science Foundation of China (No. 60833008), the 111 project (No. B08038), the Fundamental Research Funds for the Central Universities (No. K50511010007), the Scientific Research Foundation of Education Department of Shaanxi Provincial Government of China (No. 11JK0503), and Science and Technology on Communication Security Laboratory (No. 9140C110201110C1102). We would like to thank the chairs, committee, and reviewers of the security track of the INCoS 2011 conference.

7. References

Bogart, K. Stein, C. and Drysdale, R. L. (2005) *Discrete Mathematics for Computer Science.* Key College Publishing, Emeryville, California, U.S.A..

Chu, W. and Colbourn, C. J. (2005) Optimal frequency-hopping sequences via cyclotomy. *IEEE Trans. Inf. Theory*, **51**(3), 1139-1141.

Courtois, N. and Meier, W.(2003) Algebraic attacks on stream ciphers with linear feedback. *Lecture Notes in Computer Science*, **2656**, 345-359. Springer-Verlag.

Ding, C. Fuji-Hara, R. Fujiwara, Y. Jimbo, M. and Mishima, M.(2009) Sets of frequency hopping sequences: bounds and optimal constructions. *IEEE Trans. Inf. Theory*, **55**(7), 3297-3304.

Ding, C. Miosio, M. J. and Yuan, J. (2007) Algebraic constructions of optimal frequency hopping sequences. *IEEE Trans. Inf. Theory*, **53**(7), 2606-2610.

Ding, C. and Yin J. (2008) Sets of optimal frequency hopping sequences. *IEEE Trans. Inf. Theory*, **54**(8), 3741-3745.

Fuji-Hara, R. Miao, Y. and Mishima, M. (2004) Optimal frequency hopping sequences: A combinatorial approach. *IEEE Trans. Inf. Theory*, **50**(10), 2408-2420.

Ge, G. Fuji-Hara, R. and Miao, Y. (2006) Further combinatorial constructions for optimal frequency hopping sequences. *J. Comb Theory A*, **113**(8), 1699-1718.

Ge, G. Miao, Y. and Yao, Z. (2009) Optimal frequency hopping sequences: Auto- and cross-correlation properties. *IEEE Trans. Inf. Theory*, **55**(2), 867-879.

Golomb, S. W. and Gong, G. (2005) *Signal Design for Good Correlation, for Wireless Communication, Cryptography, and Radar.* Cambridge Univ. Press, Cambridge, U.K.

Komo, J. J. and Liu, S. C. (1990) Maximal length sequences for frequency hopping. *IEEE J. Sel. Areas Commun.*, **8**(5), 819-822.

Kumar, P. V. (1988) Frequency-hopping code sequence designs having large linear span. *IEEE Trans. Inf. Theory*, 34(1), 146-151.

Laigle-Chapuy, Y. (2007) Permutation polynomials and applications to coding theory. *Finite Fields Th. App.*, **13**(1), 58-70.

Lempel, A. and Greenberger, H. (1974) Families of sequences with optimal Hamming correlation properties. *IEEE Trans. Inf. Theory*, **20**(1), 90-94.

Lidl, R. and Harald, N. (1983) *Finite fields. Encyclopedia of Mathematics and Its Applications*, **20**. Addison-Wesley, Reading, Massachusetts, U.S.A..

Meier, W. and Staffelbach, O. (1998) Fast correlation attacks on stream ciphers. *Lecture Notes in Computer Science* **330**, 301-314.

PENG, D. and FAN, P. (2004) Lower bounds on the Hamming auto- and cross correlations of frequency-hopping sequences. *IEEE Trans. Inf. Theory*, **50**(9), 2149-2154.

SIMON, M. K. OMURA, J. K. SCHOLZ, R. A. and LEVITT, B. K. (2002) *Spread Spectrum Communications Handbook*. McGraw-Hill, New York, U.S.A.

UDAYA, P. and SIDDIQI, M. U. (1998) Optimal large linear complexity frequency hopping patterns derived from polynomial residue class rings. *IEEE Trans. Inf. Theory*, **44**(4), 1492-1503.

WANG, Q. (2010) Optimal sets of frequency hopping sequences with large linear spans. *IEEE Trans. Inf. Theory*, **56**(4), 1729-1736.

WANG, Q. (2011) The linear span of the frequency hopping sequences in optimal sets. *Design. Code. Cryptogr.*, **61**(3), 331-344.

ZHOU, Z. and TANG, X. (2009) A new construction of optimal frequency hopping sequence sets. In: *Proceedings of IWSDA 2009*, Fukuoka, Japan. IEEE Press, New Jersey, 92-95.