Linear Complexity of Two Classes of Binary Interleaved Sequences with Low Autocorrelation

Shidong Zhang[1,2], Tongjiang Yan[1,2], Yuhua Sun[1,3], Lianhai Wang[3]
(Corresponding author: Tongjiang Yan)

College of Science, China University of Petroleum, Qingdao, Shandong 266580, China[1]
Key Laboratory of Applied Mathematics, Fujian Province University (Putian University), Fujian 350117, China[2]
Qilu University of Technology (Shandong Academy of Sciences), Shandong Computer Science Center (National Supercomputer Center in Jinan), Shandong Provincial Key Laboratory of Computer Networks[3]
(Email: yantoji@163.com)

(Received Sep. 28, 2018; Revised and Accepted Dec. 7, 2018; First Online Jan. 11, 2019)

Abstract

The linear complexity of a key stream sequence in a stream cipher is an important cryptographic property. In this paper, we discuss the linear complexity of two classes of binary interleaved sequences of period $4N$ with low autocorrelation. Results show that the linear complexity of these two classes of sequences is large enough to resist the Berlekamp-Massey algorithm.

Keywords: Interleaved Sequence; Linear Complexity; Minimal Polynomial; Stream Cipher

1 Introduction

Sequences with good autocorrelation and large linear complexity have many applications in cryptography and communication systems [3, 10, 14].

Given two binary sequences $a = (a_t)_{t=0}^{\infty}$ and $b = (b_t)_{t=0}^{\infty}$ of period n defined on the Galois field $GF(2)$, the periodic correlation between them is defined by

$$R_{a,b}(\tau) = \sum_{t=0}^{n-1}(-1)^{a(t)+b(t+\tau)}, 0 \le \tau < n,$$

where the addition $t+\tau$ is performed modulo n. If $a = b$, $R_{a,b}(\tau)$ is called the (periodic) autocorrelation function of a, denoted by $R_a(\tau)$, otherwise, $R_{a,b}(\tau)$ is called the (periodic) cross-correlation function of a and b [13].

Binary sequences with optimal autocorrelation values can be classified into four types as follows according to the remainders of n modulo 4: (1) $R_a(\tau) = -1$ if $n \equiv 3 \bmod 4$; (2) $R_a(\tau) \in \{-2, 2\}$ if $n \equiv 2 \bmod 4$; (3) $R_a(\tau) \in \{1, -3\}$ if $n \equiv 1 \bmod 4$; (4) $R_a(\tau) \in \{0, -4\}$ or $\{0, 4\}$ if $n \equiv 0 \bmod 4$, where $0 < \tau < n$ [7]. In the first case, $R_a(\tau)$ is often called ideal autocorrelation. For the last type, if $R_a(\tau) \in \{0, \pm 4\}$, $R_a(\tau)$ is called almost optimal autocorrelation. For more details about optimal autocorrelation, the reader is referred to [1, 10, 12]. However, in applications, sequences with low autocorrelation values rather than optimal autocorrelation values also play important roles.

The linear complexity of a sequence is often described in terms of the shortest linear feedback shift register (LFSR) that generates the sequence. Generally speaking, for a sequence with the linear complexity is $LC(s)$, if $2LC(s)$ consecutive elements of the sequence are known, then we can find the linear recurrence relation of the sequence by solving homogeneous linear equations or B-M algorithm. Thus the whole sequence can be recovered easily [6, 15]. So the linear complexity of a key sequence must be large enough to oppugn the known-plaintext attack [2, 5].

In [9], we have proposed two new constructions of binary interleaved sequences of period $4N$ as the following:

$$a = \mathbf{I}(s^1, L^d(\overline{s^1}), s^2, L^d(\overline{s^2})). \tag{1}$$

$$a = \mathbf{I}(s^1, L^d(\overline{s^1}), \overline{s^2}, L^d(s^2)). \tag{2}$$

where s^1 is the even decimated sequence of a binary ideal autocorrelation sequence s of period N, s^2 is the odd decimated sequence of the sequence s, $\overline{s^1}$ and $\overline{s^2}$ are the complement sequences of s^1 and s^2 respectively, and d is an arbitrary integer. We have proved that both these two interleaved sequences have low autocorrelation, especially, when $d = \frac{N+1}{4}$, the sequence a in Equation (2) is a binary sequence with almost optimal autocorrelation. Ideally, a key stream sequence need to combine the low autocorrelation property with large linear complexity. So we continue to discuss the linear complexity of these two classes of sequences in this paper.

The remainder of this paper is organized as follows. Section 2 introduces some related definitions and lemmas which would be used later. In Section 3, we give both the minimal polynomials and linear complexity of these two sequences defined by Equations (1) and (2). Conclusions and remarks are given in Section 4.

2 Preliminaries

Definition 1. *[8] Let $\{a_0, a_1, \cdots, a_{T-1}\}$ be a set of T sequences of period N. An $N \times T$ matrix U is formed by placing the sequence a_i on the ith column, where $0 \le i \le T-1$. Then one can obtain an interleaved sequence u of period NT by concatenating the successive rows of the matrix U. For simplicity, the interleaved sequence u can be written as*

$$u = \mathbf{I}(a_0, a_1, \cdots, a_{T-1}),$$

where $\mathbf{I}$ denotes the interleaved operator.

Definition 2. *[8] Let $s = (s_i)_{i=0}^{\infty}$ be a sequence over a Galois field $GF(2)$. A polynomial of the form*

$$f(x) = 1 + c_1x + c_2x^2 + \cdots + c_rx^r \in GF[x]$$

is called the characteristic polynomial of the sequence s if

$$s_i = c_1s_{i-1} + c_2s_{i-2} + \cdots + c_rs_{i-r}, \forall i \ge r.$$

Among all the characteristic polynomials of s, the monic polynomial $m_s(x)$ with the lowest degree is called its minimal polynomial. The linear complexity of s is defined as the degree of $m_s(x)$, which is described as $\mathbf{LC}(s)$.

Definition 3. *[8] Let $s = (s_i)_{i=0}^{\infty}$ be a binary sequence of period N and define the sequence polynomial*

$$s(x) = s_0 + s_1x + \cdots + s_{N-1}x^{N-1}. \tag{3}$$

Then, its minimal polynomial and linear complexity can be determined by Lemma 1.

Lemma 1. *[14] Assume s is a sequence of period N with the sequence polynomial s(x) defined by Equation (3). Then the minimal polynomial is*

$$m_s(x) = \frac{x^N - 1}{\gcd(x^N - 1, s(x))};$$

the linear complexity is

$$\mathrm{LC}(s) = N - \deg(\gcd(x^N - 1, s(x))),$$

where $\gcd(x^N - 1, s(x))$ denotes the greatest common divisor of $x^N - 1$ and $s(x)$.

For the sequence polynomial, we have the following results.

Lemma 2. *[11] Let a be a binary sequence of period N, and $s_a(x)$ be its sequence polynomial. Then*

1) $s_b(x) = x^{N-\tau}s_a(x)$, if $b = L^{\tau}(a)$;

2) $s_b(x) = s_a(x) + \frac{x^N - 1}{x - 1}$, if b is the complement sequence of a;

3) $s_u(x) = s_a(x^4) + xs_b(x^4) + x^2s_c(x^4) + x^3s_d(x^4)$, if $u = \mathbf{I}(a, b, c, d)$.

Lemma 3. *Let N be an odd integer. The even decimated sequence and odd decimated sequence of a binary sequence of period N $s = (s_i)_{i=0}^{\infty}$ is denoted by $s^1 = (s_{2t})_{t=0}^{\infty}$ and $s^2 = (s_{2t+1})_{t=0}^{\infty}$, where $2t$ and $2t+1$ are performed modulo N. Let $s_{s^1}(x)$, $s_{s^2}(x)$ denote the sequence polynomials of s^1, s^2 respectively. Then we have*

$$s_{s^1}(x^4) + x^2s_{s^2}(x^4) = (1 + x^{2N})s(x^2). \tag{4}$$

Proof By Equation (3), $s_{s^1}(x)$, $s_{s^2}(x)$ can be represented as the following

$$\begin{aligned} s_{s^1}(x) &= s_0 + s_2x + s_4x^2 + \cdots + s_{(2(N-1))}x^{N-1} \\ &= \sum_{t=0}^{N-1} s_{2t}x^t, \\ s_{s^2}(x) &= s_1 + s_3x + \cdots + s_{(2(N-1)+1)}x^{N-1} \\ &= \sum_{t=0}^{N-1} s_{2t+1}x^t. \end{aligned}$$

So we have

$$\begin{aligned} & s_{s^1}(x^4) + x^2s_{s^2}(x^4) \\ = \; & s_0 + s_1x^2 + \cdots + s_{N-2}x^{2(N-2)} \\ & + s_{N-1}x^{2(N-1)} + s_0x^{2N} \\ & + s_1x^{2(N+1)} + \cdots + s_{N-1}x^{2(2N-1)} \\ = \; & (1 + x^{2N})s(x^2). \end{aligned}$$

It should be noted that we take the Legendre sequence with period of $N \equiv 3 \bmod 8$ as the base sequence of interleaved structures in Equations (1) and (2). So we have to introduce some preliminaries about Legendre sequences.

Definition 4. *[4] Let $\mathbf{Q}$ and $\mathbf{NQ}$ denote all the quadratic residues and quadratic nonresidues in Z_N respectively, where N is a prime. The Legendre sequence $l = (l_i)_{i=0}^{\infty}$ of period N is defined as*

$$l(i) = \begin{cases} 0 \text{ or } 1, & \text{if } i = 0; \\ 1, & \text{if } i \in \mathbf{Q}; \\ 0, & \text{if } i \in \mathbf{NQ}. \end{cases}$$

Specifically, l is called the first type Legendre sequence if $l(0) = 1$ otherwise the second type Legendre sequence. For simplicity, we employ l and l' to describe the first and second type of Legendre sequences respectively.

Let s be the second type Legendre sequence of period N. Then by Equation (3), we have $s(x) = \sum_{i \in \mathbf{Q}} x^i$.

Lemma 4. *[4] Let β be a primitive Nth root of unity over the field $GF(2^m)$ that is the splitting field of $x^N - 1$. Then we obtain the following basic facts:*

1) $(\mathbf{Q}, \cdot)$ is a group with $|\mathbf{Q}| = (N-1)/2$ and $q \cdot \mathbf{NQ} = \mathbf{NQ}$ for any $q \in \mathbf{Q}$, where $\cdot$ denotes integer multiplication modulo N.

2) $s(\beta^q) = s(\beta)$ for any $q \in \mathbf{Q}$, and $s(\beta^n) = 1 + s(\beta)$ for any $n \in \mathbf{NQ}$.

3) $s(\beta) \in \{0,1\}$ if and only if $2 \in \mathbf{Q}$.

4) $2 \in \mathbf{Q}$ if and only if $N = 8t+1$ for some t.

Let $q(x) = \prod_{q\in\mathbf{Q}}(x-\beta^q)$ and $n(x) = \prod_{n\in\mathbf{NQ}}(x-\beta^n)$. Then

$$x^N - 1 = (x-1)q(x)n(x).$$

3 Minimal Polynomial and Linear Complexity

3.1 The Linear Complexity of the First Class Interleaved Sequences

Theorem 1. *Let $a = \mathbf{I}(s^1, L^d(\overline{s^1}), s^2, L^d(\overline{s^2}))$ be a binary interleaved sequence of period $4N$ defined by Equation (1), where the base sequence s is a Legendre sequence of period $N \equiv 3 \bmod 8$, $d \neq \frac{N+1}{4}$. Then the minimal polynomial is $m_a(x) = x^{2N}+1$, and the linear complexity is $\mathbf{LC}(a) = 2N$.*

Proof By Lemmas 2 and 3, $s_a(x)$ can be written as

$$\begin{aligned}
& s_a(x) \\
= \; & s_{s^1}(x^4) + x s_{L^d(\overline{s^1})}(x^4) + x^2 s_{s^2}(x^4) + x^3 s_{L^d(\overline{s^2})}(x^4) \\
= \; & s_{s^1}(x^4) + x^{4(N-d)+1}(s_{s^1}(x^4) + \frac{x^{4N}-1}{x^4-1}) \\
& + x^2 s_{s^2}(x^4) + x^{4(N-d)+3}(s_{s^2}(x^4) + \frac{x^{4N}-1}{x^4-1}) \\
= \; & (x^{4N-4d+1}+1)s_{s^1}(x^4) + (x^{4N-4d+3}+x^2)s_{s^2}(x^4) \\
& + \frac{x^{4N-1}}{x^4-1}(x^{4N-4d+1}+x^{4N-4d+3}) \\
= \; & (x^{4N-4d+1}+1)(s_{s^1}(x^4) + x^2 s_{s^2}(x^4)) \\
& + x^{4N-4d+1}(1+x^2)\frac{x^{4N}-1}{x^4-1} \\
= \; & (x^{4N-4d+1}+1)(x^{2N}+1)s(x^2) \\
& + x^{4N-4d+1}(1+x^2)\frac{x^{4N}-1}{x^4-1}.
\end{aligned}$$

Since the finite field $GF(2^m)$ with characteristic 2 is the splitting field of x^N-1, we have $x^{4N}-1 = (x^N-1)^4$. Then by Lemma 1

$$\begin{aligned}
& \gcd(x^{4N}-1, s_a(x)) \qquad (5) \\
= \; & (x^2-1)\gcd\Big(\frac{x^{4N}-1}{x^2-1}, x^{4N-4d+1}\frac{x^{4N}-1}{x^4-1} \\
& + (x^{4N-4d+1}+1)s(x^2)\frac{x^{2N}-1}{x^2-1}\Big) \\
= \; & (x^2-1)\gcd\Big(\frac{x^{4N}-1}{x^4-1}, \\
& (x^{4N-4d+1}+1)s(x^2)\frac{x^{2N}-1}{x^2-1}\Big) \\
= \; & (x^2-1)\frac{x^{2N}-1}{x^2-1}\gcd\Big(\frac{x^{2N}-1}{x^2-1}, \\
& (x^{4N-4d+1}+1)s(x^2)\Big).
\end{aligned}$$

Next, we analyse the above Equation (5). By Lemma 4, we have

$$\frac{x^{2N}-1}{x^2-1} = q^2(x)n^2(x) = \prod_{q\in\mathbf{Q}}(x-\beta^q)^2 \prod_{n\in\mathbf{NQ}}(x-\beta^n)^2.$$

So we only need consider whether $x-\beta^j$ is a divisor of $(x^{4N-4d+1}+1)s(x^2)$, where $1 \le j < N$. Since the base sequence s is a Legendre sequence of period $N \equiv 3 \bmod 8$, by 2), 3) and 4) in Lemma 4, we have $s(\beta) \notin \{0,1\}$, $s(\beta^q) = s(\beta)$ for any $q \in Q$, and $s(\beta^n) = 1 + s(\beta)$ for $n \in N$. So $s(\beta^j) \neq 0$ for any $1 \le j < N$. $s(x) \in GF(2)[x]$. Thus

$$s(x^2) = s(x)^2.$$

Then $x-\beta^j$ is not a divisor of $s(x^2)$, where $1 \le j < N$.

Besides, since $d \neq \frac{N+1}{4}$, $4N-4d+1 \not\equiv 0 \bmod N$ and $1+(\beta^j)^{4N-4d+1} \neq 0, 1 \le j < N$. Hence $x-\beta^j$ is not the divisor of $1+x^{4N-4d+1}$, where $1 \le j < N$. Then

$$\gcd\Big(\frac{x^{2N}-1}{x^2-1}, (x^{4N-4d+1}+1)s(x^2)\Big) = 1.$$

According to the above discussion, it follows that $\gcd\Big(x^{4N}-1, s_a(x)\Big) = x^{2N}-1$.

Then by Lemma 1, the minimal polynomial of the sequence a defined in Theorem 1 is $m_a(x) = x^{2N}-1$, and the linear complexity is $\mathbf{LC}(a) = 2N$.

Hence, we complete the proof of Theorem 1.

3.2 The Linear Complexity of the Second Class Interleaved Sequences

Theorem 2. *Let $a = \mathbf{I}(s^1, L^d(\overline{s^1}), \overline{s^2}, L^d(s^2))$ be a binary interleaved sequence of period $4N$ defined by Equation (2), where the base sequence s is a Legendre sequence of period $N \equiv 3 \bmod 8$, $d \neq \frac{N\pm1}{4}$. Then the minimal polynomial is $m_a(x) = (x-1)(x^{2N}-1)$, and the linear complexity is $\mathbf{LC}(a) = 2N+1$.*

Proof By Lemmas 1 and 2, $s_a(x)$ can be written as

$$\begin{aligned}
& s_a(x) \\
= \;& s_{s^1}(x^4) + x s_{L^d(\overline{s^1})}(x^4) + x^2 s_{\overline{s^2}}(x^4) + x^3 s_{L^d(s^2)}(x^4) \\
= \;& s_{s^1}(x^4) + xL^d(s_{s^1}(x^4) + \frac{x^{4N}-1}{x^4-1}) \\
& + x^2(s_{s^2}(x^4) + \frac{x^{4N}-1}{x^4-1}) + x^{4N-4d+3}s_{s^2}(x^4) \\
= \;& (x^{4N-4d+1}+1)s_{s^1}(x^4) + (x^{4N-4d+3}+x^2)s_{s^2}(x^4) \\
& + \frac{x^{4N-1}}{x^4-1}(x^{4N-4d+1}+x^2) \\
= \;& (x^{4N-4d+1}+1)(s_{s^1}(x^4) + x^2 s_{s^2}(x^4)) \\
& + (x^{4N-4d+1}+x^2)\frac{x^{4N}-1}{x^4-1} \\
= \;& (x^{4N-4d+1}+1)(x^{2N}+1)s(x^2) \\
& + x^2(x^{4N-4d-1}+1)\frac{x^{4N}-1}{x^4-1}.
\end{aligned}$$

Next, we consider $\gcd(x^{4N}-1, s_a(x))$. By Lemma 4, we have

$$\begin{aligned}
x^{4N}-1 &= (x-1)^4 q^4(x) n^4(x) \\
&= (x-1)^4 \prod_{q\in\mathbf{Q}}(x-\beta^q)^4 \prod_{n\in\mathbf{NQ}}(x-\beta^n)^4.
\end{aligned}$$

So we only need to consider whether $x-\beta^j, j\in Z_N$, is a divisor of $s_a(x)$. Since the base sequence s is the Legendre sequence of period $N\equiv 3 \bmod 8$, by 2), 3) and 4) in Lemma 4, we have $s(\beta^j)\neq 0$ for any $1\leq j<N$. Then by 1) in Lemma 4, we have

$$s(1) \equiv \frac{N-1}{2} \bmod 2 = 1 \neq 0.$$

So we can obtain $s(\beta^j)\neq 0$ for any $j\in Z_N$. Additionally, since $d\neq \frac{N\pm 1}{4}$, we have $4N-4d+1 \not\equiv 0 \bmod N$ and $4N-4d-1\not\equiv 0 \bmod N$. Thus

$$1+(\beta^j)^{4N\pm 4d+1}\neq 0, 1\leq j<N.$$

Then $x-\beta^j, 1\leq j<N$, is not a divisor of $1+x^{4N-4d+1}$ and $1+x^{4N-4d-1}$. Moreover, since both $4N-4d+1$ and $4N-4d-1$ are odd, $x-1$ is the only nontrivial common divisor of $1+x^{4N-4d+1}$, $1+x^{4N-4d-1}$ and $x^{4N}-1$. Combining the above analysis, we have

$$\begin{aligned}
& \gcd(x^{4N}-1, s_a(x)) \\
= \;& (x-1)\gcd\left(\frac{x^{4N}-1}{x^4-1}, (1+x^{2N}) + \frac{x^{4N}-1}{x^4-1}\right) \\
= \;& (x-1)\frac{x^{2N}-1}{x^2-1} \\
= \;& \frac{x^{2N}-1}{x-1}.
\end{aligned}$$

Then by Lemma 1, the minimal polynomial of the sequence a is

$$m_a(x) = (x-1)(x^{2N}-1),$$

and the linear complexity is $\mathbf{LC}(a) = 2N+1$.

Hence, the proof of Theorem 2 is completed.

Example 1. *Let $s=(0,1,0,1,1,1,0,0,0,1,0)$ be a Legendre sequence of period $N=11$, $d=1$. Then the new binary interleaved sequence $a=\mathbf{I}(s^1, L^d(\overline{s^1}), s^2, L^d(\overline{s^2}))$ of period $4N=44$ defined in Theorem 1 is*

$$\begin{aligned}
a \;=\; & (0,1,1,0,0,0,1,0,1,1,1,1,0,1,0,0,0,1,1,1,0,0, \\
& 0,1,1,0,0,0,1,0,1,1,1,1,0,1,0,0,0,1,1,1,0,0).
\end{aligned}$$

By Magma program, the minimal polynomial of a is $m_a(x)=x^{22}-1$ and the linear complexity of a is $\mathbf{LC}(a)=22$, which are compatible with the results given by Theorem 1.

Example 2. *Let $s=(0,1,0,1,1,1,0,0,0,1,0)$ be a Legendre sequence of period $N=11$, $d=2$. Then the new binary interleaved sequence $a=\mathbf{I}(s^1, L^d(\overline{s^1}), \overline{s^2}, L^d(s^2))$ of period $4N=44$ defined in Theorem 2 is*

$$\begin{aligned}
a \;=\; & (0,0,0,1,0,1,0,0,1,1,0,1,0,1,1,0,0,0,0,0,0,0, \\
& 1,1,1,0,1,0,1,1,0,0,1,0,1,0,0,1,1,1,1,1,1,1).
\end{aligned}$$

By Magma program, the minimal polynomial of a is $m_a(x)=(x-1)(x^{22}-1)$ and the linear complexity of a is $\mathbf{LC}(a)=23$, which are compatible with the results given by Theorem 2.

4 Conclusion

In this paper, based on the discussion of roots of the sequence polynomials in the splitting field of x^N-1, we determine both minimal polynomials and linear complexity of two classes of binary interleaved sequences of period $4N$ with low autocorrelation value/magnitude constructed in [9]. Results show that when the base sequence s is a Legendre sequence of period $N\equiv 3 \bmod 8$, and $d\neq\frac{N\pm 1}{4}$, the linear complexity of these two classes of sequences is enough to resist the Berlekamp-Massey algorithm. Especially, the linear complexity of the first class sequence a is just right one half of its period, which can be applied in the construction of cyclic codes with proper dimension.

Furthermore, apart from autocorrelation property and linear complexity, the 2-adic complexity of these two classes of sequences remains to be solved.

Acknowledgments

This work was supported by Shandong Provincial Natural Science Foundation of China (No. ZR2017MA001, No. ZR2016FL01), the Open Research Fund from Shandong provincial Key Laboratory of Computer Networks, Grant No. SDKLCN-2017-03, Qingdao application research on special independent innovation plan project (No.16-5-1-5-jch), the Open Research Fund from Key Laboratory of Applied Mathematics of Fujian Province University (Putian University) (No.SX201702, No.SX201806), and the Fundamental Research Funds for the Central Universities (No.17CX02030A).

References

[1] K. T. Arasu, C. Ding, T. Helleseth, P. V. Kumar, and H. M. Martinsen, "Almost difference sets and their sequences with optimal autocorrelation," *IEEE Transactions on Information Theory*, vol. 47, no. 7, pp. 2934–2943, 2001.

[2] Z. Chen and V. Edemskiy, "Linear Complexity of Quaternary Sequences Over Z4 Derived From Generalized Cyclotomic Classes Modulo $2p$," *International Journal of Network Security*, vol. 19, no. 4, pp. 613–622, 2017.

[3] T. W. Cusick, C. Ding, and Ari Renvall, *Stream Ciphers and Number Theory*, Amsterdam: Elsevier, 2004.

[4] C. Ding, T. Helleseth, and W. Shan, "On the linear complexity of Legendre sequences," *IEEE Transactions on Information Theory*, vol. 44, no. 3, pp. 1276–1278, 1998.

[5] V. Edemskiy, C. Li, X. Zeng, and T. Helleseth, "The linear complexity of generalized cyclotomic binary sequences of period p^n," *Designs, Codes and Cryptography*, vol. 30, pp. 1–15, 2018.

[6] C. Fan, "The linear complexity of a class of binary sequences with optimal autocorrelation," *Designs, Codes and Cryptography*, vol. 86, no. 10, pp. 2441–2450, 2018.

[7] N. Li and X. Tang, "On the linear complexity of binary sequences of period 4N with optimal autocorrelation value/magnitude," *IEEE Transactions on Information Theory*, vol. 57, no. 11, pp. 7597–7604, 2011.

[8] X. Ma, T. Yan, D. Zhang, and Y. Liu, "Linear complexity of some binary interleaved sequences of period 4N," *International Journal of Network Security*, vol. 18, no. 2, pp. 244–249, 2016.

[9] R. Meng and T. Yan, "New Constructions of two binary interleaved sequences with low autocorrelation," *International Journal of Network Security*, vol. 19, no. 4, pp. 546–560, 2017.

[10] W. Su, Y. Yang, and C. Fan, "New optimal binary sequences with period $4p$ via interleaving Ding-Helleseth-Lam sequences," *Designs, Codes and Cryptography*, vol. 86, no. 6, pp. 1329–1338, 2018.

[11] Q. Wang and X. Du, "The linear complexity of binary sequences with optimal autocorrelation," *IEEE Transactions on Information Theory*, vol. 56, no. 12, pp. 6388–6397, 2010.

[12] T. Yan, "New binary sequences of period pq with low values of correlation and large linear complexity," *International Journal of Network Security*, vol. 10, no. 3, pp. 185–189, 2010.

[13] T. Yan, Z. Chen, and B. Li, "A general construction of binary sequences with optimal autocorrelation," *Information Sciences*, vol. 287, pp. 26–31, 2014.

[14] T. Yan, X. Du, and S. Li, "Trace representations and multi-rate constructions of two classes of generalized cyclotomic sequences," *International Journal of Network Security*, vol. 7, no. 2, pp. 269–272, 2008.

[15] J. Zhou and W. Xiong, "An algorithm for computing m-tight error linear complexity of sequences over $GF(p^m)$ with period pm," *International Journal of Network Security*, vol. 15, no. 1, pp. 59–63, 2013.

Biography

Shidong Zhang was born in 1992 in Shandong Province of China. He was graduated from Jining University . He will study for a postgraduate degree at China University of Petroleum in 2016. And his tutor is Tongjiang Yan. Email: zhangshdo1992@163.com

Tongjiang Yan was born in 1973 in Shandong Province of China. He was graduated from the Department of Mathematics, Huaibei Coal-industry Teachers College, China, in 1996. In 1999, he received the M.S. degree in mathematics from the Northeast Normal University, Lanzhou, China. In 2007, he received the Ph.D. degree in Xidian University. He is now a professor of China University of Petroleum. His research interests include cryptography and algebra. Email: yantoji@163.com

Yuhua Sun was born in 1979. She was graduated from Shandong Normal University, China, in 2001. In 2004, she received the M.S. degree in mathematics from the Tongji University, Shanghai and a Ph.D. in Cryptography from the Xidian University. She is currently a lecturer of China University of Petroleum. Her research interests include cryptography, coding and information theory. Email: sunyuha_1@163.com

Lianhai Wang was born in 1969 in Shandong Province of China. He was graduated from the Department of Mathematics, Shandong University, China, in 1992. In 2003, he received the M.S. degree in computer science from the Shandong University, China, China. In 2014, he received the Ph.D. degree in Shandong University. He is now a professor of Shandong Computer Science Center (National Supercomputer Center in Jinan). His research interests include digital forensics,network security and blockchain. Email: Wanglh@sdas.org