New Constructions of Binary Interleaved Sequences with Low Autocorrelation

Ruifang Meng, Tongjiang Yan
(Corresponding author: Tongjiang Yan)

College of Science, China University of Petroleum, Qingdao, Shandong 266580, China
Key Laboratory of Network Security and Cryptology, Fujian Normal University, Fuzhou, Fujian 350117, China
(Email: yantoji@163.com)

(Received Apr. 24, 2016; revised and accepted June 29 & July 19, 2016)

Abstract

The autocorrelation of a key stream sequence in a stream cipher is an important cryptographic property. This paper proposes two constructions of binary interleaved sequences of period $4N$ by selecting appropriate shift sequences, subsequences and complement sequences. And the autocorrelation functions of new sequences are given. The results show that these sequences have low autocorrelation under certain conditions.

Keywords: Interleaved sequences, low autocorrelation, stream cipher, subsequences

1 Introduction

Pseudorandom sequences with low autocorrelation have wide applications in code-division multi-access system, spread spectrum communication and many other engineering fields [4].

Given two binary sequences $a = a(t)$ and $b = b(t)$ of period N, the periodic correlation between them is defined by

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

where the addition $t+\tau$ is performed modulo N. $R_{a,b}(\tau)$ is called the (periodic) cross correlation function of a and b. If $a = b$, $R_{a,b}(\tau)$ is called the (period) autocorrelation function of a, denoted by $R_a(\tau)$ for short [11].

According to the remainder of N modulo 4, the optimal values of out-of-phase autocorrelations of binary sequences are classified into four types as follows:

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) $R_a(\tau) \in \{0, -4, 4\}$ if $N \equiv 0 \bmod 4$, where $0 < \tau < N$.

In the first case, $R_a(\tau)$ is often called ideal autocorrelation. In the last case, $R_a(\tau)$ is three level, then it can also be called optimal autocorrelation magnitude [11]. Specially, except one point, the out-of-phase autocorrelation values of sequence a are all included in the set $\{0, -4, 4\}$, we call $R_a(\tau)$ almost optimal autocorrelation magnitude [12]. For more details about optimal autocorrelation, the reader is referred to [1, 2, 10].

The interleaved structure of sequences for constructing sequences with low out-of-phase autocorrelation and crosscorrelation was firstly introduced by Gong [5]. There are some known constructions of binary interleaved sequences with low autocorrelation.

In 2010, Tang and Gong gave three new interleaved constructions of binary sequences with low autocorrelation value or magnitude [8]. Subsequently, Yan showed a more general construction and searched for a new construction of binary interleaved sequences with optimal autocorrelation [11].

In 2011, based on an arbitrary ideal autocorrelation sequence, generalized GMW sequence and its modified version, two types of Legendre sequences, twin-prime sequence and its modified version respectively, Zhang,Wen and Qin found five constructions of binary interleaved sequences of period $2N \times 2$ with almost optimal autocorrelation magnitude [12]. Furthermore, Ke and Lin also obtained several binary sequences with optimal autocorrelation value by using decimated sequences [6]. In this paper, we propose two new constructions of binary sequences with low autocorrelation based on interleaving technology.

This paper is organized as follows. Section 2 introduces some related definitions and lemmas which would be used later. In Section 3, we present two new constructions of binary sequences with low autocorrelation magnitude, and give the complete autocorrelation distributions of these sequences. Conclusions are given in Section 4.

2 Preliminaries

2.1 Interleaved Sequence

Definition 1. *[7] 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.

Lemma 1. *[11] Let the binary sequence $s = \mathbf{I}(a_0(k), a_1(k), \cdots, a_{T-1}(k))$, be a binary interleaved sequence of period KT, where $0 \le k \le K-1$, and $T = \tau_1 T + \tau_2$, where $0 \le \tau_2 \le T-1$. Its left shifted version is shown as:*

$$\begin{aligned} L^\tau(s) &= \mathbf{I}(a_{\tau_2}(k+\tau_1), a_{1+\tau_2}(k+\tau_1), \cdots, a_{T-1}(k+\tau_1), \\ &\quad a_0(k+\tau_1+1), \cdots, a_{\tau_2-1}(k+\tau_1+1)), \end{aligned}$$

where L denotes the left cyclic shift operator.

2.2 Subsequence

Lemma 2. *Let N be an odd number, $s = (s(0), s(1), \cdots, s(N-1))$ be a binary sequence of period N. Take two subsequences of sequence s: $s_1 = (s(0), s(2), \cdots, s(2t), \cdots)$ and $s_2 = (s(1), s(3), \cdots, s(2t+1), \cdots)$, where $t = 0, 1, 2, \cdots, N-1$, $2t$ and $2t+1$ are performed modulo N respectively. Then we have some results as follows:*

1) $R_{s_1}(\tau) = R_s(2\tau)$;

2) $R_{s_2}(\tau) = R_s(2\tau)$;

3) $R_{s_1,s_2}(\tau) = R_s(2\tau+1)$;

4) $R_{s_2,s_1}(\tau) = R_s(2\tau-1)$.

Proof By Equation (1), we have

$$\begin{aligned} R_{s_1}(\tau) &= \sum_{t=0}^{N-1} (-1)^{s_1(t)+s_1(t+\tau)} \\ &= \sum_{t=0}^{N-1} (-1)^{s(2t)+s(2t+2\tau)} \\ &= \sum_{t=0}^{N-1} (-1)^{s(t')+s(t'+2\tau)} \\ &= R_s(2\tau), \end{aligned}$$

where $t' = 2t$. So 1) is proved. Similarly, the other three results can be proved obviously.

3 Two New Constructions

In this section, we introduce two new constructions of binary sequences of period $4N$ with low autocorrelation.

3.1 Construction A

Let $N \equiv 3 \pmod 4$, $s = (s(0), s(1), \cdots, s(N-1))$ be a binary ideal autocorrelation sequence of period N. Define a new binary interleaved sequence of period $4N$ as the following:

$$a = I(s_1, L^d(\overline{s_1}), s_2, L^d(\overline{s_2})), \tag{2}$$

where $\overline{s_1}$ is the complement sequence of s_1, $\overline{s_2}$ is the complement sequence of s_2, $d \ne \frac{N+1}{4}$ is an integer. Obviously, the sequence a possesses the balance property with the symbols "1" and "0" [9]. Next we consider the autocorrelation of the new sequence a.

Let $\tau = 4\tau_1 + \tau_2$, $\tau_2 = 0, 1, 2, 3$. By Lemmas 1 and 2, the autocorrelation of sequence a due to four different values of τ_2 can be given by the following.

Case 1. $\tau_2 = 0$, $0 < \tau_1 < N$.

$$\begin{aligned} & R_a(\tau) \\ = \; & R_a(4\tau_1) \\ = \; & R_{s_1}(\tau_1) + R_{L^d(\overline{s_1})}(\tau_1) + R_{s_2}(\tau_1) + R_{L^d(\overline{s_2})}(\tau_1) \\ = \; & 4R_s(2\tau_1). \end{aligned}$$

Since $0 < \tau_1 < N$, $2\tau_1 \ne 0 \pmod N$, $R_s(2\tau_1) = -1$. Then $R_a(\tau) = -4$, and it turns up $N-1$ times altogether.

Case 2. $\tau_2 = 1$, $0 \le \tau_1 < N$.

$$\begin{aligned} & R_a(\tau) \\ = \; & R_a(4\tau_1 + 1) \\ = \; & R_{s_1,\overline{s_1}}(\tau_1 + d) + R_{\overline{s_1},s_2}(\tau_1 - d) \\ & + R_{s_2,\overline{s_2}}(\tau_1 + d) + R_{\overline{s_2},s_1}(\tau_1 + 1 - d) \\ = \; & -R_{s_1}(\tau_1 + d) - R_{s_1,s_2}(\tau_1 - d) \\ & - R_{s_2}(\tau_1 + d) - R_{s_2,s_1}(\tau_1 + 1 - d) \\ = \; & -R_s(2(\tau_1 + d)) - R_s(2(\tau_1 - d) + 1) \\ & - R_s(2(\tau_1 + d)) - R_s(2(\tau_1 + 1 - d) - 1) \\ = \; & -2R_s(2\tau_1 + 2d) - 2R_s(2\tau_1 - 2d + 1). \end{aligned}$$

1) If $\tau_1 = N - d$, $(2\tau_1 + 2d) = 0 \pmod N$, $2\tau_1 - 2d + 1 \ne 0 \pmod N$. Then $R_s(2\tau_1 + 2d) = N$, $R_s(2\tau_1 - 2d + 1) = -1$. So $R_a(\tau) = -2N + 2$;

2) If $\tau_1 = \frac{N+2d-1}{2}$, $2\tau_1 + 2d \ne 0 \pmod N$, $2\tau_1 - 2d + 1 = 0 \pmod N$. Then $R_s(2\tau_1 + 2d) = -1$, $R_s(2\tau_1 - 2d + 1) = N$. So $R_a(\tau) = 2 - 2N$;

3) If $\tau_1 \ne N - d$ and $\tau_1 \ne \frac{N+2d-1}{2}$, $2\tau_1 + 2d \ne 0 \pmod N$ and $2\tau_1 - 2d + 1 \ne 0 \pmod N$. Then $R_s(2\tau_1 + 2d) = R_s(2\tau_1 - 2d + 1) = -1$. So $R_a(\tau) = 4$.

In this case, $R_a(\tau) = -2N + 2$ turns up 2 times, and $R_a(\tau) = 4$ turns up $N - 2$ times.

Case 3. $\tau_2 = 2$, $0 \le \tau_1 < N$.

$$\begin{aligned} & R_a(\tau) \\ = \; & R_a(4\tau_1+2) \\ = \; & R_{s_1,s_2}(\tau_1) + R_{\overline{s_1},\overline{s_2}}(\tau_1) \\ & + R_{s_2,s_1}(\tau_1+1) + R_{\overline{s_2},\overline{s_1}}(\tau_1+1) \\ = \; & R_s(2\tau_1+1) + R_s(2\tau_1+1) \\ & + R_s(2(\tau_1+1)-1) + R_s(2(\tau_1+1)-1) \\ = \; & 4R_s(2\tau_1+1). \end{aligned}$$

1) If $\tau_1 = \frac{N-1}{2}$, $2\tau_1+1 = 0 \pmod N$. Then $R_s(2\tau_1+1) = N$. So $R_a(\tau) = 4N$, and it turns up only 1 time;
2) If $\tau_1 \neq \frac{N-1}{2}$, $2\tau_1+1 \neq 0 \pmod N$. Then $R_s(2\tau_1+1) = -1$. So $R_a(\tau) = -4$, and it turns up $N-1$ times.

Case 4. $\tau_2 = 3$, $0 \le \tau_1 < N$.

$$\begin{aligned} & R_a(\tau) \\ = \; & R_a(4\tau_1+3) \\ = \; & R_{s_1,\overline{s_2}}(\tau_1+d) + R_{\overline{s_1},s_1}(\tau_1+1-d) \\ & + R_{s_2,\overline{s_1}}(\tau_1+1+d) + R_{\overline{s_2},s_2}(\tau_1+1-d) \\ = \; & -R_s(2(\tau_1+d)+1) - R_s(2(\tau_1+1-d)) \\ & - R_s(2(\tau_1+1+d)-1) - R_s(2(\tau_1+1-d)) \\ = \; & -2R_s(2\tau_1+2d+1) - 2R_s(2\tau_1-2d+2). \end{aligned}$$

1) If $\tau_1 = \frac{N-2d+1}{2}$, $2\tau_1+2d+1 = 0 \pmod N$, $2\tau_1-2d+2 \neq 0 \pmod N$. Then $R_s(2\tau_1+2d+1) = N$, $R_s(2\tau_1-2d+2) = -1$. So $R_a(\tau) = -2N+2$;
2) If $\tau_1 = \frac{N+2d-2}{2}$, $2\tau_1+2d+1 \neq 0 \pmod N$, $2\tau_1-2d+2 = 0 \pmod N$. Then $R_s(2\tau_1+2d+1) = -1$, $R_s(2\tau_1-2d+2) = N$. So $R_a(\tau) = 2-2N$;
3) If $\tau_1 \neq \frac{N-2d+1}{2}$ and $\tau_1 \neq \frac{N+2d-2}{2}$, $2\tau_1+2d+1 \neq 0 \pmod N$, and $2\tau_1-2d+2 \neq 0 \pmod N$. Then $R_s(2\tau_1+2d+1) = R_s(2\tau_1-2d+2) = -1$. So $R_a(\tau) = 4$.

In this case, $R_a(\tau) = -2N+2$ turns up 2 times, and $R_a(\tau) = 4$ turns up $N-2$ times altogether.

According to the above discussion about $R_a(\tau)$, we obtain the following theorem.

Theorem 1. *Let $0 \le \tau < 4N$, and $d \neq \frac{N+1}{4}$. The autocorrelation function of the new sequence a defined by Equation (2) is:*

$$R_a(\tau) = \begin{cases} 4N & 2 \text{ times}, \\ 2-2N & 4 \text{ times}, \\ 4 & 2N-4 \text{ times}, \\ -4 & 2N-2 \text{ times}. \end{cases}$$

Specially, let $d = \frac{N+1}{4}$. Then $2\tau_1+2d = 2\tau_1-2d+1 \pmod N$ and $2\tau_1+2d+1 = 2\tau_1-2d+2 \pmod N$. So in Case 2, the autocorrelation of the sequence a can be reduced to $R_a(\tau) = -4R_s(2\tau_1+2d)$. If $\tau_1 = \frac{3N-1}{4}$, then $2\tau_1+2d = 0 \pmod N$, $R_s(2\tau_1+2d) = N$. So $R_a(\tau) = -4N$ and it turns up 1 time. Otherwise, together with the facts that s has ideal autocorrelation, $R_a(\tau) = 4$. Similarly, in Case 4, $R_a(\tau) = -4R_s(2\tau_1+2d+1)$. If $\tau_1 = \frac{N-3}{4}$, then $2\tau_1+2d+1 = 0 \pmod N$, $R_s(2\tau_1+2d+1) = N$. So $R_a(\tau) = -4N$ and it turns up 1 time. Otherwise, $R_a(\tau) = 4$. Naturally, based on Theorem 1, we can get the following corollary.

Corollary 1. *Let $0 \le \tau < 4N$, and $d = \frac{N+1}{4}$. The autocorrelation function of the new sequence a defined by Equation (2) is:*

$$R_a(\tau) = \begin{cases} 4N & 2 \text{ times}, \\ -4N & 2 \text{ times}, \\ 4 & 2N-2 \text{ times}, \\ -4 & 2N-2 \text{ times}. \end{cases}$$

3.2 Construction B

Let $N \equiv 3 \pmod 4$, $s = (s(0), s(1), \cdots, s(N-1))$ be a binary ideal autocorrelation sequence of period N. Define a new binary interleaved sequence of period $4N$ as the following:

$$a = I(s_1, L^d(\overline{s_1}), \overline{s_2}, L^d(s_2)), \tag{3}$$

where $\overline{s_1}$ is the complement sequence of s_1, $\overline{s_2}$ is the complement sequence of s_2, d is an arbitrary integer and $d \neq \frac{(N+1)}{4}$.

Similarly to the Construction A, the new sequence a constructed as above is also balanced, and we can gain the autocorrelation of the new sequence a by calculation.

Let $\tau = 4\tau_1+\tau_2$, $\tau_2 = 0,1,2,3$. By Lemmas 1 and 2, the autocorrelation of sequence a given by Construction B due to four different values of τ_2 can be given by the following.

Case 1. $\tau_2 = 0$, $0 < \tau_1 < N$.

$$\begin{aligned} & R_a(\tau) \\ = \; & R_a(4\tau_1) \\ = \; & R_{s_1}(\tau_1) + R_{L^d(\overline{s_1})}(\tau_1) + R_{\overline{s_2}}(\tau_1) + R_{L^d(s_2)}(\tau_1) \\ = \; & 4R_s(2\tau_1). \end{aligned}$$

Since $0 < \tau_1 < N$, $2\tau_1 \neq 0 \pmod N$, $R_s(2\tau_1) = -1$. Then $R_a(\tau) = -4$, and it turns up $N-1$ times altogether.

Case 2. $\tau_2 = 1$, $0 \le \tau_1 < N$.

$$\begin{aligned} & R_a(\tau) \\ = \; & R_a(4\tau_1+1) \\ = \; & R_{s_1,\overline{s_1}}(\tau_1+d) + R_{\overline{s_1},\overline{s_2}}(\tau_1-d) \\ & + R_{\overline{s_2},s_2}(\tau_1+d) + R_{s_2,s_1}(\tau_1+1-d) \\ = \; & -R_{s_1}(\tau_1+d) + R_{s_1,s_2}(\tau_1-d) \\ & - R_{s_2}(\tau_1+d) + R_{s_2,s_1}(\tau_1+1-d) \\ = \; & -R_s(2(\tau_1+d)) + R_s(2(\tau_1-d)+1) \\ & - R_s(2(\tau_1+d)) + R_s(2(\tau_1+1-d)-1) \\ = \; & -2R_s(2\tau_1+2d) + 2R_s(2\tau_1-2d+1). \end{aligned}$$

1) If $\tau_1 = N-d$, $2\tau_1+2d = 0 \pmod N$, $2\tau_1 - 2d+1 \neq 0 \pmod N$. Then $R_s(2\tau_1+2d) = N$, $R_s(2\tau_1-2d+1) = -1$. So $R_a(\tau) = -2N-2$;
2) If $\tau_1 = \frac{N+2d-1}{2}$, $2\tau_1+2d \neq 0 \pmod N$, $2\tau_1 - 2d+1 = 0 \pmod N$. Then $R_s(2\tau_1+2d) = -1$, $R_s(2\tau_1-2d+1) = N$. So $R_a(\tau) = 2+2N$;
3) If $\tau_1 \neq N-d$ and $\tau_1 \neq \frac{N+2d-1}{2}$, $2\tau_1+2d \neq 0 \pmod N$ and $2\tau_1-2d+1 \neq 0 \pmod N$. Then $R_s(2\tau_1+2d) = R_s(2\tau_1-2d+1) = -1$. So $R_a(\tau) = 0$.

In this case, $R_a(\tau) = -2N-2$ turns up 1 time, $R_a(\tau) = 2N+2$ turns up 1 time, and $R_a(\tau) = 0$ turns up $N-2$ times.

Case 3. $\tau_2 = 2$, $0 \leq \tau_1 < N$.

$$\begin{aligned} & R_a(\tau) \\ = \; & R_a(4\tau_1+2) \\ = \; & R_{s_1,\overline{s_2}}(\tau_1) + R_{\overline{s_1},s_2}(\tau_1) \\ & + R_{\overline{s_2},s_1}(\tau_1+1) + R_{s_2,\overline{s_1}}(\tau_1+1) \\ = \; & -R_s(2\tau_1+1) - R_s(2\tau_1+1) \\ & - R_s(2(\tau_1+1)-1) - R_s(2(\tau_1+1)-1) \\ = \; & -4R_s(2\tau_1+1). \end{aligned}$$

1) If $\tau_1 = \frac{N-1}{2}$, $2\tau_1+1 = 0 \pmod N$. Then $R_s(2\tau_1+1) = N$. So $R_a(\tau) = -4N$, and it turns up only 1 time;
2) If $\tau_1 \neq \frac{N-1}{2}$, $2\tau_1+1 \neq 0 \pmod N$. Then $R_s(2\tau_1+1) = -1$. So $R_a(\tau) = 4$, and it turns up $N-1$ times.

Case 4. $\tau_2 = 3$, $0 \leq \tau_1 < N$.

$$\begin{aligned} & R_a(\tau) \\ = \; & R_a(4\tau_1+3) \\ = \; & R_{s_1,s_2}(\tau_1+d) + R_{\overline{s_1},s_1}(\tau_1+1-d) \\ & + R_{\overline{s_2},\overline{s_1}}(\tau_1+1+d) + R_{s_2,\overline{s_2}}(\tau_1+1-d) \\ = \; & R_s(2(\tau_1+d)+1) - R_s(2(\tau_1+1-d)) \\ & + R_s(2(\tau_1+1+d)-1) - R_s(2(\tau_1+1-d)) \\ = \; & 2R_s(2\tau_1+2d+1) - 2R_s(2\tau_1-2d+2). \end{aligned}$$

1) If $\tau_1 = \frac{N-2d+1}{2}$, $2\tau_1+2d+1 = 0 \pmod N$, $2\tau_1 - 2d+2 \neq 0 \pmod N$. Then $R_s(2\tau_1+2d+1) = N$, $R_s(2\tau_1-2d+2) = -1$. So $R_a(\tau) = 2N+2$;
2) If $\tau_1 = \frac{N+2d-2}{2}$, $2\tau_1+2d+1 \neq 0 \pmod N$, $2\tau_1 - 2d+2 = 0 \pmod N$. Then $R_s(2\tau_1+2d+1) = -1$, $R_s(2\tau_1-2d+2) = N$. So $R_a(\tau) = -2-2N$;
3) If $\tau_1 \neq \frac{N-2d+1}{2}$ and $\tau_1 \neq \frac{N+2d-2}{2}$. Then $2\tau_1 + 2d+1 \neq 0 \pmod N$, $2\tau_1 - 2d+2 \neq 0 \pmod N$. So $R_s(2\tau_1+2d+1) = R_s(2\tau_1-2d+2) = -1$, $R_a(\tau) = 0$.

In this case, $R_a(\tau) = 2N+2$ turns up 1 time, $R_a(\tau) = -2N-2$ turns up 1 time, and $R_a(\tau) = 0$ turns up $N-2$ times altogether.

According to the above discussion about $R_a(\tau)$, we prove the following theorem.

Theorem 2. *Let $0 \leq \tau < 4N$, and $d \neq \frac{N+1}{4}$. The autocorrelation function of the new sequence a defined by Equation (3) is:*

$$R_a(\tau) = \begin{cases} 4N & 1 \text{ time}, \\ -4N & 1 \text{ time}, \\ -4 & N-1 \text{ times}, \\ 4 & N-1 \text{ times}, \\ 0 & 2N-4 \text{ times}, \\ -2-2N & 2 \text{ times}, \\ 2+2N & 2 \text{ times}. \end{cases}$$

In a special case: $d = \frac{N+1}{4}$, similarly to Corollary 1, we can conclude the following corollary.

Corollary 2. *Let $0 \leq \tau < 4N$, and $d = \frac{N+1}{4}$. The autocorrelation function of the new sequence a defined by Equation (3) is:*

$$R_a(\tau) = \begin{cases} 4N & 1 \text{ time}, \\ -4N & 1 \text{ time}, \\ 4 & N-1 \text{ times}, \\ -4 & N-1 \text{ times}, \\ 0 & 2N \text{ times}. \end{cases}$$

Obviously, except for $-4N$, the values of out-of-phase autocorrelation of the sequence a are all contained in the set $\{0, -4, 4\}$. Therefore, the sequence a in Corollary 2 is a binary sequence with almost optimal autocorrelation magnitude.

Example 1. *Let $N = 7$, $d = \frac{N+1}{4}$, and $s = (1,1,1,0,0,1,0)$, a m-sequence of period 7. The new sequence a of period $4N = 28$ defined by Construction A is*

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

By calculation, the autocorrelation of a is

$$\begin{aligned} R_a(\tau) = \{ & 28,4,-4,4,-4,4,-4,-28,-4,4,-4,4,-4,4, \\ & 28,4,-4,4,-4,4,-4,-28,-4,4,-4,4,-4,4\}, \end{aligned}$$

which is compatible with the result given by Corollary 1.

Example 2. *Let $N = 7$, $d = \frac{N+1}{4}$, and $s = (1,1,1,0,0,1,0)$, a m-sequence of period 7. The new sequence a of period $4N = 28$ defined by Construction B is*

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

By calculation, the autocorrelation of a is

$$\begin{aligned} R_a(\tau) = \{ & 28,0,4,0,-4,0,4,0,-4,0,4,0,-4,0, \\ & -28,0,-4,0,4,0,-4,0,4,0,-4,0,4,0\}, \end{aligned}$$

which is compatible with the result given by Corollary 2.

4 Conclusion

In this paper, two new constructions of binary interleaved sequences of period $4N$ with low autocorrelation and balance property are proposed. From the autocorrelation distributions given by Corollaries 1 and 2, we can conclude that two new binary sequences defined in this paper have good autocorrelation properties. Especially, when $d = \frac{N+1}{4}$, the sequence a in Construction B is a binary sequence with almost optimal autocorrelation magnitude.

Ideally, good sequences combine the low autocorrelation properties with high linear complexity [3]. Furthermore, apart from balance property and autocorrelation property, the linear complexity of these sequences constructed in this paper remains to be solved.

Acknowledgments

The project is supported by the open fund of Fujian Provincial Key Laboratory of Network Security and Cryptology Research Fund (Fujian Normal University) (No.15002), the Natural Science Fund of Shandong Province (No.ZR2014FQ005), the National Natural Science Foundations of China(No.61170319)and the Fundamental Research Funds for the Central Universities (No.11CX04056A, 15CX08011A,15CX05060A).

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] C. Ding, T. Helleseth, and K. Y. Lam, "Several classes of binary sequences with three-level autocorrelation," *IEEE Transactions on Information Theory*, vol. 45, no. 7, pp. 2606–2612, 1999.

[3] V. Edemskiy and A. Ivanov, "Linear complexity of quaternary sequences of length with low autocorrelation," *Journal of Computational and Applied Mathematics*, vol. 259, Part B, pp. 555–560, 2014.

[4] A. D. Elbayoumy and S. J. Shepherd, "Stream or block cipher for securing voip?," *International Journal of Network Security*, vol. 5, no. 2, pp. 128–133, 2007.

[5] G. Gong, "Theory and applications of q-ary interleaved sequences," *IEEE Transactions on Information Theory*, vol. 41, no. 20, pp. 400–411, 1995.

[6] P. Ke and F. Lin, "Constructions of binary sequences with optimal autocorrelation value," *IEEE Transactions on Information Theory*, vol. 46, no. 20, pp. 1381–1382, 2010.

[7] 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.

[8] X. Tang and G. Gong, "New constructions of binary sequences with optimal autocorrelation value/magnitude," *IEEE Transactions on Information Theory*, vol. 56, no. 3, pp. 1278–1286, 2010.

[9] H. Xiong, L. Qu, and C. Li, "2-adic complexity of binary sequences with interleaved structure," *Finite Fields and Their Applications*, vol. 33, pp. 14–28, 2015.

[10] 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, 2008.

[11] T. Yan and G. Gong, "Some notes on constructions of binary sequences with optimal autocorrelation," 2014. (`http://arxiv.org/abs/1411.4340`)

[12] X. Zhang, Q. Wen, and J. Qin, "Constructions of sequences with almost optimal autocorrelation magnitude," *Journal of Electronics and Information Technology*, vol. 33, no. 8, pp. 1908–1912, 2011.

Biography

Ruifang Meng was born in 1991 in Shandong Province of China. She was graduated from China University of Petroleum. She will study for a postgraduate degree at China University of Petroleum in 2015. And her tutor is Tongjiang YAN. Email:mmrrfang@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