PAPER

Constructions of 2-Correlation Immune Rotation Symmetric Boolean Functions*

Jiao DU[†,††a)], **Ziwei ZHAO**[†,††], **Shaojing FU**[†††], **Longjiang QU**[††††], ***and*** **Chao LI**[††††], ***Nonmembers***

SUMMARY In this paper, we first recall the concept of 2-tuples distribution matrix, and further study its properties. Based on these properties, we find four special classes of 2-tuples distribution matrices. Then, we provide a new sufficient and necessary condition for n-variable rotation symmetric Boolean functions to be 2-correlation immune. Finally, we give a new method for constructing such functions when $n = 4t - 1$ is prime, and we show an illustrative example.

key words: *rotation symmetric boolean function, correlation immune, support table,* 2*-tuples distribution matrix*

1. Introduction

Boolean functions are used for designing stream ciphers, block ciphers and hash functions in cryptography. Their cryptographic properties greatly influence cryptosystem security. Rotation symmetric Boolean functions (RSBFs) are a special class of Boolean functions, which are invariant under circular translation of indices. RSBFs were introduced by Filiol and Fontaine in [1], [2] under the name of idempotent functions and studied by Pieprzyk and Qu [3] under their final name. The fact that the special structure of RSBFs allows for faster computation makes it possible to quickly search for Boolean functions with good cryptographic properties. For instance, nonlinearity and correlation immunity of RSBFs were studied in [4], [5].

A Boolean function f is said to be correlation immune of order d (in brief, d-correlation immune or d-CI) if the output distribution of f does not change when at most d input variables are fixed [6]. In 1988, Xiao and Massey [7] gave a characterization of d-CI Boolean functions by use of the Fourier-Hadamand transform. Since then, the correlation immune Boolean function has been an active area of research, and correlation immunity has been one of the main design criteria for shift registers based on stream ciphers [8], [9]. In addition, the correlation immune functions are closely related to orthogonal arrays, which was introduced by C.R. Rao [10].

In terms of the counting and constructions of correlation immune RSBFs, Stănică P. [4] first gave the enumerative results of 1-CI RSBFs when n is prime. Fu et al. [11] studied the number of 1-CI RSBFs, and gave the exact number of 1-CI RSBFs with 11 variables. The resilient functions is a special class of correlation immune functions. Some elaborate sufficient and necessary conditions for the existence of 1- and 2-RSBFs in a given number of variables are given in [12]. In 2020, Du et al. [13] proposed the concept of 2-tuples distribution matrix of the rotation symmetric orbits, and then constructed a class of 2-resilient RSBFs with $4t-1$ variables. Recently, Du et al. [14] proposed a new characterization of 2-resilient RSBFs by the 2-tuples distribution matrix. So far as we know, there are few results about 2-CI RSBFs. We will study the constructions of 2-CI RSBFs based on the results proposed in [4].

In this work, we first further study the properties of the 2-tuples distribution matrix, and give four special classes of 2-tuples distribution matrices. Based on these results, a new sufficient and necessary condition of 2-correlation immune RSBFs is proposed. At last, we give a new method to construct such functions with n variables, where $n = 4t-1$ is prime, and an example is given to illustrate the method.

The rest of the paper is organized as follows. In Sect. 2, we recall some necessary notions and definitions. In Sect. 3, we introduce the properties of the 2-tuples distribution matrix. In Sect. 4, we propose a new sufficient and necessary condition of 2-correlation immune RSBFs, and a concrete constructions of 2-correlation immune RSBFs are demonstrated. Moreover, an illustrative examples are given. Finally, Sect. 5 concludes the article.

2. Preliminaries

Let $\mathbb{F}_2^n$ be the n-dimensional vector space over the binary finite field, i.e., $\mathbb{F}_2 = \{0, 1\}$. An n-variable Boolean function is a mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. Define $\mathbf{B}_n$ to be the set of all n-variable Boolean functions. The support of $f \in \mathbf{B}_n$ is defined as $supp(f) = \{\boldsymbol{x} \in \mathbb{F}_2^n | f(\boldsymbol{x}) = 1\}$. In this paper, for simplicity, and if there is no confusion, we continue to write

Manuscript received November 7, 2023.
Manuscript revised January 18, 2024.
Manuscript publicized March 22, 2024.

[†]Henan Engineering Laboratory for Big Data Statistical Analysis and Optimal Control, Henan Normal University, Xinxiang, 453007, China.
[††]State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, 100876, China.
[†††]College of Computer Science, National University of Defense Technology, Changsha, 410073, China.
[††††]College of Science, National University of Defense Technology, Changsha, 410073, China.

*This work is supported by National Natural Science Foundation of China (Grant No.62372157, No.62172427, No.62072466, No.62032009); Open Foundation of State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications (Grant No.SKLNST-2022-1-01).

a) E-mail: jiaodudj@126.com (Corresponding author)

DOI: 10.1587/transfun.2023EAP1144

$supp(f)$ for the support table of f, i.e., a matrix whose row vectors are elements in the support of f [12].

Let $A = (a_{i,j})_{m\times n}$ and B be $m \times n$ and $p \times q$ matrices, respectively. The Kronecker product of A and B is defined as the $mp \times nq$ matrix $A \otimes B = (a_{i,j}B)_{mp\times nq}$. Let A^{T} be the transpose of the matrix A, and let $\lfloor n \rfloor$ denote the largest integer less than or equal to n, i.e., $n-1 \le \lfloor n \rfloor \le n$. Let $\mathbf{1}_k$ be the $k \times 1$ vector of $1s$, and $\mathbf{0}_k$ be the $k \times 1$ vector of $0s$. To avoid confusion, we denote the sum over $\mathbb{Z}$ by $+$, and the sum over $\mathbb{F}_2$ by $\oplus$. Given a vector $\boldsymbol{x} = (x_0, x_1, \cdots, x_{n-1}) \in \mathbb{F}_2^n$, we define its support as the set $supp(\boldsymbol{x}) = \{0 \le i \le n-1 | x_i = 1\}$, and its Hamming weight as $\mathtt{wt}(\boldsymbol{x}) = x_0 + x_1 + \cdots + x_{n-1}$. We denote by $\overline{\boldsymbol{x}} = (x_0 \oplus 1, x_1 \oplus 1, \cdots, x_{n-1} \oplus 1)$ the complement of $\boldsymbol{x}$. For $0 \le k \le n-1$, we define

$$\rho_n^k(x_i) = \begin{cases} x_{i+k}, & \text{if } i+k < n; \\ x_{i+k-n}, & \text{if } i+k \ge n, \end{cases}$$

where $x_i \in \mathbb{F}_2$ and $0 \le i \le n-1$. We can also extend the definition of ρ_n^k to n-tuples as $\rho_n^k(x_0, x_1, \cdots, x_{n-1}) = (\rho_n^k(x_0), \rho_n^k(x_1), \cdots, \rho_n^k(x_{n-1}))$.

Definition 1 [3], [4] For $f \in \mathbf{B}_n$, if $f(\rho_n^k(x_0, x_1, \cdots, x_{n-1})) = f(x_0, x_1, \cdots, x_{n-1})$ holds for any $0 \le k \le n-1$ and $(x_0, x_1, \cdots, x_{n-1}) \in \mathbb{F}_2^n$, then f is called a rotation symmetric Boolean function (RSBF). We denote by $\mathbf{RSBF}_n$ the set of all the n-variable RSBFs.

Definition 2 [4], [5], [11], [12] The orbit generated by $\boldsymbol{x} \in \mathbb{F}_2^n$ under the action of cyclic group $C_n = \{\rho_n^k | 0 \le k \le n-1\}$ is defined as $O_n(\boldsymbol{x}) = \{\rho_n^k(\boldsymbol{x}) | \boldsymbol{x} \in \mathbb{F}_2^n, 0 \le k \le n-1\}$. If $|O_n(\boldsymbol{x})| = n$, we say $O_n(\boldsymbol{x})$ is a long orbit, and if $|O_n(\boldsymbol{x})| = l < n$, we call it a short orbit.

In this paper, $O_n(\boldsymbol{x})$ also represents the following orbit matrix when no confusion can arise [12]–[15],

$$O_n(\boldsymbol{x}) = \begin{pmatrix} \rho_n^0(\boldsymbol{x}) \\ \rho_n^1(\boldsymbol{x}) \\ \vdots \\ \rho_n^{l-1}(\boldsymbol{x}) \end{pmatrix} = \begin{pmatrix} x_0 & x_1 & \cdots & x_{n-1} \\ x_1 & x_2 & \cdots & x_0 \\ \vdots & \vdots & \ddots & \vdots \\ x_{l-1} & x_l & \cdots & x_{l-2} \end{pmatrix} \quad (1)$$
$$= (X_0, X_1, \cdots, X_{n-1}),$$

where $|O_n(\boldsymbol{x})| = l$, $l|n$. If $|O_n(\boldsymbol{x})| = n$, it is clear that $O_n(\boldsymbol{x})$ is a symmetric matrix.

If $|O_n(\boldsymbol{x})| = l < n$ satisfies $n = tl$, then $\boldsymbol{x} = \mathbf{1}_t^{\mathrm{T}} \otimes (x_0, x_1, \cdots, x_{l-1})$ and $O_n(\boldsymbol{x}) = \mathbf{1}_t^{\mathrm{T}} \otimes (X_0, X_1, \cdots, X_{l-1})$. Assume that $\widetilde{O_n}(\boldsymbol{x}) = \mathbf{1}_t \otimes O_n(\boldsymbol{x})$. It is easily seen that the number of the rows of $\widetilde{O_n}(\boldsymbol{x})$ is n, then the matrix $\widetilde{O_n}(\boldsymbol{x})$ can be seen as a long orbit, which is given by the matrix $O_n(\boldsymbol{x})$.

Definition 3 [14] Let $O_n(\boldsymbol{x}) = (X_0, X_1, \cdots, X_{n-1})$ for $\boldsymbol{x} \in \mathbb{F}_2^n$, where X_i is the $(i+1)$-th column vector of $O_n(\boldsymbol{x})$. Let b_{i1}, b_{i2} and b_{i3} denote respectively the number of times that 2-tuples, i.e., 00, 01(10) and 11, appear in the row vectors of (X_0, X_i), where $1 \le i \le \lfloor \frac{n}{2} \rfloor$, then the following matrix is called the 2-tuples distribution matrix of $O_n(\boldsymbol{x})$,

$$B_{O_n(\boldsymbol{x})} = \begin{pmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \\ \vdots & \vdots & \vdots \\ b_{\lfloor \frac{n}{2} \rfloor 1} & b_{\lfloor \frac{n}{2} \rfloor 2} & b_{\lfloor \frac{n}{2} \rfloor 3} \end{pmatrix} = \begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_{\lfloor \frac{n}{2} \rfloor} \end{pmatrix} \quad (2)$$
$$= (\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3)$$

where $\boldsymbol{b}_i$ is the i-th column vector of $B_{O_n(\boldsymbol{x})}$ for $1 \le i \le 3$ and β_j is the j-th row vector of $B_{O_n(\boldsymbol{x})}$ for $1 \le j \le \lfloor \frac{n}{2} \rfloor$.

Moreover, $B_{O_n(\boldsymbol{x}) \cup O_n(\boldsymbol{y})} = B_{O_n(\boldsymbol{x})} + B_{O_n(\boldsymbol{y})}$ if $O_n(\boldsymbol{x}) \ne O_n(\boldsymbol{y})$, where $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_2^n$, and it is easy to verify that $B_{O_n(\overline{\boldsymbol{x}})} = (\boldsymbol{b}_3, \boldsymbol{b}_2, \boldsymbol{b}_1)$.

Definition 4 [16] Let $\boldsymbol{a} = (a_0, a_1, \cdots, a_{n-1}, \cdots)$ be a sequence with the period n, where $a_i \in \mathbb{F}_2$. If the elements of a sequence $\boldsymbol{b} = \{b_i\}$ are defined by

$$b_i = a_{si}, \ \forall i \ge 0,$$

then $\boldsymbol{b}$ is called an s-decimation sequence of $\boldsymbol{a}$, denoted by $\boldsymbol{b} = \boldsymbol{a}^{(s)}$, where the period of s-decimation $\boldsymbol{a}^{(s)}$ is $n/(s,n)$.

For simplicity, we also regard $\boldsymbol{a}$ with the period n as vectors over $\mathbb{F}_2^n$, i.e., $\boldsymbol{a} = (a_0, a_1, \cdots, a_{n-1})$.

Definition 5 [17] An $N \times n$ array A with entries from $\mathbb{F}_2$ is said to be an orthogonal array with 2 levels, strength t and index λ if every $N \times t$ subarray of A contains each t-tuples based on $\mathbb{F}_2$ exactly λ times as a row. We will denote such an array by $\mathrm{OA}(N, n, 2, t)$.

3. Properties of 2-Tuples Distribution Matrix

In this section we will further analyze the basic properties of 2-tuples distribution matrix.

Lemma 1 [13] For each $\boldsymbol{x} \in \mathbb{F}_2^n$, suppose that $O_n(\boldsymbol{x})$ is defined by (1). Define

$$\widehat{B}_{O_n(\boldsymbol{x})} = \begin{pmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \\ \vdots & \vdots & \vdots \\ b_{(n-1)1} & b_{(n-1)2} & b_{(n-1)3} \end{pmatrix} = \begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_{n-1} \end{pmatrix},$$

and let b_{i1}, b_{i2} and b_{i3} denote respectively the number of times that 2-tuples, i.e., 00, 01(10) and 11, appear in the row vectors of (X_0, X_i) for $1 \le i \le n-1$, where β_i is the i-th row vector of $\widehat{B}_{O_n(\boldsymbol{x})}$. Then $\beta_i = \beta_{n-i}$.

Property 1 Suppose that $O_n(\boldsymbol{x})$ and $B_{O_n(\boldsymbol{x})}$ are defined by (1) and (2), where $\boldsymbol{x} \in \mathbb{F}_2^n$. If $\mathtt{wt}(\boldsymbol{x}) = \omega$ and $|O_n(\boldsymbol{x})| = l$ satisfies $n = tl$, where t is a positive integer, then $\boldsymbol{b}_1 - \boldsymbol{b}_3 = \mathbf{1}_{\lfloor \frac{n}{2} \rfloor} \otimes (\frac{n-2\omega}{t})$, $\boldsymbol{b}_1 + \boldsymbol{b}_2 = \mathbf{1}_{\lfloor \frac{n}{2} \rfloor} \otimes (\frac{n-\omega}{t})$ and $\boldsymbol{b}_2 + \boldsymbol{b}_3 = \mathbf{1}_{\lfloor \frac{n}{2} \rfloor} \otimes (\frac{\omega}{t})$.

Proof. If $t = 1$, we have $|O_n(\boldsymbol{x})| = n$. According to Definition 3, it is easy to know that $b_{i1} + b_{i2} = n - \omega$ and $b_{i2} + b_{i3} = \omega$, which leads to $b_{i1} - b_{i3} = n - 2\omega$. Hence, $\boldsymbol{b}_1 - \boldsymbol{b}_3 = \mathbf{1}_{\lfloor \frac{n}{2} \rfloor} \otimes (n-2\omega)$, $\boldsymbol{b}_1 + \boldsymbol{b}_2 = \mathbf{1}_{\lfloor \frac{n}{2} \rfloor} \otimes (n-\omega)$ and $\boldsymbol{b}_2 + \boldsymbol{b}_3 = \mathbf{1}_{\lfloor \frac{n}{2} \rfloor} \otimes (\omega)$.

If $t > 1$, we have $|O_n(\boldsymbol{x})| = l < n$. Assume that $\widetilde{O_n}(\boldsymbol{x}) = \mathbf{1}_t \otimes O_n(\boldsymbol{x})$, then we continue in the same way as above. Obviously, $t(b_{i1} + b_{i2}) = n - \omega$ and $t(b_{i2} + b_{i3}) = \omega$. We get $t(b_{i1} - b_{i3}) = n - 2\omega$. Thus, $\boldsymbol{b}_1 - \boldsymbol{b}_3 = \mathbf{1}_{\lfloor \frac{n}{2} \rfloor} \otimes (\frac{n-2\omega}{t})$, $\boldsymbol{b}_1 + \boldsymbol{b}_2 = \mathbf{1}_{\lfloor \frac{n}{2} \rfloor} \otimes (\frac{n-\omega}{t})$ and $\boldsymbol{b}_2 + \boldsymbol{b}_3 = \mathbf{1}_{\lfloor \frac{n}{2} \rfloor} \otimes (\frac{\omega}{t})$. □

Property 2 Let n be prime, $O_n(\boldsymbol{x})$ and $B_{O_n(\boldsymbol{x})}$ be defined by (1) and (2) for $\boldsymbol{x} \in \mathbb{F}_2^n$, and let $\boldsymbol{x}^{(s)}$ be s-decimation of $\boldsymbol{x}$, where $1 \le s \le n-1$. Then $B_{O_n(\boldsymbol{x}^{(s)})} = B_{O_n(\boldsymbol{x}^{(n-s)})}$ and

the row vectors of $B_{O_n(\boldsymbol{x}^{(s)})}$ are the permutations of the row vectors of $B_{O_n(\boldsymbol{x})}$.

Proof. On the one hand, recall that $\boldsymbol{x}^{(s)} = (x_0, x_{s(\bmod n)}, x_{2s(\bmod n)}, \cdots, x_{(n-1)s(\bmod n)})$. We have

$$B_{O_n(\boldsymbol{x}^{(s)})} = \begin{pmatrix} \beta_{s(\bmod n)} \\ \beta_{2s(\bmod n)} \\ \vdots \\ \beta_{\lfloor \frac{n}{2} \rfloor s(\bmod n)} \end{pmatrix}, \ B_{O_n(\boldsymbol{x}^{(n-s)})} = \begin{pmatrix} \beta_{(n-s)(\bmod n)} \\ \beta_{2(n-s)(\bmod n)} \\ \vdots \\ \beta_{\lfloor \frac{n}{2} \rfloor (n-s)(\bmod n)} \end{pmatrix}.$$

From $\beta_i = \beta_{n-i}$ we get $B_{O_n(\boldsymbol{x}^{(s)})} = B_{O_n(\boldsymbol{x}^{(n-s)})}$.

On the other hand, obviously $is \not\equiv js(\bmod n)$ for any $1 \le j < i \le \lfloor \frac{n}{2} \rfloor$. Moreover, we have $is(\bmod n) + js(\bmod n) \ne n$. Otherwise, $(i+j)s \equiv 0(\bmod n)$. It follows that $i = n-j$, which contradicts with $1 \le j < i \le \lfloor \frac{n}{2} \rfloor$. Thus, by $\beta_i = \beta_{n-i}$ for $1 \le i \le n-1$, the set $\{\beta_{s(\bmod n)}, \beta_{2s(\bmod n)}, \cdots, \beta_{\lfloor \frac{n}{2} \rfloor s(\bmod n)}\}$ is equal to the set $\{\beta_1, \beta_2, \cdots, \beta_{\lfloor \frac{n}{2} \rfloor}\}$ for $1 \le s \le \lfloor \frac{n}{2} \rfloor$. Then the row vectors of $B_{O_n(\boldsymbol{x}^{(s)})}$ are the permutations of the row vectors of $B_{O_n(\boldsymbol{x})}$. □

Remark 1 With the help of Property 2, it can be easily verified that if $B_{O_n(\boldsymbol{x})}$ has two different row vectors, then $B_{O_n(\boldsymbol{x}^{(1)})}, B_{O_n(\boldsymbol{x}^{(2)})}, \cdots, B_{O_n(\boldsymbol{x}^{(\lfloor \frac{n}{2} \rfloor)})}$ are different from each other.

For any $\boldsymbol{x} \in \mathbb{F}_2^n$, given $O_n(\boldsymbol{x})$ and $B_{O_n(\boldsymbol{x})}$ by (1) and (2). Let n be an odd prime, $\boldsymbol{x}^{(s)}$ be s-decimation of $\boldsymbol{x}$, where $1 \le s \le \lfloor \frac{n}{2} \rfloor$, and let $S = \{i_1, i_2, \cdots, i_m\} \subseteq T = \{1, 2, 3, \cdots, \lfloor \frac{n}{2} \rfloor\}$.

Property 3 Let the notions and symbols be defined as before, we have

$$\sum_{i \in T} B_{O_n(\boldsymbol{x}^{(i)})} = \mathbf{1}_{\lfloor \frac{n}{2} \rfloor} \otimes (\sum_{i \in T} b_{i1}, \sum_{i \in T} b_{i2}, \sum_{i \in T} b_{i3}).$$

Proof. According to Lemma 1 and Property 2, we have

$$\begin{aligned} \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} B_{O_n(\boldsymbol{x}^{(i)})} &= \frac{1}{2} \sum_{i=1}^{n-1} B_{O_n(\boldsymbol{x}^{(i)})} = \mathbf{1}_{\lfloor \frac{n}{2} \rfloor} \otimes \frac{1}{2}(\beta_1 + \beta_2 + \cdots + \beta_{n-1}) \\ &= \mathbf{1}_{\lfloor \frac{n}{2} \rfloor} \otimes (\beta_1 + \beta_2 + \cdots \beta_{\lfloor \frac{n}{2} \rfloor}) \\ &= \mathbf{1}_{\lfloor \frac{n}{2} \rfloor} \otimes (\sum_{i \in T} b_{i1}, \sum_{i \in T} b_{i2}, \sum_{i \in T} b_{i3}). \end{aligned}$$

□

Property 4 Let the notions and symbols be defined as before. Suppose that $\boldsymbol{x} \in \mathbb{F}_2^n$ and $\mathtt{wt}(\boldsymbol{x}) = \omega$, then

$$\sum_{i \in S} B_{O_n(\overline{\boldsymbol{x}}^{(i)})} + \sum_{i \in T \setminus S} B_{O_n(\boldsymbol{x}^{(i)})} = \mathbf{1}_{\lfloor \frac{n}{2} \rfloor} \otimes (\mu_1, \mu_2, \mu_3),$$

where $\mu_1 = \sum_{i \in T} b_{i1} - m(n-2\omega)$, $\mu_2 = \sum_{i \in T} b_{i2}$ and $\mu_3 = \sum_{i \in T} b_{i3} + m(n-2\omega)$.

Proof. From Definition 3 we have

$$B_{O_n(\overline{x})} - B_{O_n(x)} = \mathbf{1}_{\lfloor \frac{n}{2} \rfloor} \otimes (2\omega - n, 0, n - 2\omega).$$

It's easy to verify that $\overline{\boldsymbol{x}^{(s)}} = \overline{\boldsymbol{x}}^{(s)}$. Thus,

$$\begin{aligned} &\sum_{i \in S} B_{O_n(\overline{\boldsymbol{x}}^{(i)})} + \sum_{i \in T \setminus S} B_{O_n(\boldsymbol{x}^{(i)})} = \sum_{i \in S} B_{O_n(\overline{\boldsymbol{x}^{(i)}})} + \sum_{i \in T \setminus S} B_{O_n(\boldsymbol{x}^{(i)})} \\ &= \sum_{i \in S} \left(B_{O_n(\overline{\boldsymbol{x}^{(i)}})} - B_{O_n(\boldsymbol{x}^{(i)})} \right) + \sum_{i \in T} B_{O_n(\boldsymbol{x}^{(i)})} \\ &= \mathbf{1}_{\lfloor \frac{n}{2} \rfloor} \otimes (\sum_{i \in T} b_{i1} - m(n-2\omega), \sum_{i \in T} b_{i2}, \sum_{i \in T} b_{i3} + m(n-2\omega)). \end{aligned}$$

□

Property 5 Let n be odd, $O_n(\boldsymbol{x})$ and $B_{O_n(\boldsymbol{x})}$ be defined by (1) and (2) for $\boldsymbol{x} \in \mathbb{F}_2^n$. Suppose that $\mathtt{wt}(\boldsymbol{x}) = \omega$ and $|O_n(\boldsymbol{x})| = l$ satisfies $n = tl$, where t is a positive integer, then

$$\sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} b_{i1} = \frac{(n-\omega)(n-\omega-1)}{2t}, \ \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} b_{i2} = \frac{\omega(n-\omega)}{2t}, \ \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} b_{i3} = \frac{\omega(\omega-1)}{2t}.$$

Proof. If $t = 1$, we have $|O_n(\boldsymbol{x})| = n$. By (1), write $X_0^{\mathrm{T}} X_i = x_0 x_i + x_1 x_{i+1} + \cdots + x_{n-1} x_{i-1}$, where $1 \le i \le n-1$. Then $\sum_{i=1}^{n-1} X_0^{\mathrm{T}} X_i = \sum_{i=0}^{n-1} x_i (x_0 + \cdots + x_{i-1} + x_{i+1} + \cdots + x_{n-1}) = \omega(\omega-1)$. It's easy to see that $\sum_{i=1}^{n-1} X_0^{\mathrm{T}} X_i$ represents the number of vector $(1,1)$ in (X_0, X_l) for all $1 \le l \le n-1$. By Definition 3 and Lemma 1, we have $\sum_{i=1}^{n-1} X_0^{\mathrm{T}} X_i = 2\sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} b_{i3}$. So $\sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} b_{i3} = \frac{1}{2}\omega(\omega-1)$. Note that $b_{i1} + b_{i2} = n - \omega$ and $b_{i2} + b_{i3} = \omega$. Then $\sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} (b_{i1} + b_{i2}) = \lfloor \frac{n}{2} \rfloor (n-\omega)$ and $\sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} (b_{i2} + b_{i3}) = \lfloor \frac{n}{2} \rfloor \omega$. Hence,

$$\sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} b_{i2} = \frac{1}{2}\omega(n-\omega), \ \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} b_{i1} = \frac{1}{2}(n-\omega)(n-\omega-1).$$

If $t > 1$, we have $|O_n(\boldsymbol{x})| = l < n$. Write $\widetilde{O_n}(\boldsymbol{x}) = \mathbf{1}_t \otimes O_n(\boldsymbol{x})$. Then we have

$$B_{\widetilde{O_n}(\boldsymbol{x})} = \begin{pmatrix} \widetilde{b}_{11} & \widetilde{b}_{12} & \widetilde{b}_{13} \\ \widetilde{b}_{21} & \widetilde{b}_{22} & \widetilde{b}_{23} \\ \vdots & \vdots & \vdots \\ \widetilde{b}_{\lfloor \frac{n}{2} \rfloor 1} & \widetilde{b}_{\lfloor \frac{n}{2} \rfloor 2} & \widetilde{b}_{\lfloor \frac{n}{2} \rfloor 3} \end{pmatrix}.$$

It is easy to see that $\widetilde{b}_{ij} = t b_{ij}$, where $1 \le i \le \lfloor \frac{n}{2} \rfloor$ and $1 \le j \le 3$. Therefore,

$$\sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} b_{i1} = \frac{(n-\omega)(n-\omega-1)}{2t}, \ \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} b_{i2} = \frac{\omega(n-\omega)}{2t}, \ \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} b_{i3} = \frac{\omega(\omega-1)}{2t}.$$

□

4. Constructions of 2-Correlation Immune RSBFs

Lemma 2 [12] Let $f \in \mathbf{RSBF}_n$ and its support table be $supp(f) = (c_0, c_1, \cdots, c_{n-1})$, where c_i is the $(i+1)$-th column vector of $supp(f)$. Then f is 2-CI if and only if (c_0, c_l) is an OA($|supp(f)|, 2, 2, 2$), where $1 \le l \le \lfloor \frac{n}{2} \rfloor$.

Based on 2-tuples distribution matrix, we privide a new sufficient and necessary condition of 2-correlation immune RSBFs as follows:

Theorem 1 Let $f \in \mathbf{RSBF}_n$. Then f is 2-CI if and

only if the 2-tuples distribution matrix of its support table $supp(f)$ satisfies

$$B_{supp(f)} = \begin{pmatrix} k & k & k \\ k & k & k \\ \vdots & \vdots & \vdots \\ k & k & k \end{pmatrix}_{\lfloor \frac{n}{2} \rfloor \times 3} = \mathbf{1}_{\lfloor \frac{n}{2} \rfloor} \otimes (k,k,k), \quad (3)$$

where $k = \frac{|supp(f)|}{4}$.

Proof. Assume that f is a 2-CI, then (c_0, c_l) is an OA($|supp(f)|, 2, 2, 2$) by Lemma 2, where $1 \le l \le \lfloor \frac{n}{2} \rfloor$. Thus, the numbers of (0,0), (0,1), (1,0) and (1,1) in (c_0, c_l) are all $|supp(f)|/4$. According to Definition 3, we have $B_{supp(f)} = \mathbf{1}_{\lfloor \frac{n}{2} \rfloor} \otimes (k,k,k)$, where $k = \frac{|supp(f)|}{4}$.

Conversely, if $B_{supp(f)} = \mathbf{1}_{\lfloor \frac{n}{2} \rfloor} \otimes (k,k,k)$, where $k = \frac{|supp(f)|}{4}$, then it is easy to know that (c_0, c_l) is an OA($|supp(f)|, 2, 2, 2$) from Definitions 3 and 5, where $1 \le l \le \lfloor \frac{n}{2} \rfloor$. Hence, by Lemma 2, f is 2-CI. □

Remark 2 When $k = 2^{n-3}$, $f(\boldsymbol{x})$ is a 2-resilient RSBF.

By Theorem 1, we know that constructing 2-correlation immune RSBFs is equivalent to finding the union of several orbits such that the sum of their corresponding 2-tuples distribution matrices is the matrix in (3). In order to construct 2-correlation immune RSBFs, we demonstrate four distinct classes of 2-tuples distribution matrices as follows:

(*i*) For $\boldsymbol{x} \in \mathbb{F}_2^n$, if $\mathtt{wt}(\boldsymbol{x}) = 1$, then the 2-tuples distribution matrix of $O_n(\boldsymbol{x})$ is

$$\mathbf{1}_{\lfloor \frac{n}{2} \rfloor} \otimes (n-2, 1, 0).$$

(*ii*) Let $n = 4t - 1$ be a prime and $t \ge 2$ be an integer. We can get a vector $\boldsymbol{x} \in \mathbb{F}_2^n$ from the cyclic Hadamard matrix [18] $H_{(n+1)\times(n+1)}$, and the method of obtaining $\boldsymbol{x}$ is described in Sect. 3 of [15], where $\mathtt{wt}(\boldsymbol{x}) = 2t$ and the 2-tuples distribution matrix of $O_n(\boldsymbol{x})$ is

$$\mathbf{1}_{\lfloor \frac{n}{2} \rfloor} \otimes (t-1, t, t).$$

(*iii*) Let n be odd prime. By Properties 3 and 5, we get

$$\sum_{s \in T} B_{O_n(\boldsymbol{x}^{(s)})} = \mathbf{1}_{\lfloor \frac{n}{2} \rfloor} \otimes \frac{1}{2}\big((n-\omega)(n-\omega-1), \omega(n-\omega), \omega(\omega-1)\big).$$

(*iv*) Let n be odd prime. By Properties 4 and 5, we obtain

$$\sum_{j \in S} B_{O_n(\overline{\boldsymbol{x}}^{(j)})} + \sum_{i \in T \setminus S} B_{O_n(\boldsymbol{x}^{(i)})} = \mathbf{1}_{\lfloor \frac{n}{2} \rfloor} \otimes (\mu_1, \mu_2, \mu_3),$$

where $\mu_1 = \frac{1}{2}(n-\omega)(n-\omega-1) - m(n-2\omega)$, $\mu_2 = \frac{1}{2}\omega(n-\omega)$ and $\mu_3 = \frac{1}{2}\omega(\omega-1) + m(n-2\omega)$.

Next we will construct 2-correlation immune RSBFs based on these four 2-tuples distribution matrices.

Construction. Let $n = 4t - 1$ be a prime and t, m be positive integers.

It is easy to see that the orbits that correspond to these four 2-tuples distribution matrices mentioned above are all long orbits, then we have $|supp(f)| = n(n+1)$. Let $T = \{1, 2, \cdots, \lfloor \frac{n}{2} \rfloor\}$, $S = \{i_1, i_2, \cdots, i_m\} \subseteq T$, $S' = \{j_1, j_2, \cdots, j_l\} \subseteq T$ and $k = \frac{n(n+1)}{4}$. Let $\boldsymbol{x}_1 = (1,0,0,\cdots,0,0) \in \mathbb{F}_2^n$, and let $\boldsymbol{x}_2$ be obtained from a cyclic Hadamard matrix of order $n+1$. Suppose that both $B_{O_n(\boldsymbol{x}_3)}$ and $B_{O_n(\boldsymbol{x}_4)}$ have two different row vectors, where $\mathtt{wt}(\boldsymbol{x}_3) = \omega_1$, $\mathtt{wt}(\boldsymbol{x}_4) = \omega_2$. We have the following Theorem 2.

Theorem 2 Let the notions be defined as before. If there exist ω_1, ω_2 and m such that one of the following equations holds, then 2-correlation immune RSBFs can be obtained.

(*1*) $B_{O_n(\boldsymbol{x}_1)} + B_{O_n(\boldsymbol{x}_2)} + \sum_{i \in T} B_{O_n(\boldsymbol{x}_3^{(i)})} + \sum_{i \in S} B_{O_n(\overline{\boldsymbol{x}_4}^{(i)})} + \sum_{i \in T \setminus S} B_{O_n(\boldsymbol{x}_4^{(i)})} = \mathbf{1}_{\lfloor \frac{n}{2} \rfloor} \otimes (k,k,k)$;

(*2*) $B_{O_n(\overline{\boldsymbol{x}_1})} + B_{O_n(\boldsymbol{x}_2)} + \sum_{i \in T} B_{O_n(\boldsymbol{x}_3^{(i)})} + \sum_{i \in S} B_{O_n(\overline{\boldsymbol{x}_4}^{(i)})} + \sum_{i \in T \setminus S} B_{O_n(\boldsymbol{x}_4^{(i)})} = \mathbf{1}_{\lfloor \frac{n}{2} \rfloor} \otimes (k,k,k)$;

(*3*) $B_{O_n(\boldsymbol{x}_1)} + B_{O_n(\overline{\boldsymbol{x}_2})} + \sum_{i \in T} B_{O_n(\boldsymbol{x}_3^{(i)})} + \sum_{i \in S} B_{O_n(\overline{\boldsymbol{x}_4}^{(i)})} + \sum_{i \in T \setminus S} B_{O_n(\boldsymbol{x}_4^{(i)})} = \mathbf{1}_{\lfloor \frac{n}{2} \rfloor} \otimes (k,k,k)$;

(*4*) $B_{O_n(\overline{\boldsymbol{x}_1})} + B_{O_n(\overline{\boldsymbol{x}_2})} + \sum_{i \in T} B_{O_n(\boldsymbol{x}_3^{(i)})} + \sum_{i \in S} B_{O_n(\overline{\boldsymbol{x}_4}^{(i)})} + \sum_{i \in T \setminus S} B_{O_n(\boldsymbol{x}_4^{(i)})} = \mathbf{1}_{\lfloor \frac{n}{2} \rfloor} \otimes (k,k,k)$;

(*5*) $B_{O_n(\boldsymbol{x}_1)} + B_{O_n(\boldsymbol{x}_2)} + \sum_{i \in S'} B_{O_n(\overline{\boldsymbol{x}_3}^{(i)})} + \sum_{i \in T \setminus S'} B_{O_n(\boldsymbol{x}_3^{(i)})} + \sum_{i \in S} B_{O_n(\overline{\boldsymbol{x}_4}^{(i)})} + \sum_{i \in T \setminus S} B_{O_n(\boldsymbol{x}_4^{(i)})} = \mathbf{1}_{\lfloor \frac{n}{2} \rfloor} \otimes (k,k,k)$;

(*6*) $B_{O_n(\overline{\boldsymbol{x}_1})} + B_{O_n(\boldsymbol{x}_2)} + \sum_{i \in S'} B_{O_n(\overline{\boldsymbol{x}_3}^{(i)})} + \sum_{i \in T \setminus S'} B_{O_n(\boldsymbol{x}_3^{(i)})} + \sum_{i \in S} B_{O_n(\overline{\boldsymbol{x}_4}^{(i)})} + \sum_{i \in T \setminus S} B_{O_n(\boldsymbol{x}_4^{(i)})} = \mathbf{1}_{\lfloor \frac{n}{2} \rfloor} \otimes (k,k,k)$;

(*7*) $B_{O_n(\boldsymbol{x}_1)} + B_{O_n(\overline{\boldsymbol{x}_2})} + \sum_{i \in S'} B_{O_n(\overline{\boldsymbol{x}_3}^{(i)})} + \sum_{i \in T \setminus S'} B_{O_n(\boldsymbol{x}_3^{(i)})} + \sum_{i \in S} B_{O_n(\overline{\boldsymbol{x}_4}^{(i)})} + \sum_{i \in T \setminus S} B_{O_n(\boldsymbol{x}_4^{(i)})} = \mathbf{1}_{\lfloor \frac{n}{2} \rfloor} \otimes (k,k,k)$;

(*8*) $B_{O_n(\overline{\boldsymbol{x}_1})} + B_{O_n(\overline{\boldsymbol{x}_2})} + \sum_{i \in S'} B_{O_n(\overline{\boldsymbol{x}_3}^{(i)})} + \sum_{i \in T \setminus S'} B_{O_n(\boldsymbol{x}_3^{(i)})} + \sum_{i \in S} B_{O_n(\overline{\boldsymbol{x}_4}^{(i)})} + \sum_{i \in T \setminus S} B_{O_n(\boldsymbol{x}_4^{(i)})} = \mathbf{1}_{\lfloor \frac{n}{2} \rfloor} \otimes (k,k,k)$.

Proof. We give the proof only for equation (*1*), the rest of the cases is similar.

It is easy to check that the sum of these four 2-tuples distribution matrices is as follows:

$$\begin{aligned} &B_{O_n(\boldsymbol{x}_1)} + B_{O_n(\boldsymbol{x}_2)} + \sum_{i \in T} B_{O_n(\boldsymbol{x}_3^{(i)})} + \sum_{i \in S} B_{O_n(\overline{\boldsymbol{x}_4}^{(i)})} + \sum_{i \in T \setminus S} B_{O_n(\boldsymbol{x}_4^{(i)})} \\ &= \mathbf{1}_{\lfloor \frac{n}{2} \rfloor} \otimes (n-2, 1, 0) + \mathbf{1}_{\lfloor \frac{n}{2} \rfloor} \otimes (t-1, t, t) \\ &+ \mathbf{1}_{\lfloor \frac{n}{2} \rfloor} \otimes \big(\frac{(n-\omega_1)(n-\omega_1-1)}{2}, \frac{\omega_1(n-\omega_1)}{2}, \frac{\omega_1(\omega_1-1)}{2}\big) + \mathbf{1}_{\lfloor \frac{n}{2} \rfloor} \otimes \\ &\big(\frac{(n-\omega_2)(n-\omega_2-1)}{2} - m(n-2\omega_2), \frac{\omega_2(n-\omega_2)}{2}, \frac{\omega_2(\omega_2-1)}{2} + m(n-2\omega_2)\big) \\ &= \mathbf{1}_{\lfloor \frac{n}{2} \rfloor} \otimes M^{\mathrm{T}}, \end{aligned}$$

where

$$M=\begin{pmatrix} n+t-3+\frac{(n-\omega_1)(n-\omega_1-1)}{2}+\frac{(n-\omega_2)(n-\omega_2-1)}{2}-m(n-2\omega_2) \\ t+1+\frac{\omega_1(n-\omega_1)}{2}+\frac{\omega_2(n-\omega_2)}{2} \\ t+\frac{\omega_1(\omega_1-1)}{2}+\frac{\omega_1(\omega_2-1)}{2}+m(n-2\omega_2) \end{pmatrix}.$$

Suppose that the equation (1) holds, then we can obtain the following system of equations

$$\begin{cases} t-3+n(n-\omega_1-\omega_2)+\frac{1}{2}\omega_1(\omega_1+1)+\frac{1}{2}\omega_2(\omega_2+1)-m(n-2\omega_2)=k \\ t+1+\frac{1}{2}\omega_1(n-\omega_1)+\frac{1}{2}\omega_2(n-\omega_2)=k \\ t+\frac{1}{2}\omega_1(\omega_1-1)+\frac{1}{2}\omega_2(\omega_2-1)+m(n-2\omega_2)=k \end{cases}, \tag{4}$$

where $k=\frac{n(n+1)}{4}$ and $1\le m\le\lfloor\frac{n}{2}\rfloor$ are all integers.

When n is determined, we set the values of ω_1 and ω_2 according to the system of equations, and if m has an integer solution in the above equation, we can choose the appropriate vectors $\boldsymbol{x}_2,\boldsymbol{x}_3$ and $\boldsymbol{x}_4$. Let the support of $f\in\mathbf{B}_n$ be

$$\begin{aligned} supp(f)=&O_n(\boldsymbol{x}_1)\bigcup O_n(\boldsymbol{x}_2)\bigcup\Big(\bigcup_{i\in T}O_n(\boldsymbol{x}_3^{(i)})\Big) \\ &\bigcup\Big(\bigcup_{i\in S}O_n(\overline{\boldsymbol{x}_4}^{(i)})\Big)\bigcup\Big(\bigcup_{i\in T\setminus S}O_n(\boldsymbol{x}_4^{(i)})\Big). \end{aligned} \tag{5}$$

By Theorem 1, f is a 2-correlation immune RSBF. The rest of the proof runs as before. We can also obtain 2-correlation immune RSBFs if the related system of equations has solutions. □

We now give a simple example that illustrates the previous construction.

Example 1 When $n=11$, we have $t=3$ and $k=33$. Let $f\in\mathbf{B}_n$, $\boldsymbol{x}_1=(1,0,0,0,0,0,0,0,0,0,0)$, and let $\boldsymbol{x}_3,\boldsymbol{x}_4\in\mathbb{F}_2^{11}$. Suppose that $\boldsymbol{x}_2=(0,0,0,1,0,1,1,0,1,1,1)$ is obtained by the cyclic Hadamard matrix $H_{12\times12}$, and $\mathtt{wt}(\boldsymbol{x}_3)=\omega_1$, $\mathtt{wt}(\boldsymbol{x}_4)=\omega_2$. From system of Eq. (4), the following system of equations is obtained.

$$\begin{cases} 11(11-\omega_1-\omega_2)+\frac{1}{2}\omega_1(\omega_1+1)+\frac{1}{2}\omega_2(\omega_2+1)-m(11-2\omega_2)=33 \\ 4+\frac{1}{2}\omega_1(11-\omega_1)+\frac{1}{2}\omega_2(11-\omega_2)=33 \\ 3+\frac{1}{2}\omega_1(\omega_1-1)+\frac{1}{2}\omega_2(\omega_2-1)+m(11-2\omega_2)=33 \end{cases}$$

Firstly, we consider the the second equation of the system of equations. For $0\le\mathtt{wt}(\boldsymbol{x})=\omega\le11$, we have Table 1. Clearly, we have $\omega_1\ne\omega_2$. From Table 1, if $\omega_1=5,6$, we can take $\omega_2=4,7$. Conversely, if $\omega_1=4,7$, then $\omega_2=5,6$. Next, we consider the first and third equations of the above system of equations. We obtain one solution that $\omega_1=6$, $\omega_2=4$ and $m=3$ for the above system of equations. Based on the solution, we can construct 2-correlation immune RSBFs. Suppose that $\boldsymbol{x}_3=(0,1,1,0,1,0,1,0,1,0,1)$ and $\boldsymbol{x}_4=(1,0,0,1,0,0,1,0,0,1,0)$. It is easy to verify that both $B_{O_{11}(\boldsymbol{x}_3)}$ and $B_{O_{11}(\boldsymbol{x}_4)}$ have two different row vectors.

Table 1 The calculation of ω.

ω	$\frac{1}{2}\omega(11-\omega)$	ω	$\frac{1}{2}\omega(11-\omega)$
$\omega=2$	9	$\omega=9$	9
$\omega=3$	12	$\omega=8$	12
$\omega=4$	14	$\omega=7$	14
$\omega=5$	15	$\omega=6$	15

Assume that $S=\{i_1,i_2,i_3\}=\{1,2,4\}\subseteq T=\{1,2,3,4,5\}$, and the support of f is

$$\begin{aligned} supp(f)=&O_{11}(\boldsymbol{x}_1)\cup O_{11}(\boldsymbol{x}_2)\cup O_{11}(\boldsymbol{x}_3)\cup O_{11}(\boldsymbol{x}_3^{(2)})\cup O_{11}(\boldsymbol{x}_3^{(3)})\cup O_{11}(\boldsymbol{x}_3^{(4)}) \\ &\cup O_{11}(\boldsymbol{x}_3^{(5)})\cup O_{11}(\overline{\boldsymbol{x}_4})\cup O_{11}(\overline{\boldsymbol{x}_4}^{(2)})\cup O_{11}(\overline{\boldsymbol{x}_4}^{(4)})\cup O_{11}(\boldsymbol{x}_4^{(3)})\cup O_{11}(\boldsymbol{x}_4^{(5)}), \end{aligned}$$

then $f(\boldsymbol{x})$ is a 2-correlation immune RSBF by Theorem 2.

5. Conclusion

In this paper, the properties of the 2-tuples distribution matrix are further studied. And a new sufficient and necessary condition of 2-CI RSBFs based on the 2-tuples distribution matrix is presented. Then a new construction is obtained for prime $n=4t-1$, and an illustrative example is also given. For further research, it is interesting to construct 2-CI RSBFs for any number of variables.

References

[1] E. Filiol and C. Fontaine, "Highly nonlinear balanced Boolean functions with a good correlation-immunity," Advances in Cryptology — EUROCRYPT'98: International Conference on the Theory and Application of Cryptographic Techniques Espoo, Finland, Proceedings, pp.475–488, Springer Berlin Heidelberg, 1998.
[2] C. Fontaine, "On some cosets of the first-order Reed-Muller code with high minimum weight," IEEE Trans. Inf. Theory, vol.45, no.4, pp.1237–1243, 1999.
[3] J. Pieprzyk and C. Qu, "Fast hashing and rotation symmetric functions," J. Univers. Comput. Sci., vol.5, no.1, pp.20–31, 1999.
[4] P. Stănică, S. Maitra, and J. Clark, "Results on rotation symmetric bent and correlation immune Boolean functions," International Workshop on Fast Software Encryption, Lecture Notes in Computer Science, vol.3017, pp.161–177, Springer, Berlin, Heidelberg, 2004.
[5] T.W. Cusick and P. Stanica, Cryptographic Boolean Functions and Applications, Academic Press, 2017.
[6] T. Siegenthaler, "Correlation attacks on certain stream ciphers with nonlinear generators," IEEE Int. Symp. Inform. Theory, Saint Jovite, Canada, pp.26–29, 1983.
[7] G.-Z. Xiao and J.L. Massey, "A spectral characterization of correlation-immune combining functions," IEEE Trans. Inf. Theory, vol.34, no.3, pp.569–571, 1988.
[8] R.A. Rueppel, Analysis and Design of Stream Ciphers, Springer, Berlin, 1986.
[9] T. Siegenthaler, "Decrypting a class of stream ciphers using ciphertext only," IEEE Trans. Comput., vol.C-34, no.1, pp.81–85, 1985.
[10] C.R. Rao, "Factorial experiments derivable from combinatorial arrangements of arrays," Suppl. J. R. Stat. Soc., vol.9, no.1, pp.128–139, 1947.
[11] S. Fu, C. Li, and L. Qu, "On the number of rotation symmetric Boolean functions," Sci. China Inf. Sci., vol.53, pp.537–545, 2010.
[12] J. Du, Q. Wen, J. Zhang, and S. Pang, "Constructions of resilient rotation symmetric Boolean functions on given number of variables," IET Inf. Secur., vol.8, no.5, pp.265–272, 2014.
[13] J. Du, C. Liu, and S. Pang, "Constructions of rotation symmetric 2-resilient functions with $4t-1$ number of variables," J. Commun., vol.41, no.11, pp.169–175, 2020 (in Chinese).
[14] J. Du, Z. Chen, L. Dong, T. Wang, and S. Pang, "A new characterization of 2-resilient rotation symmetric Boolean functions," IEICE Trans. Fundamentals., vol.E106-A, no.9, pp.1268–1271, Sept. 2023.
[15] J. Du, Z. Chen, S. Fu, L. Qu, and C. Li, "Constructions of 2-resilient rotation symmetric Boolean functions through symbol transformations of cyclic Hadamard matrix," Theor. Comput. Sci., vol.919, pp.80–91, 2022.

[16] S.W. Golomb and G. Gong, Signal Design for Good Correlation: For Wireless Communication, Cryptography, and Radar, Cambridge University Press, 2005.
[17] A.S. Hedayat, N.J.A. Sloane, and J. Stufken, Orthogonal Arrays: Theory and Applications, Springer Science, 1999.
[18] C. Shi and B. Tang, "Designs from good Hadamard matrices," Bernoulli, vol.24, no.1, pp.661–671, 2018.

Jiao Du received the M.S. degree in mathematics from Henan Normal University, Xinxiang, China, and the PH.D. Degree in cryptography from Beijing University of Posts and Telecommunications, Beijing, China, in 2008 and 2013 respectively. He is currently an associate professor of Henan Normal University. His present research interests include Boolean function, cryptography, and applied mathematics.

Ziwei Zhao is currently pursuing the master's degree with Henan Normal University, Xinxiang, China. Her research interests include Boolean function and cryptography.

Shaojing Fu received the Ph.D degree in mathematics in 2010 from National Universitry of Defense Technology, Changsha, China. He is currently an associate professor in College of Computer Science, National University of Defense Technology, China. His research fields include Boolean functions, Cloud and Outsourcing Security. Shaojing Fu is a member of CACR.

Longjiang Qu received the B.S. degree in 2002 and the Ph.D. degree in 2007 in mathematics from National University of Defense Technology, Changsha, China. He is now a professor with the Department of Mathematics and System Science, National University of Defense Technology. His research fields include cryptography and coding theory.

Chao Li received the B.S. degree in mathematics in 1987 from the University of Information Engineering of China, the M.S. degree in mathematics in 1990 from the University of Science and Technology of China, and the Ph.D. degree in engineering in 2002 from the National University of Defense Technology of China. Since December 2001, he has been a professor with the Department of Mathematics and System Science, National University of Defense Technology. His research fields include coding theory, cryptography and sequences.