A NEW CONSTRUCTION OF ODD-VARIABLE ROTATION
SYMMETRIC BOOLEAN FUNCTIONS WITH GOOD
CRYPTOGRAPHIC PROPERTIES

BINGXIN WANG AND SIHONG SU*
School of Mathematics and Statistics, Henan University, Kaifeng, 475004, China

(Communicated by Claude Carlet)

Abstract. Rotation symmetric Boolean functions constitute a class of cryptographically significant Boolean functions. In this paper, based on the theory of ordered integer partitions, we present a new class of odd-variable rotation symmetric Boolean functions with optimal algebraic immunity by modifying the support of the majority function. Compared with the existing rotation symmetric Boolean functions on odd variables, the newly constructed functions have the highest nonlinearity.

1. Introduction

Boolean functions have many applications in stream ciphers and block ciphers. Construction of Boolean functions with good cryptographic properties is a research hotspot in these fields. To resist the main known attacks, Boolean functions used in stream ciphers should have good cryptographic properties: balancedness, high algebraic degree, high algebraic immunity, high nonlinearity and good immunity to fast algebraic attacks. To avoid statistical dependence between the plaintext and the ciphertext, Boolean functions must be balanced [2]. In stream cryptosystems, balancedness is a basic criterion that Boolean functions should satisfy. To resist the best affine approximation attack [9] and fast correlation attack [1], Boolean functions used in cryptosystems should have high nonlinearity. In 2003, the algebraic attack against Linear Feedback Shift Register-based stream ciphers was proposed by Courtois and Meier [7], which is an important tool in the cryptanalysis of stream cryptosystems. In 2004, the algebraic immunity of a Boolean function, which expresses its ability to resist algebraic attack, was introduced by Meier et al. [13]. For each $n$-variable Boolean function $f$, its algebraic immunity is bounded by $\left\lceil \frac{n}{2} \right\rceil$. If this bound is achieved with equality, we say that the function $f$ has an optimal algebraic immunity.

Rotation symmetric Boolean functions are invariant under the action of the cyclic group. The appeal of these functions arises from the facts that they can be stored in less space and allow faster computation of their Walsh spectra. The class of rotation symmetric Boolean functions is rich in cryptographically significant Boolean functions [10, 11, 15, 19]. However, it must be pointed out that finding rotation
symmetric Boolean functions having the main cryptographic parameters all satisfactory for a use in a stream cipher is an open problem and will remain open after this paper. In addition, rotation symmetric bent functions have also been extensively investigated in recent years [4, 12, 16, 18].

The construction of odd-variable rotation symmetric Boolean functions with optimal algebraic immunity has been a research hotspot. For an odd integer \(n = 2k+1\), in 2007, Sarkar and Maitra provided a construction of \(n\)-variable rotation symmetric Boolean functions with optimal algebraic immunity [14]. In 2014, Su and Tang presented a class of \(n\)-variable rotation symmetric Boolean functions with optimal algebraic immunity [17]. In 2016, the authors in paper [11] provided a construction of \(n\)-variable rotation symmetric Boolean functions with optimal algebraic immunity. In 2019, a class of \(n\)-variable rotation symmetric Boolean functions with optimal algebraic immunity and good behavior for resisting fast algebraic attacks was proposed by Zhao et al. [21]. In the same year, Zhang and Su presented a class of theoretical construction of \(n\)-variable rotation symmetric Boolean functions with optimal algebraic immunity [20]. Furthermore, Chen et al. constructed a class of \(n\)-variable rotation symmetric Boolean functions with optimal algebraic immunity and nonlinearity higher than the nonlinearities of the functions in some previous papers but still insufficient [6], since the nonlinearity of Carlet-Feng functions [3] is much higher than the nonlinearities of the above functions. For convenience, the nonlinearities of these \(n\)-variable rotation symmetric Boolean functions are listed in Table 1, where \(|T_h| = \sum_{m=1}^{h-2} p_m(h-2)(h-3)\), \(L_k = \sum_{h=3}^k |T_h|\), and \(p_m(k) = p_{m-1}(k-1) + p_m(k-m)\) with \(p_1(k) = p_k(k) = 1\).

### Table 1. The nonlinearities of the rotation symmetric Boolean functions

| function | nonlinearity |
|----------|--------------|
| [14]     | \(2^{n-1} - \binom{n-1}{k} + 2\) |
| [17]     | \(2^{n-1} - \binom{n-1}{k} + 2^k - 2\) |
| [11]     | \(2^{n-1} - \binom{n-1}{k} + 2^k + 2^{k-2} - k\) |
| [21]     | \(2^{n-1} - \binom{n-1}{k} + 2^k + 2^{k-1} - 2k\) |
| [20]     | \(2^{n-1} - \binom{n-1}{k} + (k - 5)2^{k-1} + 2k + 2\) |
| [6]      | \(2^{n-1} - \binom{n-1}{k} + \sum_{h=3}^k (n - 2h)|T_h| + L_k\) |

In this paper, based on the theory of ordered integer partitions, we construct a new class of rotation symmetric Boolean functions with optimal algebraic immunity on odd variables by modifying the support of the majority function. Compared with the known constructions of odd-variable rotation symmetric Boolean functions with optimal algebraic immunity, this class of rotation symmetric Boolean functions has the highest nonlinearity.

The organization of this paper is given as follows. The preliminaries about Boolean functions and rotation symmetric Boolean functions are introduced in Section 2. The construction of rotation symmetric Boolean functions on odd variables is given in Section 3. In Section 4, the algebraic immunity and the nonlinearity of the newly constructed rotation symmetric Boolean functions are determined. We summarize the main work of this paper in Section 5.
2. Preliminaries

Let $F_2^n$ be the $n$-dimensional vector space over the finite field $F_2 = \{0, 1\}$. Given a vector $\alpha = (a_0, a_1, \ldots, a_{n-1}) \in F_2^n$, we define its support as $\text{supp}(\alpha) = \{0 \leq i < n \mid a_i = 1\}$. The Hamming weight of the vector $\alpha$ is defined as the cardinality of its support, i.e., $\text{wt}(\alpha) = |\text{supp}(\alpha)|$. In this paper, for simplicity, we do not distinguish the vector $(a_0, a_1, \ldots, a_{n-1}) \in F_2^n$ and the integer $\sum_{i=0}^{n-1} a_i 2^i \in \{0, 1, \ldots, 2^n - 1\}$ if the context is clear, since they are one-to-one corresponding. Given two vectors $\alpha = (a_0, a_1, \ldots, a_{n-1})$ and $\beta = (b_0, b_1, \ldots, b_{n-1}) \in F_2^n$, if $a_i \leq b_i$ holds for all $0 \leq i < n$, then $\alpha$ is said to be covered by $\beta$, written as $\alpha \preceq \beta$.

A Boolean function on $n$ variables is a mapping from $F_2^n$ into $F_2$. We denote by $B_n$ the set of all the $n$-variable Boolean functions. The support of an $n$-variable Boolean function $f$ is defined as $\text{supp}(f) = \{ x \in F_2^n \mid f(x) = 1 \}$. The Hamming weight of the function $f$ is the cardinality of its support, i.e., $\text{wt}(f) = |\{ x \in F_2^n \mid f(x) = 1 \}|$. The Hamming distance between two $n$-variable Boolean functions $f$ and $g$ is defined as $d_H(f, g) = \text{wt}(f \oplus g)$. The truth table of the Boolean function $f(x)$ is defined as

$$f = [f(0,0, \ldots, 0), f(1,0, \ldots, 0), f(0,1, \ldots, 0), \ldots, f(1,1, \ldots, 1)].$$

We say that an $n$-variable Boolean function $f$ is balanced if $\text{wt}(f) = 2^{n-1}$, that is, if its truth table contains an equal number of 1’s and 0’s. In cryptography, an $n$-variable Boolean function $f$ can be seen as a multivariate polynomial over $F_2$ as

$$f(x) = \bigoplus_{\alpha \in F_2^n} c_\alpha x^\alpha,$$

where $c_\alpha \in F_2$, $x^\alpha = x_0^{a_0} x_1^{a_1} \cdots x_{n-1}^{a_{n-1}}$ for $x = (x_0, x_1, \ldots, x_{n-1})$ and $\alpha = (a_0, a_1, \ldots, a_{n-1})$. This representation is called the algebraic normal form (ANF) of the function $f$. The algebraic degree of the function $f$ in (1) is defined as

$$\deg(f) = \max\{ \text{wt}(\alpha) \mid \alpha \in F_2^n, c_\alpha = 1 \}.$$

A Boolean function with degree at most one is called an affine function.

The Walsh spectrum of an $n$-variable Boolean function $f$ is an integer-valued function over $F_2^n$, which is defined as

$$W_f(\omega) = \sum_{x \in F_2^n} (-1)^{f(x) \oplus x \cdot \omega},$$

where $\omega \in F_2^n$ and $\omega \cdot x = \omega_0 x_0 + \omega_1 x_1 + \cdots + \omega_{n-1} x_{n-1}$ is the inner product of the vector $\omega = (\omega_0, \omega_1, \ldots, \omega_{n-1})$ and the vector $x = (x_0, x_1, \ldots, x_{n-1})$. The nonlinearity of the function $f$ is the minimum Hamming distance between $f$ and all the affine functions, which can be expressed according to its Walsh spectra as

$$\text{nl}(f) = 2^{n-1} - \frac{1}{2} \max_{\omega \in F_2^n} |W_f(\omega)|.$$

The algebraic immunity of a Boolean function, which expresses its ability to resist algebraic attack, is defined as follows.

**Definition 2.1.** Given an $n$-variable Boolean function $f$, denote

$$\text{AI}(f) = \min\{ \deg(g) \mid 0 \neq g \in B_n \text{ such that } fg = 0 \text{ or } (f \oplus 1)g = 0 \},$$

which is called the algebraic immunity of the function $f$. 
An $n$-variable Boolean function $f$ is said to have an optimal algebraic immunity if $\text{AI}(f) = \left\lceil \frac{n}{2} \right\rceil$.

For a vector $(x_0, x_1, \cdots, x_{n-1}) \in \mathbb{F}_2^n$ and an integer $l \geq 0$, define
\[
\rho_n^l(x_0, x_1, \cdots, x_{n-1}) = (\rho_n^l(x_0), \rho_n^l(x_1), \cdots, \rho_n^l(x_{n-1})),
\]
where $\rho_n^l(x_i) = x_{(i+l \mod n)}$ for $0 \leq i < n$. For instance, $\rho_2^2(1,1,0,1) = (0,1,1,1)$. The orbit generated by the vector $x = (x_0, x_1, \cdots, x_{n-1})$ is defined as
\[
O_n(x) = \{ \rho_n^l(x) \mid 0 \leq l < n \}.
\]
It is clear that the union of all the orbits is equal to the vector space $\mathbb{F}_2^n$. For example, if $n = 3$, then
\[
\begin{align*}
O_3(0,0,0) &= \{(0,0,0)\}; \\
O_3(1,0,0) &= \{(1,0,0), (0,0,1), (0,1,0)\}; \\
O_3(1,1,0) &= \{(1,1,0), (1,0,1), (0,1,1)\}; \\
O_3(1,1,1) &= \{(1,1,1)\}.
\end{align*}
\]

**Definition 2.2.** For an $n$-variable Boolean function $f$, if $f(\rho_n^l(x)) = f(x)$ holds for all the vectors $x \in \mathbb{F}_2^n$, then $f$ is called a rotation symmetric Boolean function.

In other words, a Boolean function is called rotation symmetric, if it is invariant under the action of the cyclic group. Construction of rotation symmetric Boolean functions with good cryptographic properties is the main content of this paper.

3. Construction of Odd-Variable Rotation Symmetric Boolean Functions

In this section, we firstly introduce a conclusion about the ordered partition of a positive integer $k$, which is an important tool for our new construction of rotation symmetric Boolean functions in this paper. And then, the construction of rotation symmetric Boolean functions on odd variables by modifying the support of the majority function is proposed.

3.1. The Ordered Integer Partition. The ordered partition of a positive integer $k$ is a sequence $(k_1, k_2, \cdots, k_l)$ of positive integers such that $k_1 + k_2 + \cdots + k_l = k$, where the order is considered. Each $k_i$ is called a part of the partition of $k$, where $1 \leq i \leq l$. For example, all the ordered partitions of 5 are: (5), (4,1), (3,2), (3,1,1), (2,3), (2,2,1), (2,1,2), (2,1,1,1), (1,4), (1,3,1), (1,2,2), (1,2,1,1), (1,1,3), (1,1,2,1), (1,1,1,2), (1,1,1,1,1). The set of all the partitions of a positive integer $k$ is denoted by
\[
\Gamma(k) = \{(k_1, k_2, \cdots, k_l) \mid k_1 \geq 1, k_2 \geq 1, \cdots, k_l \geq 1, k_1 + k_2 + \cdots + k_l = k\}.
\]

Given two positive integers $i \leq k$, for any fixed integer $l \in \{1, 2, \cdots, k - i + 1\}$, denote
\[
\Gamma^{(l)}(k, i) = \{(k_1, k_2, \cdots, k_l) \in \Gamma(k) \mid k_1 \geq i\},
\]
which is the set of all the partitions of $k$ into $l$ parts with the first part no less than $i$.

The following result might be known, but unfortunately we could not find the original in the literature. So, for completeness, we give a short proof.
Lemma 3.1. The cardinality of the set $\Gamma^{(l)}(k, i)$, defined in (4), is

$$|\Gamma^{(l)}(k, i)| = \binom{k - i}{l - 1},$$

where $i \leq k$ and $1 \leq l \leq k - i + 1$.

Proof. We use mathematical induction on $l$ to complete the proof. Firstly, it is easy to see that $\Gamma^{(1)}(k, i) = \{k\}$ and $\Gamma^{(2)}(k, i) = \{(k - 1, 1), (k - 2, 2), \ldots, (i, k - i)\}$, which implies that the formula in (5) holds for $l = 1$ and 2. Assume that the formula in (5) holds for $l - 1$, i.e., $|\Gamma^{(l-1)}(k, i)| = \binom{k-i}{l-2}$. Then, for a partition $(k_1, k_2, \ldots, k_l) \in \Gamma^{(l-1)}(k, i)$, we know $i \leq k_1 \leq k - (l - 1)$ and $(k_2, k_3, \ldots, k_l) \in \Gamma^{(l-1)}(k - k_1, 1)$, which gives

$$|\Gamma^{(l)}(k, i)| = \sum_{k_1=i}^{k-l+1} |\Gamma^{(l-1)}(k-k_1, 1)|$$

$$= \sum_{k_1=i}^{k-l+1} \binom{k-k_1-1}{l-2}$$

$$= \binom{k-i}{l-1}$$

where the third identity holds by the extended Pascal's rule as $\sum_{s=0}^{p} \binom{k+s}{k} = \binom{k+p+1}{k+1}$.

The proof is done. \qed

3.2. Construction of rotation symmetric Boolean functions. From now on, we always assume $n = 2k + 1$ with $k \geq 4$, and denote

$$W^n_{\leq k} = \{x \in \mathbb{F}_2^n | \text{wt}(x) \leq k\};$$
$$W^n_k = \{x \in \mathbb{F}_2^n | \text{wt}(x) = k\};$$
$$W^n_{\geq k} = \{x \in \mathbb{F}_2^n | \text{wt}(x) \geq k\}.$$

Firstly, according to the theory of ordered integer partitions in the previous subsection, we define five subsets of $\mathbb{F}_2^n$ as

$$T_r = \left\{(1, \ldots, 1, 0, \ldots, 0, 1, \ldots, 1, 0, \ldots, 0, \ldots, 0, 1, \ldots, 0, 0, \ldots, 0) \in \mathbb{F}_2^{n+1} \mid k_1 \geq r + 2, k_2, k_3, \ldots, k_i \geq 1, a_j \in \{1, 2\}, 1 \leq j \leq i - 1\right\},$$

where $r \in \{1, 2, 3, 4, 5\}$. In (6), it is easy to see that $k_1 + k_2 + \cdots + k_i = k$ since $\text{wt}(\alpha) = k$ for every $\alpha \in T_r$, where $1 \leq r \leq 5$. Furthermore, we know $a_1 + a_2 + \cdots + a_{i-1} = n - k - (k - i + 2 - r) = i + r - 1$ and $k - k_1 \geq i - 1$. Hence, for the vectors in each subset $T_r$ defined in (6), there exist $r$ integers $l_1, l_2, \ldots, l_r \in \{1, 2, \ldots, i-1\}$ such that

$$a_t = \begin{cases} 2, & t \in \{l_1, l_2, \ldots, l_r\}, \\ 1, & t \in \{1, 2, \ldots, i-1\} \setminus \{l_1, l_2, \ldots, l_r\}, \end{cases}$$

since $a_j \in \{1, 2\}$ for all $1 \leq j \leq i-1$, where $1 \leq r \leq 5$. Therefore, $T_1 \cap T_2 \cap \cdots \cap T_5 = \emptyset$. It should be noted that some of the subsets $T_r$ in (6) may be empty for small values of $k$. For example, when $k = 4$, we have $T_2 = T_3 = T_4 = T_5 = \emptyset$. 


Denote
\begin{equation}
T = \bigcup_{r=1}^{5} T_r,
\end{equation}
which is a subset of $W_n$, where $T_1$, $T_2$, $\ldots$, $T_5$ are defined in (6). For convenience, list all the vectors in the subset $T$ defined in (7) according to the lexicographical order (note that all of these vectors have the same Hamming weight) as
\begin{equation}
T = \{\alpha_1, \alpha_2, \ldots, \alpha_{|T|}\}.
\end{equation}
According to the definition of the subset $T_r$ in (6), $1 \leq r \leq 5$, let us figure out the number of the different vectors in the subset $T$ defined in (8) as follows.

(1) If $k = 4$, then $|T| = |T_1| = 1$.
(2) If $k = 5$, then $|T| = |T_1| = 4$.
(3) If $k = 6$, then $|T| = |T_1| + |T_2| = 13$.
(4) If $k \geq 7$, then
\begin{align*}
|T| &= \sum_{r=1}^{5} |T_r| \\
&= \sum_{r=1}^{5} \sum_{i=2}^{k-r-1} |\Gamma^{(i)}(k, r+2)| \binom{i-1}{r} \\
&= \sum_{r=1}^{5} \sum_{i=2}^{k-r-1} \binom{k-r-2}{i-1} \binom{i-1}{r} \\
&= (k-3)2^{k-4} + (k-4)(k-5)2^{k-7} + \frac{1}{3}(k-5)(k-6)(k-7)2^{k-9} + \\
&\quad + \frac{1}{3}(k-6)(k-7)(k-8)(k-9)2^{k-13} + \\
&\quad + \frac{1}{15}(k-7)(k-8)(k-9)(k-10)(k-11)2^{k-15} \\
&= \left(\frac{1}{15}k^5 - \frac{5}{3}k^4 + 35k^3 - \frac{475}{3}k^2 + \frac{28994}{15}k - 5168\right)2^{k-15}
\end{align*}
where $\Gamma^{(i)}(k, r+2)$ is defined in (4), and the third identity holds by Lemma 3.1.

**Remark 1.** If $k = 4$ (5, 6 resp.), by a direct calculation, we have
\begin{align*}
\left(\frac{1}{15}k^5 - \frac{5}{3}k^4 + 35k^3 - \frac{475}{3}k^2 + \frac{28994}{15}k - 5168\right)2^{k-15} &= 1 - \frac{17}{256}(4 - \frac{1}{64}, 13 - \frac{1}{64} \text{ resp.})
\end{align*}
In this paper, for convenience, if $k = 4, 5,$ or 6, we always denote
\begin{align*}
\left(\frac{1}{15}k^5 - \frac{5}{3}k^4 + 35k^3 - \frac{475}{3}k^2 + \frac{28994}{15}k - 5168\right)2^{k-15} &= [\left(\frac{1}{15}k^5 - \frac{5}{3}k^4 + 35k^3 - \frac{475}{3}k^2 + \frac{28994}{15}k - 5168\right)2^{k-15}].
\end{align*}

**Example 1.** According to the definition of the subset $T$ in (8), when $n = 9$, we have
\begin{equation}
T = \{(1, 1, 0, 0, 1, 0, 0, 0)\}.
\end{equation}
When \( n = 11 \), we have
\[
T = \{(1, 1, 1, 0, 0, 1, 0, 0, 0, 0), (1, 1, 1, 0, 0, 1, 0, 0, 0, 0), (1, 1, 0, 0, 1, 0, 0, 0, 0, 0)\}.
\]

When \( n = 13 \), the vectors in the subset \( T \) defined in (8) are illustrated in Table 2.

| \( \alpha_1 \) | \( \alpha_2 \) | \( \alpha_3 \) | \( \alpha_4 \) | \( \alpha_5 \) | \( \alpha_6 \) | \( \alpha_7 \) | \( \alpha_8 \) | \( \alpha_9 \) | \( \alpha_{10} \) | \( \alpha_{11} \) | \( \alpha_{12} \) | \( \alpha_{13} \) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 3 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 4 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |
| 5 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0 |
| 6 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 |
| 7 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 |
| 8 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 |
| 9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 |
| 10 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 11 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 12 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Secondly, let’s define five more subsets of \( F^n_2 \) as
\[
U_r = \left\{ u_s = \alpha_s \oplus (0, 0, \cdots, 0, 1, \cdots, 1, 0) \mid \alpha_s = (1, \cdots, 1), \right. \\
\left. \begin{array}{c}
\alpha_s = (1, \cdots, 1), \\
k_1 - r - 1 \\
0, \cdots, 0, \cdots, 0, \cdots, 1, \cdots, 1, 0, \cdots, 0 \\
k_1 - k - 1 - k - 1 + 2 - r
\end{array} \right\} \in T_r,
\]
where \( 1 \leq r \leq 5 \) and \( k_1 - r - 1 \geq 1 \) since \( k_1 \geq r + 2 \). Obviously, \( |U_r| = |T_r| \) for \( 1 \leq r \leq 5 \). Note that \( k - i + 2 - r - (k_1 - r - 1) = k - k_1 - i + 3 \geq 2 \) since \( k - k_1 \geq i - 1 \). Hence, we get \( U_r \subseteq W^n_{2k+1} \) for \( 1 \leq r \leq 5 \). Similarly, denote
\[
U = \bigcup_{r=1}^{5} U_r.
\]
Then, \( U = \{ u_1, u_2, \cdots, u_{|T|} \} \), and
\[
|U| = |T| = \left( \frac{1}{15} k^5 - \frac{5}{3} k^4 + 35 k^3 - \frac{475}{3} k^2 + \frac{28994}{15} k - 5168 \right) 2^{k-15},
\]
where the subset \( T \) of \( F^n_2 \) is defined in (8).

Among all the known Boolean functions with optimal algebraic immunity, the most famous one is the \( n \)-variable majority function as
\[
F(x) = \left\{ \begin{array}{ll}
1, & \text{wt}(x) \geq \left\lfloor \frac{n}{2} \right\rfloor, \\
0, & \text{otherwise},
\end{array} \right.
\]
where $x \in \mathbb{F}_2^n$. The construction of new $n$-variable Boolean functions by modifying the support of the majority function is given as

\[(13) \quad f(x) = \begin{cases} F(x) \oplus 1, & x \in \bigcup_{\alpha_i \in T} O_n(\alpha_i) \cup \bigcup_{u_i \in U} O_n(u_i), \\ F(x), & \text{otherwise}, \end{cases}\]

where $x \in \mathbb{F}_2^n$, $F(x)$ is the $n$-variable majority function given in (12), and the subsets $T$ and $U$ of $\mathbb{F}_2^n$ are defined in (8) and (10) respectively.

By Definition 2.2, it is easy to see that the function $f(x)$ in (13) is rotation symmetric.

4. THE CRYPTOGRAPHIC PROPERTIES OF THE FUNCTION $f(x)$ IN (13)

In this section, the cryptographic properties (algebraic immunity and nonlinearity) of the $n$-variable rotation symmetric Boolean function $f(x)$ in (13) are determined. Furthermore, its algebraic degree and fast algebraic immunity are also discussed for small values of $n$.

4.1. THE ALGEBRAIC IMMUNITY OF THE FUNCTION $f(x)$ IN (13)

In this subsection, we consider the algebraic immunity of the rotation symmetric Boolean function $f(x)$ defined in (13). Recall that the most simple method to prove that the Boolean function $f(x)$ has an optimal algebraic immunity is by using the following conclusion.

**Lemma 4.1** ([5]). Let $S = \{\beta_1, \beta_2, \ldots, \beta_l\} \subseteq W_n^n$ and $V = \{v_1, v_2, \ldots, v_l\} \subseteq W_{\geq k+1}^n$ for some integer $0 < l \leq \binom{n}{k}$. If the vectors in $S$ and $V$ satisfy

$$\beta_i \preceq v_i \text{ for } 1 \leq i \leq l, \quad \beta_j \preceq v_i \text{ for } 1 \leq i < j \leq l \text{ (or } 1 \leq j < i \leq l),$$

the Boolean function

$$f_1(x) = \begin{cases} F(x) \oplus 1, & x \in S \cup V \\ F(x), & \text{otherwise} \end{cases}$$

has an optimal algebraic immunity, where $x \in \mathbb{F}_2^n$ and $F(x)$ is the majority function given in (12).

**Lemma 4.2.** For any vectors $\alpha_s \in T$ in (8) and $u_s \in U$ in (10), we have

1. If $u_s \in U_r$, then $wt(u_s) = k+k_1-r-1$, where $U_r$ is defined in (9), $1 \leq r \leq 5$, and $r+2 \leq k_1 \leq k$;
2. $\rho_n(\alpha_s) \leq \rho_n(u_s)$ for $0 \leq l < n$;
3. $\rho_n(\alpha_s) \neq \alpha_s$ and $\rho_n(u_s) \neq u_s$ for $1 \leq l < n$;
4. $\rho_n(\alpha_s) \neq \rho_n(u_s)$ for $1 \leq l < n$;
5. $\rho_n(\alpha_s) \neq \rho_n(u_s)$ for $0 \leq l < n$ and $1 \leq s < t \leq |T|$.

**Proof.** For $1 \leq r \leq 5$, given two vectors $\alpha_s \in T_r$ in (6) and $u_s \in U_r$ in (9), they can be written as

$$\alpha_s = (1, \ldots, 1, 0, \ldots, 0, 1, \ldots, 1, 0, \ldots, 0), \quad k_1 a_1 k_2 a_2 k_{i-1} k_i k_{i+2-r},$$
where \( k_1 \geq r + 2, k_2, k_3, \ldots, k_i \geq 1, a_j \in \{1, 2\}, \) and \( 1 \leq j \leq i - 1. \)

1. By (9), it is easy to see that \( \text{wt}(u_s) = \text{wt}(\alpha_s) + (k_1 - r - 1) = k + k_1 - r - 1 \)
   for any vector \( u_s \in U_r. \)
2. We can easily get \( \rho_n^l(\alpha_s) \leq \rho_n^l(u_s) \) for \( 0 \leq l < n \) since \( k - k_1 - i + 2 \geq 1. \)
3. Firstly, \( \rho_n^l(\alpha_s) \neq \alpha_s \) for \( 1 \leq l < n \) since \( k - i + 2 - r \geq 3. \) Secondly, \( \rho_n^l(u_s) \neq u_s \)
   for \( 1 \leq l < n \) since \( k - k_1 - i + 2 \geq 1 \) and by the fact that
   \[
   \begin{cases}
   k_2 = k_3 = \cdots = k_1 = 1, & \text{if } k - k_1 - i + 2 = 1, \\
   k_2 = \cdots = k_{t-1} = k_t - 1 = k_{t+1} = \cdots = k_i = 1, & \text{if } k - k_1 - i + 2 = 2,
   \end{cases}
   \]
   where \( t \in \{2, 3, \ldots, i\}. \)
4. By the same reason for \( \rho_n^l(u_s) \neq u_s \) above, it is easy to see that \( \alpha_s \not\leq \rho_n^l(u_s), \)
   where \( 1 \leq l < n. \)
5. Since all the vectors in the subset \( T \) are listed according to the lexicographical order, we know \( \alpha_s \not\leq \rho_n^l(u_t) \) for \( 0 \leq l < n. \)

The proof is done.

**Theorem 4.3.** The rotation symmetric Boolean function \( f(x) \) defined in (13) has an optimal algebraic immunity.

**Proof.** Denote \( \tilde{T} = \bigcup_{\alpha_i \in T} O_n(\alpha_i) \) and \( \tilde{U} = \bigcup_{u_i \in U} O_n(\alpha_i), \)
where \( T \) and \( U \) are two subsets of \( \mathbb{F}_2^n \) given in (8) and (10) respectively. In fact, by Lemma 4.2, we know the vectors in the subsets \( \tilde{T} \) and \( \tilde{U} \) can be listed as
\[
\tilde{T} = \{\rho_n^0(\alpha_1), \rho_n^1(\alpha_1), \ldots, \rho_n^{n-1}(\alpha_1), \ldots, \rho_n^0(\alpha_T), \rho_n^1(\alpha_T), \ldots, \rho_n^{n-1}(\alpha_T)\},
\]
\[
\tilde{U} = \{\rho_n^0(u_1), \rho_n^1(u_1), \ldots, \rho_n^{n-1}(u_1), \ldots, \rho_n^0(u_T), \rho_n^1(u_T), \ldots, \rho_n^{n-1}(u_T)\}.
\]

To prove that the Boolean function \( f(x) \) in (13) has an optimal algebraic immunity, we only need to check that the following three conditions hold.

1. \( \rho_n^l(\alpha_s) \leq \rho_n^l(u_s) \) for \( 1 \leq s \leq |T| \) and \( 0 \leq l < n; \)
2. \( \rho_n^m(\alpha_s) \not\leq \rho_n^m(u_s) \) for \( 1 \leq s \leq |T| \) and \( 0 \leq m < l < n; \)
3. \( \rho_n^m(\alpha_s) \not\leq \rho_n^m(u_t) \) for \( 1 \leq s < t \leq |T| \) and \( 0 \leq m, l < n. \)

According to Lemma 4.2, the above three conclusions are obviously true.

The proof is done.

### 4.2. The Nonlinearity of the Function \( f(x) \) in (13)

In this subsection, we determine the nonlinearity of the rotation symmetric Boolean function \( f(x) \) defined in (13).

First of all, given the two subsets \( T \) and \( U \) of \( \mathbb{F}_2^n \) being defined in (8) and (10) respectively, from Lemma 4.2, we know \( \rho_n^l(\alpha_i) \neq \alpha_i \) and \( \rho_n^l(u_i) \neq u_i \) for \( 1 \leq l < n, \)
in other words,
\[
|O_n(\alpha_i)| = |O_n(u_i)| = n,
\]
where $\alpha_i \in T$ and $u_i \in U$ for $1 \leq i \leq |T|$. Hence, by (11), we have

$$\left| \bigcup_{\alpha_i \in T} O_n(\alpha_i) \right| = \left| \bigcup_{u_i \in U} O_n(u_i) \right| = n\left(\frac{1}{15} k^5 - \frac{5}{3} k^4 + 35 k^3 - \frac{475}{3} k^2 + \frac{28994}{15} k - 5168\right)2^{k-15}.$$ 

To compute the nonlinearity of the newly constructed odd-variable rotation symmetric Boolean function $f(x)$ defined in (13), we should introduce the Walsh spectra of the majority function $F(x)$ in (12) as follows.

**Lemma 4.4** ([8, 14]). $F(x)$ is the majority function on $n$ variables given in (12). If $n = 2k + 1$, the following results hold.

1. If $\text{wt}(\omega) = 1$, then $W_F(\omega) = 2^{(n-1)}$.
2. If $\text{wt}(\omega) = n$, then $W_F(\omega) = 2(-1)^k (n-1)\binom{n}{k}.$
3. If $2 \leq \text{wt}(\omega) \leq n - 1$, then $|W_F(\omega)| \leq 2\left(\binom{n-3}{k-1}\right)$, where $n \geq 7$.

To compare the absolute value of the Walsh spectra of the newly constructed odd-variable rotation symmetric Boolean function $f(x)$ defined in (13) at the different vectors in $F_2^n$, we need one more lemma as follows.

**Lemma 4.5.** When $k \geq 6$, we have

$$\frac{4k - 3}{4k - 2} \binom{2k}{k} > \frac{1}{3} k^6 2^{k-14}.$$ 

**Proof.** The proof can be completed by mathematical induction on $k$. When $6 \leq k \leq 10$, by a direct calculation, we have $\frac{4k - 3}{4k - 2} \binom{2k}{k} > \frac{1}{3} k^6 2^{k-14}$. Assume that (14) holds for $k - 1$, i.e., $\frac{4k - 7}{4k - 6} \binom{2k-2}{k-1} > \frac{1}{3} (k-1)^6 2^{k-15}$, where $k \geq 11$. Then, as for $k$, we have

$$\frac{4k - 3}{4k - 2} \binom{2k}{k} - \frac{1}{3} k^6 2^{k-14} = \frac{(4k - 3)(2k)(2k - 1)(4k - 6)}{(4k - 2)k^2(4k - 7)} \frac{4k - 7}{4k - 6} \binom{2k - 2}{k - 1} - \frac{2k^6}{(k-1)^6} \frac{1}{3} (k - 1)^6 2^{k-15} > \frac{4k - 3}{4k - 6} \frac{4k - 7}{(k - 1)^6} \binom{2k - 2}{k - 1} - \frac{2k^6}{(k-1)^6} \frac{1}{3} (k - 1)^6 2^{k-15} > 0$$

where the first inequality holds since $\frac{4k - 7}{4k - 6} > 1$, and the last inequality holds by the assumption that (14) holds for $k - 1$ and the fact that if $k \geq 11$ then

$$\frac{4k - 3}{k} - \frac{2k^6}{(k-1)^6} = 4 - \frac{3}{k} - \frac{2k^6}{(k-1)^6} > 0.$$ 

The proof is done. \hfill $\square$

**Theorem 4.6.** The nonlinearity of the rotation symmetric Boolean function $f(x)$ defined in (13) is

$$\text{nl}(f) = 2^{n-1} - \binom{n-1}{k} + \left(\frac{4}{15} k^5 - 8k^4 + \frac{524}{3} k^3 - 1208k^2 + \frac{160576}{15} k - 32768\right)2^{k-15} + 2,$$

where $n = 2k + 1 \geq 13$. 
Proof. According to the definition of the function \( f(x) \) in (13), its Walsh spectrum at the vector \( \omega \in \mathbb{F}_2^n \), defined in (2), is

\[
W_f(\omega) = \sum_{x \in \mathbb{F}_2^n \setminus \bigcup_{i=1}^{\mid T \mid} (O_n(\alpha_i) \cup O_n(u_i))} (-1)^{F(x) \oplus \omega \cdot x} + \\
\sum_{x \in \bigcup_{i=1}^{\mid T \mid} (O_n(\alpha_i) \cup O_n(u_i))} (-1)^{F(x) \oplus 1 \oplus \omega \cdot x}
\]

\[
= \sum_{x \in \mathbb{F}_2^n} (-1)^{F(x) \oplus \omega \cdot x} - 2 \sum_{x \in \bigcup_{i=1}^{\mid T \mid} (O_n(\alpha_i) \cup O_n(u_i))} (-1)^{F(x) \oplus \omega \cdot x}
\]

\[
= W_F(\omega) - 2 \sum_{i=1}^{\mid T \mid} \sum_{x \in O_n(\alpha_i)} (-1)^{\omega \cdot x} + 2 \sum_{i=1}^{\mid T \mid} \sum_{x \in O_n(u_i)} (-1)^{\omega \cdot x}
\]

which will be discussed in the following cases, where \( F(x) \) is the \( n \)-variable majority function in (12), \( \alpha_i \in T \) in (8), and \( u_i \in U \) in (10).

(C1) When \( \text{wt}(\omega) = 0 \), we know \( W_f(\omega) = 0 \) since \( W_F(\omega) = 0 \) and \( \omega \cdot x = 0 \).

(C2) When \( \text{wt}(\omega) = 1 \), by Lemma 3.1 and Lemma 4.4, we have

\[
W_f(\omega) = 2 \binom{n-1}{k} - 2 \left( \frac{1}{15} k^5 - \frac{5}{3} k^4 + 35k^3 - \frac{475}{3} k^2 + \frac{28994}{15} k - 5168 \right) 2^{k-15} - \\
2 \sum_{k_1=3}^{k-1} (2k_1 - 5) \sum_{i=2}^{k-k_1+1} \binom{k-k_1-1}{i-2} (i-1) - \\
2 \sum_{k_1=4}^{k-2} (2k_1 - 7) \sum_{i=2}^{k-k_1+1} \binom{k-k_1-1}{i-2} (i-1) - \\
2 \sum_{k_1=5}^{k-3} (2k_1 - 9) \sum_{i=2}^{k-k_1+1} \binom{k-k_1-1}{i-2} (i-1) - \\
2 \sum_{k_1=6}^{k-4} (2k_1 - 11) \sum_{i=2}^{k-k_1+1} \binom{k-k_1-1}{i-2} (i-1) - \\
2 \sum_{k_1=7}^{k-5} (2k_1 - 13) \sum_{i=2}^{k-k_1+1} \binom{k-k_1-1}{i-2} (i-1) -
\]
When \( \omega_i \) is even, we have \( \sum_{x \in O_n(\alpha_i)} (-1)^{\omega_x} = n(-1)^k \) for \( \alpha_i \in T \) since \( \text{wt}(\alpha_i) = k \), and \( \sum_{x \in O_n(\alpha_i)} (-1)^{\omega_x} = -2k_1 + 2r + 3 \) for \( u_i \in U_r \) since \( \text{wt}(u_i) = k + k_1 - r - 1 \) by Lemma 4.2 with \( U_r \) being defined in (9) for \( 1 \leq r \leq 5 \).

(C3) When \( \text{wt}(\omega) = n \), we have \( \sum_{x \in O_n(\alpha_i)} (-1)^{\omega_x} = n(-1)^k \) for \( \alpha_i \in T \) since \( \text{wt}(\alpha_i) = k \), and \( \sum_{x \in O_n(\alpha_i)} (-1)^{\omega_x} = n(-1)^{k + k_1 - r - 1} \) for \( u_i \in U_r \) since \( \text{wt}(u_i) = k + k_1 - r - 1 \), where \( 1 \leq r \leq 5 \). Hence, by Lemma 4.4, we have

\[
W_f(\omega) = 2^n (-1)^k \left( \binom{n-1}{k} - \left( \frac{1}{15} k^5 - \frac{5}{3} k^4 + 35k^3 - \frac{475}{3} k^2 + \frac{28994}{15} k - 5168 \right) 2^{k-15} + 
\right.
\]

where the first identity holds by the facts that \( \sum_{x \in O_n(\alpha_i)} (-1)^{\omega_x} = -k + k + 1 = 1 \) for \( \alpha_i \in T \) since \( \text{wt}(\alpha_i) = k \), and \( \sum_{x \in O_n(\alpha_i)} (-1)^{\omega_x} = -2k_1 + 2r + 3 \) for \( u_i \in U_r \) since \( \text{wt}(u_i) = k + k_1 - r - 1 \) by Lemma 4.2 with \( U_r \) being defined in (9) for \( 1 \leq r \leq 5 \).
and the second inequality is also true by Lemma 4.5.

Furthermore, by a direct verification, we get

$$
2(-1)^k \left[ \left( \frac{n-1}{k} \right) - \left( \frac{1}{15} k^5 - \frac{5}{3} k^4 + 35k^3 - \frac{475}{3} k^2 + \frac{28994}{15} k - 5168 \right) 2^{k-15} + 
\sum_{k_1=3}^{k-1} n(-1)^{k_1-2}(k-k_1+1)2^{k-k_1-2} + 
\sum_{k_1=4}^{k-2} n(-1)^{k_1-3}(k-k_1-1)(k-k_1+2)2^{k-k_1-4} + 
\frac{1}{3} \sum_{k_1=5}^{k-3} n(-1)^{k_1-4}(k-k_1-1)(k-k_1-2)(k-k_1+3)2^{k-k_1-5} + 
\frac{1}{3} \sum_{k_1=6}^{k-4} n(-1)^{k_1-5}(k-k_1-1)(k-k_1-2)(k-k_1-3)(k-k_1+4)2^{k-k_1-8} + 
\frac{1}{15} \sum_{k_1=7}^{k-5} n(-1)^{k_1-6}(k-k_1-1) \cdots (k-k_1-4)(k-k_1+5)2^{k-k_1-9} \right]
$$

$$
= 2(-1)^k \left[ \left( \frac{n-1}{k} \right) - \left( \frac{1}{15} k^5 - \frac{14}{27} k^4 + \frac{883}{81} k^3 - \frac{3302}{81} k^2 + \frac{735688}{1215} k - \frac{1096000}{729} \right) n^{2^{k-13}} - \frac{242}{729} n(-1)^k \right]
$$

Furthermore, by a direct verification, we get

$$
2 \left[ \left( \frac{n-1}{k} \right) - \left( \frac{1}{15} k^5 - \frac{14}{27} k^4 + \frac{883}{81} k^3 - \frac{3302}{81} k^2 + \frac{735688}{1215} k - \frac{1096000}{729} \right) n^{2^{k-13}} - \frac{242}{729} n(-1)^k \right]
$$

$$< 2 \left[ \left( \frac{n-1}{k} \right) - \left( \frac{4}{15} k^5 - 8k^4 + \frac{524}{3} k^3 - 1208k^2 + \frac{160576}{15} k - 32768 \right) 2^{k-15} - 2 \right].
$$

(C4) When $2 \leq \text{wt}(\omega) \leq n - 1$, we have

$$
|W_f(\omega)| \leq 2 \left[ \left( \frac{n-3}{k-1} \right) - \left( \frac{n-3}{k} \right) + 2n \left( \frac{1}{15} k^5 - \frac{5}{3} k^4 + 35k^3 - \frac{475}{3} k^2 + \frac{28994}{15} k - 5168 \right) 2^{k-15} \right]
$$

$$< 2 \left[ \left( \frac{n-1}{k} \right) - \left( \frac{4}{15} k^5 - 8k^4 + \frac{524}{3} k^3 - 1208k^2 + \frac{160576}{15} k - 32768 \right) 2^{k-15} - 2 \right]
$$

where the first inequality is true because

$$
\left| \sum_{x \in O_n(a_i)} (-1)^{\omega \cdot x} \right| \leq n, \quad \left| \sum_{x \in O_n(u_i)} (-1)^{\omega \cdot x} \right| \leq n,
$$

and the second inequality is also true by Lemma 4.5.
Therefore, by (3), the nonlinearity of the rotation symmetric Boolean function \( f(x) \) in (13) is

\[
\text{nl}(f) = 2^{n-1} - \binom{n-1}{k} + \left( \frac{4}{15}k^5 - 8k^4 + \frac{524}{3}k^3 - 1208k^2 + \frac{160576}{15}k - 32768 \right)2^{k-15} + 2.
\]

The proof is done. \( \square \)

**Remark 2.** If \( k = 4 \) (5 resp.), we have

\[
2^{n-1} - \binom{n-1}{k} + \left( \frac{4}{15}k^5 - 8k^4 + \frac{524}{3}k^3 - 1208k^2 + \frac{160576}{15}k - 32768 \right)2^{k-15} + 2
\]

\[= 188 + \frac{1}{16} \left( 782 + \frac{1}{32} \right) \text{ resp.}.
\]

On the other hand, if \( k = 4 \) (5 resp.), by a direct calculation, the nonlinearity of the \( n \)-variable rotation symmetric Boolean function \( f(x) \) defined in (13) is equal to 188 (782 resp.).

So far, only a few classes of odd-variable rotation symmetric Boolean functions with optimal algebraic immunity were given. When \( n \in \{9, 11, 13, 15, 17, 19, 21, 27, 37, 47, 57\} \), the nonlinearities of the majority function \( F(x) \) in (12), Carlet-Feng functions in [3], the rotation symmetric Boolean functions given before, and the rotation symmetric Boolean function \( f(x) \) defined in (13) are listed in Table 3 and Table 4.

### Table 3. Comparison of the nonlinearities

| \( n \) | 9   | 11  | 13  | 15  | 17  | 19  | 21  |
|--------|-----|-----|-----|-----|-----|-----|-----|
| \( F(x) \) | 186 | 772 | 3172| 12952| 52666| 213524| 863820 |
| [3]     | 232 | 980 | 3988| 16212| 65210| 261428| 1046552 |
| [17]    | 802 | 3234| 13078| 52920| 214034| 864842 |
| [21]    | 810 | 3256| 13130| 53034| 214274| 865336 |
| [20]    | 784 | 3218| 13096| 53068| 214568| 86402 |
| [6]     | 794 | 3230| 13098| 53044| 214486| 866294 |
| \( f \) in (13) | 188 | 782 | 3208| 13064| 52988| 214406| 866160 |

### Table 4. Comparison of the nonlinearities

| \( n \) | 27  | 37  | 47  | 57  |
|--------|-----|-----|-----|-----|
| \( F(x) \) | 56708264 | 59644341436| 62135313450064| 64408903437167496 |
| [17]   | 56716454 | 59644603578| 62135321838670| 64408903705602950 |
| [21]   | 56720526 | 59644734616| 62135326032930| 64408903839820624 |
| [20]   | 56741060 | 59646045410| 62135388947584| 64408906524175298 |
| [6]    | 56748298 | 5964802864| 62135605652036| 64408924613659456 |
| \( f \) in (13) | 56747394 | 59647951550| 62135614817362| 64408926590774154 |
From Table 3, we find that although the nonlinearities of these rotation symmetric Boolean functions are higher than that of the majority function $F(x)$, there is still a big gap from the nonlinearity of Carlet-Feng functions. So, they are insufficient to be used in stream ciphers. Any way, from Table 4, we find that the nonlinearity of our newly constructed rotation symmetric Boolean functions on $n$ variables is higher than that of previous ones for $n \geq 47$. In fact, if $n \geq 43$, our newly constructed functions on $n$ variables have the highest nonlinearity of all the rotation symmetric Boolean functions with optimal algebraic immunity.

To quantify the efficiency of fast correlation attacks on Boolean functions, we should know their nonlinearity biases. The nonlinearity bias of an $n$-variable Boolean function $f$ is defined as $1 - 2^{-(n-1)\text{nl}(f)}$. The nonlinearity bias of the majority function $F(x)$ in (12), Carlet-Feng functions in [3], the known rotation symmetric Boolean functions, and the $n$-variable Boolean functions $f(x)$ in (13) are given in Table 5 for $n \in \{9, 11, 13, 15, 17, 19, 21, 27, 37, 47, 57\}$.

| $n$ | 9   | 11  | 13  | 15  | 17  | 19  | 21  | 27  | 37  | 47  | 57  |
|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| $F(x)$ | 0.273 | 0.246 | 0.226 | 0.209 | 0.1964 | 0.1855 | 0.1762 | 0.15498 | 0.132061 | 0.11700499 | 0.10614691 |
| [3] | 0.094 | 0.043 | 0.026 | 0.010 | 0.0050 | 0.0027 | 0.0019 | 0.0019 | 0.0019 | 0.0019 | 0.0019 |
| [17] | 0.217 | 0.210 | 0.202 | 0.1925 | 0.1835 | 0.1752 | 0.15486 | 0.132057 | 0.11700397 | 0.10614690 |
| [21] | 0.209 | 0.205 | 0.199 | 0.1908 | 0.1826 | 0.1748 | 0.15480 | 0.132055 | 0.11700391 | 0.10614690 |
| [20] | 0.234 | 0.214 | 0.201 | 0.1902 | 0.1815 | 0.1737 | 0.15449 | 0.132036 | 0.11699994 | 0.10614686 |
| [6]  | 0.224 | 0.211 | 0.201 | 0.1906 | 0.1818 | 0.1738 | 0.15438 | 0.132007 | 0.11699994 | 0.10614690 |
| $f$ in (13) | 0.266 | 0.236 | 0.217 | 0.203 | 0.1915 | 0.1821 | 0.1740 | 0.15440 | 0.132008 | 0.11699981 | 0.10614658 |

In Table 5, the nonlinearity biases of the $n$-variable Carlet-Feng functions are only listed for $n \leq 21$ because it takes too long to get the actual values of the nonlinearity of the $n$-variable Carlet-Feng functions for $n \geq 27$.

4.3. CONCRETE CRYPTOGRAPHIC PROPERTIES OF THE $n$-VARIABLE FUNCTION $f(x)$ IN (13) FOR $n = 9, 11, 13, 15$. It is known that an $n$-variable Boolean function $f$ can be considered as optimal with respect to fast algebraic attacks if there do not exist two nonzero functions $g$ and $h$ such that $fg = h$ and $\deg(g) + \deg(h) < n$ with $\deg(g) < \frac{n}{2}$. Generally, the fast algebraic immunity, resistance to fast algebraic attacks, of the function $f$ is defined as

$$FAI(f) = \min\{2AI(f), \min\{\deg(g) + \deg(fg) \mid 1 \leq \deg(g) < AI(f)\}\}.$$ 

Nevertheless, the fast algebraic immunity of a Boolean function on $n$ variables is very hard to be determined. So, we must rely on computer simulations only for relatively small value of $n$.

For $n = 9, 11, 13, 15$, some cryptographic properties of the $n$-variable rotation symmetric Boolean function $f(x)$ defined in (13) are listed as follows.

1. If $n = 9$, the subsets $T$ and $U$ defined in (7) and (10) are

$$T = \{39\},$$
$$U = \{167\}.$$

The algebraic degree of $f$ is 8 and the fast algebraic immunity of $f$ is 6.

2. If $n = 11$, the subsets $T$ and $U$ defined in (7) and (10) are

$$T = \{79, 103, 151, 167\},$$
$$U = \{615, 663, 679, 847\}.$$
The algebraic degree of \( f \) is 10 and the fast algebraic immunity of \( f \) is 8.

(3) If \( n = 13 \), the subsets \( T \) and \( U \) defined in (7) and (10) are
\[
T = \{ 159, 207, 231, 303, 311, 335, 359, 407, 591, 599, 663, 679 \},
\]
\[
U = \{ 2279, 2359, 2407, 2455, 2471, 2639, 2647, 2711, 2727, 3279, 3375, 3407, 3743 \}.
\]

The algebraic degree of \( f \) is 12 and the fast algebraic immunity of \( f \) is 10.

(4) If \( n = 15 \), the subsets \( T \) and \( U \) defined in (7) and (10) are
\[
T = \{ 319, 415, 463, 487, 607, 623, 631, 719, 743, 815, 823, 847, 871, 919, 935, 1183, 1199, 1207, 1231, 1239, 1237, 1335, 1359, 1383, 1431, 1447, 1615, 1623, 1687, 1703, 2351, 2383, 2391, 2639, 2647, 2711, 2727 \},
\]
\[
U = \{ 8679, 8823, 8935, 9015, 9063, 9111, 9127, 9399, 9423, 9431, 9527, 9575, 9623, 9639, 9807, 9815, 9879, 9895, 10543, 10575, 10583, 10831, 10839, 10903, 10919, 12751, 12911, 13007, 13103, 13135, 13471, 13487, 13615, 13647, 14751, 14943, 15007, 15679 \}.
\]

The algebraic degree of \( f \) is 14 and the fast algebraic immunity of \( f \) is 10.

At the end of this subsection, the fast algebraic immunities of Carlet-Feng functions in [3], the rotation symmetric Boolean functions in [6, 20, 21], and the rotation symmetric Boolean function \( f(x) \) in (13) are given in Table 6.

| \( n \) | 9 | 11 | 13 | 15 |
|-------|---|----|----|----|
| [3]   | 8 | 10 | 12 | 14 |
| [21]  |   | 10 | 12 | 14 |
| [20]  |   | 10 | 12 | 13 |
| [6]   |   | 10 | 12 | 14 |
| \( f \) in (13) | 6 | 8  | 10 | 10 |

From Table 6, we find that the fast algebraic immunity of our newly constructed rotation symmetric Boolean functions is not as good as that of the previous ones.

5. Conclusion

In this paper, we present a new construction of odd-variable rotation symmetric Boolean functions with optimal algebraic immunity by using a similar method of constructing rotation symmetric Boolean functions given by Su and Tang in paper [17]. In that paper, they partitioned the \( k \) 1’s into \( i \) parts and put one 0 into any two adjacent parts. In this paper, we put one 0 or two 0’s into any two adjacent parts. Our study is a step forward in the study of rotation symmetric Boolean functions for stream ciphers but it does not provide functions usable in stream ciphers since the nonlinearity is still not high enough. Anyway, when \( n \geq 43 \), our newly constructed functions on \( n \) variables in this paper have the highest nonlinearity of all the rotation symmetric Boolean functions with optimal algebraic immunity. How to construct \( n \)-variable rotation symmetric Boolean functions with higher nonlinearity is our future work.

Acknowledgments

The authors would like to thank the associate editor and the anonymous reviewers for their constructive comments and suggestions which improved the quality of the paper.
References

[1] A. Canteaut and M. Trabbia, Improved fast correlation attacks using parity-check equations of weight 4 and 5, in Advances in Cryptology-EUROCRYPT 2000 (eds. B. Preneel), Springer, Berlin, Heidelberg, 2000, 573–588.

[2] C. Carlet, Boolean functions for cryptography and error correcting codes, to appear in Cambridge University Press.

[3] C. Carlet and K. Feng, An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity, in ASIACRYPT 2008 (eds. J. Pieprzyk), Lecture Notes in Computer Science, 5350, Springer, Heidelberg, 2008, 425–440.

[4] C. Carlet, G. Gao and W. Liu, A secondary construction and a transformation on rotation symmetric functions, and their action on bent and semi-bent functions, J. Combin. Theory Ser. A, 127 (2014), 161–175.

[5] C. Carlet, X. Zeng, C. Li and L. Hu, Further properties of several classes of Boolean functions with optimum algebraic immunity, Des. Codes Cryptogr., 52 (2009), 303–338.

[6] Y. Chen, F. Guo and J. Ruan, Constructing odd-variables RSBFs with optimal algebraic immunity, good nonlinearity and good behavior against fast algebraic attacks, Discrete Appl. Math., 262 (2019), 1–12.

[7] N. Courtois and W. Meier, Algebraic attacks on stream ciphers with linear feedback, in EUROCRYPT 2003, Lecture Notes in Computer Science, 2656, Springer-Verlag, Heidelberg, 2003, 345–359.

[8] D. Dalal, S. Maitra and S. Sarkar, Basic theory in construction of Boolean functions with maximum possible annihilator immunity, Des. Codes Cryptogr. 40 (2006), 41–58.

[9] C. Ding, G. Xiao and W. Shan, The stability theory of stream ciphers, in Lecture Notes in Computer Science, 561, Springer-Verlag, Berlin, 1991.

[10] J. Du, Q. Wen, J. Zhang and S. Pang, Constructions of resilient rotation symmetric Boolean functions on given number of variables, IET Inform. Secur., 8 (2014), 265–272.

[11] S. Fu, J. Du, L. Qu and C. Li, Construction of odd-variable rotation symmetric boolean functions with maximum algebraic immunity, IEICE Trans. Fundam. Electron. Commun. Comput. Sci., 99 (2016), 853–855.

[12] G. Gao, Constructions of quadratic and cubic rotation symmetric bent functions, IEEE Trans. Inform. Theory, 58 (2012), 4908–4913.

[13] W. Meier, E. Pasalic and C. Carlet, Algebraic attacks and decomposition of Boolean functions, in Advances in Cryptology-EUROCRYPT 2004, Lecture Notes in Computer Science, 3027, Springer Heidelberg, 2004, 474–491.

[14] S. Sarkar and S. Maitra, Construction of rotation symmetric Boolean functions with maximum algebraic immunity on odd number of variables, in AAECC 2007, Lecture Notes in Computer Science, 4851, 2007, 271–280.

[15] P. Stnic and S. Maitra, Rotation symmetric Boolean functions-count and cryptographic properties, Discrete Appl. Math., 156 (2002), 1567–1580.

[16] S. Su, A new construction of rotation symmetric bent functions with maximal algebraic degree, Adv. Math. Commun., 13 (2019), 253–265.

[17] S. Su and X. Tang, Construction of rotation symmetric Boolean functions with optimal algebraic immunity and high nonlinearity, Des. Codes Cryptogr., 71 (2014), 183–199.

[18] S. Su and X. Tang, Systematic constructions of rotation symmetric bent functions, 2-rotation symmetric bent functions, and bent idempotent functions, IEEE Trans. Inf. Theory, 63 (2017), 4658–4667.

[19] L. Sun, F. Fu and X. Guang, Two classes of 1-resilient prime-variable rotation symmetric Boolean functions, IEICE Trans Fund. Electron. Comm. Comput. Sci., E100-A (2017), 902–907.

[20] H. Zhang and S. Su, A new construction of rotation symmetric Boolean functions with optimal algebraic immunity and higher nonlinearity, Discrete Appl. Math., 262 (2019), 13–28.

[21] Q. Zhao, G. Han, D. Zheng and X. Li, Constructing odd-variable rotation symmetric Boolean functions with optimal algebraic immunity and high nonlinearity, Chinese J. Electron., 28 (2019), 45–51.

Received April 2020; 1st revision July 2020; final revision September 2020.
E-mail address: 1342728729@qq.com
E-mail address: sush@henu.edu.cn