IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 9, 2021, accepted April 25, 2021, date of publication May 3, 2021, date of current version May 13, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3077145

Balanced Rotation Symmetric Boolean Functions With Good Autocorrelation Properties

LEI SUN[1] AND ZEXIA SHI[2]
[1]College of Information Technology, Hebei University of Economics and Business, Shijiazhuang 050061, China
[2]School of Mathematical Sciences, Hebei Normal University, Shijiazhuang 050024, China

Corresponding author: Lei Sun (sunlei@mail.nankai.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61902107, in part by the Natural Science Foundation of Hebei Province under Grant F2019207112, in part by the Project Supported by Science Foundation of Hebei Normal University under Grant L2021B04, and in part by the Research Foundation of Hebei University of Economics and Business under Grant 2020YB17.

ABSTRACT Rotation symmetric Boolean functions (RSBFs) are used widely in symmetric cryptography. In this paper, a systematic construction of balanced odd-variable RSBFs satisfying strict avalanche criterion is proposed. Hence, a class of $(6k + 3)$-variable resilient RSBFs satisfying strict avalanche criterion is also presented for any $k \geq 2$. Some of the obtained RSBFs have many other good cryptographic properties at the same time, that is, optimal algebraic degree, good global avalanche characteristics, high nonlinearity and nonexistence of nonzero linear structures. Moreover, we obtain some count results of RSBFs satisfying strict avalanche criterion. This is the first time that the autocorrelation properties of RSBFs are investigated systemically.

INDEX TERMS Cryptography, global avalanche characteristics, resilient, Rotation symmetric Boolean functions, strict avalanche criterion.

I. INTRODUCTION

Boolean functions are central building blocks for many symmetric cryptosystems, which should satisfy some cryptography criteria to resist known attacks, such as nonlinearity, balancedness, algebraic degree, etc. To express the avalanche effect of cryptographic functions, Webster and Tavares [23] proposed the strict avalanche criterion (SAC). Note that the SAC is only a measure for local avalanche. To characterize the overall avalanche characteristics, the global avalanche characteristics (GAC) was introduced by Zhang and Zheng [25]. The GAC consists of two indicators: the sum-of-squares indicator and the absolute indicator. The SAC and GAC indicate a function's autocorrelation properties. Although bent functions have the best autocorrelation properties, they are not balanced and only exist when the number of variables is even. Therefore, constructing Boolean functions with balancedness and good autocorrelation properties is favored [10], [16], [18], [22].

Rotation symmetric Boolean functions (RSBFs) is a subclass of Boolean functions which are invariant under the action of cyclic group. RSBFs have import applications in cryptography since they allow faster computation and need smaller storage space. The cryptographic parameters of BSBFs have been investigated widely, such as resilient RSBFs [7], [10], [14], bent RSBFs [2], [9], [19], [21], RSBFs with optimal algebraic immunity [3], [8], [13]. However, there are no results on investigating the autocorrelation properties of RSBFs so far.

This paper first gives a theoretical framework for constructing balanced RSBFs satisfying SAC, which have some other good cryptographic properties simultaneously. The main idea behind our method is to modify the outputs of a quadratic RSBF on a selected set of orbits. When $n = 6k+3$, we obtain n-variable RSBFs with good autocorrelation properties, resiliency, highest algebraic degree, nonexistence of nonzero linear structures, high nonlinearity. Moreover, the enumeration of RSBFs satisfying SAC is also discussed based on integer partition. This is the first time that the construction and enumeration of RSBFs satisfying SAC are investigated.

This paper is organized as follows. Sect. 2 introduces some necessary notions on Boolean functions and RSBFs. Sect. 3 presents the constructions of odd-variable balanced RSBFs with good autocorrelation properties. In Sect. 4, some count results of RSBFs satisfying SAC is provided. Sect. 5 concludes this paper.

The associate editor coordinating the review of this manuscript and approving it for publication was Aneel Rahim.

II. PRELIMINARIES

Let $\mathbb{F}_2^n$ be the n-dimensional vector space over the binary field $\mathbb{F}_2$. An n-variable Boolean function f is a mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2$, which can be uniquely represented by its algebraic normal form (ANF):

$$f(x_1, x_2, \ldots, x_n) = \sum_{I \subseteq \{1,2,\ldots,n\}} a_I \prod_{i \in I} x_i, a_I \in \mathbb{F}_2.$$

Its algebraic degree is defined as $deg(f) = \max\{|I| : a_I \neq 0\}$. The Hamming weight of f is $wt(f) = |\{\alpha \in \mathbb{F}_2^n : f(\alpha) = 1\}|$, and f is balanced if $wt(f) = 2^{n-1}$. Denote by $\mathfrak{B}_n$ the set of all n-variable Boolean functions.

Let $\alpha = (a_1, a_2, \ldots, a_n) \in \mathbb{F}_2^n$, $supp(\alpha) = \{1 \leq i \leq n : a_i = 1\}$ is called the support of α, and $wt(\alpha) = |supp(\alpha)|$ is called the Hamming weight of α. For any $1 \leq j \leq n$ and $i \in supp(\alpha)$, $i+j$ is meant cyclically in the set $\{1, 2, 3, \ldots, n\}$. The complement of α is defined as $\bar{\alpha} = (1+a_1, 1+a_2, \ldots, 1+a_n)$. For a vector $\beta = (b_1, b_2, \ldots, b_n) \in \mathbb{F}_2^n$, the dot product of β and α is $\beta \cdot \alpha = b_1 a_1 + \cdots + b_n a_n$. For any nonempty set $T \subseteq \mathbb{F}_2^n$, let $\alpha + T = \{\alpha + \beta : \beta \in T\}$.

Let $f \in \mathfrak{B}_n$. The Walsh transform of f at $\alpha \in \mathbb{F}_2^n$ is defined as

$$W_f(\alpha) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+\alpha \cdot x}. \tag{1}$$

Clearly, f is balanced if and only if $W_f(0) = 0$, where $\mathbf{0}$ is the all-zero vector in $\mathbb{F}_2^n$. The nonlinearity of f is

$$nl(f) = 2^{n-1} - \frac{1}{2} \max_{\alpha \in \mathbb{F}_2^n} |W_f(\alpha)|.$$

It is well known that $nl(f) \leq 2^{n-1} - 2^{\frac{n}{2}-1}$, and if $nl(f) = 2^{n-1} - 2^{\frac{n}{2}-1}$, we call f a bent function.

Cryptographic functions with low autocorrelation have nice diffusion property. Let $f \in \mathfrak{B}_n$ and $\alpha \in \mathbb{F}_2^n$, its autocorrelation function at α is

$$C_f(\alpha) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x+\alpha)+f(x)}.$$

f is said to satisfy the strict avalanche criterion (SAC) if $C_f(\alpha) = 0$ for all $wt(\alpha) = 1$. Global avalanche characteristics (GAC) contains two indicators: the absolute indicator

$$\Delta_f = \max_{\alpha \neq 0} |C_f(\alpha)|$$

and the sum-of-squares indicator

$$\sigma_f = \sum_{\alpha \in \mathbb{F}_2^n} C_f^2(\alpha).$$

In [25], Zheng showed that $2^{2n} \leq \sigma_f \leq 2^{3n}$ and $0 \leq \Delta_f \leq 2^n$, and proved that only bent functions can achieve the lower bounds.

Cryptographic functions with resiliency are robust against correlation attacks.

Definition 1 [24]: Let $f \in \mathfrak{B}_n$ and $\alpha \in \mathbb{F}_2^n$. f is called a k-resilient function if $W_f(\alpha) = 0$ holds for all $wt(\alpha) \leq k$.

Lemma 1 [15]: Let $f \in \mathfrak{B}_n$. If f is k-resilient, then $deg(f) + k \leq n - 1$.

Let $f(x) \in \mathfrak{B}_n$, its derivative at point $\alpha \in \mathbb{F}_2^n$ is defined as $\Delta_\alpha f(x) = f(x + \alpha) + f(x)$. Clearly, $deg(\Delta_\alpha f) < deg(f)$. α is called a linear structure of f if $\Delta_\alpha f(x)$ is a constant for all $x \in \mathbb{F}_2^n$.

To resist against algebraic and fast algebraic attacks [5], [6], Boolean functions used in cryptography should have high algebraic immunity and fast algebraic immunity.

Definition 2: Let $f, h \in \mathfrak{B}_n$. The algebraic immunity of f is

$$AI(f) = \min_{h \neq 0}\{deg(h) : hf = 0 \text{ or } h(f+1) = 0\},$$

and the fast algebraic immunity of f is

$$FAI(f) = \min\{2AI(f), \min\{deg(fh) + deg(h) : 1 \leq deg(h) < AI(f)\}\}.$$

We say that f has optimal AI if $AI(f) = \lceil \frac{n}{2} \rceil$, and f has optimal FAI if $FAI(f) = n$.

Let $\alpha = (a_1, a_2, \ldots, a_n) \in \mathbb{F}_2^n$. For any $0 \leq m \leq n-1$, define

$$\rho_n^m(\alpha) = (a_{1+m}, a_{2+m}, \ldots, a_{n+m}),$$

where the addition of index is meant cyclically in the set $\{1, 2, 3, \ldots, n\}$.

Definition 2: Let $f \in \mathfrak{B}_n$. If $f(\rho_n^m(\alpha)) = f(\alpha)$ holds for any $0 \leq m \leq n-1$ and $\alpha \in \mathbb{F}_2^n$, then f is called a rotation symmetric Boolean function (RSBF).

Denote by $G_n(\alpha) = \{\rho_n^m(\alpha) : 0 \leq m \leq n-1\}$ the orbit generated from α. Hence, we call $G_n(\alpha)$ a long orbit if $|G_n(\alpha)| = n$, and call it a short orbit if $|G_n(\alpha)| < n$. It is shown that [17] $W_f(\alpha) = W_f(\beta)$ for $\alpha \in G_n(\beta)$ if f is rotation symmetric.

III. CONSTRUCTIONS OF RSBFs SATISFYING SAC

A. BALANCED RSBFs HAVING GOOD AUTOCORRELATION PROPERTIES

We first present the following necessary result on quadratic RSBFs.

Lemma 2: For odd n and $2 \leq s \leq \frac{n+1}{2}$, let $k = \gcd(s-1, n)$ and

$$g_s = x_1 x_s + x_2 x_{s+1} + \cdots + x_n x_{s-1}. \tag{2}$$

Then $wt(g_s) = 2^{n-1}$, $nl(g_s) = 2^{n-1} - 2^{\frac{n+k}{2}-1}$.

We assume hereafter that n is an odd integer. For $2 \leq s \leq \frac{n+1}{2}$ with $\gcd(s-1, n) = 1$, we set

$$d_s = \min\{n - 2(s-1), 2(s-1)\}$$

and define a subset $R_s \subseteq \mathbb{F}_2^n$ as

$$R_s = \{\alpha_1^s, \alpha_2^s, \alpha_3^s, \ldots, \alpha_{n-1}^s\}, \tag{3}$$

where

$$supp(\alpha_1^s) = \{1\},$$
$$supp(\alpha_{2j}^s) = \{1, s, 1 + 2d_s, s + 2d_s, \ldots, 1 + 2(j-1)d_s, s + 2(j-1)d_s\}, 1 \leq j \leq \lfloor \frac{n-1}{4} \rfloor,$$

$$supp(\alpha^s_{2j+1}) = \{1, s, \ldots, 1+2(j-1)d_s, s+2(j-1)d_s, 1+2jd_s\}, 1 \le j \le \lfloor \frac{n-3}{4} \rfloor,$$
$$\alpha^s_i = \bar{\alpha}^s_{n-i}, \frac{n+1}{2} \le i \le n-1.$$

For $1 \le i \le n-1$ and $1 \le j \le n$, define

$$A^s_j(i) = \sum_{x \in G_n(\alpha^s_i)} (-1)^{g_s(x)+g_s(x+e_j)}, \tag{4}$$

where $e_j = (\underbrace{0, \ldots, 0}_{j-1}, 1, 0, \ldots, 0)$, $g_s(x)$ is defined in (2).

Lemma 3: R_s and $A^s_j(i)$ defined above have the following properties.

1) $wt(\alpha^s_i) = i$.
2) $|G_n(\alpha^s_i)| = n$.
3) *If* $i < \frac{n+1}{2}$, *then*

$$g_s(\alpha^s_i) = \begin{cases} 1, & i \bmod 4 \equiv 2, 3, \\ 0, & i \bmod 4 \equiv 0, 1; \end{cases}$$

and if $i \ge \frac{n+1}{2}$, *then* $g_s(\alpha^s_i) = 1 - g_s(\alpha^s_{n-i})$.
4) $A^s_j(i) = n - 4\min\{i, n-i\}$.

Proof:

1) This holds obviously by the definition of R_s.
2) Note that $|G_n(\alpha^s_i)| = |G_n(\alpha^s_{n-i})|$ and $|G_n(\alpha^s_1)| = n$. For $2 \le i \le \frac{n-1}{2}$, assume that $|G_n(\alpha^s_i)| = k < n$. Since $1+k, s+k \in supp(\alpha^k_i)$, then we have the following four cases:

$$a) \begin{cases} 1+k = s+t_1d_s - k_1n \\ s+k = s+t_2d_s - k_2n \end{cases}$$
$$b) \begin{cases} 1+k = 1+t_1d_s - k_1n \\ s+k = 1+t_2d_s - k_2n \end{cases}$$
$$c) \begin{cases} 1+k = s+t_1d_s - k_1n \\ s+k = 1+t_2d_s - k_2n \end{cases}$$
$$d) \begin{cases} 1+k = 1+t_1d_s - k_1n \\ s+k = s+t_2d_s - k_2n \end{cases}$$

where $0 \le t_1, t_2 \le \frac{n-1}{2}$ and $k_1, k_2 \ge 0$.
Here we only prove that case a) doesn't hold, and other cases can be proved similarly. For case a), we have

$$s-1 = (t_2-t_1)d_s + (k_1-k_2)n.$$

If $d_s = 2(s-1)$, then $(1+2(t_1-t_2))(s-1) = (k_1-k_2)n$. Note that $|1+2(t_1-t_2)| < n$. Since $\gcd(s-1, n) = 1$, then $k_1 - k_2$ is a multiple of $s-1$, that is $|s-1| \le |k_1-k_2|$. Hence

$$|(1+2(t_1-t_2))(s-1)| < |(k_1-k_2)n|,$$

a contradiction. If $d_s = n-2(s-1)$, we have

$$s-1 = (t_2-t_1)(n-2(s-1)) + (k_1-k_2)n,$$

then $(2(t_2-t_1)+1)(s-1) = (k_1-k_2+t_2-t_1)n$. Since $\gcd(s-1, n) = 1$, then $k_1-k_2+t_2-t_1$ is a multiple of $s-1$, that is $|s-1| \le |k_1-k_2+t_2-t_1|$. Note that $|2(t_2-t_1)+1| < n$. Hence

$$|(2(t_2-t_1)+1)(s-1)| < |(k_1-k_2+t_2-t_1)n|,$$

a contradiction. Then the desired result follows.
3) This holds obviously according to the definitions of g_s and R_s.
4) For $1 \le j \le n$, we have

$$\begin{aligned} &g_s(x) + g_s(x+e_j) \\ &= \sum_{i=1}^{n} x_{1+i}x_{s+i} + \sum_{i \ne j-1, i \ne n+j-s}^{n} x_{1+i}x_{s+i} \\ &\quad + (x_j+1)x_{s+j-1} + x_{n+j-s+1}(x_j+1) \\ &= x_{s+j-1} + x_{n+j-s+1} \\ &= x_{s+j-1} + x_{s+j-1+n-2(s-1)}. \end{aligned}$$

By the definition of α^s_i that

$$|\{x \in G_n(\alpha^s_i) : x_{s+j-1} + x_{s+j-1+n-2(s-1)} = 1\}| = 2\min\{wt(\alpha^s_i), n - wt(\alpha^s_i)\},$$

that is,

$$|\{x \in G_n(\alpha^s_i) : x_{s+j-1} + x_{s+j-1+n-2(s-1)} = 1\}| = 2\min\{i, n-i\}.$$

Therefore $A^s_j(i) = n - 4\min(i, n-i)$.

Lemma 4: For $T \subseteq \mathbb{F}_2^n$ and $T \ne \varnothing$, let $\widetilde{T} = \bigcup_{\alpha \in T} G_n(\alpha)$. For any $\alpha \in \mathbb{F}_2^n$ and $\alpha \ne 0$, we have

$$\mathbb{F}_2^n \backslash [\widetilde{T} \cup (\widetilde{T} + \alpha)] + \alpha = \mathbb{F}_2^n \backslash [\widetilde{T} \cup (\widetilde{T} + \alpha)].$$

Proof: Assume that there exists $\gamma \in \mathbb{F}_2^n \backslash [\widetilde{T} \cup (\widetilde{T} + \alpha)]$ such that $\gamma + \alpha \in \widetilde{T} \cup (\widetilde{T} + \alpha)$. Then we have $\gamma + \alpha \in \widetilde{T}$ or $\gamma + \alpha \in \widetilde{T} + \alpha$. Hence, $\gamma \in \widetilde{T} \cup (\widetilde{T} + \alpha)$, a contradiction. This completes the proof.

Now we are ready to construct RSBFs having good auto-correlation properties. Let $n \ge 11$ be odd. For $1 \le m \le \lceil n/16 \rceil$ and $1 \le i_1, i_2, \ldots, i_{4m} \le n-1$, let $I = \{i_1, i_2, \ldots, i_{4m}\}$ and $T_{s,I} = \{\alpha^s_{i_1}, \alpha^s_{i_2}, \ldots, \alpha^s_{i_{4m}}\} \subseteq R_s$. Define U_I, a subset of I, as:

$$\begin{aligned} U_I &= \{i_t \in I : i_t \bmod 4 \equiv 0, 1\} \text{ if } n \equiv 3 \bmod 4, \\ U_I &= \{i_t \in I : i_t < \frac{n+1}{2}, i_t \bmod 4 \equiv 0, 1 \text{ or } \\ &\qquad i_t \ge \frac{n+1}{2}, i_t \bmod 4 \equiv 2, 3\} \text{ if } n \equiv 1 \bmod 4. \end{aligned} \tag{5}$$

Note that $g_s(\alpha^s_i) = 0$ if and only if $i \in U_I$. Denote

$$n - I = \{n - i_1, n - i_2, \ldots, n - i_{4m}\}, \quad D_I = |I \cap (n-I)|. \tag{6}$$

Define

$$f_{s,I}(x) = \begin{cases} g_s(x), & x \in \mathbb{F}_2^n \backslash \widetilde{T}_{s,I}, \\ 1 + g_s(x), & x \in \widetilde{T}_{s,I}, \end{cases} \tag{7}$$

where $\widetilde{T}_{s,I} = \bigcup_{\alpha\in T_{s,I}} G_n(\alpha)$. Clearly, $f_{s,I}$ is an n-variable RSBF.

Theorem 1: $f_{s,I}$ defined in (7) has the following properties.

1) *If* $\sum_{t=1}^{4m} \min\{i_t, n-i_t\} = mn$ *and* $|i_{t_1} - i_{t_2}| \geq 2$ *holds for any* $i_{t_1}, i_{t_2} \in I$, *then* $f_{s,I}$ *satisfies the strict avalanche criterion.*
2) *If* $|U_I| = 2m$ *then* $f_{s,I}$ *is balanced.*
3) $\Delta_{f_{s,I}} = 2^n - 4n(4m - D_I)$.
4) $\sigma_{f_{s,I}} < 2^{2n+1} + 2^{n+8}m^2n^2$.
5) *If* $|D_I| \neq 4m$, $f_{s,I}$ *has no nonzero linear structures.*
6) $nl(f_{s,I}) > 2^{n-1} - 2^{\frac{n-1}{2}} - 4mn$.

Proof: 1). Assume that $\alpha \in \widetilde{T}_{s,I}$ and $wt(\alpha) = i_t \in I$. For $1 \leq j \leq n$, we have $wt(\alpha + e_j) = i_t \pm 1$. Since $|i_{t_1} - i_{t_2}| \geq 2$ holds for any $i_{t_1}, i_{t_2} \in I$, then $i_t \pm 1 \notin I$. It follows that $\alpha + e_j \notin \widetilde{T}_{s,I}$, that is $(\widetilde{T}_{s,I} + e_j) \cap \widetilde{T}_{s,I} = \varnothing$. Hence, by Lemma 4 we have

$$\mathbb{F}_2^n \backslash [\widetilde{T}_{s,I} \cup (\widetilde{T}_{s,I} + e_j)] + e_j = \mathbb{F}_2^n \backslash [\widetilde{T}_{s,I} \cup (\widetilde{T}_{s,I} + e_j)].$$

Denote $\mathfrak{T}_j = \widetilde{T}_{s,I} \cup (\widetilde{T}_{s,I} + e_j)$. For $1 \leq j \leq n$, we have

$$\begin{aligned}
&\sum_{x\in\mathbb{F}_2^n} (-1)^{f_{s,I}(x)+f_{s,I}(x+e_j)} \\
&= \sum_{x\in\mathbb{F}_2^n\backslash\mathfrak{T}_j} (-1)^{f_{s,I}(x)+f_{s,I}(x+e_j)} + \sum_{x\in\mathfrak{T}_j} (-1)^{f_{s,I}(x)+f_{s,I}(x+e_j)} \\
&= \sum_{x\in\mathbb{F}_2^n\backslash\mathfrak{T}_j} (-1)^{g_s(x)+g_s(x+e_j)} - \sum_{x\in\mathfrak{T}_j} (-1)^{g_s(x)+g_s(x+e_j)} \\
&= \sum_{x\in\mathbb{F}_2^n} (-1)^{g_s(x)+g_s(x+e_j)} - 2\sum_{x\in\mathfrak{T}_j} (-1)^{g_s(x)+g_s(x+e_j)} \\
&= -2\sum_{x\in\mathfrak{T}_j} (-1)^{g_s(x)+g_s(x+e_j)} \\
&= -4\sum_{i\in I} A_j^s(i).
\end{aligned}$$

By Lemma 3, we have

$$\sum_{i\in I} A_j^s(i) = 4mn - 4\sum_{t=1}^{4m} \min\{i_t, n-i_t\}.$$

If $\sum_{t=1}^{4m} \min\{i_t, n-i_t\} = mn$, then $\sum_{i\in I} A_j^s(i) = 0$. It follows that

$$\sum_{x\in\mathbb{F}_2^n} (-1)^{f_{s,I}(x)+f_{s,I}(x+e_j)} = 0.$$

Therefore, $f_{s,I}$ satisfies SAC.

2). Observe that

$$\begin{aligned}
|supp(f_{s,I})| = |supp(g_s)| &- |\{x \in \widetilde{T}_{s,I} : g_s(x) = 1\}| \\
&+ |\{x \in \widetilde{T}_{s,I} : g_s(x) = 0\}|.
\end{aligned}$$

By Lemma 2, we know that g_s is balanced, then $|supp(g_s)| = 2^{n-1}$. If $|U_I| = 2m$, then

$$|\{i_t \in I : g_s(\alpha_{i_t}^s) = 1\}| = |\{i_t \in I : g_s(\alpha_{i_t}^s) = 0\}|.$$

By Lemma 3, we have

$$|\{x \in \widetilde{T}_{s,I} : g_s(x) = 1\}| = |\{x \in \widetilde{T}_{s,I} : g_s(x) = 0\}|.$$

Therefore, $|supp(f_{s,I})| = 2^{n-1}$, that is $f_{s,I}(x)$ is balanced.

3). For any $\alpha \in \mathbb{F}_2^n \backslash \{0\}$, denote $\mathfrak{T}_\alpha = \widetilde{T}_{s,I} \cup (\widetilde{T}_{s,I} + \alpha)$. By Lemma 4, we have

$$\begin{aligned}
C_{f_{s,I}}(\alpha) &= \sum_{x\in\mathbb{F}_2^n\backslash\mathfrak{T}_\alpha} (-1)^{f_{s,I}(x)+f_{s,I}(x+\alpha)} \\
&\quad + \sum_{x\in\mathfrak{T}_\alpha} (-1)^{f_{s,I}(x)+f_{s,I}(x+\alpha)} \\
&= \sum_{x\in\mathbb{F}_2^n\backslash\mathfrak{T}_\alpha} (-1)^{g_s(x)+g_s(x+\alpha)} \\
&\quad + \sum_{x\in\mathfrak{T}_\alpha} (-1)^{f_{s,I}(x)+f_{s,I}(x+\alpha)} \\
&= \sum_{x\in\mathbb{F}_2^n} (-1)^{g_s(x)+g_s(x+\alpha)} \\
&\quad - \sum_{x\in\mathfrak{T}_\alpha} (-1)^{g_s(x)+g_s(x+\alpha)} \\
&\quad + \sum_{x\in\mathfrak{T}_\alpha} (-1)^{f_{s,I}(x)+f_{s,I}(x+\alpha)}.
\end{aligned}$$

Denote by 1 the all-one vector in $\mathbb{F}_2^n$. When $\alpha \neq 1$, $g_s(x) + g_s(x+\alpha)$ is a linear function. Then $\sum_{x\in\mathbb{F}_2^n} (-1)^{g_s(x)+g_s(x+\alpha)} = 0$, and hence $|C_{f_{s,I}}(\alpha)| \leq 16mn$. When $\alpha = 1$, then $g_s(x)+g_s(x+1) = 1$. Hence,

$$\begin{aligned}
&\sum_{x\in\mathbb{F}_2^n} (-1)^{g_s(x)+g_s(x+1)} = -2^n, \\
&\sum_{x\in\widetilde{T}_{s,I}\cup(\widetilde{T}_{s,I}+1)} (-1)^{g_s(x)+g_s(x+1)} = -|\widetilde{T}_{s,I} \cup (\widetilde{T}_{s,I}+1)| \\
&\qquad\qquad = -n(8m - D_I), \\
&\sum_{x\in\widetilde{T}_{s,I}\cup(\widetilde{T}_{s,I}+1)} (-1)^{f_{s,I}(x)+f_{s,I}(x+1)} = n(8m - 3D_I).
\end{aligned}$$

Thus,

$$\begin{aligned}
|C_{f_{s,I}}(1)| &= |-2^n + n(8m - D_I) + n(8m - 3D_I)| \\
&= 2^n - 4n(4m - D_I).
\end{aligned}$$

Consequently, $\Delta_{f_{s,I}} = |C_{f_{s,I}}(1)| = 2^n - 4n(4m - D_I)$.

4). We have

$$\begin{aligned}
\sigma_{f_{s,I}} &= \sum_{\alpha\in\mathbb{F}_2^n\backslash\{0,1\}} C_{f_{s,I}}^2(\alpha) + C_{f_{s,I}}^2(0) + C_{f_{s,I}}^2(1) \\
&< 2^{2n+1} + 2^{n+8}m^2n^2.
\end{aligned}$$

5). If $\alpha \in \mathbb{F}_2^n$ is a nonzero linear structure of $f_{s,I}$, then $|C_{f_{s,I}}(\alpha)| = 2^n$, which implies that $\alpha = 1$ and $|D_I| = 4m$. Therefore, if $|D_I| \neq 4m$, then $f_{s,I}$ has no nonzero linear structures.

6). For any $\alpha \in \mathbb{F}_2^n$, by (1) and (7) we have

$$\begin{aligned}|W_{f_{s,I}}(\alpha)| &= |\sum_{x\in\mathbb{F}_2^n\setminus\widetilde{T}_{s,I}}(-1)^{g_s(x)+\alpha\cdot x} - \sum_{x\in\widetilde{T}_{s,I}}(-1)^{g_s(x)+\alpha\cdot x}| \\ &= |W_{g_s}(\alpha) - 2\sum_{x\in\widetilde{T}_{s,I}}(-1)^{g_s(x)+\alpha\cdot x}| \\ &< |W_{g_s}(\alpha)| + 2|\widetilde{T}_{s,I}| \\ &= |W_{g_s}(\alpha)| + 8mn.\end{aligned}$$

Since $\gcd(n, s-1) = 1$, it follows Lemma 2 that $nl(g_s) = 2^{n-1} - 2^{\frac{n-1}{2}}$, that is $\max\{|W_{g_s}(\alpha)| : \alpha \in \mathbb{F}_2^n\} = 2^{\frac{n+1}{2}}$. Thus $|W_{f_{s,I}}(\alpha)| < 2^{\frac{n+1}{2}} + 8mn$, and then $nl(f_{s,I}) > 2^{n-1} - 2^{\frac{n-1}{2}} - 4mn$.

Example 1: Let $n = 11$ *and* $s = 2$, *then* $g_2(x) = \sum_{i=1}^{n} x_{1+i}x_{2+i}$,

$$R_2 = \{\alpha_i^2 : i = 1, 2, \ldots, 10\},$$

where

$$\begin{aligned}&supp(\alpha_1^2) = \{1\}, supp(\alpha_{10}^2) = \{2, 3, 4, 5, 6, 7, 8, 9, 10, 11\},\\ &supp(\alpha_2^2) = \{1, 2\}, supp(\alpha_9^2) = \{3, 4, 5, 6, 7, 8, 9, 10, 11\},\\ &supp(\alpha_3^2) = \{1, 2, 5\}, supp(\alpha_8^2) = \{3, 4, 6, 7, 8, 9, 10, 11\},\\ &supp(\alpha_4^2) = \{1, 2, 5, 6\}, supp(\alpha_8^2) = \{3, 4, 7, 8, 9, 10, 11\},\\ &supp(\alpha_5^2) = \{1, 2, 5, 6, 9\}, supp(\alpha_8^2) = \{3, 4, 7, 8, 10, 11\}.\end{aligned}$$

Let $I = \{1, 5, 7, 10\}$, $T_{2,I} = \{\alpha_1^2, \alpha_5^2, \alpha_7^2, \alpha_{10}^2\}$, $\widetilde{T}_{2,I} = \bigcup_{\alpha\in T_{2,I}} G_n(\alpha)$, *then*

$$f_{2,I}(x) = \begin{cases} g_2(x), & x \in \mathbb{F}_2^n\setminus\widetilde{T}_{2,I},\\ 1 + g_2(x), & x \in \widetilde{T}_{2,I},\end{cases}$$

is a 11-variable balanced RSBF satisfying SAC, and with $nl(f_{2,I}) = 982$, $\Delta_{f_{2,I}} = 1960$, $\sigma_{f_{2,I}} = 1.16 \times 2^{23}$ *and* $deg(f_{2,I}) = 10$.

Theorem 2: Let notions be defined as above. For $k \geq 1$, *we set*

$$T = \begin{cases} \{\alpha_1^2, \alpha_{4k+1}^2, \alpha_{4k+3}^2, \alpha_{n-1}^2\}, & n = 8k+3,\\ \{\alpha_2^2, \alpha_{4k}^2, \alpha_{4(k+1)}^2, \alpha_{n-2}^2\}, & n = 8k+5,\\ \{\alpha_1^2, \alpha_{4k+3}^2, \alpha_{4k+5}^2, \alpha_{n-1}^2\}, & n = 8k+7,\\ \{\alpha_2^2, \alpha_{4k+2}^2, \alpha_{4k+6}^2, \alpha_{n-2}^2\}, & n = 8k+9,\end{cases}$$

and $\widetilde{T} = \bigcup_{\alpha\in T} G_n(\alpha)$. *Define a new n-variable RSBF as:*

$$f(x) = \begin{cases} g_2(x), & x \in \mathbb{F}_2^n\setminus\widetilde{T},\\ 1 + g_2(x), & x \in \widetilde{T}.\end{cases} \tag{8}$$

Then $f(x)$ *has the following properties.*

1) f *is a balanced .*
2) f *satisfies SAC.*
3) $nl(f) \geq 2^{n-1} - 2^{\frac{n-1}{2}} - 4n$.
4) $\Delta_f = 2^n - 16n$.
5) $\sigma_f \leq 2^{2n+1} + 2^{n+8}n^2$.
6) f *has no nonzero linear structures.*
7) $\deg(f) = n - 1$.

Proof: 1)∼6) can be verified according to Theorem 1.

7). Here we only prove the case of $n = 8k + 3$, and the proof of other cases can be got similarly. Let $\alpha_i = (a_{i_1}, a_{i_2}, \ldots, a_{i_n}) \in supp(f)$, $1 \leq i \leq |supp(f)|$, then

$$f(x) = \sum_{i=1}^{|supp(f)|}\prod_{j=1}^{n}(x_j + a_{i_j} + 1).$$

We denote c_1 the coefficient of $x_1x_2\cdots x_n/x_1$ in the ANF of $f(x)$. Let S be a subset of $\mathbb{F}_2^n$, and denote N_S the number of vectors in the S with the 1-th entry being 0. Obviously, $c_1 = N_{supp(f)} \bmod 2$.

Note that

$$supp(f) = supp(g_2)\bigcup(G_n(\alpha_1^2) \cup (\alpha_{4k+1}^2)) \setminus(G_n(\alpha_{4k+3}^2) \cup \alpha_{n-1}^2).$$

Then we have

$$N_{supp(f)} = N_{supp(g_2)} - N_{G_n(\alpha_{n-1}^2)} - N_{G_n(\alpha_{4k+3}^2)} + N_{G_n(\alpha_1^2)} + N_{G_n(\alpha_{4k+1}^2)}.$$

Since $\deg(g_2) = 2$, then $N_{supp(g_2)} \equiv 0 \bmod 2$. It follows that

$$N_{supp(f_2)} \equiv N_{G_n(\alpha_{n-1}^2)} + N_{G_n(\alpha_{4k+3}^2)} + N_{G_n(\alpha_1^2)} + N_{G_n(\alpha_{4k+1}^2)}.$$

Note that $N_{G_n(\alpha)} = n - wt(\alpha)$ holds all $|G_n(\alpha)| = n$. Hence,

$$N_{supp(f)} \equiv n - 1 + 1 + 4k + 4k + 2 \equiv 1 \bmod 2.$$

Thus, the monomial $x_1x_2\cdots x_n/x_1$ appears in $f(x)$, then $deg(f) \geq n - 1$. As f is balanced, then $deg(f) = n - 1$. This completes the proof.

Although it is different to analyze the AI and FAI of f in (8) systematically, we can give some experiment results when n is small. Using Algorithm 1 of [1] implemented by Magma program, we can obtain the minimal degree of g such that $gf = 0$ and $(g + 1)f = 0$ by exhaustive search. We find that $AI(f) = (n-3)/2$ for $n = 11, 13$, and $AI(f) = (n-5)/2$ for $n = 15$. For $n = 2k + 1$, let $g_1, h_1 \in \mathfrak{B}_n$ with $deg(h_1) = e$ and $1 \leq deg(g_1) = d < k$ such that $fg_1 = h_1$. We need to obtain the minimal value of $d + e$ to analyze the FAI of f in (8). Using Algorithm 2 of [1], we can find that (e, d) exist only for $e + d \geq n - 4$ when $n = 11, 13$, and (e, d) exist for $e + d \geq n - 6$ when $n = 15$. Thus, $FAI(f) = n - 4$ for $n = 11, 13$, and $FAI(f) = n-6$ for $n = 15$. This shows that f in (8) has a good behavior against algebraic and fast algebraic attacks at least for small n.

B. RESILIENT RSBFs HAVING GOOD AUTOCORRELATION PROPERTIES

In this subsection, let n be odd with $n \equiv 0 \bmod 3$, and let $g(x) = \sum_{i=1}^{n} x_{i+1}x_{i+n/3}$. Define a vector $v \in \mathbb{Z}^{(n-1)/2}$ as

- $n = 12k + 3, k \geq 1$:

$$\begin{aligned}v = (&1, 4, \ldots, 12(k-1)+1, 12(k-1)+4, 2,\\ &5, \ldots, 12(k-1)+2, 12(k-1)+5, 3,\\ &6, \ldots, 12(k-1)+3, 12(k-1)+6, 12k+1);\end{aligned}$$

- $n = 12k + 9, k \geq 1$:

$$v = (1, 4, \ldots, 12(k-1)+1, 12(k-1)+4, 2, 5, \ldots, 12(k-1)+2, 12(k-1)+5, 3, 6, \ldots, 12(k-1)+3, 12(k-1)+6, 12k+1, 12k+4, 12k+2, 12k+5).$$

Denote by

$$R = \{\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_{n-1}\} \subseteq \mathbb{F}_2^n,$$

where

$$supp(\alpha_i) = \{v(j) : 1 \leq j \leq i\}, \alpha_{n-i} = \bar{\alpha}_i, 1 \leq i \leq \frac{n-1}{2}.$$

For $1 \leq i \leq n-1$ and $1 \leq j \leq n$, define

$$A_j(i) = \sum_{x \in G_n(\alpha_i)} (-1)^{g(x+e_j)+g(x)}, \tag{9}$$

where $\alpha_i \in R$, $e_j = (\underbrace{0, 0, \ldots, 0}_{j-1}, 1, 0, 0, \ldots, 0)$.

Similarly as Lemma 4, we can prove the following result.

Lemma 5: For $\alpha_i \in R$ and $A_j(i)$ defined in (9), we have

1) $wt(\alpha_i) = i$.
2) $|G_n(\alpha_i)| = n$.
3) *If $i \leq (n-1)/2$, then*

$$g(\alpha_i) = \begin{cases} 1, & i \bmod 4 \equiv 2, 3, \\ 0, & i \bmod 4 \equiv 0, 1; \end{cases}$$

and if $i \geq (n+1)/2$, then $g(\alpha_i) = 1 - g(\alpha_{n-i})$.

4) *If $n = 12k+3$, $A_j(i) = n - 4\min\{i, n-i\}$ for $i \leq 6k$, $A_j(6k+1) = 3 - 12k$.*
If $n = 12k+9$, $A_j(i) = n - 4\min\{i, n-i\}$ for $i \leq 6k$, $A_j(6k+1) = A_j(6k+2) = 5 - 12k$, $A_j(6k+3) = A_j(6k+4) = 1 - 12k$.

For $1 \leq m \leq \lceil n/16 \rceil$ and $1 \leq i_1, i_2, \ldots, i_{4m} \leq n-1$, let $I = \{i_1, i_2, \ldots, i_{4m}\}$ and $T_I = \{\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_{4m}}\} \subseteq R$. Let $U_I, n-I, D_I$ be defined as (5) and (6). Note that $g(\alpha_i) = 0$ if and only if $i \in U_I$.

Define

$$f_I(x) = \begin{cases} g(x), & x \in \mathbb{F}_2^n \backslash \widetilde{T}_I, \\ 1 + g(x), & x \in \widetilde{T}_I, \end{cases} \tag{10}$$

where $\widetilde{T}_I = \bigcup_{\alpha \in T_I} G_n(\alpha)$. Then f_I is an n-variable RSBF.

To investigate the properties of $f_I(x)$ in (10), we need the following result.

Lemma 6: [20] Assume $n = 3m$, where m is an integer. Then $g(x) = \sum_{i=1}^{n} x_{i+1}x_{i+m}$ is a $(m-1)$-resilient RSBF.

Theorem 3: The following properties hold for $f(x)$ defined in (10).

1) *If $\sum_{t=1}^{4m} A_j = mn$ and $|i_{t_1} - i_{t_2}| \geq 2$ holds for any $i_{t_1}, i_{t_2} \in I$, then f_I satisfies the strict avalanche criterion.*
2) *If $|U_I| = 2m$ and $\sum_{i \in U_I} i = \sum_{i \in (I \backslash U_I)} i$, then f_I is 1-resilient.*
3) $\Delta_{f_I} = 2^n - 4n(4m - D_I)$.
4) $\sigma_{f_I} < 2^{2n+1} + 2^{n+8}m^2n^2$.
5) *If $|D_I| \neq 4m$, f_I has no nonzero linear structures.*
6) $nl(f_I) > 2^{n-1} - 2^{\frac{n-1}{2}} - 4mn$.

Proof: 1), 3)∼6) can be proved similarly as Theorem 1, and next we only prove 2).

Denote $\widetilde{T}_1 = \bigcup_{i \in U_I} G_n(\alpha_i)$ and $\widetilde{T}_2 = \bigcup_{i \in (I \backslash U_I)} G_n(\alpha_i)$. Note that $\widetilde{T} = \widetilde{T}_1 \cup \widetilde{T}_2$ and $\widetilde{T}_1 \cap \widetilde{T}_2 = \varnothing$. Then $supp(f_I) = supp(g) \cup \widetilde{T}_2 \backslash \widetilde{T}_1$ and $|supp(f_I)| = |supp(g)| - |\widetilde{T}_1| + |\widetilde{T}_2|$. Clearly, we have $|\widetilde{T}_1| = n\sum_{i \in U_I} i$ and $|\widetilde{T}_2| = n\sum_{i \in (I \backslash U_I)} i$. Note that $|I| = 4m$. If $|U_I| = 2m$, then $|I \backslash U_I| = 2m$. It follow that $|\widetilde{T}_1| = |\widetilde{T}_2|$. By Lemma 6, $g(x)$ is resilient, then $|supp(g)| = 2^{n-1}$. Thus $|supp(f_I)| = 2^{n-1}$, that is, $f_I(x)$ is balanced. Assume that $\alpha = (1, 0, 0, \ldots, 0) \in \mathbb{F}_2^n$. Note that $wt(\alpha) = 1$.

$$\begin{aligned} W_f(\alpha) &= \sum_{x \in \mathbb{F}_2^n \backslash \widetilde{T}} (-1)^{f(x)+\alpha \cdot x} + \sum_{x \in \widetilde{T}} (-1)^{f(x)+\alpha \cdot x} \\ &= \sum_{x \in \mathbb{F}_2^n} (-1)^{g(x)+\alpha \cdot x} - 2\sum_{x \in \widetilde{T}} (-1)^{g(x)+\alpha \cdot x} \\ &= \sum_{x \in \mathbb{F}_2^n} (-1)^{g(x)+x_1} - 2\sum_{x \in \widetilde{T}} (-1)^{g(x)+x_1}. \end{aligned}$$

Since $g(x)$ is resilient, then $\sum_{x \in \mathbb{F}_2^n} (-1)^{g(x)+x_1} = 0$, it follows that

$$\begin{aligned} W_f(\alpha) &= -2\sum_{x \in \widetilde{T}} (-1)^{g(x)+x_1} \\ &= -2\sum_{x \in \widetilde{T}_1} (-1)^{x_1} + 2\sum_{x \in \widetilde{T}_2} (-1)^{x_1} \\ &= -2\sum_{i \in U_I} (n-2i) + 2\sum_{i \in (I \backslash U_I)} (n-2i) \\ &= 2n(|I| - 2|U_I|)) + 4\left(\sum_{i \in U_I} i - \sum_{i \in (I \backslash U_I)} i\right) \\ &= 0. \end{aligned}$$

Hence, $W_f(\alpha) = 0$ holds for any $wt(\alpha) = 1$. Thus, f_I is 1-resilient.

Theorem 4: Let $n \geq 33$ be an integer with $n \equiv 3 \bmod 6$. If $n \equiv 3 \bmod 24$, let

$$T = \{\alpha_1, \alpha_3, \alpha_5, \alpha_{\frac{n-18}{3}}, \alpha_{\frac{n+6}{3}}, \alpha_{\frac{n-9}{2}}, \alpha_{\frac{n+3}{2}}, \alpha_{\frac{2n-3}{3}}\};$$

if $n \equiv 9 \bmod 24$, let

$$T = \{\alpha_1, \alpha_3, \alpha_{\frac{n-7}{2}}, \alpha_{\frac{n-3}{2}}, \alpha_{\frac{n+5}{2}}, \alpha_{\frac{n+9}{2}}, \alpha_{n-8}, \alpha_{n-2}\};$$

if $n \equiv 15 \bmod 24$, let

$$T = \{\alpha_1, \alpha_3, \alpha_5, \alpha_{\frac{n-18}{3}}, \alpha_{\frac{n+6}{3}}, \alpha_{\frac{n-5}{2}}, \alpha_{\frac{n+7}{2}}, \alpha_{\frac{2n-3}{3}}\};$$

if $n \equiv 21 \bmod 24$, let

$$T = \{\alpha_1, \alpha_3, \alpha_{\frac{n-7}{2}}, \alpha_{\frac{n-3}{2}}, \alpha_{\frac{n+5}{2}}, \alpha_{\frac{n+9}{2}}, \alpha_{n-6}, \alpha_{n-4}\}.$$

Denote $\widetilde{T} = \bigcup_{\alpha\in T} G_n(\alpha)$ *and define an n-variable RSBF as*

$$f(x) = \begin{cases} g(x), & x \in \mathbb{F}_2^n \backslash \widetilde{T}, \\ 1 + g(x), & x \in \widetilde{T}. \end{cases} \tag{11}$$

Then $f(x)$ *has the following properties.*

1) f *satisfies SAC.*
2) f *is 1-resilient.*
3) $\Delta_f = 2^n - 32n$.
4) $\sigma_f \le 2^{2n+1} + 2^{n+10}n^2$.
5) $nl(f) \ge 2^{n-1} - 2^{\frac{n-1}{2}} - 8n$.
6) f *has no nonzero linear structures.*
7) $\deg(f) = n - 2$.

Proof: 1)∼6) can be verified easily according to Theorem 3. Now we only need to consider $deg(f)$. Denote c_2 the coefficient of $x_1x_2\cdots x_n/x_1x_2$ in the ANF of $f(x)$. Let S be a subset of $\mathbb{F}_2^n$, and denote $\mathcal{N}_S$ the number of vectors in the S with the 1-th entry and 2-th entry being 0. Obviously, $c_2 = \mathcal{N}_{supp(f)} \bmod 2$.

It is not difficult to find that

$$\mathcal{N}_{supp(f)} \equiv \mathcal{N}_{supp(g)} + \sum_{\alpha\in T} \mathcal{N}_{G_n(\alpha)} \bmod 2.$$

Since $\deg(g) = 2$, then $\mathcal{N}_{supp(g)} \equiv 0 \bmod 2$. It follows that

$$\mathcal{N}_{supp(f)} \equiv \sum_{\alpha\in T} \mathcal{N}_{G_n(\alpha)} \bmod 2.$$

When $n = 24k + 3$ for $k \ge 1$, we have

$$\begin{aligned} \mathcal{N}_{G_n(\alpha_1)} &= 24k + 1, \mathcal{N}_{G_n(\alpha_3)} = 24k - 4, \\ \mathcal{N}_{G_n(\alpha_5)} &= 24k - 8, \mathcal{N}_{G_n(\alpha_{8k-5})} = 12k - 8, \\ \mathcal{N}_{G_n(\alpha_{8k+3})} &= 12k - 7, \mathcal{N}_{G_n(\alpha_{12k-3})} = 10k - 4, \\ \mathcal{N}_{G_n(\alpha_{12k+3})} &= 10k, \mathcal{N}_{G_n(\alpha_{16k+1})} = 4k + 3. \end{aligned}$$

Hence, we have $\mathcal{N}_{supp(f)} \equiv 1 \bmod 2$, that is, $c_2 = 1$. Then $deg(f) \ge n - 2$. Furthermore, by Lemma 1 we have $deg(f) = n - 2$. Similarly, we also can prove that this holds for other cases.

IV. ENUMERATION OF ODD-VARIABLE RSBFs SATISFYING SAC

In this section, we investigate the lower bound on the number of odd-variable RSBFs satisfying SAC based on integer partition. Firstly, we recall some notions about integer partition. For three integers s, t and r, denote $L(r; t, s)$ the number of partitions of r satisfying the following conditions:

- $a_1 + a_2 + \cdots + a_t = r$
- $1 \le a_1, a_2, \cdots, a_t \le s$,

denote $M(r; t, s)$ the number of partitions of r satisfying the following conditions:

- $a_1 + a_2 + \cdots + a_t = r$
- $1 \le a_1 \le a_2 \le \cdots \le a_t \le s$,

and denote $N(r; t, s)$ the number of partitions of r satisfying the following conditions:

- $a_1 + a_2 + \cdots + a_t = r$
- $1 \le a_1 < a_2 < \cdots < a_t \le s$.

Theorem 5: Let $n \ge 13$ *be odd and* A_n *be the number of n-variable RSBFs satisfying SAC, then we have*

$$A_n \ge \frac{\phi(n)}{2} \sum_{m=1}^{\lceil n/16\rceil} \sum_{k=0}^{4m} \sum_{l=k^2}^{mn-(4m-k)^2} h(m, k, l),$$

where

$$h(m, k, l) = \prod_{r\in\{k,4m-k\}} \left(\sum_{u=0}^{r} M(g(r); r - u, \frac{n + 1 - 4r}{2}) \right)$$

with $g(k) = l - k^2$ *and* $g(4m - k) = mn - l - (4m - k)^2$.

Proof: For $2 \le s \le \frac{n+1}{2}$ with $\gcd(s - 1, n) = 1$ and $1 \le m \le \lceil n/16\rceil$, let $I = \{i_1, i_2, \ldots, i_{4m}\}$, $1 \le i_1, i_2, \ldots, i_{4m} \le n - 1$, and $f_{s,I}$ be defined in (7). Denote

$$\mathcal{I} = \{I : \sum_{t=1}^{4m} \min\{i_t, n - i_t\} = mn, |i_{t_1} - i_{t_2}| \ge 2\}.$$

Then $f_{s,I}$ satisfies SAC if $I \in \mathcal{I}$. Denote $\mathcal{F}_s = \{f_{s,I} : I \in \mathcal{I}\}$, that is, the set of $f_{s,I}$ satisfying SAC. Note that $\mathcal{F}_{s_1} \cap \mathcal{F}_{s_2} = \varnothing$ for $s_1 \ne s_2$. Since

$$|\{2 \le s \le \frac{n+1}{2} : \gcd(s, n) = 1\}| = \frac{\phi(n)}{2},$$

then $A_n \ge \frac{\phi(n)}{2}|\mathcal{I}|$.

Assume that $I \in \mathcal{I}$ and

$$1 \le i_1 < i_2 < \cdots < i_k \le \frac{n-1}{2} < i_{k+1} \cdots < i_{4m} \le n - 1,$$

$1 \le k \le 4m - 1$. Clearly, there exists a sequence $\Delta_1, \Delta_2, \ldots, \Delta_{4m}$ such that $i_j = (2j - 1) + \Delta_j$ for $1 \le j \le k$ and $n - i_j = 2(4m - j) + 1 + \Delta_j$ for $k + 1 \le j \le 4m$, where

$$\begin{aligned} &0 \le \Delta_1 \le \Delta_2 \le \cdots \le \Delta_k \le \frac{1 + n - 4k}{2}, \\ &0 \le \Delta_{4m} \le \Delta_{4m-1} \le \cdots \le \Delta_{k+1} \le \frac{1 + n - 4(4m - k)}{2}. \end{aligned} \tag{12}$$

For given m, k and $l = i_1 + i_2 + \cdots + i_k$, we now consider the possible values of Δ_j, $1 \le j \le 4m$. Note that

$$\begin{aligned} l &= k^2 + \Delta_1 + \Delta_2 + \cdots + \Delta_k, \\ mn - l &= (4m - k)^2 + \Delta_{k+1} + \Delta_{k+2} + \cdots + \Delta_{4m}. \end{aligned} \tag{13}$$

By (12) and (13), we have

$$k^2 \le l = \sum_{j=1}^{k} i_j \le mn - (4m - k)^2.$$

Hence, if $\Delta_1 = \cdots = \Delta_u = 0 < \Delta_{u+1} \le \cdots \le \Delta_k$, $0 \le u \le k$, the number of choices of $\Delta_1, \Delta_2, \ldots, \Delta_k$ is $M(l - k^2; k - u, \frac{n+1-4k}{2})$. Similarly, the number of choices of $\Delta_{k+1}, \Delta_{k+2}, \ldots, \Delta_{4m}$ is

$$M(mn - l - (4m - k)^2; 4m - k - u, \frac{n + 1 - 4(4m - k)}{2}),$$

where $0 \le u \le 4m-k$. Then, for given m, k and l, the total number of possible choices of $\Delta_1, \Delta_2, \ldots, \Delta_{4m}$ is

$$h(m,k,l) = \prod_{r\in\{k,4m-k\}} \left(\sum_{u=0}^{r} M(g(r); r-u, \frac{n+1-4r}{2}) \right),$$

where $g(k) = l - k^2$, $g(m-k) = mn - l - (4m-k)^2$. By considering the cases of $k = 0$ ($i_1, i_2, \ldots, i_{4m} > \frac{n-1}{2}$) and $k = 4m$ ($i_1, i_2, \ldots, i_{4m} \le \frac{n-1}{2}$), we have

$$|\mathcal{I}| = \sum_{m=1}^{\lceil n/16 \rceil} \sum_{k=0}^{4m} \sum_{l=k^2}^{mn-(4m-k)^2} h(m,k,l). \tag{14}$$

Then the result follows.

Theorem 6: Let B_n be the number of n-variable balanced RSBFs satisfying SAC for odd $n \ge 39$. If $n \equiv 1 \bmod 4$, then

$$B_n > 132\phi(n)N(\frac{n-13}{4}; 3, \lfloor\frac{n-9}{8}\rfloor) + 120\phi(n)N(\frac{n-13}{4}; 4, \lfloor\frac{n-9}{8}\rfloor).$$

If $n \equiv 3 \bmod 4$, then

$$B_n > 192\phi(n)N(\frac{n-11}{4}; 3, \lfloor\frac{n-9}{8}\rfloor) + 96\phi(n)N(\frac{n-11}{4}; 4, \lfloor\frac{n-9}{8}\rfloor).$$

Proof: For $2 \le s \le \frac{n+1}{2}$ with $\gcd(s-1, n) = 1$ and $1 \le m \le \lceil n/16 \rceil$, let $I = \{i_1, i_2, \ldots, i_{4m}\}$, $1 \le i_1, i_2, \ldots, i_{4m} \le n-1$, and $f_{s,I}$ be defined in (7). Denote $i'_t = \min\{i_t, n-i_t\}$, $1 \le t \le 4m$, and $M_I = \{i'_1, i'_2, \ldots, i'_{4m}\}$. Denote

$$\mathfrak{I} = \{I : \sum_{i'_t \in M_I} i'_t = mn, |i_{t_1} - i_{t_2}| \ge 2, |\{i_t \in I : i_t \bmod 4 \equiv 0, 1\}| = 2m\}$$

for $n \equiv 3 \bmod 4$, and denote

$$\mathfrak{I} = \{I : \sum_{i'_t \in M_I} i'_t = mn, |i_{t_1} - i_{t_2}| \ge 2, |\{i_t \in I : i_t < \frac{n+1}{2}, i_t \bmod 4 \equiv 0, 1\}| + |\{i_t \in I : i_t \ge \frac{n+1}{2}, i_t \bmod 4 \equiv 2, 3\}| = 2m\}$$

for $n \equiv 1 \bmod 4$. Note that $f_{s,I}$ is a balanced RSBF satisfying SAC if and only if $I \in \mathcal{I}$. Clearly, we have $B_n \ge \frac{\phi(n)}{2}|\mathfrak{I}|$. Next we set $m = 1$ and give an estimate of $|\mathfrak{I}|$ by considering the possible cases of M_I. When $n \equiv 3 \bmod 4$, if $f_{s,I}$ satisfies SAC, then M_I should be one of the following cases:

$$M_I = \{4k_1+1, 4k_2+1, 4k_3+2, 4k_4+3\},$$
$$M_I = \{4k_1+1, 4k_2+1, 4k_3+1, 4k_4+4\},$$
$$M_I = \{4k_1+1, 4k_2+2, 4k_3+2, 4k_4+2\},$$
$$M_I = \{4k_1+1, 4k_2+2, 4k_3+4, 4k_4+4\},$$
$$M_I = \{4k_1+2, 4k_2+2, 4k_3+3, 4k_4+4\},$$
$$M_I = \{4k_1+1, 4k_2+3, 4k_3+3, 4k_4+3\},$$
$$M_I = \{4k_1+2, 4k_2+3, 4k_3+3, 4k_4+3\},$$
$$M_I = \{4k_1+3, 4k_2+4, 4k_3+4, 4k_4+4\},$$

where $k_1, k_2, k_3, k_4 \ge 0$. And when considering the balancedness of $f_{s,I}$, M_I should be one of the following cases:

$$M_I = \{4k_1+1, 4k_2+1, 4k_3+2, 4k_4+3\},$$
$$M_I = \{4k_1+1, 4k_2+3, 4k_3+3, 4k_4+4\}.$$

For the case of $M_I = \{4k_1+1, 4k_2+1, 4k_3+2, 4k_4+3\}$, we have

$$4k_1+1+4k_2+1+4k_3+2+4k_4+3 = n,$$

that is, $k_1+k_2+k_3+k_4 = \frac{n-7}{4}$, where $k_1, k_2, k_3, k_4 \le \frac{n-7}{8}$. Now we consider the possible values of k_i by assuming that the values of k_i are different. The discussion is divide into the following cases.

- $k_1 = 0$. The number of k'_1, k'_2, k'_3 satisfying $0 < k'_1 < k'_2 < k'_3 \le \frac{n-7}{8}$ and $k'_1 + k'_2 + k'_3 = \frac{n-7}{4}$ is $N(\frac{n-7}{4}; 3, \lfloor\frac{n-7}{8}\rfloor)$. Considering the relationship of k_2, k_3, k_4, we have $|M_I| = 6N(\frac{n-7}{4}; 3, \lfloor\frac{n-7}{8}\rfloor)$. Hence, for given $i'_t \in M_I$, either $i_t < \frac{n}{2}$ or $i_t > \frac{n}{2}$. Thus, the number of $I \in \mathfrak{I}$ is
$$96N(\frac{n-7}{4}; 3, \lfloor\frac{n-7}{8}\rfloor).$$
- $k_3 = 0$ or $k_4 = 0$. The number of $I \in \mathfrak{I}$ is $48N(\frac{n-7}{4}; 3, \lfloor\frac{n-7}{8}\rfloor)$.
- $k_1, k_2, k_3, k_4 \ne 0$. The number of $I \in \mathfrak{I}$ is $96N(\frac{n-7}{4}; 4, \lfloor\frac{n-7}{8}\rfloor)$.

Thus, the number of $I \in \mathfrak{I}$ in this cases is

$$192N(\frac{n-7}{4}; 3, \lfloor\frac{n-7}{8}\rfloor) + 96N(\frac{n-7}{4}; 4, \lfloor\frac{n-7}{8}\rfloor).$$

For the cases of $M_I = \{4k_1+1, 4k_2+3, 4k_3+3, 4k_4+4\}$, we also can also deduce that the number of $I \in \mathfrak{I}$ is

$$192N(\frac{n-11}{4}; 3, \lfloor\frac{n-9}{8}\rfloor) + 96N(\frac{n-11}{4}; 4, \lfloor\frac{n-9}{8}\rfloor).$$

Therefore,

$$B_n > 192\phi(n)N(\frac{n-11}{4}; 3, \lfloor\frac{n-9}{8}\rfloor) + 96\phi(n)(\frac{n-11}{4}; 4, \lfloor\frac{n-9}{8}\rfloor).$$

When $n \equiv 1 \bmod 4$, we can similarly deduce that

$$B_n > 132\phi(n)N(\frac{n-15}{4}; 3, \lfloor\frac{n-9}{8}\rfloor) + 120\phi(n)N(\frac{n-15}{4}; 4, \lfloor\frac{n-9}{8}\rfloor).$$

This completes the proof.

Remark 1: Note that the bounds in Theorems 5 and 6 are stated by $N(r; t, s)$ and $M(r; t, s)$, which don't have concrete expressions yet. Fortunately, the formula of $L(r; t, s)$ has been presented in [4]:

$$L(r; t, s) = \sum_{j=0}^{t} (-1)^j \binom{t}{j} \binom{t+r-j(s+1)-1}{t-1}.$$

TABLE 1. The lower bounds on number of RSBFs satisfying SAC.

n	11	13	15	17	19	21	23
A_n	≥ 40	≥ 132	≥ 176	≥ 672	≥ 1413	≥ 2064	≥ 9460
B_n	≥ 20	≥ 60	≥ 64	≥ 240	≥ 621	≥ 870	≥ 3630

Based on $L(r;t,s)$, we can give an estimation of $M(r;t,s)$ and $N(r;t,s)$ as

$$\begin{aligned} &M'(r;t,s)\\ &=\frac{L(r;t,s)}{t!}\\ &=\sum_{j=0}^{t}(-1)^j\binom{t}{j}\binom{t+r-j(s+1)-1}{t-1}\Big/t!,\\ &N'(r;t,s)\\ &=\frac{L(r-\frac{t(t-1)}{2};t,s)}{t!}\\ &=\sum_{j=0}^{t}(-1)^j\binom{t}{j}\binom{t+r-\frac{t(t-1)}{2}-j(s+1)-1}{t-1}\Big/t!. \end{aligned}$$

Obviously, we have $M(r;t,s)\geq M'(r;t,s), N(r;t,s)\geq N'(r;t,s)$.

In Table 1, we present the lower bounds on the number of odd-variable RSBFs satisfying SAC (A_n) and the number of balanced odd-variable RSBFs satisfying SAC (B_n) for some n by considering all of the possible choices of $T_{s,I}$ in Theorem 1.

V. CONCLUSION

This paper presents a theoretical framework for constructing balanced odd-variable RSBFs satisfying SAC. Some of the obtained functions have good GAC properties, optimal algebraic degree, resiliency, high nonlinearity and nonexistence of nonzero linear structures at the same time. In addition, the count results about odd-variable RSBFs satisfying SAC are also considered.

REFERENCES

[1] F. Armknecht, C. Carlet, P. Gaborit, S. Kunzli, W. Meier, and O. Ruatta, "Efficient computation of algebraic immunity for algebraic and fast algebraic attack," in *Advances in Cryptology—EUROCRYPT 2006* (Lecture Notes in Computer Science), vol. 4004. Berlin, Germany: Springer, 2006, pp. 147–164.
[2] 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. Combinat. Theory A*, vol. 127, pp. 161–175, Sep. 2014.
[3] Y. Chen, F. Guo, and J. Ruan, "Constructing odd-variable RSBFs with optimal algebraic immunity, good nonlinearity and good behavior against fast algebraic attacks," *Discrete Appl. Math.*, vol. 262, pp. 1–12, Jun. 2019.
[4] R. P. Stanley, *Enumerative Combinatorics*, New York, NY, USA: Cambridge Univ. Press, 2011.
[5] N. Courtois, "Fast algebraic attacks on stream ciphers with linear feedback," in *Advances in Cryptology—CRYPTO 2003* (Lecture Notes in Computer Science), vol. 2719. Berlin, Germany: Springer, 2003, pp. 176–194.
[6] N. T. Courtois and W. Meier, "Algebraic attacks on stream ciphers with linear feedback," in *Advances in Cryptology—EUROCRYPT 2003* (Lecture Notes in Computer Science), vol. 2656. Berlin, Germany: Springer, 2003, pp. 345–359.
[7] 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, Sep. 2014.
[8] S. Fu, C. Li, K. Matsuura, and L. Qu, "Construction of even-variable rotation symmetric Boolean functions with maximum algebraic immunity," *Sci. China Inf. Sci.*, vol. 56, no. 3, pp. 1–9, Dec. 2011.
[9] G. Gao, X. Zhang, W. Liu, and C. Carlet, "Constructions of quadratic and cubic rotation symmetric bent functions," *IEEE Trans. Inf. Theory*, vol. 58, no. 7, pp. 4908–4913, Jul. 2012.
[10] S. Kavut, S. Maitra, and D. Tang, "Construction and search of balanced Boolean functions on even number of variables towards excellent autocorrelation profile," *Des., Codes Cryptogr.*, vol. 87, nos. 2–3, pp. 261–276, Jul. 2018.
[11] H. Kim, S.-M. Park, and S. G. Hahn, "On the weight and nonlinearity of homogeneous rotation symmetric Boolean functions of degree 2," *Discrete Appl. Math.*, vol. 157, no. 2, pp. 428–432, Jan. 2009.
[12] M. Liu, D. Lin, and D. Pei, "Fast algebraic attacks and decomposition of symmetric Boolean functions," *IEEE Trans. Inf. Theory*, vol. 57, no. 7, pp. 4817–4821, Jul. 2011.
[13] S. Mesnager, S. Su, and H. Zhang, "A construction method of balanced rotation symmetric Boolean functions on arbitrary even number of variables with optimal algebraic immunity," *Des., Codes Cryptogr.*, vol. 89, no. 1, pp. 1–17, Oct. 2020.
[14] S. Pang, X. Wang, J. Wang, J. Du, and M. Feng, "Construction and count of 1-resilient rotation symmetric Boolean functions," *Inf. Sci.*, vol. 450, pp. 336–342, Jun. 2018.
[15] T. Siegenthaler, "Correlation-immunity of nonlinear combining functions for cryptographic applications," *IEEE Trans. Inf. Theory*, vol. IT-30, no. 5, pp. 776–780, Sep. 1984.
[16] P. Stănică, "Nonlinearity, local and global avalanche characteristics of balanced Boolean functions," *Discrete Math.*, vol. 248, nos. 1–3, pp. 181–193, Apr. 2002.
[17] P. Stănică and S. Maitra, "Rotation symmetric Boolean functions—Count and cryptographic applications," *Discret. Appl. Math.*, vol. 156, no. 10, pp. 1567–1580, May 2008.
[18] P. Stănică and S. H. Sung, "Boolean functions with five controllable cryptographic properties," *Des., Codes Cryptogr.*, vol. 31, no. 2, pp. 147–157, Feb. 2004.
[19] 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*, vol. 63, no. 7, pp. 4658–4667, Jul. 2017.
[20] L. Sun, Z. Shi, and F. Fu, "Several classes of $2k$-variable 1-resilient rotation symmetric Boolean functions with high algebraic degree and nonlinearity," *Discrete Math.*, 2019.
[21] C. Tang, Z. Zhou, Y. Qi, X. Zhang, C. Fan, and T. Helleseth, "Generic construction of bent functions and bent idempotents with any possible algebraic degrees," *IEEE Trans. Inf. Theory*, vol. 63, no. 10, pp. 6149–6157, Oct. 2017.
[22] D. Tang, W. Zhang, and X. Tang, "Construction of balanced Boolean functions with high nonlinearity and good autocorrelation properties," *Des., Codes Cryptogr.*, vol. 67, no. 1, pp. 77–91, Apr. 2013.
[23] A. Webster and S. Tavares, "On the design of S-box," in *Advances in Cryptology—CRYPTO'85* (Lecture Notes in Computer Science), vol. 218. Berlin, Germany: Springer, 1986, pp. 523–524.
[24] G.-Z. Xiao and J. L. Massey, "A spectral characterization of correlation-immune combining functions," *IEEE Trans. Inf. Theory*, vol. IT-34, no. 3, pp. 569–571, May 1988.
[25] X. Zhang and Y. Zheng, "GAC—The criterion for global avalanche characteristics of cryptographic functions," *J. Univ. Comput. Sci*, vol. 1, no. 5, pp. 320–337, May 1995.

LEI SUN was born in Xuzhou, Jiangsu, China, in 1984. He received the B.S. degree in computer science from the Nanjing University of Posts and Telecommunications, in 2007, and the Ph.D. degree in mathematics from Nankai University, in 2017. He is currently a Lecturer with the Hebei University of Economics and Business, China. His research interests include cryptology and information security.

ZEXIA SHI was born in Shijiazhuang, Hebei, China, in 1991. She received the B.S. degree in mathematics from Hebei University, in 2013, and the Ph.D. degree in mathematics from Nankai University, in 2020. She is currently a Lecturer with Hebei Normal University, China. Her research interests include coding theory and cryptology.