IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 19, 2019, accepted August 12, 2019, date of publication September 5, 2019, date of current version September 26, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2939296

Constructing Higher Nonlinear Odd-Variable RSBFs With Optimal AI and Almost Optimal FAI

YINDONG CHEN[1,2,3], **LIMIN LIN**[1], **LUMIN LIAO**[1], **JIE RUAN**[1], **FEI GUO**[1,4], **AND WEIHONG CAI**[1,2,3]

[1]Department of Computer Science, Shantou University, Shantou 515063, China
[2]Guangdong Provincial Key Laboratory of Digital Signal and Image Processing Techniques, Shantou 515063, China
[3]Key Laboratory of Intelligent Manufacturing Technology (Shantou University), Ministry of Education, Shantou 515063, China
[4]School of Cyber Engineering, Xidian University, Xi'an 710071, China

Corresponding author: Yindong Chen (ydchen@stu.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61103244, Grant U1509213, Grant 61672303, and Grant 61702318, in part by the Science and Technology Planning Project of Guangdong Province under Grant 2016B010124012, Grant 2019B010116001, Grant 180917104960489, and Grant 190827105555406, in part by the Natural Science Foundation of Guangdong Province under Grant 2018A030313291, Grant 2018A030313438, and Grant 2018A030313889, in part by the Special Funds for Discipline and Specialty Construction of Guangdong Higher Education Institutions under Grant 2016KTSCX040, Grant 2016KQNCX056, Grant 2018KQNCX079, and Grant 2018GXJK048, in part by the STU Scientific Research Foundation for Talents under Grant NTF18006, Grant NTF18022, and Grant NTF18024, and in part by the National Training Program of Innovation and Entrepreneurship for Undergraduates under Grant 201910560015.

ABSTRACT Rotation symmetric Boolean functions (RSBFs) are nowadays studied a lot because of its easy operations and good performance in cryptosystem. This paper constructs a new class of odd-variable RSBFs with optimal algebraic immunity (AI). The nonlinearity of the new function, $2^{n-1}-\binom{n-1}{k}+2^{k-4}(k-3)(k-2)$, is the highest among all existing RSBFs with optimal AI and known nonlinearity, and its algebraic degree is also almost highest. Besides, the class of functions have almost optimal fast algebraic immunity (FAI) at least for $n < 17$, which is actually the highest possible value for the designated number of variables.

INDEX TERMS Rotation symmetric Boolean function, algebraic immunity, nonlinearity, algebraic degree, fast algebraic immunity.

I. INTRODUCTION

Boolean functions play an important role in cryptosystems of stream ciphers. They are required to satisfy kinds of cryptographic properties in order to resist many attacks. In 2003, the algebraic attack was proposed by Courtois and Meier in [1]. Then algebraic immunity (AI), a new cryptographic property, was introduced [2], [3]. Boolean functions should have high AI to resist algebraic attacks. The algebraic immunity of an n-variable Boolean function f can at highest be $\mathrm{AI}(f) = \lceil \frac{n}{2} \rceil$ [3], in which case we say that the function have optimal AI. Since a tiny difference of AI may change the resistance much, functions with optimal AI have been chased, and efforts are paid to find them and their properties [5]–[16]. Later, Courtois introduced fast algebraic attacks [4]. The fast algebraic attack is possible if a nonzero function g exists such that $\deg(g)$ and $\deg(g{\cdot}f)$ are low enough. In 2011, another new cryptographic property called fast algebraic immunity (FAI) was introduced in [17], which works as a measurement of the ability of Boolean functions to resist fast algebraic attacks. Some effort have been paid to study about FAI [18]–[20], but they are still under too much limitation.

Rotation symmetric Boolean functions (RSBFs) don't change under the action of cyclic group, and lots of them have optimal AI. Up to now, lots of functions with good properties, including optimal algebraic immunity, are RSBFs [21]–[37]. In 2007, Sarkar and Maitra [22] firstly constructed a class of odd-variable RSBFs with optimal AI and nonlinearity $2^{n-1} - \binom{n-1}{\frac{n-1}{2}} + 2$. In 2009, 2011 and 2013, [24], [26], [27] presented constructions of even-variable RSBFs with optimal AI, with their nonlinearity polynomial higher than $2^{n-1} - \binom{n-1}{\frac{n-1}{2}}$. In 2014, Su and Tang [31] made use of integer partition to present new kinds of RSBFs with optimal AI and first

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

exponentially higher nonlinearity, $2^{n-1}-\binom{n-1}{k}-2+2^k$ ($n=2k+1\geq 11$) and $2^{n-1}-\binom{n-1}{k}-2+3\cdot 2^{k-2}$ ($n=2k\geq 10$), both of which are later improved in [32]–[34]. However, the constructions of [31]–[33] totally ignore the fast algebraic attack. In 2017, Sun and Fu [35] presented two classes of even-variable RSBFs with optimal AI, high nonlinearity and high fast algebraic immunity. In 2019, Chen *et al.* [36] presented a class of odd-variable RSBFs with optimal AI and higher nonlinearity. These two classes of functions have almost optimal immunity for $n=11,13$ and $n=11,13,15$, respectively. In the same year, Zhang and Su [37] constructed another type of RSBFs, whose AI is optimal and nonlinearity equals to $2^{n-1}-\binom{n-1}{k}+(k-5)2^{k-1}+2k+2$ ($n=2k+1\geq 11$).

We here construct a new type of odd-variable RSBFs with the following properties: i) They are balanced with optimal AI. ii) Nonlinearity is the highest among all odd-variable RSBFs with exact known nonlinearity. iii) Algebraic degree reaches optimal upper bound of balanced Boolean functions, i.e., $n-1$. iv) The fast algebraic immunity reaches the highest possible value for the number of variables $n<17$.

In this paper, Section II provides some basic definitions and propositions, Section III constructs the odd-variable RSBFs and shows that the functions behave well on some aspects, and Section IV concludes this paper.

II. PRELIMINARIES

Let $\mathbb{F}_2^n$ be the n-dimensional vector space over the finite field $\mathbb{F}_2=\{0,1\}$. A Boolean function is a mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. We'll later use B_n to represent the set of the 2^{2^n} possible n-variable Boolean functions.

For a vector $x=(x_1,x_2,\cdots,x_n)\in\mathbb{F}_2^n$, supp$(x)$ is defined as $\{i|x_i=1, 1\leq i\leq n\}$, and wt$(x)$ is $|\text{supp}(x)|$. For any two vectors $\alpha=(\alpha_1,\alpha_2,\cdots,\alpha_n)$ and $u=(u_1,u_2,\cdots,u_n)$ in $\mathbb{F}_2^n$, we define $\alpha\preceq u$, if $\alpha_i\leq u_i$ for all $1\leq i\leq n$.

A quite usually used way to represent a Boolean function $f(x_1,x_2,\cdots,x_n)$ is the algebraic normal form (ANF), that is to say,

$$f(x_1,x_2,\cdots,x_n)=\bigoplus_{\alpha\in\mathbb{F}_2^n} c(\alpha)x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n}, \quad (1)$$

where $c(\alpha)\in\mathbb{F}_2$ and "$\oplus$" means the addition on $\mathbb{F}_2$. By the Möbius transform,

$$c(\alpha)=\bigoplus_{x\in\mathbb{F}_2^n, x\preceq\alpha} f(x). \quad (2)$$

Definition 1: The algebraic degree of function f expressed in format (1) is defined as

$$\deg(f)=\max\{\text{wt}(\alpha)|\alpha\in\mathbb{F}_2^n, c(\alpha)=1\}.$$

A_n represents the set containing all n-variable functions whose algebraic degree is at most one.

supp(f) is denoted by $\{x|f(x)=1, x\in\mathbb{F}_2^n\}$, and wt$(f)=|\text{supp}(f)|$. A Boolean function $f\in B_n$ is balanced if wt$(f)=$ wt$(f\oplus 1)$, or equally, its Hamming weight is 2^{n-1}.

Definition 2: The Walsh spectrum of a Boolean function $f\in B_n$ is defined as

$$W_f(\omega)=\sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)\oplus x\cdot\omega}, \quad \omega\in\mathbb{F}_2^n$$

where $(x_1,x_2,\cdots,x_n)\cdot(\omega_1,\omega_2,\cdots,\omega_n)=x_1\omega_1\oplus x_2\omega_2\oplus\cdots\oplus x_n\omega_n$.

Definition 3: The nonlinearity (NL) of a Boolean function f with n variables is defined as

$$\text{NL}(f)=\min_{g\in A_n}\text{wt}(f\oplus g).$$

or equally,

$$\text{NL}(f)=2^{n-1}-\frac{1}{2}\max_{\omega\in\mathbb{F}_2^n}|\text{W}_f(\omega)|. \quad (3)$$

Definition 4 [3]: The algebraic immunity of a Boolean function f, denoted by AI(f), *is*

$$\text{AI}(f)=\min\{\deg(g)|0\neq g\in B_n, f\cdot g=0 \text{ or } (f\oplus 1)\cdot g=0\}.$$

Functions without high AI will be easily attacked. But even for ones which having high AI, fast algebraic attacks is still possible if someone can find two nonzero functions g and h with low algebraic degree such that $f\cdot g=h$ [4], [38]. Fast algebraic immunity was later introduced as a measurement of the resistance of Boolean functions against fast algebraic attacks.

Definition 5 [17]: The fast algebraic immunity of a Boolean function f, denoted by FAI(f) *is defined as*

$$\text{FAI}(f)=\min\Big\{2\,\text{AI}(f), \min\{\deg(g)+\deg(f\cdot g)| 1\leq\deg(g)<\text{AI}(f)\}\Big\}.$$

We say that f has *almost optimal* fast algebraic immunity if FAI(f) is $n-1$. We won't get a balanced function with its FAI higher than n, and can only have n reached if $n=2^m+1$ for some integer m [39].

A simple function,

$$F(x)=\begin{cases}1, & \text{if wt}(x)\geq\lceil\frac{n}{2}\rceil;\\ 0, & \text{else,}\end{cases}$$

called the majority function [40], is showed to achieve the optimal AI in [6] by Dalai et al. Yet, NL$(F(x))$ is $2^{n-1}-\binom{n-1}{\lfloor\frac{n}{2}\rfloor}$, which is exactly Lobanov's lowerbound [41].

Proposition 1 [6], [22]: Let $F(x)$ be the n-variable majority function with $n=2k+1$. For $\omega\in\mathbb{F}_2^n$,

i) If wt$(\omega)=1$, *then* $\text{W}_F(\omega)=2\binom{n-1}{k}$;
ii) If wt$(\omega)=n$, *then* $\text{W}_F(\omega)=2(-1)^k\binom{n-1}{k}$;
iii) Otherwise, $|\text{W}_F(\omega)|\leq 2\left(\binom{n-3}{k-1}-\binom{n-3}{k}\right)$ *for* $n\geq 7$.

Definition 6 [23]: Let $x=(x_1,x_2,\cdots,x_n)\in\mathbb{F}_2^n$, then for any x and $0\leq h<n$, $\rho_n^h(x)$ is defined as

$$\rho_n^h(x_1,x_2,\cdots,x_n)=(x_{h+1},x_{h+2},\cdots,x_n,x_1,x_2,\cdots,x_h).$$

Definition 7 [23]: A Boolean function $f \in B_n$ satisfying that $f\left(\rho_n^k(x)\right) = f(x)$ holds for all $x \in \mathbb{F}_2^n$ and $0 \le k < n$ is called rotation symmetric Boolean function (RSBF).

Since $f\left(\rho_n^k(x)\right)$ and $f(x)$ are always equal, we can separate $\mathbb{F}_2^n$ into several orbits such that, x and y are in same orbit if there exists some k, $y = \rho_n^k(x)$.

III. CONSTRUCTION OF ODD-VARIABLE RSBFS

In this paper, we'll assume that $n = 2k+1 \ge 11$, construct a kind of balanced RSBF on n variables, and prove that $f(x)$ has optimal AI, high nonlinearity, almost optimal algebraic degree, then check that it has almost optimal FAI.

A. CONSTRUCTION

For convenience, we denote by $W_{\le i} = \{\alpha \in \mathbb{F}_2^n | \operatorname{wt}(\alpha) \le i\}$ and $W_i = \{\alpha \in \mathbb{F}_2^n | \operatorname{wt}(\alpha) = i\}$. For $1 \le i \le k-2$ and $2 \le j \le i$, we define:

$$T_{i,j} = \Big\{(1,1,\underbrace{1,\cdots,1}_{i-j},0,\underbrace{1,\cdots,1}_{j-1},1,1,\underbrace{0,\cdots,0}_{k_1},1,\underbrace{0,\cdots,0}_{k_2},1,\cdots,\underbrace{0,\cdots,0}_{k_{k-i-1}}) \in W_{k+1}\Big| k_1,k_2,\cdots,k_{k-i-1} \ge 1\Big\}.$$

It is quite obvious that $k_1 + k_2 + \cdots + k_{k-i-1} = k-1$, as by definition $\operatorname{wt}(\alpha) = k+1$ for all $\alpha \in T_{i,j}$. Therefore,

$$T = \bigcup_{i=2}^{k-2}\bigcup_{j=2}^{i} T_{i,j} \subseteq W_{k+1}.$$

We write the vectors defined in T as

$$\begin{aligned}T = \Big\{&\alpha_{2,2,1},\alpha_{2,2,2},\cdots,\alpha_{2,2,|T_{2,2}|},\\ &\alpha_{3,2,1},\alpha_{3,2,2},\cdots,\alpha_{3,2,|T_{3,2}|},\\ &\alpha_{3,3,1},\alpha_{3,3,2},\cdots,\alpha_{3,3,|T_{3,3}|},\\ &\cdots,\\ &\alpha_{k-2,2,1},\alpha_{k-2,2,2},\cdots,\alpha_{k-2,2,|T_{k-2,2}|},\\ &\alpha_{k-2,3,1},\alpha_{k-2,3,2},\cdots,\alpha_{k-2,3,|T_{k-2,3}|},\\ &\cdots,\\ &\alpha_{k-2,k-2,1},\alpha_{k-2,k-2,2},\cdots,\alpha_{k-2,k-2,|T_{k-2,k-2}|}\Big\},\end{aligned}$$

where $\alpha_{i,j,s}$ means the sth smallest vector according to the lexicographic order in $T_{i,j}$.

We can find $u_{i,j,s}$ for each $\alpha_{i,j,s}$ as

$$\begin{aligned}U_{i,j} = \Big\{&u_{i,j,s} = \alpha_{i,j,s} \oplus (\underbrace{0,\cdots,0}_{i-j+3},\underbrace{1,\cdots,1}_{j-1},\underbrace{0,\cdots,0}_{2k-1-i})\Big|\alpha_{i,j,s} \in T_{i,j}\Big\}\\ &\subseteq W_{k-j+2}\end{aligned}$$

and similarly

$$\begin{aligned}U = \bigcup_{i=2}^{k-2}\bigcup_{j=2}^{i} U_{i,j} = \Big\{&u_{2,2,1},u_{2,2,2},\cdots,u_{2,2,|U_{2,1}|},\\ &u_{3,2,1},u_{3,2,2},\cdots,u_{3,2,|U_{3,2}|},\\ &u_{3,3,1},u_{3,3,2},\cdots,u_{3,3,|U_{3,3}|},\\ &\cdots,\\ &u_{k-2,2,1},u_{k-2,2,2},\cdots,u_{k-2,2,|T_{k-2,2}|},\\ &u_{k-2,3,1},u_{k-2,3,2},\cdots,u_{k-2,3,|T_{k-2,3}|},\\ &\cdots,\\ &u_{k-2,k-2,1},u_{k-2,k-2,2},\cdots,u_{k-2,k-2,|T_{k-2,k-2}|}\Big\},\end{aligned}$$

which is a subset of $W_{\le k}$. It's a direct result that $\left|T_{i,j}\right| = \left|U_{i,j}\right|$ for every possible i and j, and $|T| = |U|$.

Example 1: For $k = 5$, i.e., $n = 11$, we have

$$\begin{aligned}T_{2,2} &= \{(1,1,0,1,1,1,0,0,0,1,0),\\ &\quad (1,1,0,1,1,1,0,0,1,0,0),\\ &\quad (1,1,0,1,1,1,0,1,0,0,0)\},\\ T_{3,2} &= \{(1,1,1,0,1,1,1,0,0,0,0)\},\\ T_{3,3} &= \{(1,1,0,1,1,1,1,0,0,0,0)\},\end{aligned}$$

and

$$\begin{aligned}U_{2,2} &= \{(1,1,0,0,1,1,0,0,0,1,0),\\ &\quad (1,1,0,0,1,1,0,0,1,0,0),\\ &\quad (1,1,0,0,1,1,0,1,0,0,0)\},\\ U_{3,2} &= \{(1,1,1,0,0,1,1,0,0,0,0)\},\\ U_{3,3} &= \{(1,1,0,0,0,1,1,0,0,0,0)\}.\end{aligned}$$

Example 2: For $k = 6$, i.e., $n = 13$, we have

$$\begin{aligned}T_{2,2} &= \{(1,1,0,1,1,1,0,0,0,1,0,1,0),\\ &\quad (1,1,0,1,1,1,0,0,1,0,0,1,0),\\ &\quad (1,1,0,1,1,1,0,0,1,0,1,0,0),\\ &\quad (1,1,0,1,1,1,0,1,0,0,0,1,0),\\ &\quad (1,1,0,1,1,1,0,1,0,0,1,0,0),\\ &\quad (1,1,0,1,1,1,0,1,0,1,0,0,0)\},\\ T_{3,2} &= \{(1,1,1,0,1,1,1,0,0,0,0,1,0),\\ &\quad (1,1,1,0,1,1,1,0,0,0,1,0,0),\\ &\quad (1,1,1,0,1,1,1,0,0,1,0,0,0),\\ &\quad (1,1,1,0,1,1,1,0,1,0,0,0,0)\},\\ T_{3,3} &= \{(1,1,0,1,1,1,1,0,0,0,0,1,0),\\ &\quad (1,1,0,1,1,1,1,0,0,0,1,0,0),\\ &\quad (1,1,0,1,1,1,1,0,0,1,0,0,0),\\ &\quad (1,1,0,1,1,1,1,0,1,0,0,0,0)\},\\ T_{4,2} &= \{(1,1,1,1,0,1,1,1,0,0,0,0,0)\},\\ T_{4,3} &= \{(1,1,1,0,1,1,1,1,0,0,0,0,0)\},\\ T_{4,4} &= \{(1,1,0,1,1,1,1,1,0,0,0,0,0)\}.\end{aligned}$$

We can see that, when k increases from 5 to 6, the amount of vectors is more than tripled.

Now, define

$$\tilde{P} = \left\{\rho_n^l(x)\middle|x \in P, 0 \le l < n\right\}$$

for P being any subset of $\mathbb{F}_2^n$, and we can have:

Construction 1: Let $F(x)$ as the majority function, then

$$f(x) = \begin{cases} F(x) \oplus 1, & x \in \tilde{T} \cup \tilde{U}; \\ F(x), & \text{otherwise.} \end{cases} \quad (4)$$

Obviously f is a balanced RSBF.

B. ALGEBRAIC IMMUNITY

Define "$(x_1, x_2, x_3, \cdots, x_h) < (y_1, y_2, y_3, \cdots, y_h)$" as "$x_1 < y_1$ or $x_1 = y_1$ and $(x_2, x_3, \cdots, x_h) < (y_2, y_3, \cdots, y_h)$", and that $() \not< ()$, then we have:

Lemma 1: For $\alpha_{i,j,s} \in T$, $u_{i,j,s}, u_{i',j',s'} \in U$, the following properties hold.

i) $\rho_n^l(u_{i,j,s}) \preceq \rho_n^l(\alpha_{i,j,s})$, *for* $0 \le l < n$.
ii) $\rho_n^l(\alpha_{i,j,s}) \neq \alpha_{i,j,s}$, $\rho_n^l(u_{i,j,s}) \neq u_{i,j,s}$, *for* $1 \le l < n$.
iii) $u_{i,j,s} \npreceq \rho_n^l(\alpha_{i,j,s})$, *for* $1 \le l < n$.
iv) $u_{i',j',s'} \npreceq \rho_n^l(\alpha_{i,j,s})$, *for* $(i',j',s') < (i,j,s)$ *and* $0 \le l < n$.

Proof: For convenience, we write

$$\alpha_{i,j,s} = (1, 1, \underbrace{1, \cdots, 1}_{i-j}, 0, \underbrace{1, \cdots, 1}_{j-1}, 1, 1, \underbrace{0, \cdots, 0}_{k_1}, 1, \underbrace{0, \cdots, 0}_{k_2}, 1, \cdots, \underbrace{0, \cdots, 0}_{k_{k-i-1}})$$

and

$$u_{i,j,s} = (1, 1, \underbrace{1, \cdots, 1}_{i-j}, 0, \underbrace{0, \cdots, 0}_{j-1}, 1, 1, \underbrace{0, \cdots, 0}_{k_1}, 1, \underbrace{0, \cdots, 0}_{k_2}, 1, \cdots, \underbrace{0, \cdots, 0}_{k_{k-i-1}}).$$

Here, we define $(x_1, x_2, \cdots, x_n)_p^q$ as $(x_p, x_{p+1}, \cdots, x_q)$.

i) holds by the definitions of $T_{i,j}$ and $U_{i,j}$.

If $1 \le l < n$, then $(u_{i,j,s})_0^1 = (u_{i,j,s})_{3+i}^{4+i} = (1, 1)$, but the existances of $(1, 1)$ only appear in the range of the bits. Therefore, $u_{i,j,s} \npreceq \rho_n^l(\alpha_{i,j,s})$ for $1 \le l < n$, and then ii) and iii) hold.

If $i' < i$, and $u_{i',j',s'} \preceq \rho_n^l(\alpha_{i,j,s})$, by the necessarity of existance of the two $(1, 1)$'s we know $u_{i',j',s'} \oplus (\underbrace{0, \cdots, 0}_{i-j+2}, \underbrace{1, \cdots, 1}_{j}, \underbrace{0, \cdots, 0}_{2k-1-i}) \preceq \alpha_{i,j,s} \oplus (\underbrace{0, \cdots, 0}_{i-j+2}, 1, \underbrace{0, \cdots, 0}_{2k-i+j-2})$. Since the two vectors have same weight, they should be equal, which is obviously impossible.

If $i' = i$ then we use the same method when proving ii) and iii) and get that $l = 0$. In this case, if $j' < j$, then $(u_{i',j',s'})_{j+2}^{j+2} > (\alpha_{i,j,s})_{j+2}^{j+2}$; otherwise, they use different partitions, so $u_{i',j',s'} \npreceq \rho_n^l(\alpha_{i,j,s})$, still. This completes the proof of iv). ■

Lemma 2 [8]: Define $F(x)$ as the majority function. Let $T = \{\alpha_1, \cdots, \alpha_l\} \subseteq W^{\le k}$ and $U = \{u_1, \cdots, u_l\} \subseteq W^{k+1}$, for some integer l. If the vectors in T and U satisfy

$$P1. \quad \alpha_i \preceq u_i \quad \text{for } 1 \le i \le l,$$

and

$$P2. \quad \alpha_i \npreceq u_j \quad \text{for } 1 \le i < j \le l,$$

then

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

has optimal AI.

Theorem 1: The Boolean function $f(x)$ in Construction 1 has optimal AI.

Proof: Since $\rho_n^l(u_{i,j,s}) \preceq \rho_n^l(\alpha_{i,j,s})$ for $0 \le l < n$, $\rho_n^l(u_{i,j,s}) \npreceq \rho_n^m(\alpha_{i,j,s})$ for $0 \le l, m < n$ and $m \neq n$, and that $\rho_n^l(u_{i',j',s'}) \npreceq \rho_n^m(\alpha_{i,j,s})$ for $(i',j',s') < (i,j,s)$ according to Lemma 1, we can renumber the elements $\rho_n^l(\alpha_{i,j,s})$ in $\tilde{T}$ in order of (i, j, s, l), and the same operation can apply on $\tilde{U}$. In this way the conditions in Lemma 2 satisfy, and the proof is completed. ■

C. NONLINEARITY

Theorem 2: The nonlinearity of $f(x)$ in (4) is

$$\mathrm{NL}(f) = 2^{n-1} - \binom{n-1}{k} + 2^{k-4}(k-3)(k-2),$$

where $n = 2k + 1 \ge 11$.

Proof: For $\omega \in \mathbb{F}_2^n$, we'll first calculate the maximum of Walsh transform on ω.

Case 1: If $\mathrm{wt}(\omega) = 1$, then

$$\begin{aligned} &\sum_{x \in \tilde{T}} \Big((-1)^{f(x) \oplus \omega \cdot x} - (-1)^{F(x) \oplus \omega \cdot x}\Big) \\ &= \sum_{x \in T} \Big(-\mathrm{wt}(x) - \big(n - \mathrm{wt}(x)\big)\Big) - \Big(\mathrm{wt}(x) - \big(n - \mathrm{wt}(x)\big)\Big) \\ &= \sum_{x \in T} \big(2n - 4\,\mathrm{wt}(x)\big) \end{aligned}$$

and

$$\begin{aligned} &\sum_{x \in \tilde{U}} \Big((-1)^{f(x) \oplus \omega \cdot x} - (-1)^{F(x) \oplus \omega \cdot x}\Big) \\ &= \sum_{x \in U} \Big(\mathrm{wt}(x) - \big(n - \mathrm{wt}(x)\big)\Big) - \Big(-\mathrm{wt}(x) + \big(n - \mathrm{wt}(x)\big)\Big) \\ &= \sum_{x \in U} \big(-2n + 4\,\mathrm{wt}(x)\big). \end{aligned}$$

Therefore,

$$\begin{aligned} W_f(\omega) &= W_F(\omega) + \sum_{x \in \tilde{T}} \Big((-1)^{f(x) \oplus \omega \cdot x} - (-1)^{F(x) \oplus \omega \cdot x}\Big) \\ &\quad + \sum_{x \in \tilde{U}} \Big((-1)^{f(x) \oplus \omega \cdot x} - (-1)^{F(x) \oplus \omega \cdot x}\Big) \\ &= 2\binom{n-1}{k} + 4 \sum_{\{(i,j,s) \mid \alpha_{i,j,s} \in T\}} \big(-\mathrm{wt}(\alpha_{i,j,s}) + \mathrm{wt}(u_{i,j,s})\big) \\ &= 2\binom{n-1}{k} - 4 \sum_{i=2}^{k-2} \sum_{j=1}^{i-1} (j-1) \binom{k-2}{k-i-2} \\ &= 2\binom{n-1}{k} - 2^{k-3}(k-3)(k-2). \end{aligned}$$

Case 2: If $\mathrm{wt}(\omega) = n$, then

$$\sum_{x\in\tilde{T}}\left((-1)^{f(x)\oplus\omega\cdot x} - (-1)^{F(x)\oplus\omega\cdot x}\right) = \sum_{x\in T} n(-1)^{f(x)+\mathrm{wt}(x)} - n(-1)^{F(x)+\mathrm{wt}(x)} = \sum_{x\in T} 2n(-1)^{\mathrm{wt}(x)}$$

and

$$\sum_{x\in\tilde{U}}\left((-1)^{f(x)\oplus\omega\cdot x} - (-1)^{F(x)\oplus\omega\cdot x}\right) = \sum_{x\in U} n(-1)^{f(x)+\mathrm{wt}(x)} - n(-1)^{F(x)+\mathrm{wt}(x)} = \sum_{x\in U} -2n(-1)^{\mathrm{wt}(x)}.$$

Thus,

$$\begin{aligned} W_f(\omega) &= 2(-1)^k\binom{n-1}{k} + \sum_{x\in T} 2n(-1)^{\mathrm{wt}(x)} + \sum_{x\in U} 2n(-1)^{\mathrm{wt}(x)} \\ &= 2(-1)^k\binom{n-1}{k} + 2n\sum_{i,j,s}\left((-1)^{\mathrm{wt}(\alpha_{i,j,s})} - (-1)^{\mathrm{wt}(u_{i,j,s})}\right) \\ &= 2(-1)^k\binom{n-1}{k} - 4(-1)^k n\sum_{i=2}^{k-2}\sum_{t=1}^{\lfloor\frac{i-1}{2}\rfloor}\binom{k-2}{k-i-2}. \end{aligned}$$

Since

$$n\sum_{i=2}^{k-2}\sum_{t=1}^{\lfloor\frac{i-1}{2}\rfloor}\binom{k-2}{k-i-2} > \sum_{i=2}^{k-2}\sum_{j=1}^{i-1}(j-1)\binom{k-2}{k-i-2}$$

as

$$\sum_{t=1}^{\lfloor\frac{i-1}{2}\rfloor}\binom{k-2}{k-i-2} \le \frac{1}{2}\sum_{j=1}^{i-1}\binom{k-2}{k-i-2}$$

and $2(j-1) < n$, and

$$4n\sum_{i=2}^{k-2}\sum_{t=1}^{\lfloor\frac{i-1}{2}\rfloor}\binom{k-2}{k-i-2} < 2\binom{n-1}{k},$$

the absolute of $W_f(\omega)$ is obviously larger when $\omega = 1$ than $\omega = n$.

Case 3: If $2 \le \mathrm{wt}(\omega) < n$, then $|W_f(\omega)| \le 2(\binom{n-3}{k-1} - \binom{n-3}{k}) + 4n|T|$, which is also smaller than the Walsh when $\omega = 1$.

Hence, the maximum absolute of Walsh transform appears when $\mathrm{wt}(\omega) = 1$, in which case we can know from (3) that the nonlinearity of f is $2^{n-1} - \binom{n-1}{k} + 2^{k-4}(k-3)(k-2)$. ■

TABLE 1. Comparisons of nonlinearities among the odd-variable RSBFs.

n	$F(x)$	Construction in [31]	Construction in [37][1]	$f(x)$ in (4)
11	772	802	784	784
13	3172	3234	3218	3218
15	12952	13078	13096	13110
17	52666	52920	53068	53146
19	213524	214034	214568	214866
21	863820	864842	866402	867402
23	3488872	3490918	3495040	3498086
25	14073060	14077154	14087422	14096098

1. The value is calculated according to the given nonlinearity formula.

D. ALGEBRAIC DEGREE

Lemma 3 [6]: For the n-variable majority function F,

$$\deg(F) = 2^{\lfloor\log_2 n\rfloor}.$$

Lemma 4: Let f be the function defined in (4), and F be the majority function, then

$$\deg(f\oplus F) < n-1.$$

Proof: Let's define $\eta_{n-1} = (\underbrace{1,\cdots,1}_{n-1},0)$. Since f is balanced, by (2), $\deg(f) < n$; Because of the rotated symmetrical of f, $\deg(f\oplus F) = n-1$ iff $\bigoplus_{t\preceq\eta_{n-1}} f(t)$, which has same parity to $\sum_{x\in T\cup U}(n-\mathrm{wt}(x))$, and same to $\frac{1}{4}W_f(1,\underbrace{0,\cdots,0}_{n-1})$. Since it's always even, $\deg(f\oplus F) < n-1$. ■

Theorem 3: For Boolean function $f(x)$ defined in (4), if $k = 2^m$, then $\deg(f) = n-1$, and vise versa.

Proof: Since $\deg(f\oplus F) < n-1$, we know that $\deg(f) = n-1$ iff $\deg(F) = n-1$. By Lemma 4, it only happens when $n = 2^{m+1}+1$, i.e., $k = 2^m$. ■

Therefore, in most situations, $\deg(f\oplus F) < n-1$. The exception happens when $k = 2^m$ for some integer m. That's quite small amount.

To improve the degree, we define:

Construction 2:

$$f'(x) = \begin{cases} f(x)\oplus 1, & \text{if } \rho_n^l(x) \in \{\alpha_{k-2,2,1}, u_{k-2,2,1}\}; \\ f(x), & \text{else.} \end{cases}$$

Because it inverts $\bigoplus_{t\preceq\eta_{n-1}} f(t)$, with the same methods used before, we can get:

Theorem 4: For function f' defined in Construction 2, where $k \ne 2^m$, f' has optimal AI, $\deg(f') = n-1$, and $\mathrm{NL}(f') = 2^{n-1} - \binom{n-1}{k} + 2^{k-4}(k-3)(k-2) - 2.$

E. FAST ATTACK IMMUNITY

Currently exact FAI is still only available for majority function on some special n [18], [19], and for our function, we're only able to analyze for small n. With the computer program in [42] we can get that, for odd $n < 17$, $\mathrm{FAI}(f') = \mathrm{FAI}(f) = n-1$. As proved in [39], this is the highest possible value for RSBFs with optimal AI.

IV. CONCLUSION

In this paper, we construct a new type of balanced odd-variable RSBFs with optimal AI, and show the exact value of nonlinearity of our construction, which is higher than the known ones before. And such functions also have highest possible algebraic degree. In addition, for odd $n < 17$, the function has almost optimal FAI. However, the value of FAI for higher n still need some work, which is a significant open research area.

REFERENCES

[1] N. T. Courtois and W. Meier, "Algebraic attacks on stream ciphers with linear feedback," in *Advances in Cryptology—EUROCRYPT*, vol. 2656. Berlin, Germany: Springer-Verlag, 2003, pp. 345–359.

[2] D. K. Dalai, K. C. Gupta, and S. Maitra, "Results on algebraic immunity for cryptographically significant Boolean functions," in *Progress in Cryptology—INDOCRYPT*, vol. 3348. Berlin, Germany: Springer, 2004, pp. 92–106.

[3] W. Meier, E. Pasalic, and C. Carlet, "Algebraic attacks and decomposition of Boolean functions," in *Advances in Cryptology—EUROCRYPT*, vol. 3027. Berlin, Germany: Springer, 2004, pp. 474–491.

[4] N. T. Courtois, "Fast algebraic attacks on stream ciphers with linear feedback," in *Advances in Cryptology—CRYPTO*, Berlin, Germany: Springer, 2003, pp. 176–194.

[5] C. Carlet, D. K. Dalai, K. C. Gupta, and S. Maitra, "Algebraic immunity for cryptographically significant Boolean functions: Analysis and construction," *IEEE Trans. Inf. Theory*, vol. 52, no. 7, pp. 3105–3121, Jul. 2006.

[6] D. K. Dalai, S. Maitra, and S. Sarkar, "Basic theory in construction of Boolean functions with maximum possible annihilator immunity," *Des., Codes Cryptogr.*, vol. 40, no. 1, pp. 41–58, 2006.

[7] C. Carlet and K. Q. Feng, "An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity," in *Advances in Cryptology—ASIACRYPT*, vol. 5350. Berlin, Germany: Springer-Verlag, 2008, pp. 425–440.

[8] C. Carlet, X. Zeng, C. Li, and L. Hu, "Further properties of several classes of Boolean functions with optimum algebraic immunity," *Des., Codes Cryptogr.*, vol. 52, no. 3, pp. 303–338, 2009.

[9] L. Qu, K. Feng, F. Liu, and L. Wang, "Constructing symmetric Boolean functions with maximum algebraic immunity," *IEEE Trans. Inf. Theory*, vol. 55, no. 5, pp. 2406–2412, May 2009.

[10] Z. Tu and Y. Deng, "A conjecture about binary strings and its applications on constructing Boolean functions with optimal algebraic immunity," *Des., Codes Cryptogr.*, vol. 60, no. 1, pp. 1–14, 2011.

[11] Y. Chen and P. Lu, "Two classes of symmetric Boolean functions with optimum algebraic immunity: Construction and analysis," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 2522–2538, Apr. 2011.

[12] K. Huang, C. Li, and S. J. Fu, "Note on the Tu-Deng conjecture," *Comput. Sci.*, vol. 39, no. 6A, pp. 6–9, 2012.

[13] D. Tang, C. Carlet, and X. Tang, "Highly nonlinear Boolean functions with optimal algebraic immunity and good behavior against fast algebraic attacks," *IEEE Trans. Inf. Theory*, vol. 59, no. 1, pp. 653–664, Jan. 2013.

[14] J. Li, C. Carlet, X. Zeng, C. Li, L. Hu, and J. Shan, "Two constructions of balanced Boolean functions with optimal algebraic immunity, high nonlinearity and good behavior against fast algebraic attacks," *Des., Codes Cryptogr.*, vol. 76, no. 2, pp. 279–305, Aug. 2015.

[15] Y. Chen, F. Guo, Z. Gong, and W. Cai, "One note about the Tu-Deng conjecture in case $w(t) = 5$," *IEEE Access*, vol. 7, pp. 13799–13802, 2019.

[16] Y. Chen, L. Zhang, D. Tang, and W. Cai, "Translation equivalence of Boolean functions expressed by primitive element," *IEICE Trans. Fundam. Electron., Commun. Comput. Sci.*, vol. E102-A, no. 4, pp. 672–675, 2019.

[17] 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.

[18] D. Tang, R. Luo, and X. Du, "The exact fast algebraic immunity of two subclasses of the majority function," *IEICE Trans. Fundam. Electron., Commun. Comput. Sci.*, vol. E99-A, no. 11, pp. 2084–2088, Nov. 2016.

[19] Y. Chen, L. Zhang, F. Guo, and W. Cai, "Fast algebraic immunity of $2^m + 2$ & $2^m + 3$ variables majority function," *IEEE Access*, vol. 7, pp. 80733–80736, 2019.

[20] Y. Chen, L. Zhang, J. Xu, and W. Cai, "A lower bound of fast algebraic immunity of a class of 1-resilient Boolean functions," *IEEE Access*, vol. 7, pp. 90145–90151, 2019.

[21] P. Stănică, S. Maitra, and J. A. Clark, "Results on rotation symmetric bent and correlation immune Boolean functions," in *Fast Software Encryption*, vol. 3017. Berlin, Germany: Springer, 2014, pp. 161–177.

[22] S. Sarkar and S. Maitra, "Construction of rotation symmetric Boolean functions with maximun algebraic immunity on odd number of variables," in *AAECC*, vol. 4851. Heidelberg, Germany: Springer, 2007, pp. 271–280.

[23] P. Stănică and S. Maitra, "Rotation symmetric Boolean functions—Count and cryptographic properties," *Discrete Appl. Math.*, vol. 156, no. 10, pp. 1567–1580, May 2008.

[24] S. Sarkar and S. Maitra, "Construction of rotation symmetric Boolean functions with optimal algebraic immunity," *Comput. Syst.*, vol. 12, no. 3, pp. 267–284, 2009.

[25] S. Fu, C. Li, K. Matsuura, and L. Qu, "Construction of rotation symmetric Boolean functions with maximum algebraic immunity," in *Proc. Int. Conf. Cryptol. Netw. Secur.*, vol. 5888, 2009, pp. 402–412.

[26] S. Fu, L. Qu, C. Li, and B. Sun, "Balanced rotation symmetric Boolean functions with maximum algebraic immunity," *IET Inf. Secur.*, vol. 5, no. 2, pp. 93–99, 2011.

[27] 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, Mar. 2013.

[28] P. Zhang, D. Dong, S. Fu, and C. Li, "New constructions of even-variable rotation symmetric Boolean functions with maximum algebraic immunity," *Math. Comput. Model.*, vol. 55, nos. 3–4, pp. 828–836, Feb. 2012.

[29] J. Du, Q. Wen, J. Zhang, and S. Pang, "Construction and counting of 1-resilient rotation symmetric Boolean functions on *pq* variables," *IEICE Trans. Fundam. Electron., Commun. Comput. Sci.*, vol. E96-A, no. 7, pp. 1653–1656, 2013.

[30] J. Du, S. Pang, Q. Wen, and X. Liao, "Construction and count of 1-resilient rotation symmetric Boolean functions on pr variables," *Chin. J. Electron.*, vol. 23, no. 4, pp. 816–820, 2014.

[31] S. Su and X. Tang, "Construction of rotation symmetric Boolean functions with optimal algebraic immunity and high nonlinearity," *Des., Codes Cryptogr.*, vol. 71, no. 2, pp. 183–199, 2014.

[32] Y. Chen, Y. Zhang, and W. Tian, "Construction of even-variable rotation symmetric Boolean functions with optimal algebraic immunity," (in Chinese), *J. Cryptol. Res.*, vol. 1, no. 5, pp. 437–448, 2014.

[33] 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.*, vol. E99-A, no. 4, pp. 853–855, 2016.

[34] Y. Chen, F. Guo, H. Xiang, W. Cai, and X. He, "Balanced odd-variable RSBFs with optimum AI, high nonlinearity and good behavior against FAAs," *IEICE Trans. Fundam. Electron., Commun. Comput. Sci.*, vol. E102-A, no. 6, pp. 818–824, 2019.

[35] L. Sun and F.-W. Fu, "Constructions of even-variable RSBFs with optimal algebraic immunity and high nonlinearity," *J. Appl. Math. Comput.*, vol. 56, nos. 1–2, pp. 593–610, Feb. 2018.

[36] 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.

[37] H. Zhang and S. Su, "A new construction of rotation symmetric Boolean functions with optimal algebraic immunity and higher nonlinearity," *Discrete Appl. Math.*, vol. 262, pp. 13–28, Jun. 2019.

[38] P. Hawkes and G. G. Rose, "Rewriting variables: The complexity of fast algebraic attacks on stream ciphers," in *Advances in Cryptology—CRYPTO*. Berlin, Germany: Springer, 2004, pp. 390–406.

[39] Y. Du and F. Zhang, "On the existence of Boolean functions with optimal resistance against fast algebraic attacks," Cryptol. ePrint Arch., Tech. Rep. 2012/210, 2012. [Online]. Available: https://eprint.iacr.org/2012/210

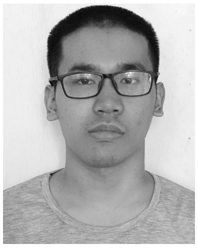
[40] C. Ding, G. Xiao, and W. Shan, *The Stability Theory of Stream Ciphers* (Lecture Notes in Computer Science), vol. 561. Berlin, Germany: Springer, 1991.

[41] M. Lobanov. (2005). *Tight Bound Between Nonlinearity and Algebraic Immunity*. [Online]. Available: http://eprint.iacr.org/2005/441

[42] S. Fischer. *FAA Equation Finder Version 1*. Accessed: Aug. 8, 2018. [Online]. Available: http://www.simonfischer.ch/software/FAA.php

YINDONG CHEN was born in Jieyang, Guangdong, China, in 1983. He received the B.S. degree in mathematics from the South China University of Technology, in 2005, and the Ph.D. degree in computer science from Fudan University, in 2010. He is currently an Associate Professor with Shantou University, China. His research interests include cryptology and information security.

JIE RUAN was born in Chaozhou, Guangdong, China, in 1998. She is currently pursuing the bachelor's degree with Shantou University, China. Her research interests include cryptology and information security.



LIMIN LIN was born in Jieyang, Guangdong, China, in 1997. He received the B.S. degree in mathematics from South China Normal University, in 2018. He is currently pursuing the master's degree with Shantou University, China. His research interests include cryptology and information security.

FEI GUO was born in Fuyang, Anhui, China, in 1993. He received the B.S. degree from Anhui University, in 2016, and the master's degree from Shantou University, in 2019, all in computer science. He is currently pursuing the Ph.D. degree with Xidian University, China. His research interests include cryptology and information security.

LUMIN LIAO was born in Ganzhou, Jiangxi, China, in 1997. She received the B.S. degree in mathematics from East China Jiaotong University, in 2018. She is currently pursuing the master's degree with Shantou University, China. Her research interests include cryptology and information security.

WEIHONG CAI was born in Chaozhou, Guangdong, China, in 1963. He received the Ph.D. degree in computer science from the South China University of Technology, in 2012. He is currently a Professor with Shantou University, China. His research interests include network and communications, and information security.