LETTER

Construction of Odd-Variable Strictly Almost Optimal Resilient Boolean Functions with Higher Resiliency Order via Modifying High-Meets-Low Technique*

Hui GE[†,††a)], **Zepeng ZHUO**[†††,††††], ***Nonmembers, and*** **Xiaoni DU**[†††††], ***Member***

SUMMARY Construction of resilient Boolean functions in odd variables having strictly almost optimal (SAO) nonlinearity appears to be a rather difficult task in stream cipher and coding theory. In this paper, based on the modified High-Meets-Low technique, a general construction to obtain odd-variable SAO resilient Boolean functions without directly using PW functions or KY functions is presented. It is shown that the new class of functions possess higher resiliency order than the known functions while keeping higher SAO nonlinearity, and in addition the resiliency order increases rapidly with the variable number n.

key words: *Boolean functions, cryptography, nonlinearity, resiliency, stream ciphers*

1. Introduction

Boolean functions are critical designing blocks used in cryptography, in particular in block and stream ciphers. An important prerequisite on these cryptographic functions is a higher resistance to the linear and (fast) correlation cryptanalyses, which are measured by nonlinearity and resiliency of functions, respectively. In other words, high nonlinearity and high order of resiliency are two of the most important criteria of Boolean functions when they are used in nonlinear combiner or nonlinear filter models of stream cipher systems. More precisely, the nonlinearity measures the minimum distance between a given Boolean function and the set of affine functions, it reflects the ability of the cipher to withstand various modes of linear attacks [1]. Resiliency ensures the cipher is not prone to (fast) correlation attacks [2], [3]. Based on their wide applications in cryptography and coding theory, construction of resilient functions with as high nonlinearity as possible has been extensively studied from the mid 1980s, see for instance Refs. [5]–[7], [10], [12].

When n is even, there have been extensive research efforts towards efficient methods for obtaining SAO resilient functions [13]–[16], [18]. For odd n, the toughest challenge is to get resilient functions having SAO nonlinearity. Unfortunately, the progress on constructing SAO resilient functions in odd number of variables has been considerably slow. In [8] and [9], some superior methods and algorithms for constructing SAO 1-resilient functions in odd variables $n \geq 41$ were proposed. In 2008, the technique of modifying a PW function to construct 1-resilient functions on 15-variables with SAO nonlinearity 16264 was first demonstrated in [4]. In 2014, Zhang and Pasalic [17] presented a generalized Maiorana-McFarland (G-M-M) construction method to obtain odd-variable SAO resilient functions. Recently, the "High-Meets-Low" construction technique via fragmentary Walsh transform to obtain odd-variable resilient functions with currently best known nonlinearity was proposed by Zhang [19], and it is shown that the nonlinearity of the constructed functions can reach $2^{n-1} - 2^{(n-1)/2} + 5 \cdot 2^{(n-11)/2}$ or $2^{n-1} - 2^{(n-1)/2} + 2^{(n-7)/2}$.

In this paper, without directly using PW functions or KY functions, we introduce a modified "High-Meets-Low" construction technique for designing odd-variable resilient functions with SAO nonlinearity. Compared to the best known design methods in [19], it is shown that we can construct odd-variable resilient functions with higher resiliency order, while keeping the same nonlinearity $2^{n-1}-2^{(n-1)/2}+2^{(n-7)/2}$ when using 21-variable 1-resilient functions (generated by the KY case in [19]). It is worth mentioning that the restricted relationship between resiliency and nonlinearity can achieve the best possible improvement through the constructed resilient functions.

2. Preliminaries

Let $\mathbb{F}_2 = \{0, 1\}$ and $\mathbb{F}_2^n$ be the vector space of all n-tuples over $\mathbb{F}_2$. A Boolean function of n variables may be viewed as a mapping from $\mathbb{F}_2^n$ into $\mathbb{F}_2$ and we denote by $\mathcal{B}_n$ the set of all the Boolean functions in n variables. A Boolean function $f(X) \in \mathcal{B}_n$ is commonly represented as a multivariate polynomial over $\mathbb{F}_2$, called Algebraic normal form (ANF), in the form:

Manuscript received April 10, 2022.
Manuscript revised June 22, 2022.
Manuscript publicized July 12, 2022.

[†]The author is with School of Computer Science and Technology, Huaibei Normal University, Huaibei 235000, China.
[††]The author is with the State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China.
[†††]The author is with School of Mathematical Science, Huaibei Normal University, Huaibei 235000, China.
[††††]The author is with School of Cyber Science, University of Science and Technology of China, Hefei 230027, China.
[†††††]The author is College of Mathematics and Statistics, Northwest Normal University, Lanzhou, 730070, China.

[*]This research was supported by the Natural Science Foundation of Anhui Higher Education Institutions of China (No.KJ2020A0034, No.KJ2020ZD008).

a) E-mail: gehui_tyf@163.com

DOI: 10.1587/transfun.2022EAL2031

$$f(X) = \bigoplus_{u \in \mathbb{F}_2^n} a_u \left(\prod_{j=1}^{n} x_j^{u_j}\right), \tag{1}$$

where $a_u \in \mathbb{F}_2$, $u = (u_1, \ldots, u_n)$. The algebraic degree of f, denoted by $\deg(f)$, corresponds to the maximum value of $wt(u)$ such that $a_u \neq 0$. Functions of degree at most one are called affine functions.

Definition 1: For any $\alpha = (\alpha_1, \ldots, \alpha_n)$, $X = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$, let $\alpha \cdot X = \alpha_1 \cdot x_1 + \alpha_2 \cdot x_2 + \cdots + \alpha_n \cdot x_n$ be the inner (dot) product of α and X. The Walsh transform of $f \in \mathcal{B}_n$ in point α is denoted by $W_f(\alpha)$ and calculated as

$$W_f(\alpha) = \sum_{X \in \mathbb{F}_2^n} (-1)^{f(X)+\alpha \cdot X}. \tag{2}$$

A function $f \in \mathcal{B}_n$ is said to be balanced if the number of ones is equal to the number of zeros in the truth table of f (i.e., $W_f(\mathbf{0}) = 0$). In terms of Walsh spectra, the nonlinearity of a Boolean function f is given by Ref. [11].

Definition 2: The nonlinearity of a Boolean function $f \in \mathcal{B}_n$ can be defined as

$$N_f = 2^{n-1} - \frac{1}{2} \max_{\alpha \in \mathbb{F}_2^n} |W_f(\alpha)|. \tag{3}$$

The upper bound on nonlinearity is limited by well-known Parseval's equation

$$\sum_{\alpha \in \mathbb{F}_2^n} (W_f(\alpha))^2 = 2^{2n}, \tag{4}$$

which then implies that $N_f \leq 2^{n-1} - 2^{n/2-1}$.

Definition 3: [17] An n-variable Boolean function is called strictly almost optimal (SAO) if its nonlinearity is strictly greater than $2^{n-1} - 2^{\lfloor n/2 \rfloor}$.

In Ref. [21], a convenient spectral characterization of resilient Boolean functions has been presented, which we use as a lemma here.

Lemma 1: [21] A Boolean function $f \in \mathcal{B}_n$ is t-resilient if and only if its Walsh transform satisfies

$$W_f(\alpha) = 0, \quad \text{for all } \alpha \in \mathbb{F}_2^n \text{ such that } 0 \leq wt(\alpha) \leq t. \tag{5}$$

Next, we introduce the notion of the fragmentary Walsh transform of an n-variable fragmentary Boolean function in [19].

Definition 4: Let S be a nonempty proper subset of $\mathbb{F}_2^n$. A function $f_S : S \to \mathbb{F}_2$ is called an n-variable fragmentary Boolean function on S. The fragmentary Walsh transform of f_S at point $\omega \in \mathbb{F}_2^n$, is an integer valued function over S defined by

$$FW_{f_S}(\omega) = \sum_{X \in S} (-1)^{f_S(X)+\omega \cdot X}. \tag{6}$$

Lemma 2: [19] For $i = 1, 2, \ldots, d$, let S_i be a nonempty subset of $\mathbb{F}_2^n$ so that $\bigcup_{i=1}^{d} S_i = \mathbb{F}_2^n$ and $S_1, S_2, \ldots, S_d$ are mutually disjoint, i.e., for all $i, j = 1, 2, \ldots, d$,

$$S_i \cap S_j = \emptyset, \; 1 \leq i < j \leq d. \tag{7}$$

Let $f \in \mathcal{B}_n$, and

$$f_{S_i}(X) = f(X), \; for \; X \in S_i, i = 1, 2, \ldots, d. \tag{8}$$

Then we have

$$W_f(\omega) = \sum_{i=1}^{d} FW_{f_{S_i}}(\omega) \tag{9}$$

and

$$|W_f(\omega)| \leq \sum_{i=1}^{d} |FW_{f_{S_i}}(\omega)|. \tag{10}$$

3. The Main Construction Method

In this section, based on a modification of High-Meets-Low technique, we will give a new construction of odd-variable resilient Boolean functions with higher resiliency order and SAO nonlinearity.

Let $g \in \mathcal{B}_{21}$ be a 1-resilient boolean function, generated by the KY case in [19], and the truth table of g can be found in [20]. The spectral distribution of g is given by:

$$W_g(\beta) = \begin{cases} 0, & \beta \in U_1, \; \#U_1 = 130816, \\ \pm 256, & \beta \in U_2, \; \#U_2 = 83904, \\ \pm 512, & \beta \in U_3, \; \#U_3 = 64512, \\ \pm 768, & \beta \in U_4, \; \#U_4 = 317376, \\ \pm 1024, & \beta \in U_5, \; \#U_5 = 34048, \\ \pm 1280, & \beta \in U_6, \; \#U_6 = 353856, \\ \pm 1792, & \beta \in U_7, \; \#U_7 = 1112640, \end{cases} \tag{11}$$

where $U_1 \cup U_2 \cup U_3 \cup U_4 \cup U_5 \cup U_6 \cup U_7 = \mathbb{F}_2^{21}$ and $U_i \cap U_j = \emptyset$ for any $1 \leq i < j \leq 7$.

Construction 1: Let $n \geq 43$ be an odd number and $t \geq 0$. Let $k = (n-21)/2$. Let

$$T_1 = \{\eta \mid wt(\eta) \geq t - 1, \; \eta \in \mathbb{F}_2^k\}.$$

For $i = 1, 2, \ldots, 6$, let

$$\Gamma_i(v, t) = \begin{cases} \{(\delta, \beta) \mid wt(\delta, \beta) \geq t + 1, \delta \in \mathbb{F}_2^v, \beta \in U_i\}, & \text{if } v \geq 0 \\ \emptyset, & \text{if } v < 0. \end{cases} \tag{12}$$

Let

$$T_2 = \Gamma_1(k-11,t) \cup \Gamma_2(k-11,t) \cup \Gamma_3(k-11,t) \cup \Gamma_4(k-11,t),$$
$$T_3 = \Gamma_1(k-12,t) \cup \Gamma_2(k-12,t) \cup \Gamma_5(k-12,t) \cup \Gamma_6(k-12,t),$$

and

$$T_4 = \Gamma_1(k-13,t) \cup \Gamma_3(k-13,t) \cup \Gamma_5(k-13,t),$$

where

Table 1 $N_i(\tau)$ for 1-resilient function $g \in \mathcal{B}_{21}$ in [19].

τ	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
$N_1(\tau)$	1	21	174	781	2337	5422	10596	17512	23672	25424	21317
$N_2(\tau)$	0	0	0	0	7	100	539	2106	5434	10591	15084
$N_3(\tau)$	0	0	16	230	1311	4196	8707	12705	13759	11429	7311
$N_4(\tau)$	0	0	0	0	139	1459	6512	18437	36371	53528	61607
$N_5(\tau)$	0	0	5	74	447	1575	3720	6248	7614	6762	4405
$N_6(\tau)$	0	0	0	0	37	432	2539	8942	21677	39031	54943
τ	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**
$N_1(\tau)$	13756	6708	2401	597	91	6	0	0	0	0	0
$N_2(\tau)$	16585	14295	10097	5519	2463	856	200	26	2	0	0
$N_3(\tau)$	3477	1134	219	18	0	0	0	0	0	0	0
$N_4(\tau)$	56425	41273	24420	11516	4250	1181	233	25	0	0	0
$N_5(\tau)$	2150	803	215	30	0	0	0	0	0	0	0
$N_6(\tau)$	62907	59814	47122	30596	16125	6778	2230	562	106	14	1

- $\#\Gamma_i(v,t) = 2^v \cdot \#U_i - \sum_{j=0}^{\min\{t,21\}}(N_i(j) \cdot \sum_{e=0}^{\min\{v,t-j\}} \binom{v}{e})$;
- $N_i(\tau) = \#\{\beta \mid wt(\beta) = \tau,\ \beta \in U_i\}$ and its values $N_i(\tau)$ for 1-resilient function $g \in \mathcal{B}_{21}$ is given in Table 1, satisfying at the same time

$$2^{k+21}\#T_1 + 2^{k+10}\#T_2 + 2^{k+9}\#T_3 + 2^{k+8}\#T_4 \geq 2^n. \quad (13)$$

Set $d = 4$. Let $S_1 = E_1 \times \mathbb{F}_2^{k+21}$, $S_2 = E_2 \times \mathbb{F}_2^{k+10}$, $S_3 = E_3 \times \mathbb{F}_2^{k+9}$ and $S_4 = E_4 \times \mathbb{F}_2^{k+8}$ be nonempty proper subsets of $\mathbb{F}_2^n$, where $E_1 \subset \mathbb{F}_2^k$, $E_2 \subset \mathbb{F}_2^{k+11}$, $E_3 \subset \mathbb{F}_2^{k+12}$, $E_4 \subset \mathbb{F}_2^{k+13}$. In view of (13), it ensures that there exist E_i, $i = 1,2,3,4$, such that

$$\#E_i \leq \#T_i,\ 1 \leq i \leq 4 \quad (14)$$

$$\bigcup_{i=1}^{4} S_i = \mathbb{F}_2^n$$

and

$$S_i \cap S_j = \emptyset,\ 1 \leq i < j \leq 4.$$

By (14), it is easy to build four injective mappings as follows:

$$\phi_i : E_i \longrightarrow T_i,\ i = 1,2,3,4. \quad (15)$$

Let $(X,Y) \in \mathbb{F}_2^n$ with $X = (x_1,\ldots,x_{2k}) \in \mathbb{F}_2^{2k}$ and $Y \in \mathbb{F}_2^{21}$. Then, we can construct fragmentary Boolean functions f_{S_i} on S_i, $i = 1,2,3,4$, as follows:

$$f_{S_1}(X,Y) = \phi_1(X_{(1,k)}) \cdot X_{(k+1,2k)} + g(Y),$$
$$f_{S_2}(X,Y) = \phi_2(X_{(1,k+11)}) \cdot (X_{(k+12,2k)},Y),$$
$$f_{S_3}(X,Y) = \phi_3(X_{(1,k+12)}) \cdot (X_{(k+13,2k)},Y),$$
$$f_{S_4}(X,Y) = \phi_4(X_{(1,k+13)}) \cdot (X_{(k+14,2k)},Y).$$

Therorem 1: The function $f \in \mathcal{B}_n$ proposed by Construction 1 is a t-resilient function with nonlinearity

$$N_f = 2^{n-1} - 2^{(n-1)/2} + 2^{(n-7)/2}.$$

Proof. Let $\alpha = (\alpha_1,\ldots,\alpha_{2k}) \in \mathbb{F}_2^{2k}$ and $\beta \in \mathbb{F}_2^{21}$. We first calculate the fragmentary Walsh spectra of f_{S_1}.

$$\begin{aligned}
&FW_{f_{S_1}}(\alpha,\beta)\\
&= \sum_{X_{(1,k)}\in E_1} \sum_{X_{(k+1,2k)}\in\mathbb{F}_2^k} \sum_{Y\in\mathbb{F}_2^{21}} (-1)^{f_{S_1}(X,Y)+(\alpha,\beta)\cdot(X,Y)}\\
&= W_g(\beta) \sum_{X_{(1,k)}\in E_1} (-1)^{\alpha_{(1,k)}\cdot X_{(1,k)}}\\
&\quad \sum_{X_{(k+1,2k)}\in\mathbb{F}_2^k} (-1)^{[\phi_1(X_{(1,k)})+\alpha_{(k+1,2k)}]\cdot X_{(k+1,2k)}}\\
&= \begin{cases} 0, & \alpha_{(k+1,2k)} \notin T_1 \ \ or \ \ \beta \in U_1,\\ \pm 2^k \cdot W_g(\beta), & \alpha_{(k+1,2k)} \in T_1,\ \beta \in U_i,\ 2 \leq i \leq 7. \end{cases}
\end{aligned} \quad (16)$$

That is,

$$FW_{f_{S_1}}(\alpha,\beta) = \begin{cases} \pm 256 \cdot 2^k, & \beta \in U_2 \text{ and } \phi_1^{-1}(\alpha_{(k+1,2k)}) \text{ exists},\\ \pm 512 \cdot 2^k, & \beta \in U_3 \text{ and } \phi_1^{-1}(\alpha_{(k+1,2k)}) \text{ exists},\\ \pm 768 \cdot 2^k, & \beta \in U_4 \text{ and } \phi_1^{-1}(\alpha_{(k+1,2k)}) \text{ exists},\\ \pm 1024 \cdot 2^k, & \beta \in U_5 \text{ and } \phi_1^{-1}(\alpha_{(k+1,2k)}) \text{ exists},\\ \pm 1280 \cdot 2^k, & \beta \in U_6 \text{ and } \phi_1^{-1}(\alpha_{(k+1,2k)}) \text{ exists},\\ \pm 1792 \cdot 2^k, & \beta \in U_7 \text{ and } \phi_1^{-1}(\alpha_{(k+1,2k)}) \text{ exists},\\ 0, & \text{otherwise}. \end{cases} \quad (17)$$

For $0 \leq wt(\alpha,\beta) \leq t-2$, we have $\alpha_{(k+1,2k)} \notin T_1$, which implies

$$FW_{f_{S_1}}(\alpha,\beta) = 0, \quad for\ 0 \leq wt(\alpha,\beta) \leq t-2. \quad (18)$$

When $t-1 \leq wt(\alpha,\beta) \leq t$, we have $0 \leq wt(\alpha), wt(\beta) \leq t$. It can be classified into the following three cases.

Case 1 $0 \leq wt(\alpha) \leq t-2$. Obviously, $\alpha_{(k+1,2k)} \notin T_1$, and then by (16), we have $FW_{f_{S_1}}(\alpha,\beta) = 0$.

Case 2 $wt(\alpha) = t-1$. For any $wt(\alpha) = t-1$, we have $0 \leq wt(\beta) \leq 1$. Since $g \in \mathcal{B}_{21}$ is a 1-resilient boolean function, it gives $W_g(\beta) = 0$, which implies $FW_{f_{S_1}}(\alpha,\beta) = 0$.

Case 3 $wt(\alpha) = t$. Similarly, we can easily deduce that $FW_{f_{S_1}}(\alpha,\beta) = 0$.

In view of Cases 1-3 and (18), it is clear that

Table 2 Comparison of resiliency order with [19] for KY case.

n	231	269	273	311	315	319	353	357	361	365	369
t (Ours)	49	58	59	68	69	70	78	79	80	81	82
t ([19])	48	57	58	67	68	69	77	78	79	80	81
n	403	407	411	415	419	423	427	449	453	457	461
t (Ours)	90	91	92	93	94	95	96	101	102	103	104
t ([19])	89	90	91	92	93	94	95	100	101	102	103

$$FW_{f_{S_1}}(\alpha,\beta) = 0, \;\; for\ 0 \leq wt(\alpha,\beta) \leq t. \tag{19}$$

Now we calculate the fragmentary Walsh spectra of f_{S_2}.

$$\begin{aligned} & FW_{f_{S_2}}(\alpha,\beta) \\ = & \sum_{X_{(1,k+11)}\in E_2} \sum_{(X_{(k+12,2k)},Y)\in\mathbb{F}_2^{k+10}} (-1)^{f_{S_2}(X,Y)+(\alpha,\beta)\cdot(X,Y)} \\ = & \sum_{X_{(1,k+11)}\in E_2} (-1)^{\alpha_{(1,k+11)}\cdot X_{(1,k+11)}} \\ & \sum_{(X_{(k+12,2k)},Y)\in\mathbb{F}_2^{k+10}} (-1)^{[\phi_2(X_{(1,k+11)})+(\alpha_{(k+12,2k)},\beta)]\cdot(X_{(k+12,2k)},Y)} \\ = & \begin{cases} \pm 2^{k+10}, & (\alpha_{(k+12,2k)},\beta) \in T_2, \\ 0, & (\alpha_{(k+12,2k)},\beta) \notin T_2. \end{cases} \end{aligned} \tag{20}$$

That is,

$$FW_{f_{S_2}}(\alpha,\beta) = \begin{cases} \pm 2^{k+10}, & \beta \in U_1 \cup U_2 \cup U_3 \cup U_4 \text{ and } \phi_2^{-1}(\alpha_{(k+12,2k)},\beta) \text{ exists}, \\ 0, & \text{otherwise}. \end{cases} \tag{21}$$

When $0 \leq wt(\alpha,\beta) \leq t$, we have $(\alpha_{(k+12,2k)},\beta) \notin T_2$, which implies

$$FW_{f_{S_2}}(\alpha,\beta) = 0, \;\; for\ 0 \leq wt(\alpha,\beta) \leq t. \tag{22}$$

By the similar calculations, we can obtain

$$FW_{f_{S_3}}(\alpha,\beta) = \begin{cases} \pm 2^{k+9}, & \beta \in U_1 \cup U_2 \cup U_5 \cup U_6 \text{ and } \phi_3^{-1}(\alpha_{(k+13,2k)},\beta) \text{ exists}, \\ 0, & \text{otherwise}. \end{cases} \tag{23}$$

$$FW_{f_{S_4}}(\alpha,\beta) = \begin{cases} \pm 2^{k+8}, & \beta \in U_1 \cup U_3 \cup U_5 \text{ and } \phi_4^{-1}(\alpha_{(k+14,2k)},\beta) \text{ exists}, \\ 0, & \text{otherwise}. \end{cases} \tag{24}$$

From the discussion above, for $i = 1,2,3,4$, according to the definitions of T_i, we have

$$FW_{f_{S_i}}(\alpha,\beta) = 0, \;\; for\ 0 \leq wt(\alpha,\beta) \leq t, \tag{25}$$

which implies that f is t-resilient. By (10),

$$\begin{aligned} |W_f(\alpha,\beta)| \leq & \sum_{i=1}^{4} |FW_{f_{S_i}}(\alpha,\beta)| \\ \leq & \begin{cases} 2^{k+10} + 2^{k+9} + 2^{k+8}, & \beta \in U_1, \\ 256 \cdot 2^k + 2^{k+10} + 2^{k+9}, & \beta \in U_2, \\ 512 \cdot 2^k + 2^{k+10} + 2^{k+8}, & \beta \in U_3, \\ 768 \cdot 2^k + 2^{k+10}, & \beta \in U_4, \\ 1024 \cdot 2^k + 2^{k+9} + 2^{k+8}, & \beta \in U_5, \\ 1280 \cdot 2^k + 2^{k+9}, & \beta \in U_6, \\ 1792 \cdot 2^k, & \beta \in U_7, \end{cases} \end{aligned}$$

which leads to

$$\max_{(\alpha,\beta)\in\mathbb{F}_2^{2k+21}} |W_f(\alpha)| = 1792 \cdot 2^k.$$

It then follows that

$$N_f = 2^{n-1} - 2^{(n-1)/2} + 2^{(n-7)/2}.$$

Example 1: When $n = 231$ with $k = 105$, let $t = 49$. Based on the data $N_i(\tau)$ for 1-resilient functions $g \in \mathcal{B}_{21}$ in Table 1, we have $\#T_1 = 3.3889e+031$, $\#T_2 = 1.0786e+034$, $\#T_3 = 5.4802e+033$ and $\#T_4 = 9.3772e+032$. Then, the relationship (13) holds, which implies that there exist E_i. $1 \leq i \leq 4$.

i) Let $E_1 \subset \mathbb{F}_2^{105}$ with $\#E_1 = \#T_1$, and $S_1 = E_1 \times \mathbb{F}_2^{126}$.

ii) Let $E_1' = \overline{E_1} \times \mathbb{F}_2^{11}$, where $\overline{E_1} = \mathbb{F}_2^{105} \backslash E_1$. Note that $\#E_1' = 1.3672e+034 > \#T_2$. Let $E_2 \subset E_1'$ with $\#E_2 = \#T_2$, and $S_2 = E_2 \times \mathbb{F}_2^{115}$.

iii) Let $E_2' = \overline{E_2} \times \mathbb{F}_2$, where $\overline{E_2} = E_1' \backslash E_2$. Note that $\#E_2' = 5.7720e+033 > \#T_3$. Let $E_3 \subset E_2'$ with $\#E_3 = \#T_3$, and $S_3 = E_3 \times \mathbb{F}_2^{114}$.

iv) Let $E_4 = \overline{E_3} \times \mathbb{F}_2$, where $\overline{E_3} = E_2' \backslash E_3$. Note that $\#E_4 = 5.8360e+032 < \#T_4$, Let $S_4 = E_4 \times \mathbb{F}_2^{113}$.

It is easy to verify that S_1, S_2, S_3 and S_4 are mutually disjoint, and $S_1 \cup S_2 \cup S_3 \cup S_4 = \mathbb{F}_2^{231}$. Therefore, a $(231, 49, 2^{230} - 2^{115} + 2^{112})$ resilient Boolean function can be obtained by Construction 1. The resiliency order of this function is better than the $(231, 48, 2^{230} - 2^{115} + 2^{112})$ resilient Boolean function in [19] while keeping the same nonlinearity. For more examples, see Table 2.

Remark 1: When the variable number n reaches a sufficiently large level, we believe that the gap between the resiliency order of our functions and the constructed functions in [19] will be greater than 1.

4. Conclusions

In this paper, we present a novel method for constructing odd-variable SAO resilient functions, and obtain a large class of resilient functions possess higher resiliency order than the known functions while keeping higher SAO nonlinearity. Further improvements toward the tradeoff relationship between nonlinearity and resiliency order appear to be an interesting research direction, and in addition it is still a challenging problem to get odd-variable resilient functions with better SAO nonlinearity than previous studies without using PW functions or KY functions.

References

[1] C. Ding, G. Xiao, and W. Shan, The Stability Theory of Stream Ciphers, Springer, 1991.
[2] W. Meier and O. Staffelbach, "Fast correlation attacks on certain stream ciphers," J. Cryptol., vol.1, no.3, pp.159–176, 1989.
[3] T. Siegenthaler, "Correlation-immunity of nonlinear combining functions for cryptographic applications (Corresp.)," IEEE Trans. Inf. Theory, vol.30, no.5, pp.776–780, 1984.
[4] S. Sarkar and S. Maitra, "Idempotents in the neighbourhood of Patterson-Wiedemann functions having walsh spectra zeros," Des. Codes Cryptogr., vol.49, no.1, pp.95–103, 2008.
[5] S. Maitra and E. Pasalic, "Further constructions of resilient Boolean functions with very high nonlinearity," IEEE Trans. Inf. Theory, vol.48, no.7, pp.1825–1834, 2002.
[6] S. Maitra and E. Pasalic, "A Maiorana-McFarland type construction for resilient functions on variables (n even) with nonlinearity $> 2^{n-1} - 2^{n/2} + 2^{n/2-2}$," Discr. Appl. Math., vol.154, no.2, pp.357–369, 2006.
[7] E. Pasalic and T. Johansson, "Further results on the relation between nonlinearity and resiliency of Boolean functions," IMA Conference on Cryptography and Coding, LNCS, vol.1746, pp.35–45, Springer, 1999.
[8] P. Sarkar and S. Maitra, "Construction of nonlinear Boolean functions with important cryptographic properties," Advances in Cryptology-EUROCRYPT 2000, vol.1807, pp.485–506, Springer, 2000.
[9] P. Sarkar and S. Maitra, "Construction of nonlinear resilient Boolean functions using "small" affine functions," IEEE Trans. Inf. Theory, vol.50, no.9, pp.2185–2193, 2004.
[10] P. Sarkar and S. Maitra, "Nonlinearity bounds and constructions of resilient functions," Advances in Cryptology-EUROCRYPT 2000, LNCS, vol.1807, pp.515–532, Springer, 2000.
[11] W. Meier and O. Staffelbach, "Nonlinearity criteria for cryptographic functions," Advances in Cryptology-EUROCRYPT 1990, LNCS, vol.434, pp.549–562, Springer, 1990.
[12] J. Seberry, X. Zhang, and Y. Zheng, "On constructions and nonlinearity of correlation immune Boolean functions," Advances in Cryptology-EUROCRYPT 1994, LNCS, vol.765, pp.181–199, Springer, 1994.
[13] D. Tang, C. Carlet, X. Tang, and Z. Zhou, "Construction of highly nonlinear 1-resilient Boolean functions with optimal algebraic immunity and provably high fast algebraic immunity," IEEE Trans. Inf. Theory, vol.63, no.9, pp.6113–6125, 2017.
[14] Y. Wei, E. Pasalic, F. Zhang, and W. Wu, "New constructions of resilient functions with strictly almost optimal nonlinearity via non-overlap spectra functions," Inform. Sci., vol.415, no.2, pp.377–396, 2017.
[15] F. Zhang, C. Carlet, Y. Hu, and T. Cao, "Secondary constructions of highly nonlinear Boolean functions and disjoint spectra plateaued functions," Inform. Sci., vol.283, no.1, pp.94–106, 2014.
[16] F. Zhang, Y. Wei, E. Pasalic, and S. Xia, "Large sets of disjoint spectra plateaued functions inequivalent to partially linear functions," IEEE Trans. Inf. Theory, vol.64, no.4, pp.2987–2999, 2018.
[17] W. Zhang and E. Pasalic, "Generalized Maiorana-McFarland construction of resilient Boolean functions with high nonlinearity and good algebraic properties," IEEE Trans. Inf. Theory, vol.60, no.10, pp.6681–6695, 2014.
[18] W. Zhang and E. Pasalic, "Constructions of resilient S-boxes with strictly almost optimal nonlinearity through disjoint linear codes," IEEE Trans. Inf. Theory, vol.60, no.3, pp.1638–1651, 2014.
[19] W. Zhang, "High-meets-low: Construction of strictly almost optimal resilient Boolean functions via fragmentary walsh spectra," IEEE Trans. Inf. Theory, vol.65, no.9, pp.5856–5864, 2019.
[20] W. Zhang, "The truth table of a 21-variable 1-resilient Boolean function with nonlinearity 1047680," IEEE Dataport, 2018. [Online]. Available: http://dx.doi.org/10.21227/mkm1-ff85. Accessed: Feb. 05, 2019.
[21] G. Xiao and J. Massey, "A spectral characterization of correlation-immune combining functions," IEEE Trans. Inf. Theory, vol.34, no.3, pp.569–571, 1988.