High-Meets-Low: Construction of Strictly Almost Optimal Resilient Boolean Functions via Fragmentary Walsh Spectra

WeiGuo Zhang, Senior Member, IEEE

Dedicated to the memory of GuoZhen Xiao (1934-2016)

Abstract—This paper considers the construction of resilient Boolean functions on odd number of variables with strictly almost optimal (SAO) nonlinearity. Through introducing the fragmentary Walsh transform, a construction technique called "High-Meets-Low" is proposed. The detailed design procedures of a 39-variable 3-resilient Boolean function with SAO nonlinearity $2^{38}-2^{19}+2^{16}+2^{14}$ are given. It is shown that the nonlinearity of an n-variable t-resilient Boolean function can reach $2^{n-1}-2^{(n-1)/2}+5\cdot 2^{(n-11)/2}$ or $2^{n-1}-2^{(n-1)/2}+2^{(n-7)/2}$, which are the largest known values for the corresponding n and t. Finally, by constructing a 29-variable balanced Boolean function with SAO nonlinearity $2^{28}-2^{14}+2^{11}+2^{9}$, we show an alternative method to realize the High-Meets-Low construction technique.

Index Terms—Boolean function, cryptography, fragmentary Walsh transform, High-Meets-Low, nonlinearity, resiliency, stream cipher.

I. Introduction

Nonlinearity is the most important cryptographic property of Boolean functions used in symmetric cryptosystems (stream ciphers and block ciphers) since linear systems are easily breakable [3], [11], which requires the Boolean functions must be at sufficiently large distance from any affine functions. Note that the Reed-Muller code of order 1, $R(1,n)$, can be regarded as the set of all affine functions on the n-dimensional vector space $\mathbb{F}_2^n$. The maximum nonlinearity of n-variable functions is just the covering radius of $R(1,n)$. For even n, it is well-known that the maximum nonlinearity $2^{n-1}-2^{n/2-1}$ is attained for the bent functions [2], [15]. For odd $n\le 7$, it has been shown that the maximal nonlinearity of n-variables Boolean functions is $2^{n-1}-2^{(n-1)/2}$ [1], [13]. Unfortunately, the maximum nonlinearity of n-variable functions for odd $n\ge 9$ is hitherto unknown.

Hereafter, we call a Boolean function on odd number of variables strictly almost optimal (SAO) if its nonlinearity greater than bent concatenation bound $2^{n-1}-2^{(n-1)/2}$. One didn't know any SAO Boolean functions on odd number of variables until Patterson and Wiedemann discovered 15-variable Boolean functions with nonlinearity 16276 (called PW functions) in 1983 [14]. More than two decades later, continued progress was made in this problem. Kavut et al. found 9-variable Boolean functions with SAO nonlinearity 241 by heuristic search in the space of rotation symmetric Boolean functions [6], [7]. Before long, by considering the k-rotation-symmetric Boolean functions, Kavut and Yücel improved the nonlinearity to 242 (called KY functions) [8]. Recently, Kavut and Maitra obtained the 21-variable Boolean functions having SAO nonlinearity 1047613 [4]. Although the nonlinearity of these functions is less than that of 21-variable Boolean functions which are obtained by composing a 15-variable PW function and a 6-variable bent function, these functions are PW type functions which were not known earlier. In addition, Kavut et al. presented nontrivial upper bounds on the nonlinearity of PW type functions and their super-sets, and gave some search strategies to get SAO Boolean functions on n-variables where n is odd and not prime [5].

Resilient (balanced correlation immune) Boolean functions have important applications in the nonlinear combiner model of a stream cipher, and ensure that the ciphers are not susceptible to a divide-and-conquer attack [20], [21]. Construction of t-resilient Boolean functions with as high nonlinearity as possible has been an important research topic since the mid 1980s, see [24], [25] and the references therein. However, when it comes to constructing SAO resilient functions on odd number of variables, very few relative results have been obtained. We give a summary of earlier results as follows. It is worth noting that balanced Boolean functions are viewed as 0-resilient Boolean functions, and by an (n,t,N_f) function we mean an n-variable t-resilient Boolean function with nonlinearity N_f.

- In 1993, by using the direct sum of a PW function and a balanced Boolean function on even number of variables with currently best nonlinearity, the earliest SAO balanced Boolean functions on odd number of variables $n\ge 29$ were obtained by Seberry et al [19].
- In 2000, Sarkar and Maitra showed that $(15,0,16262)$ functions can be found by modifying the truth tables of the PW functions [10], [16]. They also obtained $(17,0,2^{16}-2^8+18)$, $(19,0,2^{18}-2^9+46)$ and $(21,0,2^{20}-2^{10}+104)$ functions. These parameters are

W.-G. Zhang is with the State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China (e-mail: zwg@xidian.edu.cn; http://web.xidian.edu.cn/wgzhang)

Digital Object Identifier: 10.1109/TIT.2019.2899397

improved by S. Sarkar and Maitra that $(15, 0, 16272)$ functions were obtained [18]. This implies that there exist $(n, 0, 2^{n-1} - 2^{(n-1)/2} + 2^{(n-7)/2})$ functions for odd $n \geq 15$. For $n = 9, 11, 13$, there are few previous literatures to discuss how to obtain an n-variable resilient Boolean function with SAO nonlinearity. We now only know that the nonlinearity of a balanced 13-variable Boolean function can reach 4036 [9].

- The earlist SAO 1-resilient Boolean functions on odd number of variables $n \geq 41$ were constructed by Sarkar and Maitra [16], [17]. Two examples show that $(41, 1, 2^{40} - 2^{20} + 52 \cdot 2^{10})$ and $(47, 2, 2^{46} - 2^{23} + 52 \cdot 2^{13})$ functions can be constructed. By modifying PW functions, the $(15, 1, 16264)$ functions are obtained, which implies that for odd $n \geq 17$, the $(n, 1, 2^{n-1} - 2^{(n-1)/2} + 2^{(n-9)/2})$ functions can be obtained [18].
- Zhang and Pasalic presented a large class of SAO t-resilient Boolean functions on odd number of variables by using the generalized Maiorana-McFarland (GMM) construction technique [24]. In the construction, PW functions or KY functions are "embedded" within the GMM structures, which makes the nonlinearity of the constructed functions be better than the one achieved by using direct sum method.
- By using initial functions with good parameters in the generalized indirect sum method, F. Zhang et al. constructed SAO resilient functions on odd number of variables with currently best nonlinearity in many cases [23]. In actual constructions, to obtain an $(n + m - 2)$-variable t-resilient Boolean function, one of the initial functions is a PW function ($m = 15$) or a KY function ($m = 9$), and the other one is an n-variable t-resilient Boolean function with currently best known nonlinearity, where n is even.

The thing that all the above constructions have in common is that PW functions or KY functions are used as the core components in the constructed functions. The nonlinearities of the constructed functions are always $< 2^{n-1} - 2^{(n-1)/2} + 5 \cdot 2^{(n-11)/2}$ when using PW functions, and always $< 2^{n-1} - 2^{(n-1)/2} + 2^{(n-7)/2}$ when using KY functions.

Our contribution: We define the so-called fragmentary Walsh transform of an n-variable fragmentary Boolean function f_S on S, where $S \subset \mathbb{F}_2^n$. With the aid of fragmentary Walsh spectra, we then describe a construction technique "High-Meets-Low" to obtain resilient Boolean functions with currently best known nonlinearity. Thanks to the PW functions and KY functions, we can respectively construct the n-variable (n odd) t-resilient Boolean functions with SAO nonlinearity $2^{n-1} - 2^{(n-1)/2} + 5 \cdot 2^{(n-11)/2}$ and $2^{n-1} - 2^{(n-1)/2} + 2^{(n-7)/2}$. What is worth mentioning, the resiliency order t increases with the variable number n.

The remainder of this paper is organized as follows. Section II establishes our notation and introduces the notions of fragmentary Boolean functions and fragmentary Walsh transform. A sufficient condition for t-resiliency of a Boolean function is also given based on fragmentary Walsh spectra. Section III describes the High-Meets-Low construction technique in general outline. In Section IV, we first use one important example to further elaborate the High-Meets-Low technique of constructing SAO resilient Boolean functions via fragmentary Walsh spectra. Then we give some general results, and compare our results with the previous work. In this section, we also pose an alternative High-Meets-Low method to show how to construct a $(29, 0, 2^{28} - 2^{14} + 2^{11} + 2^9)$ function. Section V presents our conclusions.

II. Preliminaries

Let $\mathcal{B}_n$ denote the set of Boolean functions of n variables. A Boolean function $f \in \mathcal{B}_n$ is a mapping from $\mathbb{F}_2^n$ into $\mathbb{F}_2$. Any Boolean function has a unique representation as a multivariate polynomial over $\mathbb{F}_2$, called algebraic normal form (ANF),

$$f(X) = \sum_{u \in \mathbb{F}_2^n} \lambda_u (\prod_{i=1}^{n} x_i^{u_i}),$$

where $\lambda_u \in \mathbb{F}_2$, $X = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$ and $u = (u_1, \ldots, u_n) \in \mathbb{F}_2^n$. The algebraic degree of $f(X)$, denoted by $deg(f)$, is the maximal value of $wt(u)$ such that $\lambda_u \neq 0$, where $wt(u)$ denotes the Hamming weight of u. A Boolean function with $deg(f) \leq 1$ is said to be affine. An affine function with the constant term equal to zero is called a linear function. Any linear function on $\mathbb{F}_2^n$ is denoted by

$$\omega \cdot X = \omega_1 x_1 + \ldots + \omega_n x_n,$$

where $\omega = (\omega_1, \ldots, \omega_n) \in \mathbb{F}_2^n$, and "$\cdot$" denotes the dot (inner) product of two vectors. The Walsh transform of $f \in \mathcal{B}_n$ at point ω is denoted by $W_f(\omega)$ and it is computed as

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

A function f is balanced if its output column in the truth table contains equal number of 0's and 1's, i.e., $W_f(0_n) = 0$, where 0_n denotes the zero vector of $\mathbb{F}_2^n$. In terms of Walsh spectra, the nonlinearity of f is given by [12]

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

In [22], a spectral characterization of t-resilient Boolean functions has been derived, which is stated here as a lemma.

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

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

We next introduce the notion of the fragmentary Walsh transform of an n-variable fragmentary Boolean function.

Definition 1. 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 ω, $\omega \in \mathbb{F}_2^n$, is an integer valued function over S defined by

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

The fragmentary Walsh spectra of f_S is the multiset $\{FW_{f_S}(\omega) \mid \omega \in \mathbb{F}_2^n\}$.

Remark 1. For $i = 1, 2, \cdots, d$, let S_i be a nonempty subset of $\mathbb{F}_2^n$ so that

$$\bigcup_{i=1}^{d} S_i = \mathbb{F}_2^n \tag{2}$$

and $S_1, S_2, \cdots, S_d$ are mutually disjoint, i.e., for all $i, j = 1, 2, \cdots, d$,

$$S_i \cap S_j = \emptyset, \quad 1 \le i < j \le d. \tag{3}$$

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

$$f_{S_i}(X) = f(X), \text{ for } X \in S_i, \ i = 1, 2, \cdots, d.$$

Then we have

$$W_f(\omega) = \sum_{i=1}^{d} FW_{f_{S_i}}(\omega). \tag{4}$$

Especially, when $d = 2$,

$$W_f(\omega) = FW_{f_{S_1}}(\omega) + FW_{f_{S_2}}(\omega). \tag{5}$$

By means of fragmentary Walsh transforms, we next give a sufficient condition for a Boolean function to be t-resilient.

Lemma 2. Let $f \in \mathcal{B}_n$. For $i = 1, 2, \cdots, d$, let S_i and f_{S_i} be defined as in Remark 1. Then f is t-resilient if $FW_{f_{S_i}}(\omega) = 0$ always holds for $0 \le wt(\omega) \le t$ and $1 \le i \le d$.

Proof. It follows immediately from Lemma 1 and (4). □

III. A brief introduction of the High-Meets-Low technique

To describe the High-Meets-Low technique clearly, we first take $d = 2$ as an illustration. By (5),

$$|W_f(\omega)| \le |FW_{f_{S_1}}(\omega)| + |FW_{f_{S_2}}(\omega)|.$$

To obtain a Boolean function with high nonlinearity, by (1), $\max_{\omega \in \mathbb{F}_2^n} |W_f(\omega)|$ should as far as possible small. This can be done by avoiding the addition between high fragmentary spectral amplitudes of f_{S_1} and f_{S_2} at any point ω. In other words, the high fragmentary spectral amplitudes of f_{S_1} always meet the low fragmentary spectral amplitudes of f_{S_2}, which makes the additions of $|FW_{f_{S_1}}(\omega)|$ and $|FW_{f_{S_2}}(\omega)|$ somewhat like that the teeth of one saw engage with the gullets of the other saw. This technique is certainly suitable for $d \ge 3$. By (4),

$$|W_f(\omega)| \le \sum_{i=1}^{d} |FW_{f_{S_i}}(\omega)|. \tag{6}$$

Generally speaking, the High-Meets-Low technique would be conducted skillfully if the following two principles are satisfied:

(P1) $\max\limits_{\omega \in \mathbb{F}_2^n} |W_f(\omega)| << \sum\limits_{i=1}^{d} \max\limits_{\omega \in \mathbb{F}_2^n} |FW_{f_{S_i}}(\omega)|$;

(P2) $\varepsilon = \max\limits_{\omega \in \mathbb{F}_2^n} |W_f(\omega)| - \max\{\max\limits_{\omega \in \mathbb{F}_2^n} |FW_{f_{S_i}}(\omega)| : i = 1, \cdots, d\}$ is relatively small.

IV. Construction

The idea of the High-Meets-Low construction technique is clearly expressed in this section. The methods we proposed realize the principles (P1) and (P2). In particular, we achieve $\varepsilon = 0$ in (P2). More specifically, based on PW or KY functions, we achieve the prospective result that

$$\max_{\omega \in \mathbb{F}_2^n} |W_f(\omega)| = \lambda \cdot 2^k,$$

where $f \in B_n$, $n = 2k+m$, is a t-resilient Boolean function and

$$(m, \lambda) = \begin{cases} (15, 216), & \text{PW case} \\ (9, 28), & \text{KY case.} \end{cases}$$

A. It is possible to construct a $(39, 3, 2^{38} - 2^{19} + 2^{16} + 2^{14})$ function

We now use High-Meets-Low technique to construct a 39-variable 3-resilient Boolean function with nonlinearity $2^{38} - 2^{19} + 2^{16} + 2^{14}$. In order to achieve this goal, a PW function will be used in the construction. Let $g \in \mathcal{B}_{15}$ be a PW function (see its truth table in Appendix A), and its spectra distribution is as follows:

$$W_g(\beta) = \begin{cases} 40, & \beta \in U_1, \ \#U_1 = 3255 \\ -88, & \beta \in U_2, \ \#U_2 = 217 \\ 168, & \beta \in U_3, \ \#U_3 = 16275 \\ -216, & \beta \in U_4, \ \#U_4 = 13021, \end{cases}$$

where $U_1 \cup U_2 \cup U_3 \cup U_4 = \mathbb{F}_2^{15}$ and $U_i \cap U_j = \emptyset$ for any $1 \le i < j \le 4$.

In this example, we set $d = 4$. We next construct four 39-variable fragmentary Boolean functions f_{S_i} on S_i, $i = 1, 2, 3, 4$. Certainly, S_1, S_2, S_3 and S_4 should satisfy the relationships in (2) and (3).

Let $X = (x_1, \cdots, x_{24}) \in \mathbb{F}_2^{24}$ and $Y \in \mathbb{F}_2^{15}$. Let $X_{(i,j)} = (x_i, \cdots, x_j) \in \mathbb{F}_2^{j-i+1}$, where $1 \le i < j \le 24$.

i) f_{S_1} and its fragmentary Walsh spectra distribution

Let $X = (x_1, \cdots, x_{24}) \in \mathbb{F}_2^{24}$ and $Y \in \mathbb{F}_2^{15}$. Let

$$T_1 = \{\eta \mid wt(\eta) \ge 4, \eta \in \mathbb{F}_2^{12}\}.$$

Let $E_1 \subset \mathbb{F}_2^{12}$ with

$$\#E_1 = \#T_1 = \sum_{j=4}^{12} \binom{12}{j} = 3797.$$

Let

$$S_1 = E_1 \times \mathbb{F}_2^{27}.$$

TABLE I
$N_i(\tau)$ for the PW function in Appendix A, $i = 1, 2, 3$

τ	0	1	2	3	4	5	6	7
$N_1(\tau)$	0	0	14	43	137	307	492	615
$N_2(\tau)$	0	1	0	0	8	27	41	54
$N_3(\tau)$	0	11	46	197	701	1445	2519	3266

τ	8	9	10	11	12	13	14	15
$N_1(\tau)$	634	527	289	146	40	10	1	0
$N_2(\tau)$	33	26	21	4	2	0	0	0
$N_3(\tau)$	3215	2414	1465	699	241	48	8	0

We construct a fragmentary Boolean function f_{S_1} on S_1 as follows:

$$f_{S_1}(X, Y) = \Phi_1(X_{(1,12)}) \cdot X_{(13,24)} + g(Y),$$

where Φ_1 is a bijective mapping from E_1 to T_1, and g is a PW function given in Appendix A. Let $\alpha = (\alpha_1, \cdots, \alpha_{24}) \in \mathbb{F}_2^{24}$ and $\beta \in \mathbb{F}_2^{15}$. The distribution of the fragmentary Walsh spectra of f_{S_1} is calculated as follows:

$$\begin{aligned} &FW_{f_{S_1}}(\alpha, \beta) \\ &= \sum_{X_{(1,12)} \in E_1} \sum_{X_{(13,24)} \in \mathbb{F}_2^{12}} \sum_{Y \in \mathbb{F}_2^{15}} (-1)^{f_{S_1}(X,Y) + (\alpha,\beta)\cdot(X,Y)} \\ &= W_g(\beta) \sum_{X_{(1,12)} \in E_1} (-1)^{\alpha_{(1,12)} \cdot X_{(1,12)}} \\ &\qquad \sum_{X_{(13,24)} \in \mathbb{F}_2^{12}} (-1)^{(\Phi_1(X_{(1,12)}) + \alpha_{(13,24)}) \cdot X_{(13,24)}} \\ &= \begin{cases} 0, & \alpha_{(13,24)} \notin T_1 \\ \pm\ 40 \cdot 2^{12}, & \alpha_{(13,24)} \in T_1, \beta \in U_1 \\ \pm\ 88 \cdot 2^{12}, & \alpha_{(13,24)} \in T_1, \beta \in U_2 \\ \pm 168 \cdot 2^{12}, & \alpha_{(13,24)} \in T_1, \beta \in U_3 \\ \pm 216 \cdot 2^{12}, & \alpha_{(13,24)} \in T_1, \beta \in U_4. \end{cases} \end{aligned} \tag{7}$$

When $0 \le wt(\alpha, \beta) \le 3$, we have $\alpha_{(13,24)} \notin T_1$. By (7), we have

$$FW_{f_{S_1}}(\alpha, \beta) = 0, \quad \text{for } 0 \le wt(\alpha, \beta) \le 3. \tag{8}$$

ii) f_{S_2} and its fragmentary Walsh spectra distribution

For $i = 1, 2, 3$, let

$$N_i(\tau) = \#\{\beta \mid wt(\beta) = \tau,\ \beta \in U_i\}. \tag{9}$$

and

$$\Gamma_i(u, t) = \{(\delta, \beta) \mid wt(\delta, \beta) \ge t + 1,\ \delta \in \mathbb{F}_2^u,\ \beta \in U_i\}.$$

In Table I, we list the values of $N_i(\tau)$ in (9) for the PW function g in Appendix A. For any $u \ge 0$, we have

$$\#\Gamma_i(u, t) = 2^u \cdot \#U_i - \sum_{j=0}^{v} \left(N_i(j) \cdot \sum_{e=0}^{\lambda} \binom{u}{e} \right), \tag{10}$$

where $v = \min\{t, 15\}$ and $\lambda = \min\{u, t - j\}$. Let

$$T_2 = \Gamma_1(4, 3) \cup \Gamma_2(4, 3).$$

Obviously, $T_2 \subset \mathbb{F}_2^{19}$. By (10), we have

$$\#T_2 = \#\Gamma_1(4, 3) + \#\Gamma_2(4, 3) = 51967 + 3461 = 55428.$$

Let $E_1' = \overline{E_1} \times \mathbb{F}_2^8$, where $\overline{E_1} = \mathbb{F}_2^{12} \setminus E_1$. Note that

$$\#E_1' = 2^8 \cdot \sum_{j=0}^{3} \binom{12}{j} = 76544 > \#T_2.$$

Let $E_2 \subset E_1'$ with $\#E_2 = \#T_2$. Let

$$S_2 = E_2 \times \mathbb{F}_2^{19}.$$

We construct a fragmentary Boolean function f_{S_2} on S_2 as follows:

$$f_{S_2}(X, Y) = \Phi_2(X_{(1,20)}) \cdot (X_{(21,24)}, Y),$$

where Φ_2 is a bijective mapping from E_2 to T_2. We then have

$$\begin{aligned} FW_{f_{S_2}}(\alpha, \beta) &= \sum_{X_{(1,20)} \in E_2} (-1)^{\alpha_{(1,20)} \cdot X_{(1,20)}} \\ &\quad \sum_{(X_{(21,24)}, Y) \in \mathbb{F}_2^{19}} (-1)^{(\Phi_2(X_{(1,20)}) + (\alpha_{(21,24)}, \beta)) \cdot (X_{(21,24)}, Y)} \\ &= \begin{cases} 0, & (\alpha_{(21,24)}, \beta) \notin T_2 \\ \pm 2^{19}, & (\alpha_{(21,24)}, \beta) \in T_2. \end{cases} \end{aligned}$$

More precisely,

$$FW_{f_{S_2}}(\alpha, \beta) = \begin{cases} \pm 2^{19}, & \beta \in U_1 \cup U_2 \text{ and} \\ & wt(\alpha_{(21,24)}, \beta) \ge 4 \\ 0, & \text{otherwise.} \end{cases} \tag{11}$$

When $0 \le wt(\alpha, \beta) \le 3$, we have $(\alpha_{(21,24)}, \beta) \notin T_2$, which implies

$$FW_{f_{S_2}}(\alpha, \beta) = 0, \quad \text{for } 0 \le wt(\alpha, \beta) \le 3. \tag{12}$$

iii) f_{S_3} and its fragmentary Walsh spectra distribution

Let

$$T_3 = \Gamma_1(2, 3) \cup \Gamma_3(2, 3) \subset \mathbb{F}_2^{17}.$$

We have

$$\#T_3 = \#\Gamma_1(2, 3) + \#\Gamma_3(2, 3) = 12935 + 64721 = 77656.$$

Let $E_2' = \overline{E_2} \times \mathbb{F}_2^2$, where $\overline{E_2} = E_1' \setminus E_2$. Note that

$$\#E_2' = 2^2 \cdot (76544 - 55428) = 84464 > \#T_3.$$

Let $E_3 \subset E_2'$ with $\#E_3 = \#T_3$. Let

$$S_3 = E_3 \times \mathbb{F}_2^{17}.$$

We construct a fragmentary Boolean function f_{S_3} on S_3 as follows:

$$f_{S_3}(X, Y) = \Phi_3(X_{(1,22)}) \cdot (X_{(23,24)}, Y),$$

where Φ_3 is a bijective mapping from E_3 to T_3. We then

have

$$FW_{f_{S_3}}(\alpha,\beta)=\sum_{X_{(1,22)}\in E_3}(-1)^{\alpha_{(1,22)}\cdot X_{(1,22)}}\sum_{(X_{(23,24)},Y)\in\mathbb{F}_2^{17}}(-1)^{(\Phi_2(X_{(1,22)})+(\alpha_{(23,24)},\beta))\cdot(X_{(23,24)},Y)}$$
$$=\begin{cases}\pm 2^{17}, & (\alpha_{(23,24)},\beta)\in T_3\\ 0, & (\alpha_{(23,24)},\beta)\notin T_3.\end{cases}$$
$$=\begin{cases}\pm 2^{17}, & \beta\in U_1\cup U_3 \text{ and } wt(\alpha_{(23,24)},\beta)\geq 4\\ 0, & \text{otherwise.}\end{cases}\quad(13)$$

When $0\leq wt(\alpha,\beta)\leq 3$, we have $(\alpha_{(23,24)},\beta)\notin T_2$, which implies

$$FW_{f_{S_3}}(\alpha,\beta)=0,\quad \text{for } 0\leq wt(\alpha,\beta)\leq 3.\quad(14)$$

iv) f_{S_4} and its fragmentary Walsh spectra distribution

Let

$$T_4=\Gamma_1(1,3)\cup\Gamma_3(1,3)\subset\mathbb{F}_2^{16}.$$

We have

$$\#T_4=\#\Gamma_1(1,3)+\#\Gamma_3(1,3)=6439+32239=38678.$$

Let $E_4=\overline{E_3}\times\mathbb{F}_2$, where $\overline{E_3}=E_2'\setminus E_3$. Note that

$$\#E_4=2\cdot(84464-77656)=13616<\#T_4.$$

We can build an injective mapping Φ_4 from E_4 to T_4. Let

$$S_4=E_4\times\mathbb{F}_2^{16}.$$

We construct a fragmentary Boolean function f_{S_4} on S_4 as follows:

$$f_{S_4}(X,Y)=\Phi_4(X_{(1,23)})\cdot(x_{24},Y).$$

We then have

$$FW_{f_{S_4}}(\alpha,\beta)=\sum_{X_{(1,23)}\in E_3}(-1)^{\alpha_{(1,23)}\cdot X_{(1,23)}}\sum_{(x_{24},Y)\in\mathbb{F}_2^{16}}(-1)^{(\Phi_4(X_{(1,23)})+(\alpha_{24},\beta))\cdot(x_{24},Y)}$$
$$=\begin{cases}\pm 2^{16}, & \beta\in U_1\cup U_3 \text{ and } \Phi_4^{-1}(\alpha_{24},\beta) \text{ exists}\\ 0, & otherwise.\end{cases}\quad(15)$$

When $0\leq wt(\alpha,\beta)\leq 3$, $\Phi_4^{-1}(\alpha_{24},\beta)$ does not exist, which implies

$$FW_{f_{S_4}}(\alpha,\beta)=0,\quad \text{for } 0\leq wt(\alpha,\beta)\leq 3.\quad(16)$$

It is not difficult to verify that S_1, S_2, S_3 and S_4 are mutually disjoint, and

$$S_1\cup S_2\cup S_3\cup S_4=\mathbb{F}_2^{39}.$$

Combining (8), (12), (14) and (16), by Lemma 2, we know f is 3-resilient.

By (6), we have

$$|W_f(\alpha,\beta)|\leq\sum_{i=0}^{3}|FW_{f_{S_i}}(\alpha,\beta)|.$$

Combining (7),(11),(13) and (15), the idea of the High-Meets-Low is shown in the following expression:

$$|W_f(\alpha,\beta)|\leq\begin{cases}40\cdot 2^{12}+2^{19}+2^{17}+2^{16}, & \beta\in U_1\\ 88\cdot 2^{12}+2^{19}, & \beta\in U_2\\ 168\cdot 2^{12}+2^{17}+2^{16}, & \beta\in U_3\\ 216\cdot 2^{12}, & \beta\in U_4.\end{cases}$$

This implies that

$$\max_{(\alpha,\beta)\in\mathbb{F}_2^{21}}|W_f(\alpha,\beta)|=216\cdot 2^{12}=2^{20}-2^{17}-2^{15}.$$

Hence, $N_f=2^{38}-2^{19}+2^{16}+2^{14}$.

B. General results and parameters comparisons

In this subsection, we give some general results on constructing SAO resilient Boolean functions on odd number of variables. A general High-Meets-Low construction technique is described in Theorem 1 and its proof. The parameters comparisons with the previous works are also proposed.

Theorem 1. (PW case:) Let $g\in B_{15}$ be a PW function as in Appendix A, and

$$\begin{aligned}U_1&=\{\beta\mid W_g(\beta)=40,\ \beta\in\mathbb{F}_2^{15}\},\\ U_2&=\{\beta\mid W_g(\beta)=-88,\ \beta\in\mathbb{F}_2^{15}\},\\ U_3&=\{\beta\mid W_g(\beta)=168,\ \beta\in\mathbb{F}_2^{15}\},\\ U_4&=\{\beta\mid W_g(\beta)=-216,\ \beta\in\mathbb{F}_2^{15}\}.\end{aligned}$$

Let t be a nonnegative integer and $n\geq 31$ be an odd number. Let $k=(n-15)/2$. Let

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

For $i=1,2,3$, let

$$\Gamma_i(u,t)=\begin{cases}\{(\delta,\beta)\mid wt(\delta,\beta)\geq t+1,\ \delta\in\mathbb{F}_2^u,\ \beta\in U_i\}, & if\ u\geq 0\\ \emptyset, & if\ u<0.\end{cases}\quad(17)$$

Let

$$T_2=\Gamma_1(k-8,\ t)\cup\Gamma_2(k-8,\ t),\quad(18)$$

$$T_3=\Gamma_1(k-10,t)\cup\Gamma_3(k-10,t),\quad(19)$$

and

$$T_4=\Gamma_1(k-11,t)\cup\Gamma_3(k-11,t).\quad(20)$$

If the inequality

$$2^{k+15}\#T_1+2^{k+7}\#T_2+2^{k+5}\#T_3+2^{k+4}\#T_4\geq 2^n\quad(21)$$

holds, then there exists an $(n,t,2^{n-1}-2^{(n-1)/2}+5\cdot 2^{(n-11)/2})$ resilient function.

Proof. In the PW case, we set $d=4$. Let $S_1=E_1\times\mathbb{F}_2^{k+15}$, $S_2=E_2\times\mathbb{F}_2^{k+7}$, $S_3=E_3\times\mathbb{F}_2^{k+5}$ and $S_4=E_4\times\mathbb{F}_2^{k+4}$

be nonempty proper subsets of $\mathbb{F}_2^n$, where $E_1 \subset \mathbb{F}_2^k$ $E_2 \subset \mathbb{F}_2^{k+8}$, $E_3 \subset \mathbb{F}_2^{k+10}$ and $E_4 \subset \mathbb{F}_2^{k+11}$. The relationship (21) guarantees that there exist E_i, $i = 1, 2, 3, 4$, such that

$$\#E_i \le \#T_i, \ 1 \le i \le 4 \tag{22}$$
$$\bigcup_{i=1}^{4} S_i = \mathbb{F}_2^n$$

and

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

hold simultaneously. By (22), we can build injective mappings Φ_i from E_i to T_i, $i = 1, 2, 3, 4$. Let $X = (x_1, \cdots, x_{2k}) \in \mathbb{F}_2^{2k}$ and $Y \in \mathbb{F}_2^{15}$. Next we construct four fragmentary Boolean functions f_{S_i} on S_i, $i = 1, 2, 3, 4$, as follows.

$$\begin{aligned} f_{S_1}(X,Y) &= \Phi_1(X_{(1,k)}) \cdot X_{(k+1,2k)} + g(Y), \\ f_{S_2}(X,Y) &= \Phi_2(X_{(1,k+8)}) \cdot (X_{(k+9,2k)}, Y), \\ f_{S_3}(X,Y) &= \Phi_3(X_{(1,k+10)}) \cdot (X_{(k+11,2k)}, Y), \\ f_{S_4}(X,Y) &= \Phi_4(X_{(1,k+11)}) \cdot (X_{k+12,2k}, Y). \end{aligned}$$

The distributions of the fragmentary Walsh spectra of f_{S_i}, $i = 1, 2, 3, 4$, are as follows:

$$FW_{f_{S_1}}(\alpha,\beta) = \begin{cases} \pm\ 40 \cdot 2^k, & \beta \in U_1 \text{ and } \Phi_1^{-1}(\alpha_{(k+1,2k)}) \text{ exists} \\ \pm\ 88 \cdot 2^k, & \beta \in U_2 \text{ and } \Phi_1^{-1}(\alpha_{(k+1,2k)}) \text{ exists} \\ \pm 168 \cdot 2^k, & \beta \in U_3 \text{ and } \Phi_1^{-1}(\alpha_{(k+1,2k)}) \text{ exists} \\ \pm 216 \cdot 2^k, & \beta \in U_4 \text{ and } \Phi_1^{-1}(\alpha_{(k+1,2k)}) \text{ exists} \\ 0, & \text{otherwise,} \end{cases}$$

$$FW_{f_{S_2}}(\alpha,\beta) = \begin{cases} \pm 2^{k+7}, & \beta \in U_1 \cup U_2 \text{ and} \\ & \Phi_2^{-1}(\alpha_{(k+9,2k)}, \beta) \text{ exists} \\ 0, & \text{otherwise,} \end{cases}$$

$$FW_{f_{S_3}}(\alpha,\beta) = \begin{cases} \pm 2^{k+5}, & \beta \in U_1 \cup U_3 \text{ and} \\ & \Phi_3^{-1}(\alpha_{(k+11,2k)}, \beta) \text{ exists} \\ 0, & \text{otherwise,} \end{cases}$$

and

$$FW_{f_{S_4}}(\alpha,\beta) = \begin{cases} \pm 2^{k+4}, & \beta \in U_1 \cup U_3 \text{ and} \\ & \Phi_4^{-1}(\alpha_{(k+12,2k)}, \beta) \text{ exists} \\ 0, & \text{otherwise.} \end{cases}$$

For $i = 1, 2, 3, 4$, by the definitions of T_i, we have

$$FW_{f_{S_i}}(\alpha,\beta) = 0, \ for \ 0 \le wt(\alpha,\beta) \le t. \tag{23}$$

By Lemma 2, f is t-resilient. By (6),

$$\begin{aligned} |W_f(\alpha,\beta)| &\le \sum_{i=0}^{3} |FW_{f_{S_i}}(\alpha,\beta)| \\ &\le \begin{cases} 40 \cdot 2^k + 2^{k+7} + 2^{k+5} + 2^{k+4}, & \beta \in U_1 \\ 88 \cdot 2^k + 2^{k+7}, & \beta \in U_2 \\ 168 \cdot 2^k + 2^{k+5} + 2^{k+4}, & \beta \in U_3 \\ 216 \cdot 2^k, & \beta \in U_4, \end{cases} \end{aligned}$$

which implies

$$\max_{(\alpha,\beta) \in \mathbb{F}_2^{21}} |W_f(\alpha,\beta)| = 216 \cdot 2^k.$$

Hence, $N_f = 2^{n-1} - 2^{(n-1)/2} + 5 \cdot 2^{(n-11)/2}$. □

In Table III, we give an extended list of $(n, t, 2^{n-1} - 2^{(n-1)/2} + 5 \cdot 2^{(n-11)/2})$ resilient Boolean functions with currently best known nonlinearity. That's what should concern us, t can increase with the variable number n on condition that $N_f = 2^{n-1} - 2^{(n-1)/2} + 5 \cdot 2^{(n-11)/2}$.

Let us now proceed to the KY case to to realize the High-Meets-Low construction technique, where we would set $d = 3$. Below is the truth table of a KY function $g \in \mathcal{B}_9$ [8].

3740B6A118A1E1965FB902DFD409B0D5
9C2A4D81E3AD4A3EE59CBDE16BF50A9D
7EC8A68E5AB09902961456E066E8A801
57C4248E1AF29C803C3CBDF8B5E8812A (24)

The spectra distribution of g is as follows:

$$W_g(\beta) = \begin{cases} \pm 4, & \beta \in U_1, \ \#U_1 = 30 \\ \pm 12, & \beta \in U_2, \ \#U_2 = 46 \\ \pm 20, & \beta \in U_3, \ \#U_3 = 226 \\ \pm 28, & \beta \in U_4, \ \#U_4 = 210, \end{cases}$$

where $U_1 \cup U_2 \cup U_3 \cup U_4 = \mathbb{F}_2^9$ and $U_i \cap U_j = \emptyset$ for any $1 \le i < j \le 4$.

Theorem 2. (KY case:) Let $g \in B_9$ be a KY function as in (24), and

$$\begin{aligned} U_1 &= \{\beta \mid W_g(\beta) = \pm 4, \ \beta \in \mathbb{F}_2^9\}, \\ U_2 &= \{\beta \mid W_g(\beta) = \pm 12, \ \beta \in \mathbb{F}_2^9\}, \\ U_3 &= \{\beta \mid W_g(\beta) = \pm 20, \ \beta \in \mathbb{F}_2^9\}, \\ U_4 &= \{\beta \mid W_g(\beta) = \pm 28, \ \beta \in \mathbb{F}_2^9\}. \end{aligned}$$

Let t be a nonnegative integer and $n \ge 21$ be an odd number. Let $k = (n-9)/2$. Let

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

For $i = 1, 2, 3$, let

$$\Gamma_i(u,t) = \{(\delta,\beta) \mid wt(\delta,\beta) \ge t + 1, \ \delta \in \mathbb{F}_2^u, \ \beta \in U_i\}.$$

Note that $\#\Gamma_i(u,t)$ can be calculated by (10), and the values of $N_i(\tau)$ are listed in Table II. Let

$$T_2 = \Gamma_1(k-5, \ t) \cup \Gamma_2(k-5, \ t),$$

TABLE II
$N_i(\tau)$ for the KY function in (24), $i = 1, 2, 3$

τ	0	1	2	3	4	5	6	7	8	9
$N_1(\tau)$	0	0	4	9	11	6	0	0	0	0
$N_2(\tau)$	0	0	1	5	13	17	5	5	0	0
$N_3(\tau)$	0	0	16	47	55	50	36	19	2	1

and

$$T_3 = \Gamma_1(k-6,t) \cup \Gamma_3(k-6,t).$$

If the inequality

$$2^{k+9}\#T_1 + 2^{k+4}\#T_2 + 2^{k+3}\#T_3 \geq 2^n$$

holds, then there exists an $(n, t, 2^{n-1} - 2^{(n-1)/2} + 2^{(n-7)/2})$ resilient function.

Proof. The proof is similar with that of Theorem 1. □

Example 1. A $(21, 1, 2^{20} - 2^{10} + 2^7)$ function $f \in B_{21}$ can be constructed by using High-Meets-Low construction technique (KY case). The Walsh spectra distribution of f is as follows.

$$W_f(\alpha,\beta) = \begin{cases} 0, & 130816 \text{ times} \\ \pm 256, & 83904 \text{ times} \\ \pm 512, & 64512 \text{ times} \\ \pm 768, & 317376 \text{ times} \\ \pm 1024, & 34048 \text{ times} \\ \pm 1280, & 353856 \text{ times} \\ \pm 1792, & 1112640 \text{ times}. \end{cases} \quad (25)$$

The truth table of f can be found at [26]. The readers can verify that f is 1-resilient and (25) is correct. More examples can be found in Table IV.

We now compare our results with those in [18], where $(n, 0, 2^{n-1} - 2^{(n-1)/2} + 2^{(n-7)/2})$ functions and $(n, 1, 2^{n-1} - 2^{(n-1)/2)} + 2^{(n-9)/2})$ functions can be obtained for odd $n \geq 15$. For odd $n \geq 21$, it is clear that our approach is superior to that of [18]. When $n = 15, 17, 19$, the resilient functions in [18] still possess the highest nonlinearity known.

In Table V, a parameters comparison with [23] is also given.

C. How to construct a $(29, 0, 2^{28} - 2^{14} + 2^{11} + 2^9)$ function

When $n = 29$, we have $k = (n-15)/2 = 7$, which implies that $T_1 = T_2 = T_3 = \emptyset$ by (17-20). This leads to that the method above is not feasible for $n = 29$. We now give another High-Meets-Low method to get a $(29, 0, 2^{28} - 2^{14} + 2^{11} + 2^9)$ function.

Let $X = (x_1, \cdots, x_{14}) \in \mathbb{F}_2^{14}$ and $Y = (y_1, \cdots, y_{15}) \in \mathbb{F}_2^{15}$. We next divide $\mathbb{F}_2^{29}$ into three parts ($d = 3$):

$$\begin{aligned} S_1 &= \mathbb{F}_2^{7^*} \times \mathbb{F}_2^{22}, \\ S_2 &= \{0_7\} \times \mathbb{F}_2^{21} \times \{0\} \\ S_3 &= \{0_7\} \times \mathbb{F}_2^{21} \times \{1\}. \end{aligned}$$

Let $g(Y)$ be a PW function as in Appendix A. We first construct a fragmentary function f_{S_1} on S_1 as follows:

$$f_{S_1}(X,Y) = \Phi_1(X_{(1,7)}) \cdot X_{(8,14)} + g(Y),$$

where Φ_1 is a bijective mapping from $\mathbb{F}_2^{7^*}$ to $\mathbb{F}_2^{7^*}$. Let $\alpha = (\alpha_1, \cdots, \alpha_{14}) \in \mathbb{F}_2^{14}$ and $\beta = (\beta_1, \cdots, \beta_{15}) \in \mathbb{F}_2^{15}$. We have

$$FW_{f_{S_1}}(\alpha,\beta) = \begin{cases} \pm 40 \cdot 2^7, & \beta \in U_1, \alpha_{(8,14)} \neq 0_7 \\ \pm 88 \cdot 2^7, & \beta \in U_2, \alpha_{(8,14)} \neq 0_7 \\ \pm 168 \cdot 2^7, & \beta \in U_3, \alpha_{(8,14)} \neq 0_7 \\ \pm 216 \cdot 2^7, & \beta \in U_4, \alpha_{(8,14)} \neq 0_7 \\ 0, & \alpha_{(8,14)} = 0_7. \end{cases} \quad (26)$$

The second fragmentary function f_{S_2} on S_2 is constructed as follows:

$$f_{S_2}(X,Y) = \begin{cases} Y_{(1,7)} \cdot Y_{(8,14)}, & Y_{(1,7)} \neq 0_7 \\ Y_{(8,10)} \cdot Y_{(11,13)} + y_{14}, & Y_{(1,7)} = 0_7. \end{cases}$$

We have

$$\begin{cases} FW_{f_{S_2}}(\alpha,\beta) \in \{\pm(2^{14} \pm 2^{11}), \pm 2^{14}\}, \\ \qquad\qquad \text{if } \alpha_{(8,14)} = 0_7 \text{ and } \beta_{(8,14)} \neq 0_7 \\ FW_{f_{S_2}}(\alpha,\beta) = 0, \quad \text{if } \alpha_{(8,14)} \neq 0_7 \quad \text{or} \quad \beta_{(8,14)} = 0_7. \end{cases} \quad (27)$$

Let

$$T = \{Y_{(1,14)} \in \mathbb{F}_2^{14} \mid Y \in U_1 \text{ for any } y_{15} \in \mathbb{F}_2\},$$

where $U_1 = \{\beta \mid W_g(\beta) = 40,\ \beta \in \mathbb{F}_2^{15}\}$ and $\#U_1 = 3255$. Note that y_{15} is the least significant bit (LSB) of $Y \in U_1$. We can get $\#T = 135 > 2^7$ by calculation. We construct the third fragmentary function f_{S_3} on S_3 as follows:

$$f_{S_3}(X,Y) = \Phi_3(X_{(8,14)}) \cdot Y_{(1,14)},$$

where Φ_3 is an injective mapping from $\mathbb{F}_2^7$ to T. We have

$$FW_{f_{S_3}}(\alpha,\beta) = \begin{cases} \pm 2^{14}, & \beta \in U_1 \text{ and } \Phi^{-1}(\beta_{(1,14)}) \textit{ exists} \\ 0, & \text{otherwise.} \end{cases} \quad (28)$$

According to (6), $|W_f(\alpha,\beta)| \leq \sum_{i=1}^{3} |FW_{f_{S_i}}(\alpha,\beta)|$. Combining (26), (27) and (28), we have

$$|W_f(\alpha,\beta)| \leq \begin{cases} 40 \cdot 2^7 + 2^{14}, & \beta \in U_1, \alpha_{(8,14)} \neq 0_7 \\ 88 \cdot 2^7, & \beta \in U_2, \alpha_{(8,14)} \neq 0_7 \\ 168 \cdot 2^7, & \beta \in U_3, \alpha_{(8,14)} \neq 0_7 \\ 216 \cdot 2^7, & \beta \in U_4, \alpha_{(8,14)} \neq 0_7 \\ 2^{14} + 2^{11}, & \alpha_{(8,14)} = 0_7. \end{cases}$$

By (1), $N_f = 2^{28} - 2^{14} + 2^{11} + 2^9$. By (26) and (27), $FW_{f_{S_1}}(0_{29}) = FW_{f_{S_2}}(0_{29}) = 0$. Noticing $0_{15} \notin U_1$, we have $\Phi^{-1}(\beta_{(1,14)}) = \emptyset$, which implies $FW_{f_{S_3}}(0_{29}) = 0$. By (6), $W_f(0_{29}) = 0$. This proves f is balanced.

V. Concluding remarks

In this paper, we provide a construction technique, called High-Meets-Low, for designing odd-variable resilient Boolean functions with currently best known nonlinearity.

TABLE III
$(n, t, 2^{n-1} - 2^{(n-1)/2} + 5 \cdot 2^{(n-11)/2})$ functions for odd n, $29 \le n \le 135$

n	29	31,33	35,37	39,41,43	45,47	49,51,53	55,57	59,61,63
t	0	1	2	3	4	5	6	7
n	65,67	69,71	73,75	77,79,81	83,85	87,89	91,93,95	97,99
t	8	9	10	11	12	13	14	15
n	101,103	105,107	109,111,113	115,117	119,121	123,125	127,129	131,133,135
t	16	17	18	19	20	21	22	23

TABLE IV
$(n, t, 2^{n-1} - 2^{(n-1)/2} + 2^{(n-7)/2})$ functions for odd n, $19 \le n \le 123$

n	19	21,23,25	27,29	31,33,35	37,39	41,43	45,47	49,51,53
t	0	1	2	3	4	5	6	7
n	55,57	59,61	63,65,67	69,71	73,75	77,79	81,83	85,87,89
t	8	9	10	11	12	13	14	15
n	91,93	95,97	99,101	103,105	107, 109,111	113,115	117,119	121,123
t	16	17	18	19	20	21	22	23

TABLE V
Parameters comparison with [23]

Ours (KY case)	Ours (PW case)	[23]
$(35, 3, 2^{34} - 2^{17} + 16 \cdot 2^{10})$	$(35, 2, 2^{34} - 2^{17} + 20 \cdot 2^{10})$	$(35, 2, 2^{34} - 2^{17} + 2 \cdot 2^{10})$
$(37, 4, 2^{36} - 2^{18} + 32 \cdot 2^{10})$	$(37, 2, 2^{36} - 2^{18} + 40 \cdot 2^{10})$	$(37, 2, 2^{36} - 2^{18} + 18 \cdot 2^{10})$
$(39, 4, 2^{38} - 2^{19} + 64 \cdot 2^{10})$	$(39, 3, 2^{38} - 2^{19} + 80 \cdot 2^{10})$	$(39, 2, 2^{38} - 2^{19} + 36 \cdot 2^{10})$
$(41, 5, 2^{40} - 2^{20} + 128 \cdot 2^{10})$	$(41, 3, 2^{40} - 2^{20} + 160 \cdot 2^{10})$	$(41, 2, 2^{40} - 2^{20} + 86 \cdot 2^{10})$
$(43, 5, 2^{42} - 2^{21} + 256 \cdot 2^{10})$	$(43, 3, 2^{42} - 2^{21} + 320 \cdot 2^{10})$	$(43, 2, 2^{42} - 2^{21} + 212 \cdot 2^{10})$
$(45, 6, 2^{44} - 2^{22} + 512 \cdot 2^{10})$	$(45, 4, 2^{44} - 2^{22} + 640 \cdot 2^{10})$	$(45, 2, 2^{44} - 2^{22} + 424 \cdot 2^{10})$
$(47, 6, 2^{46} - 2^{23} + 2^{20})$	$(47, 4, 2^{46} - 2^{23} + 2^{20} + 256 \cdot 2^{10})$	$(47, 2, 2^{46} - 2^{23} + 956 \cdot 2^{10})$
$(49, 7, 2^{48} - 2^{24} + 2 \cdot 2^{20})$	$(49, 5, 2^{48} - 2^{24} + 2 \cdot 2^{20} + 512 \cdot 2^{10})$	$(49, 2, 2^{48} - 2^{24} + 2 \cdot 2^{20} + 80 \cdot 2^{10})$
$(51, 7, 2^{50} - 2^{25} + 4 \cdot 2^{20})$	$(51, 5, 2^{50} - 2^{25} + 5 \cdot 2^{20})$	$(51, 2, 2^{50} - 2^{25} + 4 \cdot 2^{20} + 160 \cdot 2^{10})$
$(53, 7, 2^{52} - 2^{26} + 8 \cdot 2^{20})$	$(53, 5, 2^{52} - 2^{26} + 10 \cdot 2^{20})$	$(53, 2, 2^{52} - 2^{26} + 9 \cdot 2^{20} + 320 \cdot 2^{10})$
$(55, 8, 2^{54} - 2^{27} + 16 \cdot 2^{20})$	$(55, 6, 2^{54} - 2^{27} + 20 \cdot 2^{20})$	$(55, 2, 2^{54} - 2^{27} + 18 \cdot 2^{20} + 320 \cdot 2^{10})$
$(57, 8, 2^{56} - 2^{28} + 32 \cdot 2^{20})$	$(57, 6, 2^{56} - 2^{28} + 40 \cdot 2^{20})$	$(57, 2, 2^{56} - 2^{28} + 38 \cdot 2^{20} + 320 \cdot 2^{10})$
$(59, 9, 2^{58} - 2^{29} + 64 \cdot 2^{20})$	$(59, 7, 2^{58} - 2^{29} + 80 \cdot 2^{20})$	$(59, 2, 2^{58} - 2^{29} + 76 \cdot 2^{20} + 768 \cdot 2^{10})$
$(61, 9, 2^{60} - 2^{30} + 128 \cdot 2^{20})$	$(61, 7, 2^{60} - 2^{30} + 160 \cdot 2^{20})$	$(61, 2, 2^{60} - 2^{30} + 154 \cdot 2^{20} + 960 \cdot 2^{10})$
$(63, 10, 2^{62} - 2^{31} + 256 \cdot 2^{20})$	$(63, 7, 2^{62} - 2^{31} + 320 \cdot 2^{20})$	$(63, 2, 2^{62} - 2^{31} + 313 \cdot 2^{20} + 256 \cdot 2^{10})$

The main tool in the analysis is the fragmentary Walsh transform, which makes the spectra distribution of the constructed functions to be more easily controlled. We next give some remarks to conclude this paper.

- It should be mentioned that Sarkar and Maitra introduced the notion of "fractional functions" in 2000 [16], which can be looked as a special case of fragmentary Boolean functions.
- The High-Meets-Low technique described in this paper is suitable to construct resilient functions with relatively large odd number of variables. For small odd n, $9 \le n \le 19$, it is still a challenging problem to get a resilient function with better SAO nonlinearity than previous studies [9], [18].
- The author believes that there exist n-variable (n odd) t-resilient Boolean functions with nonlinearity $> 2^{n-1} - 2^{(n-1)/2} + 5 \cdot 2^{(n-11)/2}$. Could we give a general construction to obtain odd-variable SAO functions without using PW functions or KY functions? Solving this problem can provide a motivation for future work.

APPENDIX A: A truth table of a PW function

https://web.xidian.edu.cn/wgzhang/files/pwfunction.txt

References

[1] E. Berlekamp and L. Welch, "Weight distributions of the cosets of the (32, 6) Reed-Muller code," IEEE Trans. Inf. Theory, vol. 18, no. 1, pp. 203-207, Jan. 1972.

[2] J. F. Dillon, "Elementary Hadamard difference sets," Ph.D. dissertation, Fac. Graduate School, Univ. Maryland, College Park, MD, USA, 1974.

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

[4] S. Kavut and S. Maitra, "Patterson-Wiedemann type functions on 21 variables with nonlinearity greater than bent concatenation bound," IEEE Trans. Inf. Theory, vol. 62, no. 4, pp. 2277-2282, Apr. 2016.

[5] S. Kavut, S. Maitra and F. Özbudak, "A super-set of Patterson-Wiedemann functions: upper bounds and possible nonlinearities," SIAM J. Discrete Math, vol. 32, no. 1, pp. 106-122, Jan. 2018.

[6] S. Kavut, S. Maitra, S. Sarkar, and M. D. Yücel, "Enumeration of 9-variable rotation symmetric Boolean functions having nonlinearity > 240," in Progress in Cryptology—INDOCRYPT 2006 (Lecture Notes in Computer Science), vol. 4329. Berlin, Germany: Springer-Verlag, 2006, pp. 266-279.

[7] S. Kavut, S. Maitra, and M. D. Yücel, "Search for Boolean functions with excellent profiles in the rotation symmetric class," IEEE Trans. Inf. Theory, vol. 53, no. 5, pp. 1743-1751, May 2007.
[8] S. Kavut and M. D. Yücel, "Generalized rotation symmetric and dihedral symmetric Boolean functions - 9 variable Boolean functions with nonlinearity 242," in Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (AAECC) (Lecture Notes in Computer Science), vol. 4851. Berlin, Germany: Springer-Verlag, 2007, pp. 321-329.
[9] S. Maitra, S. Kavut, and M. D. Yücel, "Balanced Boolean function on 13-variables having nonlinearity greater than the bent concatenation bound," in Proceedings of the Fourth International Workshop on Boolean Functions: Cryptography and Applications (BFCA), Copenhagen, Denmark, 2008, pp. 109-118.
[10] S. Maitra and P. Sarkar, "Modifications of Patterson-Wiedemann functions for cryptographic applications," IEEE Trans. Inf. Theory, vol. 48, no. 1, pp. 278-284, Jan. 2002.
[11] M. Matsui, "Linear cryptanalysis method for DES cipher," in Advances in Cryptology—EUROCRYPT'93, (Lecture Notes in Computer Science), vol. 765. Berlin, Germany: Springer-Verlag, 1994, pp. 386-397.
[12] W. Meier and O. Staffelbach, "Nonlinearity criteria for cryptographic functions," in Advances in Cryptology—EUROCRYPT'89 (Lecture Notes in Computer Science), vol. 434. Berlin, Germany: Springer-Verlag, 1990, pp. 549-562.
[13] J. Mykkelveit, "The covering radius of the $(128, 8)$ Reed-Muller code is 56," IEEE Trans. Inf. Theory, vol. 26, pp. 359-362, May 1980.
[14] N. J. Patterson and D. H. Wiedemann, "The covering radius of the $(2^{15}, 16)$ Reed-Muller code is at least 16276," IEEE Trans. Inf. Theory, vol. 29, no. 3, pp. 354-356, May 1983, see also the correction in IEEE Trans. Inf. Theory, vol. 36, no. 2, pp. 443, Mar. 1990.
[15] O. S. Rothaus, "On 'bent' functions," Journal of Combinatorial Theory, Ser. A, vol. 20, pp. 300-305, May 1976.
[16] P. Sarkar and S. Maitra, "Construction of nonlinear Boolean functions with important cryptographic properties," in Advances in Cryptology—EUROCRYPT 2000 (Lecture Notes in Computer Sceince), vol. 1807. Berlin, Germany: Springer-Verlag, 2000, pp. 485-506.
[17] 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, Sep. 2004.
[18] S. Sarkar, S. Maitra, "Idempotents in the neighbourhood of Patterson-Wiedemann functions having walsh spectra zeros," Designs, Codes and Cryptography, vol. 49, no. 1-3, pp. 95-103, Dec. 2008.
[19] J. Seberry, X.-M. Zhang, and Y. Zheng, "Nonlinearly balanced Boolean functions and their propagation characteristics," in Advances in Cryptology—CRYPTO'93, (Lecture Notes in Computer Science), vol. 773. Berlin, Germany: Springer-Verlag, 1993, pp. 49-60.
[20] T. Siegenthaler, "Decrypting a class of stream ciphers using ciphertext only," IEEE Trans. Computers, vol. 34, no. 1, pp. 81-85, Jan. 1985.
[21] T. Siegenthaler, "Correlation-immunity of nonlinear combining functions for cryptographic applications," IEEE Trans. Inform. Theory, vol. 30, no. 5, pp. 776-780, Sep. 1984.
[22] G.-Z. Xiao and J. L. Massey, "A spectral characterization of correlation-immune combining functions," IEEE Trans. Inf. Theory, vol. 34, no. 3, pp. 569-571, May 1988.
[23] 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, Apl. 2018.
[24] W.-G. Zhang, 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, Oct. 2014.
[25] W.-G. Zhang and G.-Z. Xiao, "Constructions of almost optimal resilient Boolean functions on large even number of variables," IEEE Trans. Inf. Theory, vol. 55, no. 12, pp. 5822-5831, Dec. 2009.
[26] W.-G. 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.