

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 $2^{28} - 2^{14} + 2^{10} + 2^9$, 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 $n \leq 7$, 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 $n \geq 9$ 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 $n \geq 29$ 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 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 earliest 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 $(29, 0, 2^{28} - 2^{14} + 2^{10} + 2^9)$ 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),

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

where $\lambda_u \in \mathbb{F}_2$, $X = (x_1, \dots, x_n) \in \mathbb{F}_2^n$ and $u = (u_1, \dots, u_n) \in \mathbb{F}_2^n$. 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

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

where $\omega = (\omega_1, \dots, \omega_n) \in \mathbb{F}_2^n$, 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., $W_f(\mathbf{0}_n) = 0$, where $\mathbf{0}_n$ 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 $f_S : S \rightarrow \mathbb{F}_2$ 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 $i = 1, 2, \dots, d$, let S_i be a nonempty subset of \mathbb{F}_2^n so that*

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

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

$$S_i \cap S_j = \emptyset, \quad 1 \leq i < j \leq d. \quad (3)$$

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

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

Then we have

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

Especially, when $d = 2$,

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

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 $i = 1, 2, \dots, d$, 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 $0 \leq wt(\omega) \leq t$ and $1 \leq i \leq d$.*

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),

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

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 $d \geq 3$. By (4),

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

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

$$(P1) \max_{\omega \in \mathbb{F}_2^n} |W_f(\omega)| \ll \sum_{i=1}^d \max_{\omega \in \mathbb{F}_2^n} |FW_{f_{S_i}}(\omega)|;$$

$$(P2) \varepsilon = \max_{\omega \in \mathbb{F}_2^n} |W_f(\omega)| - \max\{\max_{\omega \in \mathbb{F}_2^n} |FW_{f_{S_i}}(\omega)| : i = 1, \dots, d\}$$

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 $f \in \mathcal{B}_n$, $n = 2k + m$, 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 $1 \leq i < j \leq 4$.

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

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

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

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

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

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

Let

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

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 $\alpha = (\alpha_1, \dots, \alpha_{24}) \in \mathbb{F}_2^{24}$ and $\beta \in \mathbb{F}_2^{15}$. The distribution of the fragmentary Walsh

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

spectra of f_{S_1} is calculated as follows:

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

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

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

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

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

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

and

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

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

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

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,

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

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

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

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

$$\begin{aligned}
 FW_{f_{S_3}}(\alpha, \beta) &= \sum_{X_{(1,22)} \in E_3} (-1)^{\alpha_{(1,22)} \cdot X_{(1,22)}} \\
 &\quad \sum_{(X_{(23,24)}, Y) \in \mathbb{F}_2^{17}} (-1)^{(\Phi_3(X_{(1,22)}) + (\alpha_{(23,24)}, \beta)) \cdot (X_{(23,24)}, Y)} \\
 &= \begin{cases} \pm 2^{17}, & (\alpha_{(23,24)}, \beta) \in T_3 \\ 0, & (\alpha_{(23,24)}, \beta) \notin T_3. \end{cases} \\
 &= \begin{cases} \pm 2^{17}, & \beta \in U_1 \cup U_3 \text{ and} \\ & wt(\alpha_{(23,24)}, \beta) \geq 4 \\ 0, & \text{otherwise.} \end{cases} \quad (13)
 \end{aligned}$$

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

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

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

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

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

$$\begin{aligned} \#E_i &\leq \#T_i, \quad 1 \leq i \leq 4 \\ \bigcup_{i=1}^4 S_i &= \mathbb{F}_2^n \end{aligned} \quad (22)$$

and

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

hold simultaneously. By (22), we can build injective mappings Φ_i from E_i to T_i , $i = 1, 2, 3, 4$. Let $X = (x_1, \dots, x_{2k}) \in \mathbb{F}_2^{2k}$

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

$$FW_{f_{S_i}}(\alpha, \beta) = 0, \text{ for } 0 \leq wt(\alpha, \beta) \leq t. \quad (23)$$

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

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

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

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

Let us now proceed to the KY case 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].

$$\begin{aligned} &3740B6A118A1E1965FB902DFD409B0D5 \\ &9C2A4D81E3AD4A3EE59CBDE16BF50A9D \\ &7EC8A68E5AB09902961456E066E8A801 \\ &57C4248E1AF29C803C3CBDF8B5E8812A \end{aligned} \quad (24)$$

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 $1 \leq i < j \leq 4$.

Theorem 2. (KY case:) Let $g \in \mathcal{B}_9$ 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 $n \geq 21$ be an odd number. Let $k = (n - 9)/2$. Let

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

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

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

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

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

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. ■

TABLE III
 $(n, t, 2^{n-1} - 2^{(n-1)/2} + 5 \cdot 2^{(n-11)/2})$ FUNCTIONS FOR ODD $n, 29 \leq n \leq 135$

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 $n, 19 \leq n \leq 123$

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

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 $(29, 0, 2^{28} - 2^{14} + 2^{10} + 2^9)$ 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 $(29, 0, 2^{28} - 2^{14} + 2^{10} + 2^9)$ function.

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

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

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 $\alpha =$

$(\alpha_1, \dots, \alpha_{14}) \in \mathbb{F}_2^{14}$ and $\beta = (\beta_1, \dots, \beta_{15}) \in \mathbb{F}_2^{15}$. We have

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

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

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

We have

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

Let

$$T = \{Y_{(1,13)} \in \mathbb{F}_2^{13} \mid Y \notin U_4 \text{ for any } Y_{(14,15)} \in \mathbb{F}_2^2\}.$$

We can get $\#T = 1074 > 2^8$ by calculation. We construct the third fragmentary function f_{S_3} on S_3 as follows:

$$f_{S_3}(X, Y) = \Phi_3(X_{(8,14)}, y_{14}) \cdot Y_{(1,13)},$$

where Φ_3 is an injective mapping from \mathbb{F}_2^8 to T . We have

$$FW_{f_{S_3}}(\alpha, \beta) = \begin{cases} \pm 2^{13}, & \beta \notin U_4 \text{ and } \Phi^{-1}(\beta_{(1,13)}) \text{ exists} \\ 0, & \text{otherwise.} \end{cases} \quad (28)$$

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

$$|W_f(\alpha, \beta)| \leq \begin{cases} 40 \cdot 2^7 + 2^{13}, & \beta \in U_1, \alpha_{(8,14)} \neq \mathbf{0}_7 \\ 88 \cdot 2^7 + 2^{13}, & \beta \in U_2, \alpha_{(8,14)} \neq \mathbf{0}_7 \\ 168 \cdot 2^7 + 2^{13}, & \beta \in U_3, \alpha_{(8,14)} \neq \mathbf{0}_7 \\ 216 \cdot 2^7, & \beta \in U_4, \alpha_{(8,14)} \neq \mathbf{0}_7 \\ 2^{14} + 2^{13} + 2^{11}, & \alpha_{(8,14)} = \mathbf{0}_7. \end{cases}$$

By (1), $N_f = 2^{28} - 2^{14} + 2^{10} + 2^9$. By (26) and (27), $FW_{f_{S_1}}(\mathbf{0}_{29}) = FW_{f_{S_2}}(\mathbf{0}_{29}) = 0$. Noticing $\mathbf{0}_{15} \notin U_1$, we have $\Phi^{-1}(\beta_{(1,14)}) = \emptyset$, which implies $FW_{f_{S_3}}(\mathbf{0}_{29}) = 0$. By (6), $W_f(\mathbf{0}_{29}) = 0$. 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. 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 , $9 \leq n \leq 19$, 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

This appendix lists a truth table of a PW function.

```

7F3BFF48506482612D288EC86AF94C0FAD2FC8B46BF5DACDC35182280771A739FF68FF73E8F82C5F71
34B02900603A89BED58D0830BD14E82B23983A94F332CD62E24621C6B402345424BDA90A6E9A96F2E
998FCE4ED7D2CEB167D63A8DAD50F263E0ADAI2CBB8C8B09886514AE7EFC843F5A12AA2266A44
7590405752674802E3382567B77B5342AE1E38A39DD052BEA6E703715F3EDC40AB7019AA2A0180B22
EC80A1A293BA9C6FFEA0C79B7337D5E37A6FFC76242D313F60ADB4AE6B3DA301A0A016C5CC74662B
DDCE7A602CD73027DEFCEB2ABEC8E28FFBCD6C262893437BBEFOA13F2CC6B43783058C5B1A35F62AB
59B4E160C873C65BF06785464D7D78D635CF8EF8D57C2929B37449001752512D209324C0E9E4F7
0D1B688A5C4534763EBC5CA3D6ABDD04FB302F255643355305BE3E25384BA9862163D399D3686D51F6
3F26C4C8D7974767436758AB193ADE89001196E93369A71310541BF6F765782DB1C1C3A7E4573EFC1B
0F533B0301791631CE9ECB33F9EFCAC4F886877453832329DDB3572445FF3CEB69B5A8A805FCEB24
FDAC448014A2CA3B9A5808A7808FE78D5255D275EA9A87D0F444D75AE4F277747E216A4530A06B9AD
23B28346A10CEA264942DBC0370AF36CFE1B8F783972D476455B3CAA3843810A5DF9E4D09B0A1588E
97DA6859A1F92739E03EB2F6C88EA817C8FCE096928870B6392969D4F12003A945C00A0C59252F2A
268875C9C43B0CA1402BFA00EDBD2EB056D24F752DE26DF2708E35D46A2714F5F17AB47ADA7666A2E8
40601AD6E7F470BBE90B62A85357656A39CD3B9006D28C940D48A88022ED0A1C8ED9984693534DA6E
BD53CA2D82A1384DDF58215D5B87C827085E2D8688012602A7DEAAA9003FA241F01F577D2049B27D
469F61CA74FDA82F880EDA619B53B5222D10C828E449A739FF7992DC5B13B2CF012D71532B92E5
24DB6A33A62602F58AAF93E6630A8121F5DFD8D6FAA46B3B6B0C1FC3181F630A6079157A318D692AB
2C2AF873168C26C905E466D071FB2DD8B1968057390B6987FB060E529472B9DF32C41676A2C72473
D039ADF58ED08BDB2E614A25DD4A8793F56B3FEF08894034412C15D8DD078F26FAC5A258D91BA507
451FC434027D7FF37AC47ED63FFF92DA8FA7E10FD13F3BAD8221D2CFFFA5A53C54EB240F1BD98E552
4EFDCEED0AC9561C7499AD30EF256B90912950A6BB9AA6CC39856A8A1D05A98C41FDD95491DA17
632324A1B9418FDA79A1DC1F3413CB8547F1FEF13F448DAF7239D1E133B2560B388FFC52847A8EE7
CE6B81606255A763E81FF090A652581D295676B78BFC17E97ACB00A0F010938BC6843AC2932
BA8A5B3EFC267EAB72945582042EEFEB4754F3697749EAC0ABC7152079142D84E1C5C075017A0DFB22
32E81574D8A3D159EC1E143EFD4CF099FF4D1494B0C4B34769CF2F3BFA952E81CE9701B09DCDF483
606113B82827AEDC437EB564B12E26FBFE9D6A841D0ADA0644A4746780FDCC35B5F3A0922DA1B58
8922AC52466C08DE397813E4BCE7646F58A94EEBF8103BEE9C191C6E17E2F8B630A1F78883641
485D56BAF43FDEDD9C9C7E099326FB32A950D23AED878068621E01642454574E866CFBD7C8541
85F343D173F2A8C9F2E1B3D3B09CF9E9F159375B4623979E903F4C973888783EF78E829177272D25
A150F7A168409DC16C3532BE3F0883A0291BB58320BC9E3F3930B60695B8F09584E413A941D949292688
A3B0C4D5E660536A7563209E5FBD10C770035EA04C93F69E90C729E9095A010C14FEF11FFBA4F7
68D386E0AF2342F13706DBD6C2360032EAF58816F1346F8D14ACB7231E6E17C4F8FEDDAB1DD9DC9C7
E1061C5452A11654A6D4497E610944DE3C9070F4BF50384833908B7897A5F59885674A38724615
56BFA8641246411A7460F5DFCB963046476AC36A0E251CE4324A6772C8C7C0A5E5DE5A4F61D
DB7CE47C66D0089E8F8A89DE58537F347A47EBC0C3F3D7AC917DFF182752A3836130C44A80B3161EA
3644040377E1CA6611B577E6BF55231379F32AFC8F76D424B6095D068A46F0E932AE47E0DFBFOCA2E
7338838526D0A7C83FAE51B110A21BA481664BF9496AC8EEB38351B543550896F8C5489C71C0F78E
B58CE682280685E929FD6D69D5CA7147DFBF069E52A7131275E9845D38E9C8A808469131C2A26E
022E1779F609D9F61CBED50FC156CF6090F1904FF9E6820EAC21301D636538927780C33D5A5EFA9
B0194C44643C1DA5A693075CB7668155841553F65BAE4F3C5580F16A2D36FC28E5938688548B8D6FC0B
1A59B98300108BD9B4EA528C48598C363397342C30DBBFFCA93F492F022FFA33F961628E1C26A7
D155FEE316B86243E999601DCBE5E4B99C0E16BD3E133383CFC61C1D6AFF0367BA37DFE6550FD093F
73198403864E156C1B71C91BB4A162C9FB9E1372DF3AD3A1391086E32802536D07C82BAA470653E
460FD3359C98F556A0285BC20F8B77632A96F057CE0FE68F5C827FA34DF8F76BB21E938B8E013
1DF6E55118BE9516C696519EAB6C4ED77C086D74ADE826032E2889083666CA4BC4D076E76CD9A71
754F051458E5D6E70E234FC431BD1A10C4F851D615C8D58E62C4B777E85044A435D5027BE23A67E
67F3A45A3C2DC9C736EB219804AB3D08A4952D8DDCOFA768BC2E34851DCADE9D71E169A9FA2BAEF
E779441D28871BCDD3BF729D6140AA9E3E01F65BAE4F3C5580F16A2D36FC28E5938688548B8D6FC0B
B0BC8C8A8FB8E115FB24CBE0CC0F77FFBCE490BC2280F5F859A8E5041BA6195EDB1861976A54D7E0
B55F163285D9B97EA2280C92D56D7205E4AE88DA48B006692F3DB58482A4A88F7670A85AC20E
4354A278D98CD16CE10DDFED857627869CF80C3311ED6D9C8FF47206176414D0E1BD46E899015E3
4403E3AC6E63D984EDB8EBA514B71E4644530BD6C9F7C56D90921FE9640771C0C6C9F640168D98D4
86F178530FA39DE5631FE74B02EF210E9FBC6142A1975F59F64388CD90DDBB7A0B3E44A488D5C90
0BD468D7483BA3FB86CC02868F5F83F12EA9A98048D3315CF5F5BBD43BBE319691524711F873999F
F2F3D4DB8CA214D0E1751269C6F2E523FE723C54AF31D5E280C0B7EE3AA98B2A4852CDB01242864
2655452A03C7367A79420CE0BF79CFC7316A2A10F328B12724B68F012BE587484205D58B955436
78B21E1BA241F8841FF456D8615E49094E80DB4B9612644D9E39DFCEC118F48156627328838789041
75304162B2D94BDD7424543153A8FADD0C287131795B32EAE3F13AEDA6880205157462301318D26
9BD2303F3F693A7537BF2E97341B94398892F83E23946C5907FFD4C37E976837D6F33765F38C3E3
485FC10B8C9DA047E92490A0503F59A4F38D5A27DE31F532C928DD3FD072AF887621BC3CF35F50B8
6C603F17B0778114A447EACE475C66C710FE45271C618F1566E412CE04A8890662005969DE28A0AD40
9BCA47C738D30244FA7308B74BA09694593519C7AB421120C4D5A237D042C780348984E47D78995F
AC2E4CC9A95950E94670277064EB8B96CD5AACE3AFF0F6497D5B468A984458CC7632F62E0583C39
521D63AE738057660F45F0A13AB6728BF4F58E2D0C49DF626B488D636935DCEA98E2B7B8C158D8E5A
6508D436A46019081A2137FE34B3EF47579F035A9F70AF72AC894D0B803033FFA3FE4C8B2582F8
03F3078481122FC0B71F6BBEED48D5B86846F30478B34F0203D050F6F59DE5C9216B5163DFD7CAD
0EE100708C0999CF4C2F569973752F7C97981AC888A8594CF48770586D33236F6E7D4816736C2D7F5E
941E2A72E2E46DD2460D8BF91389955B4F2FF747D11963CAB5F7B4489B087A7C131497BFAE0F8A0
B41F6E262D9B9F287C1DFB2B92D2754AED01C87AB9BA426E7FA25B3C16D8952A8592CB08A48ED29744
E5CDAD8A7BB2638F39E499E5AC0405224519202961A515378C85A788A93F178801B38D8289020839
1E11044795F621AD8E535297EFC6A50DDF288FF982256A59A04946772D902D80DA797195AA8F12A8
83E5E9A7CFC6A4DDECF5A36813AF3B1306061E5CAAB1B288140016852FDA91CDFE7226460497A565
8249D294B8E8A8ACE9F5A43C7DCE03A760B6149CC4E4BCE4F02F7C736FD14E2A5520E1E93085F8
0727773089B24DE8A9135DA266A803BA9F33C8941F713005629B8E1CDFB65A02A4FFB534DCC19
A93072A072B9E3FE3F135A2655D5C8585ED5CCF04A2F3A4030593FC28DCC4D60298D07941823C44F3FC
5AB2AF5E2605D101335BF6B2C1C5B0BBD4CE0265ADA24A131BDAC02068324E24A551164836110A90
    
```


C54EF13D7E388F95CE283E675127B4460CDEEA2D57EE9911086F9117616BC75BE5A7BF582653642AF4
 6C0FA63518F364C11EAB4E663777255ADC7149324668C05F4514ED513762CD51BD847F46A79A61E635
 D5F7E0B1A150E9F9D150D558771667029AC2748C650DF79CD24710BDE7B0C92BFDADF1A76052C05BF5
 7B4FE3D05024828AAD17D0E569E0A8729402A74EFEDA593F3B7C82D9A88C164F7A7DC3FFD414FE376
 1C0EA688A051AC1CF3DCBFE14688EC385736D8250D555A44458912D7933B1F4086DF49FD013217795
 8605B993E824297432F0951E36895AC4B954031FF196276D992B6510F4ADB43134132FC832FA579FA
 874F8B3B49F1009EA9B734A4B33A3BD7085DCA4E2FA8B9A439A8EBDCF4FB18354737406E4FBD578
 D6161F785507E9B8F04B24068CEBDC9042067A8F8AE7428178F3A6BF17EFCDF8A59449B939860FFB86
 95459C7670CE67BC5CAE4456BD6295B3EC48CF4A7076D0205AF1B7258DD512DC842A5905F383CE3
 7FF87161D872A098C27B74B266C9DCDE5DE4921A24B1C21C01E57EAF96ECF71D78F05BDEE7B23B6C7F
 C7C06EFD6F493F0E5F09FB978259520FCE2A82C56CFE174F8C5A93B6970A69B6A17CC49393E51D3F
 01C23B35DD247E67F2C08E8E84DC7AC6A16D37932B2067C73B7C172EFF620556160D72FCF74929BC308
 2E6F97BA78634288A11B016D9B7ED9524C49FFAE67BE3BAA08BB4A57D596DE774B93FEC02EAA60CB93
 4295C9CF9B7C11E9E71909580C4E1169DCE6E738E2D938E2D516793E2EED3892310D3166118E84CB
 1AC49BF49DDE2C77928973F4F9BBE8FFC10BB9E283ADAC93B46893C83F8A4E22282BE39725E3A31F82
 B2349DD92A5E2E378CEE9277E5BB5AC1E0553B129E75734B89A36CB012559B80C4AE5760E012DDCE163
 A028167EB6C76C4B5D32B2B8BC156812A26587BED9E88E3A1AF13C8BDC48DF1AEBFE7570FFEB3C638
 1AA422CB390D1D6E135C681AFD5541192A4456F75D80B0887C4DFF1D5866501C3CCFF0F1A83D66B35
 48FE3CBA68DC3E45C8B75A64D7E031F59D8262E4F6A4FCEAA7DCFA3F96CCEA9F85C7FB337E6AF1F
 754D975747A380CDF90B2E18381369956D108EE61B6841EEA4DFCC0B6EB2E2828CA3C8E22

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. Mykkelleit, "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 Science), 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.