IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 9, 2020, accepted December 5, 2020, date of publication December 10, 2020, date of current version December 23, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3043601

SAO 1-Resilient Functions With Lower Absolute Indicator in Even Variables

YANJUN LI[1,2,3], HAIBIN KAN[2,4,5,6], (Member, IEEE), JIE PENG[1], AND CHIK HOW TAN[3]
[1]Mathematics and Science College, Shanghai Normal University, Shanghai 200234, China
[2]Shanghai Key Laboratory of Intelligent Information Processing, School of Computer Science, Fudan University, Shanghai 200433, China
[3]Temasek Laboratories, National University of Singapore, Singapore 117411
[4]Fudan-Zhongan Joint Laboratory of Blockchain and Information Security, Shanghai Engineering Research Center of Blockchain, Fudan University, Shanghai 200433, China
[5]Shanghai Institute of Intelligent Electronics and Systems, Fudan University, Shanghai 200433, China
[6]Shanghai Institute for Advanced Communication and Data Science, Fudan University, Shanghai 200433, China

Corresponding author: Haibin Kan (hbkan@fudan.edu.cn)

This work was supported in part by the National Key Research and Development Program of China under Grant 2019YFB2101703; in part by the National Natural Science Foundation of China under Grant 61672166, Grant 61972258, and Grant U19A2066; and in part by the Innovation Action Plan of Shanghai Science and Technology under Grant 20222420800 and Grant 20511102200.

ABSTRACT In 2018, Tang and Maitra presented a class of balanced Boolean functions in n variables with the absolute indicator $\Delta_f < 2^{n/2}$ and the nonlinearity $NL(f) > 2^{n-1} - 2^{n/2}$, that is, f is SAO (strictly almost optimal), for $n = 2k \equiv 2 \pmod 4$ and $n \geq 46$ in [IEEE Ttans. Inf. Theory 64(1):393-402, 2018]. However, there is no evidence to show that the absolute indicator of any 1-resilient function in n variables can be strictly less than $2^{\lfloor (n+1)/2 \rfloor}$, and the previously best known upper bound of which is $5 \cdot 2^{n/2} - 2^{n/4+2} + 4$. In this paper, we concentrate on two directions. Firstly, to complete Tang and Maitra's work for k being even, we present another class of balanced functions in n variables with the absolute indicator $\Delta_f < 2^{n/2}$ and the nonlinearity $NL(f) > 2^{n-1} - 2^{n/2}$ for $n \equiv 0 \pmod 4$ and $n \geq 48$. Secondly, we obtain two new classes of 1-resilient functions possessing very high nonlinearity and very low absolute indicator, from bent functions and plateaued functions, respectively. Moreover, one class of them achieves the currently known highest nonlinearity $2^{n-1} - 2^{n/2-1} - 2^{n/4}$, and the absolute indicator of which is upper bounded by $2^{n/2} + 2^{n/4+1}$ that is a new upper bound of the minimum of absolute indicator of 1-resilient functions, as it is clearly optimal than the previously best known upper bound $5 \cdot 2^{n/2} - 2^{n/4+2} + 4$.

INDEX TERMS Absolute indicator, balanced Boolean functions, nonlinearity, resilient functions, SAO functions.

I. INTRODUCTION

Boolean functions are crucial in symmetric cryptographic systems including the stream ciphers and block ciphers, which are used as nonlinear filters and combiners in stream ciphers, and utilized for designing substitution boxes (S-box) in block ciphers. To against different cryptanalytic attacks, the Boolean functions used in a cryptosystem must satisfy a number of cryptographic criteria, such as balancedness (to avoid statistical dependence between the plaintext and ciphertext), high nonlinearity (to resist the fast correlation attack [19] and the best affine approximation (BAA) [6]), high algebraic degree (to resist the Rønjom-Helleseth attack [20] and the Berlekamp-Massey algorithm [18]), low absolute indicator (to measure the global avalanche characteristics (GAC) of cryptographic functions [31]) and proper order of resiliency etc. In the filter model, it is commonly considered that a resiliency of order 1 is sufficient. While in the combiner model, it requires higher order resiliency for resisting the correlation attacks [22]. Besides, there is a close relationship between 1-order resiliency and the problem of determining the covering radius of the first order Reed-Muller code [14]. But it is challenging to construct a Boolean function with optimal cryptographic criteria as much as possible, as many criteria cannot be optimized simultaneously in the most of cases.

The best nonlinear Boolean functions is bent functions (introduced in [21]), which possess the highest possible Hamming distance to the set of affine functions and have the lowest possible absolute indicator 0. However, it is improper to use bent functions directly in cryptosystem, since they are not balanced and exist only in even variables. Therefore, designing a class of balanced or resilient Boolean functions with higher nonlinearity and lower absolute indicator is desirable. In this direction, there are two long outstanding conjectures as follows:

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

Conjecture 1 [7]: Let $NLB(n)$ denote the maximum nonlinearity of n-variable balanced Boolean functions. Then $NLB(n) \leq 2^{n-1} - 2^{n/2} + NLB(n/2)$, where n is even.

Conjecture 2 [31, Conjecture 1]: The absolute indicator of every n-variable balanced Boolean function, whose algebraic degree is at least 3, is greater than or equal to $2^{\lfloor (n+1)/2 \rfloor}$.

Conjecture 1 is still outstanding, which has been generalized by Zhang *et al.* to the resilient functions. Zhang *et al.* conjectured that the maximum nonlinearity of m-resilient Boolean functions in n variables ($n \geq 8$) is upper bounded by $2^{n-1} - \lfloor 2^{n/2-1} \rfloor - 2^{\lfloor n/4 \rfloor + m-1}$, see [28, Conjecture] or [29, Conjecture 1], which is related to Conjecture 1 when $m = 0$ since $NLN(n/2) \leq 2^{n/2-1} - 2^{n/4-1}$. Conjecture 2 was disproved only for even $n = 10$ [11] and 14 [1], and for odd $n = 9, 11$ [11], $n = 15$ [15] and $n = 21$ [9], [12] before. Until 2018, Tang and Maitra [24] disproved Conjecture 2 for $n \equiv 2 \pmod 4$ and $n \geq 46$ by a modification of $\mathcal{PS}^-$ class of bent functions, and then Kavut *et al.* [13] disproved Conjecture 2 for $n \equiv 0 \pmod 4$ and $n \geq 52$ by a modification of the initial functions in Tang and Maitra's construction. Recently, Tang *et al.* [25] also gave another balanced Boolean functions, which was a modification of Maiorana-McFarland bent functions, to disprove Conjecture 2 for even $n \geq 20$. But there is still no theoretical construction to disprove Conjecture 2 for odd n, and the best result of this case is $\Delta_f = 2^{(n+1)/2}$, see [2].

Then a natural question is whether there are m-resilient ($m \geq 1$) functions in n variables with their absolute indicators strictly less than $2^{\lfloor (n+1)/2 \rfloor}$ or not. However, no matter the balanced Boolean functions given in [13], [24] or in [25], they cannot be transformed into m-resilient ($m \geq 1$) functions, and there is no evidence to show the existence of such functions. Many works on resilient functions are devoted to estimating the nonlinearity or other cryptographic criteria of resilient functions, but seldom considering their absolute indicators (see [4], [5], [16], [23], [27]–[30] and the references therein). Until now, there are only a few works (see [10], [17]) on this topic and the best known upper bound of the minimum absolute indicator of 1-resilient functions on n-variables (n even) is $5 \cdot 2^{n/2} - 2^{n/4+2} + 4$, which was obtained by Ge *et al.* [10] for the calculation of the absolute indicator of 1-resilient functions designed by Zhang and Pasalic in [30], and it turned out that those 1-resilient functions possess the currently highest nonlinearity $2^{n-1} - 2^{n/2-1} - 2^{\lceil n/4 \rceil}$ and lowest absolute indicator $5 \cdot 2^{n/2} - 2^{n/4+2} + 4$.

The aim of this paper is two-fold. Firstly, we give another simpler method to disprove Conjecture 2 for $n \equiv 0 \pmod 4$ and $n \geq 48$, which is more direct and more effective than Kavut *et al.*'s method given in [13]. Secondly, we obtain two new classes of 1-resilient functions having very high nonlinearity and very low absolute indicator, from bent functions and from plateaued functions, respectively. Moreover, we prove that our 1-resilient functions from bent functions possess the currently highest known nonlinearity $2^{n-1} - 2^{n/2-1} - 2^{n/4}$ and possess the currently known lowest absolute indicator $2^{n/2} + 2^{n/4+1}$ simultaneously, which breaks the previously best upper bound of the minimum absolute indicator of 1-resilient functions given by Ge *et al.* in [10], and allows us to give another new smaller upper bound for the minimum absolute indicator of 1-resilient functions.

The rest of this paper is organized as follows. In Section II, we give some basic notations required in this paper and some basic knowledge associated to Boolean functions. In Section III, we present a new method to disprove Conjecture 2 for $n \equiv 0 \pmod 4$ and $n \geq 48$. Section IV is devoted to constructing two classes of SAO 1-resilient functions with the currently best known absolute indicator from bent functions and from plateaued functions, respectively. Finally, Section V concludes the paper.

II. PRELIMINARIES

Throughout the paper, let $\mathbb{F}_2^n$ be the n-dimensional linear space over the finite field $\mathbb{F}_2$ of two elements and let $\mathbb{F}_2^{n*} = \mathbb{F}_2^n \backslash \{0\}$. In order to avoid the confusion, the addition over $\mathbb{F}_2$ is denoted by "$\oplus$", while the additions over $\mathbb{F}_2^n$ ($n > 1$) and $\mathbb{Z}$ are denoted by "+". The set of all *Boolean functions* on $\mathbb{F}_2^n$ is denoted by $\mathcal{B}_n$, which is formed by all the mappings from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. The *Hamming weight* of an n-variable Boolean function f, denoted by $wt(f)$, is defined to be the cardinality of the *support* of f, that is, $wt(f) = \#\{\alpha \in \mathbb{F}_2^n : f(\alpha) \neq 0\}$. We say $f \in \mathcal{B}_n$ is *balanced* if $wt(f) = 2^{n-1}$. The *Hamming distance* of two functions $f, g \in \mathcal{B}_n$ is the number of $x \in \mathbb{F}_2^n$ such that $f(x) \neq g(x)$, whose value is equal to the Hamming weight of $f \oplus g$. Every Boolean function f on $\mathbb{F}_2^n$ can be represented uniquely using many ways [26], where one of the most commonly representations is the multivariate polynomial representation (also called the *algebraic normal form* of f), that is,

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

The algebraic degree of $f \in \mathcal{B}_n$, denoted by $\deg(f)$, is the maximum cardinality of I with $a_I \neq 0$. The function $f \in \mathcal{B}_n$ is said to be *affine* if $\deg(f) \leq 1$.

The *autocorrelation function* of an n-variable Boolean function f is defined as

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

To provide diffusion to the cryptosystems, all the values $|C_f(\alpha)|$ with $\alpha \neq 0$ should be as low as possible. This property can be characterized by the so-called *absolute indicator*.

Definition 1: The absolute indicator of a Boolean function f on $\mathbb{F}_2^n$ is defined by

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

The *Walsh-Hadamard transform* of $f \in \mathcal{B}_n$ is the discrete Fourier transform of the sign function $\chi_f := (-1)^f$ of f, whose value at $\mu \in \mathbb{F}_2^n$ is equal to

$$\widehat{\chi_f}(\mu) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus \mu \cdot x}.$$

Similarly to the support of Boolean functions, we define the set $S_f = \{\mu \in \mathbb{F}_2^n : \widehat{\chi_f}(\mu) \neq 0\}$ to be the *Walsh-Hadamard* *support* of f. A Boolean function f on $\mathbb{F}_2^n$ is called an *r-plateaued* if its Walsh-Hadamard transform $\widehat{\chi_f}(\mu)$ belongs to $\{0, \pm 2^{(n+r)/2}\}$ for any $\mu \in \mathbb{F}_2^n$, where r and n have the same parity, and $0 \le r \le n$. In particular, f is a *bent function* if and only if $r = 0$. Every bent function f admits a unique Boolean function $\widetilde{f} \in \mathcal{B}_n$ such that $\widehat{\chi_f}(\mu) = 2^{n/2}(-1)^{\widetilde{f}(\mu)}$, where $\widetilde{f}$ is usually said to be the *dual* of f. Clearly, $\widetilde{f}$ is also a bent function whose dual is f itself.

An r-plateaued function $f \in \mathcal{B}_n$ is said to be *r-partially bent* if its Walsh-Hadamard support is an affine subspace of $\mathbb{F}_2^n$. Obviously, all affine and quadratic Boolean functions are partially bent functions.

Definition 2: A Boolean function f on $\mathbb{F}_{2^n}$ is said to be an m-resilient function if and only if its Walsh-Hadamard transform at any point $\alpha \in \{\alpha \in \mathbb{F}_{2^n} : 0 \le wt(\alpha) \le m\}$ is equal to zero.

The minimum Hamming distance between f and the set of affine Boolean functions is defined to be the *nonlinearity* of $f \in \mathcal{B}_n$, denoted by $NL(f)$, which can be computed by Walsh-Hadamard transform as

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

We say f is *strictly almost optimal* (SAO) if its nonlinearity is strictly great than $2^{n-1} - 2^{\lfloor n/2 \rfloor}$.

III. ANOTHER METHOD FOR DISPROVING CONJECTURE 2 IN EVEN VARIABLES

In 2018, Tang and Maitra [24] disproved Conjecture 2 for $n \equiv 2 \pmod 4$ and $n \ge 46$ by the following construction:

Construction 1: Let $k \ge 9$ be an odd integer, $n = 2k$ and $\lambda, \mu \in \mathbb{F}_{2^k}^*$. Let f be an n-variable Boolean function defined as

$$f(x, y) = \begin{cases} h_0(y), & \text{if } x = 0 \\ h_1(y), & \text{if } x = \mu \\ Tr_1^k(\frac{\lambda x}{y}), & \text{otherwise} \end{cases}, \qquad (1)$$

where

$$\begin{cases} h_0(y_1, \ldots, y_k) = g_0(y_1, \ldots, y_4) \oplus y_k s_0(y_5, \ldots, y_{k-1}) \\ h_1(y_1, \ldots, y_k) = g_1(y_1, \ldots, y_4) \oplus y_k s_1(y_5, \ldots, y_{k-1}), \end{cases} \qquad (2)$$

g_0 and g_1 are 4-variable Boolean functions defined as [24, Lemma 3], s_0 and s_1 are two quadratic bent functions in $k-5$ variables such that $wt(s_0) = wt(s_1) = 2^{k-6} - 2^{(k-7)/2}$ and $\widetilde{s_0} \oplus \widetilde{s_1}$ is also bent.

Tang and Maitra have proved that the function f in the above construction is a balanced Boolean function satisfying the algebraic degree $\deg(f) = n - 1$, the absolute indicator $\Delta_f < 2^k$ for $k \ge 23$, and the nonlinearity $NL(f) > 2^{n-1} - 2^k$ for $k \ge 11$.

To complete Tang and Maitra's work for any even integer $k \ge 24$, our method is to modify the initial functions h_0 and h_1 of Construction 1, such that

$$\begin{cases} h_0(y_1, \ldots, y_k) = g_0(y_1, \ldots, y_4) \oplus y_k s_0(y_5, \ldots, y_{k-2}), \\ h_1(y_1, \ldots, y_k) = g_1(y_1, \ldots, y_4) \oplus y_{k-1} s_1(y_5, \ldots, y_{k-2}), \end{cases} \qquad (3)$$

where $k \ge 10$ is even, g_0 and g_1 are the same as Construction 1, s_0 and s_1 are two quadratic bent functions in $k-6$ variables such that $wt(s_0) = wt(s_1) = 2^{k-7} - 2^{(k-8)/2}$ and $\widetilde{s_0} \oplus \widetilde{s_1}$ is also bent. Then our result is presented as follows.

Theorem 1: Let $k \ge 10$ be even and $h_0, h_1 \in \mathcal{B}_k$ be defined by (3). Then the function $f \in \mathcal{B}_n$ defined by (1) satisfies:

(1) f is a balanced function of algebraic degree $n-1$;

(2) $\Delta_f < 2^k - 2^{(k+4)/2}$ for $k \ge 24$;

(3) $NL(f) \ge 2^{n-1} - 2^k$ for $k \ge 12$.

Proof: The proof of this theorem is similar to that of [24], we only give a sketch of proof.

Firstly, similarly as that of [24, Lemma 6], for any even integer $k \ge 10$, we can deduce that

(i) $\deg(h_0) = \deg(h_1) = 3$;

(ii) $2^{\frac{k+6}{2}} \le C_{h_0}(\beta) + C_{h_1}(\beta) \le 2^k + 2^{k-1}$ for any $\beta \in \mathbb{F}_2^{k*}$;

(iii) $-2^{k-2} - 2^{k-3} - 9 \cdot 2^{\frac{k}{2}} \le \Lambda \le -2^{k-2} - 2^{\frac{k+2}{2}}$ for any $\beta \in \mathbb{F}_2^k$, where $\Lambda = 2\sum_{y \in \mathbb{F}_2^k} (-1)^{h_0(y) + h_1(y+\beta)}$;

(iv) $\max_{\beta \in \mathbb{F}_2^k} |W_{h_0}(\beta)| = \max_{\beta \in \mathbb{F}_2^k} |W_{h_1}(\beta)| = 3 \cdot 2^{k-3} + 3 \cdot 2^{\frac{k}{2}}$;

(v) $wt(h_0) + wt(h_1) = 2^k$.

Then by (v), it is easily seen that f is balanced, whose algebraic degree can be derived by the same way as that of [24, Theorem 3]. Similarly to the proof of [24, Theorem 1], one can prove (2), and similarly to that of [24, Theorem 2], one can obtain (3). $\square$

Compared Tang and Maitra's main function with ours, the main difference is the definition of h_0 and h_1, see (2) and (3), respectively. Using this way, we transform Tang and Maitra's work into the case of even k, and hence give a complement for their work.

Remark 1: Theorem 1 disproves Conjecture 2 for any $n \equiv 0 \pmod 4$ and $n \ge 48$. It together with [24] disprove Conjecture 2 for any even integer $n \ge 46$.

Remark 2: Notice that the initial functions g_0 and g_1 in Construction 1 are four variables, by changing them into five variables (see [13, Lemma 2]), Kavut et al. [13] also disproved Conjecture 2 for any $n \equiv 0 \pmod 4$ and $n \ge 52$. This was not an easy task as to find another pair of g_0 and g_1 in Construction 1 such that $\Delta_f < 2^k$ is not an easy task. In addition, it increased the variables of g_0 and g_1 making the search more complex. Compared Theorem 1 with Kavut et al.'s work [13], obviously, Theorem 1 is more direct and more effective.

IV. SAO 1-RESILIENT FUNCTIONS WITH THE CURRENTLY LOWEST ABSOLUTE INDICATOR

From the previous section, we know that the absolute indicator of balanced functions on $\mathbb{F}_2^n$ can be strictly less than $2^{\lfloor (n+1)/2 \rfloor}$. However, there is no evidence to show that the absolute indicator of any m-resilient ($m \ge 1$) Boolean functions in n variables can be strictly less than $2^{\lfloor (n+1)/2 \rfloor}$. Many papers of constructing m-resilient functions are mainly focused on the discussions of the nonlinearity and other cryptographic criteria of resilient functions, but seldom consider their absolute indicators, mostly because the analysis of which is rather complicated. Until now, the best upper bound of the minimum absolute indicator of 1-resilient functions in n (n even) variables is $5 \cdot 2^{n/2} - 2^{n/4+2} + 4$, see [10, Theorem 2], which was obtained by computing the absolute indicator of 1-resilient functions obtained by Zhang and Pasalic in [30], and it turned out that the absolute indicator of which is smaller than that of derived by Maitra and Pasalic in [17]. In this section, we will break this limitation and give an even smaller upper bound, by constructing another new class of 1-resilient Boolean functions. Moreover, we will show that our 1-resilient functions can be SAO. For this purpose, the following construction of 1-resilient functions in [30] is required, and the proof of which is included for completeness.

Lemma 1: Let f be an n-variable Boolean function and M be the complement of the Walsh-Hadamard support of f, i.e., $M = \{\alpha \in \mathbb{F}_2^n : \widehat{\chi_f}(\alpha) = 0\}$. If there are n linearly independent vectors $\omega_1, \omega_2, \ldots, \omega_n \in M$ and another vector $\alpha = a_1\omega_1 + a_2\omega_2 + \cdots + a_n\omega_n \in M$ such that $\sum_{i=1}^n a_i \equiv 0 \pmod 2$, where $a_i \in \mathbb{F}_2$ for each $i = 1, \ldots, n$, then f can be transformed into a 1-resilient Boolean function.

Proof: Let $f_0(x) = f(x) \oplus \alpha \cdot x$. Then the Walsh-Hadamard transform of f_0 at $\mu \in \mathbb{F}_2^n$ satisfies $\widehat{\chi_{f_0}}(\mu) = \widehat{\chi_f}(\mu + \alpha)$, which implies that f_0 is balanced as $\alpha \in M$. Observe that the determinant

$$\begin{vmatrix} a_1 \oplus 1 & a_2 & \cdots & a_n \\ a_1 & a_2 \oplus 1 & \cdots & a_n \\ \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & \cdots & a_n \oplus 1 \end{vmatrix} = 1 \oplus \bigoplus_{i=1}^{n} a_i \neq 0,$$

thus the vectors $\alpha + \omega_1, \alpha + \omega_2, \ldots, \alpha + \omega_n$ are linearly independent. Let R be a matrix over $\mathbb{F}_2$ of size $n \times n$ defined as

$$R = \begin{pmatrix} \alpha + \omega_1 \\ \alpha + \omega_2 \\ \vdots \\ \alpha + \omega_n \end{pmatrix} \tag{4}$$

and $f_1(x) = f_0(R^{-1}x)$. Then for any $\mu \in \{\mu \in \mathbb{F}_2^n : 0 \leq wt(\mu) \leq 1\}$, it holds $\widehat{\chi_{f_1}}(\mu) = 0$, since $\widehat{\chi_{f_1}}(\mu) = \widehat{\chi_{f_0}}(R^T\mu)$ for any $\mu \in \mathbb{F}_2^n$, where R^T is the transpose of R. This completes the proof. □

Remark 3: For an n-variable balanced Boolean function f, if there are n linearly independent vectors $\omega_1, \ldots, \omega_n$ belong to M such that $\omega_{i_1} + \omega_{i_2} + \cdots + \omega_{i_e}$ belongs to M for any $1 \leq e \leq m$ and any $1 \leq i_1 < i_2 < \cdots < i_e \leq n$, then similar to the proof of Lemma 1, one can obtain that $f_m(x) = f(A^{-1}x)$ is an m-resilient Boolean function, where A is a matrix over $\mathbb{F}_2$ of size $n \times n$ defined as $A = (\omega_1, \ldots, \omega_n)^T$.

In what follows, we shall give a class of 1-resilient Boolean functions in even variables with the currently highest nonlinearity and lowest absolute indicator by means of Lemma 1. Our main function is presented as follows.

Construction 2: Let $n = 2k$ be an even integer and $s(x, y)$ be a bent function on $\mathbb{F}_2^k \times \mathbb{F}_2^k$ with $s(0, y) = s(x, 0) = \widetilde{s}(0, y) = \widetilde{s}(x, 0) = 0$. Let g and h be two Boolean functions on $\mathbb{F}_2^k$ with $h(0) = 0$. We define a Boolean function f on $\mathbb{F}_2^k \times \mathbb{F}_2^k$ as

$$f(x, y) = s(x, y) \oplus \delta_0(x)g(y) \oplus h(x)\delta_0(y), \tag{5}$$

where $\delta_0(x)$ equals 1 if $x = 0$, and equals 0 otherwise.

We shall choose a pair of suitable (g, h) such that the Boolean function f in Construction 2 can be transformed to a 1-resilient function having very high nonlinearity and very low absolute indicator simultaneously. To this end, it requires first to compute the Walsh-Hadamard transform and the autocorrelation function of f.

Lemma 2: The Walsh-Hadamard transform of f generated in Construction 2 is given by

$$\widehat{\chi_f}(\mu, \nu) = \begin{cases} -2^k + \widehat{\chi_h}(0) + \widehat{\chi_g}(0), & \text{if } \mu = 0, \nu = 0 \\ \widehat{\chi_h}(0) + \widehat{\chi_g}(\nu), & \text{if } \mu = 0, \nu \neq 0 \\ \widehat{\chi_h}(\mu) + \widehat{\chi_g}(0), & \text{if } \mu \neq 0, \nu = 0 \\ 2^k(-1)^{\widetilde{s}(\mu,\nu)} + \widehat{\chi_h}(\mu) + \widehat{\chi_g}(\nu), & \text{otherwise} \end{cases}.$$

Proof: By the definition of Walsh-Hadamard transform, for any $\mu, \nu \in \mathbb{F}_2^k$, we have

$$\begin{aligned} &\widehat{\chi_f}(\mu, \nu) \\ &= \Big(\sum_{x,y \in \mathbb{F}_2^{k*}} + \sum_{x=0, y \in \mathbb{F}_2^k} + \sum_{x \in \mathbb{F}_2^{k*}, y=0} \Big) (-1)^{f(x,y) \oplus \mu \cdot x \oplus \nu \cdot y} \\ &= \Big(\sum_{x,y \in \mathbb{F}_2^k} - \sum_{x=0, y \in \mathbb{F}_2^k} - \sum_{x \in \mathbb{F}_2^{k*}, y=0} \Big) (-1)^{s(x,y) \oplus \mu \cdot x \oplus \nu \cdot y} \\ &\quad + \widehat{\chi_g}(\nu) + \widehat{\chi_h}(\mu) - (-1)^{h(0)}. \end{aligned}$$

Since s is bent with $s(0, y) = s(x, 0) = \widetilde{s}(0, y) = \widetilde{s}(x, 0) = 0$ and $h(0) = 0$, we arrive at

$$\widehat{\chi_f}(\mu, \nu) = 2^k\left((-1)^{\widetilde{s}(\mu,\nu)} - \delta_0(\mu) - \delta_0(\nu)\right) + \widehat{\chi_g}(\nu) + \widehat{\chi_h}(\mu).$$

The result follows. □

Lemma 3: The autocorrelation function of the Boolean function f generated by Construction 2 is given by

$$C_f(\mu, \nu) = \begin{cases} 2^n, & \text{if } \mu = 0, \nu = 0 \\ C_g(\nu) + 2\sum_{x \in \mathbb{F}_2^k} (-1)^{h(x) \oplus s(x,\nu)} \\ \quad -2S(\nu) - 2^k, & \text{if } \mu = 0, \nu \neq 0 \\ C_h(\mu) + 2\sum_{y \in \mathbb{F}_2^k} (-1)^{g(y) \oplus s(\mu,y)} \\ \quad -2S(\mu) - 2^k + 2p(\mu), & \text{if } \mu \neq 0, \nu = 0 \\ 2\sum_{x \in \mathbb{F}_2^k} (-1)^{h(x) \oplus s(x+\mu,\nu)} \\ \quad +2\sum_{y \in \mathbb{F}_2^k} (-1)^{g(y) \oplus s(\mu,y+\nu)} \\ \quad -2S(\nu) - 2S(\mu) + 2q(\mu, \nu), & \text{otherwise} \end{cases},$$

where $p(\mu) = 1 - (-1)^{g(0)} - (-1)^{h(\mu)} + (-1)^{g(0) \oplus h(\mu)}$, $q(\mu, \nu) = 1 - (-1)^{g(\nu)} - (-1)^{h(\mu)} + (-1)^{g(\nu) \oplus h(\mu)}$, $S(\nu) = \sum_{x \in \mathbb{F}_2^k} (-1)^{s(x,\nu)}$ and $S(\mu) = \sum_{y \in \mathbb{F}_2^k} (-1)^{s(\mu,y)}$.

Proof: According to the relationship between μ, ν and 0, the autocorrelation function

$$C_f(\mu, \nu) = \sum_{x,y \in \mathbb{F}_2^k} (-1)^{f(x,y) \oplus f(x+\mu, y+\nu)}$$

can be determined by the following four cases.

Case 1. $\mu = \nu = 0$. Obviously it holds $C_f(\mu,\nu) = 2^n$ in this case.

Case 2. $\mu = 0$, $\nu \neq 0$. In this case we have

$$\begin{aligned} C_f(\mu,\nu) &= \Big(\sum_{x\in\mathbb{F}_2^k, y\in\mathbb{F}_2^k\setminus\{0,\nu\}} + \sum_{x\in\mathbb{F}_2^k, y=0} + \sum_{x\in\mathbb{F}_2^k, y=\nu}\Big) \times (-1)^{f(x,y)\oplus f(x,y+\nu)} \\ &= \Big(\sum_{x\in\mathbb{F}_2^{k*}, y\in\mathbb{F}_2^k\setminus\{0,\nu\}} + \sum_{x=0, y\in\mathbb{F}_2^k\setminus\{0,\nu\}}\Big) \times (-1)^{f(x,y)\oplus f(x,y+\nu)} + 2\sum_{x\in\mathbb{F}_2^k}(-1)^{f(x,0)\oplus f(x,\nu)} \\ &= T_1 + \big(C_g(\nu) - 2(-1)^{g(0)\oplus g(\nu)}\big) + 2\sum_{x\in\mathbb{F}_2^{k*}}(-1)^{h(x)\oplus s(x,\nu)} + 2(-1)^{g(0)\oplus g(\nu)} \\ &= T_1 + C_g(\nu) + 2\sum_{x\in\mathbb{F}_2^k}(-1)^{h(x)\oplus s(x,\nu)} - 2, \end{aligned}$$

where

$$T_1 = \sum_{x\in\mathbb{F}_2^{k*}, y\in\mathbb{F}_2^k\setminus\{0,\nu\}} (-1)^{s(x,y)\oplus s(x,y+\nu)}.$$

Case 3. $\mu \neq 0$, $\nu = 0$. In this case, similarly to the Case 2, one can deduce that

$$C_f(\mu,\nu) = T_2 + C_h(\mu) + 2\sum_{y\in\mathbb{F}_2^k}(-1)^{g(y)\oplus s(\mu,y)} + 2\big[(-1)^{g(0)\oplus h(\mu)} - (-1)^{g(0)} - (-1)^{h(\mu)}\big],$$

where

$$T_2 = \sum_{x\in\mathbb{F}_2^k\setminus\{0,\mu\}, y\in\mathbb{F}_2^{k*}} (-1)^{s(x,y)\oplus s(x+\mu,y)}.$$

Case 4. $\mu \neq 0$, $\nu \neq 0$. In this case, we deduce that

$$\begin{aligned} C_f(\mu,\nu) = T_3 &+ 2\sum_{x\in\mathbb{F}_2^k}(-1)^{h(x)\oplus s(x+\mu,\nu)} + 2\sum_{y\in\mathbb{F}_2^k}(-1)^{g(y)\oplus s(\mu,y+\nu)} + 2\big[(-1)^{g(\nu)\oplus h(\mu)} \\ &- (-1)^{s(\mu,\nu)} - (-1)^{h(\mu)} - (-1)^{g(\nu)}\big], \end{aligned}$$

where

$$T_3 = \sum_{x\in\mathbb{F}_2^k\setminus\{0,\mu\}, y\in\mathbb{F}_2^k\setminus\{0,\nu\}} (-1)^{s(x,y)\oplus s(x+\mu,y+\nu)}.$$

Note that $s(x,y) \oplus s(x+\mu,y+\nu)$ is balanced over $\mathbb{F}_2^k \times \mathbb{F}_2^k$ for any $(\mu,\nu) \neq (0,0)$, so we have

$$\begin{aligned} T_1 &= \Big(\sum_{x,y\in\mathbb{F}_2^k} - \sum_{x\in\mathbb{F}_2^k, y=0} - \sum_{x\in\mathbb{F}_2^k, y=\nu} - \sum_{x=0, y\in\mathbb{F}_2^k\setminus\{0,\nu\}}\Big) \times (-1)^{s(x,y)\oplus s(x,y+\nu)} \\ &= -2\sum_{x\in\mathbb{F}_2^k}(-1)^{s(x,\nu)} - (2^k - 2). \end{aligned}$$

Similarly, one can deduce that

$$T_2 = -2\sum_{y\in\mathbb{F}_2^k}(-1)^{s(\mu,y)} - (2^k-2) \quad \textit{and}$$

$$T_3 = -2\sum_{x\in\mathbb{F}_2^k}(-1)^{s(x,\nu)} - 2\sum_{y\in\mathbb{F}_2^k}(-1)^{s(\mu,y)} + 2[1 + (-1)^{s(\mu,\nu)}].$$

Then the result follows from the calculation by putting T_1, T_2 and T_3 into the above cases. □

Applying Lemma 3 to $s(x,y) = x\cdot y$, we have the following corollary.

Corollary 1: Let s be a bent function over $\mathbb{F}_2^k \times \mathbb{F}_2^k$ defined as $s(x,y) = x\cdot y$ and let f be a Boolean function over $\mathbb{F}_2^k \times \mathbb{F}_2^k$ generated by Construction 2. Then for any $(\mu,\nu) \in \mathbb{F}_2^k \times \mathbb{F}_2^k$, it holds that

$$C_f(\mu,\nu) = \begin{cases} 2^n, & \text{if } \mu=0,\ \nu=0 \\ C_g(\nu) + 2\widehat{\chi}_h(\nu) - 2^k, & \text{if } \mu=0,\ \nu\neq 0 \\ C_h(\mu) + 2\widehat{\chi}_g(\mu) - 2^k + 2p(\mu), & \text{if } \mu\neq 0,\ \nu=0, \\ 2(-1)^{\mu\cdot\nu}(\widehat{\chi}_g(\mu) + \widehat{\chi}_h(\nu)) & \\ +2q(\mu,\nu), & \text{otherwise} \end{cases}$$

where $p(\mu) = 1 - (-1)^{g(0)} - (-1)^{h(\mu)} + (-1)^{g(0)\oplus h(\mu)}$ and $q(\mu,\nu) = 1 - (-1)^{g(\nu)} - (-1)^{h(\mu)} + (-1)^{g(\nu)\oplus h(\mu)}$.

Notice that $p(\mu), q(\mu,\nu) \in \{0,4\}$ for any $\mu,\nu \in \mathbb{F}_2^k$, which can be negligible for $C_f(\mu,\nu)$ when k is larger. So we ignore them in the following discussions.

By Lemma 1 and Lemma 2, to enforce that the Boolean function f in Construction 2 can be transformed into a 1-resilient function, it suffices to find two Boolean functions g and h on $\mathbb{F}_2^k$, and a pair of k linearly independent vectors $\{\omega'_1,\ldots,\omega'_k\}$ and $\{\omega'_{k+1},\ldots,\omega'_n\}$, where $\omega'_i \in \mathbb{F}_2^k$, and a vector $\alpha' = a_1\omega'_1 + \cdots + a_k\omega'_k \in \mathbb{F}_2^k$, such that $\sum_{i=1}^k a_i \equiv 0 \pmod 2$, $\widehat{\chi}_g(\omega'_i) = \widehat{\chi}_g(\alpha') = -\widehat{\chi}_h(0)$ for each $i = 1,\ldots,k$, and $\widehat{\chi}_h(\omega'_i) = -\widehat{\chi}_g(0)$ for each $i = k+1,\ldots,n$. Then, by the proof of Lemma 1, we obtain that

$$f_1(X) = f_0(R^{-1}X) = f(R^{-1}X) \oplus \alpha\cdot R^{-1}X \tag{6}$$

is 1-resilient, where $X = (x,y)$, $\alpha = (0,\alpha') \in \mathbb{F}_2^k \times \mathbb{F}_2^k$, R is defined by (4), $\omega_i = (0,\omega'_i) \in \mathbb{F}_2^k \times \mathbb{F}_2^k$ for $i = 1,\ldots,k$ and $\omega_j = (\omega'_j, 0) \in \mathbb{F}_2^k \times \mathbb{F}_2^k$ for $j = k+1,\ldots,n$.

A. SAO 1-RESILIENT FUNCTIONS FROM BENT FUNCTIONS

In this subsection, we present a class of SAO 1-resilient functions from bent functions.

Theorem 2: Let $n = 2k = 4t$ with $t > 4$ and s be a bent function on $\mathbb{F}_2^k \times \mathbb{F}_2^k$ defined as $s(x,y) = x\cdot y$. Let $g, h \in \mathcal{B}_k$ be two bent functions with $h(0) = \widetilde{h}(0) = 0$ and $g(0) = \widetilde{g}(0) = 1$. Then the Boolean function $f \in \mathcal{B}_n$ generated by Construction 2 can be transformed to a 1-resilient function f_1 satisfying

(1) $\deg(f_1) = k + \max\{\deg(g), \deg(h)\}$;
(2) $NL(f_1) = 2^{n-1} - 2^{k-1} - 2^t$;
(3) $\Delta_{f_1} \le 2^k + 2^{t+1}$.

Proof: By the assumption that g and h are bent functions with $h(0)=\widetilde{h}(0)=0$ and $g(0)=\widetilde{g}(0)=1$, we have

$$\begin{aligned}&\#\{\nu\in\mathbb{F}_2^k:\widehat{\chi}_h(0)+\widehat{\chi}_g(\nu)=0\}\\&=\#\{\mu\in\mathbb{F}_2^k:\widehat{\chi}_h(\mu)+\widehat{\chi}_g(0)=0\}\\&=2^{k-1}+2^{t-1},\end{aligned}$$

since $\widehat{\chi}_g(0)=-2^t$, $\widehat{\chi}_h(0)=2^t$, $\#\{\nu\in\mathbb{F}_2^k:\widehat{\chi}_g(\nu)=-2^t\}=wt(\widetilde{g})=2^{k-1}+2^{t-1}$ and $\#\{\mu\in\mathbb{F}_2^k:\widehat{\chi}_h(\mu)=2^t\}=2^k-wt(\widetilde{h})=2^{k-1}+2^{t-1}$. This implies that there are a pair of k linearly independent vectors $\{\omega'_1,\ldots,\omega'_k\}$ and $\{\omega'_{k+1},\ldots,\omega'_n\}$ such that $\widehat{\chi}_h(0)+\widehat{\chi}_g(\omega'_i)=0$ for each $i=1,\ldots,k$ and $\widehat{\chi}_h(\omega'_j)+\widehat{\chi}_g(0)=0$ for each $j=k+1,\ldots,n$. In addition, there is also a vector $\alpha'=a_1\omega'_1+\cdots+a_k\omega'_k\in\mathbb{F}_2^k$ with $\sum_{i=1}^k a_i\equiv 0\pmod 2$ such that $\widehat{\chi}_h(0)+\widehat{\chi}_g(\alpha')=0$, as $\#\{(a_1,\ldots,a_k)\in\mathbb{F}_2^k:\sum_{i=1}^k a_i\equiv 0\pmod 2\}=2^{k-1}$ and $2^{k-1}+2^{t-1}-k>2^{k-1}$ for any $t>4$. Thus, according to the discussion before this subsection, the function f_1 defined by (6) is a 1-resilient function.

The algebraic degree of f is clearly $k+\max\{\deg(g),\deg(h)\}$. Now we determine the nonlinearity and the absolute indicator of f. By Lemma 2, we obtain that

$$\max_{\mu,\nu\in\mathbb{F}_2^k}|\widehat{\chi}_f(\mu,\nu)|=2^k+2^{t+1},$$

which implies that

$$NL(f)=2^{n-1}-2^{k-1}-2^t.$$

By Corollary 1, we derive that

$$\Delta_f\le 2^k+2^{t+1},$$

since $C_g(\nu)$ and $C_h(\mu)$ are equal to 0 for any $\mu\ne 0$, $\nu\ne 0$, and $2^{t+2}<2^k+2^{t+1}$ for any $t>2$. Note that f_1 and f have the same algebraic degree, the same nonlinearity and the same absolute indicator, the result then follows. □

The 1-resilient functions in Theorem 2 are obviously SAO.

Remark 4: Note that the currently known highest nonlinearity of 1-resilient functions is $2^{n-1}-\lfloor 2^{n/2-1}\rfloor-2^{\lfloor n/4\rfloor}$ [30] and the previously best known upper bound of the minimum absolute indicator of 1-resilient functions is $5\cdot 2^{n/2}-2^{n/4+2}+4$ [10]. Theorem 2 provides a class of 1-resilient functions with the currently highest nonlinearity and the currently lowest absolute indicator simultaneously. Moreover, it also enables us to give another new upper bound for the minimum absolute indicator of 1-resilient functions, which is clearly optimal than $5\cdot 2^{n/2}-2^{n/4+2}+4$.

*Example 1: Let $t=5$, $n=2k=4t=20$. Let $x=(x',x'')\in\mathbb{F}_2^5\times\mathbb{F}_2^5$ and $y=(y',y'')\in\mathbb{F}_2^5\times\mathbb{F}_2^5$, where $x'=(x_1,\ldots,x_5)$, $x''=(x_6,\ldots,x_{10})$, $y'=(y_1,\ldots,y_5)$ and $y''=(y_6,\ldots,y_{10})$. Let $g(y)=y'\cdot y''\oplus 1$ and $h(x)=x'\cdot x''$. Then for the vectors in $\mathbb{F}_2^k$ given as $\omega'_1=\omega'_{11}=(1,0,\ldots,0)$, $\omega'_2=\omega'_{12}=(0,1,\ldots,0),\ldots,\omega'_{10}=\omega'_{20}=(0,0,\ldots,1)$ and $\alpha'=\omega'_1+\omega'_2$, it is easy to verify that $\widehat{\chi}_g(\omega'_i)=\widehat{\chi}_g(\alpha')=-\widehat{\chi}_h(0)=-2^t$ for each $i=1,\ldots,10$ and $\widehat{\chi}_h(\omega'_j)=-\widehat{\chi}_g(0)=2^t$ for each $j=11,\ldots,20$, that is, the conditions (**a**) and (**b**) are satisfied. Let*

$$f(x,y)=x\cdot y\oplus\delta_0(x)g(y)\oplus\delta_0(y)h(x).$$

TABLE 1. The absolute indicator comparison of 1-resilient functions.

n	12	16	20	24	28
[17]	512	8192	131072	20971512	33554432
[10]	292	1220	4996	20228	81412
Ours	80	288	1088	4224	16640

Then

$$f_1(X)=f(R^{-1}X)\oplus\alpha\cdot R^{-1}X$$

is a 1-resilient function, where $X=(x,y)$, R is a matrix defined as $R=(\alpha+\omega_1,\ldots,\alpha+\omega_n)^T$, $\alpha=(0,\alpha')\in\mathbb{F}_2^{10}\times\mathbb{F}_2^{10}$, $\omega_i=(0,\omega'_i)\in\mathbb{F}_2^{10}\times\mathbb{F}_2^{10}$ for $i=1,\ldots,10$ and $\omega_j=(\omega'_j,0)\in\mathbb{F}_2^{10}\times\mathbb{F}_2^{10}$ for $j=11,\ldots,20$. By calculation, we obtain that

$$f_1(x,y)=X'\cdot Y'\oplus\delta_0(X')g(Y')\oplus\delta_0(Y')h(X')\oplus x_1\oplus x_2,$$

where $X'=(x_1\oplus x_2\oplus y_1, x_1\oplus x_2\oplus y_2,\ldots,x_1\oplus x_2\oplus y_{10})\in\mathbb{F}_2^{10}$ and $Y'=(x_2,x_1,x_1\oplus x_2\oplus x_3,x_1\oplus x_2\oplus x_4,\ldots,x_1\oplus x_2\oplus x_{10})\in\mathbb{F}_2^{10}$. Moreover, this function satisfies

$$NL(f_1)=2^{n-1}-2^{k-1}-2^t=523744\ \text{and}$$
$$\Delta_{f_1}=2^k+2^{t+1}=1088.$$

Remark 5: Observe that $t>4$ is needed in the proof of Theorem 2. However, by Example 1, it is easy to see that Theorem 2 also holds for $t>2$ when $g(y',y'')=y'\cdot y''\oplus 1$ and $h(x',x'')=x'\cdot x''$, where $(x',x''),(y',y'')\in\mathbb{F}_2^t\times\mathbb{F}_2^t$.

In [10], the authors gave a table to compare the absolute indicator of their 1-resilient functions with [17]. In the following table, we compare our result with theirs.

From the above table, our result is obviously better than that of [17] and [10]. Note that k is even in Theorem 2. In the following subsection, we will present another class of SAO 1-resilient functions without this restriction.

B. SAO 1-RESILIENT FUNCTIONS FROM PLATEAUED FUNCTIONS

In this subsection, we exhibit a class of SAO 1-resilient functions from plateaued functions.

Theorem 3: Let $k>4$, r_1 and r_2 be three integers with the same parity and $1<r_1,r_2\le k-2$. Let $n=2k$, $s\in\mathcal{B}_n$ be a bent function defined as $s(x,y)=x\cdot y$, $g\in\mathcal{B}_k$ be a balanced r_1-plateaued function and $h\in\mathcal{B}_k$ be a balanced r_2-plateaued function with $h(0)=0$. Then the Boolean function $f\in\mathcal{B}_n$ generated by Construction 2 can be transformed into a 1-resilient function f_1 satisfying

(1) $NL(f_1)\ge 2^{n-1}-2^{k-1}-2^{(k+r)/2}$, where $r=\max\{r_1,r_2\}$;

(2) $\Delta_{f_1}\le 2^{k+1}+2^{(k+r+2)/2}$.

In particular, if g and h are r_1-partially bent and r_2-partially bent, respectively, then $\Delta_{f_1}\le 2^k+2^{(k+r+2)/2}$.

Proof: By Parseval's relation, it is easy to obtain that the cardinality of the Walsh-Hadamard supports of g and h are equal to 2^{k-r_1} and 2^{k-r_2}, respectively, which implies that $\#\{\nu\in\mathbb{F}_2^k:\widehat{\chi}_g(\nu)=0\}=2^k-2^{k-r_1}>2^{k-1}$ and $\#\{\mu\in\mathbb{F}_2^k:\widehat{\chi}_h(\mu)=0\}=2^k-2^{k-r_2}>2^{k-1}$. Then similarly to the proof of Theorem 2, one can show that the function f_1 determined by (6) is a 1-resilient function. Moreover, by

Lemma 2, we have

$$\max_{\mu,\nu\in\mathbb{F}_2^k} |\widehat{\chi}_f(\mu,\nu)| = 2^k+2^{(k+r_1)/2}+2^{(k+r_2)/2} \le 2^k+2^{(k+r+2)/2},$$

which shows that

$$NL(f)\ge 2^{n-1}-2^{k-1}-2^{(k+r)/2}.$$

By Corollary 1, we have

$$\Delta_f \le 2^{k+1}+2^{(k+r+2)/2}.$$

In particular, if g is r_1-partially bent, then by a well known relationship [3] of autocorrelation function and Walsh-Hadamard transform as

$$2^k C_g(\nu)=\sum_{\alpha\in\mathbb{F}_2^k} \widehat{\chi}_g{}^2(\alpha)(-1)^{\nu\cdot\alpha}, \forall\ \nu\in\mathbb{F}_2^k,$$

we deduce that $C_g(\nu)\in\{0,2^k\}$ for any $\nu\in\mathbb{F}_2^k$, since

$$\sum_{\alpha\in\mathbb{F}_2^k} \widehat{\chi}_g{}^2(\alpha)(-1)^{\nu\cdot\alpha}=2^{k+r_1}\sum_{\alpha\in S_g}(-1)^{\nu\cdot\alpha},$$

which equals 2^{2k} if $\nu\in S_f^{\perp}$, and equals 0 otherwise, where $S_g=\{\alpha\in\mathbb{F}_2^k:\widehat{\chi}_g(\alpha)\ne 0\}$ is the Walsh-Hadamard support of g. Similarly, we have $C_h(\mu)\in\{0,2^k\}$ for any $\mu\in\mathbb{F}_2^k$ when h is partially bent. Then from Corollary 1, it is easily obtained that

$$\Delta_f \le 2^k+2^{(k+r+2)/2}.$$

The proof is completed. □

Remark 6: The 1-resilient function f_1 determined by Theorem 3 is SAO for any $1<r<k-2$, and the upper bound of the absolute indicator of 1-resilient functions given by Theorem 3 is also better than the best known bound $5\cdot 2^{n/2}-2^{n/4+2}+4$.

*Example 2: Let $n=2k=10$, $x=(x_1,\ldots,x_5)\in\mathbb{F}_2^5$ and $y=(y_1,\ldots,y_5)\in\mathbb{F}_2^5$. Let $s(x,y)=x\cdot y$, $g(y)=y_1y_2\oplus y_3$ and $h(x)=x_1x_2\oplus x_4$. Then it is easy to check that g and h are two balanced 3-partially bent functions on $\mathbb{F}_2^5$ with $h(0)=0$, and for the vectors in $\mathbb{F}_2^k$ given as $\omega_1'=\omega_6'=(1,0,0,0,0)$, $\omega_2'=\omega_7'=(0,1,0,0,0)$, $\omega_3'=(0,0,1,0,0)$, $\omega_4'=\omega_8'=(0,0,1,1,0)$, $\omega_5'=\omega_{10}'=(0,0,0,0,1)$, $\omega_9'=(0,0,0,1,0)$ and $\alpha'=\omega_1'+\omega_2'$, we have $\widehat{\chi}_g(\omega_i')=\widehat{\chi}_g(\alpha')=\widehat{\chi}_h(0)=0$ for each $i=1,\ldots,5$ and $\widehat{\chi}_h(\omega_j')=\widehat{\chi}_g(0)=0$ for each $j=6,\ldots,10$, that is, the conditions (**a**) and (**b**) are satisfied. Let*

$$f(x,y)=x\cdot y\oplus\delta_0(x)g(y)\oplus\delta_0(y)h(x).$$

Then

$$f_1(X)=f(R^{-1}X)\oplus\alpha\cdot R^{-1}X$$

is a 1-resilient function, where $X=(x,y)$, R is a matrix defined as $R=(\alpha+\omega_1,\ldots,\alpha+\omega_n)^T$, $\alpha=(0,\alpha')\in\mathbb{F}_2^5\times\mathbb{F}_2^5$, $\omega_i=(0,\omega_i')\in\mathbb{F}_2^5\times\mathbb{F}_2^5$ for $i=1,\ldots,5$ and $\omega_j=(\omega_j',0)\in\mathbb{F}_2^5\times\mathbb{F}_2^5$ for $j=6,\ldots,10$. By calculation, we obtain that

$$f_1(x,y)=X'\cdot Y'\oplus\delta_0(X')g(Y')\oplus\delta_0(Y')h(X')\oplus x_1\oplus x_2,$$

where $X'=(x_1\oplus x_2\oplus y_1, x_1\oplus x_2\oplus y_2, x_1\oplus x_2\oplus y_3, y_3\oplus y_4, x_1\oplus x_2\oplus y_5)$, $Y'=(x_2,x_1,x_3\oplus x_4, x_1\oplus x_2\oplus x_4, x_1\oplus x_2\oplus x_5)$. Moreover, this function satisfies

$$NL(f_1)=2^{n-1}-2^{k-1}-2^{(k+3)/2}=480 \text{ and } \Delta_{f_1}=2^k+2^{(k+3+2)/2}=64.$$

Remark 7: A vector $\alpha\in\mathbb{F}_2^n$ is called a linear structure of $f\in\mathcal{B}_n$ if $f(x)\oplus f(x+\alpha)$ is a constant function. To ensure that a particular block cipher is secure, the Boolean functions used in block cipher should have no nonzero linear structure [8]. All SAO 1-resilient functions constructed in this paper clearly satisfy this cryptographic criterion, since an n-variable Boolean function has no nonzero linear structure if and only if its absolute indicator is strictly less than 2^n.

By Corollary 1, to make $|C_f(\mu,\nu)|$ as low as possible for any $(\mu,\nu)\ne(0,0)$, it requires to take $\max_{\mu,\nu\in\mathbb{F}_2^{k*}}\{|C_g(\nu)+2\widehat{\chi}_h(\nu)-2^k|, |C_h(\mu)+2\widehat{\chi}_g(\mu)-2^k|, |\widehat{\chi}_g(\mu)+\widehat{\chi}_h(\nu)|\}$ as low as possible. In particular, if h and g satisfy the following four conditions:

(**a**) there are k linearly independent vectors $\omega_1',\ldots,\omega_k'\in\mathbb{F}_2^k$ and a vector $\alpha'=a_1\omega_1'+\cdots+a_k\omega_k'\in\mathbb{F}_2^k$ such that $\sum_{i=1}^k a_i\equiv 0 \pmod 2$ and $\widehat{\chi}_g(\omega_i')=\widehat{\chi}_g(\alpha')=-\widehat{\chi}_h(0)$ for each $i=1,\ldots,k$;

(**b**) there are k linearly independent vectors $\omega_{k+1}',\ldots,\omega_n'\in\mathbb{F}_2^k$ such that $\widehat{\chi}_h(\omega_i')=-\widehat{\chi}_g(0)$ for each $i=k+1,\ldots,n$;

(**c**) $C_g(\nu)+2\widehat{\chi}_h(\nu)$ and $C_h(\mu)+2\widehat{\chi}_g(\mu)$ are strictly greater than zero and less than 2^{k+1} for any $\mu,\nu\in\mathbb{F}_2^{k*}$;

(**d**) $\max_{\mu,\nu\in\mathbb{F}_2^{k*}}|\widehat{\chi}_h(\nu)+\widehat{\chi}_g(\mu)|<2^{k-1}$.

Then f_1 defined by (6) is a 1-resilient Boolean function with the absolute indicator $\Delta_{f_1}<2^k$. Unfortunately, we do not know whether such functions exist or not, and we do not know how to find them. It would be of great interest and great progress if someone can give a proof or an example to show the existence of g and h satisfying the above 4 conditions, as it implies that the absolute indicator of 1-resilient functions can be strictly less than $2^{n/2}$ as well.

V. CONCLUDING REMARKS

In this paper, we first gave a new method to disprove Conjecture 2 for $n\equiv 0 \pmod 4$ and $n\ge 48$. It turns out that our method is more direct than that of method given by Kavut *et al.* in [13]. Then we presented two new classes of SAO 1-resilient functions having the currently best known absolute indicator, from bent functions and plateaued functions, respectively, which allows us to give another new upper bound (optimal than the previous one given by Ge *et al.* in [10]) of the minimum absolute indicator of 1-resilient functions. Moreover, we derived a class of 1-resilient functions attaining the currently known highest nonlinearity and the currently known lowest absolute indicator simultaneously. However, there is still no evidence to show that there are 1-resilient functions $f\in\mathcal{B}_n$ whose absolute indicator $\Delta_f<2^{\lfloor(n+1)/2\rfloor}$. It would be great interest if someone can find such functions.

REFERENCES

[1] L. Burnett, W. Millan, E. Dawson, and A. Clark, "Simpler methods for generating better Boolean functions with good cryptographic properties," *Australas. J. Combinat.*, vol. 29, pp. 231–248, Mar. 2004.

[2] A. Canteaut, L. Kölsch, and F. Wiemer, "Observations on the DLCT and absolute indicators," Cryptol. ePrint Arch., Tech. Rep., 2019. [Online]. Available: https://eprint.iacr.org/2019/848.pdf

[3] C. Carlet, "Partially-bent functions," *Des., Codes Cryptogr.*, vol. 3, no. 2, pp. 135–145, May 1993.

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

[5] Y. Chen, L. Zhang, Z. Gong, and W. Cai, "Constructing two classes of Boolean functions with good cryptographic properties," *IEEE Access*, vol. 7, pp. 149657–149665, 2019.

[6] C. Ding, G. Xiao, and W. Shan, *The Stability Theory of Stream Ciphers*, vol. 561. Berlin, Germany: Springer, 1991.

[7] H. Dobbertin, "Construction of bent functions and balanced Boolean functions with high nonlinearity," in *Fast Software Encryption*. Berlin, Germany: Springer, 1995, pp. 61–74.

[8] J.-H. Evertse, "Linear structures in blockciphers," in *Advances in Cryptology* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 1988, pp. 249–266.

[9] S. Gangopadhyay, P. H. Keskar, and S. Maitra, "Patterson–Wiedemann construction revisited," *Discrete Math.*, vol. 306, no. 14, pp. 1540–1556, Jul. 2006, doi: 10.1016/j.disc.2005.06.033.

[10] H. Ge, Y. Sun, and C. Xie, "The GAC property of a class of 1-resilient functions with high nonlinearity," *Chin. J. Electron.*, vol. 29, no. 2, pp. 220–227, Mar. 2020.

[11] S. Kavut, S. Maitra, and M. D. Yucel, "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.

[12] S. Kavut, "Correction to the paper: Patterson–Wiedemann construction revisited," *Discrete Appl. Math.*, vol. 202, pp. 185–187, Mar. 2016, doi: 10.1016/j.dam.2015.07.044.

[13] S. Kavut, S. Maitra, and D. Tang, "Construction and search of balanced Boolean functions on even number of variables towards excellent autocorrelation profile," *Des., Codes Cryptogr.*, vol. 87, nos. 2–3, pp. 261–276, Mar. 2019.

[14] F.-J. MacWilliams and N. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.

[15] S. Maitra and P. Sarkar, "Modifications of Patterson-Wiedemann functions for cryptographic applications," *IEEE Trans. Inf. Theory*, vol. 48, no. 1, pp. 278–284, Aug. 2002.

[16] S. Maitra and E. Pasalic, "Further constructions of resilient Boolean functions with very high nonlinearity," *IEEE Trans. Inf. Theory*, vol. 48, no. 7, pp. 1825–1834, Jul. 2002.

[17] S. Maitra and E. Pasalic, "A Maiorana–Mcfarland type construction for resilient functions on variables (n even) with nonlinearity $> 2^{n-1} - 2^{n/2} + 2^{n/2-2}$," *Discrete App. Math.*, vol. 154, no. 2, pp. 357–369, 2006.

[18] J. Massey, "Shift-register synthesis and BCH decoding," *IEEE Trans. Inf. Theory*, vol. IT-15, no. 1, pp. 122–127, Jan. 1969.

[19] W. Meier and O. Staffelbach, "Fast correlation attacks on stream ciphers," in *Advances in Cryptology*. Berlin, Germany: Springer, 1988, pp. 301–314.

[20] S. Ronjom and T. Helleseth, "A new attack on the filter generator," *IEEE Trans. Inf. Theory*, vol. 53, no. 5, pp. 1752–1758, May 2007.

[21] O. Rothaus, "On 'bent' functions," *J. Combinat. Theory A*, vol. 20, pp. 300–305, May 1976.

[22] T. Siegenthaler, "Decrypting a class of stream ciphers using ciphertext only," *IEEE Trans. Comput.*, vol. C-34, no. 1, pp. 81–85, Jan. 1985.

[23] D. Tang, C. Carlet, X. Tang, and Z. Zhou, "Construction of highly nonlinear 1-resilient Boolean functions with optimal algebraic immunity and provably high fast algebraic immunity," *IEEE Trans. Inf. Theory*, vol. 63, no. 9, pp. 6113–6125, Sep. 2017.

[24] D. Tang and S. Maitra, "Construction of n-variable ($n \equiv 2 \bmod 4$) balanced Boolean functions with maximum absolute value in autocorrelation spectra $< 2^{\frac{n}{2}}$," *IEEE Trans. Inf. Theory*, vol. 64, no. 1, pp. 393–402, Jan. 2018.

[25] D. Tang, S. Kavut, B. Mandal, and S. Maitra, "Modifying Maiorana–McFarland type bent functions for good cryptographic properties and efficient implementation," *SIAM J. Discrete Math.*, vol. 33, no. 1, pp. 238–256, Jan. 2019.

[26] Q. Wang, C. Nie, and Y. Xu, "Constructing Boolean functions using blended representations," *IEEE Access*, vol. 7, pp. 107025–107031, 2019.

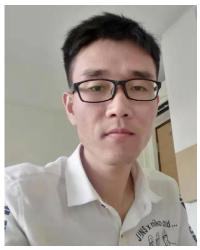
[27] J. Yang, "Constructions of highly nonlinear resilient vectorial Boolean functions via perfect nonlinear functions," *IEEE Access*, vol. 5, pp. 23166–23170, 2017.

[28] W. Zhang and G. 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.

[29] W.-G. Zhang and E. Pasalic, "Generalized Maiorana–McFarland construction of resilient Boolean functions with high nonlinearity and good algebraic properties," *IEEE Trans. Inf. Theory*, vol. 60, no. 10, pp. 6681–6695, Oct. 2014.

[30] W. Zhang and E. Pasalic, "Improving the lower bound on the maximum nonlinearity of 1-resilient Boolean functions and designing functions satisfying all cryptographic criteria," *Inf. Sci.*, vol. 376, pp. 21–30, Jan. 2017.

[31] X.-M. Zhang and Y. Zheng, "GAC—The criterion for global avalanche characteristics of cryptographic functions," in *J.UCS the Journal of Universal Computer Science*. Berlin, Germany: Springer, 1996, pp. 320–337.



YANJUN LI was born in Gansu, China, in 1990. He received the M.S. degree from the Lanzhou University of Technology, Gansu, China, in 2017. He is currently pursuing the Ph.D. degree in mathematics and science with Shanghai Normal University, Shanghai, China. From September 2019 to September 2020, he was with the Temasek Laboratories, National University of Singapore, as a Visiting Research Scientist. His research interests include cryptography and coding theory.

HAIBIN KAN (Member, IEEE) received the Ph.D. degree from Fudan University, Shanghai, China, in 1999. He became a Faculty Member with Fudan University, in 1999. From June 2002 to February 2006, he was with the Japan Advanced Institute of Science and Technology, as an Assistant Professor. In February 2006, he joined Fudan University, where he has been a Full Professor with the School of Computer Science, since April 2006. His research interests include coding theory, cryptography, and computation complexity. He is also the Director of the Shanghai Blockchain Engineering Research Center.

JIE PENG received the Ph.D. degree in mathematics from Fudan University, in 2011. From April 2014 to August 2015, he was with Temasek Laboratories, National University of Singapore, as a Visiting Research Scientist. He is currently an Associate Professor with the College of Mathematics and Science, Shanghai Normal University. His research interests include coding theory and information security.

CHIK HOW TAN received the B.Sc. degree (Hons.) in mathematics from the National University of Singapore, in 1984, and the M.A. and Ph.D. degrees in mathematics from the University of Wisconsin–Madison, USA, in 1990 and 1992, respectively. He is currently a Principal Research Scientist with Temasek Laboratories, National University of Singapore. His research interests include cryptography, discrete mathematics, and information security.