Balanced Boolean Functions with (Almost) Optimal Algebraic Immunity and Very High Nonlinearity

Xiaohu Tang[1], Deng Tang[1], Xiangyong Zeng[2] and Lei Hu[3]

In this paper, we present a class of $2k$-variable balanced Boolean functions and a class of $2k$-variable 1-resilient Boolean functions for an integer $k \geq 2$, which both have the maximal algebraic degree and very high nonlinearity. Based on a newly proposed conjecture by Tu and Deng, it is shown that the proposed balanced Boolean functions have optimal algebraic immunity and the 1-resilient Boolean functions have almost optimal algebraic immunity. Among all the known results of balanced Boolean functions and 1-resilient Boolean functions, our new functions possess the highest nonlinearity. Based on the fact that the conjecture has been verified for all $k \leq 29$ by computer, at least we have constructed a class of balanced Boolean functions and a class of 1-resilient Boolean functions with the even number of variables ≤ 58, which are cryptographically optimal or almost optimal in terms of balancedness, algebraic degree, nonlinearity, and algebraic immunity.

Keywords- Boolean functions, balancedness, algebraic immunity, nonlinearity, algebraic degree, 1-resilient function

1 Introduction

Boolean functions are the building blocks of symmetric cryptographic systems. They are used for S-box designing in block ciphers and utilized as nonlinear filters and combiners in stream ciphers. Generally speaking, before 2003 cryptographic Boolean functions were required to satisfy various criteria simultaneously, mainly balancedness, large algebraic degree, and high nonlinearity. In addition, 1-resilient property is commonly preferred in the filter model [6].

[1]X.H. Tang and Deng Tang are with the Provincial Key Lab of Information Coding and Transmission, Institute of Mobile Communications, Southwest Jiaotong University, Chengdu, China. Email: xhutang@ieee.org, dengtanghome@qq.com.

[2]X. Zeng is with Faculty of Mathematics and Computer Science, Hubei University, Wuhan 430062, China. Email: xzeng@hubu.edu.cn.

[3]L. Hu is the State Key Laboratory of Information Security, Graduate University of the Chinese Academy of Sciences, Beijing 100049, China. Email: hu@is.ac.cn.

In 2003, Courtois and Meier successfully proposed algebraic attacks on several stream ciphers [7]. As a result, a new criterion called algebraic immunity was imposed on cryptographic Boolean functions.

Definition 1 ([20]). *Given two n-variable Boolean functions f and h, h is said to be an annihilator of f if $f \cdot h = 0$. The algebraic immunity $AI(f)$ of Boolean function f is defined to be the minimum algebraic degree of nonzero Boolean functions h such that h is an annihilator of f or $f + 1$.*

For resisting the standard algebraic attack, a Boolean function should have algebraic immunity as high as possible. But in [7] it was proved that $AI(f) \leq \lceil \frac{n}{2} \rceil$ for any n-variable Boolean function f. In this paper, f is said to have optimal algebraic immunity if it achieves the equality, and have almost optimal algebraic immunity if $AI(f) = \lceil \frac{n}{2} \rceil - 1$.

Up to now, several classes of Boolean functions achieving optimal algebraic immunity haven been proposed [3, 4, 9, 16, 17]. However, the nonlinearities of most such functions are often not exceeding $2^{n-1} - \binom{n-1}{\lfloor \frac{n}{2} \rfloor}$, which is almost the worst possible value according to Lobanov's bound [18]. Even when they do exceed it, they are not much larger than this number. Hence, they are insufficient for the resistance to fast correlation attacks.

In 2008, Carlet and Feng presented an infinite class of n-variable balanced Boolean functions with optimal algebraic immunity, maximal algebraic degree, and high nonlinearity $\geq 2^{n-1} - n2^{n/2} \cdot \ln 2 - 1$ [5]. It is the first class of Boolean functions almost satisfying all the cryptographic necessities. In [28], the nonlinearity was further improved to $\max\left\{6\lfloor \frac{2^{n-1}}{2n} \rfloor - 2,\ 2^{n-1} - \left(\frac{\ln 2}{3}(n-1) + \frac{3}{2}\right) 2^{\frac{n}{2}}\right\}$ by Wang *et al.*

Very recently, applying the similar idea to a class of Partial Spread bent functions, Tu and Deng constructed $2k$-variable balanced Boolean functions with maximal algebraic degree, and higher nonlinearity $\geq 2^{n-1} - 2^{n/2-1} - (n/2)2^{n/4} \cdot \ln 2 - 1$ where $n = 2k$ [26]. Most notably, based on a combinatorial conjecture, they were able to show that their Boolean functions possess optimal algebraic immunity. Indeed, they validated the conjecture until $k = 29$. In this sense, a class of functions with the even number of variables $n \leq 58$ was obtained, which is cryptographically optimal in terms of balancedness, algebraic degree, nonlinearity, and algebraic immunity. Later in [27], Tu and Deng constructed a class of 1-resilient Boolean functions with maximal algebraic degree, high nonlinearity, and almost optimal algebraic immunity by a modification.

In this paper, firstly we slightly modify Tu-Deng's method to get a class of $2k$-variable balanced Boolean functions. The new function still maintains optimal algebraic immunity, and maximal algebraic degree. Specifically, the nonlinearity of the new function is dramatically increased to $\geq 2^{n-1} - \sum_{i=0}^{t-1} 2^{\frac{n}{2^{i+1}}-1} - 2^{\frac{m-1}{2}}$ where $n = 2k = 2^t m$ for some positive

integers t and m such that $\gcd(m, 2) = 1$. We believe that the new function achieves the best nonlinearity of the balanced Boolean functions with optimal algebraic immunity since its nonlinearity is as good as the best result of the known balanced Boolean functions. Next, extending our technique to Tu-Deng's 1-resilient function, we also improve the nonlinearity but keep the almost optimal algebraic immunity and maximal algebraic degree unchanged. Even compared with all the known 1-resilient ones without considering the optimality of the algebraic immunity, our function still has better nonlinearity.

The remainder of this paper is organized as follows. In Section 2 we introduce some necessary notations and related results of Boolean functions. In Section 3, firstly we review an iterative construction of balanced Boolean functions with very high nonlinearity by Dobbertin. Next, we give a degree optimized method such that balanced Boolean functions also possess maximal algebraic degree. In Sections 4 and 5, we present our main results.

2 Preliminaries

Throughout this paper, let $\mathbf{F}_2^n$ be the vector space of n-tuples over the field $\mathbf{F}_2 = \{0, 1\}$ of two elements, and $\mathbf{F}_{2^n}$ be the finite field of order 2^n. For a vector $a = (a_1, \cdots, a_n) \in \mathbf{F}_2^n$, its *support* $\mathrm{Supp}(a)$ is the set $\{1 \le i \le n \,|\, a_i = 1\}$, and its *Hamming weight* $\mathrm{wt}(a)$ is defined as the cardinality of its support, i.e., $\mathrm{wt}(a) = |\mathrm{Supp}(a)|$.

2.1 Boolean functions over $\mathbf{F}_2^n$

Let $\mathcal{B}_n$ be the set of Boolean functions of n variables. Normally, a *Boolean function* is defined from $\mathbf{F}_2^n$ into $\mathbf{F}_2$. A basic representation for a Boolean function $f(x_1, \cdots, x_n)$ is given by its truth table, namely the binary string of length 2^n which lists all of its output values, i.e.,

$$f = \big[f(0, 0, \cdots, 0), f(1, 0, \cdots, 0), f(0, 1, \cdots, 0), f(1, 1, \cdots, 0), \cdots, f(1, 1, \cdots, 1)\big].$$

We say that a Boolean function f is *balanced* if its truth table contains an equal number of ones and zeros, that is, if its Hamming weight equals to 2^{n-1}. The *Hamming weight* of f, $\mathrm{wt}(f)$, is defined as the Hamming weight of this string, or in other words, the size of the support $\mathrm{supp}(f) = \{x \in \mathbf{F}_2^n \,|\, f(x) = 1\}$. The *Hamming distance* $\mathrm{d_H}(f, g)$ between two Boolean functions f and g is the Hamming weight of their difference $f + g$, i.e., $\mathrm{d_H}(f, g) = |\{x \in \mathbf{F}_2^n \,|\, f(x) + g(x) = 1\}|$ (by abuse of notation, we use $+$ to denote the addition on $\mathbf{F}_2$, i.e., the XOR, and also for a usual integer addition).

Any Boolean function has a unique representation as a multivariate polynomial over $\mathbf{F}_2$, called the *algebraic normal form* (ANF),

$$f(x_1, \cdots, x_n) = \sum_{u \in \mathbf{F}_2^n} a_u \Big(\prod_{j=1}^{n} x_j^{u_j} \Big)$$

where $a_u \in \mathbf{F}_2$ and $u = (u_1, \cdots, u_n) \in \mathbf{F}_2^n$. The *algebraic degree*, $\deg(f)$, is the number of variables in a highest order term with non zero coefficient, i.e., $\deg(f) = \max\{\mathrm{wt}(u) | a_u \neq 0, u \in \mathbf{F}_2^n\}$. A Boolean function is affine if it is of algebraic degree at most 1. The set of all affine functions is denoted by $\mathbf{A}_n$. To resist the Berlekamp-Massey attack, the Boolean functions used in a cryptographic system should have high algebraic degree [6].

Besides, cryptographic Boolean functions must have high nonlinearity to withstand linear and correlation attacks [1, 11]. The *nonlinearity* of an n-variable function f is its distance from the set of all n-variable affine functions, i.e.,

$$N_f = \min_{g \in \mathbf{A}_n} (\mathrm{d_H}(f, g)).$$

This parameter can also be expressed by means of the Walsh transform. Let $x = (x_1, \cdots, x_n)$ and $a = (a_1, \cdots, a_n)$ both belong to $\mathbf{F}_2^n$ and $a \cdot x = a_1 x_1 + \cdots + a_n x_n$. The *Walsh transform* of an n-variable Boolean function $f(x)$ is an integer valued function over $\mathbf{F}_2^n$ which is defined as

$$W_f(a) = \sum_{x \in \mathbf{F}_2^n} (-1)^{f(x) + a \cdot x}.$$

Consequently, the nonlinearity of f can be equivalently expressed as

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

2.2 Boolean functions over $\mathbf{F}_{2^n}$

Note that $\mathbf{F}_{2^n}$ is isomorphic to $\mathbf{F}_2^n$ by some basis of $\mathbf{F}_{2^n}$ over $\mathbf{F}_2$. In this paper, sometimes for convenience we need another representation of Boolean function over the finite field $\mathbf{F}_{2^n}$. Let α be a primitive element of $\mathbf{F}_{2^n}$. A Boolean function $f(x)$ can be defined from $\mathbf{F}_{2^n}$ to $\mathbf{F}_2$ as

$$[f(0), f(1), f(\alpha), \cdots, f(\alpha^{2^n - 2})],$$

which is equivalent to the truth table from $\mathbf{F}_2^n$ to $\mathbf{F}_2$.

Similarly to ANF of its vector version over $\mathbf{F}_2^n$, the Boolean function over $\mathbf{F}_{2^n}$ can also be uniquely expressed by a univariate polynomial [5]

$$f(x) = \sum_{i=0}^{2^n - 1} a_i x^i$$

where $a_0, a_{2^n-1} \in \mathbf{F}_2$, $a_i \in \mathbf{F}_{2^n}$ for $1 \leq i < 2^n - 1$ such that $a_i = a_{2i(\bmod 2^n-1)}$, and the addition is modulo 2. In [5], it was shown that the algebraic degree $deg(f) = \max\{\mathrm{wt}(i)|a_i \neq 0, 0 \leq i < 2^n\}$.

Besides, over $\mathbf{F}_{2^n}$ the Walsh transform of the Boolean function f can be equivalently defined by

$$W_f(a) = \sum_{x \in \mathbf{F}_2^n} (-1)^{f(x)+tr(ax)}$$

where $tr(x) = \sum_{i=0}^{n-1} x^{2^i}$ is the trace function from $\mathbf{F}_{2^n}$ to $\mathbf{F}_2$.

2.3 $\mathcal{PS}_{ap}$ bent class

Definition 2 ([6]). *A Boolean function $f \in \mathcal{B}_n$ is called bent function if its Walsh transform spectrum is two-valued, i.e., $W_f(a) = \pm 2^{n/2}$ for all $a \in \mathbf{F}_2^n$ where n is necessarily even.*

The nonlinearity of bent function equals $2^{n-1} - 2^{n/2-1}$, which achieves the optimal nonlinearity according to the well-known Parseval's relation $\sum_{a \in \mathbf{F}_2^n} W_f^2(a) = 2^{2n}$. Bent functions are not balanced and they exist only for even number of variables, then they are improper for direct cryptographic use.

The class of bent functions called partial spread (PS) was introduced by Dillon [10], whose supports are the unions of $2^{\frac{n}{2}-1}$ or $2^{\frac{n}{2}-1}+1$ disjoint $\frac{n}{2}$-dimensional subspaces of $\mathbf{F}_2^n$, where n is an even positive integer and "disjoint" means that any two of these subspaces intersect in 0 only. In particular, Dillon exhibited a subclass of PS, denoted by $\mathcal{PS}_{ap}$, in an explicit form.

For $n = 2k$, the finite field $\mathbf{F}_{2^n}$ can be viewed as a 2-dimensional vector space $\mathbf{F}_{2^k} \times \mathbf{F}_{2^k}$ over $\mathbf{F}_{2^k}$, which is equal to the disjoint union of its $2^{\frac{n}{2}} + 1$ lines through the origin. By arbitrarily picking up 2^{k-1} lines except for the origin as the support, Dillon presented the $\mathcal{PS}_{ap}$ bent function class $f(x, y)$ from $\mathbf{F}_{2^n}$ to $\mathbf{F}_2$ as

$$f(x, y) = g\left(\frac{x}{y}\right) \tag{1}$$

where g is a balanced Boolean function on $\mathbf{F}_{2^k}$ with $g(0) = 0$, and $\frac{x}{y}$ is defined to be 0 if

$y = 0$. The function $f(x, y)$ is a bent function since

$$\begin{aligned} W_f(a,b) &= \sum_{x\in\mathbf{F}_{2^k}} \sum_{y\in\mathbf{F}_{2^k}^*} (-1)^{g(x/y)+tr(ax+by)} + \sum_{x\in\mathbf{F}_{2^k}, y=0} (-1)^{tr(ax+by)} \\ &= \sum_{y\in\mathbf{F}_{2^k}^*} (-1)^{tr(by)} \sum_{z\in\mathbf{F}_{2^k}} (-1)^{g(z)+tr(ayz)} + \sum_{x\in\mathbf{F}_{2^k}} (-1)^{tr(ax)} \\ &= \sum_{z\in\mathbf{F}_{2^k}} (-1)^{g(z)} \left[\sum_{y\in\mathbf{F}_{2^k}} (-1)^{tr((b+az)y)} - 1 \right] + \sum_{x\in\mathbf{F}_{2^k}} (-1)^{tr(ax)} \\ &= \sum_{z\in\mathbf{F}_{2^k}} (-1)^{g(z)} \sum_{y\in\mathbf{F}_{2^k}} (-1)^{tr((b+az)y)} + \sum_{x\in\mathbf{F}_{2^k}} (-1)^{tr(ax)} \\ &= \begin{cases} 2^k, & a = 0 \\ 2^k(-1)^{g(b/a)}, & a \neq 0 \end{cases} \end{aligned} \tag{2}$$

where the balanced property of g is used in the fourth identity and fifth identity (for the case of $a = 0$) and $\sum_{y\in\mathbf{F}_{2^k}} (-1)^{tr((b+az)y)} = 0$ unless $z = b/a$ when $a \neq 0$ in the fifth identity.

2.4 Tu-Deng's conjecture

Very recently, based on a combinatorial conjecture, Tu and Deng proved that $\mathcal{PS}_{ap}$ function $f(x, y)$ given in (1) has optimal algebraic immunity by a suitable choice of the support of g.

Conjecture ([26]): Let $k > 1$ be an integer. Denote $\overline{x}$ the binary expansion of the integer $0 \leq x < 2^k - 1$. For any $0 < t < 2^k - 1$, define

$$S_t = \left\{ (a, b) | 0 \leq a, b < 2^k - 1, a + b = t \,(\mathrm{mod} 2^k - 1), \mathrm{wt}(\overline{a}) + \mathrm{wt}(\overline{b}) \leq k - 1 \right\} \tag{3}$$

then $|S_t| \leq 2^{k-1}$.

Proposition 1 ([26]). *Let α be the primitive root of the finite field $\mathbf{F}_{2^k}$. Set $\Delta = \{1, \alpha, \cdots, \alpha^{2^{k-1}-1}\}$. Assume that the conjecture is correct, then the $\mathcal{PS}_{ap}$ bent function $f(x, y)$ given by* (1) *satisfies*

$$AI(f) = \frac{n}{2} = k$$

if Supp$(g) = \Delta$.

Tu and Deng validated the conjecture by computer for $k \leq 29$. Towards this conjecture, some advances have been achieved. In [8, 13], the authors proved it is true in many cases. However, the complete proof remains open.

3 Degree optimized balanced Boolean functions in Dobbertin's construction

Up to now, for the balanced Boolean functions of even variables, Dobbertin's construction provides highest nonlinearity [12]. In this section, we present a degree optimized method for Dobbertin's construction such that balanced Boolean functions have both highest nonlinearity and maximal algebraic degree.

From now on, let $\mathbf{0}_n$ and $\mathbf{1}_n$ be the all zero and one vectors of dimension n respectively.

Definition 3 ([12]). *A $2n$-variable Boolean function u is said to be normal if $u(x,y)=0$ on an affine subspace W with dimension n. Without loss of generality, W can be assumed to be $\{x=\mathbf{0}_n, y\in\mathbf{F}_2^n\}$, i.e., $u(\mathbf{0}_n,y)=0$ for all $y\in\mathbf{F}_2^n$.*

Based on normal bent functions, Dobbertin proposed an iterative method for constructing balanced Boolean function with very high nonlinearity [12].

Dobbertin's iterative construction [12]: Let n be even integer no less than 4. Write $n=2^t m$ such that $t\geq 1$ and m is an odd integer. Then a balanced Boolean function $u(x,y)\in\mathcal{B}_n$ over $\mathbf{F}_2^n$ is defined by

$$u(x,y)=\begin{cases} u_0(x,y), & \text{if } x\neq \mathbf{0}_{\frac{n}{2}} \\ v_1(y), & \text{if } x=\mathbf{0}_{\frac{n}{2}} \end{cases} \tag{4}$$

where $u_0(x,y)$ is an n-variable normal bent function and v_1 is generated by an iterative procedure as

$$v_i(x,y)=\begin{cases} u_i(x,y), & \text{if } x\neq \mathbf{0}_{\frac{n}{2^{i+1}}} \\ v_{i+1}(y), & \text{if } x=\mathbf{0}_{\frac{n}{2^{i+1}}}, \end{cases} \quad i=1,\cdots, \tag{5}$$

where $x,y\in\mathbf{F}_2^{\frac{n}{2^{i+1}}}$. The iterative process will continue until $i=t-1$ with $v_t=s\in\mathcal{B}_m$ being a balanced m-variable Boolean function with $\max_{a\in\mathbf{F}_2^m}|W_s(a)|\leq 2^{\frac{m+1}{2}}$ and $s(0)=0$. In each iterative step for $1\leq i<t$, u_i is an $\frac{n}{2^i}$-variable normal bent function.

Theorem 1 ([12]). *Let u be the balanced Boolean function given by (4) and (5), then*

$$\max_{a\in\mathbf{F}_2^n}|W_u(a)|\leq\sum_{i=0}^{t-1}2^{\frac{n}{2^{i+1}}}+2^{\frac{m+1}{2}}.$$

That is,

$$N_u\geq 2^{n-1}-\sum_{i=0}^{t-1}2^{\frac{n}{2^{i+1}}-1}-2^{\frac{m-1}{2}}.$$

However, the algebraic degree of u in (4) was not considered in [12]. In what follows, we discuss it.

Lemma 1 ([31]). *Let $u \in \mathcal{B}_n$ and $a = (a_1, \cdots, a_n)$ be a vector in $\mathbf{F}_2^n$. Then the term $x_1^{a_1} \cdots x_n^{a_n}$ appears in u if and only if $\sum_{\gamma \preceq a} u(\gamma) = 1$ where $\gamma \preceq a$ means $Supp(\gamma) \subseteq Supp(a)$ and the addition is taken modulo 2.*

Lemma 2. *Let $s \in \mathcal{B}_k$ with $deg(s) = d$, $1 \leq d \leq k$. Let $v(x, y)$ be a $2k$-variable normal Boolean function with $deg(v) < k + d$. Then the $2k$-variable Boolean function defined by*

$$u(x,y) = \begin{cases} v(x,y), & \text{if } x \neq \mathbf{0}_k \\ s(y), & \text{if } x = \mathbf{0}_k \end{cases}$$

has $deg(u) = k + d$.

***Proof*:** Without loss of generality, we assume that the term $y_1 \cdots y_d$ appears in the ANF of $s(x)$, which implies that $\sum_{\gamma \preceq (\mathbf{1}_d \mathbf{0}_{k-d})} s(\gamma) = 1$ by Lemma 1. Applying Lemma 1 to the function u, we have

$$\begin{aligned} & \sum_{\gamma \preceq (\mathbf{1}_k, \mathbf{1}_d \mathbf{0}_{k-d})} u(\gamma) \\ = & \sum_{\gamma_1 \neq 0, \gamma_1 \preceq \mathbf{1}_k, \gamma_2 \preceq (\mathbf{1}_d \mathbf{0}_{k-d})} u(\gamma_1, \gamma_2) + \sum_{\gamma_1 = 0, \gamma_2 \preceq (\mathbf{1}_d \mathbf{0}_{k-d})} u(\gamma_1, \gamma_2) \\ = & \sum_{\gamma_1 \preceq \mathbf{1}_k, \gamma_2 \preceq (\mathbf{1}_d \mathbf{0}_{k-d})} v(\gamma_1, \gamma_2) + \sum_{\gamma_1 = 0, \gamma_2 \preceq (\mathbf{1}_d \mathbf{0}_{k-d})} s(\gamma_2) \\ = & \sum_{\gamma_1 = 0, \gamma_2 \preceq (\mathbf{1}_d \mathbf{0}_{k-d})} s(\gamma_2) \\ = & \ 1 \end{aligned}$$

where we make use of the fact that $v(\gamma_1, \mathbf{0}_k) = 0$ in the second identity since v is a normal Boolean function and the fact that

$$\sum_{\gamma_1 \preceq \mathbf{1}_k, \gamma_2 \preceq (\mathbf{1}_d \mathbf{0}_{k-d})} v(\gamma_1, \gamma_2) = 0$$

in the third identity again by Lemma 1 since $deg(v) < k + d$. That is, $deg(u) \geq k + d$.

Further, by a similar argument we can conclude that $\sum_{\gamma \preceq \delta} u(\gamma) = 0$ for all vectors $\delta \in \mathbf{F}_2^k$ with $\mathrm{wt}(\delta) > k + d$, which indicates $deg(u) \leq k + d$. Hence, $deg(u) = k + d$.

□

Rothaus's inequality states that any n-variable bent function has algebraic degree at most $n/2$ when $n \geq 4$ [22]. When $n = 2$, obviously bent function $u(x_1, x_2)$ has $deg(u) = 2$.

That is, all the bent functions $u_i(x, y)$ in (4) and (5), $0 \leq i < t$, satisfy the hypothesis of Theorem 2 except for the case that $m = 1$ and $i = t - 1$.

For the balanced function, we have the following result on its algebraic degree.

Lemma 3 ([23]). *For a balanced Boolean function $f \in \mathcal{B}_n$, $deg(f) \leq n - 1$ for $n \geq 2$.*

Therefore, sequentially applying Lemma 2 to the Boolean functions $v_i(x, y)$, $i = t - 1, \cdots, 0$ if $m > 1$ otherwise $i = t - 2, \cdots, 0$, and then $u(x, y)$ in (4), we can get the Boolean function with maximal algebraic degree by the Dobbertin's construction.

Theorem 2. *Suppose that $deg(v_{t-1}) = 1$ when $m = 1$ and $deg(s) = m - 1$ when $m > 1$. Let u be the balanced Boolean function iteratively generated by (4) and (5). Then,*

$$deg(u) = n - 1,$$

which is optimal by Lemma 3.

By means of Theorems 1 and 2, we are able to construct balanced function $u \in \mathcal{B}_n$ with both maximal algebraic degree $n - 1$ and very high nonlinearity. The key is to have

1. 2-variable balanced function v_{t-1} has algebraic degree 1 when $m = 1$; and
2. m-variable balanced function s with maximal algebraic degree $m - 1$ and very high nonlinearity when $m > 1$.

Straightforwardly, when $m = 1$, it is easy to verify that $s(x) = x$ yields the desirable 2-variable balanced function $v_{t-1}(x, y) = x$ by choosing $u_{t-1}(x, y) = x \cdot y$. For the case of $m > 1$, many such functions can be obtained from the Maiorana-McFarland bent class construction or its modifications in [23]. But, as pointed out in [2], there may exist a weakness in these functions as the derived functions, by fixing certain input bits of these functions, are affine. To avoid this drawback, Zeng and Hu have constructed balanced n-variable Boolean functions with a high nonlinearity and an optimal algebraic degree $n - 1$ for $n \geq 6$, by modifying the Maiorana-McFarland's superclass functions [29].

Then, employing the following m-variable Boolean function s:

- $s(x) = x$ is the 1-variable balanced function with with $\max_{a \in \mathbf{F}_2} |W_s(a)| = 2$ and $deg(s) = 1$;
- s is a balanced semi-bent function on $\mathbf{F}_2^3$ for $m = 3$ with $\max_{a \in \mathbf{F}_2^3} |W_s(a)| = 4$ and $deg(s) = 2$;

- $s = x_2x_3x_4+x_3x_4x_5+x_1x_2x_5+x_2x_4x_5+x_2x_3x_5+x_1x_3x_5+x_1+x_1x_2+x_5+x_1x_2x_3x_5+x_2x_5+x_4x_5$ is a balanced Boolean fucntion of 5 variables with $\max_{a\in\mathbf{F}_2^3}|W_s(a)| = 8$ and $deg(s) = 4$;
- s is a balanced function on $\mathbf{F}_2^m$ given in [29] for $m \geq 7$ with $\max_{a\in\mathbf{F}_2^m}|W_s(a)| = 2^{\frac{m+1}{2}}$ and $deg(s) = m-1$.

we can construct n-variable balanced Boolean function with $N_u \geq 2^{n-1} - \sum_{i=0}^{t-1} 2^{\frac{n}{2^{i+1}}-1} - 2^{\frac{m-1}{2}}$ from Theorem 1 and the maximal algebraic degree $n-1$ from Theorem 2, where $n = 2^t m$ and $\gcd(m, 2) = 1$. In the forthcoming sections, the function u will be used in our constructions. It should be noted that $u(0) = 0$ which follows from the fact that $s(0) = 0$.

Furthermore, it is possible to improve the nonlinearity by taking s as the balanced function proposed in [19, 24], which has the highest nonlinearity among all the known balanced functions of odd variables. However, in view that its algebraic degree is unknown yet, we can modify it to get the balanced functions s by the following degree optimization method by Sarkar and Maitra.

Lemma 4 ([23]). *Given a balanced function $f \in \mathcal{B}_n$ with nonlinearity N_f, one can construct balanced function $f' \in \mathcal{B}_n$ with nonlinearity $N_{f'} = N_f - 2$ and $deg(f') = n-1$.*

In contrast to the original one, the resultant s has the maximal algebraic degree but little decrease of nonlinearity by 2. Table 1 summarizes these nonlinearity values.

Table 1. Summary of the best nonlinearity results for odd $n \geq 13$

n	13	15	$n \geq 17$
Semi-bent function	4032	16256	$2^{n-1} - 2^{\frac{n-1}{2}}$
Balanced function in [19, 24]	4036	16272	$2^{n-1} - 2^{\frac{n-1}{2}} + 16 \cdot 2^{\frac{n-15}{2}}$
Balanced function s	4034	16270	$2^{n-1} - 2^{\frac{n-1}{2}} + 16 \cdot 2^{\frac{n-15}{2}} - 2$

4 Balanced Boolean functions with optimal algebraic immunity, maximal algebraic degree, and very high nonlinearity

From now on, we always assume that α is a primitive root of the finite field $\mathbf{F}_{2^k}$, and the set $\Delta = \{1, \alpha, \cdots, \alpha^{2^{k-1}-1}\}$.

Construction 1: Let $n = 2k = 2^t m$ be an even integer no less than 4 such that $t \geq 1$ and $\gcd(m, 2) = 1$. Over $\mathbf{F}_{2^n}$ construct

$$F(x, y) = \begin{cases} g(x/y), & x \neq 0 \text{ or } (x = 0 \text{ and } y = 0) \\ u(y), & \text{else} \end{cases}$$

where $\mathrm{Supp}(g) = \Delta$ and $u(y)$ is the balanced Boolean function over $\mathbf{F}_{2^k}$ discussed in the last section satisfying $u(0) = 0$, $deg(u) = k-1$, and $\max_{a\in\mathbf{F}_2^k} |W_u(a)| \le \sum_{i=1}^{t-1} 2^{\frac{n}{2^{i+1}}} + 2^{\frac{m+1}{2}}$.

The fact $\mathrm{wt}(F) = \mathrm{wt}(g) + \mathrm{wt}(u) = \mathrm{wt}(g) + 2^{k-1} = 2^{k-1}(2^k-1) + 2^{k-1} = 2^{n-1}$ implies that F is balanced.

4.1 Algebraic immunity and algebraic degree of the constructed functions

In contrast to the specific $\mathcal{PS}_{ap}$ bent functions in Proposition 1 by Tu-Deng, $F(x,y)$ given by Construction 1 is almost the same except that the all zero function over $x = 0$ and $y \in \mathbf{F}_{2^k}^*$ is replaced by a balanced function s. But the change does not effect the optimality of the algebraic immunity.

Theorem 3. *Let $F(x,y)$ be the n-variable Boolean function generated by Construction 1. If Tu-Deng's conjecture is true, then $AI(F) = \frac{n}{2}$.*

***Proof*:** The proof is the same as that of Proposition 1 in [26]. For completeness, we describe a sketch.

Let $h(x,y) = \sum_{i=0}^{2^k-1}\sum_{j=0}^{2^k-1} h_{i,j}x^i y^j$, $h_{i,j} \in \mathbf{F}_2^k$, be a polynomial from $\mathbf{F}_{2^k} \times \mathbf{F}_{2^k} \to \mathbf{F}_2$. Assume that $deg(h) < k$. Then, $h_{2^k-1,t}$ and $h_{t,2^k-1}$ have to be 0 for all $0 \le t < 2^k$, otherwise $deg(h) = k$ by the definition since $\mathrm{wt}(t) + \mathrm{wt}(2^k-1,t) = k$. Thus, we can rewrite the polynomial $h(x)$ as

$$h(x,y) = \sum_{i=0}^{2^k-2}\sum_{j=0}^{2^k-2} h_{i,j}x^i y^j,$$

where $h_{i,j} \in \mathbf{F}_2^k$.

R1. If h is an annihilator of F, then $h(\gamma y, y) = 0$ for all $\gamma \in \Delta$ and $y \in \mathbf{F}_{2^k}^*$. By some manipulations, it follows that

$$h_t(\gamma) = \sum_{i=0}^{2^k-2} h_{i,t-i}\gamma^i = 0,$$

for $1 \le t < 2^k - 1$ and $\forall\, \gamma \in \Delta$. In fact, $\hbar = (h_{0,t}, \cdots, h_{t,0}, h_{t+1,2^k-2}, \cdots, h_{2^k-2,t+1})$ is a $2k$-ary BCH code of length 2^k-1 with designed distance $2^{k-1}+1$. According to the well-known BCH bound, then $\mathrm{wt}(\hbar) \ge 2^{k-1}+1$ if $\hbar$ is nonzero codeword, which contradicts the conjecture.

R2. If h is an annihilator of $F+1$, then it indicates $h(x,0)=0$ for $x \in \mathbf{F}_{2^k}$, i.e., $h_{t,0}=0$, $1 \le t < 2^k-1$. Additionally, it results in $h_t(\gamma)=0$, $1 \le t < 2^k-1$ and $\forall\, \gamma \in \mathbf{F}_{2^k} \setminus \Delta$. Then, $\hbar = (h_{0,t}, \cdots, h_{t,0}, h_{t+1,2^k-2}, \cdots, h_{2^k-2,t+1})$ is a $2k$-ary BCH code of length 2^k-1 with designed distance 2^{k-1}, having $\mathrm{wt}(\hbar) \ge 2^{k-1}$ if $\hbar \neq \mathbf{0}_{2^k-1}$. But by the conjecture and $h_{t,0}=0$, the weight should be less than 2^{k-1}, a contradiction.

Summarized from the above two cases, both F and $F+1$ have no annihilators with algebraic degrees less than k. According to bound that $AI(F) \le \lceil \frac{n}{2} \rceil = k$, $AI(F)$ then equals k achieving the optimal algebraic immunity.

□

By Lemma 2, the function $F(x,y)$ possesses the maximal algebraic degree as well.

Theorem 4. *Let $F(x,y)$ be the n-variable Boolean function generated by Construction 1, then $deg(F) = n-1$.*

4.2 Nonlinearity

In this subsection, we show that $F(x,y)$ has very high nonlinearity.

Theorem 5. *Let $F(x,y)$ be the n-variable Boolean function generated by Construction 1, then*

$$\max_{a,b \in \mathbf{F}_{2^k}} |W_F(a,b)| \le \sum_{i=0}^{t-1} 2^{\frac{n}{2^{i+1}}} + 2^{\frac{m+1}{2}}.$$

That is,

$$N_F \ge 2^{n-1} - \sum_{i=0}^{t-1} 2^{\frac{n}{2^{i+1}}-1} - 2^{\frac{m-1}{2}}$$

***Proof*:** The Fourier transform of the $\mathcal{PS}_{ap}$ function $f(x,y)$ in (2) can be rewritten as

$$\begin{aligned}
W_f(a,b) &= \sum_{x \in \mathbf{F}_{2^k}^*} \sum_{y \in \mathbf{F}_{2^k}} (-1)^{f(x,y)+tr(ax+by)} + \sum_{x=0, y \in \mathbf{F}_{2^k}} (-1)^{f(x,y)+tr(ax+by)} \\
&= \sum_{x \in \mathbf{F}_{2^k}^*} \sum_{y \in \mathbf{F}_{2^k}} (-1)^{g(x/y)+tr(ax+by)} + \sum_{x=0, y \in \mathbf{F}_{2^k}} (-1)^{tr(ax+by)} \\
&= W_T(a,b) + \sum_{y \in \mathbf{F}_{2^k}} (-1)^{tr(by)} \\
&= \begin{cases} W_T(a,0) + 2^k, & b=0 \\ W_T(a,b), & b \neq 0 \end{cases}
\end{aligned}$$

where $W_T(a,b) = \sum_{x \in \mathbf{F}_{2^k}^*} \sum_{y \in \mathbf{F}_{2^k}} (-1)^{g(x/y)+tr(ax+by)}$.

Associating (2) and the above equation, we get

$$W_T(a,b) = \begin{cases} 0, & a=b=0 \\ 2^k, & a=0, b\neq 0 \\ 0, & a\neq 0, b=0 \\ \pm 2^k, & a\neq 0, b\neq 0 \end{cases}$$

Then for the new function $F(x,y)$ generated by Construction 1, clearly

$$\begin{aligned} |W_F(a,b)| &= \left| \sum_{x\in \mathbf{F}_{2^k}^*} \sum_{y\in \mathbf{F}_{2^k}} (-1)^{F(x,y)+tr(ax+by)} + \sum_{x=0, y\in \mathbf{F}_{2^k}} (-1)^{F(x,y)+tr(ax+by)} \right| \\ &= \left| \sum_{x\in \mathbf{F}_{2^k}^*} \sum_{y\in \mathbf{F}_{2^k}} (-1)^{g(x/y)+tr(ax+by)} + (-1)^{F(0,0)} + \sum_{y\in \mathbf{F}_{2^k}^*} (-1)^{u(y)+tr(by)} \right| \\ &= \left| \sum_{x\in \mathbf{F}_{2^k}^*} \sum_{y\in \mathbf{F}_{2^k}} (-1)^{g(x/y)+tr(ax+by)} + 1 + \sum_{y\in \mathbf{F}_{2^k}^*} (-1)^{u(y)+tr(by)} \right| \\ &= |W_T(a,b) + W_u(b)| \\ &\leq |W_T(a,b)| + |W_u(b)| \\ &= \sum_{i=0}^{t-1} 2^{\frac{n}{2^{i+1}}} + 2^{\frac{m+1}{2}}, \end{aligned}$$

where $F(0,0)=0$ and $u(0)=0$ are used in the third and fourth identity. This completes the proof.

□

In Theorem 5, our lower bound is based on the k-variable balanced functions generated from Dobbertin's iterative construction by choosing s as an m-variable semi-bent function. As mentioned in Section 3, the nonlinearity can be increased by employing the balanced function s in Table 1.

4.3 Comparison with the known results

For convenience, let $N_1 = 2^{n-1} - \frac{2\ln 2}{\pi} n 2^{\frac{n}{2}}$, $N_2 = 2^{n-1} - 2^{\frac{n}{2}-1} - \frac{\ln 2}{2} n 2^{\frac{n}{4}} - 1$, $N_3 = \max\left\{ 6\lfloor \frac{2^{n-1}}{2n} \rfloor - 2, 2^{n-1} - \left(\frac{\ln 2}{3}(n-1) + \frac{3}{2}\right) 2^{\frac{n}{2}} \right\}$ denote the lower bounds of the nonlinearity of the results in [5], [26], [28], respectively, where $n = 2^t m$ with $\gcd(2,m)=1$.

Roughly speaking, our $N_F = 2^{n-1} - \sum_{i=0}^{t-1} 2^{\frac{n}{2^{i+1}}-1} - 2^{\frac{m-1}{2}}$ is much better than N_1, N_2, and N_3. More precisely, by a tedious computation we can verify that N_F is larger than N_1, N_2, and N_3 if $n \geq 4$. In [5], [26], and [28], some concrete values of the nonlinearity were

given, which are respectively denoted by $\mathcal{N}_1$, $\mathcal{N}_2$, and $\mathcal{N}_3$ for short, which are much better than their bounds. For comparison, we list our N_F for even $4 \leq n \leq 18$ in Table 2.

Table 2. Comparison of the nonlinearity of balanced Boolean functions (n even)

n	$\mathcal{N}_1 = \mathcal{N}_3$ in [5, 28]	$\mathcal{N}_2$ in [26]	Our result N_F
4	4	4	4
6	24	26	26
8	112	116	116
10	478	490	492
12	1970	2008	2010
14	8036	8118	8120
16	32530	32624	32628
18	130442	130792	130800

5 1-Resilient functions with high nonlinearity and almost optimal algebraic immunity

In this section, we modify Construction 1 to obtain Boolean function with 1-resilient property at the cost of a little decrease of its algebraic immunity.

Definition 4 ([6]). *A Boolean function $f \in \mathcal{B}_n$ is called* 1*-resilient if the Walsh transform $W_f(a) = 0$ for all $a \in \mathbf{F}_2^n$ satisfying* $\mathrm{wt}(a) \leq 1$.

Construction 2: Let $n = 2k = 2^t m$ be an even integer no less than 4 such that $t \geq 1$ and $\gcd(m, 2) = 1$. We construct an n-variable Boolean function over $\mathbf{F}_{2^n}$ as follows

$$F(x,y) = \begin{cases} g(x/y), & x \cdot y \neq 0, x \neq y \\ 1 + u(x), & x = y \neq 0 \\ u(x), & x \in \mathbf{F}_{2^k}, y = 0 \\ u(y), & x = 0, y \in \mathbf{F}_{2^k}^* \end{cases}$$

where $\mathrm{Supp}(g) = \Delta$ and $u(y)$ is balanced Boolean over $\mathbf{F}_2^k$ discussed in Section 3 satisfying $u(0) = 0$, $deg(u) = k - 1$, and $\max_{a \in \mathbf{F}_2^k} |W_u(a)| \leq \sum_{i=1}^{t-1} 2^{\frac{n}{2^{i+1}}} + 2^{\frac{m+1}{2}}$.

Denote $U = \mathrm{Supp}(u)$. Then, the support of F consists of the following four parts:

- $\{\gamma y, y\}$, $\gamma \in \Delta \setminus \{1\}$, $y \in \mathbf{F}_{2^k}^*$
- $\{x, y\}$, $x = y \in \overline{U} \setminus \{0\}$
- $\{x, 0\}$, $x \in U$

- $\{0, y\}$, $y \in U$

Compared with Construction 1, much more values are changed in Construction 2. Due to these changes, we are not able to guarantee that the new function has optimal algebraic immunity. But we can show that at least it has almost optimal algebraic immunity, and further it has 1-resilient property.

5.1 1-resiliency

Theorem 6. *Let $F(x, y) \in \mathcal{B}_n$ generated by Construction 2. Then, F is 1-resilient.*

***Proof*:** Firstly, F is balanced, i.e, $\mathrm{wt}(F) = (2^{k-1}-1)(2^k-1)+2^{k-1}-1+2\cdot 2^{k-1} = 2^{n-1}$, which implies $W_F(0) = 0$. So, it is sufficient to investigate

$$\begin{aligned}
W_F(a,b) &= \sum_{x,y\in\mathbf{F}_{2^k}} (-1)^{F(x,y)+tr(ax+by)} \\
&= \sum_{x,y\in\mathbf{F}_{2^k}} (-1)^{tr(ax+by)} - 2\sum_{(x,y)\in \mathrm{Supp}(F)} (-1)^{tr(ax+by)} \\
&= -2\sum_{(x,y)\in \mathrm{Supp}(F)} (-1)^{tr(ax+by)} \\
&= -2\sum_{\gamma\in\Delta\setminus\{1\}}\sum_{y\in\mathbf{F}^*_{2^k}} (-1)^{tr((a\gamma+b)y)} - 2\sum_{y\in\overline{U}\setminus\{0\}} (-1)^{tr((a+b)y)} \\
&\quad -2\sum_{x\in U}(-1)^{tr(ax)} - 2\sum_{y\in U}(-1)^{tr(by)}
\end{aligned}$$

in following two cases, where $a \neq 0$ or $b \neq 0$. Basically, our discuss is built on the fact that $\sum\limits_{x\in\mathbf{F}_{2^k}} (-1)^{tr(ax)} = 2^k$ if $a = 0$ and $\sum\limits_{x\in\mathbf{F}_{2^k}} (-1)^{tr(ax)} = 0$ otherwise.

Case 1. $a \neq 0$ and $b = 0$.

$$\begin{aligned}
W_F(a,b) &= -2\sum_{\gamma\in\Delta\setminus\{1\}}\sum_{y\in\mathbf{F}^*_{2^k}} (-1)^{tr(a\gamma y)} - 2\sum_{y\in\overline{U}\setminus\{0\}} (-1)^{tr(ay)} \\
&\quad -2\sum_{x\in U}(-1)^{tr(ax)} - 2|U| \\
&= -2\sum_{\gamma\in\Delta\setminus\{1\}}\left[\sum_{y\in\mathbf{F}_{2^k}} (-1)^{tr(a\gamma y)} - 1\right] - 2\sum_{y\in\overline{U}\setminus\{0\}} (-1)^{tr(ay)} \\
&\quad -2\sum_{x\in U}(-1)^{tr(ax)} - 2|U| \\
&= 2(2^{k-1}-1) - 2\sum_{x\in\mathbf{F}_{2^k}} (-1)^{tr(ax)} + 2 - 2\cdot 2^{k-1} \\
&= 0
\end{aligned}$$

Case 2. $a = 0$ and $b \neq 0$. Similarly,

$$\begin{aligned} W_F(a,b) &= -2\sum_{\gamma\in\Delta\setminus\{1\}}\sum_{y\in\mathbf{F}_{2^k}^*}(-1)^{tr(by)} - 2\sum_{y\in\overline{U}\setminus\{0\}}(-1)^{tr(by)} \\ &\quad -2|U| - 2\sum_{y\in U}(-1)^{tr(by)} \\ &= 0 \end{aligned}$$

Suppose that k elements $c_1, \cdots, c_k \in \mathbf{F}_{2^k}$ are linearly independent over $\mathbf{F}_2$. It is easy to see that $\{(c_i, 0), (0, c_i), 1 \leq i \leq k\}$ form a basis of $\mathbf{F}_{2^n}$ over $\mathbf{F}_2$. By the above two cases, we have $W_F(c_i, 0) = W_F(0, c_i) = 0$ for all $1 \leq i \leq n$. That is, the vector representation of f over $\mathbf{F}_2^n$ under this basis is 1-resilient.

□

5.2 Algebraic immunity and algebraic degree

Theorem 7. *Let $F(x, y)$ be the n-variable Boolean function generated by Construction 2. If the conjecture is true, then $AI(F) \geq \frac{n-2}{2}$.*

***Proof*:** Let

$$h(x,y) = \sum_{i=0}^{2^k-2}\sum_{j=0}^{2^k-2} h_{i,j}x^i y^j,\ h_{i,j} \in \mathbf{F}_2^k,$$

be a polynomial from $\mathbf{F}_{2^k} \times \mathbf{F}_{2^k} \to \mathbf{F}_2$ with $deg(h) < k - 1$.

Similarly to R1 and R2 in the proof of Theorem 3, if h is an annihilator of f or $f + 1$, then

$$h_t(\gamma) = \sum_{i=0}^{2^k-2} h_{i,t-i}\gamma^i = 0$$

holds for $1 \leq t < 2^k - 1$ and $\forall\gamma \in \Delta'$, where $\Delta' = \Delta \setminus \{1\}$ if h is an annihilator of f and $\Delta' = \overline{\Delta}\cup\{1\}$ if h is an annihilator of $f+1$. Consequently, $\hbar = (h_{0,t}, \cdots, h_{t,0}, h_{t+1,2^k-2}, \cdots, h_{2^k-2,t+1})$ is a $2k$-ary BCH code of length $2^k - 1$ with designed distance $2^{k-1} - 1$, having $\mathrm{wt}(\hbar) \geq 2^{k-1}$ if $\hbar \neq \mathbf{0}_{2^k-1}$.

On the other hand, it was proved in [27] that the equations $a + b = t(\mathrm{mod}2^k - 1)$ and $w(\overline{a}) + w(\overline{b}) = k - 1$ has at least one pair of solution for every $1 \leq t < 2^k - 1$. Then $\mathrm{wt}(\hbar) < 2^{k-1}$ if the conjecture is true, which leads to a contradiction.

Therefore, neither f nor $f + 1$ have annihilators with algebraic degrees less than $k - 1$. Hence, $AI(f) \geq k - 1$ has almost optimal algebraic immunity.

□

Additionally, the Boolean function F has algebraic degree $n-2$, which achieves the upper bound on the algebraic degree of a 1-resilient Bollean function according to Siegenthaler's inequality [25].

Theorem 8. *Let $F(x,y)$ be the n-variable Boolean function generated by Construction 2. Then, $deg(F) = n-2$.*

***Proof*:** Let $x, y \in \mathbf{F}_2^k$. Write the Boolean function F in its vector expression $F(x,y) = g(x,y)+u(x,y)$ over $\mathbf{F}_2^k$, where $\mathrm{Supp}(u) = \{(\mathbf{0}_k, y)|u(y)=1, y \in \mathbf{F}_2^k\} \bigcup \{(x, \mathbf{0}_k|u(x)=1, x \in \mathbf{F}_2^k)\} \bigcup \{(x,x)|u(x)=1, x \in \mathbf{F}_2^k \setminus \{\mathbf{0}_k\}\}$.

Since $deg(u) = k-1$, without loss of generality, we suppose that the term $x_1x_2\cdots x_{k-1}$ appears in $u(x)$. Then by Lemma 1 we have

$$\begin{aligned} & \sum_{\gamma \preceq (\mathbf{1}_{k-1}0, \mathbf{1}_{k-1}0)} F(\gamma) \\ = & \sum_{\gamma \preceq (\mathbf{1}_{k-1}0, \mathbf{1}_{k-1}0)} g(\gamma) + \sum_{\gamma_1 \preceq (\mathbf{1}_{k-1}0)} u(\gamma_1) + \sum_{\gamma_2 \preceq (\mathbf{1}_{k-1}0)} u(\gamma_2) + \sum_{\gamma_1 \preceq (\mathbf{1}_{k-1}0)} u(\gamma_1) \\ = & \ 1+1+1 \\ = & \ 1 \end{aligned}$$

which means that the term $x_1x_2\cdots x_{k-1}y_1y_2\cdots y_{k-1}$ appears in the ANF of F, i.e. $deg(F) \geq 2k-2$. Further, by Siegenthaler's inequality in [25], which indicates that $deg(F) \leq 2k-2$ for a 1-resilient function $f \in \mathcal{B}_n$. Hence, we have $deg(F) = 2k-2$.

□

5.3 Nonlinearity

Theorem 9. *Let $F(x,y)$ be the n-variable Boolean function generated by Construction 2, then*

$$\max_{a,b \in \mathbf{F}_{2^k}} |W_F(a,b)| \leq 2^k + 3\left[\sum_{i=1}^{t-1} 2^{\frac{n}{2^{i+1}}} + 2^{\frac{m+1}{2}}\right].$$

That is,

$$N_F \geq 2^{n-1} - 2^{k-1} - 3\left[\sum_{i=1}^{t-1} 2^{\frac{n}{2^{i+1}}-1} + 2^{\frac{m-1}{2}}\right]$$

***Proof*:** We express the Fourier transform in (2) as another manner

$$\begin{aligned}
& W_F(a,b) \\
= & \sum_{x\cdot y\neq 0, x\neq y} (-1)^{g(x/y)+tr(ax+by)} - \sum_{x\in \mathbf{F}_{2^k}^*} (-1)^{tr((a+b)x)} \\
& + \sum_{x\in \mathbf{F}_{2^k}} (-1)^{tr(ax)} + \sum_{y\in \mathbf{F}_{2^k}^*} (-1)^{tr(by)} \\
= & W_T(a,b) - \sum_{x\in \mathbf{F}_{2^k}^*} (-1)^{tr((a+b)x)} + \sum_{x\in \mathbf{F}_{2^k}} (-1)^{tr(ax)} + \sum_{y\in \mathbf{F}_{2^k}^*} (-1)^{tr(by)} \\
= & \begin{cases} W_T(a,b)+2^k, & a=0, b=0 \\ W_T(a,b)+2^k, & a=0, b\neq 0 \\ W_T(a,b)+2^k, & a\neq 0, b=0 \\ W_T(a,b)-2^k, & a=b\neq 0 \\ W_T(a,b), & a\neq 0, b\neq 0, a\neq b \end{cases}
\end{aligned}$$

where $W_T(a,b) = \sum_{x\cdot y\neq 0, x\neq y} (-1)^{g(x/y)+tr(ax+by)}$. Associated with (2), it gives

$$W_T(a,b) = \begin{cases} 0, & a=0, b=0 \\ 0, & a=0, b\neq 0 \\ 0, & a\neq 0, b=0 \\ 0, & a=b\neq 0 \\ \pm 2^k, & a\neq 0, b\neq 0, a\neq b \end{cases}$$

Immediately, we get

$$\begin{aligned}
W_F(a,b) &= |W_T(a,b) + W_u(a+b) + W_u(a) + W_u(b)| \\
&\leq |W_T(a,b)| + 3\max_b |W_u(b)| \\
&\leq 2^k + 3\sum_{i=1}^{t-1} 2^{\frac{n}{2^{i+1}}} + 3\cdot 2^{\frac{m+1}{2}}
\end{aligned}$$

and then the desired nonlinearity.

□

Except for the case of $m=1$, we can further improve the nonlinearity by constructing $s\in\mathcal{B}_m$ as follows.

1. Let $m = 2m_1+1$. Choose a injection π from $\mathbf{F}_{2^{m_1}}$ to $\mathbf{F}_{2^{m_1+1}} \setminus \{\mathbf{0}_{m_1+1}\}$ such that $x, y\in\Omega \Rightarrow x+y\notin\Omega$ where $\Omega = \pi(\mathbf{F}_{2^{m_1}})$;

2. Set $s'(x,y) = \pi(x)\cdot y$ for $x\in\mathbf{F}_{2^{m_1}}$ and $y\in\mathbf{F}_{2^{m_1+1}}$;

3. Obtain $s \in \mathcal{B}_m$ by applying the Sakar-Maitra's degree optimization method to the balanced function s'.

It is easy to check that $s' \in \mathcal{B}_m$ is a balanced semi-bent function, i.e., $W_{s'}(a) \in \{0, \pm 2^{\frac{m+1}{2}}\}$ and $N_{s'} = 2^m - 2^{\frac{m-1}{2}}$. Specifically, s' satisfies that $W_{s'}(x+y) = 0$ if $W_{s'}(x) \neq 0$ and $W_{s'}(y) \neq 0$ for all $x, y \in \mathbf{F}_{2^m}$. According to Lemma 4, we have that $s \in \mathcal{B}_m$ is a balanced function with $N_s = 2^m - 2^{\frac{m-1}{2}} - 2$, the maximal degree $m-1$,

$$\begin{aligned} |W_s(a)| &\leq 2^m - 2N_s \\ &= 2^m - 2(N_s - 2) \\ &= \max_{c \in \mathbf{F}_{2^m}} |W_{s'}(c)| + 4, \end{aligned}$$

and

$$|W_s(a+b) + W_s(a) + W_s(b)| \leq 2 \max_{c \in \mathbf{F}_{2^m}} |W_{s'}(c)| + 12$$

for all $a, b \in \mathbf{F}_{2^m}$. Employing s to construct the balanced Boolean function u in the Dobbertin's iterative construction and then using u for our Construction 2, we can increase the nonlinearity.

Theorem 10. *When $n = 2^t m$ and $m > 1$. Let s be the above m-variable balanced boolean function, and F be the resultant n-variable Boolean function generated by Construction 2, then*

$$N_F \geq 2^{n-1} - 2^{k-1} - 3 \cdot \sum_{i=1}^{t-1} 2^{\frac{n}{2^{i+1}} - 1} - 2^{\frac{m+1}{2}} - 6$$

5.4 Comparison with the known results

Finally we compare the nonlinearity of our result with the 1-resilient Boolean function in [27], which has almost optimal algebraic immunity $n/2 - 1$ as well. In general, it is easily seen that our bounds are much better than the bound in [27]. In addition, Table 3 compares our bounds with the numerical result of the bound and some concrete values given [27] for even $4 \leq n \leq 18$, which are respectively denoted by N_4 and $\mathcal{N}_4$ for short.

Table 3. Comparison of the nonlinearity of 1-resilient Boolean functions (n even)

n	N_4 in [27]	$\mathcal{N}_4$ in [27]	Our bound in Theorem 9	Our bound in Theorem 10
4	0	4	0	–
6	4	24	22	18
8	80	112	108	103
10	431	484	484	482
12	1910	1996	1998	1994
14	7957	8100	8104	8106
16	32367	32588	32604	–
18	130386	130760	130768	130778

When compared with the newly proposed 1-resilient function in [30], which is recorded to have the best nonlinearity among all the known 1-resilient function constructions, our function still has better nonlinearity, even the algebraic immunity property of that function is unknown yet. For the comparison, first of all we establish an upper bound on the nonlinearity of the 1-resilient function in [30].

Theorem 11. *Let $f \in \mathcal{B}_n$ be the 1-resilient Boolean function constructed in [30], then the nonlinearity*

$$N_f < 2^{n-1} - 2^{n/2-1} - 2^{n/4-\lceil \log_2(n/2) \rceil/2-3/2}$$

***Proof*:** Let $w = \lfloor n/4 \rfloor - 1$. According to Theorem 1 in [30],

$$N_f = \max_A \left(2^{n-1} - 2^{n/2-1} - \sum_{k=1}^{w} a_k \cdot 2^{n/2-k-1} \right), \tag{6}$$

where $A = \{(a_1, \cdots, a_w) : a_k \in \mathbf{F}_2, 1 \le k \le w\}$ satisfies

$$\sum_{k=1}^{w} a_k \cdot \sum_{j=2}^{n/2-2k} \binom{n/2-2k}{j} \ge \frac{n}{2} + 1.$$

Define r to be the integer such that $a_r = 1$ and $a_i = 0$ for all $i < r$. To attain the maximal nonlinearity, it is easily seen from (6) that r should be as large as possible, say close to w.

Clearly, $\sum_{j=2}^{n/2-2k} \binom{n/2-2k}{j} < 2^{n/2-2k}$ and then

$$\sum_{k=r}^{w} \sum_{j=2}^{n/2-2k} \binom{n/2-2k}{j} < 2^{n/2-2r+1}$$

which leads to

$$2^{n/2-2r+1} > \frac{n}{2}.$$

Hence, $r < (n+2)/4 - \lceil \log_2(n/2) \rceil/2$. Then,

$$\begin{aligned} N_f &\leq 2^{n-1} - 2^{n/2-1} - 2^{n/2-r-1} \\ &< 2^{n-1} - 2^{n/2-1} - 2^{n/4+\lceil \log_2(n/2) \rceil/2-3/2} \end{aligned}$$

□

Set $n = 2^t m$ in Theorem 11, we arrive at $N_f < 2^{n-1} - 2^{n/2-1} - 2^{n/4+(t-1)/2+\lceil \log_2 m \rceil/2-3/2}$, which is worse than our bounds in Theorems 9 and 10 provided that $t + \lceil \log_2 m \rceil > 2\log_2 3 + 2$. Therefore, our bounds are much better in most cases.

Finally, in Table 4 we compare some small concrete values.

Table 4. Comparison of the nonlinearity of 1-resilient Boolean functions (n even)

n	N_F in [30]	Our bound in Theorem 9	Our bound in Theorem 10
12	1996	1998	1994
14	8092	8104	8106
16	32604	32604	–
18	130748	130768	130778
20	523708	523716	523714
22	2095996	2096032	2096058
24	8386300	8386446	8386442
26	33550076	33550144	33550202
28	134209020	134209320	134209322
30	536854012	536854144	536854266
32	2147449852	2147450460	–
34	8589868028	8589868288	8589868538
36	34359605244	34359606480	34359606490
38	137438689276	137438689792	137438690298
40	549755285500	549755288004	549755288002
42	2199022202876	2199022203904	2199022204922
44	8796090916860	8796090921888	8796090921914
46	35184367886332	35184367888384	35184367890426
48	140737479950332	140737479960462	140737479960458
50	562949936627708	562949936631808	562949936635898

References

[1] A. Canteaut and M. Trabbia, "Improved fast correlation attacks using parity-check equations of weight 4 and 5," in *Advances in Cryptology-EUROCRYPT 2000 (Lecture Notes in Computer Science)*, Springer-Verlag, 2000, vol. 1807, pp. 573-588.

[2] C. Carlet, "A larger class of cryptographic Boolean functions via a study of the Maiorana-Mcfarland construction," in *Advances in Cryptology-CRYPTO 2002 (Lecture Notes in Computer Science)*, Springer-Verlag, 2002, vol. 2442, pp. 549-564.

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

[4] C. Carlet, X. Zeng, C. Li, and L. Hu, "Further properties of several classes of Boolean functions with optimum algebraic immunity," *Des. Codes Cryptogr.* vol. 52, pp. 303-338, 2009.

[5] C. Carlet and K. Feng, "An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity," in *Advances in Cryptology-ASIACRYPT 2008 (Lecture Notes in Computer Science)*, Springer-Verlag, 2008, vol. 5350, pp. 425-440.

[6] C. Carlet, "The monography Boolean Methods and Models," In *Boolean Functions for Cryptography and Error Correcting Codes*, Y. Crama and P. Hammer, Eds, Cambridge University Press, Cambridge.

[7] N. Courtois and W. Meier, "Algebraic attacks on stream ciphers with linear feedback," in *Advances in Cryptology - EUROCRYPT 2003 (Lecture Notes in Computer Science)*, Springer-Verlag, 2003, vol. 2656, pp. 345-359.

[8] T.W. Cusick, Y. Li, and P. Stanica, "On a combinatoric conjecture," Cryptology ePrint Archive, Report 2009/554, 2009. http: //eprint.iacr.org/2009/554.pdf.

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

[10] J.F. Dillon, "Elementary Hadamard difference sets." Ph.D. Thesis, Univ. of Maryland, 1974.

[11] C. Ding, G.Z. Xiao, and W. Shan, *The Stability Theory of Stream Ciphers*, Lecture Notes in Computer Science, vol. 561. Springer-Verlag, 1991.

[12] H. Dobbertin, "Construction of bent functions and balanced boolean functions with high nonlinearity," in *Workshop on Fast Software Encryption (Lecture Notes in Computer Science)*, Springer-Verlag, 1995, vol. 1008, pp. 61-74.

[13] J.P. Flori, H. Randriambololona, G. Cohen, and S. Mesnager, "On a conjecture about binary strings distribution," Cryptology ePrint Archive, Report 2010/170, 2010. http: //eprint.iacr.org/.

[14] S. Kavut and M.D. Yücel, "9-variable Boolean functions with nonlinearity 242 in the generalized rotation symmetric class," *Information and Computation*, vol. 208, pp. 341-350, 2010.

[15] 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, 2007.

[16] N. Li and W. Qi, "Construction and analysis of boolean functions of 2t+1 variables with maximum algebraic immunity," In *Advances in Cryptology - Asiacrypt 2006 (Lecture Notes in Computer Science)*, Springer-Verlag, 2006, vol. 4284, pp. 84-98.

[17] N. Li, L. Qu, W. Qi, G. Feng, C. Li, and D. Xie, "On the construction of Boolean functions with optimal algebraic immunity," *IEEE Trans. Inf. Theory*, vol. 54, pp. 1330-1334, 2008.

[18] M. Lobanov, "Tight bound between nonlinearity and algebraic immunity," Cryptology ePrint Archive, Report 2005/441, 2005. http: //eprint.iacr.org/2005/441.pdf

[19] 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'08*, Copenhagen, Denmark, 2008, pp. 109-118.

[20] W. Meier, E. Pasalic, and C. Carlet, "Algebraic attacks and decomposition of boolean functions," In *Advances in Cryptology - EUROCRYPT 2004 (Lecture Notes in Computer Science)*, Springer-Verlag, 2004, vol. 3027, pp. 474-491.

[21] N.J. Patterson and D.H. Wiedemann, "The covering radius of the (215, 16) Reed-Muller code is at least 16276," *IEEE Trans. Inf. Theory*, vol. 29, no. 3, pp. 354-356, 1983. See also correction in vol. 36, no. 2, pp. 443, 1990.

[22] O.S. Rothaus, "On bent functions," *J. Comb. Theory*, ser. 20A, pp. 300-305, 1976.

[23] P. Sarkar and S. Maitra, "Construction of nonlinear Boolean functions with important cryptographic properties," *Advances in Cryptology-EUROCRYPT 2000 (Lecture Notes in Computer Science)*, Springer-Verlag, 2000, vol. 1807, pp. 485-506.

[24] S. Sarkar, S. Maitra, "Idempotents in the neighbourhood of Patterson-Wiedemann functions having Walsh spectra zeros," *Designs, Codes Cryptogr.*, vol. 9, no. 1-3, pp. 95-103, 2008.

[25] T. Siegenthaler, "Correlation-immunity of nonlinear combining functions for cryp- tographic applications," *IEEE Trans. Inf. Theory*, vol. 30, no. 5, pp. 776-780, 1984.

[26] Z. Tu and Y. Deng, "A conjecture on binary string and its applications on constructing boolean functions of optimal algebraic immunity," *Designs, Codes Cryptogr.*, 2010. Online First Articles. DOI 10.1007/s10623-010-9413-9

[27] Z. Tu and Y. Deng, "A class of 1-resilient function with high nonlinearity and algebraic immunity," Cryptography ePrint Archive, Report 2010/179, 2010. http://eprint.iacr.org/2010/179.pdf.

[28] Q. Wang, J. Peng, H. Kan, and X. Xue, "Constructions of cryptographically significant Boolean functions using primitive polynomials," *IEEE Trans. Inf. Theory*, vol. 56, no. 6, pp. 3048-3053, 2010.

[29] X. Zeng and L. Hu, "Constructing boolean functions by modifying Maiorana-McFarland's superclass functions," *IEICE Trans. Fundamentals,*, vol. 88-A, no. 1, pp. 59-66, 2005.

[30] W. Zhang and G. Xiao, "Constructions of Almost optimal resilient functions on Large Even Number of Variables," *IEEE Trans. Inf. Theory*, vol. 55, no. 12, pp. 5822-5831, 2009.

[31] Y. Zheng, X.M. Zhang, and H. Imai, "Duality of boolean functions and its cryptographic significance," *In Advances in Cryptology-ICICS97 (Lecture Notes in Computer Science)*, Springer-Verlag, 1997, vol. 1334, pp. 159-169.