Boolean functions with all main cryptographic properties*

Ziran Tu[1] · Yingpu Deng[2]
[1]Faculty of Science, Henan University of Science and Technology,
Luoyang 471003, People's Republic of China
e-mail: naturetu@gmail.com
[2]Key Laboratory of Mathematics Mechanization,
Academy of Mathematics and Systems Science,
Chinese Academy of Sciences, Beijing 100190, People's Republic of China
e-mail: dengyp@amss.ac.cn

Abstract In this paper, we propose a class of $2k$-variable Boolean functions which have optimal algebraic degree, very high nonlinearity, and are 1-resilient. Based on our newly proposed conjecture, it can be shown that the algebraic immunity of our functions is at least suboptimal. Moreover, when k is odd, the algebraic immunity is actually optimal, and for even k, we find that the algebraic immunity is optimal at least for $k \leqslant 28$.

Keywords Boolean function · Correlation immunity · Algebraic immunity · Resiliency · Balancedness · Nonlinearity · Algebraic degree

Mathematics Subject Classification (2000) 94A60

1 Introduction

In many symmetric cryptosystems, Boolean functions are critical building blocks. To resist known attacks, there have been many criteria for designing Boolean functions. Generally speaking, before 2003, cryptographic Boolean functions were usually required to be balanced, have high algebraic degree and high nonlinearity. The concept of correlation immunity was proposed by Siegenthaler [24], then Xiao and Massey [27] gave a simple spectral characterization. Many papers discussed functions with high nonlinearity and high-order correlation immunity, and there have been many constructions [2, 7, 14, 20], but many of which are Maiorana-McFarland like functions. When n is small, some resilient functions with maximal nonlinearity have been obtained [23, 21, 18]. Since 2003, the algebraic attacks proposed by Courtois and Meier [1, 8, 9, 19] have received the world's attention, as a result, the algebraic immunity of Boolean functions has been introduced, and the study of annihilators of Boolean functions becomes important.

*This is an enlarged and revised version of the paper: Ziran Tu and Yingpu Deng: A Class of 1-Resilient Function with High Nonlinearity and Algebraic Immunity. Cryptology ePrint Archive, Report 2010/179. http://eprint.iacr.org/2010/179.

Definition 1.1. [19] *The algebraic immunity $AI_n(f)$ of an n-variable Boolean function is defined to be the lowest degree of nonzero functions g such that $fg = 0$ or $(f + 1)g = 0$.*

To resist standard algebraic attacks, cryptographic Boolean functions should have high algebraic immunity. Up to now, several classes of Boolean functions which are algebraic immunity optimal have been proposed in [4, 6, 11, 15, 16]. Well, designing a Boolean function to meet all criteria is really a challenge. Most known constructions that are algebraic immunity optimal are improper for cryptographic applications. In 2008, Carlet and Feng made a breakthrough at this point in [5] and they constructed an infinite class of n-variable Boolean functions with optimal algebraic immunity, maximal algebraic degree and high nonlinearity. It is the first class of functions which meet the most cryptographic necessities. Very recently, Tu and Deng proposed in [25] a class of algebraic immunity optimal functions of even number variables under an assumption of a combinatoric conjecture, the nonlinearity of these functions were even better than functions proposed in [5]. Although Carlet proved in [3] that the functions in [25] were weak against fast algebraic attacks, he could repair this weakness through small modifications. However, among all the main designing criteria of Boolean functions, the correlation immunity or resiliency was ignored by [5, 25] and all other known functions with optimal algebraic immunity.

In this paper, we propose an infinite class of $2k$-variable Boolean functions, which satisfy all the main cryptographic criteria: 1-resilient, algebraic degree optimal, have very high nonlinearity. Based on the conjecture proposed in [25], it can be proved that the algebraic immunity of our functions is at least suboptimal. Moreover, when k is odd, the algebraic immunity is actually optimal, and for even k, we find that the algebraic immunity is optimal at least for $k \leqslant 28$.

2 Preliminaries

Let n be a positive integer. A Boolean function on n variables is a mapping from $\mathbb{F}_2^n$ into $\mathbb{F}_2$, which is the finite field with two elements. We denote B_n the set of all n-variable Boolean functions.

Every Boolean function f in B_n has a unique representation as a multivariate polynomial over $\mathbb{F}_2$

$$f(x_1, x_2, ..., x_n) = \sum_{I \subseteq \{1,...,n\}} a_I \prod_{i \in I} x_i$$

where the a_I's are in $\mathbb{F}_2$, such kind of representation is called the algebraic normal form (ANF). The algebraic degree $deg(f)$ of f is defined to be the maximum degree of those monomials with nonzero coefficients in its algebraic normal form. A Boolean function f is called affine if $deg(f) \leqslant 1$, we denote A_n the set of all affine functions in B_n. The support of f is defined as $supp(f) = \{x \in \mathbb{F}_2^n : f(x) = 1\}$, and the $wt(f)$ is the number of vectors which lie in $supp(f)$. For two functions f and g in B_n, the Hamming distance $d(f, g)$ between f and g is defined as $wt(f + g)$. The nonlinearity $nl(f)$ of a Boolean function f is defined as the minimum Hamming distance between f and all affine functions, i.e. $\mathrm{nl}(f) = \mathrm{Min}_{g \in A_n} d(f, g)$.

For any $a \in \mathbb{F}_2^n$, the value

$$\mathrm{W}_f(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+<x,a>}$$

is called the Walsh spectrum of f at a, where $< x, a >$ denotes the inner product between x and a, i.e. $< x, a >= x_1a_1 + \ldots + x_na_n$. If $W_f(a) = 0$ for $1 \leqslant wt(a) \leqslant m$, then f is called m-th order correlation immune, this is the famous Xiao-Massey [27] characterization of correlation immune functions. Moreover, if f is also balanced, we call f is m-th order resilient. The nonlinearity of a Boolean function f can be expressed via its Walsh spectra by the next formula

$$\mathrm{nl}(f) = 2^{n-1} - \frac{1}{2}\mathrm{Max}_{a \in \mathbb{F}_2^n} |\mathrm{W}_f(a)|.$$

Notice that for $f : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_2$, the Walsh spectrum of f at $a \in \mathbb{F}_{2^n}$ is defined by

$$\mathrm{W}_f(a) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+tr(a \cdot x)},$$

where tr is the trace function from $\mathbb{F}_{2^n}$ onto $\mathbb{F}_2$. For $f : \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \longrightarrow \mathbb{F}_2$, the Walsh spectrum of f at $(a, b) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$ is defined by

$$\mathrm{W}_f(a, b) = \sum_{(x,y) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}} (-1)^{f(x,y)+tr(a \cdot x + b \cdot y)},$$

where tr is the trace function from $\mathbb{F}_{2^k}$ onto $\mathbb{F}_2$. It is well-known that the nonlinearity satisfies the following inequality

$$\mathrm{nl}(f) \leqslant 2^{n-1} - 2^{\frac{n}{2}-1}.$$

When n is even, the above upper bound can be attained, and such Boolean functions are called bent [22]. Bent function has several equivalent definitions, for instance, a function f is *bent* is equivalent to say that $supp(f)$ is a $(2^n, 2^{n-1} \pm 2^{\frac{n}{2}-1}, 2^{n-2} \pm 2^{\frac{n}{2}-1})$-difference set in the additive group of $\mathbb{F}_2^n$.

3 Boolean functions with all main cryptographic properties

In this section, we give our construction inspired by Dillon's *partial spread* function [12] and discuss its main cryptographic properties. Firstly we recall Dillon's functions.
Dillon's construction [12]. Let $n = 2k$, $\mathbb{F}_{2^n} \approx \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$, $g : \mathbb{F}_{2^k} \longrightarrow \mathbb{F}_2$ is a balanced function which vanishes at 0, define $f : \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$ by

$$f(x, y) = g(xy^{2^k-2})$$

then f is bent.

In the following construction, we try to consider functions' resiliency property in addition to algebraic degree, nonlinearity and algebraic immunity.

Construction 3.1. *Let $n = 2k, k \geqslant 3$ and $\mathbb{F}_{2^k}$ be the finite field with 2^k elements, α be a primitive element of $\mathbb{F}_{2^k}$. Set $A = \{0, 1, \alpha, \alpha^2, \cdots, \alpha^{2^{k-1}-1}\}$. We define an n-variable Boolean function $f : \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$, whose support $supp(f)$ is constituted by the following four disjoint parts:*

- $\{(x, y) : y = \alpha^i x, x \in \mathbb{F}_{2^k}^*, i = 1, 2, \cdots, 2^{k-1} - 1\}$
- $\{(x, y) : y = x, x \in A\}$
- $\{(x, 0) : x \in \mathbb{F}_{2^k} \setminus A\}$
- $\{(0, y) : y \in \mathbb{F}_{2^k} \setminus A\}$

3.1 1-resiliency, algebraic degree and nonlinearity

Proposition 3.2. *Let function f be defined as in Construction 3.1, then f is 1-resilient.*

Proof. Since $wt(f) = (2^k - 1)(2^{k-1} - 1) + (2^{k-1} + 1) + (2^{k-1} - 1) + (2^{k-1} - 1) = 2^{n-1}$, so f is balanced. We need to verify that $W_f(a, b) = 0$ for each $(a, b) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$ satisfying $wt(a, b) = 1$. In fact, we can prove more. When a, b are not all zero, first note that

$$\sum_{(x,y)\in\mathbb{F}_{2^k}\times\mathbb{F}_{2^k}} (-1)^{tr(ax+by)}$$

$$= \sum_{x\in\mathbb{F}_{2^k}} (-1)^{tr(ax)} \cdot \sum_{y\in\mathbb{F}_{2^k}} (-1)^{tr(by)} = 0,$$

where tr is the trace function from $\mathbb{F}_{2^k}$ onto $\mathbb{F}_2$, then we have

$$\begin{aligned} W_f(a, b) &= \sum_{(x,y)\in\mathbb{F}_{2^k}} (-1)^{f(x,y)+tr(ax+by)} \\ &= -2 \sum_{(x,y)\in supp(f)} (-1)^{tr(ax+by)}. \end{aligned}$$

We can see

$$\begin{aligned} \sum_{(x,y)\in supp(f)} (-1)^{tr(ax+by)} &= \sum_{i=1}^{2^{k-1}-1} \sum_{x\in\mathbb{F}_{2^k}^*} (-1)^{tr((a+b\alpha^i)x)} + \sum_{x\in A} (-1)^{tr((a+b)x)} \\ &+ \sum_{x\in\mathbb{F}_{2^k}\setminus A} (-1)^{tr(ax)} + \sum_{y\in\mathbb{F}_{2^k}\setminus A} (-1)^{tr(by)}. \end{aligned}$$

We consider the Walsh spectra of two kinds of points:

1. $a \neq 0, b = 0$, then

$$\begin{aligned}\sum_{(x,y)\in supp(f)} (-1)^{tr(ax+by)} &= 1 - 2^{k-1} + 2^k - |A| \\ &+ \sum_{x\in\mathbb{F}_{2^k}\setminus A} (-1)^{tr(ax)} + \sum_{x\in A}(-1)^{tr(ax)};\end{aligned}$$

2. $b \neq 0, a = 0$, then

$$\begin{aligned}\sum_{(x,y)\in supp(f)} (-1)^{tr(ax+by)} &= 1 - 2^{k-1} + 2^k - |A| \\ &+ \sum_{y\in\mathbb{F}_{2^k}\setminus A} (-1)^{tr(by)} + \sum_{y\in A}(-1)^{tr(by)}.\end{aligned}$$

Combining with the equality $|A| = 2^{k-1} + 1$, it is obvious to see that $W_f(a, b) = 0$ for $ab = 0$. Therefore f is 1-resilient. □

From Siegenthaler's inequality[24], we know that for an n-variable, m-th order resilient Boolean function g, it should be satisfied that $m + deg(g) \leqslant n - 1$. We will see that f in Construction 3.1 is algebraic degree optimal in this sense.

Proposition 3.3. *Let function f be defined as in Construction 3.1, then $deg(f) = n - 2$.*

Proof. Let $g, h : \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$ be two Boolean functions as defined by $supp(g) = \{(x, y) : y = \alpha^i x, x \in \mathbb{F}_{2^k}^*, i = 0, 1, \cdots, 2^{k-1} - 1\}$ and by $supp(h) = \{(0, 0)\} \cup \{(x, x) : x \in \mathbb{F}_{2^k} \setminus A\} \cup \{(x, 0) : x \in \mathbb{F}_{2^k} \setminus A\} \cup \{(0, y) : y \in \mathbb{F}_{2^k} \setminus A\}$. So $f = g + h$. Since g is a function in the PS^- class, it is a bent function, we know that $deg(g) \leqslant k < n - 2$ from [22]. To prove $deg(f) = n - 2$, we only need to prove $deg(h) = n - 2$. By Lagrange's interpolation formula, we have

$$\begin{aligned}h(x, y) &= (x^{2^k-1} + 1)(y^{2^k-1} + 1) + \sum_{a\notin A}((x + a)^{2^k-1} + 1)((y + a)^{2^k-1} + 1) \\ &+ \sum_{a\notin A}((x + a)^{2^k-1} + 1)(y^{2^k-1} + 1) + \sum_{a\notin A}(x^{2^k-1} + 1)((y + a)^{2^k-1} + 1).\end{aligned}$$

Expanding the terms, we have

$$h(x, y) = \sum_{a\notin A}\sum_{i=1}^{2^k-1}\sum_{j=1}^{2^k-1}\binom{2^k - 1}{i}\binom{2^k - 1}{j}x^{2^k-1-i}y^{2^k-1-j}a^{i+j}.$$

It is easy to see $deg(h) \leqslant n - 2$. The coefficient of $x^{2^k-1-1}y^{2^k-1-1}$ is

$$\sum_{a\notin A} a^2 = \left(\frac{1 + \alpha^{2^{k-1}}}{1 + \alpha}\right)^2$$

which is obviously nonzero in $\mathbb{F}_{2^k}$. Therefore $deg(h) = n - 2$. □

Now we consider the nonlinearity of functions from Construction 3.1, we need a result in [5].

Proposition 3.4. *[5] Let $\omega \in \mathbb{F}_{2^n}^*$ be a primitive element and $\lambda \in \mathbb{F}_{2^n}$, denote*

$$S_\lambda = \sum_{i=2^{n-1}-1}^{2^n-2} (-1)^{tr(\lambda\omega^i)}.$$

If $\lambda \neq 0$, then

$$|S_\lambda| \leqslant 2^{\frac{n}{2}} n \cdot ln2 + 1.$$

Proposition 3.5. *Let function f be defined as in Construction 3.1, then $nl(f) \geqslant 2^{n-1} - 2^{k-1} - 3 \cdot k \cdot 2^{\frac{k}{2}} ln2 - 7$.*

Proof. From the above proof we only need to consider

$$K_{(a,b)} := \sum_{(x,y)\in supp(f)} (-1)^{tr(ax+by)}$$

for $(a, b) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$ with $a \cdot b \neq 0$, and where tr is the trace function from $\mathbb{F}_{2^k}$ onto $\mathbb{F}_2$. We know that

$$\begin{aligned} K_{(a,b)} \quad &= \sum_{i=1}^{2^{k-1}-1} \sum_{x\in\mathbb{F}_{2^k}^*} (-1)^{tr((a+b\alpha^i)x)} + \sum_{x\in A} (-1)^{tr((a+b)x)} \\ &+ \sum_{x\in\mathbb{F}_{2^k}\setminus A} (-1)^{tr(ax)} + \sum_{y\in\mathbb{F}_{2^k}\setminus A} (-1)^{tr(by)}. \end{aligned}$$

By Proposition 3.4, we know that

$$|\sum_{x\notin A} (-1)^{tr(ax)}| = |\sum_{i=2^{k-1}}^{2^k-2} (-1)^{tr(a\alpha^i)}| = |\sum_{i=2^{k-1}-1}^{2^k-2} (-1)^{tr(a\alpha^i)} - (-1)^{tr(a\alpha^{2^{k-1}-1})}|$$

$$\leqslant (k \cdot 2^{\frac{k}{2}} ln2 + 1) + 1 = k \cdot 2^{\frac{k}{2}} ln2 + 2.$$

Similarly, we have

$$|\sum_{y\notin A} (-1)^{tr(by)}| \leqslant k \cdot 2^{\frac{k}{2}} ln2 + 2.$$

If $a + b \neq 0$, we also have

$$|\sum_{x\in A} (-1)^{tr((a+b)x)}| = |-\sum_{x\notin A} (-1)^{tr((a+b)x)}| \leqslant k \cdot 2^{\frac{k}{2}} ln2 + 2.$$

Now we can obtain an upper bound for $|K_{(a,b)}|$ easily:

1. $a+b=0$, then

$$|K_{(a,b)}| = |(2^{k-1}-1)(-1)+(2^{k-1}+1)+\sum_{x\notin A}(-1)^{tr(ax)}+\sum_{y\notin A}(-1)^{tr(by)}|$$

$$\leqslant 2+2\cdot(k\cdot 2^{\frac{k}{2}}ln2+2);$$

2. $a+b\alpha^i=0$ for some i, $0<i<2^{k-1}$, then

$$|K_{(a,b)}| = |(2^k-1)+(-1)\cdot(2^{k-1}-2)+\sum_{x\in A}(-1)^{tr((a+b)x)}+\sum_{x\in\mathbb{F}_{2^k}\setminus A}(-1)^{tr(ax)}$$

$$+\sum_{y\in\mathbb{F}_{2^k}\setminus A}(-1)^{tr(by)}| \leqslant 2^{k-1}+1+3\cdot(k\cdot 2^{\frac{k}{2}}ln2+2);$$

3. otherwise

$$|K_{(a,b)}| = |-(2^{k-1}-1)+\sum_{x\in A}(-1)^{tr((a+b)x)}+\sum_{x\in\mathbb{F}_{2^k}\setminus A}(-1)^{tr(ax)}$$

$$+\sum_{y\in\mathbb{F}_{2^k}\setminus A}(-1)^{tr(by)}| \leqslant 2^{k-1}+1+3\cdot(k\cdot 2^{\frac{k}{2}}ln2+2).$$

Finally we get

$$nl(f) = 2^{n-1}-\frac{1}{2}Max_{a,b\in\mathbb{F}_{2^k}}|W_f(a,b)| = 2^{n-1}-Max_{a,b\in\mathbb{F}^*_{2^k}}|K(a,b)|$$

$$\geqslant 2^{n-1}-2^{k-1}-3\cdot k\cdot 2^{\frac{k}{2}}ln2-7.$$

□

In fact, we can improve this lower bound according to the method in [26]. We use Magma system to compute the nonlinearity of f in Construction 3.1, see the following table. We can see that the nonlinearity of f is very high and satisfying.

Table 1 The nonlinearity of functions in Construction 3.1

n	$2^{n-1}-2^{\frac{n}{2}-1}$	$nl(f)$
6	28	24
8	120	112
10	496	484
12	2016	1996
14	8128	8100
16	32640	32588
18	130816	130760

3.2 The algebraic immunity

In this section we discuss the algebraic immunity property of Boolean functions from Construction 3.1. We first recall a combinatorial conjecture proposed in [25].

Conjecture 3.6. [25] *Assume $k \in \mathbb{Z}$, $k > 1$. For every $x \in \mathbb{Z}$, $0 \leqslant x \leqslant 2^k - 1$, we expand x as a binary string of length k, and denote the number of one's in the string by $w(x)$. For any $t \in \mathbb{Z}$, $0 < t < 2^k - 1$, let*

$$S_t = \{(a, b) | a, b \in \mathbb{Z}, 0 \leqslant a, b < 2^k - 1, a + b = t \ mod \ 2^k - 1, w(a) + w(b) \leqslant k - 1\}$$

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

In fact, the authors designed in [25] an algorithm and validated their conjecture until $k \leqslant 29$. As a cornerstone of the algebraic immunity property of functions in [25], the conjecture attracts people's attention, the authors in [10, 13] tried to attack this problem theoretically and some advances had been made, and they verified that the conjecture is correct for many cases of t. In the remainder of this paper, we always assume that this conjecture is correct.

In the course of the proof, we need the knowledge of BCH code (see, for example, [17]). For the convenience of the reader, we recall the definition of a BCH code.

Theorem 3.7. (*The BCH bound*) *Let Φ be a cyclic code of length n and with generator polynomial $g(x)$ such that for some integers $b \geqslant 0$, $\delta \geqslant 1$*

$$g(\alpha^b) = g(\alpha^{b+1}) = \cdots = g(\alpha^{b+\delta-2}) = 0$$

i.e. the code has a string of $\delta - 1$ consecutive powers of α as zeros, where α is a primitive $n-$th root of unity, then the minimal distance of Φ is at least δ.

This induces the definition of a BCH code.

Definition 3.8. *A cyclic code of length n over $\mathbb{F}_q$ is a BCH code of designed distance δ if, for some integer $b \geqslant 0$,*

$$g(x) = lcm\{m^{(b)}(x), m^{(b+1)}(x), \cdots, m^{(b+\delta-2)}(x)\}$$

i.e. $g(x)$ is the lowest degree monic polynomial over $\mathbb{F}_q$ having $\alpha^b, \alpha^{b+1}, \cdots, \alpha^{b+\delta-2}$ as zeros, where $m^{(i)}(x)$ is the minimal polynomial of α^i over $\mathbb{F}_q$.

We will use the BCH bound repeatedly, for later convenience we introduce the following corollary:

Corollary 3.9. *Let $f(x)$ be a univariate polynomial over the finite field $\mathbb{F}_{2^k}$ with $deg(f) \leqslant 2^k - 2$, α be a primitive element of $\mathbb{F}_{2^k}$. If $f(x)$ has $\delta - 1$ consecutive roots $\alpha^s, \alpha^{s+1}, \cdots, \alpha^{s+\delta-2}$, in which s is a nonnegative integer, and if f is not the zero polynomial, then the number of nonzero coefficients in $f(x)$ is larger than or equal to δ.*

Proof. Write $f(x) = a_0 + a_1 x + \ldots + a_{2^k-2} x^{2^k-2}$ with $a_i \in \mathbb{F}_{2^k}$. From the assumed condition, we know that $(a_0, a_1, \ldots, a_{2^k-2})$ is a codeword in some BCH code of length $2^k - 1$ over $\mathbb{F}_{2^k}$, having $\alpha^s, \alpha^{s+1}, \cdots, \alpha^{s+\delta-2}$ as zeros and with designed distance δ. According to the BCH bound, if this codeword is nonzero, then its weight should be larger than or equal to δ. □

Firstly, we show that the algebraic immunity in Construction 3.1 is at least suboptimal. For this we need the following lemma.

Lemma 3.10. *For every $0 < t < 2^k - 1$, the modular equation $a + b = t \ mod\ 2^k - 1, w(a) + w(b) = k - 1$ has at least one pair of solution.*

Proof. At first we observe that, if t and t' belong to a same cyclotomic coset $mod\ 2^k - 1$, then the modular equations for t and for t' have exactly the same number of solutions. Without loss of generality we suppose that t has the following form:

$$t = \underbrace{11\cdots1}_{n_1}\underbrace{00\cdots0}_{n_2}\underbrace{1\cdots1}_{n_3}\underbrace{0\cdots0}_{n_4}\cdots\cdots\underbrace{1\cdots1}_{n_{2r-1}}\underbrace{0\cdots0}_{n_{2r}}$$

In order to prove the lemma, we only need to construct a pair of (a, b) to be a solution. If $0 \leqslant a, b < 2^k - 1$ satisfy $a + b = t \ \ mod\ \ 2^k - 1$, then $w(a) + w(b) = w(t) + s$, in which s represents the number of carries when doing the modular addition. Since $w(t) = n_1 + n_3 + \ldots + n_{2r-1}$ and $k = n_1 + n_2 + \ldots + n_{2r-1} + n_{2r}$, we have that (a, b) is a required solution if and only if $a + b = t \ mod\ 2^k - 1$ and the number of carries is $n_2 + n_4 + \ldots + n_{2r} - 1$ when doing the modular addition.

If $n_{2r} > 1$, we construct a pair (a, b) as follows:

$$a = \underbrace{1\cdots1}_{n_1-1}0\underbrace{1\cdots11}_{n_2}\underbrace{1\cdots1}_{n_3-1}0\underbrace{1\cdots11}_{n_4}\cdots\cdots\underbrace{1\cdots1}_{n_{2r-1}-1}0\underbrace{1\cdots110}_{n_{2r}}$$

$$b = \underbrace{0\cdots0}_{n_1-1}0\underbrace{0\cdots01}_{n_2}\underbrace{0\cdots0}_{n_3-1}0\underbrace{0\cdots01}_{n_4}\cdots\cdots\underbrace{0\cdots0}_{n_{2r-1}-1}0\underbrace{0\cdots010}_{n_{2r}}$$

If $n_{2r} = 1$, we construct (a, b) as

$$a = \underbrace{1\cdots1}_{n_1-1}0\underbrace{1\cdots11}_{n_2}\underbrace{1\cdots1}_{n_3-1}0\underbrace{1\cdots11}_{n_4}\cdots\cdots\underbrace{1\cdots1}_{n_{2r-1}}0$$

$$b = \underbrace{0\cdots0}_{n_1-1}0\underbrace{0\cdots01}_{n_2}\underbrace{0\cdots0}_{n_3-1}0\underbrace{0\cdots01}_{n_4}\cdots\cdots\underbrace{0\cdots0}_{n_{2r-1}}0$$

It's not difficult to verify that (a, b) is a required solution. □

Proposition 3.11. *Assume Conjecture 3.6 is correct. Let $n = 2k$, then the algebraic immunity of function f in Construction 3.1 is at least suboptimal, i.e. $AI_n(f) \geqslant k - 1$.*

Proof. We need to prove that both $f, f + 1$ have no annihilators with degrees $\leqslant k - 2$. Let $h : \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$ satisfy $deg(h) \leqslant k - 2$ and $f \cdot h = 0$. We will prove $h = 0$. Observe that h can be written as a polynomial of two variables on $\mathbb{F}_{2^k}$ as

$$h(x, y) = \sum_{i=0}^{2^k-1}\sum_{j=0}^{2^k-1} h_{i,j}x^i y^j,$$

where $h_{i,j} \in \mathbb{F}_{2^k}$. By $deg(h) \leqslant k-2$, we have $h_{i,j} = 0$ with $w(i) + w(j) \geqslant k-1$. Since $h(x, \gamma x) = 0$ for $x \in \mathbb{F}_{2^k}^*, \gamma \in \Delta := \{\alpha, \alpha^2, \ldots, \alpha^{2^{k-1}-1}\}$. Write

$$h(x, \gamma x) = \sum_{i,j} h_{i,j} x^i (\gamma x)^j = h_{0,0} + \sum_{t=1}^{2^k-2} h_t(\gamma) x^t$$

in which

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

We have $h_{0,0} = 0, h_t(\gamma) = 0$ for $1 \leqslant t \leqslant 2^k - 2, \gamma \in \Delta$. Since h_t has consecutive $2^{k-1} - 1$ roots, by Corollary 3.9, if h_t is not the zero polynomial, then the number of nonzero coefficients of h_t should be greater than or equal to 2^{k-1}. Set $J = \{j \mid j \in \mathbb{Z}, 0 \leqslant j \leqslant 2^k - 2, w(t-j) + w(j) \leqslant k-2\}$. However, by Conjecture 3.6 and Lemma 3.10, we have $|J| \leqslant 2^{k-1} - 1$. Hence $h_t = 0$ for $1 \leqslant t \leqslant 2^k - 2$. So $h = 0$.

Since $supp(f+1) \supseteq \{(x, \alpha^i x) \mid x \in \mathbb{F}_{2^k}^*, i = 2^{k-1}, \ldots, 2^k - 2\}$, a similar argument is applicable to $f+1$, and we can show that $f+1$ has no annihilator of degree $\leqslant k-2$. Therefore $AI_n(f) \geqslant k-1$. □

In fact, we can analyze the algebraic immunity of the given functions in Construction 3.1 more accurately. We will prove that the functions in Construction 3.1 have optimal algebraic immunity when k is odd under the assumption of the correctness of Conjecture 3.6. For this we need the following lemma.

Lemma 3.12. *With the notation of Conjecture 3.6. Assume Conjecture 3.6 is correct. Let k be an odd integer. If $w(t) \leqslant \frac{k-1}{2}$, then $|S_t|$ is strictly less than 2^{k-1}.*

Proof. The proof is straightforward. If $(a, b) \in S_t$, then obviously $(b, a) \in S_t$. Since $(\frac{t}{2}, \frac{t}{2})$ is a solution of S_t if and only if $w(\frac{t}{2}) + w(\frac{t}{2}) = 2w(t) \leqslant k-1$. Hence if $w(t) \leqslant \frac{k-1}{2}$, then $|S_t|$ must be odd, i.e. $|S_t|$ is strictly less than 2^{k-1}. □

Proposition 3.13. *Assume Conjecture 3.6 is correct. Let $n = 2k$. If k is odd, then the algebraic immunity of the function f in Construction 3.1 is optimal, i.e. $AI_n(f) = k$.*

Proof. Similar to the proof of Proposition 3.11, we need to prove that both $f, f+1$ have no annihilators with degrees $\leqslant k-1$. For the sake of completeness, we repeat appropriate parts of the proof of Proposition 3.11. Let $h : \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$ satisfy $deg(h) \leqslant k-1$ and $f \cdot h = 0$. We will prove $h = 0$. Write

$$h(x, y) = \sum_{i=0}^{2^k-1} \sum_{j=0}^{2^k-1} h_{i,j} x^i y^j,$$

where $h_{i,j} \in \mathbb{F}_{2^k}$. By $deg(h) \leqslant k-1$, we have $h_{i,j} = 0$ when $w(i) + w(j) \geqslant k$. Since $h(x, \gamma x) = 0$ for $x \in \mathbb{F}_{2^k}^*, \gamma \in \Delta := \{\alpha, \alpha^2, \ldots, \alpha^{2^{k-1}-1}\}$. Write

$$h(x, \gamma x) = \sum_{i,j} h_{i,j} x^i (\gamma x)^j = h_{0,0} + \sum_{t=1}^{2^k-2} h_t(\gamma) x^t$$

in which

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

We have $h_{0,0} = 0, h_t(\gamma) = 0$ for $1 \leqslant t \leqslant 2^k - 2, \gamma \in \Delta$. Since h_t has consecutive $2^{k-1} - 1$ roots, by Corollary 3.9, if h_t is not the zero polynomial, then the number of nonzero coefficients of h_t should be greater than or equal to 2^{k-1}. Set $J_t = \{j \mid j \in \mathbb{Z}, 0 \leqslant j \leqslant 2^k - 2, w(t-j) + w(j) \leqslant k-1\}$. If $w(t) \leqslant \frac{k-1}{2}$, by Lemma 3.12, we have $|J_t| < 2^{k-1}$. Hence $h_t = 0$ for $w(t) \leqslant \frac{k-1}{2}$. In particular, we have $h_{t,0} = 0$ for $w(t) \leqslant \frac{k-1}{2}$.

Since $h(x, 0) = 0$ for $x \in \mathbb{F}_{2^k} \setminus A = \{\alpha^{2^{k-1}}, \ldots, \alpha^{2^k-2}\}$, i.e.

$$0 = h_{0,0} + \sum_{i=1}^{2^k-2} h_{i,0}x^i := h_0(x).$$

By Corollary 3.9, if h_0 is not the zero polynomial, then the number of nonzero coefficients of h_0 should be greater than or equal to 2^{k-1}. Since the number of $h_{i,0}$ for which $0 \leqslant i \leqslant 2^k - 2$ and $w(i) \leqslant \frac{k-1}{2}$ is $\sum_{j=0}^{(k-1)/2} \binom{k}{j} = 2^{k-1}$, the number of nonzero coefficients of h_0 is $\leqslant 2^k - 1 - 2^{k-1} = 2^{k-1} - 1$. So $h_0 = 0$. Hence $h_{t,0} = 0$ for all $1 \leqslant t \leqslant 2^k - 2$. Therefore, the number of nonzero coefficients of h_t is $\leqslant 2^{k-1} - 1$. So $h_t = 0$ for all $1 \leqslant t \leqslant 2^k - 2$. We have $h = 0$.

Since

$$supp(f+1) \supseteq \{(x, \alpha^i x) \mid x \in \mathbb{F}_{2^k}^*, i = 2^{k-1}, \ldots, 2^k - 2\} \bigcup \{(x, 0) \mid x = 1, \alpha, \ldots, \alpha^{2^{k-1}-1}\},$$

a similar argument is applicable to $f + 1$, and we can show that $f + 1$ has no annihilator of degree $\leqslant k - 1$. Therefore $AI_n(f) = k$. □

For the case of even k, the actual computation by Magma system shows that the functions in Construction 3.1 have optimal algebraic immunity for small k. To deal with this case, we first make some assumption related to Conjecture 3.6.

Assumption A With the notation of Conjecture 3.6. Set $T = \{t \mid 1 \leqslant t \leqslant 2^k - 2, |S_t| = 2^{k-1}\}$. Then $|T| < 2^{k-1}$.

Remark 3.14. *By Lemma 3.12, if the Conjecture 3.6 is correct, then the Assumption A is also true for odd k. For even k, we use the algorithm for validating Conjecture 3.6 in [25] to verify that the Assumption A is true for all even $k \leqslant 28$.*

Proposition 3.15. *Assume both Conjecture 3.6 and Assumption A are correct. Let $n = 2k$. If k is even, then the algebraic immunity of the function f in Construction 3.1 is optimal, i.e. $AI_n(f) = k$.*

Proof. Similarly, we need to prove that both $f, f + 1$ have no annihilators with degrees $\leqslant k - 1$. For the sake of completeness, we repeat appropriate parts of the proof of

Proposition 3.11. Let $h : \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$ satisfy $deg(h) \leqslant k-1$ and $f \cdot h = 0$. We will prove $h = 0$. Write

$$h(x,y) = \sum_{i=0}^{2^k-1} \sum_{j=0}^{2^k-1} h_{i,j} x^i y^j,$$

where $h_{i,j} \in \mathbb{F}_{2^k}$. By $deg(h) \leqslant k-1$, we have $h_{i,j} = 0$ when $w(i) + w(j) \geqslant k$. Since $h(x, \gamma x) = 0$ for $x \in \mathbb{F}_{2^k}^*, \gamma \in \Delta := \{\alpha, \alpha^2, \ldots, \alpha^{2^{k-1}-1}\}$. Write

$$h(x,\gamma x) = \sum_{i,j} h_{i,j} x^i (\gamma x)^j = h_{0,0} + \sum_{t=1}^{2^k-2} h_t(\gamma) x^t$$

in which

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

We have $h_{0,0} = 0, h_t(\gamma) = 0$ for $1 \leqslant t \leqslant 2^k - 2, \gamma \in \Delta$. Since h_t has consecutive $2^{k-1} - 1$ roots, by Corollary 3.9, if h_t is not the zero polynomial, then the number of nonzero coefficients of h_t should be greater than or equal to 2^{k-1}.

Since $h(x,x) = 0$ for $x \in \{\alpha, \alpha^2, \ldots, \alpha^{2^{k-1}-1}\}$, and $h(x,x) = h_{0,0} + \sum_{t=1}^{2^k-2} a_t x^t$, where $a_t := \sum_{i+j \equiv t} h_{i,j} = \sum_{i=0}^{2^k-2} h_{i,t-i}$, we have $\sum_{t=1}^{2^k-2} a_t x^t = 0$ for $x \in \{\alpha, \alpha^2, \ldots, \alpha^{2^{k-1}-1}\}$. Set $T_1 = \{t \mid 1 \leqslant t \leqslant 2^k - 2, |S_t| < 2^{k-1}\}$ and $T_2 = \{t \mid 1 \leqslant t \leqslant 2^k - 2, |S_t| = 2^{k-1}\}$. By Assumption A, we have $|T_2| < 2^{k-1}$. Hence $|T_1| = 2^k - 1 - |T_2| > 2^{k-1} - 1$, i.e. $|T_1| \geqslant 2^{k-1}$. For $t \in T_1$, since $|S_t| < 2^{k-1}$, we have $h_t = 0$, hence $a_t = 0$. So the number of nonzero $a_t (1 \leqslant t \leqslant 2^k - 2)$ is at most $2^{k-1} - 1$. By Corollary 3.9, we have $a_t = 0$ for all $1 \leqslant t \leqslant 2^k - 2$. Thus, since $h_t(1) = a_t$, we have $h_t(\gamma) = 0$ for all $1 \leqslant t \leqslant 2^k - 2$ and for $\gamma \in \{1, \alpha, \alpha^2, \ldots, \alpha^{2^{k-1}-1}\}$. By Conjecture 3.6 and Corollary 3.9, we have $h_t = 0$ for all $1 \leqslant t \leqslant 2^k - 2$, hence $h = 0$.

Since

$$supp(f+1) \supseteq \{(x, \alpha^i x) \mid x \in \mathbb{F}_{2^k}^*, i = 2^{k-1}, \ldots, 2^k - 2\} \bigcup \{(x,x) \mid x = \alpha^{2^{k-1}}, \ldots, \alpha^{2^k-2}\},$$

a similar argument is applicable to $f+1$, and we can show that $f+1$ has no annihilator of degree $\leqslant k-1$. Therefore $AI_n(f) = k$. □

4 Conclusion

In this paper, we construct an infinite class of $2k$-variable boolean functions, which seem to meet all the main criteria for designing Boolean functions: 1-resilient, algebraic degree optimal, having very high nonlinearity. Based on the conjecture proposed in [25], it can be proved that the algebraic immunity of our functions is at least suboptimal. Moreover, when k is odd, the algebraic immunity is actually optimal, and for even k, we find that the

algebraic immunity is optimal at least for $k \leqslant 28$. We believe that this class of functions are of both theoretical and practical importance.

Acknowledgments The work of the first author was supported by the NNSF of China (Grants Nos. 11071285, 61003234). The work of the second author was supported by the NNSF of China (Grants Nos. 11071285, 60821002, 10971250) and 973 Project (2011CB302401).

References

[1] Armknecht F.: Improving fast algebraic attacks. In: 11th International Workshop on Fast Software Encryption, FSE 2004. Lecture Notes in Computer Science, vol. 3017, pp. 65–82 (2004).

[2] Camion P., Carlet C., Charpin P., Sendrier N.: On correlation immune functions. In: Advances in Cryptology, Crypto 91, Lecture Notes in Computer Science, vol. 576, pp. 86–100 (1992).

[3] Carlet C.: On a weakness of the Tu-Deng function and its repair. Cryptology ePrint Archive, Report 2009/606. http://eprint.iacr.org/2009/606.

[4] Carlet C., Dalai D.K., Gupta K.C., Maitra S.: Algebraic immunity for cryptographically significant Boolean functions: analysis and construction. IEEE Trans. Inform. Theory **52**, 3105–3121 (2006).

[5] Carlet C., Feng K.: 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, vol. 5350, pp. 425–440 (2008).

[6] Carlet C., Zeng X., Li C., Hu L.: Further properties of several classes of Boolean functions with optimum algebraic immunity. Des. Codes Cryptogr. **52**, 303–338 (2009).

[7] Chee S., Lee S., Lee D., Sung S.H.: On the correlation immune functions and their nonlinearity. In: Advances in Cryptology, Asiacrypt 96, Lecture Notes in Computer Science, vol. 1163, pp. 232–243 (1996).

[8] Courtois N.T.: Fast algebraic attacks on stream ciphers with linear feedback. In: Advances in Cryptology, Crypto 2003. Lecture Notes in Computer Science, vol. 2729, pp. 176–194 (2003).

[9] Courtois N.T., Meier W.: Algebraic attacks on stream ciphers with linear feedback. In: Advances in Cryptology, Eurocrypt 2003. Lecture Notes in Computer Science, vol. 2656, pp. 345–359 (2003).

[10] Cusick T.W., Li Y., Stănică P.: On a combinatoric conjecture. Cryptology ePrint Archive, Report 2009/554. http://eprint.iacr.org/2009/554.

[11] Dalai D.K., Maitra S., Sarkar S.: Basic theory in construction of Boolean functions with maximum possible annihilator immunity. Des. Codes Cryptogr. **40**, 41–58 (2006).

[12] Dillon J.F.: Elementary Hadamard Difference Sets. PhD thesis, University of Maryland (1974).

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

[14] Filiol E., Fontaine C.: Highly nonlinear balanced Boolean functions with a good correlation-immunity. In Advances in Cryptology, Eurocrypt 98, Lecture Notes in Computer Science, vol. 1403, pp. 475–488 (1998).

[15] Li N., Qi W.: 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, vol. 4284, pp. 84–98 (2006).

[16] Li N., Qu L., Qi W., Feng G., Li C., Xie D.: On the construction of Boolean functions with optimal algebraic immunity. IEEE Trans. Inform. Theory **54**, 1330–1334 (2008).

[17] MacWilliams F.J., Sloane N.J.A.: The Theory of Error-Correcting Codes. North-Holland, Amsterdam (1977).

[18] Maitra S., Pasalic E.: Further constructions of resilient Boolean functions with very high nonlinearity. IEEE Trans. Informa. Theory **48**, 1825–1834 (2002).

[19] Meier W., Pasalic E., Carlet C.: Algebraic attacks and decomposition of Boolean functions. In: Advances in Cryptology, Eurocrypt 2004. Lecture Notes in Computer Science, vol. 3027, pp. 474–491 (2004).

[20] Pasalic E., Johansson T.: Further results on the relation between nonlinearity and resiliency of Boolean functions. In: IMA Conference on Cryptography and Coding, Lecture Notes in Computer Science, vol. 1746, pp. 35–45 (1999).

[21] Pasalic E., Maitra S., Johansson T., Sarkar P.: New Constructions of Resilient and Correlation Immune Boolean Functions Achieving Upper Bound on Nonlinearity. In: International Workshop on Coding and Cryptography, Electronic Notes in Discrete Mathematics, vol. 6, pp. 158–167 (2001).

[22] Rothaus O.S.: On bent functions. J. Combin. Theory A **20**, 300–305 (1976).

[23] Sarkar P., Maitra S.: Nonlinearity bounds and constructions of resilient Boolean Functions. In: Advances in Cryptology, Crypto 2000, Lecture Notes in Computer Science, vol. 1880, pp. 515–532 (2000).

[24] Siegenthaler T.: Correlation-immunity of nonlinear combining functions for cryptographic applications. IEEE Trans. Inform. Theory **IT-30**, 776–780 (1984).

[25] Tu Z, Deng Y.: A conjecture about binary strings and its applications on constructing Boolean functions with optimal algebraic immunity. Des. Codes Cryptogr., 2010. Online First Articles. DOI 10.1007/s10623-010-9413-9.

[26] Wang Q., Peng J., Kan H., Xue X.: Constructions of cryptographiclly significant boolean functions using primitive polynomials. IEEE Trans. Inform. Theory **56**, 3048–3053 (2010).

[27] Xiao G., Massey J.: A spectral characterization of correlation immune combining functions. IEEE Trans. Inform. Theory **34**, 569–571 (1988).