Int J Software Informatics, Volume 8, Issue 2 (2014), pp. 177–192
International Journal of Software and Informatics, ISSN 1673-7288

E-mail: ijsi@iscas.ac.cn
http://www.ijsi.org
Tel: +86-10-62661040

On the Nonlinearity and Correlation Immunity of Two Classes of Boolean Functions

Shaoyu Du[1,2], Meicheng Liu[3], Yin Zhang[3], and Dongdai Lin[3]

[1] (Trusted Computing and Information Assurance Laboratory, Institute of Software, Chinese Academy of Sciences, Beijing 100190, China)

[2] (University of Chinese Academy of Sciences, Beijing 100049, China)

[3] (State Key Laboratory Of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China)

Abstract Recently, Liu et al. have proved a class of $2k$-variable Boolean functions to have optimal algebraic immunity and good immunity to fast algebraic attacks. In this paper, we proceed to study those functions in aspect of correlation immunity and nonlinearity and through restrictions to those functions we propose two sub-classes of $2k$-variable Boolean functions with good cryptographic properties. To the best of our knowledge, this is the first time whole classes of Boolean functions with high nonlinearity, 1-correlation immunity and good immunity against FAA can be found.
Key words: cryptography; Boolean functions; nonlinearity; correlation immunity; resiliency; algebraic immunity

Du SY, Liu MC, Zhang Y, Lin DD. On the nonlinearity and correlation immunity of two classes of Boolean functions. *Int J Software Informatics*, **Vol.8, No.2 (2014): 177–192. http://www.ijsi.org/1673-7288/8/i187.htm**

1 Introduction

A fundamental objective of cryptography is to enable two persons to communicate over an insecure channel in such a way that any other person is unable to recover their message (called the plaintext) from what is sent in its place over the channel (the ciphertext). The transformation of the plaintext into the ciphertext is called encryption. The encryption algorithm takes as input the plaintext and an encryption key and it outputs the ciphertext. If the encryption key is secret, then we speak of symmetric cryptography. In symmetric cryptography, Boolean functions (that is, functions from the vector space F_2^n of all binary vectors of length n, to the finite field with two elements F_2) play important roles. They are frequently used in the design of block ciphers and hash functions and stream ciphers. One of the most vital roles in

Funding by the National 973 Program of China under Grant 2011CB302400, the National Basic Research of China under Grant 2013CB338002, the National Natural Science Foundation of China under Grant 61303258, the Strategic Priority Research Program of the Chinese Academy of Sciences under Grant XDA06010701, and SKLOIS Research Project under Grant 2014-ZD-04.
Corresponding author: Shaoyu Du, Email: du_shaoyu@163.com
Received 2014-06-09; Revised 2014-08-24; Accepted 2014-09-02.

cryptography of Boolean functions is to be used as filter and combination generators of stream cipher based on linear feedback shift registers (LFSR).

The study of the cryptographic criteria of Boolean functions is important because of the connection between known cryptanalysis attacks and these criteria. There are plenty of criteria for Boolean functions, such as balance, nonlinearity, algebraic immunity, the immunity against fast algebraic attack (FAA) and correlation immunity (for balanced functions, correlation immunity is referred to resiliency). Nonlinearity measures the distance between the Boolean function and any affine functions. If the Boolean functions have low nonlinearity then the cryptographic scheme is not secure against linear cryptographic analysis[1,2]. For stream cipher, if the Boolean functions have high correlation immunity[3], then the attacker can conduct the divide-and-conquer correlation attacks[4]. Algebraic immunity[22], which is used to measure functions' ability to resist algebraic attack[9] has been a major parameter in the field of stream cipher since 2003. Later the standard algebraic attack was improved in Ref. [8], where the so-called fast algebraic attack (FAA) was introduced which leads to that Boolean functions need to resist FAA as well.

Unfortunately, all the criteria cannot be maximized together. Constructions of Boolean functions with good cryptography properties are very significant and notable. In the last decade, many constructions of Boolean functions with good algebraic immunity emerged[5,7,10,16,17]. However most of them don't behave well in nonlinearity and correlation immunity and their behaviors in resisting FAA need to be further studied.

In 2008, Carlet-Feng functions[6] which is constructed in finite field were proved to have optimal algebraic immunity, maximal algebraic degree and high nonlinearity. The k-variable Carlet-Feng functions' support has the specific form of $\{1, \alpha, \ldots, \alpha^{2^{k-1}-1}\}$, where α is a primitive element of the $\mathbb{F}_{2^k}$ finite field. It is the first class of functions that meet most of the cryptographic criteria. And it is also the first class of Boolean functions that are proved to have optimal immunity to FAA[19]. For simplicity, here and hereafter ϕ stands the Carlet-Feng functions.

In 2011, Tu and Deng[26] proposed a class of $2k$-variable balanced Boolean functions with optimal algebraic immunity (under an assumption) and very high nonlinearity which is better than Carlet-Feng functions. The functions' form is,

$$F(x, y) = \phi(xy^{-1}) + (x^{2^k-1} + 1)u(y).$$

But functions in Ref. [26] cannot resist FAA.

Using a similar technique as Ref. [26], Tang et al.[25] put forward new constructions. One of the $2k$-variable function in Ref. [25] is of the form,

$$F(x, y) = \phi(xy) + (x^{2^k-1} + 1)u(y),$$

which is proved to have balance, optimal algebraic immunity, good behavior against FAA as well as high nonlinearity.

Furthermore, Jin et al.[14] constructed a class of Boolean functions with 1-resilience, high nonlinearity and optimal algebraic immunity (under some assumption) through modifications to two classes of Boolean functions proposed in Ref. [15] which are inspired by the Boolean functions in Refs. [26,27,25]. However the immunity of the functions against FAA is not discussed.

More recently, Ref. [18] summarized the constructions of Refs. [27,25,15] in aspect of immunity against FAA. A class of functions generalized in Ref. [18] which will be specifically analyzed in the rest of the paper has the form as follows.

$$\tau(x,y) = \phi(xy) + (x^{2^k-1}+1)\psi(y) + (y^{2^k-1}+1)\varphi(x).$$

It is denoted as τ for short in this paper. In Ref. [18], the function τ is proved to have optimal algebraic immunity and good immunity to FAA.

In this paper, we proceed to study other cryptographic properties of τ in aspect of correlation immunity and nonlinearity. If both the function φ and ψ are 1-resilient Boolean functions with high nonlinearity or rotation symmetry Bent functions, we propose two classes of Boolean functions with $2k$ variables. Functions in both classes have high nonlinearity, 1-correlation immunity, optimal algebraic immunity and good immunity to FAA, where the first class contains functions with almost perfect algebraic immune (PAI) which means their immunity to FAA is also almost optimal. The lower nonlinearity bound of functions in the second class is $2^{2k-1} - \frac{k\ln 2+\frac{25}{12}-\ln\frac{9\pi}{8}}{\pi}2^k - 2^{k/2} - 2$, which is very close to that of functions proposed by Tang et al.[25]. We do experiments to verify the nonlinearity of the two classes of functions, which show they behave better in reality.

The structure of this paper is as follows. In Section 2, the notations and the necessary preliminaries are presented. In Section 3, we analyze τ functions in consideration of correlation immunity and nonlinearity. Two specific constructions by restricting ψ and φ are proposed respectively in Section 4, as well as the proofs of cryptographic properties. The implement methods and experimental results on nonlinearity compared with Ref. [25] are listed in Section 5. Finally, Section 6 concludes the paper.

2 Preliminaries

In this section, we first define Boolean functions and its different representations, including algebraic normal form, univariate representation and bivariate representation. We then give brief descriptions of the criteria m-correlation immunity, nonlinearity, algebraic immunity, optimal algebraic immunity etc..

Let $\mathbb{F}_2^n$ denote the n-dimensional vector space over the field $\mathbb{F}_2 = \{0,1\}$ of two elements and $\mathbb{F}_{2^n}$ denote the finite field of order 2^n. An n-variable Boolean function is a mapping from $\mathbb{F}_2^n$ into $\mathbb{F}_2$. We denote by $\mathbf{B}_n$ the set of all the Boolean functions of n variables. The *truth table* of a Boolean function $f(x_1,\cdots,x_n)$ is $f = [f(0,0,\cdots,0), f(1,0,\cdots,0), f(0,1,\cdots,0), f(1,1,\cdots,0),\cdots, f(1,1,\cdots,1)]$.

The support of f is denoted by $supp(f) = \{x \in \mathbb{F}_2^n | f(x) = 1\}$. The size of set $supp(f)$ is the *hamming weight* of the function f, denoted by $wt(f)$. If $wt(f) = 2^{n-1}$, then f is called *balanced*. Similarly, for $x = (x_1,\ldots,x_n) \in \mathbb{F}_{2^n}$ where $x_i \in \mathbb{F}_2$ ($i \in [1,\ldots,n]$) and $(x_1,\ldots,x_n)$ is the binary vector of length n relative to a fixed basis, $wt(x)$ is the number of ones in $(x_1,\ldots,x_n)$.

Another representation of f is *algebraic normal form* (ANF),

$$f(x_1,\cdots,x_n) = \bigoplus_{u\in\mathbb{F}_2^n} a_u \left(\prod_{j=1}^{n} x_j^{u_j}\right),$$

where $a_u \in \mathbb{F}_2$ and $u = (u_1, \cdots, u_n)$. The *algebraic degree* of f $deg(f)$ is defined as $\max\{wt(c)|a_c \neq 0\}$. A Boolean function is called *affine function* if $deg(f) \leqslant 1$. We denote $\mathbb{A}_n$ as the set of all affine functions in $\mathbb{B}_n$.

The *univariate representation* of Boolean function f is denoted in the field $\mathbb{F}_{2^n}$,i.e.,

$$f(x) = \sum_{i=0}^{2^n-1} \lambda_i x^i, \lambda_i \in \mathbb{F}_{2^n},$$

where $f^2(x) \equiv f(x)(\mathrm{mod}x^{2^n} - x)$. It is well known that $f^2(x) \equiv f(x)(\mathrm{mod}x^{2^n} - x)$ if and only if $\lambda_0, \lambda_{2^n-1} \in \mathbb{F}_2$ and for $1 \leqslant i \leqslant 2^n - 2$, $\lambda_{2i \bmod (2^n-1)} = \lambda_i^2$. Moreover, when n is even, the Boolean function f can be uniquely expressed by a *bivariate representation* over $\mathbb{F}_{2^{n/2}}^2$

$$f(x, y) = \sum_{i,j=0}^{2^{n/2}-1} a_{i,j} x^i y^j,$$

where $a_{i,j} \in \mathbb{F}_{2^{n/2}}$.

The *Walsh spectrum* of a Boolean function f at point w is defined as

$$W_f(w) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+w \cdot x}, w \in \mathbb{F}_2^n,$$

where $\cdot$ means inner product. Notice that the Walsh spectrum of Boolean function f defined in the field $\mathbb{F}_{2^n}$ is

$$W_f(w) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+tr(wx)}, w \in \mathbb{F}_{2^n},$$

where tr is the trace from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. And for bivariate polynomial expressed function f, it is

$$W_f(a, b) = \sum_{(x,y) \in \mathbb{F}_{2^{n/2}} \times \mathbb{F}_{2^{n/2}}} (-1)^{f(x,y)+tr(ax+by)}, a, b \in \mathbb{F}_{2^{n/2}},$$

where tr is the trace from $\mathbb{F}_{2^{n/2}}$ to $\mathbb{F}_2$.

If $W_f(w) = 0$ for $1 \leqslant wt(w) \leqslant m$, then f is said to have *m-correlation immunity*. Besides, we say f is *m-resilient* if f is balanced.

The *nonlinearity* of f is the minimum Hamming distance between f and any affine functions. Considering the Walsh spectrum, the nonlinearity of $f \in \mathbb{B}_n$ is

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

or

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

The *algebraic immunity* $AI(f)$ of the n-variable Boolean function f is defined to be the lowest degree of nonzero functions g such that $fg = 0$ or $(f+1)g = 0$. In order to resist algebraic attacks, Boolean functions should have high algebraic immunity. The optimal algebraic immunity for n-variable Boolean function f is $\lceil \frac{n}{2} \rceil$.

Furthermore, if there is a nonzero Boolean function g with degree at most e such that the product gf has degree at most d, with e small and d not too large, then

the Boolean function f is considered to be weak against fast algebraic attacks. The exact values of e and d for which a fast algebraic attack is feasible depends on several parameters, like the size of the memory and the key size of the stream cipher[13].

3 On the Correlation Immunity and Nonlinearity of τ Function

The elaborate definition of function τ, as well as the limits of function ϕ, φ and ψ in Ref. [18], is provided as follows.

Definition 3.1. Define a $2k$-variable Boolean function

$$\tau(x,y) = \phi(xy) + (x^{2^k-1}+1)\psi(y) + (y^{2^k-1}+1)\varphi(x),$$

where ϕ, φ and ψ are k-variable Boolean functions from $\mathbb{F}_{2^k}$ to $\mathbb{F}_2$. And $\tau(x,y)$ satisfies the two conditions below,

1. $supp(\phi) = \{\alpha^i | 0 \leqslant i \leqslant 2^{k-1}-1\}, \alpha$ *is a primitive element of* $\mathbb{F}_{2^k}$,
2. $0 \notin supp(\psi)$ *or* $0 \notin supp(\varphi)$.

3.1 Correlation immunity

The correlation immunity of the function τ in Definition 3.1 can be trivially derived. For simplicity, we use $\Phi(x,y)$ to denote $\phi(xy)$. Then τ can be expressed as

$$\tau(x,y) = \Phi(x,y) + (x^{2^k-1}+1)\psi(y) + (y^{2^k-1}+1)\varphi(x).$$

Theorem 3.1. The function τ in Definition 3.1 has 1-correlation immunity if for $a \in \mathbb{F}_{2^k}$ such that $wt(a) = 1$, the functions φ and ψ satisfy that

$$W_\psi(0) + W_\varphi(a) = 0, \tag{1}$$
$$W_\psi(a) + W_\varphi(0) = 0. \tag{2}$$

Proof: We need to verify that $W_\tau(a,b) = 0$ for every $(a,b) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$ satisfying $wt(a,b) = 1$. Firstly note that for $(a,b) \neq (0,0)$,

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

where tr is the trace from $\mathbb{F}_{2^k}$ to $\mathbb{F}_2$. Then

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

Next since

$$supp(\Phi(x,y)) \cap supp((x^{2^k-1}+1)\psi(y)) \cap supp((y^{2^k-1}+1)\varphi(x)) = \emptyset$$

from the second item of Definition 3.1, it infers that

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

$$
\begin{aligned}
&= \sum_{(x,y)\in supp(\Phi(x,y))} (-1)^{tr(ax+by)} \\
&\quad + \sum_{(x,y)\in supp((x^{2^k-1}+1)\psi(y))} (-1)^{tr(ax+by)} + \sum_{(x,y)\in supp((y^{2^k-1}+1)\varphi(x))} (-1)^{tr(ax+by)} \\
&= \sum_{i=0}^{2^{k-1}-1} \sum_{x\in\mathbb{F}_{2^k}^*} (-1)^{tr(ax+bx^{-1}\alpha^i)} + \sum_{y\in supp(\psi)} (-1)^{tr(by)} + \sum_{x\in supp(\varphi)} (-1)^{tr(ax)}.
\end{aligned}
$$

Then Classify $(a,b) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$ into two kinds of points and consider their Walsh spectra:

- $b = 0$, $a \neq 0$ and $wt(a) = 1$,

$$
\begin{aligned}
&\sum_{(x,y)\in supp(f)} (-1)^{tr(ax+by)} \\
&= \sum_{i=0}^{2^{k-1}-1} \sum_{x\in\mathbb{F}_{2^k}^*} (-1)^{tr(ax)} + \sum_{y\in supp(\psi)} (-1)^{tr(0)} + \sum_{x\in supp(\varphi)} (-1)^{tr(ax)} \\
&= -2^{k-1} + wt(\psi) - \frac{1}{2}W_\varphi(a) = -\frac{1}{2}W_\psi(0) - \frac{1}{2}W_\varphi(a);
\end{aligned} \tag{3}
$$

- $a = 0$, $b \neq 0$ and $wt(b) = 1$,

$$
\begin{aligned}
&\sum_{(x,y)\in supp(f)} (-1)^{tr(ax+by)} \\
&= \sum_{i=0}^{2^{k-1}-1} \sum_{x\in\mathbb{F}_{2^k}^*} (-1)^{tr(bx^{-1}\alpha^i)} + \sum_{y\in supp(\psi)} (-1)^{tr(by)} + \sum_{x\in supp(\varphi)} (-1)^{tr(0)} \\
&= -2^{k-1} + wt(\varphi) - \frac{1}{2}W_\psi(b) = -\frac{1}{2}W_\varphi(0) - \frac{1}{2}W_\psi(b).
\end{aligned} \tag{4}
$$

Finally if (3) and (4) are both equal to 0, then τ has 1-correlation immunity. Therefore this theorem is verified. □

There are plenty of φ and ψ functions satisfying Theorem 3.1, since in this theorem the specific values of $W_\varphi(0)$ and $W_\psi(0)$ are not limited. For example, if φ and ψ are 1-resilient Boolean functions, then the theorem holds. But not all the τ functions that have 1-correlation immunity behave good in other cryptographic properties.

3.2 Resiliency

Furthermore, if τ is balanced, i.e., $wt(\tau) = 2^{2k-1}$, then it will be 1-resilient. Since $supp(\Phi) \cap supp((x^{2^k-1}+1)\psi(y)) \cap supp((y^{2^k-1}+1)\varphi(x)) = \emptyset$, we have $wt(\tau) = wt(\Phi) + wt(\psi) + wt(\varphi)$. Remind the fact that $supp(\Phi) = \{(x, x^{-1}\alpha^i) | 0 \leqslant i \leqslant 2^{k-1} - 1, x \in \mathbb{F}_{2^k}^*\}$, which means $wt(\Phi) = (2^k - 1) \cdot 2^{k-1} = 2^{2k-1} - 2^{k-1}$. Consequently when $wt(\tau) = 2^{2k-1}$, it can be deduced that

$$
wt(\varphi) + wt(\psi) = 2^{k-1}. \tag{5}
$$

Then we have the following corollary.

Corollary 3.1. The function τ in Definition 3.1 is 1-resilient only when $k = 2$ or $k = 3$.

Proof: Based on Eq. (5) we classify ψ and φ into two cases.

Case1 : $wt(\varphi) = wt(\psi) = 2^{k-2}$.

From the condition, it can be derived that $W_\psi(0) = W_\varphi(0) = 2^{k-1}$. And in order to satisfy (1)(2) in Theorem 3.1, we get $W_\psi(b) = W_\varphi(a) = -2^{k-1}$, i.e., $W^2_\varphi(a) = W^2_\psi(b) = 2^{2k-2}$, for $a, b \in \mathbb{F}_{2^k}$ that $wt(a) = wt(b) = 1$.

Then due to the **Parseval** identical relation

$$\sum_{w\in\mathbb{F}_{2^k}} W^2_f(w) = 2^{2k},$$

k can only take values 2 or 3 to make φ and ψ satisfy the condition.

Case2 : $wt(\varphi) \neq wt(\psi)$.

Consider the function whose weight is larger than 2^{k-2}, which is assumed to be φ. Then as a similar analysis of Case 1, it can induces that $W_\varphi(0) > 2^{k-1}$ and $W^2_\psi(a) > 2^{2k-2}$, for $a \in \mathbb{F}_{2^k}$ that $wt(a) = 1$. We can also conclude that only when $k = 2$ or $k = 3$ can τ be 1-resilient based on the **Parseval** identical relation. □

The results show that τ is not 1-resilient when k is large.

3.3 Nonlinearity

Next we focus on the nonlinearity of τ. Before obtaining a lower bound on the nonlinearity of τ, we need the following lemma.

Lemma 3.1.[28] For $n = 2k$, the lower bound on the nonlinearity of the function $\Phi(x, y)$ is:

$$N_\Phi > 2^{n-1} - \frac{k\ln 2 + \frac{25}{12} - \ln\frac{9\pi}{8}}{\pi} 2^k - 1.$$

The proof of Lemma 3.1 excerpted from Ref. [28] can be found in Appendix B. Next the lower bound on the nonlinearity of τ can be proved.

Theorem 3.2. The nonlinearity of the function τ in Definition 3.1 satisfies that

$$N_\tau > 2^{2k-1} - \frac{k\ln 2 + \frac{25}{12} - \ln\frac{9\pi}{8}}{\pi} 2^k - 2^{k+1} - 2.$$

Proof: According to the definition of Walsh transform, for any $(a, b) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$, we have

$$\begin{aligned}
&W_\tau(a, b)\\
&= \sum_{x,y\in\mathbb{F}_{2^k}} (-1)^{\tau(x,y)+tr(ax+by)}\\
&= \sum_{x,y\in\mathbb{F}^*_{2^k}} (-1)^{\Phi(x,y)+tr(ax+by)} + \sum_{y\in\mathbb{F}^*_{2^k}} (-1)^{\psi(y)+tr(by)} + \sum_{x\in\mathbb{F}^*_{2^k}} (-1)^{\varphi(x)+tr(ax)} + 1\\
&= \sum_{x,y\in\mathbb{F}_{2^k}} (-1)^{\Phi(x,y)+tr(ax+by)} - \sum_{y\in\mathbb{F}_{2^k}} (-1)^{tr(by)} - \sum_{x\in\mathbb{F}_{2^k}} (-1)^{tr(ax)} + 1
\end{aligned}$$

$$
\begin{aligned}
&+\sum_{y\in\mathbb{F}_{2^k}}(-1)^{\psi(y)+tr(by)}-(-1)^{\psi(0)}+\sum_{x\in\mathbb{F}_{2^k}}(-1)^{\varphi(x)+tr(ax)}-(-1)^{\varphi(0)}+1\\
&=W_\Phi(a,b)+W_\psi(b)+W_\varphi(a)\\
&\quad-\sum_{y\in\mathbb{F}_{2^k}}(-1)^{tr(by)}-\sum_{x\in\mathbb{F}_{2^k}}(-1)^{tr(ax)}+2-(-1)^{\psi(0)}-(-1)^{\varphi(0)}
\end{aligned}
$$

Since for n-variable Boolean function f, $W_f(0)=2^n-2wt(f)$, then

$$
W_\tau(a,b)=\begin{cases}
2^k-2wt(\varphi)-2wt(\psi)+2-(-1)^{\psi(0)}-(-1)^{\varphi(0)}, & \text{if } a=0,b=0;\\
2^k-2wt(\varphi)+W_\psi(b)+2-(-1)^{\psi(0)}-(-1)^{\varphi(0)}, & \text{if } a=0,b\neq 0;\\
2^k-2wt(\psi)+W_\varphi(a)+2-(-1)^{\psi(0)}-(-1)^{\varphi(0)}, & \text{if } a\neq 0,b=0;\\
W_\Phi(a,b)+W_\psi(b)+W_\varphi(a)+2-(-1)^{\psi(0)}-(-1)^{\varphi(0)}, & \text{if } a\neq 0,b\neq 0.
\end{cases}
$$

Remind that $0\notin supp(\psi)$ or $0\notin supp(\varphi)$ and note the facts: $\max_{a,b\in\mathbf{F}_{2^k}}|W_\Phi(a,b)|>2^k$, $\min_\varphi wt(\varphi)=\min_\psi wt(\psi)=0$ and $\max_{a\in\mathbf{F}_{2^k}}|W_\varphi(a)|=\max_{b\in\mathbf{F}_{2^k}}|W_\psi(b)|=2^k$.

Consequently,

$$
\max_{a,b\in\mathbb{F}_{2^k}}|W_\tau(a,b)|\leqslant\max_{a,b\in\mathbf{F}_{2^k}}|W_\Phi(a,b)|+\max_{a\in\mathbf{F}_{2^k}}|W_\varphi(a)|+\max_{b\in\mathbf{F}_{2^k}}|W_\psi(b)|+2. \tag{6}
$$

Finally, due to Lemma 3.1 and the definition of nonlinearity of the function τ, the theorem is proved. □

The bound is directly derived from the definition of Φ, φ and ψ and it is relax, which means there should be plenty of τ function that have much higher nonlinearity.

4. Constructing Two Sub-Classes of Boolean Functions Based on τ Function

In Ref. [18], τ is proved to achieve optimal algebraic immunity and (almost) optimal immunity against FAA. And from Eq. (6), we find if we choose ψ and φ from functions with high nonlinearity, the lower bound on the nonlinearity of the function τ in Definition 3.1 will be higher. Moreover the correlation immunity of τ need to be guaranteed as well. Then there are two classes of functions with high nonlinearity that can satisfy Theorem 3.1: 1-resilient Boolean functions with high nonlinearity and certain class of Bent functions. We utilize them to construct two sub-classes of functions which both process high nonlinearity, 1-correlation immunity, optimal algebraic immunity and good immunity to FAA from τ functions in this section. It is notable that there are two propositions in aspect of τ's immunity against FAA which will be used.

Proposition 4.1.[18] Let $k\geqslant 3$ and $1\leqslant e\leqslant k$. If e is even and $\binom{k-1}{\frac{e}{2}}\equiv 1 mod 2$, then τ admits no zero function $g\in\mathbf{B}_{2k}$ with algebraic degree at most e such that $g\tau$ has degree at most $2k-e-3$; otherwise, τ admits no nonzero function $g\in\mathbf{B}_{2k}$ with algebraic degree at most e such that $g\tau$ has degree at most $2k-e-2$.

Proposition 4.2.[18] Let $k\geqslant 3$. If the univariate polynomial representation of φ and ψ has a monomial with algebraic degree equal to $k-1$, $k-2$ (when $k\geqslant 4$), or $k-3$ (when $k\geqslant 6$), then for any positive integer e with $e<k$, τ admits no nonzero

function $g \in \mathbf{B}_{2k}$ with algebraic degree at most e such that $g\tau$ has degree at most $2k-e-2$.

4.1 Functions constructed using 1-resilient Boolean functions and their properties

Construction 4.1. Let $k \geqslant 4$ be an even integer. Define a $2k$-variable Boolean function $\tau_1(x,y) = \phi(xy) + (x^{2^k-1}+1)\psi(y) + (y^{2^k-1}+1)\varphi(x)$, where ϕ, φ and ψ are k-variable Boolean functions from $\mathbb{F}_{2^k}$ to $\mathbb{F}_2$, and τ_1 satisfies

1. $supp(\phi) = \{\alpha^i | 0 \leqslant i \leqslant 2^{k-1}-1\}, \alpha is\ a\ primitive\ element\ of \mathbb{F}_{2^k}$,
2. $0 \notin supp(\psi)\ or\ 0 \notin supp(\varphi)$,
3. φ and ψ are 1-resilient functions with nonlinearity NL whose univariate polynomial representation has a monomial with algebraic degree equal to $k-2$ (when $k \geqslant 4$), or $k-3$ (when $k \geqslant 6$).

Remark 4.1. The third item of Construction 4.1 guarantees the function's (almost) optimal immunity against FAA based on Proposition 4.2. Actually the algebraic degree of φ and ψ in Construction 4.1 can be smaller, then τ_1 will have nearly (almost) optimal immunity against FAA according to Proposition 4.1.

Theorem 4.1. The function τ_1 in Construction 4.1 has optimal algebraic immunity, (almost) optimal immunity against FAA and 1-correlation immunity. The nonlinearity of τ_1 is

$$N_{\tau_1} > 2^{2k-1} - \frac{k\ln 2 + \frac{25}{12} - \ln\frac{9\pi}{8}}{\pi} 2^k - 2^k + 2NL - 2.$$

Proof: Due to Ref. [18] and Proposition 4.2, τ_1 has optimal algebraic immunity and (almost) optimal immunity against FAA.

For k-variable 1-resilient Boolean function f, $wt(f) = 2^{k-1}$ and $W_f(\omega) = 0$ for $\omega \in \mathbb{F}_{2^k}$ that $wt(\omega) = 1$. Since φ and ψ are 1-resilient, then we can deduce that

$$W_\psi(0) + W_\varphi(a) = 0,$$
$$W_\psi(a) + W_\varphi(0) = 0,$$

for $a \in \mathbb{F}_{2^k}$ satisfy that $wt(a) = 1$. Then combining Theorem 3.1 we know τ_1 has 1-correlation immunity.

Since the nonlinearity of ψ and φ is NL from the third item in Construction 4.1, it can be deduce that

$$max_a|W_\varphi(a)| = max_b|W_\psi(b)| = 2^k - 2NL.$$

Substituting it to the proof of Theorem 3.2 we get this theorem. □

Theorem 4.1 shows the lower nonlinearity bound of τ_1 increases with NL. In order to improve the nonlinearity of τ_1 we can choose 1-resilient Boolean functions satisfying the items in Construction 4.1 whose nonlinearity is as high as possible to be φ and ψ. A class of functions of such kind are used in Section 5 to verify the nonlinearity of τ_1. Below is a small example when $k = 4$.

Example 4.1. Let the 4-variable Boolean function $f(x_4, x_3, x_2, x_1) = x_4x_3 + x_4x_1 + x_4 + x_3 + x_2 + 1$ be φ and ψ. One of f' univariate polynomial representations is $f(x) = w^4x^{12} + w^{10}x^{10} + w^7x^8 + w^2x^6 + w^5x^5 + w^{11}x^4 + wx^3 + w^{13}x^2 + w^{14}x + 1$, where $w \in \mathbb{F}_{2^4}$ is a primitive element and (x_1, x_2, x_3, x_4) corresponds to $x_1 + x_2w + x_3w^2 + x_4w^3$. The function f is 1-resilient and its nonlinearity is 4. Obviously all the items in Construction 4.1 are satisfied. Then we can verify that the constructed τ_1 function has 1-correlation immunity and its nonlinearity is 108, with optimal algebraic immunity and (almost) optimal immunity against FAA.

4.2 Functions constructed using bent functions and their properties

Construction 4.2. Let $k \geqslant 4$ be an even integer. Define a $2k$-variable Boolean function $\tau_2(x, y) = \phi(xy) + (x^{2^k-1} + 1)\psi(y) + (y^{2^k-1} + 1)\varphi(x)$, where ϕ, φ and ψ are k-variable Boolean functions from $\mathbb{F}_{2^k}$ to $\mathbb{F}_2$, and τ_2 satisfies

1. $supp(\phi) = \{\alpha^i | 0 \leqslant i \leqslant 2^{k-1} - 1\}$, α *is a primitive element of* $\mathbb{F}_{2^k}$,
2. $0 \notin supp(\psi)$ *or* $0 \notin supp(\varphi)$,
3. φ and ψ are Bent functions,
4. $W_\psi(0) + W_\varphi(a) = 0$ and $W_\varphi(0) + W_\psi(a) = 0$, for $a \in \mathbb{F}_{2^k}$ satisfying $wt(a) = 1$.

Because the nonlinearity of n-variable Bent function reaches the highest nonlinearity bound $(2^{n-1} - 2^{n/2-1})$, the lower bound on nonlinearity of the function τ_2 in Construction 4.2 is larger than that of the function τ_1 in Construction 4.1.

Theorem 4.2. The function τ_2 in Construction 4.2 has optimal algebraic immunity, nearly (almost) optimal immunity against FAA and 1-correlation immunity. The nonlinearity of τ_2 is

$$N_{\tau_2} > 2^{2k-1} - \frac{k \ln 2 + \frac{25}{12} - \ln \frac{9\pi}{8}}{\pi} 2^k - 2^{k/2} - 2.$$

Proof: Due to Ref. [18] and Proposition 4.1, τ_2 has optimal algebraic immunity and can only have nearly (almost) optimal immunity against FAA since the algebraic degree of k-variable Bent functions cannot exceed $k/2$. The fourth item in Construction 4.2 guarantees τ_2 to have 1-correlation immunity, obviously.

For nonlinearity, the functions φ and ψ are Bent functions, which means

$$\max_a |W_\varphi(a)| = \max_b |W_\psi(b)| = 2^{k/2}.$$

Substituting it to the proof of Theorem 3.2, we get this theorem. □

Generally, it seems hard to construct the functions φ and ψ in Construction 4.2. But it is common in the class of rotation symmetric Bent Boolean functions[11,12].

Lemma 4.1.[24] Let $k \geqslant 2$, $u, v \in \{0, 1\}^k$ and $u \neq v$. Let f be a k-variable rotation symmetry Boolean function. Then $W_f(u) = W_f(v)$ for $wt(u) = wt(v) = 1$.

Theorem 4.3. The function τ_2 in Construction 4.2 exists.

Proof: Firstly choose k-variable rotation symmetry Bent Boolean functions f that satisfy $f(0) = 0$. Actually, if there is a k-variable rotation symmetry Bent

Boolean function g satisfies $g(0) = 1$, then we can choose $f = g + 1$, which is also a k-variable rotation symmetry Bent Boolean function but satisfies $f(0) = 0$. Next, Classify the discussion into two cases based on the value of $W_f(0)$.

Case1 : $W_f(0) = 2^{\frac{k}{2}}$.

Based on Lemma 4.2, for a satisfying $wt(a) = 1$, we set $\varphi = f$ and $\psi = f$ if $W_f(a) = -2^{\frac{k}{2}}$. Otherwise we set $\varphi = f + 1$ and $\psi = f$. Then the fourth item in Construction 4.2 is satisfied.

Case2 : $W_f(0) = -2^{\frac{k}{2}}$.

Based on Lemma 4.2, for a satisfying $wt(a) = 1$, we set $\varphi = f$ and $\psi = f$ if $W_f(a) = 2^{\frac{k}{2}}$. Otherwise we set $\varphi = f + 1$ and $\psi = f$. Then the fourth item in Construction 4.2 can also be satisfied.

Furthermore, the second item has already been satisfied because $f(0) = 0$. Then Construction 4.2 are effective. □

The construction of rotation symmetric Bent Boolean functions is an important issue for many years. Recently, Gao et al.[12] proposed classes of quadratic and cubic rotation symmetric Bent Functions, one of which have functions with algebraic degree equal to 3. Along with more constructions of symmetric rotation Bent Boolean functions with good cryptographic properties being constructed, the functions in Construction 4.2 are more robust. The following example is a simple rotation symmetric Bent Boolean function which can be used to construct τ_2.

Example 4.2. The 4-variable function $f(x_1, x_2, x_3, x_4) = x_1x_2+x_1x_3+x_1x_4+x_2x_3+x_2x_4+x_3x_4+1$ can be φ and ψ in Construction 4.2. It can be verified that f is a rotation symmetric Bent Boolean function and $W_f(0) = 4$, $W_f(a) = -4$ for every a satisfying $wt(a) = 1$.

It is worth to mention that we only give the existence of such functions and there should be more functions satisfying the items of construction 4.2, which are not only restricted to rotation symmetric Bent Boolean functions. In example 3, two common 4-variable Bent Boolean functions are given, which satisfy the items in Construction 4.2.

Example 4.3. The 4-variable functions $f1(x_1, x_2, x_3, x_4) = x_1x_4 + x_2x_3$ can be φ and $f2(x_1, x_2, x_3, x_4) = x_1x_4 + x_2x_3 + 1$ can be ψ. They are Bent Boolean functions but not belonging to the class of rotation symmetric functions. And $W_{f1}(0) = W_{f1}(a) = -4$ while $W_{f2}(0) = W_{f2}(a) = 4$ for all a that $wt(a) = 1$.

Actually, experiments show that there are 112 4-variable Bent Boolean functions (see Appendix A) that satisfy the condition $W_f(a)$ take the same value for all $a \in \mathbb{F}_{2^k}$ satisfying $wt(a) = 1$ when the total number of 4-variable Bent Boolean function is 896. It means that about 12.5% 4-variable Bent functions can be choose to be φ and ψ functions in Construction 4.2, which is a remarkable percentage.

5 Experimental Nonlinearity Results and Comparisons

For many years, different methods have been used to find 1-resilient functions reaching high nonlinearity bounds. Among them there are certain classes of functions f that satisfy the items in Construction 4.1 and own high nonlinearity such as the

functions of small number variables in Refs. [21,20], whose nonlinearity can reach

$$N_f = \begin{cases} 2^{k-1} - 4, & k = 4, \\ 2^{k-1} - 2^{\frac{k}{2}-1} - 4, & k \text{ is even and } 6 \leqslant k \leqslant 14. \end{cases}$$

Using them to construct the functions τ_1 in Construction 4.1 can make the nonlinearity behave better. For this reason, we choose them as φ and ψ in Construction 4.1 to verify the theoretical bounds and implement experiments when $k \leqslant 14$. And for Construction 4.2 we let φ and ψ be quadratic symmetric Bent function shown in Proposition 5.1 in experiments.

Proposition 5.1.[23] If f is a symmetric function of an even number n of variables, then the following statements are equivalent:

1. the function f is a Bent function;
2. the ANF of f is

$$f(x) = \bigoplus_{i<j} x_i x_j \oplus \Big(\bigoplus_i c x_i \Big) \oplus d, \ c, d \in \mathbb{F}_2.$$

Table 1[1] and Table 2 show the comparisons on nonlinearity among τ_1, τ_2 and functions constructed in Ref. [25] (called TCT for short). From the tables we know that our functions, especially τ_2, have better theoretical lower bounds of nonlinearity than that of TCT functions in Ref. [25]. Though the application of Lemma 3.1 to TCT functions will make their theoretical lower bounds higher, the actual nonlinearity of our functions are quite higher than the theoretical lower bounds on nonlinearity and they are very close to the actual nonlinearity of the TCT functions. Moreover, TCT functions are balanced, while the functions τ_1 and τ_2 have 1-correlation immunity. As to immunity against FAA, τ_1 even τ_2 have better behavior than almost all the other constructions.

Table 1 Comparison of theoretical lower bounds on nonlinearity

$2k$	8	12	16	20	24	28	32	36
TCT[25]	102	1929	32195	521577	8376003	134160165	2147224628	34358586905
τ_1	99	1928	32223	521719	8376619	134162700	–	–
τ_2	103	1936	32231	521727	8376627	134162708	2147234913	34358628272

Table 2 Comparison of experimental values of nonlinearity

$2k$	8	12	16	20
TCT	108	1982	32508	523144
τ_1	108	1976	32498	523118
τ_2	108	1980	32504	523132

[1]There are no values corresponding to the cases where 2k is 32 and 36 since we only use the 1-resilient functions proved to have the highest nonlinearity[21,20] to be φ and ψ. It will make the theoretical lower nonlinearity bound of τ_2 higher. But only functions of small number variables ($k \leqslant 14$) have been proved to reach the bound until now.

6 Conclusion

In this paper, we mainly analyze the properties, such as correlation immunity and nonlinearity, of a class of functions proposed in Ref. [18] by Liu et.al. Based on functions in Ref. [18], we proposed two sub-classes of functions reaching 1-correlation immunity, high nonlinearity, optimal algebraic immunity and good immunity against FAA. Specifically, the first sub-class of functions have (almost) optimal immunity against FAA and the second sub-class of functions reach nearly (almost) optimal immunity against FAA with higher nonlinearity. To the best of our knowledge, this is the first time whole classes of Boolean functions with 1-correlation immunity and good behavior to FAA can be found.

The summary of the theoretical lower nonlinearity bounds and the experimental nonlinearity results are revealed in Table 1 and Table 2, which are compared with that of the TCT functions. Experiments show that the gap of actual nonlinearity between our functions and the balanced TCT functions is small. Moreover, the functions proposed in this paper may have higher nonlinearity by trying more φ and ψ and they have optimized almost all the cryptographic criteria. However, our functions are not balanced. It is worth further studying the constructions of resilient functions with good immunity to FAA.

References

[1] Matsui M. Linear cryptanalysis methord for DES cipher. Proc. of Eurocrypt'93, Lecture Notes in Computer Science, 1994, 765: 386–397.

[2] Meier W, Staffelbach O. Fast correlation attacks on stream ciphers. Advances in Cryptology, Euroctypt'88, Lecture Notes in Computer Science, 1988, 330: 301–314.

[3] Siegenthaler T. Correlation-immunity of nonlinear combining functions for cryptographic applications. IEEE Trans. on Information Theory, 1984, 30(5): 776–780.

[4] Siegenthaler T. Decrypting a class of stream cihpers using ciphertext only. IEEE Trans. on Computer, 1985, C-34(1): 81–85.

[5] Carlet C, Dalai DK, Gupta KC, Maitra S. Algebraic immunity for cryptographically significant Boolean functions: analysis and construction. IEEE Trans. on Information Theory, 2006, 52(7): 3105–3121.

[6] Carlet C, Feng K. An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity. Advances in Cryptology-ASIACRYPT 2008, LNCS 5350. Springer Berlin Heidelberg. 2008. 425–440.

[7] Carlet C, Zeng X, Li C, Hu L. Further properties of several classes of Boolean functions with optimum algebraic immunity. Designs, Codes and Cryptography, 2009, 52(3): 303–338.

[8] Courtois N. Fast algebraic attacks on stream ciphers with linear feedback. Advances in Cryptology - CRYPTO 2003, LNCS 2729. Springer Berlin Heidelberg. 2003. 176–194.

[9] Courtois N, Meier W. Algebraic attacks on stream ciphers with linear feedback. Advances in Cryptology - EUROCRYPT 2003, LNCS 2656. Springer Berlin Heidelberg. 2003. 644–644.

[10] Dalai DK, Maitra S, Sarkar S. Basic theory in construction of Boolean functions with maximum possible annihilator immunity. Designs, Codes and Cryptography, 2006, 40(1): 41–58.

[11] Dalai DK, Maitra S, Sarkar S. Results on rotation symmetric bent functions. Discrete Mathematics, 2009, 309(8): 2398–2409.

[12] Gao G, Zhang X, Liu W, Carlet C. Constructions of quadratic and cubic rotation symmetric bent functions. IEEE Trans. on Information Theory, 2012, 58(7): 4908–4913.

[13] Hawkes P, Rose G. Rewriting variables: The complexity of fast algebraic attacks on stream ciphers. Advances in Cryptology - CRYPTO 2004, LNCS 3152, chapter.24. Springer Berlin Heidelberg. 2004. 390–406.

[14] Jin Q, Liu Z, Wu B. 1-resilient Boolean function with optimal algebraic immunity.

http://eprint.iacr.org/, 2011.

[15] Jin Q, Liu Z, Wu B, Zhang X. A general conjecture similar to T-D conjecture and its applications in constructing Boolean functions with optimal algebraic immunity. http://eprint.iacr.org/, 2011.

[16] Li N, Qi W. Construction and analysis of Boolean functions of 2t+1 variables with maximum algebraic immunity. Advances in Cryptology - ASIACRYPT 2006, LNCS 4284. Springer Berlin Heidelberg, 2006. 84–986.

[17]] Li N, Qu L, Qi W, Feng G, Li C, Xie D. On the construction of Boolean functions with optimal algebraic immunity. IEEE Trans. on Information Theory, 2008, 54(3): 1330–1334.

[18] Liu M, Zhang Y, Lin D. On the immunity of Boolean functions against fast algebraic attacks using bivariate polynomial representation. http://eprint.iacr.org/, 2012.

[19] Liu M, Zhang Y, Lin D. Perfect algebraic immune functions. Advances in Cryptology - ASIACRYPT 2012, LNCS 7658, chapter.12. Springer Berlin Heidelberg, 2012. 172–189.

[20] Maity S, Johansson T. Construction of cryptographically important Boolean functions. Progress in Cryptology - INDOCRYPT 2002, LNCS 2551. Springer Berlin Heidelberg, 2002. 234–245.

[21] Maity S, Maitra S. Minimum distance between bent and 1-resilient Boolean functions. Advances in Fast Software Encryption, LNCS 3017. Springer Berlin Heidelberg, 2004. 143–160.

[22] Meier W, Pasalic E, Carlet C. Algebraic attacks and decomposition of Boolean functions. Advances in Cryptology-EUROCRYPT 2004, LNCS 3027. Springer Berlin Heidelberg, 2004. 474–491.

[23] Savicky P. On the bent Boolean functions that are symmetric. European Journal of Combinatorics, 1994, 15(4): 407–410.

[24] Stanica P, Maitra S, Clark J. Results on rotation symmetric bent and correlation immune Boolean functions. Advances in Fast Software Encryption, LNCS 3017. Springer Berlin Heidelberg, 2004. 161–177.

[25] Tang D, Carlet C, Tang X. Highly nonlinear Boolean functions with optimal algebraic immunity and good behavior against fast algebraic attacks. IEEE Trans. on Information Theory, 2013, 59(1): 653–664.

[26] Tu Z, Deng Y. A conjecture about binary strings and its applications on constructing Boolean functions with optimal algebraic immunity. Designs, Codes and Cryptography, 2011, 60(1): 1–14.

[27] Tu Z, Deng Y. Boolean functions optimizing most of the cryptographic criteria. Discrete Applied Mathematics, 2012, 160(4-5): 427–435.

[28] Almost perfect algebraic immune functions with good nonlinearity. Manuscript.

A 4-variable Bent Functions Satisfying the Items in Construction 4.2

The coefficients of the 112 special Bent Functions' ANF are revealed in the Table 3, where $a_0, \ldots, a_{15}$ stands that

$$f(x) = a_0+a_1x_1+a_2x_2+a_3x_2x_1+a_4x_3+a_5x_3x_1+a_6x_3x_2+a_7x_3x_2x_1+a_8x_4+a_9x_4x_1 \\ +a_{10}x_4x_2+a_{11}x_4x_2x_1+a_{12}x_4x_3+a_{13}x_4x_3x_1+a_{14}x_4x_3x_2+a_{15}x_4x_3x_2x_1.$$

B Proof of Lemma 3.1 (Excerpted from Ref. [28])

Proof: For $x > 0$, we have $\sin x > x - \frac{x^3}{6}$ by Taylor's theorem. Then, for $0 < x < 1$, it holds that

$$\frac{1}{x} - \frac{1}{\sin x} + \frac{x}{5} = \frac{\sin x - x + \frac{x^2}{5}\sin x}{x \sin x} > \frac{-\frac{x^3}{6} + \frac{x^2}{5}(x - \frac{x^3}{6})}{x \sin x} = \frac{\frac{x^2}{30}(1 - x^2)}{\sin x} > 0$$

and thus

$$\frac{1}{\sin x} < \frac{1}{x} + \frac{x}{5}. \tag{7}$$

Then, for $k \geqslant 3$, we have

$$\begin{aligned} \sum_{\mu=1}^{4} \frac{1}{\sin \frac{\mu\pi}{2(2^k-1)}} &< \sum_{\mu=1}^{4} \left(\frac{2(2^k-1)}{\mu\pi} + \frac{1}{5} \cdot \frac{\mu\pi}{2(2^k-1)} \right) \\ &\leqslant \frac{2(2^k-1)}{\pi} \sum_{\mu=1}^{4} \frac{1}{\mu} + \frac{\pi}{70} \sum_{\mu=1}^{4} \mu \\ &< \frac{25(2^k-1)}{6\pi} + \frac{1}{2}. \end{aligned} \tag{8}$$

Since for $0 \leqslant \theta < t$ and $t + \theta \leqslant \pi$,

$$\frac{\theta}{\sin t} \leqslant \int_{t-\frac{\theta}{2}}^{t+\frac{\theta}{2}} \frac{\mathrm{d}\, x}{x}, \tag{9}$$

taking $t = \frac{\mu\pi}{2(2^k-1)}$ and $\theta = \frac{\pi}{2(2^k-1)}$ gives

$$\begin{aligned} \sum_{\mu=5}^{2^k-2} \frac{\frac{\pi}{2(2^k-1)}}{\sin \frac{\mu\pi}{2(2^k-1)}} &\leqslant \sum_{\mu=5}^{2^k-2} \int_{\frac{\mu\pi}{2(2^k-1)} - \frac{\pi}{4(2^k-1)}}^{\frac{\mu\pi}{2(2^k-1)} + \frac{\pi}{4(2^k-1)}} \frac{\mathrm{d}\, x}{\sin x} = \int_{\frac{9\pi}{4(2^k-1)}}^{\frac{\pi(2^k-\frac{3}{2})}{2(2^k-1)}} \frac{\mathrm{d}\, x}{\sin x} \\ &< \int_{\frac{9\pi}{4(2^k-1)}}^{\frac{\pi}{2}} \frac{\mathrm{d}\, x}{\sin x} = \left[\ln \left(\tan \frac{x}{2} \right) \right]_{\frac{9\pi}{4(2^k-1)}}^{\frac{\pi}{2}} = -\ln \left(\tan \frac{9\pi}{8(2^k-1)} \right) \\ &< -\ln(\frac{9\pi}{8(2^k-1)}) < k \ln 2 - \ln \frac{9\pi}{8}. \end{aligned} \tag{10}$$

The proofs of Theorem 3 and Lemma 1 of Ref. [8] show that

$$\mathrm{NL}(\Phi) \geqslant 2^{2k-1} - \frac{2^k}{2(2^k-1)} \left(1 + \sum_{\mu=1}^{2^k-2} \frac{1}{\sin \frac{\mu\pi}{2(2^k-1)}} \right). \tag{11}$$

Hence, for $k \geqslant 3$, by (8) and (10) we can see that

$$\begin{aligned}\mathrm{NL}(\Phi) &\geqslant 2^{2k-1} - \frac{2^k}{2(2^k-1)}\left(1 + \sum_{\mu=1}^{4} \frac{1}{\sin\frac{\mu\pi}{2(2^k-1)}} + \sum_{\mu=5}^{2^k-2} \frac{1}{\sin\frac{\mu\pi}{2(2^k-1)}}\right)\\ &> 2^{2k-1} - \frac{2^k}{2(2^k-1)}\left(\frac{3}{2} + \frac{25(2^k-1)}{6\pi} + \frac{2(2^k-1)}{\pi}\left(k\ln 2 - \ln\frac{9\pi}{8}\right)\right)\\ &> 2^{2k-1} - \frac{2^k}{\pi}\left(k\ln 2 + \frac{25}{12} - \ln\frac{9\pi}{8}\right) - 1.\end{aligned}$$

This ends the proof of the lemma. □

Table 3 The ANF of the 4-variable special Bent functions ($a_0, \ldots, a_{15}$)

0000001001000000	1000001001000000	0001001001000000	1001001001000000
0000011001000000	1000011001000000	0101011001000000	1101011001000000
0110101011000000	1110101011000000	0001101011000000	1001101011000000
0010011011000000	1010011011000000	0001011011000000	1001011011000000
0000010000100000	1000010000100000	0001010000100000	1001010000100000
0000011000100000	1000011000100000	0011011000100000	1011011000100000
0110110010100000	1110110010100000	0001110010100000	1001110010100000
0100011010100000	1100011010100000	0001011010100000	1001011010100000
0000010001100000	1000010001100000	0101010001100000	1101010001100000
0010110001100000	1010110001100000	0001110001100000	1001110001100000
0000001001100000	1000001001100000	0011001001100000	1011001001100000
0100101001100000	1100101001100000	0001101001100000	1001101001100000
0001000000001000	1001000000001000	0001010000001000	1001010000001000
0001001000001000	1001001000001000	0001111000001000	1001111000001000
0111100010001000	1111100010001000	0011010010001000	1011010010001000
0101001010001000	1101001010001000	0001011010001000	1001011010001000
0001000001001000	1001000001001000	0011100001001000	1011100001001000
0101010001001000	1101010001001000	0011010001001000	1011010001001000
0000001001001000	1000001001001000	0110001001001000	1110001001001000
0010011001001000	1010011001001000	0000111001001000	1000111001001000
0001000000101000	1001000000101000	0101100000101000	1101100000101000
0000010000101000	1000010000101000	0110010000101000	1110010000101000
0101001000101000	1101001000101000	0011001000101000	1011001000101000
0100011000101000	1100011000101000	0000111000101000	1000111000101000
0001100001101000	1001100001101000	0010010001101000	1010010001101000
0100001001101000	1100001001101000	0001011001101000	1001011001101000
0001000011101000	1001000011101000	0000010011101000	1000010011101000
0000001011101000	1000001011101000	0111111011101000	1111111011101000