Information Sciences 376 (2017) 21–30

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

Improving the lower bound on the maximum nonlinearity of 1-resilient Boolean functions and designing functions satisfying all cryptographic criteria

WeiGuo Zhang[a,b,*], Enes Pasalic[c]

[a] ISN Laboratory, Xidian University, Xi'an 710071, China
[b] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
[c] University of Primorska, FAMNIT, Koper 6000, Slovenia

ARTICLE INFO

Article history:
Received 19 June 2015
Revised 28 September 2016
Accepted 2 October 2016
Available online 4 October 2016

Keywords:
Boolean functions
Nonlinearity
Resiliency
Algebraic immunity
Stream ciphers

ABSTRACT

In this article we improve the lower bound on the maximum nonlinearity of 1-resilient Boolean functions, for n even, by proposing a method of constructing this class of functions attaining the best nonlinearity currently known. Thus for the first time, at least for small values of n, the upper bound on nonlinearity can be reached in a deterministic manner in difference to some heuristic search methods proposed previously. The nonlinearity of these functions is extremely close to the maximum nonlinearity attained by bent functions and it might be the case that this is the highest possible nonlinearity of 1-resilient functions. Apart from this theoretical contribution, it turns out that the cryptographic properties of these functions are overall good apart from their moderate resistance to fast algebraic attacks (FAA). This weakness is repaired by a suitable modification of the original functions giving a class of balanced functions with almost optimal resistance to FAA whose nonlinearity is better than the nonlinearity of other methods.

1. Introduction

In a modern design of certain stream cipher encryption schemes there are many cryptographic criteria that affect the choice of Boolean functions commonly used for the purpose of nonlinear filtering of one or several outputs of linear feedback shift registers (LFSR). These multiple criteria imposed on Boolean functions originate from various cryptographic attacks on these schemes such as Berlekamp-Massey linear complexity attacks [15], linear distinguishing and inversion attacks of Golić [9,10], algebraic attacks [5], fast algebraic attacks [6] and probabilistic algebraic attacks [1,19]. Since the early 1990s, the construction of resilient functions with high nonlinearity has been an important challenge in cryptography and it was extensively studied, see [3,4,8,13,14,18,20–22,30] and the references therein. The 1-order resiliency is closely related to the problem of determining the covering radius of the first order Reed-Muller code [16]. This problem has been resolved for even n and the covering radius corresponds to the nonlinearity of bent functions, whereas for odd n an exact specification of the covering radius appears to be hard. By imposing an additional constraint so that the Hamming distance of an n-variable Boolean function to the set of basis vectors of the first-order Reed-Muller code is exactly 2^{n-1}, one essentially attempts to

[*] Corresponding author.
E-mail addresses: zwg@xidian.edu.cn, weiguozhang@vip.qq.com (W. Zhang), enes.pasalic6@gmail.com (E. Pasalic).

http://dx.doi.org/10.1016/j.ins.2016.10.001
0020-0255/© 2016 Elsevier Inc. All rights reserved.

determine the covering radius under this constraint. This class of Boolean, apart from its importance when considered as the covering radius problem, is also of great importance in cryptography.

In [21], based on the weight divisibility results, it was shown that if f is an n-variable, m-resilient Boolean function, then the nonlinearity $N_f \equiv 0 \bmod 2^{m+1}$ which gives a nontrivial upper bound on the nonlinearity of resilient functions, i.e.,

$$N_f \leq \max\{\kappa \mid \kappa \equiv 0 \bmod 2^{m+1}, \kappa < \text{ nlmax } (n)\},$$

where nlmax(n) denotes the maximum nonlinearity of an n-variable Boolean function. In particular, when n is even then $\kappa < 2^{n-1} - 2^{\frac{n}{2}-1}$, and this maximum nonlinearity is achieved by bent functions. Since we are dealing with 1-resilient functions, thus $m = 1$, it follows that the upper bound in this case is given by $N_f \leq 2^{n-1} - 2^{\frac{n}{2}-1} - 4$. Indeed, while this upper bound is easily achieved for $n = 6$ by for instance using the Maiorana-McFarland method [12], when $n = 8$ to construct a 1-resilient functions with nonlinearity 116 a computer search was necessary [13]. In some recent works [11,23,28], other techniques for constructing resilient functions with high nonlinearity were proposed, but none of these methods improves significantly the lower bound on nonlinearity in such an extent and in a deterministic manner.

In this article, we show that for even n this upper bound is achievable by a deterministic method, which in general gives functions whose nonlinearity is exactly $N_f = 2^{n-1} - 2^{\frac{n}{2}} - 2^{\lceil \frac{n}{4} \rceil}$ which only deviates by a constant $2^{\lceil \frac{n}{4} \rceil}$ from the nonlinearity of bent functions. The method is based on a suitable modifications of functions in the so-called $\mathcal{PS}^-$ class along with the introduction of a provable technique for transforming originally nonbalanced functions into 1-resilient functions. Whereas the previous methods was based on guaranteeing the resiliency order of Boolean functions due to the choice of its subfunctions, in this work we attempt to optimize the nonlinearity of functions without paying any regard to resiliency. The class of functions obtained is not even balanced (and therefore not 1-resilient either) but it turns out that we are able to find n linearly independent vectors for which the Walsh spectral values, which gives us the possibility of turning these functions into 1-resilient while keeping the same nonlinearity value.

Our class of functions possesses the currently best known nonlinearity of 1-resilient functions, thus providing a better lower bound than previously known such as the nonlinearities values attained by the methods in [11,13,23]. The Walsh spectral values of our functions are “approximately” uniformly distributed around the bent spectral values $\pm\ 2^{n/2}$ which leaves a rather small space for further improvements upon our results. Essentially, the obtained nonlinearity is so close to the nonlinearity of bent functions that it is a tempting conjecture that the above lower bound is tight, quite likely reaching the achievable upper bound in which case no further improvements are possible (this seems to be especially true for the case $n \equiv 0 \mod 4$). However, we do not turn this comment into a formal conjecture.

Even though most of the other cryptographic criteria for this class of functions are optimized (for instance the algebraic immunity is optimized) these functions offer only a moderate resistance to fast algebraic attacks (FAA) and therefore we consider some appropriate modifications which give a nice trade-off between the relevant cryptographic properties. More precisely, a suitable modification of these functions can in the first place yield balanced cryptographic functions whose resistance to FAA is almost optimal though the nonlinearity value is then slightly decreased. Thus, apart from a purely theoretical contribution regarding the improvement of the lower bound, the modified class provides the best known trade-off of cryptographic parameters in most of the cases. Therefore, the constructed functions can be considered as good candidates for applications in real-life encryption schemes that use a Boolean function as a nonlinear filtering mechanism.

The rest of the paper is organized as follows. In Section 2 some basic definitions concerning Boolean functions and in particular a brief overview of the $\mathcal{PS}$ class is given. The main construction method, based on a suitable modification of bent functions in $\mathcal{PS}^-$, is given in Section 3 and furthermore it is shown that these nonbalanced functions can always be turned into 1-resilient functions without affecting any of relevant cryptographic parameters. In Section 4, we demonstrate that a suitable modification of our basic construction may lead to a class of balanced functions satisfying all relevant cryptographic criteria at the same time. Finally, some concluding remarks are given in Section 5.

2. Preliminaries

In this section we recall some basic definitions related to Boolean functions as well as some main ideas about the construction of bent functions in the partial spread ($\mathcal{PS}$) class.

2.1. Boolean functions

Let $\mathcal{B}_n$ denote the set of Boolean functions in n variables. A Boolean function $f(X) \in \mathcal{B}_n$ is a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$, where $X = (x_1, \cdots, x_n) \in \mathbb{F}_2^n$ and $\mathbb{F}_2^n$ is the vector space of n-tuples of elements from $\mathbb{F}_2$. To avoid the confusion with the addition of integers in $\mathbb{R}$ denoted by + and Σ_i, we denote the addition over $\mathbb{F}_2$ by $\oplus$ and $\bigoplus_i$. For simplicity, we denote by + the addition of vectors of $\mathbb{F}_2^n$. $f(X)$ is generally represented by its algebraic normal form (ANF):

$$f(X) = \bigoplus_{b \in \mathbb{F}_2^n} \lambda_b \left(\prod_{i=1}^{n} x_i^{b_i} \right) \tag{1}$$

where $\lambda_b \in \mathbb{F}_2$, $b = (b_1, \cdots, b_n)$. The algebraic degree of $f(X)$, denoted by *deg*(f), is the maximal value of $wt(u)$ such that $\lambda_b \neq 0$, where $wt(b)$ denotes the Hamming weight of b. f is called an affine function when $deg(f) = 1$. An affine function whose constant term is equal to zero is called a linear function. Any linear function on $\mathbb{F}_2^n$ is denoted by:

$$\alpha \cdot X = \alpha_1 x_1 \oplus \cdots \oplus \alpha_n x_n,$$

where $\alpha = (\alpha_1, \cdots, \alpha_n) \in \mathbb{F}_2^n$. The Walsh transform of $f \in \mathcal{B}_n$ in point α is denoted by $W_f(\alpha)$ and calculated as

$$W_f(\alpha) = \sum_{X \in \mathbb{F}_2^n} (-1)^{f(X) \oplus \alpha \cdot X}. \tag{2}$$

Let $supp(f) = \{X \in \mathbb{F}_2^n \mid f(X) = 1\}$ denote the support of *f*. $f \in \mathcal{B}_n$ is said to be balanced if its output column in the truth table contains equal number of 0's and 1's, i.e., $\#supp(f) = 2^{n-1}$ or equivalently $W_f(0) = 0$.

Definition 1. The nonlinearity of a Boolean function $f \in \mathcal{B}_n$ is defined as the minimum Hamming distance to the set of all affine functions,

$$N_f = \min_{\rho \in A(n)} |\{X \in \mathbb{F}_2^n : f(X) \neq \rho(X)\}|,$$

where $A(n)$ is the set of all affine functions on $\mathbb{F}_2^n$.

The nonlinearity of *f* can be obtained through the Walsh transform as follows :

$$N_f = 2^{n-1} - \frac{1}{2}\mathcal{L}(f), \ \text{ where } \mathcal{L}(f) = \max_{\alpha \in \mathbb{F}_2^n} |W_f(\alpha)|. \tag{3}$$

The Parseval's equation [16] states that

$$\sum_{\alpha \in \mathbb{F}_2^n} (W_f(\alpha))^2 = 2^{2n} \tag{4}$$

and implies that

$$N_f \leq 2^{n-1} - 2^{n/2-1}.$$

The equality occurs if and only if $f \in \mathcal{B}_n$ are bent functions, where n is even.

In [26], a spectral characterization of resilient Boolean functions has been presented, which we use here as a definition.

Definition 2. A Boolean function $f \in \mathcal{B}_n$ is t-resilient if and only if its Walsh transform satisfies

$$W_f(\alpha) = 0, \quad \text{for } 0 \leq wt(\alpha) \leq t, \alpha \in \mathbb{F}_2^n. \tag{5}$$

Definition 3 [5,17]**.** For $f \in \mathcal{B}_n$, we define

$$AN(f) = \{g \in \mathcal{B}_n \mid fg = 0\}. \tag{6}$$

A Boolean function $g \in AN(f)$ is an annihilator of *f*. The algebraic immunity of *f*, denoted by *AI*(*f*), is defined as

$$AI(f) = \min\{deg(g) \mid g \in AN(f) \ or \ g \in AN(f \oplus 1), \ \ g \neq 0\} \tag{7}$$

f is said to have optimal algebraic immunity if $AI(f) = \lceil \frac{n}{2} \rceil$ (For any $f \in \mathcal{B}_n$, $AI(f) \leq \lceil \frac{n}{2} \rceil$).

Good algebraic immunity is a necessary but not sufficient condition for good resistance against FAA. The resistance against FAA of $f \in \mathcal{B}_n$ is measured by considering the sum of the degrees of functions $g \in \mathcal{B}_n$ and $h \in \mathcal{B}_n$ in the relation of the form $fg = h$. Set $e = deg(g)$, $d = deg(h)$. The cryptanalyst seeks for nonzero $g, h \in \mathcal{B}_n$ so that $e + d$ in the above relation is minimized. In other words, if one can find g of low degree and $h \neq 0$ of reasonable degree such that $fg = h$, then FAA becomes efficient. The tuple (e, d) completely determines the complexity of the associated FAA. The ability to resist FAA is optimal if $e + d \geq n$, and suboptimal if $e + d \geq n - 1$, for any $e \in [1, \lceil n/2 \rceil - 1]$. The parameter *FAI*(*f*) refers to the immunity to resist FAA and it is defined as follows:

$$FAI(f) = \min_{\substack{g,h \in \mathcal{B}_n \\ g,h \neq 0}} \{deg(g) + deg(h) : fg = h\}. \tag{8}$$

2.2. Disjoint linear codes and $\mathcal{PS}$ bent functions

We here briefly recall some basic facts concerning the Dillon's $\mathcal{PS}$ class [7] of bent functions. Since our main construction method (cf. Section 3) uses the disjoint code representation of this class we give a recent (more general) result related to the problem of finding a set of disjoint linear codes.

Construction 1 [31]**.** Let $n = 2k$, and $\gamma \in \mathbb{F}_{2^k}$ be a root of a primitive polynomial *f*(*x*) of degree k over $\mathbb{F}_2$. Define a bijective mapping $\pi : \mathbb{F}_{2^k} \mapsto \mathbb{F}_2^k$ by

$$\pi(a_0 + a_1\gamma + a_2\gamma^2 + \cdots + a_{k-1}\gamma^{k-1}) = (a_0, a_1, \cdots, a_{k-1}) \tag{9}$$

For $i = 0,\ 1, \cdots, 2^k - 2$, let

$$G_i = \begin{pmatrix} 100\cdots00 & \pi(\gamma^i) \\ 010\cdots00 & \pi(\gamma^{i+1}) \\ \ddots & \vdots \\ 000\cdots01 & \pi(\gamma^{i+k-1}) \end{pmatrix}_{k\times n} \tag{10}$$

be the generator matrix of an $[n,\ k]$ code C_i. Let $G_{2^k-1} = (I_k\ \mathbf{0}_{k\times k})$ and $G_{2^k} = (\mathbf{0}_{k\times k}\ I_k)$ be the generator matrix of C_{2^k-1} and C_{2^k} respectively, where I_k be a k-order identity matrix and $\mathbf{0}_{k\times k}$ be a $k \times k$ zero matrix. Then, $\{C_0, C_1, \cdots, C_{2^k}\}$ is a set of $[n,\ k]$ disjoint linear codes.

Lemma 1. *[7,32] Let $f \in \mathcal{B}_n$ with $n = 2k$. Let $\mathcal{C} = \{C_0, C_1, \ldots, C_{2^k}\}$ be a set of $[n,\ k]$ disjoint linear codes. Then f is a $\mathcal{PS}^-$ (resp. $\mathcal{PS}^+$) bent function when it satisfies (i) (resp. (ii)):*

(i) *$supp(f) = \bigcup_{i=0}^{2^{k-1}-1} C_i^*$, where $C_i^* = C_i \backslash \{\mathbf{0}\}$,*
(ii) *$supp(f) = \bigcup_{i=0}^{2^{k-1}} C_i$.*

3. The main construction method

The main idea behind the construction presented below is to extend the support of a bent function $b \in \mathcal{B}_n$ in $\mathcal{PS}^-$ class by either additionally defining a bent function and its complement (when $n \equiv 0 \pmod 4$) on two suitably chosen subspaces; or defining a semi-bent function and its complement on the same subspaces when $n \equiv 2 \pmod 4$. In this way, the resulting function achieves extremely high nonlinearity but more importantly, as demonstrated below, it can always be turned into 1-resilient function by applying a suitable linear transformation of the input variables.

Construction 2. Let $n = 2k$, and $\mathcal{C} = \{C_0, C_1, \ldots, C_{2^k}\}$ be a set of $[n,\ k]$ disjoint linear codes as in Construction 1. Let $X', X'' \in \mathbb{F}_2^k$, and $X = (X', X'') \in \mathbb{F}_2^n$. We construct a function $f(X) \in \mathcal{B}_n$ as follows:

$$f(X) = \begin{cases} 1 & \text{if } X \in C_i^*, 0 \le i \le 2^{k-1} - 2 \\ 0 & \text{if } X \in C_i^*, 2^{k-1} - 1 \le i \le 2^k - 2 \\ g(X') & \text{if } X \in C_{2^k-1} \\ g(X'') \oplus 1 & \text{if } X \in C_{2^k}^* \end{cases} \tag{11}$$

where

- $g \in \mathcal{B}_k$ is a bent function if k is even;
- $g \in \mathcal{B}_k$ is a 1-resilient semi-bent function with $W_g(\mathbf{0}) = 0$ if k is odd.

Theorem 1. *Let $f \in \mathcal{B}_n$ be as in Construction 2. Then $N_f = 2^{n-1} - 2^{n/2-1} - 2^{\lceil n/4 \rceil}$.*

Proof. Note that $f(\mathbf{0}) = 0$. For any $\alpha = (\alpha', \alpha'') \in \mathbb{F}_2^n$, where $\alpha', \alpha'' \in \mathbb{F}_2^k$, we have

$$\begin{aligned} W_f(\alpha) &= \sum_{X\in\mathbb{F}_2^n} (-1)^{f(X)\oplus\alpha\cdot X} \\ &= (-1)^{f(\mathbf{0})} + \sum_{i=0}^{2^k} \sum_{X\in C_i^*} (-1)^{f(X)\oplus\alpha\cdot X} \\ &= \sum_{i=0}^{2^{k-1}-2} \sum_{X\in C_i} (-1)^{1\oplus\alpha\cdot X} + \sum_{i=2^{k-1}-1}^{2^k-2} \sum_{X\in C_i} (-1)^{\alpha\cdot X} \\ &\quad + \sum_{X\in C_{2^k-1}} (-1)^{g(X')\oplus\alpha'\cdot X'} + \sum_{X\in C_{2^k}} (-1)^{g(X'')\oplus\alpha''\cdot X''\oplus 1} \\ &= U(\alpha) + W_g(\alpha') - W_g(\alpha''), \end{aligned}$$

where

$$U(\alpha) = -\sum_{i=0}^{2^{k-1}-2} \sum_{X\in C_i} (-1)^{\alpha\cdot X} + \sum_{i=2^{k-1}-1}^{2^k-2} \sum_{X\in C_i} (-1)^{\alpha\cdot X}. \tag{12}$$

In the above derivation the term $(-1)^{f(\mathbf{0})}$ vanishes as we use the sum $\sum_{X\in C_{2^k}} (-1)^{g(X'')\oplus\alpha''\cdot X''}$ to yield $W_g(\alpha'')$ instead of $\sum_{X\in C_{2^k}^*} (-1)^{g(X'')\oplus\alpha''\cdot X''}$. In a similar manner, $(-1)^{f(\mathbf{0})}$ is added 2^{k-1} times to each sum in $U(\alpha)$ thus extending the summation to be over C_i rather than over C_i^*.

For $i = 0, 1, \dots, 2^k$, let $C_i^\perp$ be the dual space of C_i. Then, $\{C_0^\perp, C_1^\perp, \dots, C_{2^k}^\perp\}$ is also a set of disjoint linear codes. Furthermore, $C_{2^k}^\perp = C_{2^k-1}$. Thus,

$$\bigcup_{i=0}^{2^k-2} C_i = \bigcup_{i=0}^{2^k-2} C_i^\perp \tag{13}$$

For any $\alpha \in C_j^\perp$, $j = 0, 1, \dots, 2^k$, we always have

$$\sum_{X \in C_i} (-1)^{\alpha \cdot X} = \begin{cases} 0\ , & \text{if } i \neq j \\ +2^k, & \text{if } i = j, \end{cases} \tag{14}$$

where $0 \le i \le 2^k$. Thus, for any $\alpha \in C_j^\perp$, we have

$$U(\alpha) = \begin{cases} \pm 2^k, & \text{if } 0 \le j \le 2^k - 2 \\ 0, & \text{if } j = 2^k - 1, 2^k. \end{cases} \tag{15}$$

For any $\beta \in \mathbb{F}_2^k$, we have

$$W_g(\beta) \in \begin{cases} \{\pm 2^{k/2}\}, & \text{if } k \text{ is even} \\ \{0, \pm 2^{(k+1)/2}\}, & \text{if } k \text{ is odd}\ . \end{cases} \tag{16}$$

Then, for any $\alpha \in C_j^\perp$, $j = 0, 1, \dots, 2^k - 2$, we have

$$W_f(\alpha) \in \begin{cases} \{\pm 2^k, \pm(2^k + 2^{k/2+1}), \pm(2^k - 2^{k/2+1})\}, & k \text{ even} \\ \{\pm 2^k, \pm(2^k + 2^{(k+1)/2}), \pm(2^k - 2^{(k+1)/2}), & \\ \pm(2^k + 2^{(k+3)/2}), \pm(2^k - 2^{(k+3)/2})\}, & k \text{ odd}\ . \end{cases}$$

For any $\alpha \in C_j^\perp$, $j = 2^k - 1, 2^k$, we have

$$W_f(\alpha) \in \begin{cases} \{0, \pm 2^{k/2+1}\}, & \text{if } k \text{ is even} \\ \{0, \pm 2^{(k+1)/2}\}, & \text{if } k \text{ is odd}\ . \end{cases} \tag{17}$$

Therefore,

$$\max_{\alpha \in \mathbb{F}_2^n} |W_f(\alpha)| = 2^k + 2^{\lceil k/2 \rceil + 1}. \tag{18}$$

By (3),

$$N_f = 2^{n-1} - 2^{k-1} - 2^{\lceil k/2 \rceil} \tag{19}$$

$$= 2^{n-1} - 2^{n/2-1} - 2^{\lceil n/4 \rceil}. \quad \square \tag{20}$$

Notice that Construction 2 always yields nonbalanced functions since $wt(f) = (2^{k-1} - 1) \cdot (2^k - 1) + (2^k - 1) = 2^{n-1} - 2^{k-1}$. Therefore, in order to make these functions 1-resilient we must in the first place ensure there are at least $n+1$ vectors whose Walsh transform is equal to zero out of which there are n linearly independent such vectors. Due to the intrinsic properties of the above construction, this is essentially always true as shown below.

Lemma 2. *Let $f \in \mathcal{B}_n$ be as in Construction 2. Let $M = \{\alpha \mid W_f(\alpha) = 0,\ \alpha \in \mathbb{F}_2^n\}$. Then there always exist n linearly independent vectors in M.*

Proof. For any $\beta \in \mathbb{F}_2^k$, we always have $W_{g\oplus 1}(\beta) = -W_g(\beta)$. By the proof of Theorem 2, we know that

$$M \subseteq C^*_{2^k-1} \cup C^*_{2^k}. \tag{21}$$

More specifically,

$$M = M_0 \cup M_1 \tag{22}$$

where

$$M_0 = \{\alpha \mid W_g(\alpha') = -W_{g\oplus 1}(\mathbf{0}),\ \alpha \in C^*_{2^k-1}\} \tag{23}$$

and

$$M_1 = \{\alpha \mid W_{g\oplus 1}(\alpha'') = -W_g(\mathbf{0}),\ \alpha \in C^*_{2^k}\}. \tag{24}$$

i) When k is even, g is a bent function. We have

$$\#M_0 = \#M_1 = 2^{k-1} + 2^{k/2-1} - 1, \tag{25}$$

Table 1
The spectral distribution of the (8, 1, 6, 116) function.

spectra	0	8	–8	16	–16	24	–24
number	18	33	33	51	67	27	27

which means

$$\#M = 2^k + 2^{k/2} - 2. \tag{26}$$

Noticing $\#M_0 = \#M_1 > 2^{k-1}$, it is obvious that there exist k linearly independent vectors in M_0 and M_1 respectively. Note that $C^*_{2^k-1} \cap C^*_{2^k} = \emptyset$. Then there must exist n linearly independent vectors in M.ii) When k is odd, g and $g\oplus1$ are 1-resilient semi-bent functions. By Definition 2,

$$\{(\alpha', \mathbf{0}) \mid wt(\alpha') = 1,\ \alpha' \in \mathbb{F}_2^k\} \subset M_0 \tag{27}$$

and

$$\{(\mathbf{0}, \alpha'') \mid wt(\alpha'') = 1,\ \alpha' \in \mathbb{F}_2^k\} \subset M_1 \tag{28}$$

Obviously,

$$\{\alpha \mid wt(\alpha) = 1,\ \alpha \in \mathbb{F}_2^n\} \subset M. \tag{29}$$

So, there must exist n linearly independent vectors in M. □

Next, we show that the constructed functions above can be transformed to a 1-resilient function. First, one can select n linearly independent vectors in M to form a set

$$G = \{\omega_1, \omega_2, \cdots, \omega_n\}. \tag{30}$$

Let $\delta = a_1\omega_1 \oplus a_2\omega_2 \oplus \cdots \oplus a_n\omega_n \in M \setminus G$ with $\sum_{i=1}^n a_i \equiv 0 \pmod 2$. Note that

$$\begin{vmatrix} a_1 \oplus 1 & a_2 & \ldots & a_n \\ a_1 & a_2 \oplus 1 & \ldots & a_n \\ \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & \ldots & a_n \oplus 1 \end{vmatrix} \neq 0. \tag{31}$$

We then have $\delta\oplus\omega_1$, $\delta\oplus\omega_2$, $\cdots$, $\delta\oplus\omega_n$ are linearly independent. Let

$$f_0(X) = f(X) \oplus \delta \cdot X. \tag{32}$$

Obviously, f_0 is a balanced function since $\delta \in M$. Let now

$$R = \begin{pmatrix} \delta + \omega_1 \\ \delta + \omega_2 \\ \vdots \\ \delta + \omega_n \end{pmatrix}. \tag{33}$$

Then $f_1(X) = f_0(R^{-1}X)$ is 1-resilient. Note that f, f_0 and f_1 have the same nonlinearity. Thus, we have the following theorem.

Theorem 2. *Let $n = 2k \geq 8$ be even. A 1-resilient Boolean function $f_1 \in \mathcal{B}_n$ with nonlinearity $2^{n-1} - 2^{n/2-1} - 2^{\lceil n/4 \rceil}$ can be constructed. Moreover, the algebraic degree of f_1 is $\lceil \frac{n+k}{2} \rceil$.*

Proof. The part on nonlinearity follows from Theorem 2 and resiliency from the proof of Lemma 2. Since f_1 and f in Construction 2 are of the same degree it suffices to estimate deg(f). Notice that f can be viewed as a bent function in $\mathcal{PS}^*$ modified by adding two functions g and $1\oplus g$. By selecting $g \in B_k$ to be of maximum degree $\lceil \frac{k}{2} \rceil$ (covering both the bent and semi-bent case) we conclude that $\deg(f) = \frac{n}{2} + \lceil \frac{k}{2} \rceil = \lceil \frac{n+k}{2} \rceil$. □

The example below illustrates the possibility of obtaining functions achieving the upper bound on nonlinearity (for small n) for 1-resilient functions through a deterministic method.

Example 1. Let $n = 8$ and let f be constructed by means of Construction 2, thus using (11), where g is a bent function in $\mathcal{B}_4$ given by $g(x_1, x_2, x_3, x_4) = x_1x_2 \oplus x_3x_4$. Its truth table in hexadecimal format is given by

6ee1 562c 722c 9527 7a0c 05d3 1726 a9d1 7a88 6ac8 0573 e8d8 962e 8537 89d3 68d1

The Walsh spectra of this function is depicted in Table 1. Noticing that $W_f(10\cdots0) = 0$, adding a linear function $\delta \cdot X = x_1$ as in (32) we get a balanced function $f_0 = f + x_1$. Then, applying a linear transformation (33) a 1-resilient function f_1 is obtained. Its truth table is given by,

7afa ba05 3b8e 2562 0477 4fa8 05e6 65e3 440d 59de 3d72 ae21 b471 ce2c d6b0 d29d

Table 2
The spectral distribution of the (12, 1, 9, 2008) function.

spectra	0	16	−16	48	−48	64	−64	80	−80
number	70	28	28	509	471	999	1011	509	471

Table 3
The nonlinearity comparison of 1-resilient functions (n even).

n	8	10	12	14	16
Ours (1-resilient)	116	488	2008	8112	32,624
Ref.[13]	116	488	1996	8096	32,576
Ref.[25]	112	484	1996	8100	32,588
Ref.[23]	108	484	2000	8108	32,604
Ref.[11]	112	484	1996	8100	32,588
Ref.[30]	-	484	2000	8096	32,608
Ref.[29]	-	484	2000	8104	32,608

The function f_1 is 1-resilient, its nonlinearity is 116, $\deg(f_1)=6$, and $AI(f_1)=4$. Thus, all these parameters attain their optimal values. It can be checked that its resistance to fast algebraic attacks is almost optimal, that is, there exists a pair of functions g, $h\neq 0$ of degree $\deg(g)=e=2$ and $\deg(h)=d=5$ satisfying the relation $fg=h$. Moreover, we always have $FAI(f)=n-1$ (i.e. $e+d\geq 7$).

Example 2. A (12, 1, 9, 2008) function with $AI(f)=6$ and $FAI(f)=9$ can be constructed whose truth table is given in Appendix. This is a large improvement over the best known nonlinearity for 1-resilient functions in [23], cf. Table 3. The Walsh spectra of this function is depicted in Table 2. A closer inspection, in terms of the Parseval's equality, indicates the hardness of suppressing further a large number (which is $509+471=980$) of the maximum absolute values (which is 80) in the spectra.

In Table 3, we compare the nonlinearity of our construction to some currently best known methods for generating 1-resilient functions. Notice that the functions in [13] are constructed recursively using an initial 1-resilient function with nonlinearity 116 found by computer search.

3.1. A comparison to other construction methods

In Table 2, we give a few instances of nonlinearity values for relatively small values of n. In this section we compare the lower bounds on nonlinearity of different construction methods to the nonlinearity $2^{n-1}-2^{n/2-1}-2^{\lceil n/4\rceil}$ given in Theorem 2. We notice that for certain methods such as the design in [11] a lower bound is not given and therefore the analysis is omitted, thus Table 2 is valid in such cases.

In [29] the so-called GMM class of resilient functions were presented and the lower bound on nonlinearity for 1-resilient functions (which is actually the exact value) was shown to be better than the bound in [30] for any n and the order of resiliency t. Since prior to the appearance of GMM class the best known method for providing resilient functions with highest nonlinearity was given in [30], it suffices to compare the lower bound for the GMM class in [29] with our nonlinearity. The lower bound for m-resilient functions in [29], for even n, equals to

$$N_f \geq 2^{n-1}-2^{n/2-1}-\sum_{i=n/2+1}^{e} a_i\cdot 2^{n-i-1}, \tag{34}$$

where $(a_{n/2},\dots,a_{n-m-1})\in\mathbb{F}_2^{n/2-m}$ (with $a_{n/2}=1$) is a binary vector such that $\sum_{i=n/2}^{n-m-1} a_i 2^i$ is maximal, satisfying at the same time,

$$\sum_{i=n/2}^{n-m-1}\left(a_i\cdot 2^{n-i}\sum_{j=m+1}^{n-i}\binom{n-i}{j}\right)\geq 2^n, \tag{35}$$

and $e=\max\{i \mid a_i\neq 0,\ n/2\leq i\leq n-m-1\}$. Therefore, for $m=1$ it is sufficient to show that $2^{\lceil n/4\rceil}<\sum_{i=n/2+1}^{e} a_i\cdot 2^{n-i-1}$. Since $a_{n/2}=1$, then the condition (35) can be rewritten as,

$$\begin{aligned}
&2^{n/2}\sum_{j=2}^{n/2}\binom{n/2}{j}+\sum_{i=n/2+1}^{n-2}\left(a_i\cdot 2^{n-i}\sum_{j=2}^{n-i}\binom{n-i}{j}\right)\\
&=2^{n/2}(2^{n/2}-n/2-1)+\sum_{i=n/2+1}^{n-2}\left(a_i\cdot 2^{n-i}\sum_{j=2}^{n-i}\binom{n-i}{j}\right)\geq 2^n,
\end{aligned}$$

Table 4
The nonlinearity comparison of balanced functions with $FAI(f) = n - 1$ (n even).

n	8	10	12	14	16
Ours	116	486	1994	8084	32,554
N (# Modif.)	0	6	36	134	518
Ref.[2]	112	478	1970	8036	32,530
Ref.[27]	114	480	1988	8072	32,530
Ref.[24]	108	476	1982	8028	32,508

which gives the condition

$$\sum_{i=n/2+1}^{n-2}\left(a_i \cdot 2^{n-i}\sum_{j=2}^{n-i}\binom{n-i}{j}\right) \geq (n/2+1)2^{n/2}. \tag{36}$$

Now, due to the bound for the GMM class given by (34), it is enough to show that taking $a_{n-1-\lceil n/4\rceil} = 1$ and $a_i = 0$ for $i > n-1-\lceil n/4\rceil$, the condition (36) is impossible to satisfy. Indeed, it can be shown that

$$2^{\lceil n/4\rceil}\sum_{j=2}^{\lceil n/4\rceil}\binom{\lceil n/4\rceil}{j} > \sum_{i=n-\lceil n/4\rceil}^{n-2}\left(a_i \cdot 2^{n-i}\sum_{j=2}^{n-i}\binom{n-i}{j}\right),$$

for any choice of the binary coefficients a_i, where $n-\lceil n/4\rceil \leq i \leq n-2$. Thus, we need to show that

$$2^{\lceil n/4\rceil+1}\sum_{j=2}^{\lceil n/4\rceil+1}\binom{\lceil n/4\rceil+1}{j} < (n/2+1)2^{n/2}, \tag{37}$$

implying the impossibility of constructing such functions using the GMM method. When $n \equiv 0 \pmod 4$ this is easily confirmed by noting that for $n \geq 8$ we have $(n/2+1)2^{n/2} > 2^{n/2+2}$ whereas $2^{\lceil n/4\rceil+1}\sum_{j=2}^{\lceil n/4\rceil+1}\binom{\lceil n/4\rceil+1}{j} < 2^{n/2+2}$. On the other hand, when $n \equiv 2 \pmod 4$ then the same reasoning is valid for $n \geq 14$ and (37) is satisfied. The case $n = 10$ can be verified directly (having $16 \cdot 11 < 6 \cdot 32$ in (37)) which then implies that the nonlinearity $2^{n-1} - 2^{n/2-1} - 2^{\lceil n/4\rceil}$ is greater than the lower bound in [29] for any even $n \geq 8$.

Unfortunately, due to a deterministic nature of Construction 2 the existence of quadratic degree multipliers g such that $fg = h$, where $\deg(h) = \frac{n}{2}+1$, could be observed for all input instances. This implies that the resistance against FAA is always given by $FAI(f) = \frac{n}{2}+3$, which for practical sizes of n, say $16 \leq n \leq 20$, gives a relatively large deviation from the optimal case $FAI(f) = n$. Nevertheless, notice that the optimal resistance to FAA is rarely satisfied by any of the known constructions, one example of such a function was found in [2] for $n = 9$. Therefore, any design achieving a suboptimal resistance which ensures that $FAI(f) = n - 1$ (providing sufficient protection of the cipher against algebraic cryptanalysis) is commonly considered as extremely good. In the next section, we show that we can apply a suitable modification to the functions designed by means of Construction 2 so that the modified functions become balanced and reach this suboptimal resistance to FAA, that is, $FAI(f) = n - 1$. On the other hand, we cannot transform these functions into 1-resilient and the nonlinearity is slightly decreased.

4. A class of balanced functions with excellent algebraic properties

Simulations show that a function $f(X)$ in Construction 2 has a moderate resistance to FAA. The ability against FAA of $f(X)$ can be efficiently improved by adding an “adjustive” function $\Delta(X)$ with “small” weight N, i.e., $\#supp(\Delta) = N$. The adjustive function $\Delta(X)$ is constructed in accordance to the following rules.

- For $i = 0, 1, \ldots, 2^k$, $\Gamma_i = supp(\Delta) \cap C_i^*$ with $\#\Gamma_i \in \{\tau_i, \tau_i + 1\}$, where

$$\tau_i = \lfloor N/(2^k+1)\rfloor.$$

- $f'(X) = f(X) \oplus \Delta(X)$ satisfy $FAI(f) = n - 1$.
- N should be as small as possible to preserve a good nonlinearity of $f(X)$.

Next we check the Walsh spectra of $f'(X)$. Suppose that $W_{f'}(\delta) = 0$. Then the function

$$f''(X) = f'(X) \oplus \delta \cdot X$$

is a balanced function as desired. Simulations confirm that f'' can have high nonlinearity, optimal algebraic degree, optimal algebraic immunity, $FAI(f) = n - 1$. The importance of this result lies in the fact that we are able to obtain a class of functions with currently best nonlinearity compared to other classes having the same resistance to FAA.

Table 4 gives a comparison of our results to other construction methods in terms of nonlinearity. We also indicate the number of points N for which the modifications have been made. Notice that since $\Gamma_i = supp(\Delta) \cap C_i^*$, in almost all the cases the modification on each C_i^* is performed on at most 2 points (apart from the case $n = 10$) since $\tau_i = 1$ and therefore $\#\Gamma_i \in \{1, 2\}$.

Remark 1. We remark that the results in Table 4 can be slightly improved in the case a larger computer search for optimized positions of modifications would be performed. Based on the computer simulations the resistance to FAA always becomes better (or remains the same) if more modifications have been performed, but the main problem is to ensure that the nonlinearity does not degrade severely.

The following two examples fully specify two functions (for $n = 10$ and $n = 12$), with excellent algebraic properties obtained by the above mentioned modification. Notice also that in Table 4 no modification was needed when $n = 8$ and only 6 entries were modified for $n = 10$.

Example 3. The truth table below corresponds to a (10,0,9,486) function f with $AI(f) = 5$ and $FAI(f) = 9$ obtained by modifying a (10,1, 8, 488) function ($FAI(f) = 8$) designed using Construction 2.

16a5 99c3 3acd b426 e532 4b59 873a 4bd9 ed32 4b19 e8e5 b826 3ac5 b426 6cf6 ca08 6db0 4b09 120d 35f7 073a 43d9 6ce5 ba24 9acd b426 930b 15f7 930b 15d7 b31a 47db 6db2 cb08 6cf4 ba24 ecf2 ea08 931b 45db 053a 4bd9 173a 43d9 931a 47d9 edf2 ea08 12cd b4a6 edb2 4b19 ecf5 ea20 6db2 cb09 930b 1ddb 130b 55db 68e5 b826 edf2 cb08

Example 4. The truth table of a balanced (12,0,11,1994) function f with $AI(f) = 6$ and $FAI(f) = 11$, obtained by modifying $N = 36$ entries of the original function, is given in Appendix.

Open problem 1. Our attempts to keep the resiliency of order one and to ensure an almost optimal resistance to FAA at the same time have failed. Nevertheless, a deterministic structure of the zeros in the Walsh spectra given in Lemma 2 may possibly be used in order to perform more sophisticated modifications (preserving n linearly independent vectors whose Walsh transform equals to zero). This is, however, left as an interesting open problem.

5. Conclusions

In this article we propose a novel construction method based on a suitable modification of bent functions in the $\mathcal{PS}^-$ class. This modification is characterized with the existence of sufficiently many linearly independent vectors for which the Walsh spectra equals to zero, thus allowing us to transform these functions into 1-resilient functions with currently best nonlinearity value and therefore to improve the lower bound on nonlinearity of this class. A moderate resistance to fast algebraic cryptanalysis of these functions is then significantly improved. That is, by transforming originally nonbalanced functions into the balanced ones, by using suitable modifications of the truth tables, a class of functions satisfying all the relevant cryptographic criteria at the same time is obtained.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China (grant no. 61373008 and 61672414) and the 111 Project (grant no. B08038).

Appendix

The truth table of a (12, 1, 9, 2008) function in Example 2, with $AI(f) = 6$ and $FAI(f) = 9$.

24cf 2ba3 c06e 6d47 ae21 59e4 2a6f 1700 3fcf 38ab d86e 6d8a ae49 89a1 216b 0c16 9fc6 b8eb d82e 798a 8749 89a1 316b 0c5f 8730 f47b 7aaf 328a 4149 891b 95e3 8c7e 81cf 0b56 625c cd7c bef3 8be4 6ad2 d401 fecf 0ba9 d854 cd82 be4c f5e4 6a2d 0c81 00cf 0b54 275e cd75 beb3 7ae4 2ad0 f300 fa54 b48c 852f 30e1 c196 76b9 951c 637f e839 4784 85d1 8e75 78b6 765e ce14 f3a0 fe31 c7a9 9891 9683 594c f55e de2d 28a1 8114 b453 72af 325e c171 8b99 95e2 dc7f 7e2b 4ba9 99d1 cf83 7e0c f446 6a2d 2a81 1734 b46b f8af 328a c149 8919 95eb 0c7f c0d4 b814 272e 3175 85b6 76b1 3594 f37e 81ab 4b53 7ad1 cf1e 3e71 8b46 6ae2 dc80 e8eb 4b84 0750 cf75 3eb6 7666 6a14 f380 8039 c754 2791 967d 59b3 3a5e ced0 f3a1 01cf 4b56 6250 cd7e 3e73 8be6 6ad2 d481 853b 4773 7ad1 8e9a 7869 895e cee3 8c81 fe31 c7a8 9d91 92a1 518c 745e de0d 2be8 17cf 0b7b 786e ed8a ae49 89e4 2aeb 0c01 01c6 3856 276e 797c 87b3 0aa1 31d2 f35f e030 f414 0791 9275 51b6 761b d594 f3ff 013b 4753 62d1 ce5e 7a73 8b4e caf2 d480 85cf 0b73 7a7e cd1a ae69 89e4 2ae3 9c00 fe30 f4ac 8591 32a1 518e 741b d51d 23ff fe54 b4a8 9daf 3081 c18c 7499 952d 2b7e 7839 c784 85d1 8665 78b6 765e ce1c 73a0 852b 4f7b 7ad1 ce9a 7a49 894e cae3 8c80 00d4 b456 272e 317d 85b3 2ab9 15d0 f37f 1730 d6eb f891 928a 5149 891b d56b 0cfe 0130 d773 7a91 921e 5171 8b1f d7e2 9ce8.

The truth table of a (12,0,11,1994) function in Example 4, with $AI(f) = 6$ and $FAI(f) = 11$.

4355 660f cc96 ff5a bd3a c2bf 8685 53dd 9d3a c29f 8685 53dd 3f32 c22f 8683 d1d9 953e c29f 8685 5bdd 2f12 db2f 8403 91c9 3d32 c22f 8605 d1d9 ab81 1d60 a13a b422 55fe c29f 8685 dbdd 2a81 3d70 797a a422 2f32 cb2f 8403 95c9 54ed 6690 7bf4 4e7e 3d1a c22f 8685 d1dd 42d1 3d40 797a ac22 2b03 9d60 a03a b422 2b02 d96d 840b b581 d5fe 629f 8685 5bdd ab03 5d69 a03b b4a3 2a01 1d60 797a a422 50ed 34d0 7bfc 6e16 af33 c32f 8603 91c9 d4fc 2692 7bd4 5b7e 54ed 2490 7bf4 4e76 50cd 3dd0 7978 2f26 3d3a c2bf 8685 f1dd ab12 db2f 840b b189 02c1 3d60 797a ac22 c2c5 3dc0 797a 2e22 ab07 9d68 a03b b422 54fc 2292 7fc4 4b5e ab02 d96f 850b b181 54fc 6296 5fc4 4b5c 55fe 629f 0e85 5bdd d5fe 629f

4ec5 5bdd ab03 dd69 803b b4a1 57fe 629f 5ec7 4bdd 2a01 9d60 717a a422 eb03 dd6d 843b b4a1 d0cd 34d0 79fc 6e36 54fe 629f 5fc5 4bdd af32 c32f 8687 91c8 aa01 9d60 f13a a422 54fc 2692 7bf4 4a7e 2b03 dd6d 842b b481 54ed 24d0 7bfc 4e76 50cd 3cd0 79f8 6e37 c0cd 3dd0 797a 2e26 d4fc 629f 5fc4 4bd9 3d3a c6bf 8685 53f5 af30 c32f 8687 d1d9 2b12 db2f 8403 9189 aa01 9d60 b13a b422 22c1 3d60 797a a422 d4fd 2692 7bf4 4e7e 42c5 3940 797a 2c22 ab03 d96d 842b b581 2b03 9d68 a03b b4a3 54ed 24d0 7bfc 6e36 54fc 2292 7bc4 4b7e 50cd 3cd0 7978 6e26 ab12 d96f 840b b189 c2cd 3dd0 797a 2e20 d4fc 2296 5fc4 0b5e d4fc 6297 5fc4 4bdc.

References

[1] A. Braeken, B. Preneel, Probabilistic algebraic attacks, in: IMA Conference on Cryptography and Coding, LNCS, vol. 3796, Springer, 2005, pp. 290–303.

[2] C. Carlet, 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, LNCS, vol. 5350, Springer, 2008, pp. 425–440.

[3] P. Camion, C. Carlet, P. Charpin, N. Sendrier, On correlation-immune functions, in: Advances in Cryptology—CRYPTO'91, LNCS, vol. 547, Springer, 1992, pp. 86–100.

[4] S. Chee, S. Lee, D. Lee, S.H. Sung, On the correlation immune functions and their nonlinearity, in: Advances in Cryptology—Asiacrypt'96, LNCS, vol. 1163, Springer, 1997, pp. 232–243.

[5] N. Courtois, W. Meier, Algebraic attacks on stream ciphers with linear feedback, in: Advances in Cryptology—EUROCRYPT 2003, LNCS, vol. 2656, Springer, 2003, pp. 346–359.

[6] N. Courtois, Fast algebraic attacks on stream ciphers with linear feedback, in: Advances in Cryptology—CRYPTO 2003, Springer, LNCS, vol. 2729, 2003, pp. 176–194.

[7] J.F. Dillon, Elementary Hadamard Difference Sets, Dept. Comput. Sci., Univ. Maryland, College Park, MD, USA, 1974 Ph.d. dissertation.

[8] S. Gangopadhyay, S. Sarkar, R. Telang, On the lower bounds of the second order nonlinearities of some boolean functions, Inf. Sci. 180 (2010) 266–273.

[9] J.D. Golić, On the security of nonlinear filter generators, in: Fast Software Encryption'96, LNCS, vol. 1039, Springer, 1996, pp. 173–188.

[10] J.D. Golic, A. Clark, E. Dawson, Generalized inversion attack on nonlinear filter generators, IEEE Trans. Comput. 49 (10) (2000) 1100–1109.

[11] M.A. Khan, F. Özbudak, Hybrid classes of balanced boolean functions with good cryptographic properties, Inf. Sci. 273 (2014) 319–328.

[12] R.L. McFarland, A family of noncyclic difference sets, J. Comb. Theory, Ser. A 15 (1973) 1–10.

[13] S. Maitra, E. Pasalic, Further constructions of resilient boolean functions with very high nonlinearity, IEEE Trans. Inf. Theory 48 (7) (2002) 1825–1834.

[14] S. Maitra, E. Pasalic, A maiorana-mcfarland type construction for resilient functions on variables (n even) with nonlinearity $> 2^{n-1} - 2^{n/2} + 2^{n/2-2}$, Discrete Appl. Math. 154 (2) (2006) 357–369.

[15] J.L. Massey, Shift-register synthesis and BCH decoding, IEEE Trans. Inf. Theory 15 (1) (1969) 122–127.

[16] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-correcting Codes, Amsterdam, The Netherlands: North-Holland, 1977.

[17] W. Meier, E. Pasalic, C. Carlet, Algebraic attacks and decomposition of boolean functions, in: Advances in Cryptology—EUROCRYPT 2004, LNCS, vol. 3027, Springer, 2004, pp. 474–491.

[18] E. Pasalic, T. Johansson, Further results on the relation between nonlinearity and resiliency of boolean functions, in: IMA Conference on Cryptography and Coding, LNCS, vol. 1746, Springer, 1999, pp. 35–45.

[19] E. Pasalic, Probabilistic versus deterministic algebraic cryptanalysis - a performance comparison, IEEE Trans. Inf. Theory 55 (11) (2009) 2182–2191.

[20] P. Sarkar, S. Maitra, Construction of nonlinear boolean functions with important cryptographic properties, in: Advances in Cryptology—EUROCRYPT'00, LNCS, vol. 1807, Springer, 2000, pp. 485–506.

[21] P. Sarkar, S. Maitra, Nonlinearity bounds and constructions of resilient functions, in: Advances in Cryptology—CRYPTO'00, LNCS, vol. 1807, Springer, 2000, pp. 515–532.

[22] J. Seberry, X.M. Zhang, Y. Zheng, On constructions and nonlinearity of correlation immune boolean functions, in: Advances in Cryptology—EUROCRYPT'93, LNCS, vol. 765, Springer, 1994, pp. 181–199.

[23] X. Tang, D. Tang, X. Zeng, L. Hu, Balanced boolean functions with (almost) optimal algebraic immunity and very high nonlinearity, 2010, Cryptology ePrint Archive, Report 2010/443.

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

[25] Z. Tu, Y. Deng, Boolean functions optimizing most of the cryptographic criteria, Discrete Appl. Math. 160 (2012) 427–435.

[26] G. Xiao, J.L. Massey, A spectral characterization of correlation-immune combining functions, IEEE Trans. Inf. Theory 34 (3) (1988) 569–571.

[27] X. Zeng, C. Carlet, J. Shan, L. Hu, More balanced boolean functions with optimal algebraic immunity and good nonlinearity and resistance to fast algebraic attacks, IEEE Trans. Inf. Theory 57 (9) (2011) 6310–6320.

[28] F. Zhang, C. Carlet, Y. Hu, T. Cao, Secondary constructions of highly nonlinear boolean functions and disjoint spectra plateaued functions, Inf. Sci. 283 (2014) 94–106.

[29] W.-G. Zhang, E. Pasalic, Generalized maiorana-mcfarland construction of resilient boolean functions with high nonlinearity and good algebraic properties, IEEE Trans. Inf. Theory 60 (10) (2014) 6681–6695.

[30] W.-G. Zhang, G.-Z. Xiao, Constructions of almost optimal resilient boolean functions on large even number of variables, IEEE Trans. Inf. Theory 55 (12) (2009) 5822–5831.

[31] W.-G. Zhang, E. Pasalic, Constructions of resilient s-boxes with strictly almost optimal nonlinearity through disjoint linear codes, IEEE Trans. Inf. Theory 60 (3) (2014) 1638–1651.