Pan SS, Fu XT, Zhang WG. Construction of 1-resilient Boolean functions with optimal algebraic immunity and good nonlinearity. JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY 26(2): 269–275 Mar. 2011. DOI 10.1007/s11390-011-1129-4

Construction of 1-Resilient Boolean Functions with Optimal Algebraic Immunity and Good Nonlinearity

Sen-Shan Pan[1] (潘森杉), Xiao-Tong Fu[1,2] (傅晓彤), and Wei-Guo Zhang[1] (张卫国), *Member*, *IEEE*

[1] *State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an 710071, China*

[2] *State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing 100190, China*

E-mail: pansenshan@gmail.com; xtfu@mail.xidian.edu.cn; w.g.zhang@qq.com

Received June 3, 2010; revised February 13, 2011.

Abstract This paper presents a construction for a class of 1-resilient functions with optimal algebraic immunity on an even number of variables. The construction is based on the concatenation of two balanced functions in associative classes. For some n, a part of 1-resilient functions with maximum algebraic immunity constructed in the paper can achieve almost optimal nonlinearity. Apart from their high nonlinearity, the functions reach Siegenthaler's upper bound of algebraic degree. Also a class of 1-resilient functions on any number $n > 2$ of variables with at least sub-optimal algebraic immunity is provided.

Keywords stream ciphers, Boolean functions, 1-resilient, algebraic immunity, algebraic degree

1 Introduction

Boolean functions are frequently used as nonlinear combiners or nonlinear filters in certain models of stream cipher systems. Nowadays, a mounting number of attacks (Berlekamp-Massey attack, correlation attack, fast algebraic attack, i.e., FAA) on stream ciphers have been proposed. This reality will lead to the result that people have to revise old methods or design new ones to generate good Boolean functions for resisting as many attacks as possible simultaneously. Balancedness, a high nonlinearity, a high algebraic immunity, and in the case of the combiner model, a proper correlation immunity (in the case of the filter model, a correlation immunity of order 1 is commonly considered as sufficient) are the cryptographic characteristics of good stream ciphers. The interactions of them are so complicated that some are even contrary to others. For instance, Maiorana-McFarland, i.e., M-M, together with its variations is a popular and favorable approach for a number of well-behaved functions. Being constructed by affine subfunctions, M-M construction, has an evident drawback against FAA[1]. It is an interesting fact that any randomly chosen balanced function on a large number of variables has good algebraic immunity with very high probability, whereas this is not so when considering a specific construction. It is unfeasible to find the functions with all good characteristics by a trial and error method.

Lately, the problem of finding resilient functions with optimized algebraic immunity and high nonlinearity has become a hot topic. It seems that in [1], a class of 1-resilient and optimal algebraic immunity functions was first obtained through a doubly indexed recursive relation. But its low nonlinearity impedes the utilization in cryptographic models. The symmetry of the functions presents a risk if attacks using this peculiarity can be found in the future. Recently, when the number of variables n only equals 6, 8, 10, 12, [2] provided 1-resilient functions with maximum degree and optimal algebraic immunity by a primary construction. Bars and Viola in [3] are trying to find a complete combinatorial characterization of well-behaved functions and good random generation algorithms for well-behaved functions. Though their classification is crude, being a first step towards their extremely tough direction, the work in [3] is of interest.

In this paper we propose a construction method to design 1-resilient Boolean functions on an even number of variables ($n \geqslant 3$). The constructed functions have the properties of maximum degree and optimal algebraic immunity. The constructions provided in Section 3 and Section 5 reveal a good adaptability: a function with higher nonlinearity can be obtained

Short Paper

This work is supported by the National Natural Science Foundations of China under Grant Nos. 60903200, 61003299.

merely by employing the base functions with improved nonlinearity not by changing the generation methods. Besides, using the examples in [4-5], we find functions with almost optimal nonlinearity.

The organization of this paper is as follows. In Section 2, the basic concepts and notions are presented. In Section 3, we propose a secondary construction (i.e., Siegenthaler's[6] construction) by concatenating two balanced Boolean functions f, g with odd variables n, where $deg(f) = n-1$, $AI(f) = (n+1)/2$, $g \in \hat{H}_f$. Then we prove the existence of a nontrivial pair (f, g) applied in the construction. But we can only construct a part of 1-resilient Boolean functions with optimal algebraic immunity by using these pairs. Our concrete realization is given in Section 4 by introducing the functions in [4-5]. In Section 5, we obtain a larger class of functions with sub-optimal algebraic immunity on any number ($\geqslant 2$) of variables. Finally, Section 6 concludes the paper.

2 Preliminary

A Boolean function $f(\boldsymbol{x})$ is a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$, where $\mathbb{F}_2^n$ is the vector space of tuples of elements from $\mathbb{F}_2$ and $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$. To avoid confusion with the additions of integers in $\mathbb{R}$, denoted by $+$ and Σ_i, we deliberately denote the additions over $\mathbb{F}_2$ by $\oplus$ and $\oplus_i$. For simplicity, we denote by $+$ the addition of vectors of $\mathbb{F}_2^n$. $f(\boldsymbol{x})$ is generally represented by its algebraic normal form (ANF):

$$f(\boldsymbol{x}) = \sum_{\boldsymbol{u} \in \mathbb{F}_2^n} \lambda_{\boldsymbol{u}} \Big(\prod_{i=1}^{n} x_i^{u_i} \Big) \tag{1}$$

where $\lambda_{\boldsymbol{u}} \in \mathbb{F}_2$, $\boldsymbol{u} = (u_1, \ldots, u_n)$. The algebraic degree of $f(\boldsymbol{x})$, denoted by $deg(f)$, is the maximal value of $wt(\boldsymbol{u})$ such that $\lambda_{\boldsymbol{u}} \neq 0$, where $wt(\boldsymbol{u})$ denotes the weight of $\boldsymbol{u}$.

In this paper, the weight of a binary vector $\boldsymbol{u}$ is always the Hamming weight, i.e., the number of nonzero components in $\boldsymbol{u}$.

Definition 1. *Let f be a Boolean function of degree d. $LT(f)$, denoting the sum of the monomials in f which are all of degree d, is called the leading term of f.*

An r-th order Reed-Muller code $R(r, n)$ is the set of all binary strings (vectors) of length 2^n associated with the Boolean polynomials $f(x_1, x_2, \ldots, x_n)$ of degree at most r. The set of the Boolean functions with the leading term $LT(f)$ is the coset $f + R(deg(f) - 1, n)$. In Section 3, we will find that LT is the crucial notion for the algebraic degree and the algebraic immunity degree.

f is called an affine function when $deg(f) = 1$. An affine function with constant term equal to zero is called a linear function. Any linear function on $\mathbb{F}_2^n$ is denoted by:

$$\boldsymbol{\omega} \cdot \boldsymbol{x} = \omega_1 x_1 + \cdots + \omega_n x_n,$$

where $\boldsymbol{\omega} = (\omega_1, \ldots, \omega_n)$, $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$. The *Walsh* spectrum of $f \in \mathbb{F}_2^n$ in point $\boldsymbol{\omega}$ is denoted by $W_f(\boldsymbol{\omega})$ and calculated by

$$W_f(\boldsymbol{\omega}) = \sum_{\boldsymbol{x} \in \mathbb{F}_2^n} (-1)^{f(\boldsymbol{x}) + \boldsymbol{\omega} \cdot \boldsymbol{x}}. \tag{2}$$

$f \in \mathbb{F}_2^n$ is said to be balanced if its output column in the truth table contains an equal number of 0's and 1's (i.e., $W_f(\boldsymbol{0}) = 0$).

In [7], a spectral characterization of resilient functions has been presented.

Lemma 1. *An n-variable Boolean function is m-resilient if and only if its Walsh transform satisfies*

$$W_f(\boldsymbol{\omega}) = 0, \ \textit{for } 0 \leqslant wt(\boldsymbol{\omega}) \leqslant m, \ \boldsymbol{\omega} \in \mathbb{F}_2^n. \tag{3}$$

The Hamming distance between two n-variable Boolean functions f and ρ is denoted by

$$d(f, \rho) = \{\boldsymbol{x} \in \mathbb{F}_2^n : f(\boldsymbol{x}) \neq \rho(\boldsymbol{x})\}.$$

The set of all affine functions on $\mathbb{F}_2^n$ is denoted by $A(n)$. The nonlinearity of a Boolean function $f \in \mathbb{F}_2^n$ is its distance to the set of all affine functions and is defined as

$$N_f = \min_{\rho \in A(n)} (d(f, \rho)).$$

In terms of *Walsh* spectra, the nonlinearity of f is given by [8]

$$N_f = 2^{n-1} - \frac{1}{2} \cdot \max_{\boldsymbol{\omega} \in \mathbb{F}_2^n} |W_f(\boldsymbol{\omega})|. \tag{4}$$

Parseval's equation[9] states that

$$\sum_{\boldsymbol{\omega} \in \mathbb{F}_2^n} (W_f(\boldsymbol{\omega}))^2 = 2^{2n}. \tag{5}$$

So any Boolean function f with n variables satisfies

$$\max_{\boldsymbol{\omega} \in \mathbb{F}_2^n} |W_f(\boldsymbol{\omega})| \geqslant 2^{n/2};$$

the functions for which equality holds are called bent functions. Obviously, the nonlinearity of bent functions is $2^{n-1} - 2^{n/2-1}$, where n is even.

Definition 2. *Let f be a Boolean function with n variables. Then f is said to be almost optimal if $N_f \geqslant 2^{n-1} - 2^{(n-1)/2}$ when n is odd, and $N_f \geqslant 2^{n-1} - 2^{n/2}$ when n is even.*

Proposition 1. *The algebraic degree, algebraic immunity and nonlinearity of a Boolean function f are invariant under an affine transformation towards its input, i.e.,*

$$g(\boldsymbol{x}) = f(\boldsymbol{A}\boldsymbol{x} + \boldsymbol{b}),$$

where $\boldsymbol{A} = (\boldsymbol{A}_1, \boldsymbol{A}_2, \ldots, \boldsymbol{A}_n)^{\mathrm{T}} \in GL_n(\mathbb{F}_2)$*, such that* $\boldsymbol{A}\boldsymbol{x} = (\boldsymbol{A}_1 \cdot \boldsymbol{x}, \boldsymbol{A}_2 \cdot \boldsymbol{x}, \boldsymbol{A}_n \cdot \boldsymbol{x})$ *and* $\boldsymbol{b} \in \mathbb{F}_2^n$*.*

The Idea of the Proof. An affine transformation preserves the degree and via this transformation we have a bijection between the annihilators of same degree. Also, an affine function is changed to another affine one, making the distance between f and the set of all affine functions invariant. □

Let $\mathbf{1}_f = \{\boldsymbol{b}_i = (b_{i1}, \ldots, b_{in}) | f(\boldsymbol{b}_i) = 1,\ 1 \leqslant i \leqslant wt(f)\}$. f can be represented as follows:

$$f(x_1, \ldots, x_n) = \sum_{i=1}^{wt(f)} \prod_{j=1}^{n} (x_j + 1 + b_{ij}),$$

where $\prod_{j=1}^{n}(x_j + 1 + b_{ij})$ is a minterm, satisfying that $f(\boldsymbol{x}) = 1$ iff $\boldsymbol{x} = \boldsymbol{b}_i$ for some $1 \leqslant i \leqslant wt(f)$.

Clearly, $deg(f) < n$ iff $wt(f)$ is even. Moveover, $deg(f) = n - 1$ iff $wt(f)$ is even and

$$\sum_{i=1}^{wt(f)} (b_{i1}, \ldots, b_{in}) \neq 0. \tag{6}$$

Definition 3. *An* $n \times wt(f)$ *matrix* $\boldsymbol{S}_f$ *with entries from* $\mathbb{F}_2$ *is called a support matrix of* f *if*

$$\boldsymbol{S}_f = (\boldsymbol{b}_1^{\mathrm{T}}, \boldsymbol{b}_2^{\mathrm{T}}, \ldots, \boldsymbol{b}_{wt(f)}^{\mathrm{T}}),$$

where $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_{wt(f)}$ *are all of vectors in* $\mathbf{1}_f$*.*

This implies that the column reordering of $\boldsymbol{S}_f$ is also a support matrix. Then we derive the following proposition from (6).

Proposition 2. *For a Boolean function* f*, if* $deg(f) = n - 1$*, then* $\exists k$*,* $1 \leqslant k \leqslant n$*, such that*

$$b_{*k} = 1 \bmod 2, \tag{7}$$

where $b_{*k} = \sum_{i=1}^{wt(f)} b_{ik}$*. Namely, if* $deg(f) = n - 1$*, at least one row of* $\boldsymbol{S}_f$ *weights odd.*

Lemma 2. *Let* $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{F}_2^n$ *be two binary vectors.*

$$wt(\boldsymbol{a} + \boldsymbol{b}) = wt(\boldsymbol{a}) + wt(\boldsymbol{b}) - 2wt(\boldsymbol{a} \cdot \boldsymbol{b}).$$

Proof.

$$\begin{aligned} wt(\boldsymbol{a} + \boldsymbol{b}) &= |\mathbf{1}_{\boldsymbol{a}} \cap \mathbf{0}_{\boldsymbol{b}}| + |\mathbf{0}_{\boldsymbol{a}} \cap \mathbf{1}_{\boldsymbol{b}}| \\ &= |\mathbf{1}_{\boldsymbol{a}} \cap \mathbf{0}_{\boldsymbol{b}}| + |\mathbf{1}_{\boldsymbol{a}} \cap \mathbf{1}_{\boldsymbol{b}}| + |\mathbf{1}_{\boldsymbol{a}} \cap \mathbf{1}_{\boldsymbol{b}}| + \\ &\quad |\mathbf{0}_{\boldsymbol{a}} \cap \mathbf{1}_{\boldsymbol{b}}| - 2|\mathbf{1}_{\boldsymbol{a}} \cap \mathbf{1}_{\boldsymbol{b}}| \\ &= |\mathbf{1}_{\boldsymbol{a}}| + |\mathbf{1}_{\boldsymbol{b}}| - 2|\mathbf{1}_{\boldsymbol{a}} \cap \mathbf{1}_{\boldsymbol{b}}| \\ &= wt(\boldsymbol{a}) + wt(\boldsymbol{b}) - 2wt(\boldsymbol{a} \cdot \boldsymbol{b}). \end{aligned}$$

□

Lemma 3. *Let* f *be a balanced Boolean function with* n *variables. If* $deg(f) = n-1$*, then* $rank(\boldsymbol{S}_f) = n$*.*

Proof. Let $n \times 2^{n-1}$ matrix $\boldsymbol{S}_f = (\boldsymbol{b}_1^{\mathrm{T}}, \boldsymbol{b}_2^{\mathrm{T}}, \ldots, \boldsymbol{b}_{2^{n-1}}^{\mathrm{T}})$. As any two columns of $\boldsymbol{S}_f$ are distinct, $n - 1 \leqslant rank(\boldsymbol{S}_f) \leqslant n$.

Suppose the rank of $\boldsymbol{S}_f$ is $n - 1$. Without loss of generality, assume the first $n - 1$ rows of the matrix is linearly independent, which is denoted by $\boldsymbol{S}'_f$. It can be deduced that any two columns of $\boldsymbol{S}'_f$ are still different. Otherwise, the extensions of the two columns of $\boldsymbol{S}_f$ are the same. Therefore, $\boldsymbol{S}'_f$ contains all 2^{n-1} possible column vectors exactly once. That means the weights of row vectors of $\boldsymbol{S}'_f$ are the same: 2^{n-2}. And the n-th row is the linear combination of the rests. So the weight of the last row $b_{*n} = \sum_{i=1}^{wt(f)} b_{in}$ is also even by Lemma 2. In other words, the weight of each row of $\boldsymbol{S}_f$ is even. For $deg(f) = n - 1$, there must exist a row with odd weight by Proposition 2, a contradiction occurs.

Hence, $rank(\boldsymbol{S}_f) = n$. □

The $n \times 2^{n-1}$ matrix $\boldsymbol{S}_f$ can be regarded as the generating matrix of a code and all of the codewords form the space of dimension n. If we denote $\{w_0, w_1, \ldots, w_{2^{n-1}}\}$ as the weight distribution of the code, where w_i is the number of codewords weighting i. Say that we have $2^{n-1} + 1$ different weights for 2^n codewords, the worst case is two codewords for $2^{n-1} - 1$ weights and one codeword for the last two weights.

Definition 4. *The algebraic immunity* $AI(f)$ *of a Boolean function* $f \in \mathbb{F}_2^n$ *is defined as the lowest degree of nonzero functions* g *such that* $fg = 0$ *or* $(f+1)g = 0$*.*

Here, the definition of the correlation class in [3] is extended in order to take other cryptographically important properties into consideration:

Definition 5. *Let* n *be the number of variables, a Boolean function with* n *variables* f *belongs to the correlation class* H_f *defined by*

$$\langle wt(f), deg(f), AI(f), LT(f); \delta_n, \ldots, \delta_1 \rangle,$$

where $wt(f)$ *is the Hamming weight of* f*,* $deg(f)$ *the algebraic degree,* $AI(f)$ *the algebraic immunity,* $LT(f)$ *the leading term and* $\delta_j = wt(f|_{x_j=0}) - wt(f|_{x_j=1})$*, for any* $1 \leqslant j \leqslant n$*.*

Generally,

$$\langle wt(f), deg(f), AI(f); \delta_n, \ldots, \delta_1 \rangle$$

is the correlation class without considering the leading term. $\langle wt(f); \delta_n, \ldots, \delta_1 \rangle$ is the correlation class without considering the degree, the algebraic immunity and the leading term.

The notations used in [3] are generalized below:

Notation 1.

- $\Omega_n^{m,d,AI} = \{\omega | \forall f \in \omega,\ f \in \mathbb{F}_2^n,\ wt(f) = m,$ $deg(f) = d$ *and* $AI(f) = AI\}$.
- $\Omega_n^{m,d} = \cup_{AI=0}^{\max\{d, \lceil n/2 \rceil\}} \Omega_n^{m,d,AI}$.
- $\Omega_n^m = \cup_{d=0}^{n} \Omega_n^{m,d}$.
- $\Omega_n = \cup_{m=0}^{2^n} \Omega_n^m$.

- $Res_n^{1,d,AI} = \langle 2^{n-1}, d, AI; 0, \ldots, 0\rangle$.
- $Res_n^{1,d} = \langle 2^{n-1}, d; 0, \ldots, 0\rangle$.
- $Res_n^1 = \langle 2^{n-1}; 0, \ldots, 0\rangle$.

The definition of the equivalence relation below is analogous to that in [3].

Definition 6. *Let f, g be two Boolean functions with n variables. The equivalence relation $\mathcal{R}$ is defined by*

$$f\mathcal{R}g \Longleftrightarrow Abs(H_f) = Abs(H_g)$$

where

$$Abs(\langle m, d, AI, LT; \delta_n, \ldots, \delta_1\rangle) =$$

$$\langle wt(f), deg(f), AI(f); |\delta_n|, \ldots, |\delta_1|\rangle,$$

and m denotes the weight of Boolean functions in ζ, d the degree, AI the algebraic immunity and LT the leading term.

Definition 7[3]**.** *Let p, $q \in \{0, \ldots, 2^n\}$,*

$$\zeta^0 \in \Omega_n^p, \zeta^1 \in \Omega_n^q.$$

The operator class $*$ is defined by

$$\zeta^0 \times \zeta^1 = \zeta,$$

where

$$\begin{aligned}\zeta &= \langle p+q; \delta_{n+1}, \delta_n, \ldots, \delta_1\rangle \\ &= \langle p+q; p-q, \delta_n^0 + \delta_n^1, \ldots, \delta_1^0 + \delta_1^1\rangle \\ &\in \Omega_{n+1}^{p+q}.\end{aligned}$$

Let $\zeta^0 \times \zeta^1$ denote the set

$$\{h \in \{0,1\}^{2^{n+1}} | h = f\|g, \quad f \in \zeta^0, g \in \zeta^1\}$$

where $f\|g = (1 + x_{n+1})f + x_{n+1}g$ is the concatenation of two strings.

The following Lemma in [3] enables the decomposition of correlation classes.

Lemma 4[3] (Decomposition).

$$\zeta = \bigcup_{\zeta^0 * \zeta^1 = \zeta} \zeta^0 \times \zeta^1.$$

An extended version of the mirror class[3] is employed as follows.

Definition 8. *Let*

$$\zeta = \langle m, d, AI, LT; \delta_n, \delta_{n-1}, \ldots, \delta_1\rangle.$$

The mirror class of ζ is the class

$$\hat{\zeta} = \langle m, d, AI, LT; -\delta_n, -\delta_{n-1}, \ldots, -\delta_1\rangle. \qquad (8)$$

Notice that the bijection $f \mapsto \hat{f}$ such that

$$\hat{f}(x_1, x_2, \ldots, x_n) = f(x_1 + 1, x_2 + 1, \ldots, x_n + 1)$$

preserves the leading term of f. Moreover, it corresponds to a mapping between the correlation class of f and the mirror one, hence the cardinalities of the two classes are the same: $|\hat{\zeta}| = |\zeta|$.

Definition 9[3]**.** *Let f be a Boolean function with n variables and Hamming weight $2m$. Then, f is first-order correlation-immune when $wt(f|_{x_j=0}) = wt(f|_{x_j=1}) = m$, for $1 \leqslant j \leqslant n$. Moreover, f is first-order resilient for $m = 2^{n-2}$.*

It is easily seen that $\zeta = \hat{\zeta}$ if and only if $\forall f \in \zeta$ are first-order correlation-immune.

3 Degree Optimized 1-Resilient Functions with Optimal Algebraic Immunity

Proposition 3. *Let f, g be two Boolean functions with $deg(f) = d_1$ and $deg(g) = d_2$. Let $h = (1 + x_{n+1})f + x_{n+1}g \in \mathbb{F}_2^{n+1}$. Then*

1) *If $d_1 \neq d_2$, then $deg(h) = \max\{d_1, d_2\} + 1$.*

2) *If $d_1 = d_2 = d$, then $d \leqslant deg(h) \leqslant d + 1$, and $deg(h) = d$ iff $LT(f) = LT(g)$.*

Clearly, for $LT(f) = LT(g)$, besides the polynomial $LT(f)$, $LT(h)$ may contain the monomials of degree d with the variable x_n. These terms are composed with the monomials of degree $d - 1$ in f and g. So those monomials of degree $d - 1$ in both f and g should be taken into account and they are composed with functions of a less degree. Hence this special case hinders a bottom-up traversal of correlation classes and enumerating them.

A similar result about the algebraic immunity is as follows.

Proposition 4[1]**.** *Let f, g be two Boolean functions on the variables $x_1, x_2, \ldots, x_n$ with $AI(f) = d_1$ and $AI(g) = d_2$. Let $h = (1 + x_{n+1})f + x_{n+1}g \in \mathbb{F}_2^{n+1}$. Then*

1) *If $d_1 \neq d_2$, then $AI_{n+1}(h) = \min\{d_1, d_2\} + 1$.*

2) *If $d_1 = d_2 = d$, then $d \leqslant AI_{n+1}(h) \leqslant d + 1$, and $AI_{n+1}(h) = d$ iff there exists f_1 (g_1) as an annihilator of f or $f+1$ (g or $g+1$) such that $deg(f_1 + g_1) \leqslant d-1$, say $LT(f_1) = LT(g_1)$.*

Construction 1. *Let n be any odd integer such that $n \geqslant 3$ and f be a balanced Boolean function with maximum degree $n-1$ and optimal algebraic immunity $(n+1)/2$, i.e.,*

$$f \in \langle 2^{n-1}, n-1, (n+1)/2, LT(f); \delta_n, \ldots, \delta_1\rangle.$$

Let

$$h = (1 + x_{n+1})f + x_{n+1}g \in \mathbb{F}_2^{n+1},$$

where $g \in \hat{H}_f$.

Notice $\hat{H}_f$ is not empty for any Boolean function f aforementioned because $\bar{f} = f + 1 \in \hat{H}_f$. Besides, there is another element $\hat{f}(\boldsymbol{x}) = f(\boldsymbol{x} + \mathbf{1})$ in $\hat{H}_f$. Here,

$(f, \bar{f})$ and $(f, \hat{f})$ are called the trivial pairs. Clearly the number of choices for g depends on the class H_f.

Theorem 1. *$h \in \mathbb{F}_2^{n+1}$ in Construction 1 is 1-resilient Boolean function with maximum degree and optimal algebraic immunity, if $g \in \hat{H}_f$.*

Proof. It can be deduced that $h \in Res_{n+1}^1$ by Definition 7. As $g \in \hat{H}_f$, $deg(h) = n-1$ by Proposition 3, so we have

$$h \in \langle 2^n, n-1, AI(h); 0, 0, \ldots, 0\rangle,$$

which is 1-resilient function of optimized degree.

Using Proposition 4, $(n+1)/2 \leqslant AI(h) \leqslant (n+3)/2$ for $AI(f) = AI(g) = (n+1)/2$. However, $AI(h)$ being upper bounded by $(n+1)/2$, h has maximum algebraic immunity $(n+1)/2$. Thus $h \in Res_{n+1}^{1,n-1,(n+1)/2}$. □

Theorem 2. *The nonlinearity of h in Construction 1 is $N_h \geqslant N_f + N_g$.*

Proof. Let $\boldsymbol{x} = (\boldsymbol{x}', x_{n+1}), \boldsymbol{\omega} = (\boldsymbol{\omega}', \omega_{n+1}) \in \mathbb{F}_2^{n+1}$.

$$\begin{aligned} W_h(\boldsymbol{\omega}) &= \sum_{\boldsymbol{x}\in\mathbb{F}_2^{n+1}} (-1)^{\boldsymbol{\omega}\cdot\boldsymbol{x}+h(\boldsymbol{x})} \\ &= \sum_{\boldsymbol{x}'\in\mathbb{F}_2^{n}} (-1)^{f(\boldsymbol{x}')+\boldsymbol{\omega}'\cdot\boldsymbol{x}'} + \\ &\quad (-1)^{\omega_{n+1}} \sum_{\boldsymbol{x}'\in\mathbb{F}_2^{n}} (-1)^{g(\boldsymbol{x}')+\boldsymbol{\omega}'\cdot\boldsymbol{x}'} \\ &= W_f(\boldsymbol{\omega}') + (-1)^{\omega_{n+1}} W_g(\boldsymbol{\omega}'). \end{aligned} \tag{9}$$

By (4), we have

$$N_h \geqslant N_f + N_g.$$

In particular, for $g = \bar{f}$ or $\hat{f}$, $N_h = 2N_f$. □

Next, we want to figure out whether there is a nontrivial function in $\hat{H}_f$ (i.e., $g \neq \bar{f}, \hat{f}$). This can be converted to the proof whether there is a third element in H_f besides f and $\hat{f}+1$. The answer seems yes, but it has not been proved yet. So we leave it as an open problem.

However, another property is enough:

Proposition 5. *A pair of Boolean functions with n variables (f^*, g^*) derived from a given function $f \in \mathbb{F}_2^n$ can always be found, where f is defined in Construction 1, $deg(f^*) = n-1$, $AI(f^*) = (n+1)/2$, $N_{f^*} = N_f$ and $g^* \in \hat{H}_{f^*}$, $g^* \neq \hat{f}, \bar{f}$.*

Proof. Let us consider an affine transformation:

$$f(\boldsymbol{x}) \mapsto f(\boldsymbol{A}\boldsymbol{x} + \boldsymbol{b}),$$

where $\boldsymbol{A} \in GL_n(\mathbb{F}_2)$ and $\boldsymbol{b} \in \mathbb{F}_2^n$.

1) If there exists $\delta_s = \delta_t$, where $1 \leqslant s < t \leqslant n$. By Lemma 3, the s-th row of $\boldsymbol{S}_f$ differs from the t-th row and its complement. A permutation matrix $\boldsymbol{P}$ can be used to swap x_s and x_t.

(a) If $\mathbf{1}_{f(\boldsymbol{P}\boldsymbol{x})} \neq \mathbf{1}_f$, then $f(\boldsymbol{P}\boldsymbol{x}) \neq f$. And $f(\boldsymbol{P}\boldsymbol{x}) \neq \hat{f}+1$ can be easily reached. So we choose $(f(\boldsymbol{x}), f(\boldsymbol{P}\boldsymbol{x})+1)$ as a nontrivial pair (f^*, g^*).

(b) $\mathbf{1}_{f(\boldsymbol{P}\boldsymbol{x})} = \mathbf{1}_f$, although $\boldsymbol{S}_{f(\boldsymbol{P}\boldsymbol{x})} \neq \boldsymbol{S}_f$: $\forall 1 \leqslant i \leqslant 2^{n-1}$, if $\boldsymbol{b}_i \in \mathbf{1}_f$ and $b_{is} \oplus b_{it} = 1$, then $\boldsymbol{b}_i + \mathbf{1}_{st} \in \mathbf{1}_f$, where $\mathbf{1}_{st} \in \mathbb{F}_2^n$ denotes all of its coordinates are 0 except the s-th and t-th ones. In this case, we can perform an invertible transformation $\boldsymbol{A}$ of adding the s-th or t-th row to any other row of $\boldsymbol{S}_f$ before the permutation. Thus, there is a new function $f'(\boldsymbol{x}) = f(\boldsymbol{A}\boldsymbol{x})$ such that $\mathbf{1}_{f'(\boldsymbol{P}\boldsymbol{x})} \neq \mathbf{1}_{f'}$ and by case (a), a nontrivial pair (f^*, g^*) can still be obtained.

2) If no two δ's are the same, due to Lemma 3, the code generated by S_f has $2^{n-1}+1$ different weights for 2^n codewords. Hence there must be an invertible matrix $\boldsymbol{A}^*$ of dimension n to renew the generating matrix, such that $\boldsymbol{S}_{f(\boldsymbol{A}^*\boldsymbol{x})}$ has two different rows with the same weight. Similar to case 1), we can obtain a required (f^*, g^*). □

For $1 \leqslant i, j \leqslant n$, denoted by $f^{i\leftrightarrow j}$ the Boolean function obtained by permuting the variables x_i and x_j, we will find that $f^{i\leftrightarrow j} = (f|_{x_i=0}) \,||\, (f|_{x_i=1})$, where $||$ means the concatenation of two strings.

Then, the following statement will be deduced:

Theorem 3. *Let h be an $(n+1)$-variable Boolean function in the correlation class $Res_{n+1}^{1,n-1,(n+1)/2}$ where n is odd. For $1 \leqslant i \leqslant n+1$, by permuting its variables, there must be an $h^{i\leftrightarrow(n+1)} \in Res_{n+1}^{1,n-1,(n+1)/2}$ which can be decomposed into $f||g$, i.e., $h = (1+x_{n+1})f + x_{n+1}g$, where f is in ω^0 and g is in ω^1,*

$$\omega^0 = \langle 2^{n-1}, n-1, AI_0; \delta_n, \ldots, \delta_1\rangle$$

and

$$\omega^1 = \langle 2^{n-1}, n-1, AI_1; -\delta_n, \ldots, -\delta_1\rangle$$

where $AI_0, AI_1 \geqslant (n-1)/2$.

Proof. As $LT(h)$ is the leading term of h of degree $n-1$, there is a monomial of degree $n-1$ in $LT(h)$ without the variables x_i and x_j, say, $\prod_{k=1}^{n+1} x_k/(x_i \cdot x_j)$, $1 \leqslant i, j \leqslant n$. Because $f = h^{i\leftrightarrow(n+1)}|_{x_{n+1}=0}$, $g = h^{i\leftrightarrow(n+1)}|_{x_{n+1}=1}$ and $LT(h^{i\leftrightarrow(n+1)})$ have a monomial without x_{n+1}, the degrees of f and g are both $n-1$. If AI_0 or AI_1 is less than $(n-1)/2$, by Proposition 4, $AI(h)$ would not be $(n+1)/2$. So $AI_0, AI_1 \geqslant (n-1)/2$. By Lemma 4 and Definition 7, we can deduce that if f is in ω^0, g will be in ω^1. □

Theorem 3 means, on an even number of variables, all of the 1-resilient Boolean functions with maximum degree and optimal algebraic immunity are equal or affinely equivalent to the functions in the set $\omega^0 \times \omega^1$. Unfortunately, Construction 1 can produce a part of the functions in $Res_{n+1}^{1,n-1,(n+1)/2}$.

4 Concrete Realization

This section uses Boolean functions in [4-5] as base function f.

Construction 2[4]. *Let $f(\boldsymbol{x})$ denote a Boolean function on $\mathbb{F}_2^n$ and $\mathbf{1}_f = \{\boldsymbol{B}^i\boldsymbol{b}_1 | 0 \leqslant i \leqslant 2^{n-1}\}$, where $0 \neq \boldsymbol{b}_1 \in \mathbb{F}_2^n$, $\boldsymbol{B}$ is the companion matrix of a primitive polynomial $p(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1x + 1$ over the field $\mathbb{F}_2$, i.e.,*

$$\boldsymbol{B} = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & c_1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & c_{n-1} \end{pmatrix}.$$

Theorem 4[4]. *f has maximum degree $n-1$ and algebraic immunity $\lceil n/2 \rceil$. Besides, it reaches a high nonlinearity, which is better than* [10].

Now, a class of 1-resilient Boolean functions which are still degree maximized and algebraic immunity optimized has been obtained by using f aforementioned.

Example 1. Let f denote a Boolean function on $\mathbb{F}_2^5$ from Construction 2 and $\mathbf{1}_f = \{\boldsymbol{B}^i\boldsymbol{b}_1 | 0 \leqslant i \leqslant 2^4\}$, where $\boldsymbol{b}_1 = (1,0,0,0,0) \in \mathbb{F}_2^5$. When $p(x) = x^5 + x^2 + 1$, the nonlinearity of f is 10. By choosing $g = f(\boldsymbol{A}\boldsymbol{x} + \boldsymbol{b}) + 1$, $\boldsymbol{b} = (1,0,0,0,0)$ and

$$\boldsymbol{A} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

we can get a 1-resilient function $h \in \mathbb{F}_2^6$, $AI(h) = 3$, $deg(h) = 4$ and $N_h = 2^5 - 2^3 = 24$, which is almost optimal. The following is the truth table of h:

6DA6C82D52953BD2.

On a large number of variables, such as $n = 15$, there exist balanced Boolean functions with currently best known nonlinearity 16 272, the degree 11 and the algebraic immunity 8[5]. Therefore we can get 16-variable 1-resilient functions with the nonlinearity at least 32 544 and the optimal algebraic immunity 8. Of course, the nonlinearity of them is almost optimal which exceeds $2^{15} - 2^8$ by 32.

5 1-Resilient Functions with Sub-Optimal Algebraic Immunity

Generally, we can get an extended version of Construction 1 for any $n \geqslant 2$. This class of Boolean functions can achieve sub-optimized algebraic immunity.

Construction 3. *Let n be any integer such that $n \geqslant 2$ and f is a balanced Boolean function with maximum degree $n-1$ and optimal algebraic immunity $\lfloor (n+1)/2 \rfloor$, i.e.,*

$$f \in \langle 2^{n-1}, n-1, (n+1)/2, LT(f); \delta_n, \ldots, \delta_1 \rangle.$$

Let

$$h = (1 + x_{n+1})f + x_{n+1}g \in \mathbb{F}_2^{n+1},$$

where $g \in \hat{H}_f$.

Theorem 5. *$h \in \mathbb{F}_2^{n+1}$ in Construction 3 is 1-resilient Boolean function with maximum degree and algebraic immunity at least $\lfloor (n+1)/2 \rfloor$, if $g \in \hat{M}_f$.*

6 Conclusion

In this paper, we have described a technique for constructing a class of 1-resilient functions with maximum degree and optimal algebraic immunity on an even number of variables. Unfortunately, this construction only generates a part of the functions belonging to $Res_{n+1}^{1,n-1,(n+1)/2}$. Besides, we have other two and only two possible decompositions:

$$\begin{aligned} &\langle 2^{n-1}, n-1, (n+1)/2; \delta_n, \ldots, \delta_1 \rangle \times \\ &\langle 2^{n-1}, n-1, (n-1)/2; -\delta_n, \ldots, -\delta_1 \rangle, \\ &\langle 2^{n-1}, n-1, (n-1)/2; \delta_n, \ldots, \delta_1 \rangle \times \\ &\langle 2^{n-1}, n-1, (n-1)/2; -\delta_n, \ldots, -\delta_1 \rangle, \end{aligned}$$

where $n \geqslant 3$ is odd. It is hard for us to find two functions exactly contained in respective classes above. Especially in the case of the last one: for two functions in the classes, there does not exist a pair of annihilators of them sharing the same leading term. But it can be seen that the functions with sub-optimal algebraic immunity should be attached great importance to, since the addition of an affine function to them may improve the algebraic immunity by one and they also can be employed to construct functions with good properties, say, functions in $Res_{n+1}^{1,n-1,(n+1)/2}$ in this paper. The reason why we did not give a bottom-up traversal and the enumeration of $Res_{n+1}^{1,n-1,(n+1)/2}$ is that when the base functions or their annihilators share the same leading term, things become more complicated. The best achievable nonlinearity of Construction 1 is unknown except that of functions over a small number of variables. Hence we gain almost optimal functions with 6 variables and the 16-variable 1-resilient functions with maximum algebraic immunity whose nonlinearity is at least 32 544. The adaptability of Construction 1 enables us to find 1-resilient functions with a higher nonlinearity only by introducing balanced functions f with the better nonlinearity than [4] in the future. In the end, we present a larger class of 1-resilient Boolean functions with sub-optimal algebraic immunity.

Acknowledgements The authors are grateful to the anonymous referees for many helpful comments which helped improve the presentation of the paper.

References

[1] Carlet C, Dalai D K, Gupta K C, Maitra S. Algebraic immunity for cryptographically significant Boolean functions: Analysis and construction. *IEEE Transactions on Information Theory*, 2006, 52(7): 3105-3121.

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

[3] Le Bars J M, Viola A. Equivalence classes of Boolean functions for first-order correlation. *IEEE Transactions on Information Theory*, 2010, 56(3): 1247-1261.

[4] Wang Q, Peng J, Kan H, Xue X. Constructions of cryptographically significant Boolean functions using primitive polynomials. *IEEE Transactions on Information Theory*, 2010, 56(6): 3048-3053.

[5] Sarkar S, Maitra S. Idempotents in the neighbourhood of Patterson-Wiedemann functions having Walsh spectra zeros. *Des. Codes Cryptogr.*, 2008, 49: 95-103.

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

[7] Xiao G Z, Massey J L. A spectral characterization of correlation-immune combining functions. *IEEE Transactions on Information Theory*, 1988, 34(3): 569-571.

[8] Meier W, Staffelbach O. Nonlinearity criteria for cryptographic functions. In *Proc. Advances in Cryptology — EUROCRYPT'89*, Houthalen, Belgium, April 10-13, 1990, pp.549-562.

[9] MacWilliams F J, Sloane N J A. The Theory of Error-Correcting Codes. Amsterdam: North-Holland Publishing Co., The Netherlands, 1977.

[10] Carlet C, Feng K. An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity. In *Proc. Advances in Cryptology-ASIACRYPT*, Melbourne, Australia, 2008, pp.425-440.

Sen-Shan Pan is an M.S. candidate in cryptography, Xidian University, Xi'an, China. He received his B.S. degree in information and computing sciences from Nanjing Normal University in 2009. His current research interests cover Boolean function and stream cipher.

Xiao-Tong Fu received her B.S., M.S and PH.D. degrees from Xidian University in 1999, 2002 and 2005 respectively. Since then she has been a lecturer in the Department of Communication Engineering, Xidian University. Her research interests include cryptography, electronic commerce, information and network security.

Wei-Guo Zhang received the B.S. degree in management and Ph.D. degree in cryptography from Xidian University, Xi'an, China, in 2001 and 2007, respectively. Then he joined ISN Lab (State Key Laboratory of Integrated Service Networks) at Xidian University, where he is currently an associate professor. His research interests include cryptography, sequence design, and coding theory.