Hindawi
Security and Communication Networks
Volume 2017, Article ID 6268230, 9 pages
https://doi.org/10.1155/2017/6268230

Research Article

1-Resilient Boolean Functions on Even Variables with Almost Perfect Algebraic Immunity

Gang Han,[1] Yu Yu,[2,3] Xiangxue Li,[3,4,5] Qifeng Zhou,[4] Dong Zheng,[5] and Hui Li[1]

[1]*School of Electronics and Information, Northwestern Polytechnical University, Shaanxi, China*
[2]*Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai, China*
[3]*Westone Cryptologic Research Center, Beijing, China*
[4]*Department of Computer Science and Technology, East China Normal University, Shanghai, China*
[5]*National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications, Xi'an, China*

Correspondence should be addressed to Yu Yu; yuyu@yuyu.hk and Xiangxue Li; xxli@cs.ecnu.edu.cn

Received 15 November 2016; Accepted 12 June 2017; Published 14 September 2017

Academic Editor: Pedro García-Teodoro

Several factors (e.g., balancedness, good correlation immunity) are considered as important properties of Boolean functions for using in cryptographic primitives. A Boolean function is perfect algebraic immune if it is with perfect immunity against algebraic and fast algebraic attacks. There is an increasing interest in construction of Boolean function that is perfect algebraic immune combined with other characteristics, like resiliency. A resilient function is a balanced correlation-immune function. This paper uses bivariate representation of Boolean function and theory of finite field to construct a generalized and new class of Boolean functions on even variables by extending the Carlet-Feng functions. We show that the functions generated by this construction support cryptographic properties of 1-resiliency and (sub)optimal algebraic immunity and further propose the sufficient condition of achieving optimal algebraic immunity. Compared experimentally with Carlet-Feng functions and the functions constructed by the method of first-order concatenation existing in the literature on even (from 6 to 16) variables, these functions have better immunity against fast algebraic attacks. Implementation results also show that they are almost perfect algebraic immune functions.

1. Introduction

Boolean functions are one of the most important cryptographic primitives for stream ciphers, block ciphers, and hash functions in cryptography [1–4]. For instance, we take Boolean functions extensively as filter and combination generators of stream ciphers based on linear feedback shift registers [3]. Cryptographic criteria for Boolean functions include balancedness, algebraic degree, nonlinearity, and correlation immunity. An overview of cryptographic criteria for Boolean functions with extensive bibliography is given in [1].

The study of the cryptographic criteria of Boolean functions is essential because of the connections between known cryptanalytic attacks and these criteria [4]. An improperly chosen Boolean function will render the system open to various kinds of attacks. Take the property of balancedness (i.e., its Hamming weight = 2^{n-1}), for example, the classical cryptographic criterion for designing Boolean function is useful in preventing the system from leaking statistical information on the plaintext when the ciphertext is known.

1.1. Related Work

1.1.1. Resilient Functions. Resilient functions (see Definition 3), first studied by Siegenthaler in [5], are a special class of Boolean functions and find many interesting applications in stream ciphers.

A function f is said to be correlation-immune of the order t if the output of the function is statistically independent of the combination of any t of its inputs [6]. In 1988, Xiao and Massey introduced (by using properties of Walsh spectra) the notion of correlation immunity as an important cryptographic measure of a Boolean function with respect to its resistance against the correlation attack (which can be seen as solving a system of multivariate linear equations) [7].

In [8], Maitra and Sakar discussed the various methods for constructing resilient functions, and their results constitute a subset of a larger set of resilient functions.

1.1.2. Algebraic Attacks. In recent years, algebraic attack [9–11] has received a lot of attention in cryptography. This kind of attacks dates back to 2003 when Courtois and Meier [10] proposed algebraic attack on stream ciphers with linear feedback, which is much powerful (breaking stream ciphers satisfying the previously known design criteria in at most the square root of the complexity of the previously known generic attack). Thus the new cryptographic property of Boolean functions-algebraic immunity (AI), the minimum algebraic degree of annihilators of f or $f+1$, was introduced by Meier et al. [11] to measure the ability of Boolean functions to resist algebraic attacks.

It was shown by Courtois and Meier [10] that maximum AI of n-variable Boolean functions is $\lceil n/2 \rceil$. The properties and constructions of Boolean functions with maximum AI are concerned in a large number of works (to name a few [9, 12–16]). The problem of efficiently constructing balanced Boolean functions with optimal algebraic immunity (and/or other cryptographic properties) is thus of great significance.

1.1.3. Fast Algebraic Attacks. Although Boolean functions with high (or optimal, ideally) algebraic immunity can effectively resist algebraic attack, it does not rule out the possibility that these functions are vulnerable to the improved algebraic attack, that is, fast algebraic attack [17, 18].

Therefore, the cryptographic community turns to address much concern on Boolean functions resisting fast algebraic attack, besides their algebraic immunity. At Asiacrypt 2012, Liu et al. [20] initiated perfect algebraic immune (PAI) functions, Boolean functions with perfect immunity against algebraic and fast algebraic attacks. Although we know that the Carlet-Feng functions [9] on 2^s+1 variables and the modified Carlet-Feng functions on 2^s variables are shown to be perfect algebraic immune functions [20], it is still not easy in general to explore perfect algebraic immune functions, and we do not see much successful attempt made in the literature on perfect algebraic immune functions on even variables. Thus, it is significant in both theory and practice to construct (almost) perfect algebraic immune functions on even variables with other cryptographic properties (such as resiliency) simultaneously.

We notice that Pan et al. [19] presented a construction for a class of 1-resilient Boolean functions with optimal algebraic immunity on an even number of variables by dividing them into two correlation classes, that is, equivalence classes. However, the cryptographic properties of the resulting functions are highly related to those of the initial functions we choose, and in particular, one would not expect strong resistance against fast algebraic attack in the resulting Boolean functions.

1.2. Our Contributions. In the paper, we use primitive polynomials to construct a class of Boolean functions on even variables, achieving at the same time several desirable features. For the resulting functions, we prove the properties of 1-resiliency (see Definition 3) and suboptimal algebraic immunity (see Definition 4). We also propose the sufficient condition of achieving optimal algebraic immunity.

Compared with Carlet-Feng functions [9] and the functions constructed by the method of first-order concatenation existing in the literature on even (from 6 to 16) variables [19], ours show better immunity against fast algebraic attacks. We check that our constructions are almost perfect algebraic immune functions (see Definition 5).

1.3. Roadmap. The remainder of the paper is organized as follows. Section 2 reviews some definitions related to Boolean functions and their cryptographic criteria. Section 3 presents our proposed construction of almost perfect algebraic immune resilient functions on even variables, followed by resiliency analysis in Section 4, by algebraic immunity analysis in Section 5, and by fast algebraic immunity analysis in Section 6, sequentially. Concluding remarks are located in Section 7.

1.4. Notations. We summarize in Notations the notations used in this paper.

2. Preliminaries

Let F_2^n be the vector space of dimension n over the finite field F_2. A Boolean function f on n variables is a mapping from F_2^n to F_2. By the truth table of a Boolean function on n input variables $x = (x_1, \ldots, x_n)$, we mean the 2^n length binary string $\{f(0,0,\ldots,0), f(0,0,\ldots,1), f(0,\ldots,1,0), \ldots, f(1,\ldots,1,1)\}$. The set of n-variable Boolean functions on F_2^n is denoted by $\mathbb{B}_n$.

The Hamming weight of f is the number of 1s in the binary string, denoted by $\mathrm{wt}(f)$. The support of f is the set $\{x \in F_2^n \mid f(x) = 1\}$ and is denoted by $\mathrm{supp}(f)$; that is, $\mathrm{wt}(f) = |\mathrm{supp}(f)|$. The Hamming distance $d_H(f,g)$ between two Boolean functions f and g is the Hamming weight of their difference $f+g$ (i.e., $d_H(f,g) = \mathrm{wt}(f+g)$), where + is the addition on F_2.

Definition 1 (balancedness). A Boolean function f is balanced if its output is equally distributed, that is, the number of 0 elements in its truth table is equal to the number of 1 elements. In other words, an n-variable Boolean function f is balanced if and only if $\mathrm{wt}(f) = 2^{n-1}$.

For $f(x) \in \mathbb{B}_n$, it can be uniquely represented as a multivariate polynomial in the ring

$$\frac{F_2[x_1, x_2, \ldots, x_n]}{(x_1^2 - x_1, \ldots, x_n^2 - x_n)}, \tag{1}$$

and its algebraic normal form (ANF) is written as follows:

$$f(x_1, \ldots, x_n) = \sum_{I \subseteq \{1,2,\ldots,n\}} a_I \prod_{i \in I} x_i, \quad a_I \in F_2. \tag{2}$$

Elements of a finite field can be represented in a variety of ways, depending on the choice of basis for the representation.

Let $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ be a basis of F_2^n over F_2. Then, we can build an isomorphism between F_2^n and F_{2^n}:

$$(x_1, x_2, \ldots, x_n) \longmapsto x_1 \cdot \alpha_1 + x_2 \cdot \alpha_2 + \cdots + x_n \cdot \alpha_n \quad (3)$$

and we can further represent $f : F_{2^n} \to F_2$ as the polynomial

$$f(x) = \sum_{i=0}^{2^n-1} a_i x^i, \quad a_i \in F_{2^n}. \quad (4)$$

Now suppose $n = 2k$. Similarly, $f : F_{2^k} \times F_{2^k} \to F_2$ can be represented uniquely as bivariate polynomial

$$f(x, y) = \sum_{i=0}^{2^k-1} \sum_{j=0}^{2^k-1} a_{i,j} x^i y^j, \quad a_{i,j} \in F_{2^k} \quad (5)$$

and the algebraic degree of f is

$$\deg(f) = \max_{a_{i,j} \neq 0} \left\{ \mathrm{wt}(i) + \mathrm{wt}(j),\ 0 \le i, j \le 2^k - 1 \right\}, \quad (6)$$

where $\mathrm{wt}(i)$ is the Hamming weight of the binary string corresponding to the integer i; namely,

$$\mathrm{wt}(i) = i_1 + i_2 + \cdots + i_\tau \quad (7)$$

if $i = \sum_{l=1}^{\tau} i_l 2^l$.

Definition 2 (Walsh spectrum). Let $f : F_{2^k} \times F_{2^k} \to F_2$, $f(x, y) = \sum_{i=0}^{2^k-1} \sum_{j=0}^{2^k-1} a_{i,j} x^i y^j, a_{i,j} \in F_{2^k}$, and $(a, b) \in F_{2^k} \times F_{2^k}$. The Walsh spectrum of f (at (a, b)) is defined as

$$W_f(a, b) = \sum_{(x,y) \in F_{2^k} \times F_{2^k}} (-1)^{f(x,y) + \mathrm{Tr}_1^n(ax+by)}, \quad (8)$$

where $\mathrm{Tr}_1^n : F_{2^n} \to F_2$ is the trace function, defined as

$$\mathrm{Tr}_1^n(\alpha) = \alpha + \alpha^2 + \alpha^{2^2} + \cdots + \alpha^{2^{n-1}}, \quad \forall \alpha \in F_{2^n}. \quad (9)$$

Correlation immunity has long been recognized as one of the critical indicators of nonlinear combining functions of shift registers in stream generators [21, 22]. A high correlation immunity is generally a very desirable property, in view of various successful correlation attacks against a number of stream ciphers (see, e.g., [23]). The concept of correlation-immune functions was introduced by Siegenthaler [5]. Xiao and Massey gave an equivalent definition [7, 24].

Definition 3 (correlation immunity). A function f is called an mth-order correlation-immune function if

$$W_f(\omega) = 0, \quad \forall \omega \in F_2^n,\ 1 \le \mathrm{wt}(\omega) \le m, \quad (10)$$

where $\mathrm{wt}(\omega)$ is the Hamming weight of ω, that is, the number of nonzero components.

If f is also balanced, then it is called m-resilient.

Definition 4 (annihilator and algebraic immunity). Given $f \in \mathbb{B}_n$, we define

$$\mathrm{AN}(f) = \{ g \in \mathbb{B}_n \mid f \cdot g = 0 \}, \quad (11)$$

where $\cdot$ is the multiplication on F_2. Any $g \in \mathrm{AN}(f)$ is called an annihilator of f.

The algebraic immunity of f, denoted by $\mathrm{AI}(f)$, is defined as the minimum degree of nonzero annihilators of f or $f + 1$; that is,

$$\mathrm{AI}(f) = \min \{ \deg(g) \mid 0 \neq g \in \mathrm{AN}(f) \cup \mathrm{AN}(f+1) \}. \quad (12)$$

It is known [10] that $\mathrm{AI}(f) \le \lceil n/2 \rceil$, for any $f \in \mathbb{B}_n$. If $\mathrm{AI}(f) = \lceil n/2 \rceil$, then we say the n-variable Boolean function f has optimal algebraic immunity.

At Crypto 2003, Courtois [17] proposed fast algebraic attacks (FAAs). The key idea is to decrease the degree of the equations (a multivariate polynomial system of equations over a finite field) using a precomputation algorithm. More formally, if there exists n-variable Boolean function g of low degree such that $\deg(f \cdot g)$ is somewhat not large, then one can perform fast algebraic attack on f with much confidence. To measure the resistance against fast algebraic attack, Liu et al. introduced fast algebraic immunity (FAI), which is considered as an important cryptographic property for Boolean functions used in stream ciphers:

$$\mathrm{FAI}(f) = \min \{ 2\,\mathrm{AI}(f), \deg(g) + \deg(f \cdot g) \}, \quad (13)$$

where $1 \le \deg(g) < \mathrm{AI}(f)$.

It is folklore that $\mathrm{FAI}(f) \le n$ [10, 25].

Almost all the symmetric Boolean functions including the functions with good algebraic immunity behave badly against FAAs [18, 25]. However, Carlet-Feng function, a class of n-variable balanced Boolean functions with the maximum algebraic immunity as well as good nonlinearity [9], was proved to have almost optimal resistance and even optimal resistance against FAAs if $n = 2^s + 1$ exactly with positive integer s [20]. Another class of even n-variable balanced Boolean functions with the maximum algebraic immunity and large nonlinearity, called Tang-Carlet function [26], was also proved to have almost optimal resistance [27]. Moreover, the immunity of some rotation symmetric Boolean functions against FAAs was also analyzed [18, 28].

The following definition provides the functionalities of both algebraic immunity and fast algebraic immunity.

Definition 5 ((almost) perfect algebraic immunity). Let f be an n-variable Boolean function. The function f is said to be perfect algebraic immune (PAI) if, for any positive integers $e < \lceil n/2 \rceil$, the product $f \cdot g$ has degree at least $n - e$ for any nonzero function g ($g \in \mathbb{B}_n$) of degree at most e.

The function f is said to be almost perfect algebraic immune if, for any positive integers $e < \lceil n/2 \rceil$, the product $f \cdot g$ has degree at least $n - e - 1$ for any nonzero function g ($g \in \mathbb{B}_n$) of degree at most e.

3. The Proposed Construction

Resilient functions (see Definition 3) are a special class of Boolean functions and find many interesting applications in stream ciphers. In [8], Maitra and Sakar discussed the various methods of creation of resilient functions, and functions constructed by these methods constitute a subset of a larger set of all resilient functions.

Pan et al. [19] presented a construction for a class of 1-resilient Boolean functions with optimal algebraic immunity on an even number of variables by dividing them into two correlation classes. More precisely, Pan et al. proposed a secondary construction (i.e., Siegenthaler's [6] construction) by concatenating two balanced Boolean functions f, g with odd variables n, where $\deg(f) = n-1$, $\mathrm{AI}(f) = (n+1)/2$. They can prove the existence of a nontrivial pair (f, g) applied in the construction. But they can only construct a part of 1-resilient Boolean functions with optimal algebraic immunity by using these pairs. Pan et al. generalized the construction to a larger class of functions with suboptimal algebraic immunity on any number (>2) of variables. However, the cryptographic properties of the resulting functions are highly related to those of the initial functions they chose as building block, and in particular, this does not rule out the possibility that these functions are vulnerable to fast algebraic attack; that is, one would not expect strong resistance against fast algebraic attack in the resulting Boolean functions. More details on the rationale of their constructions can be found in [19] where two constructions are presented and security properties are analyzed mathematically step by step. In Section 6, we also compare the properties of fast algebraic immunity between our construction and the proposal of Pan et al. [19].

This section will present our construction followed by cryptographic property analysis in the next sections.

Throughout the rest of the paper, let k, s, u, v, m be positive integers, $n = 2k$, $k \geq 3$, $0 \leq s \leq 2^k - 2$, and $2^{k-1} - 1 \leq m \leq 2^k - 2$. Let α be a primitive element of finite field F_{2^k}, and $\beta = \alpha^{(u+v)^{-1}} \in F_{2^k}$.

Set

$$\begin{aligned} &Z_{2^k-1} \triangleq \left\{0, 1, \ldots, 2^k - 1\right\}, \\ &\Delta_{m,s} \triangleq \left\{s, s+1, \ldots, 2^{k-1} + s - 2\right\} \cup \{m + s\}, \\ &P \triangleq \left\{(u, v) \mid \gcd\left((u+v)u, 2^k - 1\right) = 1,\ 0 < u, v < 2^k - 1\right\}. \end{aligned} \tag{14}$$

For any $(u, v) \in P$, define n-variable Boolean function f whose support $\mathrm{supp}(f)$ consists of the following four sets:

$$\begin{aligned} &\bigcup_{i=s}^{2^{k-1}+s-2} \left\{(x, y) \mid x = \alpha^i y^{-1},\ y \in F_{2^k}^*\right\}, \\ &\left\{\left(\beta^{ui}, \beta^{vi}\right) \mid i \in Z_{2^k-1} \setminus \Delta_{m,s}\right\}, \\ &\left\{\left(\beta^{ui}, 0\right) \mid i \in \Delta_{m,s}\right\}, \\ &\left\{\left(0, \beta^{vi}\right) \mid i \in \Delta_{m,s}\right\}. \end{aligned} \tag{15}$$

In the coming sections, we will discuss its cryptographic properties: resiliency, algebraic immunity, and fast algebraic immunity. In particular, we will show that the functions derived from our construction are 1-resilient and with almost perfect algebraic immunity.

4. Resiliency of the Proposed Construction

Nonlinear Boolean functions are generally used in symmetry cryptography. It is not surprising that the functions should have sufficiently simple scheme implementation in hardware. Besides, they must satisfy certain criteria to resist different attacks (e.g., correlation attacks suggested by Siegenthaler [29] and different types of linear attacks). One of the important factors is good correlation immunity (of order m); namely, the output should be statistically independent of combination of any m its inputs. And 1-resiliency specifies a balanced correlation-immune of order 1 Boolean function.

Theorem 6. *Suppose that f is a Boolean function derived from our construction. Then we have that f is 1-resilient.*

Proof. According to the definition of resiliency (see Definition 3), we first show that the function derived from our construction is balanced.

In fact, we have that

$$\begin{aligned} \mathrm{wt}(f) = &\left(2^{k-1} - 1\right)\left(2^k - 1\right) + \left|Z_{2^k-1} \setminus \Delta_{m,s}\right| \\ &+ 2\left|\Delta_{m,s}\right| = 2^{2k-1}; \end{aligned} \tag{16}$$

thus, the function f is balanced as expected.

Set $\Omega = F_{2^k} \times F_{2^k}$. We know that

$$\sum_{(x,y)\in\Omega} (-1)^{\mathrm{Tr}_1^k(ax+by)} = 0; \tag{17}$$

then, for any $(a, b) \in \Omega \setminus \{(0, 0)\}$, it holds that

$$\begin{aligned} W_f(a, b) &= \sum_{(x,y)\in\Omega} (-1)^{f(x,y)+\mathrm{Tr}_1^k(ax+by)} \\ &= \sum_{(x,y)\in\Omega\setminus\mathrm{supp}(f)} (-1)^{\mathrm{Tr}_1^k(ax+by)} \\ &\quad - \sum_{(x,y)\in\mathrm{supp}(f)} (-1)^{\mathrm{Tr}_1^k(ax+by)} \\ &= -2 \sum_{(x,y)\in\mathrm{supp}(f)} (-1)^{\mathrm{Tr}_1^k(ax+by)}. \end{aligned} \tag{18}$$

Plugging the four sets of $\mathrm{supp}(f)$ into $\sum_{(x,y)\in\mathrm{supp}(f)} (-1)^{\mathrm{Tr}_1^k(ax+by)}$, we have that

$$\begin{aligned} &\sum_{(x,y)\in\mathrm{supp}(f)} (-1)^{\mathrm{Tr}_1^k(ax+by)} \\ &= \sum_{i=s}^{2^{k-1}+s-2} \sum_{y\in F_{2^k}^*} (-1)^{\mathrm{Tr}_1^k(a\alpha^i y^{-1}+by)} + \sum_{i\in\Delta_{m,s}} (-1)^{\mathrm{Tr}_1^k(a\beta^{ui})} \\ &\quad + \sum_{i\in Z_{2^k-1}\setminus\Delta_{m,s}} (-1)^{\mathrm{Tr}_1^k(a\beta^{ui}+b\beta^{vi})} \\ &\quad + \sum_{i\in\Delta_{m,s}} (-1)^{\mathrm{Tr}_1^k(b\beta^{vi})}. \end{aligned} \tag{19}$$

Now we consider the following two cases.

Case 1 ($a \neq 0$ *and* $b = 0$). We have

$$\begin{aligned}&\sum_{(x,y)\in \mathrm{supp}(f)} (-1)^{\mathrm{Tr}_1^k(ax+by)}\\ &= \left(2^{k-1}-1\right)(-1) + \left|\Delta_{m,s}\right| \\ &\quad + \sum_{i\in Z_{2^{k-1}}\setminus\Delta_{m,s}} (-1)^{\mathrm{Tr}_1^k(a\beta^{ui})} + \sum_{i\in\Delta_{m,s}} (-1)^{\mathrm{Tr}_1^k(a\beta^{ui})}\\ &= 0.\end{aligned} \tag{20}$$

Case 2 ($a = 0$ *and* $b \neq 0$). We have

$$\begin{aligned}&\sum_{(x,y)\in \mathrm{supp}(f)} (-1)^{\mathrm{Tr}_1^k(ax+by)}\\ &= \left(2^{k-1}-1\right)(-1) + \left|\Delta_{m,s}\right| + \sum_{i\in Z_{2^{k-1}}\setminus\Delta_{m,s}} (-1)^{\mathrm{Tr}_1^k(b\beta^{vi})}\\ &\quad + \sum_{i\in\Delta_{m,s}} (-1)^{\mathrm{Tr}_1^k(b\beta^{vi})} = 0.\end{aligned} \tag{21}$$

Therefore, we can conclude that $W_f(a,b) = 0$, for any $(a,b) \in \Omega \setminus \{(0,0)\}$ and $ab = 0$. According to Definition 3, we know that f is 1-resilient. □

5. Algebraic Immunity of the Proposed Construction

Algebraic attacks have become a powerful tool that can be used for almost all types of cryptographic systems. Algebraic immunity defined for a Boolean function measures the resistance of the function against algebraic attacks. The properties and constructions of Boolean functions with high algebraic immunity are concerned in extensive work, for example, [9, 12–16].

In this section, we will analyze the algebraic immunity of the proposed construction. First we have the following lemma.

Lemma 7 (see [30, 31]). *Suppose the integer* $k \geq 3$*; it holds that*

(1) for any $0 \leq t \leq 2^k - 2$ *we have*

$$\begin{aligned}&\#\left\{(i,j) \mid 0 \leq i, j \leq 2^k-2,\ i-j \right.\\ &\qquad \left. \equiv t \left(\mathrm{mod}\ 2^k-1\right),\ \mathrm{wt}(i)+\mathrm{wt}(j) \leq k-1\right\} \leq 2^{k-1};\end{aligned} \tag{22}$$

(2) for any $1 \leq t \leq 2^k - 2$ *we have*

$$\begin{aligned}&\#\left\{(i,j) \mid 0 \leq i, j \leq 2^k-2,\ i-j \right.\\ &\qquad \left. \equiv t \left(\mathrm{mod}\ 2^k-1\right),\ \mathrm{wt}(i)+\mathrm{wt}(j) \leq k-1\right\} \leq 2^{k-1}\\ &\qquad -1.\end{aligned} \tag{23}$$

Theorem 8. *Let the Boolean function* f *be derived from the proposed construction. We have*

(1) $\mathrm{AI}(f) \geq k-1$*;*

(2) $\mathrm{AI}(f) = k$ *(i.e.,* f *has optimal algebraic immunity) if* $m + s = 2^{k-1} - 1$ *or* $0 \pmod{2^k-1}$.

Proof. Let h be an annihilator of f such that $f \cdot h = 0, \deg(h) < k$. Suppose that

$$h(x,y) = \sum_{i=0}^{2^k-2}\sum_{j=0}^{2^k-2} h_{i,j} x^i y^j. \tag{24}$$

For any $(x,y) \in \mathrm{supp}(f)$, we have $h(x,y) = 0$ and

$$\bigcup_{i=s}^{2^{k-1}+s-2} \left\{(x,y) \mid x = \alpha^i y^{-1},\ y \in F_{2^k}^*\right\} \subset \mathrm{supp}(f). \tag{25}$$

Then, for any $s \leq l \leq 2^{k-1} + s - 2$, $0 \leq s \leq 2^k - 2$, and $y \in F_{2^k}^*$, it holds that

$$0 = h\left(\alpha^l y^{-1}, y\right) = \sum_{i=0}^{2^k-2}\sum_{j=0}^{2^k-2} h_{i,j}\alpha^{li} y^{j-i} = \sum_{t=0}^{2^k-2} h_t(\alpha)\, y^t, \tag{26}$$

where

$$\begin{aligned}h_t(\alpha) &= \sum_{0\leq i,j\leq 2^k-2, i-j\equiv t(\mathrm{mod}\ 2^k-1)} h_{i,j}\alpha^{li},\\ &\qquad 0 \leq t \leq 2^k-2.\end{aligned} \tag{27}$$

Suppose that y travels in $F_{2^k}^*$. Then the coefficients y^t in (26) will make up a coefficient matrix which is Vandermonde-like. From the invertibility property of Vandermonde matrix, we know that

$$\sum_{0\leq i,j\leq 2^k-2, i-j\equiv t(\mathrm{mod}\ 2^k-1)} h_{i,j}\alpha^{li} = 0 \tag{28}$$

for any $0 \leq t \leq 2^k - 2$ and $s \leq l \leq 2^k + s - 2$.

Now we consider the following two cases.

Case 1 ($1 \leq t \leq 2^k - 2$). From Lemma 7, we know that the number of different $h_{i,j}$ in (28) is no more than $2^{k-1} - 1$. Thus we can further assume these $h_{i,j}$ are $\{h_{i_1,j_1}, h_{i_2,j_2}, \ldots, h_{i_{2^{k-1}-1},j_{2^{k-1}-1}}\}$.

Set

$$\begin{aligned}H &\triangleq \left(h_{i_1,j_1}, h_{i_2,j_2}, \ldots, h_{i_{2^{k-1}-1},j_{2^{k-1}-1}}\right)^T,\\ M &\triangleq \begin{pmatrix} \left(\alpha^{i_1}\right)^s & \left(\alpha^{i_2}\right)^s & \cdots & \left(\alpha^{i_{2^{k-1}-1}}\right)^s \\ \left(\alpha^{i_1}\right)^{s+1} & \left(\alpha^{i_2}\right)^{s+1} & \cdots & \left(\alpha^{i_{2^{k-1}-1}}\right)^{s+1} \\ \vdots & \vdots & \ddots & \vdots \\ \left(\alpha^{i_1}\right)^{2^{k-1}+s-2} & \left(\alpha^{i_2}\right)^{2^{k-1}+s-2} & \cdots & \left(\alpha^{i_{2^{k-1}-1}}\right)^{2^{k-1}+s-2} \end{pmatrix};\end{aligned} \tag{29}$$

then, we have

$$M \cdot H = 0. \tag{30}$$

Now, the invertibility property of Vandermonde matrix tells that

$$H = 0. \tag{31}$$

Namely, for any $0 \le i, j \le 2^k - 2$, and $1 \le t \le 2^k - 2$, we have

$$h_{i,j} = 0 \quad \text{if } i - j \equiv t \left(\bmod 2^k - 1\right). \tag{32}$$

Therefore, for any $1 \le j \le 2^k - 2$, it holds that

$$h_{0,j} = 0. \tag{33}$$

As $(0, 1) \in \text{supp}(f)$, we have

$$h(0,1) = 0 = \sum_{j=0}^{2^k-2} h_{0,j}; \tag{34}$$

thus $h_{0,0} = 0$ follows.

Case 2 ($t = 0$, *i.e.*, $i = j$). From Lemma 7, we know that the number of different $h_{i,j}$ in (28) is no more than $2^{k-1} - 1$. Thus, for any $1 \le i \le 2^k - 2$, we have

$$h_{i,i} = 0. \tag{35}$$

Putting all together, we know that

$$h \equiv 0; \tag{36}$$

namely, there is not any annihilator of degree lower than k.

Next we consider $f + 1$. Its support $\text{supp}(f + 1)$ consists of the following sets:

(i) $\bigcup_{i=2^{k-1}+s-1}^{2^{k-1}+s-2} \{(x, y) \mid x = \alpha^i y^{-1},\ y \in F_{2^k}^* \setminus \{\beta^{vi}\}\}$

(ii) $\{(\beta^{ui}, 0) \mid i \in Z_{2^k-1} \setminus \Delta_{m,s}\}$

(iii) $\{(0, \beta^{vi}) \mid i \in Z_{2^k-1} \setminus \Delta_{m,s}\}$

(iv) $\{(0, 0), (\beta^{u(m+s)}, \beta^{v(m+s)})\}$.

Assume that h is an annihilator of $f + 1$, $\deg(h) < k$.

Without loss of generality, set

$$h(x, y) = \sum_{i=0}^{2^k-2} \sum_{j=0}^{2^k-2} h_{i,j} x^i y^j. \tag{37}$$

Denote

$$\begin{aligned} h^{(1)} &\triangleq \sum_{i=0}^{2^k-3} \sum_{j=0}^{2^k-3} h_{i,j} x^i y^j \\ h^{(2)} &\triangleq \sum_{i=0}^{2^k-2} h_{i,2^k-2} x^i y^{2^k-2} \\ h^{(3)} &\triangleq \sum_{j=0}^{2^k-2} h_{2^k-2,j} x^{2^k-2} y^j; \end{aligned} \tag{38}$$

then

$$h(x, y) = h^{(1)} + h^{(2)} + h^{(3)}. \tag{39}$$

For any $(x, y) \in \text{supp}(f + 1)$, we have

$$\begin{aligned} &h(x, y) = 0, \\ &\bigcup_{i=2^{k-1}+s-1}^{2^k+s-2} \left\{(x, y) \mid x = \alpha^i y^{-1},\ y \in F_{2^k}^* \setminus \left\{\beta^{vi}\right\}\right\} \\ &\quad \subset \text{supp}(f + 1). \end{aligned} \tag{40}$$

Then, for any $2^{k-1} + s - 1 \le l \le 2^k + s - 2$ and $y \in F_{2^k}^* \setminus \{\beta^v\}$, it holds that

$$0 = h^{(1)}\left(\alpha^l y^{-1}, y\right) = \sum_{t=0}^{2^k-3} h_t(\alpha) y^t, \tag{41}$$

where

$$h_t(\alpha) = \sum_{0 \le i,j \le 2^k-3, i-j \equiv t (\bmod 2^k-1)} h_{i,j} \alpha^{li}, \quad 0 \le t \le 2^k - 3. \tag{42}$$

Suppose that y travels in $F_{2^k}^* \setminus \{\beta^v\}$. Then the coefficients y^t in (41) will make up a coefficient matrix which is Vandermonde-like. Similarly, Lemma 7 will lead to the fact that

$$h^{(1)} = 0, \tag{43}$$

and $\text{AI}(f) \ge k - 1$ follows.

If $m + s = 2^{k-1} - 1$ or $0 \pmod{2^k - 1}$, then (note that $\deg(h^{(2)}) < k$)

$$h^{(2)} = h_{0,2^k-2} y^{2^k-2}. \tag{44}$$

On the other hand, we have

$$\left\{\left(0, \beta^{vi}\right) \mid i \in Z_{2^k-1} \setminus \Delta_{m,s}\right\} \subset \text{supp}(f + 1). \tag{45}$$

Thus for any $i \in Z_{2^k-1} \setminus \Delta_{m,s}$,

$$h^{(2)}\left(0, \beta^{vi}\right) = 0; \tag{46}$$

therefore

$$h_{0,2^k-2} = 0. \tag{47}$$

Similarly, we have

$$h_{2^k-2,0} = 0. \tag{48}$$

In a nutshell, one can conclude that $\text{AI}(f) = k$ (i.e., f has optimal algebraic immunity) if $m + s = 2^{k-1} - 1$ or $0 \pmod{2^k - 1}$. And this completes the proof. □

6. Fast Algebraic Immunity of the Proposed Construction

Algebraic attacks are based on the establishment and processing of an overdefined system of nonlinear equations involving the secret key and the keystream sequence. The system can be practically solved, and thus the secret key is compromised, only if the equations are of low degree. Courtois and Meier demonstrated that a successful algebraic attack exists when the Boolean function f (or its complement $f+1$) has a low degree annihilator (a nonzero Boolean function g, such that $fg=0$). At crypto 2003, Courtois [17] further generalized the standard algebraic attack to an improved version, fast algebraic attack (see also [32]), by presenting a method that allows substantially reducing the complexity of the attack. Several stream ciphers appeared to be vulnerable to the FAA, such as Toyocrypt, LILI-128, and the keystream generator that is used in E0 cipher. Fast algebraic attacks are considered to be more difficult to study than the standard algebraic attack, and thus a design with good immunity against FAA is expected.

Definition 9 (Carlet-Feng function [9]). Let f be an n-variable Boolean function, α be a primitive element in F_{2^n}, and s be an integer, $0 \le s \le 2^n - 2$. Denote

$$\Delta_s \triangleq \left\{\alpha^s, \alpha^{s+1}, \ldots, \alpha^{s+2^{n-1}-2}\right\}. \tag{49}$$

We call f a Carlet-Feng function if $\mathrm{supp}(f) = \Delta_s$.

Theorem 10 (see [9]). *Carlet-Feng function f derived from Definition 9 has a good behavior against fast algebraic attacks.*

In particular, Carlet and Feng checked that no nonzero function g of degree at most e and no function h of degree at most d exist such that $f \cdot g = h$, when $(e,d) = (1, n-2)$ for n odd and $(e,d) = (1, n-3)$ for n even.

This has been checked for $n \le 12$ and also conjectured for every n; for $e > 1$, pairs (g,h) of degrees (e,d) such that $e + d < n - 1$ were never observed; precisely, the nonexistence of such pairs could be checked exhaustively for $n \le 9$ and $e < n/2$, for $n = 10$ and $e \le 3$, and for $n = 11$ and $e \le 2$.

This suggests that this class of functions, even if not always optimal against fast algebraic attacks, has a very good behavior.

Pan et al. presented [19] a construction for a class of 1-resilient Boolean functions with optimal algebraic immunity on an even number of variables by dividing them into two correlation classes, that is, equivalence classes. The coming result states the construction.

Theorem 11 (see [19]). *Let n be any odd integer ($n \ge 3$), f be a balanced Boolean function with maximum degree $n-1$ and optimal algebraic immunity $(n+1)/2$, and g be an annihilator of f. Then the following is 1-resilient Boolean function with optimal algebraic immunity:*

$$h = f \parallel g = (1 + x_{n+1}) f + x_{n+1} g \in F_2^{n+1}. \tag{50}$$

Table 1: Fast algebraic immunities of three classes of functions.

n	Carlet-Feng Functions [9]	Functions by [19]	The Proposed construction
6	5	5	5
8	6	6	7
10	9	9	9
12	10	10	11
14	13	12	13
16	15	14	15

Let $f \in \mathbb{B}_n$. There exist $g, h \in \mathbb{B}_n$ such that $f \cdot g = h$. Assume that $d \triangleq \deg(h)$ and $e \triangleq \deg(g)$. Following the notion of fast algebraic immunity, one may just multiply f (over F_2) by g of degree e, $1 \le e < n/2$, and get $e + d$ by enumerating all possible (e,d).

Comparatively, one can take two odd-variable Carlet-Feng functions as initial functions and construct a class of 1-resilient functions on even variables by the method proposed in [19].

Thus we can determine the appropriate values of (e,d) for the three classes of Boolean functions, the first two by Carlet-Feng method [9] and the method in [19], respectively, and the last one from the method proposed in Section 3. Implemented via Maple language, Table 1 presents the minimal values of (e,d) for the functions on even variables (from 6 to 16). In the table, the last column takes $(s,m,u,v) = (0, 2^{k-1}, 1, 2^{k-1} - 1)$.

One can check that when $n = 8$, 12, 14, and 16, the minimal values of (e,d) by the proposed method are closer to the bounds (i.e., n) than those in [19]. In fact, when $n = 8$ and 12, the results by our method are even better than those by Carlet-Feng functions [9], which makes the resistance against fast algebraic attack emerge stronger.

Moreover, one can find that, for all the (e,d) of the last column, we have $e + d \ge n - 1$. Combining this with the results in the previous section, we may expect that the functions constructed by the proposed method are almost perfect algebraic immune.

7. Conclusion

Based on bivariate representation over finite field, the paper constructed a class of 1-resilient Boolean functions on even variables with almost perfect algebraic immunity. The resulting construction can resist algebraic attack and fast algebraic attack almost perfectly along with corresponding immunity against correlation attack.

We mention that it is expected for the cryptographic community to construct Boolean function with as much cryptographic properties as possible. A natural but interesting question is how to extend the proposed construction to other important cryptographic properties such as algebraic degree and nonlinearity. We leave it as a future work.

Notations

f, g, h: Boolean functions from F_2^n to F_2
$\mathbb{B}_n$: The set of n-variable Boolean functions on F_2^n
$\mathrm{supp}(f)$: Support of f
$\mathrm{wt}(f)$: Hamming weight of f
$d_H(f, g)$: Hamming distance between f and g
$\deg(f)$: Algebraic degree of f
$W_f(a, b)$: Walsh spectrum of f at (a, b)
Tr_1^n: Trace function $\mathrm{Tr}_1^n : F_{2^n} \to F_2$
$\mathrm{AI}(f)$: Algebraic immunity of f
$\mathrm{FAI}(f)$: Fast algebraic immunity of f
$\gcd(a, b)$: The greatest common divisor of two positive integers a and b
F_2^n: The vector space of dimension n over the finite field F_2
F_{2^n}: Finite field of order 2^n.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (Grant nos. 61472249, 61572192, 61571191, and 61672238) and International Science & Technology Cooperation & Exchange Projects of Shaanxi Province (2016KW-038).

References

[1] C. Carlet, "Boolean functions for cryptography and error correcting codes," in *Boolean Methods And Models in Mathematics, Computer Science, And Engineering*, Y. Crama and P. Hammer, Eds., pp. 257–397, Cambridge University Press, Cambridge, UK, 2010.

[2] C. Carlet, D. K. Dalai, K. C. Gupta, and S. Maitra, "Algebraic immunity for cryptographically significant boolean functions: analysis and construction," *Institute of Electrical and Electronics Engineers. Transactions on Information Theory*, vol. 52, no. 7, pp. 3105–3121, 2006.

[3] N. T. Courtois and W. Meier, "Algebraic attacks on stream ciphers with linear feedback," in *Advances in cryptology—EUROCRYPT 2003*, vol. 2656 of *Lecture Notes in Comput. Sci.*, pp. 345–359, Springer, Berlin, 2003.

[4] T. W. Cusick and P. Stanica, *Cryptographic Boolean functions and applications*, Academic Press, San Diego, CA, USA, 2009.

[5] T. Siegenthaler, "Correlation-immunity of nonlinear combining functions for cryptographic applications," *Institute of Electrical and Electronics Engineers. Transactions on Information Theory*, vol. 30, no. 5, pp. 776–780, 1984.

[6] A. Canteaut and M. Trabbia, "Improved fast correlation attacks using parity-check equations of weight 4 and 5," in *Eurocrypt 2000, LNCS 1807*, vol. 1807, pp. 573–588, Springer-Verlag, 2000.

[7] G. Z. Xiao and J. L. Massey, "A spectral characterization of correlation-immune combining functions," *Institute of Electrical and Electronics Engineers. Transactions on Information Theory*, vol. 34, no. 3, pp. 569–571, 1988.

[8] S. Maitra and P. Sarkar, "Highly nonlinear resilient functions optimizing Siegenthaler's inequality," in *Advances in cryptology—CRYPTO '99 (SANta Barbara, CA)*, vol. 1666 of *Lecture Notes in Comput. Sci.*, pp. 198–215, Springer, Berlin, 1999.

[9] C. Carlet and K. Feng, "An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity," in *Advances in cryptology—ASIACRYPT 2008*, vol. 5350 of *Lecture Notes in Comput. Sci.*, pp. 425–440, Springer, Berlin, 2008.

[10] N. T. Courtois and W. Meier, "Algebraic attacks on stream ciphers with linear feedback," in *Advances in cryptology—EUROCRYPT 2003*, vol. 2656, pp. 345–359, Springer, Berlin, Germany, 2003.

[11] W. Meier, E. Pasalic, and C. Carlet, "Algebraic attacks and decomposition of Boolean functions," in *Advances in Cryptology—EUROCRYPT 2004*, vol. 3027, pp. 474–491, Springer, Berlin, Germany, 2004.

[12] D. K. Dalai, S. Maitra, and S. Sarkar, "Basic theory in construction of boolean functions with maximum possible annihilator immunity," *Designs, Codes and Cryptography*, vol. 40, no. 1, pp. 41–58, 2006.

[13] N. Li, L. Qu, W.-F. Qi, G. Feng, C. Li, and D. Xie, "On the construction of Boolean functions with optimal algebraic immunity," *IEEE Transactions on Information Theory*, vol. 54, no. 3, pp. 1330–1334, 2008.

[14] N. Li and W.-F. Qi, "Construction and analysis of Boolean functions of 2t + 1 variables with maximum algebraic immunity," in *Advances in cryptology—ASIACRYPT 2006*, vol. 4284, pp. 84–98, Springer, Berlin, Heidelberg, 2006.

[15] Z. Tu and Y. Deng, "A conjecture about binary strings and its applications on constructing Boolean functions with optimal algebraic immunity," *Designs, Codes and Cryptography. An International Journal*, vol. 60, no. 1, pp. 1–14, 2011.

[16] X. Zeng, C. Carlet, J. Shan, and L. Hu, "More balanced Boolean functions with optimal algebraic immunity and good nonlinearity and resistance to fast algebraic attacks," *Institute of Electrical and Electronics Engineers. Transactions on Information Theory*, vol. 57, no. 9, pp. 6310–6320, 2011.

[17] N. T. Courtois, "Fast algebraic attacks on stream ciphers with linear feedback," in *Advances in cryptology—CRYPTO 2003*, vol. 2729 of *Lecture Notes in Comput. Sci.*, pp. 176–194, Springer, Berlin, Germany, 2003.

[18] X. Li, Q. Zhou, H. Qian, Y. Yu, and S. Tang, "Balanced 2p-variable rotation symmetric Boolean functions with optimal algebraic immunity, good nonlinearity, and good algebraic degree," *Journal of Mathematical Analysis and Applications*, vol. 403, no. 1, pp. 63–71, 2013.

[19] S.-S. Pan, X.-T. Fu, and W.-G. Zhang, "Construction of 1-resilient Boolean functions with optimal algebraic immunity and good nonlinearity," *Journal of Computer Science and Technology*, vol. 26, no. 2, pp. 269–275, 2011.

[20] M. Liu, Y. Zhang, and D. Lin, "Perfect algebraic immune functions," in *Advances in cryptology—ASIACRYPT 2012*, vol. 7658 of *Lecture Notes in Comput. Sci.*, pp. 172–189, Springer, Heidelberg, 2012.

[21] P. Camion and A. Canteaut, "Correlation-immune and resilient functions over a finite alphabet and their applications in cryptography," *Designs, Codes and Cryptography*, vol. 16, no. 2, pp. 121–149, 1999.

[22] J. Seberry, X.-M. Zhang, and Y. Zheng, "On constructions and nonlinearity of correlation immune functions (extended abstract)," in *Eurocrypt 1993, LNCS 765*, pp. 181–199, 1994.

[23] M. Hermelin and K. Nyberg, "Correlation Properties of the Bluetooth Combiner," in *Information Security and Cryptology - ICISC'99*, vol. 1787, pp. 17–29, Springer Berlin Heidelberg, Berlin, Heidelberg, 2000.

[24] P. Camion, C. Carlet, P. Charpin, and N. Sendrier, "On correlation-immune functions," in *Advances in cryptology—CRYPTO '91*, vol. 576 of *Lecture Notes in Comput. Sci.*, pp. 86–100, Springer, Berlin, Santa Barbara, CA, USA, 1992.

[25] M. Liu, D. Lin, and D. Pei, "Fast algebraic attacks and decomposition of symmetric Boolean functions," *Institute of Electrical and Electronics Engineers. Transactions on Information Theory*, vol. 57, no. 7, pp. 4817–4821, 2011.

[26] D. Tang, C. Carlet, and X. Tang, "Highly nonlinear Boolean functions with optimal algebraic immunity and good behavior against fast algebraic attacks," *Institute of Electrical and Electronics Engineers. Transactions on Information Theory*, vol. 59, no. 1, pp. 653–664, 2013.

[27] M. Liu and D. Lin, "Almost perfect algebraic immune functions with good nonlinearity," in *Proceedings of the 2014 IEEE International Symposium on Information Theory, ISIT 2014*, pp. 1837–1841, usa, July 2014.

[28] Y. Zhang, M. Liu, and D. Lin, "On the immunity of rotation symmetric Boolean functions against fast algebraic attacks," *Discrete Applied Mathematics. The Journal of Combinatorial Algorithms, Informatics and Computational Sciences*, vol. 162, pp. 17–27, 2014.

[29] T. Siegenthaler, "Decrypting a Class of Stream Ciphers Using Ciphertext Only," *IEEE Transactions on Computers*, vol. C-34, no. 1, pp. 81–85, 1985.

[30] G. Cohen and J. P. Flori, "On a generalized combinatorial conjecture involving addition mod 2k," Tech. Rep. 1., 2011.

[31] Y. Du, F. Zhang, and M. Liu, "On the resistance of Boolean functions against fast algebraic attacks," in *Information security and cryptology—ICISC 2011*, vol. 7259 of *Lecture Notes in Comput. Sci.*, pp. 261–274, Springer, Heidelberg, 2012.

[32] P. Hawkes and G. G. Rose, "Rewriting variables: the complexity of fast algebraic attacks on stream ciphers," in *Advances in cryptology—CRYPTO 2004*, vol. 3152, pp. 390–406, Springer, Berlin, 2004.