Perfect Algebraic Immune Functions *

Meicheng Liu, Yin Zhang, and Dongdai Lin

SKLOIS, Institute of Information Engineering, CAS, Beijing 100195, P. R. China
meicheng.liu@gmail.com, zhangy@is.iscas.ac.cn, ddlin@iie.ac.cn

Abstract. A perfect algebraic immune function is a Boolean function with perfect immunity against algebraic and fast algebraic attacks. The main results are that for a perfect algebraic immune balanced function the number of input variables is one more than a power of two; for a perfect algebraic immune unbalanced function the number of input variables is a power of two. Also, for n equal to a power of two, the Carlet-Feng functions on $n+1$ variables and the modified Carlet-Feng functions on n variables are shown to be perfect algebraic immune functions.

Keywords: Boolean functions, Algebraic immunity, Fast algebraic attacks

1 Introduction

The study of the cryptanalysis of the filter and combination generators of stream ciphers based on linear feedback shift registers (LFSRs) has resulted in a wealth of cryptographic criteria for Boolean functions, such as balancedness, high algebraic degree, high nonlinearity, high correlation immunity and so on. An overview of cryptographic criteria for Boolean functions with extensive bibliography is given in [3].

In recent years, algebraic and fast algebraic attacks [1,5,6] have been regarded as the most successful attacks on LFSR-based stream ciphers. These attacks cleverly use overdefined systems of multivariable nonlinear equations to recover the secret key. Algebraic attacks make use of the equations by multiplying a nonzero function of low degree, while fast algebraic attacks make use of the equations by linear combination.

Thus the algebraic immunity ($\mathcal{AI}$), the minimum algebraic degree of nonzero annihilators of f or $f+1$, was introduced by W. Meier et al. [20] to measure the ability of Boolean functions to resist algebraic attacks. It was shown by N. Courtois and W. Meier [5] that maximum $\mathcal{AI}$ of n-variable Boolean functions is $\lceil \frac{n}{2} \rceil$. The properties and constructions of Boolean functions with maximum $\mathcal{AI}$ were researched in a large number of papers, e.g., [8,15,16,18,4,24,25].

* Supported by the National 973 Program of China under Grant 2011CB302400, the National Natural Science Foundation of China under Grants 10971246, 60970152, and 61173134, the Strategic Priority Research Program of the Chinese Academy of Sciences under Grant XDA06010701, and the CAS Special Grant for Postgraduate Research, Innovation and Practice.

The resistance against fast algebraic attacks is not covered by algebraic immunity [7,2,17]. At Eurocrypt 2006, F. Armknecht et al. [2] introduced an effective algorithm for determining the immunity against fast algebraic attacks, and showed that a class of symmetric Boolean functions (the majority functions) have poor resistance against fast algebraic attacks despite their resistance against algebraic attacks. Later M. Liu et al. [17] stated that almost all the symmetric functions including these functions with good algebraic immunity behave badly against fast algebraic attacks. In [22] P. Rizomiliotis introduced a method to evaluate the behavior of Boolean functions against fast algebraic attacks using univariate polynomial representation. However, it is unclear what is maximum immunity to fast algebraic attacks.

A preprocessing of fast algebraic attacks on LFSR-based stream ciphers, which use a Boolean function $f : GF(2)^n \to GF(2)$ as the filter or combination generator, is to find a nonzero function g of small algebraic degree such that the multiple gf has algebraic degree not too large [6]. N. Courtois [6] proved that for any pair of positive integers (e, d) such that $e+d \geq n$, there is a nonzero function g of degree at most e such that gf has degree at most d. This result reveals an upper bound on maximum immunity to fast algebraic attacks. It implies that the function f has maximum possible resistance against fast algebraic attacks, if for any pair of positive integers (e, d) such that $e + d < n$ and $e < n/2$, there is no nonzero function g of degree at most e such that gf has degree at most d. Such functions are said to be perfect algebraic immune ($\mathcal{PAI}$). Note that one can use the fast general attack [6, Theorem 7.1.1] by splitting the function into two $f = h + l$ with l being the linear part of f. In this case, $h = f + l$ rather than $h = gf$ is used, then e equals 1, i.e., the degree of the linear function l, and d equals the degree of the function h, i.e., the degree of f. Thus $\mathcal{PAI}$ functions have algebraic degree at least $n - 1$.

A $\mathcal{PAI}$ function also achieves maximum $\mathcal{AI}$. As a consequence, a $\mathcal{PAI}$ function has perfect immunity against classical and fast algebraic attacks. Although preventing classical and fast algebraic attacks is not sufficient for resisting algebraic attacks on the augmented function [12], the resistance against these attacks depends on the update function and tap positions used in a stream cipher and in actual fact it is not a property of the Boolean function. Thus the use of $\mathcal{PAI}$ functions does not guarantee that a stream cipher is not vulnerable to algebraic attacks since the attacker can also exploit suitable relations for the augmented functions as suggested in [6,12].

It is an open question whether there are $\mathcal{PAI}$ functions for arbitrary number of input variables. This problem was also noticed in [4] at Asiacrypt 2008. It seems that $\mathcal{PAI}$ functions are quite rare. In [4] C. Carlet and K. Feng observed that the Carlet-Feng functions on 9 variables are $\mathcal{PAI}$. One can check that the Carlet-Feng functions on 5 variables are also $\mathcal{PAI}$ (see also [10]). However, no function is shown to be $\mathcal{PAI}$ for arbitrary number of variables. On the contrary, M. Liu et al. [17] proved that no symmetric functions are $\mathcal{PAI}$, and in [26] the authors proved that no rotation symmetric functions are $\mathcal{PAI}$ for even number (except a power of two) of variables.

In this paper, we study the upper bounds on the immunity to fast algebraic attacks, and solve the above question. The immunity against fast algebraic attacks is related to a matrix thanks to Theorem 1 of [2]. By a simple transformation on this matrix we obtain a symmetric matrix whose elements are the coefficients of the algebraic normal form of a given Boolean function. We improve the upper bounds on the immunity to fast algebraic attacks by proving that the symmetric matrix is singular in some cases. The results are that for an n-variable function, we have: (1) if n is a power of 2 then a $\mathcal{PAI}$ function has algebraic degree n (showing that the function is unbalanced); (2) if n is one more than a power of 2 then a $\mathcal{PAI}$ function has algebraic degree $n-1$ (which is also balanced); (3) otherwise, the function is not $\mathcal{PAI}$. We then prove that the Carlet-Feng functions, which have algebraic degree $n-1$, are $\mathcal{PAI}$ for n equal to one more than a power of 2, and are almost $\mathcal{PAI}$ for the other cases. Also we prove that the modified Carlet-Feng functions, which have algebraic degree n, are $\mathcal{PAI}$ for n equal to a power of 2, and are almost $\mathcal{PAI}$ for the other cases. The results show that our bounds on the immunity to fast algebraic attacks are tight, and that the Carlet-Feng functions are optimal against fast algebraic attacks as well as classical algebraic attacks. Our results explain the experimental observations of C. Carlet and K. Feng [4] and also prove their conjecture.

The remainder of this paper is organized as follows. In Section 2 some basic concepts are provided. Section 3 presents the improved upper bounds on the immunity of Boolean functions against fast algebraic attacks while Section 4 shows that the Carlet-Feng functions and their modifications achieve these bounds. Section 5 concludes the paper.

2 Preliminary

Let $\mathbb{F}_2$ denote the binary field $GF(2)$ and $\mathbb{F}_2^n$ the n-dimensional vector space over $\mathbb{F}_2$. An n-variable Boolean function is a mapping from $\mathbb{F}_2^n$ into $\mathbb{F}_2$. Denote by $\mathbf{B}_n$ the set of all n-variable Boolean functions. An n-variable Boolean function f can be uniquely represented as its truth table, i.e., a binary string of length 2^n,

$$f = [f(0,0,\cdots,0), f(1,0,\cdots,0), \cdots, f(1,1,\cdots,1)].$$

The support of f is given by $\mathrm{supp}(f) = \{x \in \mathbb{F}_2^n \mid f(x) = 1\}$. The Hamming weight of f, denoted by $\mathrm{wt}(f)$, is the number of ones in the truth table of f. An n-variable function f is said to be balanced if its truth table contains equal number of zeros and ones, that is, $\mathrm{wt}(f) = 2^{n-1}$.

An n-variable Boolean function f can also be uniquely represented as a multivariate polynomial over $\mathbb{F}_2$,

$$f(x) = \sum_{c \in \mathbb{F}_2^n} a_c x^c,\ a_c \in \mathbb{F}_2,\ x^c = x_1^{c_1} x_2^{c_2} \cdots x_n^{c_n},\ c = (c_1, c_2, \cdots, c_n),$$

called the algebraic normal form (ANF). The algebraic degree of f, denoted by $\deg(f)$, is defined as $\max\{\mathrm{wt}(c) \mid a_c \neq 0\}$.

Let $\mathbb{F}_{2^n}$ denote the finite field $GF(2^n)$. The Boolean function f considered as a mapping from $\mathbb{F}_{2^n}$ into $\mathbb{F}_2$ can be uniquely represented as

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

where $f^2(x) \equiv f(x) (\mathrm{mod}\, x^{2^n} - x)$. Expression (1) is called the univariate polynomial representation of the function f. It is well known that $f^2(x) \equiv f(x) (\mathrm{mod}\, x^{2^n} - x)$ if and only if $a_0, a_{2^n-1} \in \mathbb{F}_2$ and for $1 \leq i \leq 2^n - 2$, $a_{2i \bmod (2^n-1)} = a_i^2$. The algebraic degree of the function f equals $\max\limits_{a_i \neq 0} \mathrm{wt}(i)$, where $i = \sum_{k=1}^{n} i_k 2^{k-1}$ is considered as $(i_1, i_2, \cdots, i_n) \in \mathbb{F}_2^n$.

Let α be a primitive element of $\mathbb{F}_{2^n}$. The a_i's of Expression (1) are given by $a_0 = f(0), a_{2^n-1} = f(0) + \sum_{j=0}^{2^n-2} f(\alpha^j)$ and

$$a_i = \sum_{j=0}^{2^n-2} f(\alpha^j)\alpha^{-ij},\ \text{for } 1 \leq i \leq 2^n - 2. \tag{2}$$

For more details with regard to the representation of Boolean functions, we refer to [3].

The algebraic immunity of Boolean functions is defined as follows. Maximum algebraic immunity of n-variable Boolean functions is $\lceil \frac{n}{2} \rceil$ [5].

Definition 1 *[20] The algebraic immunity of a function $f \in \mathbf{B}_n$, denoted by $\mathcal{AI}(f)$, is defined as*

$$\mathcal{AI}(f) = \min\{\deg(g) \mid gf = 0 \text{ or } g(f+1) = 0, 0 \neq g \in \mathbf{B}_n\}.$$

The immunity of f against fast algebraic attacks is related to the algebraic degree e of a function g and the algebraic degree d of gf with $e \leq d$. For an n-variable function f and any positive integer e with $e < n/2$, there is a nonzero function g of degree at most e such that gf has degree at most $n-e$ [6]. There are several notions about the immunity of Boolean functions against fast algebraic attacks in previous literatures, such as [13,21]. The perfect algebraic immune function we define below is actually a Boolean function which is algebraic attack resistant (see [21]) and has degree at least $n-1$. The latter is necessary for perfect algebraic immune function since a function of degree less than $n-1$ admits $e = 1$ and $d = \deg(f) < n - 1 = n - e$ (taking g being a nonzero constant).

Definition 2 *Let f be an n-variable Boolean function. The function f is said to be perfect algebraic immune if for any positive integers $e < n/2$, the product gf has degree at least $n - e$ for any nonzero function g of degree at most e.*

A perfect algebraic immune ($\mathcal{PAI}$) function achieves maximum $\mathcal{AI}$ and is therefore a Boolean function perfectly resistant to classical and fast algebraic attacks. As a matter of fact, if a function does not achieve maximum $\mathcal{AI}$, then it admits a nonzero function g of degree less than $n/2$ such that $gf = 0$ or $gf = g$, which means that it is not $\mathcal{PAI}$.

3 The immunity of Boolean functions against fast algebraic attacks

In this section, we present the upper bounds on the immunity of Boolean functions against fast algebraic attacks. We first recall the previous results for determining the immunity against fast algebraic attacks, then state our bounds.

Denote by $\mathcal{W}_i$ the ordered set $\{x \in \mathbb{F}_2^n | \operatorname{wt}(x) \leq i\}$ in lexicographic order and by $\overline{\mathcal{W}}_i$ the ordered set $\{x \in \mathbb{F}_2^n | \operatorname{wt}(x) \geq i+1\}$ in the reverse of lexicographic order. According to the definitions of $\mathcal{W}_i$ and $\overline{\mathcal{W}}_i$, it follows that if x is the j-th element in $\mathcal{W}_e$, then $\bar{x}$ is the j-th element in $\overline{\mathcal{W}}_{n-e-1}$, where $\bar{x} = (x_1 + 1, \ldots, x_n + 1)$. Here are some additional notational conventions: for $y, z \in \mathbb{F}_2^n$, let $z \subset y$ be an abbreviation for $\operatorname{supp}(z) \subset \operatorname{supp}(y)$, where $\operatorname{supp}(x) = \{i | x_i = 1\}$, and let $y \cap z = (y_1 \wedge z_1, \ldots, y_n \wedge z_n)$, $y \cup z = (y_1 \vee z_1, \ldots, y_n \vee z_n)$, where $\wedge$ and $\vee$ are the AND and OR operations respectively. We can see that $z \subset y$ if and only if $y^z = y_1^{z_1} y_2^{z_2} \cdots y_n^{z_n} = 1$.

Let g be a function of algebraic degree at most e ($e < n/2$) such that $h = gf$ has algebraic degree at most d ($e \leq d$). Let

$$f(x) = \sum_{c \in \mathbb{F}_2^n} f_c x^c, \ f_c \in \mathbb{F}_2,$$

$$g(x) = \sum_{z \in \mathcal{W}_e} g_z x^z, \ g_z \in \mathbb{F}_2,$$

and

$$h(x) = \sum_{y \in \mathcal{W}_d} h_y x^y, \ h_y \in \mathbb{F}_2$$

be the ANFs of f, g and h respectively. For $y \in \overline{\mathcal{W}}_d$, we have $h_y = 0$ and therefore

$$0 = h_y = \sum_{c \in \mathbb{F}_2^n} \sum_{\substack{c \cup z = y \\ z \in \mathcal{W}_e}} f_c g_z = \sum_{z \in \mathcal{W}_e} g_z \sum_{\substack{c \cup z = y \\ c \in \mathbb{F}_2^n}} f_c. \tag{3}$$

The above equations on g_z's are homogeneous linear. Denote by $V(f; e, d)$ the coefficient matrix of the equations, which is a $\sum_{i=d+1}^{n} \binom{n}{i} \times \sum_{i=0}^{e} \binom{n}{i}$ matrix with the (i, j)-th element equal to

$$v_{yz} = \sum_{\substack{c \cup z = y \\ c \in \mathbb{F}_2^n}} f_c = \sum_{\substack{y \cap \bar{z} \subset c \subset y \\ z \subset y}} f_c = y^z \sum_{y \cap \bar{z} \subset c \subset y} f_c, \tag{4}$$

where y is the i-th element in $\overline{\mathcal{W}}_d$ and z is the j-th element in $\mathcal{W}_e$. Then f admits no nonzero function g of algebraic degree at most e such that $h = gf$ has algebraic degree at most d if and only if the rank of the matrix $V(f; e, d)$ equals the number of g_z's which is $\sum_{i=0}^{e} \binom{n}{i}$, i.e., $V(f; e, d)$ has full column rank (see also [2,10]).

Theorem 1 *[2,10] Let $f \in \mathbf{B}_n$ and $\sum_{c\in\mathbb{F}_2^n} f_c x^c$ be the ANF of f. Let $V(f;e,d)$ be the matrix whose (i,j)-th element equals $\sum_{c\cup z=y} f_c$, where y is the i-th element in $\overline{\mathcal{W}}_d$ and z is the j-th element in $\mathcal{W}_e$.*

Then there exists no nonzero function g of degree at most e such that the product gf has degree at most d if and only if the matrix $V(f;e,d)$ has full column rank.

Remark 1. The theorem shows that $\mathcal{AI}(f) > e$ if and only if the matrix $V(f;e,e)$ has full column rank (since $\mathcal{AI}(f) > e$ if and only if there exists no nonzero function g of degree at most e such that $h = gf$ has degree at most e). Then $\mathcal{AI}(f) = \lceil \frac{n}{2} \rceil$ if and only if the matrix $V(f; \lceil \frac{n}{2} \rceil - 1, \lceil \frac{n}{2} \rceil - 1)$ has full column rank.

Now we show that performing some column operations on the matrix $V(f;e,d)$ creates a matrix with f_c's as its elements.

Lemma 2 $\sum_{z^*\subset z} v_{yz^*} = f_{y\cap\bar{z}}$.

Proof. Note that $c \cup z = y$ if and only if $c \subset y, z \subset y$ and $y \subset c \cup z$, that is, $y^c = 1, y^z = 1$ and $(c \cup z)^y = 1$. By (4) we have

$$\begin{aligned}
\sum_{z^*\subset z} v_{yz^*} &= \sum_{z^*\subset z} \sum_{c\cup z^*=y} f_c \\
&= \sum_{z^*\subset z} \sum_{c\in\mathbb{F}_2^n} y^c y^{z^*} (c \cup z^*)^y f_c \\
&= \sum_{c\in\mathbb{F}_2^n} y^c f_c \sum_{z^*\subset z} y^{z^*} (c \cup z^*)^y \\
&= \sum_{c\subset y} f_c \sum_{\substack{z^*\subset y\cap z \\ y\subset c\cup z^*}} 1 \\
&= \sum_{c\subset y} f_c \sum_{y\cap\bar{c}\subset z^*\subset y\cap z} 1 \\
&= \sum_{c\subset y, y\cap\bar{c}=y\cap z} f_c \\
&= f_{y\cap\bar{z}}.
\end{aligned}$$

□

Lemma 2 shows that the matrix $V(f;e,d)$ can be transformed into a matrix, denoted by $W(f;e,d)$, with the (i,j)-th element equal to

$$w_{yz} = f_{y\cap\bar{z}}, \tag{5}$$

where y is the i-th element in $\overline{\mathcal{W}}_d$ and z is the j-th element in $\mathcal{W}_e$.

The (j,i)-th element of $W(f;e,d)$ is equal to

$$w_{\bar{z}\bar{y}} = f_{\bar{z}\cap\bar{\bar{y}}} = f_{y\cap\bar{z}} = w_{yz},$$

since $\bar{z}$ is the j-th element in $\overline{\mathcal{W}}_d$ and $\bar{y}$ is the i-th element in $\mathcal{W}_e$ by the definitions of $\overline{\mathcal{W}}_d$ and $\mathcal{W}_e$. Recall that $V(f;e,d)$ and $W(f;e,d)$ are $\sum_{i=d+1}^{n}\binom{n}{i}\times\sum_{i=0}^{e}\binom{n}{i}$ matrices. Therefore the matrix $W(f;e,n-e-1)$ is a symmetric $\sum_{i=0}^{e}\binom{n}{i}\times\sum_{i=0}^{e}\binom{n}{i}$ matrix, denoted by $W(f;e)$.

Theorem 3 *Let $f\in\mathbf{B}_n$ and $\sum_{c\in\mathbb{F}_2^n}f_cx^c$ be the ANF of f. Let $W(f;e,d)$ be the matrix whose (i,j)-th element equals $f_{y\cap\bar{z}}$, where y is the i-th element in $\overline{\mathcal{W}}_d$ and z is the j-th element in $\mathcal{W}_e$.*

Then there exists no nonzero function g of degree at most e such that gf has degree at most d if and only if $W(f;e,d)$ has full column rank.

Proof. Lemma 2 shows that $V(f;e,d)$ and $W(f;e,d)$ have the same rank. Then the theorem follows from Theorem 1. □

Remark 2. The theorem shows that $\mathcal{AI}(f)>e$ if and only if the matrix $W(f;e,e)$ has full column rank. Then $\mathcal{AI}(f)=\lceil\frac{n}{2}\rceil$ if and only if the matrix $W(f;\lceil\frac{n}{2}\rceil-1,\lceil\frac{n}{2}\rceil-1)$ has full column rank.

Next we concentrate on the upper bounds on the immunity of Boolean functions against fast algebraic attacks. As mentioned in Section 2, for an n-variable function f and any positive integer e with $e<n/2$, there is a nonzero function g of degree at most e such that gf has degree at most $n-e$. This can also be explained by Theorem 1 or Theorem 3: the matrices $V(f;e,n-e)$ and $W(f;e,n-e)$ do not have full column rank since they are $\sum_{i=0}^{e-1}\binom{n}{i}\times\sum_{i=0}^{e}\binom{n}{i}$ matrices. From Theorem 3 the bounds on the immunity to fast algebraic attacks are related to the question whether the symmetric matrix $W(f;e)$ is invertible.

Before stating our main results, we list a useful lemma about the determinant of a symmetric matrix over a field with characteristic 2.

Lemma 4 *Let $A=(a_{ij})_{m\times m}$ be a symmetric $m\times m$ matrix over a field with characteristic 2, and $a_{ii}=a_{1i}^2$ for $2\le i\le m$, that is,*

$$A=\begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1m}\\ a_{12} & a_{12}^2 & a_{23} & \cdots & a_{2m}\\ a_{13} & a_{23} & a_{13}^2 & \cdots & a_{3m}\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ a_{1m} & a_{2m} & a_{3m} & \cdots & a_{1m}^2 \end{pmatrix}. \tag{6}$$

If $a_{11}=(m+1)\bmod 2$, then $\det(A)=0$.

Proof. Let S_m be the symmetric group of degree m. Then

$$\begin{aligned}\det(A)&=\sum_{\sigma\in S_m}\prod_{i=1}^{m}a_{i,\sigma(i)}\\ &=\sum_{\sigma\in S_m,\sigma^2=1}\prod_{i=1}^{m}a_{i,\sigma(i)}+\sum_{\sigma\in S_m,\sigma^2\neq 1}\prod_{i=1}^{m}a_{i,\sigma(i)}\end{aligned}$$

$$\left(\text{since } \prod_{i=1}^{m} a_{i,\sigma(i)} = \prod_{i=1}^{m} a_{\sigma(i),i} = \prod_{i=1}^{m} a_{\sigma(i),\sigma^{-1}(\sigma(i))} = \prod_{i=1}^{m} a_{i,\sigma^{-1}(i)}\right)$$
$$= \sum_{\sigma\in S_m,\sigma^2=1} \prod_{i=1}^{m} a_{i,\sigma(i)}.$$

If m is odd, then $a_{11} = 0$ and therefore

$$\begin{aligned}
\det(A) &= \sum_{j=2}^{m} \sum_{\substack{\sigma^2=1\\ \sigma(1)=j}} a_{1j} \prod_{i=2}^{m} a_{i,\sigma(i)} \\
&= \sum_{j=2}^{m} \sum_{\substack{\sigma^2=1\\ \sigma(1)=j}} a_{1j}^2 \prod_{\substack{2\le i\le m\\ i\neq j}} a_{i,\sigma(i)} \\
&\quad \text{(for odd } m \text{ and } \sigma^2 = 1, \text{ there is } j' \text{ such that } j' \neq j \text{ and } \sigma(j') = j') \\
&= \sum_{j=2}^{m} \sum_{\substack{\sigma^2=1\\ \sigma(1)=j,\sigma(j')=j'}} a_{1j}^2 a_{1j'}^2 \prod_{\substack{2\le i\le m\\ i\neq j,j'}} a_{i,\sigma(i)} \\
&\quad \text{(there is unique } \sigma' \text{ such that } \sigma'(1) = j',\ \sigma'(j') = 1,\ \sigma'(j) = j, \\
&\quad \text{and } \sigma'(i) = \sigma(i) \text{ for } i \notin \{1, j, j'\}) \\
&= 0.
\end{aligned}$$

If m is even, then $a_{11} = 1$ and therefore

$$\begin{aligned}
\det(A) &= \sum_{\substack{\sigma^2=1\\ \sigma(1)=1}} \prod_{i=2}^{m} a_{i,\sigma(i)} + \sum_{j=2}^{m} \sum_{\substack{\sigma^2=1\\ \sigma(1)=j}} a_{1j}^2 \prod_{\substack{2\le i\le m\\ i\neq j}} a_{i,\sigma(i)} \\
&= \sum_{j=2}^{m} \sum_{\substack{\sigma^2=1\\ \sigma(1)=1,\sigma(j)=j}} a_{1j}^2 \prod_{\substack{2\le i\le m\\ i\neq j}} a_{i,\sigma(i)} + \sum_{j=2}^{m} \sum_{\substack{\sigma^2=1\\ \sigma(1)=j}} a_{1j}^2 \prod_{\substack{2\le i\le m\\ i\neq j}} a_{i,\sigma(i)} \\
&= 0.
\end{aligned}$$

□

Remark 3. For the matrix A of Lemma 4 it holds that $\det(A) = \det(A^{(1,1)})$ if $a_{11} = m \bmod 2$, where $A^{(i,j)}$ is the $(m-1)\times(m-1)$ matrix that results from A by removing the i-th row and the j-th column.

Theorem 5 *Let $f \in \mathbf{B}_n$ and f_{2^n-1} be the coefficient of the monomial $x_1x_2\cdots x_n$ in the ANF of f. Let e be a positive integer less than $n/2$. If $f_{2^n-1} = \binom{n-1}{e} + 1 \bmod 2$, then there exists a nonzero function g with degree at most e such that gf has degree at most $n-e-1$.*

Proof. According to Theorem 3 we need to prove that the square matrix $W(f;e)$ is singular when $f_{2^n-1} = \binom{n-1}{e} + 1 \bmod 2$. Let W_{ij} be the (i,j)-th element of $W(f;e)$. Since $\mathbf{1} = (1,1,\cdots,1)$ and $\mathbf{0} = (0,0,\cdots,0)$ are the first elements in $\overline{\mathcal{W}}_{n-e-1}$ and $\mathcal{W}_e$ respectively, by (5) we have $W_{11} = w_{\mathbf{1},\mathbf{0}} = f_{2^n-1}$. Because $\sum_{i=0}^{e}\binom{n}{i} = \sum_{i=1}^{e}\binom{n-1}{i} + \sum_{i=1}^{e}\binom{n-1}{i-1} + 1 \equiv \binom{n-1}{e} (\bmod 2)$, we know $W_{11} = \sum_{i=0}^{e}\binom{n}{i} + 1 \bmod 2$ when $f_{2^n-1} = \binom{n-1}{e} + 1 \bmod 2$. As mentioned previously, $W(f;e)$ is a symmetric $\sum_{i=0}^{e}\binom{n}{i} \times \sum_{i=0}^{e}\binom{n}{i}$ matrix over $\mathbb{F}_2$. We wish to show that $W(f;e)$ has the form of (6). By (5) we have $W_{1i}^2 = W_{1i} = w_{\mathbf{1}z} = f_{\mathbf{1}\cap\bar{z}} = f_{\bar{z}} = f_{\bar{z}\cap\bar{z}} = w_{\bar{z}z} = W_{ii}$ where $\bar{z}$ is the i-th element in $\overline{\mathcal{W}}_{n-e-1}$ and z is the i-th element in $\mathcal{W}_e$. It follows from Lemma 4 that the matrix $W(f;e)$ is singular. □

Corollary 6 *Let n be an even number and $f \in \mathbf{B}_n$. If f is balanced, then there exists a nonzero function g with degree at most 1 such that the product gf has degree at most $n-2$.*

Proof. If f is balanced, then $f_{2^n-1} = 0$. For even n, it holds that $\binom{n-1}{1} + 1 \equiv 0 (\bmod 2)$. Therefore the result follows from Theorem 5. □

From Corollary 6 it seems that for the number n of input variables, odd numbers are better than even ones from a cryptographic point of view (since cryptographic functions must be balanced).

Lucas' theorem states that for positive integers m and i, the following congruence relation holds:

$$\binom{m}{i} \equiv \prod_{k=1}^{s}\binom{m_k}{i_k} (\bmod 2),$$

where $m = \sum_{k=1}^{s} m_k 2^{k-1}$ and $i = \sum_{k=1}^{s} i_k 2^{k-1}$ are the binary expansion of m and i respectively. It means that $\binom{m}{i} \bmod 2 = 1$ if and only if $i \subset m$.

Note that $f_{2^n-1} = 1$ if and only if $\deg(f) = n$. Theorem 5 shows that for an n-variable function f of degree n and $e \not\subset n-1$, there is a nonzero function g of degree at most e such that gf has degree at most $n-e-1$, and that for an n-variable function f of degree less than n and $e \subset n-1$, there is a nonzero function g of degree at most e such that gf has degree at most $n-e-1$.

For the case $n-1 \notin \{2^s, 2^s-1\}$, there are integers e, e^* with $0 < e, e^* < n/2$ such that $e \subset n-1$ and $e^* \not\subset n-1$, and thus an n-variable function is not $\mathcal{PAI}$. This shows that for a $\mathcal{PAI}$ function the number n of input variables is 2^s+1 or 2^s. For $n = 2^s+1$ (resp. 2^s), it holds that $e \not\subset n-1$ (resp. $e \subset n-1$) for positive integer $e < n/2$, and thus an n-variable function with degree equal to n (resp. less than n) is not $\mathcal{PAI}$. Recall that a function on odd number of variables with maximum $\mathcal{AI}$ is always balanced [9]. For $n = 2^s+1$, a $\mathcal{PAI}$ function has degree $n-1$ and is balanced since it has maximum $\mathcal{AI}$. For $n = 2^s$, a $\mathcal{PAI}$ function has degree n and is then unbalanced, since a function has an odd Hamming weight if and only if it has degree n. Consequently the following theorem is obtained.

Theorem 7 *Let $f \in \mathbf{B}_n$ be a perfect algebraic immune function. Then n is one more than or equal to a power of 2. Further, if f is balanced, then n is one more than a power of 2; if f is unbalanced, then n is a power of 2.*

4 The immunity of Boolean functions against fast algebraic attacks using univariate polynomial representation

In this section we focus on the immunity of Boolean functions against fast algebraic attacks using univariate polynomial representation and show that the bounds presented in Section 3 can be achieved.

Recall that $\mathcal{W}_e$ is the ordered set $\{x \in \mathbb{F}_2^n | \operatorname{wt}(x) \le e\}$ in lexicographic order and $\overline{\mathcal{W}}_d$ is the ordered set $\{x \in \mathbb{F}_2^n | \operatorname{wt}(x) \ge d+1\}$ in the reverse of lexicographic order. Hereinafter, an element $x = (x_1, x_2, \cdots, x_n)$ in $\mathcal{W}_e$ or $\overline{\mathcal{W}}_d$ is considered as an integer $x_1 + x_2 2 + \cdots + x_n 2^{n-1}$ from 0 to $2^n - 1$, and the operations "+" and "−" may be considered as addition and subtraction operations modulo $2^n - 1$ respectively if there is no ambiguity.

Let f, g and h be n-variable Boolean functions, and let g be a function of algebraic degree at most e ($e < n/2$) satisfying that $h = gf$ has algebraic degree at most d ($e \le d$). Let

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

$$g(x) = \sum_{z \in \mathcal{W}_e} g_z x^z, \ g_z \in \mathbb{F}_{2^n},$$

and

$$h(x) = \sum_{y \in \mathcal{W}_d} h_y x^y, \ h_y \in \mathbb{F}_{2^n},$$

be the univariate polynomial representations of f, g and h respectively. For $y \in \overline{\mathcal{W}}_d$, we have $h_y = 0$ and thus

$$0 = h_y = \sum_{\substack{i+z=y \\ z \in \mathcal{W}_e}} f_i g_z = \sum_{z \in \mathcal{W}_e} f_{y-z} g_z. \tag{7}$$

The above equations on g_z's are homogeneous linear. Denote by $U(f; e, d)$ the coefficient matrix of the equations, which is a $\sum_{i=d+1}^{n} \binom{n}{i} \times \sum_{i=0}^{e} \binom{n}{i}$ matrix with the (i, j)-th element equal to

$$u_{yz} = f_{y-z}, \tag{8}$$

where y is the i-th element in $\overline{\mathcal{W}}_d$ and z is the j-th element in $\mathcal{W}_e$. More precisely, for $(i, j) = (1, 1)$ we have $(y, z) = (2^n - 1, 0)$ and $u_{yz} = f_{2^n-1}$; for $(i, j) \ne (1, 1)$ we have $y - z \notin \{0, 2^n - 1\}$ and $u_{yz} = f_{(y-z) \bmod (2^n-1)}$ when $e \le d$.

If the matrix $U(f; e, d)$ has full column rank, i.e., the rank of $U(f; e, d)$ equals the number of g_z's, then f admits no nonzero function g of algebraic degree at most e such that $h = gf$ has algebraic degree at most d.

If the matrix $U(f;e,d)$ does not have full column rank, then there always exists a nonzero Boolean function satisfying Equations (7). More precisely, if $g(x)=\sum_{z\in\mathcal{W}_e} g_z x^z$ $(g_z\in\mathbb{F}_{2^n})$ satisfies (7), then

$$0=h_y^2=\sum_{z\in\mathcal{W}_e} f_{y-z}^2 g_z^2=\sum_{z\in\mathcal{W}_e} f_{2y-2z} g_z^2,\ y\in\overline{\mathcal{W}}_d, \tag{9}$$

where $f_{2(2^n-1)}=f_{2^n-1}$ and f_{2i} is considered as $f_{2i \bmod (2^n-1)}$ for $i\neq 2^n-1$, and thus $g^2(x)=\sum_{z\in\mathcal{W}_e} g_z^2 x^{2z} \bmod (x^{2^n}-x)$ satisfies (9). Note that the system of (7) and the system of (9) are actually the same. Therefore, if $g(x)$ satisfies Equations (7) then $\mathrm{Tr}(g(x))$ satisfies Equations (7), where $\mathrm{Tr}(x)=x+x^2+\cdots+x^{2^{n-1}}$. Also it follows that if $g(x)$ satisfies Equations (7) then $\beta g(x)$ and $\mathrm{Tr}(\beta g(x))$ satisfy Equations (7) for any $\beta\in\mathbb{F}_{2^n}$. If $g(x)\neq 0$, then there is $c\in\mathbb{F}_{2^n}$ such that $g(c)\neq 0$, and there is $\beta\in\mathbb{F}_{2^n}$ such that $\mathrm{Tr}(\beta g(c))\neq 0$ and thus $\mathrm{Tr}(\beta g(x))\neq 0$. Now we can see that $\mathrm{Tr}(\beta g(x))$ is a nonzero Boolean function and satisfies (7). Hence if there is a nonzero solution for (7), then there always exists a nonzero Boolean function g satisfying (7).

Thus the following theorem is obtained.

Theorem 8 *Let $f\in\mathbf{B}_n$ and $\sum_{i=0}^{2^n-1} f_i x^i$ be the univariate polynomial representation of f. Let $U(f;e,d)$ be the matrix whose (i,j)-th element equals f_{y-z}, where y is the i-th element in $\overline{\mathcal{W}}_d$ and z is the j-th element in $\mathcal{W}_e$.*

Then there exists no nonzero function g of algebraic degree at most e such that the product gf has algebraic degree at most d if and only if the matrix $U(f;e,d)$ has full column rank.

Remark 4. As described at the beginning of this section, the sets $\mathcal{W}_e$ and $\overline{\mathcal{W}}_d$ of Theorem 8 are subsets of $\{0,1,\cdots,2^n-1\}$, while the sets $\mathcal{W}_e$ and $\overline{\mathcal{W}}_d$ of Theorem 1 and Theorem 3 are subsets of $\mathbb{F}_2^n$.

Remark 5. The theorem gives a method using one matrix to evaluate the immunity of Boolean functions against fast algebraic attacks based on univariate polynomial representation while in [22] P. Rizomiliotis used three matrices.

Remark 6. The theorem shows that $\mathcal{AI}(f)>e$ if and only if the matrix $U(f;e,e)$ has full column rank. Then $\mathcal{AI}(f)=\lceil\frac{n}{2}\rceil$ if and only if the matrix $U(f;\lceil\frac{n}{2}\rceil-1,\lceil\frac{n}{2}\rceil-1)$ has full column rank.

Remark 7. The matrix $U(f;e,n-e-1)$, denoted by $U(f;e)$, is symmetric since

$$u_{\bar{z}\bar{y}}=f_{\bar{z}-\bar{y}}=f_{(2^n-1-z)-(2^n-1-y)}=f_{y-z}=u_{yz}.$$

Further, we have

$$u_{y\bar{y}}=f_{y-\bar{y}}=f_{y-(2^n-1-y)}=f_{2y}=f_y^2=u_{y,0}^2,$$

and therefore $U(f;e)$ has the form of (6). Hence Theorem 5 can also be derived from Theorem 8 and Lemma 4.

4.1 Carlet-Feng functions

The class of the Carlet-Feng functions were first presented in [11] and further studied by C. Carlet and K. Feng [4]. Such functions have maximum algebraic immunity and good nonlinearity. It was observed through computer experiments by Armknecht's algorithm [2] that the functions also have good behavior against fast algebraic attacks. In [23], P. Rizomiliotis determined the immunity of the Carlet-Feng functions against fast algebraic attacks by computing the linear complexity of a sequence, which is more efficient than Armknecht's algorithm but is not yet feasible for large n. In this section, we further discuss the immunity of the Carlet-Feng functions against fast algebraic attacks and prove that the functions achieve the bounds of Theorem 5.

Let n be an integer and α a primitive element of $\mathbb{F}_{2^n}$. Let $f \in \mathbf{B}_n$ and

$$\mathrm{supp}(f) = \{\alpha^l, \alpha^{l+1}, \alpha^{l+2}, \cdots, \alpha^{l+2^{n-1}-1}\}, 0 \le l \le 2^n - 2. \tag{10}$$

Then $\mathcal{AI}(f) = \lceil \frac{n}{2} \rceil$ according to [11,4]. As a matter of fact, the support of the function $f(\alpha^{l+2^{n-1}}x) + 1$ is $\{0, 1, \alpha, \cdots, \alpha^{2^{n-1}-2}\}$, which is a Carlet-Feng function. It means that these functions are affine equivalent.

A similar proof of [4, Theorem 2] applies to the following result. Here we give a proof for self-completeness.

Proposition 9 *Let $\sum_{i=0}^{2^n-1} f_i x^i$ be the univariate polynomial representation of the function f of (10). Then $f_0 = 0$, $f_{2^n-1} = 0$, and for $1 \le i \le 2^n - 2$,*

$$f_i = \frac{\alpha^{-il}}{1 + \alpha^{-i/2}}.$$

Hence the algebraic degree of f is equal to $n - 1$.

Proof. We have $f_0 = f(0) = 0$ and $f_{2^n-1} = 0$ since f has even Hamming weight and thus algebraic degree less than n. For $1 \le i \le 2^n - 2$, by (2) we have

$$\begin{aligned} f_i &= \sum_{j=0}^{2^n-2} f(\alpha^j)\alpha^{-ij} = \sum_{j=l}^{l+2^{n-1}-1} \alpha^{-ij} = \alpha^{-il} \sum_{j=0}^{2^{n-1}-1} \alpha^{-ij} \\ &= \alpha^{-il} \frac{1 + \alpha^{-i2^{n-1}}}{1 + \alpha^{-i}} = \alpha^{-il} \frac{1 + \alpha^{-i/2}}{1 + \alpha^{-i}} = \frac{\alpha^{-il}}{1 + \alpha^{-i/2}}. \end{aligned}$$

We can see that $f_{2^n-2} \neq 0$ and therefore f has algebraic degree $n - 1$. □

Remark 8. For the function f of (10), the (i, j)-th element of the matrix $U(f; e, d)$ with $e \le d$ is equal to

$$u_{yz} = f_{y-z} = \frac{\alpha^{-yl}\alpha^{zl}}{1 + \alpha^{-y/2}\alpha^{z/2}}, \text{ for } (i, j) \neq (1, 1),$$

where y is the i-th element in $\overline{\mathcal{W}}_d$ and z is the j-th element in $\mathcal{W}_e$.

Lemma 10 *Let K be a field of characteristic 2. Let $A = (a_{ij})_{m\times m}$ be an $m \times m$ matrix over K and $a_{ij} = (1 + \beta_i\gamma_j)^{-1}$, $\beta_i, \gamma_j \in K$ and $\beta_i\gamma_j \neq 1$, $1 \leq i, j \leq m$. Then the determinant of A is equal to*

$$\prod_{1\leq i<j\leq m} (\beta_i + \beta_j)(\gamma_i + \gamma_j) \prod_{1\leq i,j\leq m} a_{ij}.$$

Furthermore, the determinant of A is nonzero if and only if $\beta_i \neq \beta_j$ and $\gamma_i \neq \gamma_j$ for $i \neq j$.

Proof. The second half part of this lemma is derived from the first half part. The proof of the first half part is given by induction on m. First we can check that the statement is certainly true for $m = 1$. Now we verify the induction step. Suppose that it holds for $m - 1$. Thus we suppose that

$$\det(A^{(1,1)}) = \prod_{2\leq i<j\leq m} (\beta_i + \beta_j)(\gamma_i + \gamma_j) \prod_{2\leq i,j\leq m} a_{ij},$$

where $A^{(i,j)}$ is the $(m-1)\times(m-1)$ matrix that results from A by removing the i-th row and the j-th column.

We wish to show that it also holds for m. Let $B = (b_{ij})_{m\times m}$ with $b_{1j} = a_{1j}$ and for $i > 1$,

$$\begin{aligned}
b_{ij} &= a_{ij} + a_{11}^{-1}a_{i1}a_{1j} \\
&= \frac{1}{1+\beta_i\gamma_j} + (\frac{1}{1+\beta_1\gamma_1})^{-1} \cdot \frac{1}{1+\beta_i\gamma_1} \cdot \frac{1}{1+\beta_1\gamma_j} \\
&= \frac{(1+\beta_i\gamma_1)(1+\beta_1\gamma_j) + (1+\beta_1\gamma_1)(1+\beta_i\gamma_j)}{(1+\beta_i\gamma_j)(1+\beta_i\gamma_1)(1+\beta_1\gamma_j)} \\
&= \frac{\beta_i\gamma_1 + \beta_1\gamma_j + \beta_1\gamma_1 + \beta_i\gamma_j}{(1+\beta_i\gamma_j)(1+\beta_i\gamma_1)(1+\beta_1\gamma_j)} \\
&= \frac{(\beta_1+\beta_i)(\gamma_1+\gamma_j)}{(1+\beta_i\gamma_j)(1+\beta_i\gamma_1)(1+\beta_1\gamma_j)} \\
&= a_{ij} \cdot (\beta_1+\beta_i)a_{i1} \cdot (\gamma_1+\gamma_j)a_{1j}.
\end{aligned}$$

Let

$$P = \mathrm{diag}(1, (\beta_1+\beta_2)a_{21}, \cdots, (\beta_1+\beta_m)a_{m1})$$

and

$$Q = \mathrm{diag}(1, (\gamma_1+\gamma_2)a_{12}, \cdots, (\gamma_1+\gamma_m)a_{1m})$$

where $\mathrm{diag}(x_1, \cdots, x_m)$ denotes a diagonal matrix whose diagonal entries starting in the upper left corner are $x_1, \cdots, x_m$. Then

$$B = P \begin{pmatrix} a_{11} & * \\ 0 & A^{(1,1)} \end{pmatrix} Q.$$

Hence

$$\det(A) = \det(B)$$

$$
\begin{aligned}
&= \det(P) \cdot a_{11} \det(A^{(1,1)}) \cdot \det(Q) \\
&= \left(\prod_{i=2}^{m} (\beta_1 + \beta_i) a_{i1} \right) \cdot a_{11} \det(A^{(1,1)}) \cdot \left(\prod_{j=2}^{m} (\gamma_1 + \gamma_j) a_{1j} \right) \\
&= \prod_{1 \le i < j \le m} (\beta_i + \beta_j)(\gamma_i + \gamma_j) \prod_{1 \le i,j \le m} a_{ij}.
\end{aligned}
$$

It has now been proved by mathematical induction that the first half part of this lemma holds for all positive integers m. □

Lemma 11 *Let $A = (a_{ij})_{m\times m}$ and $B = (b_{ij})_{m\times m}$ be $m \times m$ matrices with $a_{ij} = \beta_i \gamma_j b_{ij}$ and $\beta_i \neq 0, \gamma_j \neq 0$ for $1 \le i, j \le m$. Then $\det(A) \neq 0$ if and only if $\det(B) \neq 0$.*

Proof. Let $P = \mathrm{diag}(\beta_1, \beta_2, \cdots, \beta_m)$ and $Q = \mathrm{diag}(\gamma_1, \gamma_2, \cdots, \gamma_m)$. Then $A = PBQ$ and hence $\det(A) = \det(B) \prod_{i=1}^{m} \beta_i \gamma_i$, which proves this lemma. □

Proposition 12 *Let e be a positive integer less than $n/2$ and f be the function of (10). Then $U(f; e)$ is invertible if $\binom{n-1}{e} \equiv 0 (\mathrm{mod}\, 2)$, and $U(f; e, n-e-2)$ has full column rank if $\binom{n-1}{e} \equiv 1 (\mathrm{mod}\, 2)$.*

Proof. Let $U = U(f; e)$ and U_{ij} be the (i, j)-th element of U. We have $U_{11} = f_{2^n-1} = 0$. By Remark 7 we know that U is a symmetric matrix of order $\sum_{i=0}^{e} \binom{n}{i}$ in the form of (6). For the case $\binom{n-1}{e} \bmod 2 = 0$, we have $\sum_{i=0}^{e} \binom{n}{i} \bmod 2 = 0 = U_{11}$. By Remark 3 it holds that $\det(U) = \det(U^{(1,1)})$. Remark 8 shows that the (i, j)-th element of $U^{(1,1)}$ is

$$
U_{ij}^{(1,1)} = \frac{\alpha^{-yl} \alpha^{zl}}{1 + \alpha^{-y/2} \alpha^{z/2}},
$$

where y is the i-th element in $\overline{\mathcal{W}}_{n-e-1} \setminus \{2^n - 1\}$ and z is the j-th element in $\mathcal{W}_e \setminus \{0\}$, since $e \le n-e-1$ for $e < n/2$. Let U^* be a $(\sum_{i=0}^{e} \binom{n}{i} - 1) \times (\sum_{i=0}^{e} \binom{n}{i} - 1)$ matrix with the (i, j)-th element equal to

$$
U_{ij}^{*} = \frac{1}{1 + \alpha^{-y/2} \alpha^{z/2}}.
$$

Since $\alpha^{-y/2} \neq \alpha^{-y'/2}$ for $y \neq y'$ $(y, y' \in \overline{\mathcal{W}}_{n-e-1} \setminus \{2^n - 1\})$ and $\alpha^{z/2} \neq \alpha^{z'/2}$ for $z \neq z'$ $(z, z' \in \mathcal{W}_e \setminus \{0\})$, from Lemma 10 we have $\det(U^*) \neq 0$. Then by Lemma 11 it holds that $\det(U^{(1,1)}) \neq 0$. Hence, U is invertible.

For the case $\binom{n-1}{e} \bmod 2 = 1$, we consider the $\sum_{i=0}^{e+1} \binom{n}{i} \times \sum_{i=0}^{e} \binom{n}{i}$ matrix $U(f; e, n-e-2)$. For even n, we always have $e \le n-e-2$ for $e < n/2$. For odd n, we always have $e \le n-e-2$ for $e \le (n-3)/2$ and $\binom{n-1}{e} \bmod 2 = 0$ for $e = \frac{n-1}{2}$. Thus for $\binom{n-1}{e} \bmod 2 = 1$ and $e < n/2$, we always have $e \le n-e-2$. Let U^{**} be the $\sum_{i=0}^{e} \binom{n}{i} \times \sum_{i=0}^{e} \binom{n}{i}$ matrix that results from $U(f; e, n-e-2)$ by removing the first $\binom{n}{e+1}$ rows. A similar proof of $\det(U^{(1,1)}) \neq 0$ also applies to $\det(U^{**}) \neq 0$. Then $U(f; e, n-e-2)$ has full column rank. □

The proof of the proposition shows that for the function f of (10) the rank of the matrix $U(f;e)$ is at least $\sum_{i=0}^{e}\binom{n}{i}-1$ (since the matrix $U^{(1,1)}$ is invertible). Then, by Theorem 5, f admits a unique nonzero function g with algebraic degree e such that gf has algebraic degree at most $n-e-1$ when $\binom{n-1}{e}\equiv 1(\bmod 2)$.

Theorem 13 *Let e be a positive integer less than $n/2$ and f be the function of (10). Then f admits no nonzero function g with algebraic degree at most e such that gf has algebraic degree at most $n-e-1$ if $\binom{n-1}{e}\equiv 0(\bmod 2)$, and admits no nonzero function g with algebraic degree at most e such that gf has algebraic degree at most $n-e-2$ if $\binom{n-1}{e}\equiv 1(\bmod 2)$.*

Proof. It is derived from Theorem 8 and Proposition 12. □

Corollary 14 *Let $n=2^s+1$ and $f\in\mathbf{B}_n$ be the function of (10). Then f is $\mathcal{PAI}$.*

Proof. It is obtained from Theorem 13 since $\binom{n-1}{e}=\binom{2^s}{e}\equiv 0(\bmod 2)$ for $1\le e<n/2$. □

Theorem 13 states that the Carlet-Feng functions achieve the bounds of Theorem 5 and thus the bounds of Theorem 5 are tight for the functions with algebraic degree less than n, while Corollary 14 states that the Carlet-Feng functions on 2^s+1 variables are $\mathcal{PAI}$. The theorem explains the experimental results of [4,10] on the immunity of the Carlet-Feng functions against fast algebraic attacks, and implies the conjecture of C. Carlet and K. Feng [4, Section 5].

Next we consider the Boolean functions with algebraic degree equal to n.

Let n be an integer and α a primitive element of $\mathbb{F}_{2^n}$. Let $f\in\mathbf{B}_n$ and

$$\mathrm{supp}(f)=\{0,\alpha^l,\alpha^{l+1},\cdots,\alpha^{l+2^{n-1}-1}\},0\le l\le 2^n-2. \tag{11}$$

The function of (11) is a function that results from the function of (10) by flipping the output at $x=0$.

A similar proof of Proposition 9 applies to the following result.

Proposition 15 *Let $\sum_{i=0}^{2^n-1}f_ix^i$ be the univariate polynomial representation of the function f of (11). Then $f_0=1$, $f_{2^n-1}=1$, and for $1\le i\le 2^n-2$,*

$$f_i=\frac{\alpha^{-il}}{1+\alpha^{-i/2}}.$$

Hence the algebraic degree of f is equal to n.

A similar proof of Proposition 12 also applies to the following result.

Proposition 16 *Let e be a positive integer less than $\frac{n-1}{2}$ and f be the function of (11). Then $U(f;e)$ is invertible if $\binom{n-1}{e}\equiv 1(\bmod 2)$, and $U(f;e,n-e-2)$ has full column rank if $\binom{n-1}{e}\equiv 0(\bmod 2)$.*

Theorem 17 *Let e be a positive integer less than $\frac{n-1}{2}$ and f be the function of (11). Then f admits no nonzero function g with algebraic degree at most e such that gf has algebraic degree at most $n-e-1$ if $\binom{n-1}{e} \equiv 1 (\mathrm{mod}\, 2)$, and admits no nonzero function g with algebraic degree at most e such that gf has algebraic degree at most $n-e-2$ if $\binom{n-1}{e} \equiv 0 (\mathrm{mod}\, 2)$.*

Proof. It is confirmed by Theorem 8 and Proposition 16. □

Similarly to the function of (10), the function of (11) admits a unique nonzero function g with algebraic degree e such that gf has algebraic degree at most $n-e-1$ when $\binom{n-1}{e} \equiv 0 (\mathrm{mod}\, 2)$.

In Theorem 17 we do not consider the case $e = \frac{n-1}{2}$ for odd n, since Theorem 5 shows that for odd n, an n-variable function f with algebraic degree n admits a nonzero function g with algebraic degree at most $\frac{n-1}{2}$ such that gf has algebraic degree at most $\frac{n-1}{2}$ (noting that $\binom{n-1}{\frac{n-1}{2}} \bmod 2 = 0$).

Corollary 18 *Let $n = 2^s$ and $f \in \mathbf{B}_n$ be the function of (11). Then f is $\mathcal{PAI}$.*

Proof. It is obtained from Theorem 17 since $\binom{n-1}{e} = \binom{2^s-1}{e} \equiv 1 (\mathrm{mod}\, 2)$ for $1 \leq e < n/2$. □

Theorem 17 states that the modified Carlet-Feng functions achieve the bounds of Theorem 5 and thus the bounds of Theorem 5 are tight for the functions with algebraic degree equal to n, while Corollary 18 states that the modified Carlet-Feng functions on 2^s variables are $\mathcal{PAI}$.

Consequently, as mentioned above, the bounds of Theorem 5 are tight and there exist $\mathcal{PAI}$ functions on 2^s and 2^s+1 variables. More precisely, there exist n-variable $\mathcal{PAI}$ functions with degree $n-1$ (balanced functions) if and only if $n = 2^s + 1$; there exist n-variable $\mathcal{PAI}$ functions with degree n (unbalanced functions) if and only if $n = 2^s$.

5 Conclusion

In this paper, several open problems about the immunity of Boolean functions against fast algebraic attacks have been solved. We proved the maximum immunity to fast algebraic attacks, and identified the immunity of the Carlet-Feng functions against fast algebraic attacks. It seems that for a balanced function, in terms of the immunity to fast algebraic attacks, the optimal value of the number n of input variables is one more than a power of two. The Carlet-Feng functions previously shown to have maximum algebraic immunity and good nonlinearity are proved to be optimal against fast algebraic attacks among the balanced functions. To the best of our knowledge this is the first time that a class of Boolean functions are shown to have such cryptographic property.

Acknowledgement

The authors thank the anonymous referees for their valuable comments on this paper. The authors are also grateful to Tianze Wang for his careful reading of the manuscript, and to Shaoyu Du, Lin Jiao, Yao Lu, Wenlun Pan, Tao Shi, and Wenhao Wang for their participation in FAA seminar at SKLOIS in December 2011. The first author would especially like to thank Dingyi Pei for his enlightening conversations on the resistance of Boolean functions against algebraic attacks.

References

1. F. Armknecht. Improving fast algebraic attacks. In: B. Roy and W. Meier (eds.) FSE 2004. LNCS 3017, pp. 65–82. Berlin, Heidelberg: Springer, 2004.
2. F. Armknecht, C. Carlet, P. Gaborit, et al. Efficient computation of algebraic immunity for algebraic and fast algebraic attacks. In: S. Vaudenay (eds.) EUROCRYPT 2006. LNCS 4004, pp. 147–164. Berlin, Heidelberg: Springer, 2006.
3. C. Carlet. Boolean functions for cryptography and error correcting codes. In: Y. Crama, P. Hammer, eds. Boolean Methods and Models in Mathematics, Computer Science, and Engineering, pp. 257–397. Cambridge: Cambridge University Press, 2010.
4. 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: ASIACRYPT 2008, LNCS 5350, 425–440. Berlin, Heidelberg: Springer, 2008.
5. N. Courtois and W. Meier. Algebraic attacks on stream ciphers with linear feedback. Advances in Cryptology-EUROCRYPT 2003, LNCS 2656, 345–359. Berlin, Heidelberg: Springer, 2003.
6. N. Courtois. Fast algebraic attacks on stream ciphers with linear feedback. Advances in Cryptology-CRYPTO 2003, LNCS 2729, 176–194. Berlin, Heidelberg: Springer, 2003.
7. N. Courtois. Cryptanalysis of Sfinks. ICISC 2005, LNCS 3935, 261–269. Berlin, Heidelberg: Springer, 2006.
8. 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, 41–58, 2006.
9. D. K. Dalai, K. C. Gupta, and S. Maitra. Results on algebraic immunity for cryptographically significant Boolean functions. INDOCRYPT 2004, LNCS 3348, 92–106. Berlin, Heidelberg: Springer, 2005.
10. Y. Du, F. Zhang, and M. Liu. On the resistance of Boolean functions against fast algebraic attacks. ICISC 2011, LNCS 7259, 261–274. Berlin, Heidelberg: Springer 2012.
11. K. Feng, Q. Liao, and J. Yang. Maximal values of generalized algebraic immunity. Designs, Codes and Cryptography, vol. 50, no. 2, pp. 243–252, 2009.
12. S. Fischer and W. Meier. Algebraic immunity of S-boxes and augmented functions. In: Biryukov, A. (ed.) FSE 2007. LNCS 4593, pp. 366–381. Springer, 2007.
13. G. Gong. Sequences, DFT and resistance against fast algebraic attacks. SETA 2008, LNCS 5203, pp. 197–218, 2008.
14. P. Hawkes and G. Rose. Rewriting variables: the complexity of fast algebraic attacks on stream ciphers, in Crypto 2004, LNCS 3152, pp. 390–406. Springer, 2004.

15. N. Li, L. Qu, W. Qi, et al. On the construction of Boolean Functions with optimal algebraic immunity. IEEE Transactions on Information Theory, vol. 54, no. 3, 1330–1334, 2008.
16. N. Li and W. Qi. Construction and analysis of Boolean functions of $2t+1$ variables with maximum algebraic immunity. ASIACRYPT 2006, LNCS 4284, pp. 84–98. Berlin, Heidelberg: Springer, 2006.
17. M. Liu, D. Lin, and D. Pei. Fast algebraic attacks and decomposition of symmetric Boolean functions. IEEE Transactions on Information Theory, vol. 57, no. 7, pp. 4817–4821, 2011.
18. M. Liu, D. Pei, and Y. Du. Identification and construction of Boolean functions with maximum algebraic immunity. SCIENCE CHINA Information Sciences, vol. 53, no. 7, pp. 1379–1396, 2010.
19. F.J. MacWilliams and N.J.A. Sloane. The theory of error correcting codes. New York: North-Holland, 1977.
20. W. Meier, E. Pasalic, and C. Carlet. Algebraic attacks and decomposition of Boolean functions. Advances in Cryptology-EUROCRYPT 2004, LNCS 3027, 474–491. Berlin, Heidelberg: Springer, 2004.
21. E. Pasalic. Almost fully optimized infinite classes of Boolean functions resistant to (fast) algebraic cryptanalysis. ICISC 2008, LNCS 5461, 399–414. Berlin, Heidelberg: Springer, 2009.
22. P. Rizomiliotis. On the resistance of Boolean functions against algebraic attacks using univariate polynomial representation. IEEE Transactions on Information Theory, vol. 56, no. 8, pp. 4014–4024, 2010.
23. P. Rizomiliotis. On the security of the Feng-Liao-Yang Boolean functions with optimal algebraic immunity against fast algebraic attacks. Designs, Codes and Cryptography, vol. 57, no. 3, pp. 283–292, 2010.
24. 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, vol. 60, no. 1, pp. 1–14, 2011.
25. 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. IEEE Transactions on Information Theory, vol. 57, no. 9, pp. 6310–6320, 2011.
26. Y. Zhang, M. Liu, and D. Lin. On the immunity of rotation symmetric Boolean functions against fast algebraic attacks. Cryptology ePrint Archive, Report 2012/111, `http://eprint.iacr.org/`.