A NOTE ON THE FAST ALGEBRAIC IMMUNITY AND ITS CONSEQUENCES ON MODIFIED MAJORITY FUNCTIONS

DENG TANG

1. School of Mathematics, Southwest Jiaotong University
   Chengdu 610031, China
2. Guangxi Key Laboratory of Cryptography and Information Security
   Guilin 541000, China

(Communicated by Subhamoy Maitra)

Abstract. Boolean functions used as nonlinear filters and/or combiners in LFSR-based stream ciphers should satisfy several desired cryptographic properties simultaneously, to withstand all known cryptographic attacks. In the past decade, the algebraic and fast algebraic immunities are the most infusive criteria on the design of cryptographic Boolean functions, due to the high efficiency of the algebraic and fast algebraic attacks on stream ciphers. Up to now, Boolean functions with optimal algebraic immunity have been built in several ways, but there are not many known results on their fast algebraic immunities. In this paper, we first derive a relation on the fast algebraic immunity between a Boolean function $f$ and its modifications $f + s$, which shows that if $f$ has low fast algebraic immunity and $s$ has low algebraic immunity then $f + s$ may also have low fast algebraic immunity in general. Thanks to this relation, we obtain some upper bounds on the fast algebraic immunity of several known classes of modified majority functions.

1. Introduction

Boolean functions play a central role in the security of stream ciphers. Before 2003, the widely accepted properties for a Boolean function to be used in stream ciphers were balancedness (for avoiding statistical dependence between the plaintext and the ciphertext), high nonlinearity (to withstand the best affine approximation [14] and the fast correlation attack [29]), high algebraic degree (to resist the Berlekamp-Massey algorithm [27] and the Rønjom-Helleseth attack [32]), and proper order of resiliency (for allowing resistance to the correlation attacks [34]). In 2003, Courtois and Meier successfully introduced algebraic attacks, which were efficient for several stream ciphers previously believed secure [11]. To resist the standard algebraic attack, a new cryptographic property of Boolean functions called algebraic immunity was introduced by Meier et al. [28]. Since then, a Boolean function of $n$ variables used in a cryptosystem should have optimal algebraic immunity $\lceil \frac{n}{2} \rceil$. Later in [10], Courtois further improved the standard algebraic attack to fast algebraic attacks. A fast algebraic attack is feasible if one can find nonzero functions $g$ of low algebraic degree and $h$ of algebraic degree not much larger than $n/2$, such that $fg = h$ [1, 10, 19]. As a response to fast algebraic attacks, a concept of fast algebraic immunity was introduced in [21]. It should be noted that if $f$ or...
$f + 1$ admits a function $g$ of low algebraic degree such that $fg = 0$, then the algebraic attack using $g$ is more efficient since it needs less data. Hence, Boolean functions used in stream ciphers should have both optimal algebraic immunity and high fast algebraic immunity for resisting algebraic and fast algebraic attacks. However, to our knowledge, there are not many known results on evaluating the values of the fast algebraic immunity of Boolean functions since computing the fast algebraic immunity of a given function with high algebraic degree is an extremely hard task in general if the number of variables is greater than 18. To say the least, up to now, proving a tight lower (or upper) bound on the fast algebraic immunity of a general Boolean function is also a hard task. So far, only a few advances have been made, see for instance [2, 40, 24, 39, 6, 25, 22, 37, 38, 23].

In the literature, the majority function, which is a subclass of symmetric Boolean functions, is the first class of functions which has been found with optimal algebraic immunity. It has been shown that the majority function has very low nonlinearity [12, 3], which is insufficient for the resistance to fast correlation attacks [29]. In addition, Armknecht et al. [2] proved that the majority function also has a bad behavior against fast algebraic attacks. Therefore, modifying the majority function to get higher nonlinearity was considered to be a natural way of working. Up to now, there are many works on the constructions of Boolean functions with optimal algebraic immunity by modifying the majority function, for instance [12, 20, 33, 8, 15, 17, 18, 35, 36]. However, it is unknown that whether modified majority functions have good behavior against fast algebraic attacks. In the present paper, we first derive a relation on the fast algebraic immunity between a Boolean function and its modifications, by introducing a new concept: the partial fast algebraic immunity. This relation shows that, in general, if an original Boolean function $f$ has low fast algebraic immunity and another Boolean function $s$ has low algebraic immunity then the function $f' = f + s$ may also have low fast algebraic immunity. As applications of this relation, we obtain some upper bounds on the fast algebraic immunity of several known classes of modified majority functions with optimal algebraic immunity. These bounds show that these modified majority functions are still have low fast algebraic immunity, which is coincident with the relation.

The remainder of this paper is organized as follows. In Section 2, the notation and the necessary preliminaries required for the subsequent sections are reviewed. In Section 3, the majority function is introduced. In section 4, a relation on the fast algebraic immunity between a Boolean function and its modifications is proposed, and some upper bounds on the fast algebraic immunity of several classes of modified majority functions with optimal algebraic immunity are obtained. Finally, Section 5 concludes this paper.

2. Preliminaries

Let $\mathbb{F}_2 = \{0, 1\}$ and $\mathbb{F}_2^n$ be the vector space of all $n$-tuples over $\mathbb{F}_2$. A Boolean function of $n$ variables is a function from $\mathbb{F}_2^n$ into $\mathbb{F}_2$. Denote by $B_n$ the set of Boolean functions of $n$ variables. The basic representation of a Boolean function $f(x_1, \cdots, x_n)$ is by its truth table, i.e.,

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

The support of $f$ is defined as $\text{supp}(f) = \{\alpha \in \mathbb{F}_2^n | f(\alpha) = 1\}$. The Hamming weight $\text{wt}(f)$ of $f$ is the cardinality of the support of $f$, i.e., $\text{wt}(f) = |\text{supp}(f)|$. 
Besides, any Boolean function \( f \in \mathcal{B}_n \) can be uniquely represented by a multivariate polynomial over \( \mathbb{F}_2 \), called the algebraic normal form (ANF), namely:

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

where \( a_u \in \mathbb{F}_2 \) and \( u = (u_1, \cdots, u_n) \). It is well-known [13] that

\[
a_u = \sum_{v \leq u} f(v),
\]

where \( v = (v_1, \cdots, v_n) \) and \( v \leq u \) means that \( v_i \leq u_i \) for all \( 1 \leq i \leq n \). The algebraic degree, denoted by \( \text{Deg}(f) \), is the maximal value of \( \text{wt}(u) \) such that \( a_u \neq 0 \), where the Hamming weight \( \text{wt}(u) \) of a binary vector \( u \in \mathbb{F}_2^n \) is the number of its nonzero coordinates (i.e., the size of its support \( \{1 \leq i \leq n \mid u_i \neq 0\} \)). A Boolean function is called an affine function if its algebraic degree is at most 1. The set of all affine functions is denoted by \( A_n \). In order to resist the Berlekamp-Massey algorithm [27] and the Ronjom-Helleseth attack [32], Boolean functions used in stream ciphers should have high algebraic degree. It should be noted that the maximum algebraic degree of a balanced Boolean function of \( n \) variables is \( n - 1 \).

In order to resist the best affine approximation (BAA) [14] and the fast correlation attack [29], Boolean functions used in a cryptosystem must have high nonlinearity. The nonlinearity \( NL(f) \) of a Boolean function \( f \in \mathcal{B}_n \) is defined as

\[
NL(f) = \min_{g \in A_n} (d_H(f, g)),
\]

where \( d_H(f, g) \) is the Hamming distance between \( f \) and \( g \), i.e., \( d_H(f, g) = |\{ x \in \mathbb{F}_2^n : f(x) \neq g(x)\}| \). In other words, the nonlinearity \( NL(f) \) is the minimum Hamming distance between \( f \) and all affine functions.

The nonlinearity of a Boolean function can also be expressed by means of the Walsh transform of this function. Let \( x = (x_1, x_2, \cdots, x_n) \) and \( \alpha = (\alpha_1, \alpha_2, \cdots, \alpha_n) \) both belong to \( \mathbb{F}_2^n \) and let \( x \cdot \alpha \) be any inner product in \( \mathbb{F}_2^n \), for instance the usual inner product \( x \cdot \alpha = x_1 \alpha_1 + x_2 \alpha_2 + \cdots + x_n \alpha_n \), then the Walsh transform of \( f \in \mathcal{B}_n \) at \( \alpha \) is defined by

\[
W_f(\alpha) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+\alpha \cdot x}.
\]

Then, by the Walsh transform the nonlinearity of a Boolean function \( f \in \mathcal{B}_n \) can be computed as

\[
NL(f) = 2^{n-1} - \frac{1}{2} \max_{\alpha \in \mathbb{F}_2^n} |W_f(\alpha)|.
\]

In recent years, algebraic attacks have become a powerful attack which have allowed to cryptanalyse some stream ciphers which were previously believed secure [11]. As a response to the standard algebraic attack, a new cryptographic property for designing Boolean functions used in stream ciphers, called algebraic immunity, has been introduced.

**Definition 2.1** ([28]). Given two \( n \)-variable Boolean functions \( f \) and \( h \), we say that \( h \) is an annihilator of \( f \) if the function \( fh \) defined as \( (fh)(x) = f(x)h(x) \) is equal to 0. The algebraic immunity \( AI(f) \) of a Boolean function \( f \) is defined to be the minimum algebraic degree of nonzero Boolean functions \( h \) such that \( h \) is an annihilator of \( f \) or \( f + 1 \).
To resist the standard algebraic attack, a Boolean function should have algebraic immunity as high as possible. It was proved in [11] that $AI(f) \leq \lceil \frac{n}{2} \rceil$ for an arbitrary $n$-variable Boolean function $f$. In this paper, $f$ is said to have optimal algebraic immunity if it achieves the maximum $\lceil \frac{n}{2} \rceil$. A high algebraic immunity is necessary but is not a sufficient condition for the resistance against all kinds of algebraic attacks. For an arbitrary Boolean function $f$, if one can find nonzero functions $g$ of low algebraic degree and $h$ of algebraic degree significantly lower than $n$ such that $fg = h$, then a fast algebraic attack is feasible [1, 10, 19]. Therefore, a notion of fast algebraic immunity was introduced in a preliminary version of [24] for quantifying the resistance of Boolean functions to fast algebraic attacks.

**Definition 2.2** ([21, 24]). The fast algebraic immunity of a Boolean function $f \in B_n$ is defined as

$$FAI(f) = \min \left\{ 2AI(f), \min_{1 \leq \deg(g) < AI(f)} \{ \deg(g) + \deg(fg) \} \right\}.$$

Let $f$ be any Boolean function defined on $F_2^n$. The following lemmas are well-known.

**Lemma 2.3** ([10]). $FAI(f) \leq n$.

**Lemma 2.4** ([7]). $FAI(f) = FAI(f + 1)$.

**Lemma 2.5.** $FAI(f) \leq \min\{n, \deg(f) + 2\}$.

**Proof.** It is sufficient to prove that $FAI(f) \leq \deg(f) + 2$ since by Lemma 2.3 we have $FAI(f) \leq n$. If $AI(f) = 1$, the result is obvious. Otherwise, it can be easily seen by setting $g$ as a linear function, i.e., $\deg(g) = 1$. \hfill \Box

**Lemma 2.6** ([39]). Define $A = \min\{\deg(h) | fh = 0, h \neq 0\}$. If $AI(f) \geq 2$ and $2AI(f) > A$, then $FAI(f) \geq A + 1 \geq AI(f) + 1$.

### 3. Symmetric Boolean functions

The symmetric Boolean functions constitute a very interesting class of Boolean functions. Every symmetric Boolean function on $n$ variables can be expressed by an $(n + 1)$-bit vector, which reduces the memory required for storing the function; moreover, a symmetric Boolean function can be efficiently implemented in both hardware and software.

From now on, we denote by $W^d$ the set of all vectors in $F_2^n$ with Hamming weight $d$, by $W^{>d}$ (resp. $W^{<d}$) the set of all vectors in $F_2^n$ with Hamming weight strictly larger than $d$ (resp. strictly smaller than $d$), and by $W^{\geq d} \cup W^{>d}$ (resp. $W^{\leq d} = W^{d} \cup W^{<d}$). We shall now introduce the definition of the symmetric function.

**Definition 3.1.** A Boolean function $f$ is called symmetric if

$$f(x_1, \cdots, x_n) = f(x_{\tau(1)}, \cdots, x_{\tau(n)}),$$

for any permutation $\tau$ on $\{1, 2, \cdots, n\}$.

We denote by $SB_n$ the set of all symmetric Boolean functions on $n$ variables. This definition implies that any symmetric Boolean function $f$ takes the same value for all the vectors with the same Hamming weight. Therefore, any symmetric Boolean function $f \in SB_n$ can be simply characterized by a vector

$$v_f = (v_f(0), v_f(1), \cdots, v_f(n)) \in F_2^{n+1},$$
where the component \( v_f(i) \) equals \( f(x) \) with \( x \in W^i \). The vector \( v_f \) is called the simplified value vector of \( f \). Besides, the symmetric Boolean function \( f \) can also be uniquely represented as

\[
f(x) = \sum_{i=0}^{n} \lambda_f(i) \sigma_i,
\]

where \( \lambda_f(i) \in \mathbb{F}_2 \) and \( \sigma_i \) denotes the \( i \)-th elementary symmetric Boolean function \( \sum_{u \in W^i} x^u \). It is well-known (see e.g. [5]) that \( v_f(i) = \sum_{k \leq i} \lambda_f(k) \) and \( \lambda_f(i) = \sum_{k \leq i} v_f(k) \) for every \( i \in \{0, 1, \cdots, n\} \).

For odd number of variables \( n \), Qu et al. proved in [31] that there are exactly two symmetric Boolean functions \( f_m \) and \( f_m+1 \) in \( \mathcal{SB}_n \) with optimal algebraic immunity \((n + 1)/2\). For even number of variables \( n \), except the majority function, some constructions of symmetric Boolean functions with optimal algebraic immunity can be found in [4, 16, 9]. In 2011, Peng et al. [30] determined all the even-variable symmetric Boolean functions with optimal algebraic immunity. The total number of such symmetric Boolean functions is \((2^{\lfloor \log_2 n \rfloor} + 1)2^{\lfloor \log_2 n \rfloor} \). The Hamming weight, algebraic degree and nonlinearity of those functions are also determined. Among this kind of functions, none is balanced \((n \geq 4)\) and the best possible nonlinearity is \( 2^{n-1} - \frac{1}{2}\left(\frac{n}{2}\right) + \left(\frac{n}{2} - 2^{\lfloor \log_2 n \rfloor} / 2\right) \), which is too low and therefore insufficient for the resistance to fast correlation attacks [29].

Let us now see the behavior of symmetric Boolean functions with optimal algebraic immunity against fast algebraic attacks. In 2011, Liu et al. [24] proved that almost all symmetric Boolean functions do not behave well against fast algebraic attacks, when the number of variables lies in the left half of an interval \([2^m, 2^{m+1}]\):

**Theorem 3.2 ([24]).** Let \( f \in \mathcal{SB}_n \) and \( 2^m \leq n < 2^m + 2^{m-1} - 1 \). Then \( AI(f) \leq 2^{m-1} - 1 \) or \( \deg(\sigma_f) = 2^{m-1} + e \) with \( e = n - 2^m + 1 \).

Note that the \( e \)-th elementary symmetric function \( \sigma_e \) has algebraic degree \( e \). It then follows from Theorem 3.2 that all symmetric Boolean functions with optimal algebraic immunity do not behave quite well against fast algebraic attacks when the number of variables is greater than 8. The situation is worse for the numbers of variables near a power of 2.

### 3.1. The Majority Function

The majority function which is a subclass of symmetric Boolean functions has been used by many researchers to construct more Boolean functions with optimal algebraic immunity. The majority function is defined as follows.

**Definition 3.3.** The \( n \)-variable majority function \( f_m \) is defined as:

\[
f_m(x) = \begin{cases} 
0, & \text{if } x \in W^{< \lfloor n/2 \rfloor} \\
1, & \text{if } x \in W^{\geq \lfloor n/2 \rfloor}.
\end{cases}
\]

In [12], the authors have studied the cryptographic properties of the majority function \( f_m \) (indeed, the considered function in [12], denoted by \( f' \), taking value 1 for all vectors with Hamming weight strictly greater than \( n/2 \)) is different from \( f_m \) when \( n \) is even, but is affine equivalent since \( f_m(x_1, \cdots, x_n) = f'(x_1 + 1, \cdots, x_n + 1) + 1 \).

**Lemma 3.4 ([12, 3]).** The function \( f_m \in \mathcal{B}_n \) has the following cryptographic properties:

1) \( \deg(f_m) = 2^{\lfloor \log_2 n \rfloor} \);
2) \( AI(f_m) = \lfloor \frac{n}{2} \rfloor \);
3) $NL(f_m) = 2^{n-1} - \binom{n-1}{\frac{n}{2}}$.

The following upper bound is a direct consequence of Lemmas 2.5 and 3.4.

**Lemma 3.5.** For $2^m \leq n < 2^{m+1}$, let $f_m$ be the $n$-variable majority function, then $FAI(f_m) \leq \min\{2^m + 2, n\}$.

In 2006, Armknecht et al. [2] obtained an upper bound on the fast algebraic immunity of the majority function.

**Lemma 3.6 ([2]).** Let $f_m$ be the majority function with variables $n \geq 2$. Then there exist Boolean functions $g$ and $h$ such that $f_m g = h$ with $\text{Deg}(h) = \lfloor n/2 \rfloor + 1$ and $\text{Deg}(g) = \text{Deg}(h) - 2^j$, where $j$ is the maximal integer such that $\text{Deg}(g) > 0$.

By Lemma 3.6 we can see that for any $4 \leq 2^m \leq n < 2^{m+1}$ we have $FAI(f_m) \leq n - 2^{m-1} + c$, where $c = 2$ for even $n$ and $c = 1$ for odd $n$. Furthermore, we can slightly improve the upper bound on the fast algebraic immunity of the majority function when $4 \leq 2^m + 2^{m-1} \leq n < 2^{m+1}$.

**Theorem 3.7.** Let $4 \leq 2^m \leq n < 2^{m+1}$ and $c = 2$ for even $n$ and $c = 1$ for odd $n$. Then $FAI(f_m) \leq n - 2^{m-1} + c$ for $2^m \leq n < 2^m + 2^{m-1}$ and $FAI(f_m) \leq 2^m + 2$ for $2^m + 2^{m-1} \leq n < 2^{m+1}$.

**Proof.** It follows from Lemma 3.6 that $FAI(f_m) \leq n - 2^{m-1} + c$ for $2^m \leq n < 2^{m+1}$. In addition, $FAI(f_m) \leq 2^m + 2$ by Lemma 3.5. Then we have $FAI(f_m) \leq n - 2^{m-1} + c$ for $2^m \leq n < 2^m + 2^{m-1}$ and $FAI(f_m) \leq 2^m + 2$ for $2^m + 2^{m-1} \leq n < 2^{m+1}$ since $n - 2^{m-1} + c \geq 2^m + 2$ if $n \geq 2^m + 2^{m-1}$. This completes the proof.

By Theorem 3.7, we can see that the majority function does not behave quite well against fast algebraic attacks for the numbers of variables greater than 8, and the situation is worse for the numbers of variables near a power of 2. We list some small concrete values of the upper bound given by Theorem 3.7 in Table 1 for the convenience of the readers.

| $n$   | 4   | 5   | 8   | 9   | 10  | 11  | 16  | 17  | 18  | 19  | 20  | 21  |
|-------|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| Theorem 3.7 | 4   | 4   | 6   | 6   | 8   | 8   | 10  | 10  | 12  | 12  | 14  | 14  |
| $n$   | 22  | 23  | 32  | 33  | 34  | 35  | 36  | 37  | 38  | 39  | 40  | 41  |
| Theorem 3.7 | 16  | 16  | 18  | 18  | 20  | 20  | 22  | 22  | 24  | 24  | 26  | 26  |
| $n$   | 42  | 43  | 44  | 45  | 46  | 47  | 47  | 64  | 65  | 66  | 67  | 68  | 69  |
| Theorem 3.7 | 28  | 28  | 30  | 30  | 32  | 32  | 32  | 34  | 34  | 36  | 36  | 38  | 38  |
| $n$   | 70  | 71  | 72  | 73  | 74  | 75  | 76  | 77  | 78  | 79  | 80  | 81  |
| Theorem 3.7 | 40  | 40  | 42  | 42  | 44  | 44  | 46  | 46  | 48  | 48  | 50  | 50  |
| $n$   | 82  | 83  | 84  | 85  | 86  | 87  | 88  | 89  | 90  | 91  | 92  | 93  |
| Theorem 3.7 | 52  | 52  | 54  | 54  | 56  | 56  | 58  | 58  | 60  | 60  | 62  | 62  |
| $n$   | 94  | 95  | 128 | 129 | 130 | 131 | 132 | 133 | 134 | 135 | 136 | 137 |
| Theorem 3.7 | 64  | 64  | 66  | 66  | 68  | 68  | 70  | 70  | 72  | 72  | 74  | 74  |
| $n$   | 138 | 139 | 140 | 141 | 142 | 143 | 144 | 145 | 146 | 147 | 148 | 149 |
| Theorem 3.7 | 76  | 76  | 78  | 78  | 80  | 80  | 82  | 82  | 84  | 84  | 86  | 86  |

Particularly, by Theorem 3.7 and Lemma 2.6, the exact values of fast algebraic immunity of the majority function in $2^m$ and $2^m + 1$ variables have been determined in [39].
Theorem 3.8 ([39]). Let $f_m \in SB_n$ be the majority function. If $n \in \{2^m, 2^m + 1\}$ where $m \geq 2$, then $FAI(f_m) = 2^{m-1} + 2$.

This was the first time that the exact values of the fast algebraic immunity of an infinite class of symmetric Boolean functions with optimal algebraic immunity were determined.

4. A RELATION ON THE FAST ALGEBRAIC IMMUNITY AND ITS CONSEQUENCES TO UPPER BOUNDS ON THE FAST ALGEBRAIC IMMUNITY OF MODIFIED MAJORITY FUNCTIONS

It follows from Lemma 3.4 that the nonlinearity of the majority function is very low, which is almost the worst case according to Lobanov’s bound [26]. The value of the nonlinearity of the majority function is insufficient for the resistance against fast correlation attacks and therefore the constructed Boolean functions are not suitable for the cryptographic use in stream ciphers. Because the majority function has optimal algebraic immunity, modifying the majority function to have higher nonlinearity was considered to be a natural way of working. Till now, there are many works on the constructions of Boolean functions with optimal algebraic immunity by modifying the majority function, for instance [12, 20, 33, 8, 15, 17, 18, 35, 36]. However, it is unknown that whether modified majority functions have good behavior against fast algebraic attacks. In this section, we first derive a relation on the fast algebraic immunity between two Boolean functions $f$ and $f+s$, where $f,s \in B_n$. Thanks to this relation, we are able to give upper bounds on the fast algebraic immunity of several known classes of Boolean functions with optimal algebraic immunity.

4.1. A RELATION BETWEEN THE FAST ALGEBRAIC IMMUNITIES OF A BOOLEAN FUNCTION AND ITS MODIFIED FUNCTIONS.

To our knowledge, there are not many known results on evaluating the values of the fast algebraic immunity of Boolean functions since computing the fast algebraic immunity of a given function with high algebraic degree is an extremely hard task in general if the number of variables is greater than 18. To say the least, up to now, proving a tight lower (or upper) bound on the fast algebraic immunity of Boolean functions is also a hard task in general (some advances can be found in [2, 40, 24, 39, 6, 25, 22, 37, 38, 23]). In this subsection, we will give a relation on the fast algebraic immunity between two Boolean functions with the same number of variables, which shows that if a function $f$ has very low fast algebraic immunity and $s$ has low algebraic immunity then the function $f' = f + s$ may have low fast algebraic immunity. Note that it may be difficult to construct functions with good fast algebraic immunity since proving or computing the fast algebraic immunity of a function is very hard if the number of variables greater than 18. Therefore, our bound sometimes can help us to evaluate the fast algebraic immunity of $f'$ by considering the fast algebraic immunity of $f$ and the algebraic immunity of $s$. This gives more hints on the fast algebraic immunity.

To derive the relation, first of all we introduce a new concept called partial fast algebraic immunity.

Definition 4.1. Let $f \in B_n$ and $a,b$ be two integers such that $0 \leq a \leq b \leq n + 1$, the partial fast algebraic immunity of $f$ is defined as

$$PFAI_f(a,b) = \min_{a \leq \text{Deg}(g) < b, 0 \neq g \in B_n} \{\text{Deg}(g) + \text{Deg}(fg)\}.$$
The following facts on the partial fast algebraic immunity of any Boolean function \( f \in B_n \) are obvious.

\begin{enumerate}[enumerate]
\item \( PFAI_f(0,0) = \text{Deg}(f) \);
\item \( PFAI_f(a,b) \leq PFAI_f(c,d) \) for all \( 0 \leq a \leq c \leq d \leq b \);
\item \( FAI(f) = \min \{ PFAI_f(1, AI(f)), 2AI(f) \} \).
\end{enumerate}

We are now ready to present and prove a relation on the fast algebraic immunity between two Boolean functions \( f \) and \( f + s \).

**Theorem 4.2.** Let \( f, f', s \in B_n \) be three Boolean functions such that \( f' = f + s \) and \( AI(f') - AI(s) \geq 2 \). Let \( g' \in B_n \) be a function such that \( 1 \leq \text{Deg}(g') < \min \{ \text{Deg}(f), AI(f') \} - AI(s) \) and \( \text{Deg}(g') + \text{Deg}(fg') = PFAI_f(1, \min \{ \text{Deg}(f), AI(f') \} - AI(s)) \), and \( g'' \in B_n \) be a nonzero function of degree \( AI(s) \) such that \( sg'' = 0 \) or \( (s+1)g'' = 0 \). If \( \text{Deg}(g'g'') \geq 1 \), then we have
\[
FAI(f') \leq PFAI_f(1, \min \{ AI(f), AI(f') \} - d) + 2d,
\]
where \( d = AI(s) \).

**Proof.** Let us define \( e = \text{Deg}(g') \). We can see that \( e < \min \{ \text{Deg}(f), AI(f') \} - d \) and thus we have \( \text{Deg}(g'g'') \leq \text{Deg}(g') + \text{Deg}(g'') \leq e + d < AI(f') \).

**Case 1.** \( sg'' = 0 \). In this case we have \( f'g'g'' = (f+s)g'g'' = fg'g'' \neq 0 \) since \( 1 \leq \text{Deg}(g'g'') < AI(f') \). Note that \( \text{Deg}(fg'g'') \leq \text{Deg}(fg') + \text{Deg}(g'') = PFAI_f(1, \min \{ AI(f), AI(f') \} - d) - e - d \). Then we have \( \text{Deg}(g'g'') + \text{Deg}(fg'g'') \leq e + d + PFAI_f(1, \min \{ AI(f), AI(f') \} - d) - e - d = PFAI_f(1, \min \{ AI(f), AI(f') \} - d) + 2d \). This implies that \( FAI(f') \leq PFAI_f(1, \min \{ AI(f), AI(f') \} - d) + 2d \).

**Case 2.** \( (s+1)g'' = 0 \). Similar to the case \( sg'' = 0 \) we can easily deduce that \( FAI(f' + 1) \leq PFAI_f(1, \min \{ AI(f), AI(f') \} - d) + 2d \), which is also true for \( FAI(f') \) by Lemma 2.4.

Then we can immediately get our assertion by combining the two cases above. \( \square \)

4.2. Upper Bounds on the Fast Algebraic Immunity of Modified Majority Functions. In this subsection, we will obtain some upper bounds on the fast algebraic immunity of several classes of modified majority functions with optimal algebraic immunity. Our results are heavily relied on Theorem 4.2. To this end, we first need the following lemma.

**Lemma 4.3.** Let \( 4 \leq 2^m \leq n < 2^m + 2^{m-1} \) and \( f_m \in B_n \) be the majority function. Define \( g'(x_1, x_2, \ldots, x_n) = \prod_{i=0}^{r' - 1} (x_{2i+1} + x_{2i+2}) \), where \( r = n - 2^m + c \) in which \( c = 2 \) for even \( n \) and \( c = 1 \) for odd \( n \). Then we have \( \text{Deg}(g') + \text{Deg}(f_mg') \leq n - 2^{m-1} + c \) and \( PFAI_{f_m}(1, t) \leq n - 2^m + c \) for \( r/2 < t \leq [n/2] \).

**Proof.** It follows from Lemma 3.6 and [2, Section 5.4] that \( \text{Deg}(g') + \text{Deg}(f_mg') \leq n - 2^{m-1} + c \). Further, by Fact F2 we have \( PFAI_{f_m}(1, t) \leq n - 2^m + c \) for \( r/2 < t < [n/2] \). This completes the proof. \( \square \)

**Theorem 4.4.** For \( 4 \leq 2^m \leq n < 2^{m+1} \), let \( f, s \in B_n \) be two functions such that \( f = f_m + s \) and \( AI(f) = \lceil \frac{n}{2} \rceil \). For \( 2^m \leq n < 2^m + 2^{m-1} \), if \( AI(s) < 2^{m-1} - 1 \) and if there exists a nonzero annihilator \( g'' \in B_n \) of \( s \) or \( s+1 \) such that \( \text{Deg}(g'') = AI(s) \) and \( \text{Deg}(g''g') \geq 1 \), then \( g'(x_1, x_2, \ldots, x_n) = \prod_{i=0}^{r' - 1} (x_{2i+1} + x_{2i+2}) \) with \( r = n - 2^m + c \) in which \( c = 2 \) for even \( n \) and \( c = 1 \) for odd \( n \). Then we have
\[
FAI(f) \leq \begin{cases} \ n - 2^{m-1} + c + 2AI(s), & \text{if } 2^m \leq n < 2^m + 2^{m-1} \\ 2^n + 2AI(s), & \text{if } 2^m + 2^{m-1} \leq n < 2^{m+1} \end{cases}
\]
Proof. It follows from Lemma 4.3, Theorem 4.2 and Fact F2 that $FAI(f) \leq n - 2^{m-1} + \epsilon + 2AI(s)$ for $2^m \leq n < 2^m + 2^{m-1}$. If $2^m + 2^{m-1} \leq n < 2^{m+1}$, according to $(f_m + s)g'' = f_m g''$ or $(f_m + s + 1)g'' = f_m g''$ we directly get that $FAI(f) \leq \text{Deg}(g'') + \text{Deg}(f_m g'') \leq 2^m + 2AI(s)$ since $\text{Deg}(f_m) = 2^m$. This completes the proof. \hfill \Box

In what follows, as applications of Theorem 4.4, we give some upper bounds on the fast algebraic immunity of three classes of modified majority functions with optimal algebraic immunity.

Class 1 ([12]). For even $n$, define $f \in \mathcal{B}_n$ as

$$
(2) \quad f_D(x) = \begin{cases}
0, & \text{if } x \in W^{< \frac{n}{2}} \\
b_x, & \text{if } x \in W^{\frac{n}{2}} \\
1, & \text{if } x \in W^{> \frac{n}{2}}
\end{cases}
$$

where $b_x$ are the elements which can take values arbitrarily in $\mathbb{F}_2$ and denoted by $b_x \in \mathbb{F}_2$ in the sequel.

It has been proved in [12] that this class of functions have optimal algebraic immunity. Toward these functions, we have the following theorem.

Theorem 4.5. For $8 \leq 2^m \leq n < 2^{m+1}$, let $f_D \in \mathcal{B}_n$ be the function defined by (2), then

$$
FAI(f_D) \leq \begin{cases}
n - 2^{m-1} + 4, & \text{if } 2^m \leq n < 2^m + 2^{m-1} \\
2^m + 2, & \text{if } 2^m + 2^{m-1} \leq n < 2^{m+1}
\end{cases}
$$

Proof. Let $s' = f_m + f_D$. We can easily see that the support of $s'$ is a subset of the set $W^{\frac{n}{2}}$. Thus we have $AI(s') \leq 1$ since $s' \sigma_1 = 0$ if $\frac{n}{2}$ is even and $s' \sigma_1 = 0$ if $\frac{n}{2}$ is odd. It can be easily checked that $\text{Deg}(g' \sigma_1) \geq 1$, $\text{Deg}(g' \sigma_1 + 1) \geq 1$ and $AI(s') \leq 2^m - c + 1$ when $2^m \leq n < 2^m + 2^{m-1}$, where $c$ and $g'$ are defined in Lemma 4.3. Then our assertion follows from Theorem 4.4. \hfill \Box

Class 2 ([18]). Let $n$ be an even integer. Define four subsets $B = \{b_1, \cdots, b_l\} \subseteq W^{< \frac{n}{2}}$, $C = \{c_1, \cdots, c_m\} \subseteq W^{\frac{n}{2}}$, $U = \{u_1, \cdots, u_l\} \subseteq W^{\frac{n}{2}}$ and $V = \{v_1, \cdots, v_m\} \subseteq W^{\frac{n}{2}}$ such that the following conditions hold 1) $U \cap V = \emptyset$, 2) $\forall 1 \leq i \leq l, b_i \leq u_i$, and $\forall 1 \leq j < i \leq l, b_i \leq u_i$, and 3) $\forall 1 \leq i \leq m, v_i \leq c_i$, and $\forall 1 \leq j < i \leq m, v_i \leq c_j$. Define the function $f \in \mathcal{B}_n$ as

$$
(3) \quad f(x) = \begin{cases}
0, & \text{if } x \in (W^{< \frac{n}{2}} \setminus B) \cup U \cup C \\
0, & \text{if } x \in W^{\frac{n}{2}} \setminus (U \cup V) \\
1, & \text{if } x \in (W^{> \frac{n}{2}} \setminus C) \cup V \cup B
\end{cases}
$$

For a set $U \in \mathbb{F}_2^n$, define $\overline{U} = \{x \mid x \in U\}$ where $\overline{x} = (x_1 \oplus 1, \cdots, x_n \oplus 1)$. Let us denote three subclasses of functions by $f_{C_1}, f_{C_2}$ and $f_{C_3}$ respectively as follows.

Class $f_{C_1}$. Let $u$ be an arbitrary nonzero vector of $\mathbb{F}_2^n$ such that $3 \leq \text{wt}(u) = k < \frac{n}{2}$. Let the sets $B$ and $U$ satisfy

$$
(4) \quad B = \{x \mid \text{wt}(x) = \frac{n}{2} - \text{wt}(u), \text{supp}(x) \cap \text{supp}(u) = \emptyset\} \text{ and } U = \{x + u \mid x \in B\}.
$$

The balanced function $f_{C_1} \in \mathcal{B}_n$ is defined as

$$
(5) \quad f_{C_1}(x) = \begin{cases}
0, & \text{if } x \in (W^{< \frac{n}{2}} \setminus B_1) \cup U_1 \cup \overline{B}_1 \\
b_x, & \text{if } x \in W^{\frac{n}{2}} \setminus (U_1 \cup \overline{U}_1) \\
1, & \text{if } x \in (W^{> \frac{n}{2}} \setminus \overline{B}_1) \cup \overline{U}_1 \cup B_1
\end{cases}
$$
the sets $B_1$ and $U_1$ are defined by

$$B_1 = \begin{cases} B, & \text{for even } \Theta_k \\ B \setminus \{x_1\} & \text{otherwise} \end{cases} \quad \text{and} \quad U_1 = \begin{cases} U, & \text{for even } \Theta_k \\ U \setminus \{u + x_1\} & \text{otherwise} \end{cases},$$

where $\Theta_k = \left( \frac{n-1}{2} \right) - \left( \frac{n-k}{2} \right)$ and $x_1$ is an element of $B$.

**Class $f_{C_2}$.** For a fixed nonzero element $v_1 \in W^{<\frac{n}{2}}$ with $\text{supp}(v_1) = \{i_1, i_2, \ldots, i_k\}$, take $v_2 \in W^{\leq \frac{n}{2}}$ with $\text{supp}(v_2) = \{i_1, i_2, \ldots, i_k, i_{k+1}\}$, where $2 \leq k \leq \frac{n}{2} - 2$. Denote

$$B^i = \{ x \mid \text{wt}(x) = \frac{n}{2} - \text{wt}(v_1), \text{supp}(x) \cap \text{supp}(v_2) = \emptyset \},$$

and $U^i = \{ x + v_1 \mid x \in B^i \}$ for $i = 1, 2$. Two sets $B$ and $U$ are defined as

$$B = B^1 \cup B^2, U = U^1 \cup U^2.$$

The balanced function $f_{C_2} \in B_n$ is obtained as

$$f_{C_2}(x) = \begin{cases} 0, & \text{if } x \in (W^{< \frac{n}{2}} \setminus B_2) \cup U_2 \cup \overline{B_2} \\ b_x \in \{0, 1\}, & \text{if } x \in W^{\frac{n}{2}} \setminus (U_2 \cup \overline{U_2}) \\ 1, & \text{if } x \in (W^{> \frac{n}{2}} \setminus \overline{B_2}) \cup \overline{U_2} \cup B_2 \end{cases},$$

where $B_2$ and $U_2$ are defined by

$$B_2 = \begin{cases} B, & \text{for even } \Theta_k \\ B \setminus \{x_2\} & \text{otherwise} \end{cases} \quad \text{and} \quad U_2 = \begin{cases} U, & \text{for even } \Theta_k \\ U \setminus \{v_1 + x_2\} & \text{otherwise} \end{cases},$$

where $x_2$ is an arbitrary element of $B$.

**Class $f_{C_3}$.** Let $u$ be an arbitrary nonzero vector of $\mathbb{F}_2^n$ such that $3 \leq \text{wt}(u) < \frac{n}{2}$. Let $B$ and $U$ be defined as in (3). Let $x_3$ be any element of $B$. Define

$$B_3 = \begin{cases} B, & \text{for even } \Theta_k \\ B \setminus \{x_3\} & \text{otherwise} \end{cases} \quad \text{and} \quad U_3 = \begin{cases} U, & \text{for even } \Theta_k \\ U \setminus \{v_1 + x_3\} & \text{otherwise} \end{cases}.$$

The balanced function $f_{C_3}$ on $\mathbb{F}_2^n$ is defined as

$$f_{C_3}(x) = \begin{cases} 0, & \text{if } x \in (W^{< \frac{n}{2}} \setminus B_3) \cup U_3 \cup \overline{U_3} \\ b_x \in \mathbb{F}_2, & \text{if } x \in W^{\frac{n}{2}} \setminus (U_3 \cup \overline{U_3}) \\ 1, & \text{if } x \in (W^{> \frac{n}{2}} \setminus B_3) \end{cases}.$$

The three subclasses of functions possess optimal algebraic immunity. Moreover, by choosing suitable parameters $k$ they have nonlinearity significantly larger than that of the majority function [8]. However, they are still vulnerable to fast algebraic attacks.

**Theorem 4.6.** For $2^m \leq n < 2^{m+1}$. Let $f_{C_1}, f_{C_2}, f_{C_3} \in B_n$ (even $n \geq 12$) be the three subclasses of functions defined by (4),(5) and (6) respectively. Then we have

1). $\text{FAI}(f_{C_1}) \leq \begin{cases} t + 2, & \text{if } \frac{n}{2} \equiv \left( \frac{n}{2} - k \right) \pmod{2} \\ t + 6, & \text{otherwise} \end{cases}$;

2). $\text{FAI}(f_{C_2}) \leq t + 6$;

3). $\text{FAI}(f_{C_3}) \leq \begin{cases} t + 2, & \text{if } \frac{n}{2} \equiv \left( \frac{n}{2} - k \right) \pmod{2} \\ t + 4, & \text{otherwise} \end{cases}$,

where

$$t = \begin{cases} n - 2m - 1 + 2, & \text{if } 2^m \leq n < 2^m + 2^{m-1} \\ 2^m, & \text{if } 2^m + 2^{m-1} \leq n < 2^{m+1} \end{cases}.$$
Proof. Assume that \( f_{C_1} = f_m + s_1, f_{C_2} = f_m + s_2 \) and \( f_{C_3} = f_m + s_3 \). We can see that 
\[ \text{supp}(s_1) \subseteq W^{\frac{n}{2} - k} \cup W^{\frac{n}{2}} \cup W^{\frac{n}{2} + k}, \]
where \( 3 \leq k < \frac{n}{2} \). Then we have \( AI(s_1) = 1 \) if 
\[ \frac{n}{2} \equiv (\frac{n}{2} - k) \pmod{2}, \]
and \( s_1 \sigma_1 = 0 \) if \( \frac{n}{2} \equiv (\frac{n}{2} - k) \pmod{2} \) otherwise. As for \( \frac{n}{2} \not\equiv (\frac{n}{2} - k) \pmod{2} \), define 
\[ g = x_i x_j + x_i, \]
where \( i, j \in \text{supp}(u) \) and \( u \) is the vector defined in Case \( f_{C_1} \). Recall that 
\( B = \{ x \mid \text{wt}(x) = \frac{n}{2} - \text{wt}(u), \text{supp}(x) \cap \text{supp}(u) = O \} \). 
Thus, for any \( x \in B \) we have \( x_i = x_j = 0 \) and hence \( g(x) = 0 \). If \( x \in \overline{B} \) we have 
\( x_i = x_j = 1 \) and therefore \( g(x) = 0 \). That is, \( g(x) = 0 \) for all \( x \in B \cup \overline{B} \), where \( B \) is defined by (3). Therefore, we have \( s_1 \sigma_1 = 0 \) if \( \frac{n}{2} \) is even and \( s_1 \sigma_1 = 1 \) if \( \frac{n}{2} \) is odd.

Note that the algebraic degrees of \( g \sigma_1 \) and \( g(\sigma_1 + 1) \) equal 3. This leads to \( AI(s_1) \leq 3 \) in this case.

Similarly, we can deduce that \( s_2(x_i x_j + x_i) \sigma_1 = 0 \) or \( s_2(x_i x_j + x_i)(\sigma_1 + 1) = 0 \), where \( i, j \in \text{supp}(v_1) \) and \( v_1 \) is defined in Case \( f_{C_2} \). Thus, \( AI(s_2) \leq 3 \).

 Toward the algebraic immunity of \( s_3 \), we have \( AI(s_3) = 1 \) if \( \frac{n}{2} \equiv (\frac{n}{2} - k) \pmod{2} \). If \( \frac{n}{2} \not\equiv (\frac{n}{2} - k) \pmod{2} \), we can deduce that \( AI(s_3) \leq 2 \) since we have 
\[ s_3(x_i + 1) \sigma_1 = 0 \] or \( s_3(x_i + 1)(\sigma_1 + 1) = 0 \), where \( i \in \text{supp}(u) \) and \( u \) is defined in Case \( f_{C_3} \).

It can be easily checked that algebraic degrees of the multiplies of \( g' \) and the nonzero annihilators of \( s_1, s_1, s_3 \) mentioned above respectively are greater than 1, where \( g' \) is defined in Lemma 4.3. Note that \( AI(s_i) < 2^{m-1} - c + 1 \) \((1 \leq i \leq 3)\) for \( 2^m \leq n < 2^m + 2^{m-1} \), where \( c \) is defined in Lemma 4.3. Therefore, it follows from Theorem 4.4 that the upper bounds on the fast algebraic immunity of \( f_{C_1}, f_{C_2} \) and \( f_{C_3} \) can be obtained. This completes the proof.

We summarize upper bounds on the fast algebraic immunity of the functions \( f_0, f_{C_1}, f_{C_2} \) and \( f_{C_3} \) in Table 2 for even numbers of variables ranging from 12 to 254.

**Table 2.** Upper bounds on the fast algebraic immunity of modified majority functions

| even n  | 12-14 | 16 | 18 | 20 | 22 | 24-30 | 32 | 34 | 36 | 40 | 42 | 44 |
|---------|-------|----|----|----|----|--------|----|----|----|----|----|----|
| \( FAI(f_D) \) | 16 | 14 | 12 | 10 | 8 | 6 | 4 | 2 | 1 |
| \( FAI(f_{C_1}) \) | 14 | 16 | 18 | 20 | 22 | 22 | 24 | 26 | 28 | 30 | 32 | 34 |
| \( FAI(f_{C_2}) \) | 12 | 14 | 16 | 18 | 20 | 20 | 22 | 24 | 26 | 28 | 30 | 32 |
| \( FAI(f_{C_3}) \) | 14 | 16 | 18 | 20 | 22 | 22 | 24 | 26 | 28 | 30 | 32 | 34 |

| even n  | 48-62 | 64 | 66 | 68 | 70 | 72 | 74 | 76 | 78 | 80 | 82 | 84 |
|---------|-------|----|----|----|----|----|----|----|----|----|----|----|
| \( FAI(f_D) \) | 48 | 46 | 44 | 42 | 40 | 40 | 40 | 40 | 40 | 40 | 40 | 40 |
| \( FAI(f_{C_1}) \) | 48 | 46 | 44 | 42 | 40 | 40 | 40 | 40 | 40 | 40 | 40 | 40 |
| \( FAI(f_{C_2}) \) | 48 | 46 | 44 | 42 | 40 | 40 | 40 | 40 | 40 | 40 | 40 | 40 |
| \( FAI(f_{C_3}) \) | 48 | 46 | 44 | 42 | 40 | 40 | 40 | 40 | 40 | 40 | 40 | 40 |

| even n  | 86 | 88 | 90 | 92 | 94 | 96 | 98 | 100 | 102 | 104 | 106 | 108 |
|---------|----|----|----|----|----|----|----|-----|-----|-----|-----|-----|
| \( FAI(f_D) \) | 86 | 88 | 90 | 92 | 94 | 96 | 98 | 100 | 102 | 104 | 106 | 108 |
| \( FAI(f_{C_1}) \) | 86 | 88 | 90 | 92 | 94 | 96 | 98 | 100 | 102 | 104 | 106 | 108 |
| \( FAI(f_{C_2}) \) | 86 | 88 | 90 | 92 | 94 | 96 | 98 | 100 | 102 | 104 | 106 | 108 |
| \( FAI(f_{C_3}) \) | 86 | 88 | 90 | 92 | 94 | 96 | 98 | 100 | 102 | 104 | 106 | 108 |

| even n  | 168 | 170 | 172 | 174 | 176 | 178 | 180 | 182 | 184 | 186 | 188 | 190 | 192-254 |
|---------|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| \( FAI(f_D) \) | 168 | 170 | 172 | 174 | 176 | 178 | 180 | 182 | 184 | 186 | 188 | 190 | 192-254 |
| \( FAI(f_{C_1}) \) | 168 | 170 | 172 | 174 | 176 | 178 | 180 | 182 | 184 | 186 | 188 | 190 | 192-254 |
| \( FAI(f_{C_2}) \) | 168 | 170 | 172 | 174 | 176 | 178 | 180 | 182 | 184 | 186 | 188 | 190 | 192-254 |
| \( FAI(f_{C_3}) \) | 168 | 170 | 172 | 174 | 176 | 178 | 180 | 182 | 184 | 186 | 188 | 190 | 192-254 |
Class 3 ([33]). Let \( n \) be an positive integer. The orbit generated by \( x \in \mathbb{F}_2^n \) is defined as the set \( O_x = \{(x_1+i, x_2+i, \ldots, x_{n+i}) | i = 0, \ldots, n-1\} \) where the sum \( k+i (1 \leq k \leq n) \) is computed modulo \( n \) with the only exception that when \( k+i = n \).
1. Take odd \( n \geq 5 \);
2. Take an element \( x \in \mathbb{F}_2^n \) of weight \( \lfloor \frac{n}{2} \rfloor \) and generate the orbit \( O_x \);
3. Choose an orbit \( O_y \) by an element \( y \in \mathbb{F}_2^n \) of weight \( \lceil \frac{n}{2} \rceil \) such that for each \( x' \in O_x \) there is a unique \( y' \in O_y \) where \( \text{supp}(x') \subset \text{supp}(y') \);
4. Construct

\[
(7) \quad f_S(x) = \begin{cases} 
    f_m, & \text{if } x \in O_x \cup O_y, \\
    f_m + 1, & \text{elsewhere}
\end{cases}
\]

This class of functions has optimal algebraic immunity and nonlinearity \( 2^{n-1} - \binom{n-1}{\lfloor \frac{n}{2} \rfloor} + 2 \). For analysing the fast algebraic immunity of \( f_S \), we need the following lemma.

**Lemma 4.7.** Let \( n \geq 3 \) be an odd integer. There always exists \( h \in B_n \) with \( \text{Deg}(h) = 2 \) such that \( h(x) = 0 \) for \( x \in W[\frac{n}{2}] \cup W[\lceil \frac{n}{2} \rceil] \).

**Proof.** We define a symmetric Boolean function as \( g(x) = \lambda_\sigma(1)\sigma_1 + \lambda_\sigma(2)\sigma_2 \), where
- \( \lambda_\sigma(1) = 0 \) and \( \lambda_\sigma(2) = 1 \) if \( n = 8k+1 \);
- \( \lambda_\sigma(1) = 0 \) and \( \lambda_\sigma(2) = 1 \) if \( n = 8k+5 \);
- \( \lambda_\sigma(1) = 1 \) and \( \lambda_\sigma(2) = 1 \) if \( n = 8k+7 \);
- \( \lambda_\sigma(1) = 1 \) and \( \lambda_\sigma(2) = 1 \) if \( n = 8k+3 \).

Recall that \( v_\sigma(i) = \sum_{j \leq i} \lambda_\sigma(j) \) and \( \lambda_\sigma(i) = \sum_{j \leq i} v_\sigma(j) \). Then we can easily deduce that: \( v_\sigma(\lfloor \frac{n}{2} \rfloor) = v_\sigma(\lceil \frac{n}{2} \rceil) = 0 \) if \( n = 8k+1 \) or \( n = 8k+7 \); and \( v_\sigma(\lfloor \frac{n}{2} \rfloor) = v_\sigma(\lceil \frac{n}{2} \rceil) = 1 \) otherwise. Finally, we get the desired \( h \) by setting \( h = g \) or \( h = g+1 \).

**Theorem 4.8.** For \( 2^m \leq n < 2^{m+1} \). Let \( f_S \in B_n \) (odd \( n \geq 9 \)) be the function defined by (7). Then,

\[
\text{FAI}(f_S) \leq \begin{cases} 
    n - 2^{m-1} + 5, & \text{if } 2^m \leq n < 2^m + 2^{m-1} \\
    2^m + 4, & \text{if } 2^m + 2^{m-1} \leq n < 2^{m+1}
\end{cases}
\]

**Proof.** Let \( s' = f_m + f_S \). Clearly, \( \text{supp}(s') \subset \{x | \text{wt}(x) = \lfloor \frac{n}{2} \rfloor \text{ or } \lceil \frac{n}{2} \rceil \} \). By Lemma 4.7, we have \( \text{AI}(s') \leq 2 \). We can see that \( \text{Deg}(g') \geq 1 \) and \( \text{Deg}(g'(h+1)) \geq 1 \) for \( 2^m \leq n < 2^m + 2^{m-1} \), where \( h \) is defined in Lemma 4.7 and \( g' \) is defined in Lemma 4.3. Hence, by Theorem 4.4 we finish the proof.

In Table 3, we list the upper bounds on the fast algebraic immunity of \( f_S \) in small numbers of variables.

| odd \( n \) | 13-15 | 17 | 19 | 21 | 23 | 25-31 | 33 | 35 | 37 | 39 | 41 | 43 | 45 |
|------------|-------|---|---|---|---|-------|---|---|---|---|---|---|---|
| \( \text{FAI}(f_S) \) | 12 | 14 | 16 | 18 | 20 | 22 | 24 | 26 | 28 | 30 | 32 | 34 |   |

| odd \( n \) | 47 | 49-63 | 65 | 67 | 69 | 71 | 73 | 75 | 77 | 79 | 81 | 83 | 85 |
|------------|----|-------|---|---|---|---|---|---|---|---|---|---|---|
| \( \text{FAI}(f_S) \) | 86 | 86 | 88 | 90 | 92 | 94 | 96 | 98 | 100 | 102 | 104 | 106 | 108 |

| odd \( n \) | 133 | 145 | 147 | 149 | 151 | 153 | 155 | 157 | 159 | 161 | 163 | 165 | 167 |
|------------|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| \( \text{FAI}(f_S) \) |   | 168 | 168 | 169 | 170 | 172 | 174 | 176 | 178 | 180 | 182 | 184 | 186 |

| odd \( n \) | 169 | 171 | 173 | 175 | 177 | 179 | 181 | 183 | 185 | 187 | 189 | 191 | 193-205 |
|------------|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|------|
| \( \text{FAI}(f_S) \) |   | 210 | 211 | 212 | 213 | 214 | 215 | 216 | 217 | 218 | 219 | 220 | 221 |

| odd \( n \) | 109 | 112 | 114 | 116 | 118 | 120 | 122 | 124 | 126 | 128 | 130 | 132 | 134 |
|------------|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| \( \text{FAI}(f_S) \) |   | 145 | 145 | 146 | 147 | 148 | 149 | 150 | 151 | 152 | 153 | 154 | 155 |

**Table 3.** Upper bounds on the fast algebraic immunity of \( f_S \)
5. Conclusion

In this paper, we first derived a relation on the fast algebraic immunity between a Boolean function and its modifications. Then we obtained some upper bounds on the fast algebraic immunity of several known classes of modified majority functions with optimal algebraic immunity. We believe that our results will bring some useful insight into the perspective of designing candidates for the filter model of pseudo-random generators of stream ciphers.

Acknowledgments

We are grateful to Xiaohu Tang and Claude Carlet for their useful information. We wish to thank the anonymous reviewers for their detailed comments that improved the editorial as well as technical quality of this paper. The first author is supported by the National Natural Science Foundation of China (grants 61872435 and 61602394) and Guangxi Key Laboratory of Cryptography and Information Security (No. GCIS201724).

References

[1] F. Armknecht, Improving fast algebraic attacks, in Fast Software Encryption, 3017 (2004), 65–82.
[2] F. Armknecht, C. Carlet, P. Gaborit, S. Künzli, W. Meier and O. Ruatta, Efficient computation of algebraic immunity for algebraic and fast algebraic attacks, in Advances in Cryptology-EUROCRYPT 2006, Springer, 4004 (2006), 147–164.
[3] A. Braeken and B. Preneel, On the algebraic immunity of symmetric Boolean functions, in Progress in Cryptology-INDOCRYPT 2005, Springer, 3797 (2005), 35–48.
[4] A. Braeken, Cryptographic Properties of Boolean Functions and S-Boxes, PhD thesis, Catholic University of Louvain, 2006.
[5] A. Canteaut and M. Videau, Symmetric Boolean functions, IEEE Transactions on Information Theory, 51 (2005), 2791–2811.
[6] C. Carlet, On a weakness of the Tu-Deng function and its repair, IACR Cryptology EPrint Archive, Report 2009/696, URL http://eprint.iacr.org/2009/696.
[7] C. Carlet and D. Tang, Enhanced Boolean functions suitable for the filter model of pseudo-random generator, Designs, Codes and Cryptography, 76 (2015), 571–587.
[8] C. Carlet, X. Y. Zeng, C. L. Li and L. Hu, Further properties of several classes of Boolean functions with optimum algebraic immunity, Designs, Codes and Cryptography, 52 (2009), 303–338.
[9] Y. Chen and P. Lu, Two classes of symmetric Boolean functions with optimum algebraic immunity: Construction and analysis, IEEE transactions on information theory, 57 (2011), 2522–2538.
[10] N. T. Courtois, Fast algebraic attacks on stream ciphers with linear feedback, in Advances in Cryptology-CRYPTO 2003, Springer, 2729 (2003), 176–194.
[11] N. T. Courtois and W. Meier, Algebraic attacks on stream ciphers with linear feedback, in Advances in Cryptology-EUROCRYPT 2003, Springer, 2656 (2003), 345–359.
[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, 40 (2006), 41–58.
[13] J. F. Dillon, Elementary Hadamard Difference Sets, PhD thesis, Univ. of Maryland, 1974, 126 pp.
[14] C. Ding, G. Xiao and W. Shan, The Stability Theory of Stream Ciphers, Lecture Notes in Computer Science, 561. Springer-Verlag, Berlin, 1991.
[15] D. Dong, S. Fu, L. Qu and C. Li, A new construction of Boolean functions with maximum algebraic immunity, in Information Security, Springer, (2009), 177–185.
[16] K. Q. Feng, F. Liu, L. J. Qu and L. Wang, Constructing symmetric Boolean functions with maximum algebraic immunity, IEEE Transactions on Information Theory, 55 (2009), 2406–2412.
[17] S. Fu, C. Li, K. Matsuura and L. Qu, Construction of rotation symmetric Boolean functions with maximum algebraic immunity, in Cryptology and Network Security, Springer, (2009), 402–412.
[18] S. Fu, L. Qu, C. Li and B. Sun, Balanced rotation symmetric Boolean functions with maximum algebraic immunity, *IET Information Security*, 5 (2011), 93–99.
[19] P. Hawkes and G. G. Rose, Rewriting variables: The complexity of fast algebraic attacks on stream ciphers, in Advances in Cryptology–CRYPTO 2004, Springer, 3152 (2004), 390–406.
[20] 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, Springer, 4284 (2006), 84–98.
[21] M. C. Liu and D. D. Lin, Fast algebraic attacks and decomposition of symmetric Boolean functions, *IEEE Trans. Inform. Theory*, 57 (2011), 4817–4821, arXiv:0910.4632.
[22] M. C. Liu and D. D. Lin, Almost perfect algebraic immune functions with good nonlinearity, in 2014 IEEE International Symposium on Information Theory (ISIT), (2014), 1837–1841.
[23] M. C. Liu and D. D. Lin, Results on highly nonlinear Boolean functions with provably good immunity to fast algebraic attacks, *Information Sciences*, 421 (2017), 181–203, URL http://www.sciencedirect.com/science/article/pii/S002002551730926X.
[24] M. C. Liu, D. D. Lin and D. Y. Pei, Fast algebraic attacks and decomposition of symmetric Boolean functions, *IEEE Transactions on Information Theory*, 57 (2011), 4817–4821.
[25] M. C. Liu, Y. Zhang and D. D. Lin, Perfect algebraic immune functions, in Advances in Cryptology–ASIACRYPT 2012, Springer, 7658 (2012), 172–189.
[26] M. Lobanov, Tight bound between nonlinearity and algebraic immunity, IACR Cryptology ePrint Archive, Report 2005/441, URL http://eprint.iacr.org/2005/441.
[27] J. L. Massey, Shift-register synthesis and BCH decoding, *IEEE Transactions on Information Theory*, 15 (1969), 122–127.
[28] W. Meier, E. Pasalic and C. Carlet, Algebraic attacks and decomposition of Boolean functions, in Advances in Cryptology-EUROCRYPT 2004, Springer, 3027 (2004), 474–491.
[29] W. Meier and O. Staffelbach, Fast correlation attacks on stream ciphers, *J. Cryptology*, 1 (1989), 159–176.
[30] J. Peng, Q. S. Wu and H. B. Kan, On symmetric Boolean functions with high algebraic immunity on even number of variables, *IEEE Transactions on Information Theory*, 57 (2011), 7205–7220.
[31] L. J. Qu, C. Li and K. Q. Feng, A note on symmetric Boolean functions with maximum algebraic immunity in odd number of variables, *IEEE Transactions on Information Theory*, 53 (2007), 2908–2910.
[32] S. Ronjom and T. Helleseth, A new attack on the filter generator, *IEEE Transactions on Information Theory*, 53 (2007), 1752–1758.
[33] S. Sarkar and S. Maitra, Construction of rotation symmetric Boolean functions on odd number of variables with maximum algebraic immunity, in Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Springer, 4851 (2007), 271–280.
[34] T. Siegenthaler, Decrypting a class of stream ciphers using ciphertext only, *IEEE Transactions on Computers*, 34 (1985), 81–85.
[35] S. H. Su and X. H. Tang, Construction of rotation symmetric Boolean functions with optimal algebraic immunity and high nonlinearity, *Designs, Codes and Cryptography*, 71 (2014), 183–199.
[36] S. H. Su, X. H. Tang and X. Y. Zeng, A systematic method of constructing Boolean functions with optimal algebraic immunity based on the generator matrix of the Reed-Muller code, *Designs, Codes and Cryptography*, 72 (2014), 653–673.
[37] D. Tang, C. Carlet and X. H. Tang, A class of 1-resilient Boolean functions with optimal algebraic immunity and good behavior against fast algebraic attacks, *International Journal of Foundations of Computer Science*, 25 (2014), 763–780, http://dx.doi.org/10.1142/S0129054114500324.
[38] D. Tang, C. Carlet, X. H. Tang and Z. C. Zhou, Construction of highly nonlinear 1-resilient Boolean functions with optimal algebraic immunity and provably high fast algebraic immunity, *IEEE Transactions on Information Theory*, 63 (2017), 6113–6125.
[39] D. Tang, R. Luo and X. N. Du, The exact fast algebraic immunity of two subclasses of the majority function, *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences*, 99 (2016), 2084–2088.
[40] Q. C. Wang and T. Johansson, A note on fast algebraic attacks and higher order nonlinearities, in Information Security and Cryptology, Springer, 6584 (2010), 404–414.

Received for publication October 2018.

E-mail address: dtang@foxmail.com