Fast Algebraic Immunity of $2^m + 2$ & $2^m + 3$ variables Majority Function

Yindong Chen[a,*], Fei Guo[a], Liu Zhang[a]

[a] *College of Engineering, Shantou University, Shantou 515063, China*

Abstract

Boolean functions used in some cryptosystems of stream ciphers should satisfy various criteria simultaneously to resist some known attacks. The fast algebraic attack (FAA) is feasible if one can find a nonzero function g of low algebraic degree and a function h of algebraic degree significantly lower than n such that $f \cdot g = h$ [5]. Then one new cryptographic property fast algebraic immunity (FAI) was proposed in [6], which measures the ability of Boolean functions to resist FAAs. It is a great challenge to determine the exact values of the fast algebraic immunity of an infinite class of Boolean functions with optimal algebraic immunity. In this letter, we explore the exact fast algebraic immunity of two subclasses of the majority function.

Keywords: Fast algebraic immunity, Majority function, Algebraic immunity, Boolean function

1. Introduction

In recent years, more efforts have been made to investigate the FAI of Boolean functions. In 2012, Carlet-Feng function [3], a class of n-variable balanced Boolean functions with the optimal AI and good nonlinearity, was proved to have perfectly resistance to FAAs on $2^s + 1$ variables [6]. In 2014, another class of balanced even-variable Boolean functions with maximum AI and high nonlinearity, called T-C-T functions [4], was also proved to have almost optimal

*Correspondent author.
Email address: ydchen@stu.edu.cn (Yindong Chen)

resistance against FAAs [9]. In 2016, Tang et al. gave the exact FAI value $2^{m-1}+2$ of the majority function of 2^m and 2^m+1 variables [10]. In 2017, Tang et al. proposed a large family of 1-resilient Boolean functions having high lower bound on nonlinearity, optimal AI, optimal algebraic degree as well as provably FAI no less than $n-6$ [11]. This letter determines the exact FAI value of 2^m+2 and 2^m+3 variables ($m \geq 2$) majority function to equal $2^{m-1}+4$.

2. Preliminaries

Let $\mathbb{F}_2^n$ be the n-dimensional vector space over the finite field $\mathbb{F}_2 = \{0,1\}$. Then a Boolean function on n-variable can be viewed as a mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. Furthermore, any Boolean function f can be given by its truth table, which is a binary string of length 2^n listed as follows (lexicographic order):

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

Let $\mathcal{B}_n$ be the set of all n-variable Boolean functions. A Boolean function $f \in \mathcal{B}_n$ can also be seen as a multivariate polynomial over $\mathbb{F}_2$, which is called the algebraic normal form (ANF), that is

$$f(x_1, x_2, \cdots, x_n) = \bigoplus_{\alpha \in \mathbb{F}_2^n} c(\alpha) x^\alpha, \tag{1}$$

where $x^\alpha = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$ for $x = (x_1, x_2, \cdots, x_n)$, $\alpha = (a_1, a_2, \cdots, a_n)$, and $c(\alpha) \in \mathbb{F}_2$ can be determined by the Möbius transform

$$c(\alpha) = \bigoplus_{\beta \in \mathbb{F}_2^n, \beta \preceq \alpha} f(\beta) \tag{2}$$

where $\beta = (\beta_1, \beta_2, \cdots, \beta_n)$ and $\beta \preceq \alpha$ means that $\beta_i \leq \alpha_i$ for all $1 \leq i \leq n$. We denote by $\mathrm{wt}(\alpha)$ the Hamming weight of α. The algebraic degree of a Boolean function in formula (1) is defined as

$$\deg(f) = \max\{\mathrm{wt}(\alpha) | \alpha \in \mathbb{F}_2^n, c(\alpha) = 1\}.$$

A Boolean function is said to be symmetric if its output is invariant under any permutation of its input bits. Denote by $\mathcal{SB}_n$ the set of all n-variable

symmetric Boolean functions. Actually, for any $f \in \mathcal{SB}_n$, the ANF can be written as

$$f(x) = \bigoplus_{i=0}^{n} \lambda_f(i)\sigma_i, \tag{3}$$

where $\lambda_f(i) \in F_2$ and σ_i denotes the n-variable elementary symmetric Boolean function which consists of all terms of degree i, i.e., $\sigma_0 = 1$, $\sigma_1 = \bigoplus_{i=0}^{n-1} x_i$, $\sigma_2 = \bigoplus_{0\le i<j<n} x_i x_j, \cdots$, and $\sigma_n = x_0 x_1 \cdots x_{n-1}$.

Now we give the definition of algebraic immunity and fast algebraic immunity.

Definition 1. *([1]) The algebraic immunity (AI) of an n-variable Boolean function f is defined as*

$$\mathrm{AI}(f) = \min\{\deg(g) | g \neq 0, fg = 0 \text{ or } (f+1)g = 0\}.$$

For resisting the standard algebraic attacks, AI of an n-variable Boolean function should reach or close to this optimal bound $\lceil \frac{n}{2} \rceil$.

Definition 2. *([6]) The fast algebraic immunity (FAI) of a Boolean function $f \in B_n$ is the number*

$$\begin{aligned}\mathrm{FAI}(f) = \min\{&2\,\mathrm{AI}(f),\\ &\min\{\deg(g) + \deg(fg) | 1 \le \deg(g) < \mathrm{AI}(f)\}\}.\end{aligned}$$

Ref.[10] gave two properties about the FAI:

Lemma 1. *([10]) If $f \in \mathcal{B}_n$, then*

i) $\mathrm{FAI}(f) \le n$;

ii) $\mathrm{FAI}(f) = \mathrm{FAI}(f+1)$.

The majority function as a class of special symmetric Boolean functions has been used to construct more Boolean functions with optimal AI. Now we present definition of the majority function.

Definition 3. *([7]) The majority function is defined as*

$$f_M(x) = \begin{cases} 1, & \text{if } \mathrm{wt}(x) \ge \lceil \frac{n}{2} \rceil \\ 0, & \text{if } \mathrm{wt}(x) < \lceil \frac{n}{2} \rceil . \end{cases}$$

Lemma 2. *([2]) Let $f_M \in \mathcal{SB}_n$ be the majority function, then*

i) $\deg(f_M) = 2^{\lfloor \log_2 n \rfloor}$;

ii) $\mathrm{AI}(f_M) = \lceil \frac{n}{2} \rceil$.

Ref. [8] presented a precious result on the behavior of the majority function against FAAs.

Theorem 1. ([8]) Let f_M be the majority function of n-variable, where $n \geq 2$. There exist Boolean Functions g and h such that $f_M g = h$, where $d = \deg(h) = \lfloor n/2 \rfloor + 1$ and $e = \deg(g) = d - 2^j$, and where j is the maximum number such that $e > 0$.

Ref.[10] deduced this result as an intuitive conclusion, which is presented in Lemma 3.

Lemma 3. ([10]) Let f_M be the majority function of n-variable, where $2^m \leq n < 2^{m+1}$. Then $\mathrm{FAI}(f_M) \leq n - 2^{m-1} + c$, where $c = 2$ for even n and $c = 1$ for odd n.

3. Main Result

Now we explore the exact FAI of the majority function on $2^m + 2$ and $2^m + 3$ variables ($m \geq 2$).

Lemma 4. *Let $2^m + 2 \leq n < 2^{m+1}$ with $m \geq 2$ and $f_M \in \mathcal{SB}_n$ be the majority function. For any n-variable Boolean function g with $\deg(g) = 1$, then $\deg(f_M g) = \deg(f_M) + 1$.*

Proof. From Lemma 2 we know $\deg(f_M) = 2^{\lfloor \log_2 n \rfloor} = 2^m$, which by formula (3) implies that the ANF of f_M consists of all terms with degree 2^m. For proving $\deg(f_M g) = 2^m + 1$, we only need to find one term with degree $2^m + 1$ appears odd times in $f_M g$.

i) Suppose $g(x) = x_0 + x_1 + \cdots + x_{n-1}$. Then $x_0 x_1 \cdots x_{2^m}$ appears $2^m + 1$ times in $f_M g$.

ii) Suppose $g(x) = x_0 + x_1 + \cdots + x_{n-1} - x_i$, where $0 \leq i \leq n-1$. For convenience, let $i = n-1$, then x_i makes no influence to the situation in i). So $x_0 x_1 \cdots x_{2^m}$ appears $2^m + 1$ times in $f_M g$.

iii) Suppose $g(x) = x_0 + x_1 + \cdots + x_{n-1} - X_1$, where X_1 express addition of even number of different x_i's with $0 \leq i \leq n-1$. For convenience, let $X_1 = x_0 + x_1 + \cdots + x_l$ where l is odd and $l < n-1$, then $x_0 x_1 \cdots x_{2^m}$ appears $2^m + 1 - (l+1) = 2^m - l$ times in $f_M g$, which is odd obviously.

iv) Suppose $g(x) = x_0 + x_1 + \cdots + x_{n-1} - X_1 - x_j$, where $0 \leq j \leq n-1$ and x_j is not contained in X_1. For convenience, let $X_1 = x_0 + x_1 + \cdots + x_l$ where l is odd and $l < n-2$, $x_j = x_{n-1}$, then x_j makes no influence to the situation in iii). So $x_0 x_1 \cdots x_{2^m}$ appears $2^m - l$ times in $f_M g$.

It is obvious that whether ANF of g consists of term '1' makes no influence to the degree of $f_M g$. Because of the high symmetry of majority function, we can infer that for all $\deg(g) = 1$, there always exists a term with degree $2^m + 1$ appears odd times. This completes the proof. □

Lemma 5. Let $2^m + 2 \leq n < 2^{m+1}$ with $m \geq 2$ and $f_M \in \mathcal{SB}_n$ be the majority function. Define $\mathrm{A} = \min\{\deg(h) | f_M h = 0, h \neq 0\}$. Then $\mathrm{FAI}(f_M) \geq \mathrm{A} + 2 \geq \mathrm{AI}(f_M) + 2$.

Proof. Firstly,

$$\min_{1 \leq \deg(g) < \mathrm{AI}(f_M + 1)} \{\deg(g) + \deg((f_M + 1)g)\} \geq \mathrm{A} + 2 \geq \mathrm{AI}(f_M) + 2$$

is an immediate consequence because of the following three facts:

- $\mathrm{AI}(f_M) \leq \mathrm{A} \leq \deg(f_M)$ because $f_M(f_M + 1) = 0$, $f_M + 1 \neq 0$ and $\deg(f_M + 1) = \deg(f_M)$;
- $\mathrm{AI}(f_M) = \mathrm{AI}(f_M + 1)$, by Definition 1;
- if $\deg(g) = 1$ we have $\deg((f_M + 1)g) = \deg(f_M) + 1 \geq \mathrm{A} + 1$ by Lemma 4; if $\deg(g) \geq 2$ we have $\deg((f_M + 1)g) \geq \mathrm{A}$ since $f_M(f_M + 1)g = 0$ and $(f_M + 1)g \neq 0$.

Secondly, $2\,\mathrm{AI}(f_M+1) \geq \mathrm{A}+2$ holds since:

- $\mathrm{A} \leq \deg(f_M+1) = 2^m$, by Lemma 2;
- $\mathrm{AI}(f_M) = \mathrm{AI}(f_M+1)$, by Definition 1;
- when $2^m+2 \leq n < 2^{m+1}$, by Lemma 2, for even n, $2\,\mathrm{AI}(f_M) = n$ and for odd n, $2\,\mathrm{AI}(f_M) = n+1$. Both the two cases indicate that $2\,\mathrm{AI}(f_M+1) \geq 2^m+2 \geq \mathrm{A}+2$.

Therefore, by Definition 2 and Lemma 1, for $2^m+2 \leq n < 2^{m+1}$ with $m \geq 2$ we have

$$\mathrm{FAI}(f_M) = \mathrm{FAI}(f_M+1) \geq \mathrm{A}+2 \geq \mathrm{AI}(f_M)+2.$$

□

Now we give an lower bound on the FAI of $2^m+2 \leq n < 2^{m+1}$ $(m \geq 2)$ variables majority functions.

Lemma 6. Let $f_M \in \mathcal{SB}_n$ be the majority function with $2^m+2 \leq n < 2^{m+1}$ where $m \geq 2$. Then $\mathrm{FAI}(f_M) \geq \lfloor \frac{n}{2} \rfloor + 3$.

Proof. There are two cases:

i) Even n. By Lemma 5, we only need to prove that f_M has no nonzero annihilator with algebraic degree less than $\frac{n}{2}+1$. It suffices to prove that $f'_M(x_1,\cdots,x_n) = f_M(x_1+1,\cdots,x_n+1)$ has no nonzero annihilator with algebraic degree less than $\frac{n}{2}+1$ since if there exists a nonzero function g of algebraic degree less than $\frac{n}{2}+1$ such that $f'_M g = 0$ then we have $f_M g' = 0$ where $g'(x_1,\cdots,x_n) = g(x_1+1,\cdots,x_n+1)$. Assume that g is an annihilator of f'_M with $\deg(g) \leq \frac{n}{2}$. Let the ANF of $g(x)$ be

$$g(x) = \bigoplus_{\alpha \in \mathbb{F}_2^n, \mathrm{wt}(\alpha) \leq n/2} c(\alpha) x^\alpha,$$

Since g is an annihilator of f'_M, $g(x) = 0$ for every x with $\mathrm{wt}(x) \leq \frac{n}{2}$. Then we have $c(\alpha) = 0$ for any $\alpha \in \mathbb{F}_2^n$ with $\mathrm{wt}(\alpha) \leq n/2$ by formula (2). This implies that $g = 0$ and hence f'_M has no nonzero annihilator with algebraic degree less than $\frac{n}{2}+1$.

ii) Odd n. It follows from Lemma 5 that $\mathrm{FAI}(f_M) \geq \mathrm{AI}(f_M) + 2 = \lfloor \frac{n}{2} \rfloor + 3$.

□

By Lemma 3 and Lemma 6, we get our main theorem:

Theorem 2. Let $f_M \in \mathcal{SB}_n$ be the majority function with $n \in \{2^m+2, 2^m+3\}$ where $m \geq 2$. Then $\mathrm{FAI}(f_M) = 2^{m-1} + 4$.

4. Conclusion

In this letter, we give a lower bound of the fast algebraic immunity of n-variable (where $2^m + 2 \leq n < 2^{m+1}$, $m \geq 2$) majority function. Combining with previous work, we determine that the exact fast algebraic immunity value of the majority function of $2^m + 2$ and $2^m + 3$ variables ($m \geq 2$) equals $2^{m-1} + 4$.

References

[1] Meier W, Pasalic E, Carlet C. Algebraic attacks and decomposition of Boolean functions. In: Advances in Cryptology-EUROCRYPT 2004, in: LNCS, 2004. 3027: 474-491.

[2] Dalai D K, Maitra S, Sarkar S. Basic theory in construction of Boolean functions with maximum possible annihilator immunity. Designs Codes and Cryptography, 2006, 40(1): 41-58.

[3] Carlet C, Feng K Q. An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity. In: Advances in Cryptology-ASIACRYPT 2008, in: LNCS, 2008. 5350: 425-440.

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

[5] Hawkes P, Rose G G. Rewriting variables: The complexity of fast algebraic attacks on stream ciphers. in: Advances in Cryptology. Berlin, Germany: Springer, 2004. 390-406.

[6] Liu M C, Lin D D, Pei D Y. Fast algebraic attacks and decomposition of symmetric Boolean functions. IEEE Trans Inf Theory, 2011, 57 (7): 4817-4821.

[7] Ding C S, Xiao G, Shan W. The stability theory of stream ciphers. In: LNCS, Springer, Heidelberg, 1991.

[8] Armknecht F, Carlet C, Gaborit P, et al. Efficient computation of algebraic immunity for algebraic and fast algebraic attacks. In Proc Adv Cryptol-EUROCRYPT, 2006. 4004: 147-164.

[9] Liu M C, Lin D D. Almost perfect algebraic immune functions with good nonlinearity. 2014 IEEE International Symposium on Information Theory, 2014. 1837-1841.

[10] Tang D, Luo R, Du X N. The exact fast algebraic immunity of two subclasses of the majority function. IEICE Trans Fundamentals, 2016, E99-A(11): 2084-2088.

[11] Tang D, Carlet C, Tang X H, Zhou Z C. Construction of Highly Nonlinear 1-Resilient Boolean Functions With Optimal Algebraic Immunity and Provably High Fast Algebraic Immunity. IEEE Trans Inf Theory, 2017, 63 (9): 6113-6125.