On the Existence of Boolean Functions with Optimal Resistance against Fast Algebraic Attacks

Yusong Du, and Fangguo Zhang

***Abstract*—It has been pointed out that an n-variable Boolean function f has optimal resistance against fast algebraic attacks if and only if there does not exist a nonzero n-variable Boolean function g of degree lower than $\frac{n}{2}$ such that $fg = h$ and $\deg(g) + \deg(h) < n$. In this corresponding, we show that there does not exist an n-variable Boolean function with optimal resistance against fast algebraic attacks for most values of n.**

***Index Terms*—stream ciphers, fast algebraic attacks, Boolean functions.**

I. INTRODUCTION

Boolean functions used in stream ciphers should have large algebraic immunity (AI) in order to resist algebraic attacks [1], [2]. Constructing Boolean functions with the maximum AI (MAI Boolean functions) and studying their cryptographic properties have been received attention for years [3]–[6].

The existence of low degree multiples (or low degree annihilators) of Boolean functions is necessary for an efficient algebraic attack. Boolean functions with large AI can resist algebraic attacks since large AI guarantees the non-existence of low degree multiples. However, Boolean functions with large AI (even the maximum AI) may not resist fast algebraic attacks (FAA's) [7], [8]. This is because the existence of low degree multiples of Boolean functions is not necessary any more for FAA's. Indeed, for an n-variable Boolean function f, if there exists a nonzero n-variable Boolean function g of low degree such that fg has reasonable algebraic degree (not large with respect to n) then a fast algebraic attack is feasible. The fast algebraic attack has been exploited in [9] to present an attack on SFINKS [10], though the cipher was designed to withstand standard algebraic attack. Therefore the resistance of Boolean functions against FAA's should be considered as another necessary cryptographic property for Boolean functions.

Just like constructing MAI Boolean functions to resist algebraic attacks, finding Boolean functions with optimal resistance against FAA's is also interesting. The study shows that an n-variable Boolean function f has *optimal resistance against FAA's* if and only if there does not exist a nonzero n-variable Boolean function g of degree lower than $\frac{n}{2}$ such that $fg = h$ and $\deg(g) + \deg(h) < n$ [5], [7], [11]. The concept of the optimal resistance against FAA's for Boolean functions can be implied from [7], but it is was firstly pointed out informally by Carlet *et al.* in [5] as far as we know.

In resent years several efforts have been made to construct Boolean functions with good resistance against FAA's, but except some instances none of them gave a class of Boolean functions which can be proven

Y. Du and F. Zhang are with the School of Information Management and the School of Information Science and Technology respectively, Sun Yat-sen University, Guangzhou, 510006 P. R. China (e-mail: yusongdu@hotmail.com, isszhfg@mail.sysu.edu.cn).

Manuscript received ; revised

to have optimal resistance against FAA's. In [5] Carlet *et al.* observed through computer experiments by Armknecht's algorithm in [12] that the class of balanced MAI Boolean functions constructed by them may have good behavior against FAA's. E. Pasalic constructed a class of balanced Boolean functions with good resistance against FAA's (called 'almostly' optimal resistance) [13]. M. Liu *et al.* proved that there does not exist a symmetric Boolean function with optimal resistance against FAA's [14]. X. Zeng *et al.* constructed some balanced MAI Boolean functions based on univariate polynomial representation which can be verified to have good resistance against FAA's [15].

In this corresponding, we consider again the optimal resistance of Boolean functions against FAA's. We show that there does not exist an n-variable Boolean function with optimal resistance against fast algebraic attacks for most values of n.

II. Some Notations

Let n be a positive integer. We denote by $\mathbb{B}_n$ the set of all the n-variable Boolean functions.

An n-variable Boolean function f may be viewed as a mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ and has a unique n-variable polynomial representation over $\mathbb{F}_2[x_1, x_2, \cdots, x_n]/(x_1^2 - x_1, x_2^2 - x_2, \cdots, x_n^2 - x_n)$, called the *algebraic normal form* (ANF) of f,

$$f(x) = f(x_1, x_2, \cdots, x_n) = \sum_{\alpha \in \mathbb{F}_2^n} f_\alpha x^\alpha,$$

where $x = (x_1, x_2, \cdots, x_n)$ is a set of binary variables, $\alpha = (a_1, a_2, \cdots, a_n) \in \mathbb{F}_2^n$ and $f_\alpha \in \mathbb{F}_2$ is the coefficient of monomial $x^\alpha = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$.

Let $\mathrm{supp}(\alpha) = \{i \,|\, a_i = 1, 1 \le i \le n\}$. The Hamming weight of α, denoted by $|\alpha|$, is the number of elements in $\mathrm{supp}(\alpha)$. The algebraic degree of Boolean function $f \in \mathbb{B}_n$, denoted by $\deg(f)$, can be given by the largest integer $d = |\alpha|$ such that $f_\alpha \neq 0$.

For $\alpha, \beta \in \mathbb{F}_2^n$, we say that α is covered by β if $\mathrm{supp}(\alpha) \subseteq \mathrm{supp}(\beta)$. For the sake of simplicity, $\mathrm{supp}(\alpha) \subseteq \mathrm{supp}(\beta)$ is written as $\alpha \subseteq \beta$.

For $f \in \mathbb{B}_n$ the following equation is well-known,

$$f_\beta = \sum_{\alpha \subseteq \beta} f(\alpha). \tag{1}$$

where $\beta \in \mathbb{F}_2^n$ is a fixed vector and f_β is the coefficient of monomial x^β in the ANF of f.

III. Prepared Work

As mentioned in Section 1 (Introduction), $f \in \mathbb{B}_n$ has optimal resistance against FAA's if and only if $\deg(fg) + \deg(g) \ge n$ holds for any nonzero n-variable Boolean function g of degree less than $\frac{n}{2}$. It clear that the optimal resistance against FAA's does not make sense for Boolean functions in 1 variables or 2 variables. We always let $n \ge 3$ in the following content of this corresponding.

Without loss of generality we let $\deg(fg) < 0$ if $fg = 0$. In other words, f has optimal resistance against FAA's if and only if $\deg(fg) \ge n - e$ holds for any nonzero n-variable Boolean function g of degree not more than e and $1 \le e \le \lceil \frac{n}{2} \rceil - 1$. Therefore it is inevitable to study the algebraic degree of Boolean function fg. About this F. Armknecht *et al.* gave an observation in [12].

Lemma 1: [12] For $f, g \in \mathbb{B}_n$, let $f(x) = \sum_{\alpha \in \mathbb{F}_2^n} f_\alpha x^\alpha$ and $g(x) = \sum_{\beta \in \mathbb{F}_2^n} g_\beta x^\beta$. Set $h(x) = f(x) \cdot g(x) = \sum_{\gamma \in \mathbb{F}_2^n} h_\gamma x^\gamma$. Then h_γ, the coefficient of monomial x^γ in the ANF of h, satisfies

$$h_\gamma = \sum_{\beta \subseteq \gamma} g_\beta \sum_{\beta \subseteq \alpha \subseteq \gamma} f(\alpha).$$

We only need to consider $g \in \mathbb{B}_n$ such that $\deg(g) \le e$, i.e., with the notations in Lemma 1,

we suppose that $g_\beta = 0$ for $|\beta| > e$. Then $h_\gamma = \sum_{\beta\subseteq\gamma,|\beta|\leq e} g_\beta \sum_{\beta\subseteq\alpha\subseteq\gamma} f(\alpha)$. Therefore $\deg(fg) \geq n-e$ holds for Boolean function g with $\deg(g) \leq e$ if and only if

$$h_\gamma = \sum_{\beta\subseteq\gamma,|\beta|\leq e} g_\beta \sum_{\beta\subseteq\alpha\subseteq\gamma} f(\alpha)$$

is nonzero for some γ with $|\gamma| \geq n-e$. This implies the following fact.

Lemma 2: Let $f \in \mathbb{B}_n$, e be a fixed integer and $1 \leq e \leq \lceil \frac{n}{2} \rceil - 1$. $\deg(fg) \geq n-e$ holds for any nonzero n-variable Boolean function g with $\deg(g) \leq e$ if and only if homogenous linear system

$$\sum_{\beta\subseteq\gamma,|\beta|\leq e} \left(\sum_{\beta\subseteq\alpha\subseteq\gamma} f(\alpha) \right) g_\beta = 0 \qquad |\gamma| \geq n-e, \quad (2)$$

has only zero solution, where all the g_β such that $|\beta| \leq e$ are viewed as the unknowns of the system.

According to Lemma 2, if $\deg(fg) \geq n-e$ holds for any nonzero n-variable Boolean function g with $\deg(g) \leq e$ if and only if the coefficient matrix of system (2) has full column rank.

We denote by $W_e(f)$ the coefficient matrix of system (2). Every entry of $W_e(f)$ can be denoted by

$$w_{\gamma\beta} = \sum_{\beta\subseteq\alpha\subseteq\gamma} f(\alpha),$$

where $|\beta| \leq e$ and $|\gamma| \geq n-e$. Without loss of generality we let $w_{\gamma\beta} = 0$ if $\beta \nsubseteq \gamma$. It is clear that $W_e(f)$ is an $E \times E$ matrix with $E = \sum_{i=0}^{e} \binom{n}{i}$ since the number of the elements of Hamming weight not more than e and the number of the elements of Hamming weight not less than $n-e$ in $\mathbb{F}_2^n$ are both equal to $E = \sum_{i=0}^{e} \binom{n}{i}$.

Recalling the definition of the optimal resistance of Boolean functions against FAA's we can obtain a sufficient and necessary condition for Boolean functions to have optimal resistance against FAA's.

Theorem 1: Let $f \in \mathbb{B}_n$. f has optimal resistance against FAA's if and only if $W_e(f)$ is invertible for every integer $e = 1, 2, \cdots, \lceil \frac{n}{2} \rceil - 1$.

For $\alpha = (a_1, a_2, \cdots, a_n)$, $\beta = (b_1, b_2, \cdots, b_n)$ and $\gamma = (c_1, c_2, \cdots, c_n)$, we can define

$$\alpha + \beta = (a_1 + b_1, a_2 + b_2, \cdots, a_n + b_n) \in \mathbb{F}_2^n,$$

$$\begin{aligned} \alpha \cup \beta &= (a_1 + b_1 + a_1 b_1, a_2 + b_2 + a_2 b_2, \\ &\quad \cdots, a_n + b_n + a_n b_n) \in \mathbb{F}_2^n, \end{aligned}$$

and

$$\begin{aligned} \gamma \setminus \beta &= (c_1 - b_1, c_2 - b_2, \cdots, c_n - b_n) \\ &= (c_1 + b_1, c_2 + b_2, \cdots, c_n + b_n) \\ &= \gamma + \beta \in \mathbb{F}_2^n \end{aligned}$$

when $\beta \subseteq \gamma$. About the entry of $W_e(f)$ we can further prove the following result with the notations above.

Proposition 1: Let $\beta \subseteq \gamma$. Every entry of $W_e(f)$ satisfies

$$w_{\gamma\beta} = \sum_{\delta\subseteq\beta} f_{\gamma+\delta}.$$

where $f_{\gamma+\delta} \in \mathbb{F}_2$ is the coefficient of the monomial $x^{\gamma+\delta}$ in the ANF of f.

Proof: Since $w_{\gamma\beta} = \sum_{\beta\subseteq\alpha\subseteq\gamma} f(\alpha)$, we have

$$\begin{aligned} \sum_{\beta\subseteq\alpha\subseteq\gamma} f(\alpha) &= \sum_{\alpha\subseteq\gamma\setminus\beta} f(\alpha \cup \beta) \\ &= \sum_{\alpha\subseteq\gamma\setminus\beta} \sum_{\delta\subseteq\beta} f(\alpha \cup \delta) \sum_{\delta\subseteq\theta\subseteq\beta} 1 \\ &= \sum_{\alpha\subseteq\gamma\setminus\beta} \sum_{\delta\subseteq\beta} \sum_{\delta\subseteq\theta\subseteq\beta} f(\alpha \cup \delta) \\ &= \sum_{\alpha\subseteq\gamma\setminus\beta} \sum_{\theta\subseteq\beta} \sum_{\delta\subseteq\theta} f(\alpha \cup \delta) \end{aligned}$$

Exchanging the order of the sums, we have

$$\begin{aligned} \sum_{\beta\subseteq\alpha\subseteq\gamma} f(\alpha) &= \sum_{\theta\subseteq\beta} \sum_{\alpha\subseteq\gamma\setminus\beta} \sum_{\delta\subseteq\theta} f(\alpha \cup \delta) \\ &= \sum_{\theta\subseteq\beta} \sum_{\alpha\subseteq(\gamma\setminus\beta)\cup\theta} f(\alpha) \\ &= \sum_{\delta\subseteq\beta} \sum_{\alpha\subseteq\gamma\setminus\delta} f(\alpha) \end{aligned}$$

Recalling Equation (1), we have

$$\sum_{\delta\subseteq\beta}\sum_{\alpha\subseteq\gamma\backslash\delta} f(\alpha)=\sum_{\delta\subseteq\beta} f_{\gamma\backslash\delta}=\sum_{\delta\subseteq\beta} f_{\gamma+\delta}.$$

This completes the proof. ∎

Proposition 1 means that given the ANF of f matrix $W_e(f)$, the coefficient matrix of system (2), can be obtained directly.

IV. About Matrix $W_e(f)$

From the discussion in section 3, for $f\in\mathbb{B}_n$, we see that the optimal resistance of f against FAA's can be determined by the invertibility of a set of binary matrixes, i.e., $W_e(f)$ with $1\le e\le\lceil\frac{n}{2}\rceil$ and the entries of $W_e(f)$ can be obtained according to the coefficients of monomials in the ANF of f. In this section we show that $W_e(f)$ can be changed into a symmetric matrix over $\mathbb{F}_2$ by applying some elementary transformations.

In order to further discuss the properties of $W_e(f)$, we need to fix the order of rows and columns in $W_e(f)$. We consider the following order for vectors in $\mathbb{F}_2^n$, which was also considered in [16] to reduce the problem on finding annihilators of Boolean functions for algebraic attacks and in [4] to construct MAI Boolean functions.

Definition 1: Let $\alpha=(a_1,a_2,\cdots,a_n)$, $\beta=(b_1,b_2,\cdots,b_n)\in\mathbb{F}_2^n$. We define $\alpha\prec\beta$ if and only if $|\alpha|<|\beta|$, or when $|\alpha|=|\beta|$ there exists $1\le i<n$ such that $a_i=1$, $b_i=0$ and $a_j=b_j$ for $1\le j<i$.

Consider three vectors in $\mathbb{F}_2^5$: $\alpha=(11000)$, $\beta=(01101)$ and $\gamma=(01011)$. According to Definition 1, $\alpha\prec\beta$ since $|\alpha|<|\beta|$, while $|\beta|=|\gamma|$ but there exists $i=3$ satisfying the definition, thus $\beta\prec\gamma$.

According to $\prec$, we can list all the vectors $\beta,\gamma\in\mathbb{F}_2^n$ such that $|\beta|\le e$ and $|\gamma|\ge n-e$ as follows

$$\beta^1\prec\beta^2\prec\cdots\prec\beta^E \quad\text{and}\quad \gamma^1\prec\gamma^2\prec\cdots\prec\gamma^E,$$

where $E=\sum_{i=0}^{e}\binom{n}{i}$. It is not hard o see that $|\beta^j|=k_1$ with $1\le k_1\le e$ and $|\gamma^i|=k_2$ with $n-e\le k_2\le n-1$ for

$$\sum_{l=0}^{k_1-1}\binom{n}{l}+1\le j\le\sum_{l=0}^{k_1}\binom{n}{l}$$

and

$$\sum_{l=0}^{k_2-1}\binom{n}{l}+1\le i\le\sum_{l=0}^{k_2}\binom{n}{l}$$

respectively. Particularly, $|\beta^1|=\mathbf{0}$ and $|\gamma^E|=(\underbrace{11\cdots1}_{n})$.

We give several useful facts about $\prec$ to help understanding Definition 1. For $\alpha=(\alpha_1,\alpha_2,\cdots,\alpha_n)\in\mathbb{F}_2^n$, we denote by $\bar{\alpha}$ the complement of vector α, i.e.,

$$\bar{\alpha}=\alpha+(\underbrace{11\cdots1}_{n})=(\alpha_1+1,\alpha_2+1,\cdots,\alpha_n+1)\in\mathbb{F}_2^n.$$

It is easy to see that $|\bar{\alpha}|=n-|\alpha|$ and $\alpha\prec\beta$ implies $\bar{\beta}\prec\bar{\alpha}$. Then for all the vectors $\beta,\gamma\in\mathbb{F}_2^n$ such that $|\beta|\le e$ and $|\gamma|\ge n-e$, we have

$$\overline{\gamma^E}\prec\overline{\gamma^{E-1}}\prec\cdots\prec\overline{\gamma^1} \quad\text{and}\quad \overline{\beta^E}\prec\overline{\beta^{E-1}}\prec\cdots\prec\overline{\beta^1},$$

which imply

$$\overline{\gamma^E}=\beta^1\prec\overline{\gamma^{E-1}}=\beta^2\prec\cdots\prec\overline{\gamma^1}=\beta^E$$

and

$$\overline{\beta^E}=\gamma^1\prec\overline{\beta^{E-1}}=\gamma^2\prec\cdots\prec\overline{\beta^1}=\gamma^E$$

which also mean that

$$\overline{\gamma^i}=\beta^{E-i+1} \quad\text{and}\quad \overline{\beta^j}=\gamma^{E-j+1} \tag{3}$$

for $1\le i\le E$ and $1\le j\le E$.

According to Definition 1 for $1\le i\le E$ and $1\le j\le E$ the entry on row i and column j of $W_e(f)$, denoted by $w_{ij}=w_{\gamma^i\beta^j}$, makes sense. After fixing the order of rows and columns in $W_e(f)$, an explicit description of $W_e(f)$ can be given.

Definition 2: Let $E=\sum_{i=0}^{e}\binom{n}{i}$. $W_e(f)$ is defined to be an $E\times E$ matrix over $\mathbb{F}_2$ such that its entry on row i and column j, denoted by w_{ij}, is equal to $\sum_{\delta\subseteq\beta^j} f_{\gamma^i+\delta}$ if $\beta^j\subseteq\gamma^i$ and zero otherwise.

With the explicit description of $W_e(f)$ given by Definition 2, we begin to prove that $W_e(f)$ can be

changed into a symmetric matrix over $\mathbb{F}_2$ by applying some elementary transformations. The proof consists of four propositions, i.e., from Proposition 2 to Proposition 5 as follows. For the sake of simplicity, in the following content, we always let $1 \leq e < \lceil \frac{n}{2} \rceil$ and $E = \sum_{i=0}^{e} \binom{n}{i}$.

Proposition 2: Let $1 \leq i \leq E$ and $1 \leq j \leq E$. Applying some elementary column transformations, $W_e(f)$ can be changed into a matrix with the entry on row i and column j equal to $f_{\gamma^i+\beta^j}$ if $\beta^j \subseteq \gamma^i$.

Proof: The entries on the first column of $W_e(f)$ are $f_{\gamma^1+\beta^1}$, $f_{\gamma^2+\beta^1}$, $\cdots$, and $f_{\gamma^E+\beta^1}$ respectively.

Since $|\beta^j| = 1$ for $j = 2, 3, \cdots, \sum_{l=0}^{1} \binom{n}{l}$ we have

$$w_{ij} = \begin{cases} f_{\gamma^i+\beta^j} + f_{\gamma^i+\beta^1} & \text{if } \beta^j \subseteq \gamma^i \\ 0 & \text{if } \beta^j \nsubseteq \gamma^i \end{cases}.$$

We add the first column to column j with $2 \leq j \leq \sum_{l=0}^{1} \binom{n}{l}$ in $W_e(f)$, then w_{ij} with $|\beta^j| = 1$ is changed into $f_{\gamma^i+\beta^j}$ if $\beta^j \subseteq \gamma^i$ and $f_{\gamma^i+\beta^1}$ otherwise.

For $j = \sum_{l=0}^{1} \binom{n}{l} + 1, \sum_{l=0}^{1} \binom{n}{l} + 2, \cdots, \sum_{l=0}^{2} \binom{n}{l}$ we have $|\beta^j| = 2$ and

$$w_{ij} = \begin{cases} f_{\gamma^i+\beta^j} + \sum_{\substack{1 \leq k < j \\ \beta^k \subseteq \beta^j}} f_{\gamma^i+\beta^k} & \text{if } \beta^j \subseteq \gamma^i \\ 0 & \text{if } \beta^j \nsubseteq \gamma^i \end{cases}.$$

We add all the columns corresponding to k to column j in $W_e(f)$ for every $j = \sum_{l=0}^{1} \binom{n}{l} + 1, \sum_{l=0}^{1} \binom{n}{l} + 2, \cdots, \sum_{l=0}^{2} \binom{n}{l}$, then w_{ij} is changed into

$$w_{ij} + \sum_{1 \leq k < j,\, \beta^k \subseteq \beta^j} w_{ik}$$

if $\beta^j \subseteq \gamma^i$. Note that k in the sum satisfies $|\beta^k| \leq 1$ and w_{ik} with $|\beta^k| = 1$ has been changed into $f_{\gamma^i+\beta^k}$ if $\beta^k \subseteq \gamma^i$. Then w_{ij} with $|\beta^j| = 2$ is changed into $f_{\gamma^i+\beta^j}$ if $\beta^j \subseteq \gamma^i$.

We continue to do similar operations on $W_e(f)$ for

$$\sum_{l=0}^{2} \binom{n}{l} + 1 \leq j \leq \sum_{l=0}^{3} \binom{n}{l},$$
$$\sum_{l=0}^{3} \binom{n}{l} + 1 \leq j \leq \sum_{l=0}^{4} \binom{n}{l},$$
$$\cdots\cdots$$
and up to
$$\sum_{l=0}^{e-1} \binom{n}{l} + 1 \leq j \leq E,$$

i.e., for columns corresponding to k such that $|\beta^k| = 3, 4, \cdots, e$ respectively.

It is not hard to see that by the elementary column transformations above $W_e(f)$ is changed into a new matrix and w_{ij} in $W_e(f)$ with $1 \leq i \leq E$ and $1 \leq j \leq E$ is changed into $f_{\gamma^i+\beta^j}$ if $\beta^j \subseteq \gamma^i$. ■

In Proposition 2 $W_e(f)$ is changed into a new matrix. For the sake of simplicity, we denote by $\bar{W}_e(f)$ the new matrix and by $\bar{w}_{ij}$ the entry on row i and column j in the new matrix.

For any $\beta, \gamma \in \mathbb{F}_2^n$, we can define

$$\gamma \cap \beta = (c_1 b_1, c_2 b_2, \cdots, c_n b_n) \in \mathbb{F}_2^n.$$

Proposition 3: Let $1 \leq i \leq E$ and $1 \leq j \leq E$. If $\beta^j \cap \gamma^i = \mathbf{0}$ then $\bar{w}_{ij}$ is equal to $f_{\gamma^i+\beta^1}$.

Proof: It is clear that $\beta^j \nsubseteq \gamma^i$ if $\beta^j \cap \gamma^i = \mathbf{0}$ and $\beta^j \neq \mathbf{0}$. Then $\bar{w}_{ij} = f_{\gamma^i+\beta^1}$ for $|\beta^j| \leq 1$ and $\beta^j \cap \gamma^i = \mathbf{0}$. Without loss of generality we suppose that $\bar{w}_{ij} = f_{\gamma^i+\beta^1}$ for $|\beta^j| \leq l$, $1 \leq l < e$ and $\beta^j \cap \gamma^i = \mathbf{0}$. Then for $|\beta^j| = l + 1$ and $\beta^j \cap \gamma^i = \mathbf{0}$, we have

$$\bar{w}_{ij} = \sum_{1 \leq k < j,\, \beta^k \subseteq \beta^j} \bar{w}_{ik},$$

where k satisfies $|\beta^k| \leq l$, $\beta^k \cap \gamma^i = \mathbf{0}$ and there are $\binom{l+1}{0} + \binom{l+1}{1} + \cdots + \binom{l+1}{l} = 2^{l+1} - 1$ in all k's such that $|\beta^k| \leq l$. Thus $\bar{w}_{ij} = f_{\gamma^i+\beta^1}$ for $|\beta^j| = l + 1$ and $\beta^j \cap \gamma^i = \mathbf{0}$, which also means that $\bar{w}_{ij} = f_{\gamma^i+\beta^1}$ for all the j with $1 \leq j \leq E$ such that $\beta^j \cap \gamma^i = \mathbf{0}$. ■

Proposition 4: Let $1 \leq i \leq E$ and $1 \leq j \leq E$. If $\beta^j \nsubseteq \gamma^i$ and $\beta^j \cap \gamma^i \neq \mathbf{0}$ then $\bar{w}_{ij}$ is equal to $f_{\gamma^i+(\gamma^i \cap \beta^j)}$.

Proof: We do mathematical induction on $|\beta^j|$, i.e., the Hamming weight of β^j. For $|\beta^j| = 2$ and $\beta^j \nsubseteq \gamma^i$, it is not hard to show that

$$\begin{aligned}\bar{w}_{ij} &= f_{\gamma^i+\beta^1} + f_{\gamma^i+\delta_1} + f_{\gamma^i+\delta_2} \\ &= f_{\gamma^i+\beta^1} + f_{\gamma^i+\beta^1} + f_{\gamma^i+(\gamma^i\cap\beta^j)} \\ &= f_{\gamma^i+(\gamma^i\cap\beta^j)}\end{aligned}$$

where $\delta_1, \delta_2 \subseteq \beta^j$, $|\delta_1| = |\delta_2| = 1$, $\delta_1 \cap \gamma^i = \mathbf{0}$ and $\delta_2 \subseteq \gamma^i$, i.e., $\delta_2 = \gamma^i \cap \beta^j$.

Assume that $\bar{w}_{ij} = f_{\gamma^i+(\gamma^i\cap\beta^j)}$ for $|\beta^j| \leq l$, $2 \leq l < e$, $\beta^j \nsubseteq \gamma^i$ and $\beta^j \cap \gamma^i \neq \mathbf{0}$. Consider the following two disjoint sets:

$$\mathcal{S}_1(i,j) = \{\delta \,|\, \delta \subseteq \beta^j, \delta \neq \mathbf{0}, \delta \cap \gamma^i = \mathbf{0}\}$$

and

$$\mathcal{S}_2(i,j) = \{\delta \,|\, \delta \subseteq \beta^j, \delta \subseteq \gamma^i\}.$$

Denote by $\delta_1^{\max}$ the element with the maximum Hamming weight in $\mathcal{S}_1(i,j)$ and by $\delta_2^{\max}$ the element with the maximum Hamming weight in $\mathcal{S}_2(i,j)$. It is easy to see that $\delta_2^{\max} = \gamma^i \cap \beta^j$ and $\delta_1^{\max} \cup \delta_2^{\max} = \beta^j$.

For $|\beta^j| = l+1$, $\beta^j \nsubseteq \gamma^i$ and $\beta^j \cap \gamma^i \neq \mathbf{0}$, since $\mathbf{0} \in \mathcal{S}_2(i,j)$ but $\mathbf{0} \bar{\in} \mathcal{S}_1(i,j)$ we have

$$\begin{aligned}\bar{w}_{ij} &= \sum_{1\leq k<j,\, \beta^k\subseteq\beta^j} \bar{w}_{ik} \\ &= \sum_{\substack{\delta_1\in\mathcal{S}_1, \delta_2\in\mathcal{S}_2 \\ \beta^k=(\delta_1\cup\delta_2)\neq\beta^j}} \bar{w}_{ik} + \sum_{\substack{\delta_2\in\mathcal{S}_2 \\ \beta^k=\delta_2}} \bar{w}_{ik}\end{aligned}$$

where k satisfies $|\beta^k| \leq l$.

If $\beta^k = (\delta_1 \cup \delta_2) \neq \beta^j$, then according to the induction assumption

$$\bar{w}_{ik} = f_{\gamma^i+(\gamma^i\cap\beta^k)} = f_{\gamma^i+(\gamma^i\cap(\delta_1\cup\delta_2))} = f_{\gamma^i+\delta_2},$$

since $\delta_1 \cap \gamma^i = \mathbf{0}$ and $\delta_2 \subseteq \gamma^i$. Therefore, by Proposition 2 we have

$$\begin{aligned}\bar{w}_{ij} &= \sum_{\substack{\delta_1\in\mathcal{S}_1 \\ \delta_1\neq\delta_1^{\max}}} \sum_{\substack{\delta_2\in\mathcal{S}_2 \\ \beta^k=\delta_2}} f_{\gamma^i+\delta_2} + \sum_{\substack{\delta_2\in\mathcal{S}_2 \\ \beta^k=\delta_2}} f_{\gamma^i+\delta_2} \\ &\quad + \sum_{\delta_1=\delta_1^{\max}} \sum_{\substack{\delta_2\in\mathcal{S}_2, \delta_2\neq\delta_2^{\max} \\ \beta^k=\delta_2}} f_{\gamma^i+\delta_2}\end{aligned}$$

Note that $\mathcal{S}_1(i,j)$ always has odd number of elements. Finally, we have

$$\begin{aligned}\bar{w}_{ij} &= \sum_{\substack{\delta_2\in\mathcal{S}_2 \\ \beta^k=\delta_2}} f_{\gamma^i+\delta_2} + \sum_{\delta_1=\delta_1^{\max}} \sum_{\substack{\delta_2\in\mathcal{S}_2, \delta_2\neq\delta_2^{\max} \\ \beta^k=\delta_2}} f_{\gamma^i+\delta_2} \\ &= f_{\gamma^i+\delta_2^{\max}} = f_{\gamma^i+(\gamma^i\cap\beta^j)}\end{aligned}$$

This completes the proof. ■

Proposition 5: Let $1 \leq i \leq E$ and $1 \leq j \leq E$. $\bar{w}_{ij} = \bar{w}_{(E-j+1)(E-i+1)}$ holds in $\bar{W}_e(f)$ for every pair of (i,j) and $\bar{w}_{(E-k+1)1} = \bar{w}_{(E-k+1)k}$ holds for every $k = 1, 2, \cdots, E$.

Proof: If $\beta^j \subseteq \gamma^i$, then $\overline{\gamma^i} \subseteq \overline{\beta^j}$ and $\beta^{E-i+1} \subseteq \gamma^{E-j+1}$. According to Proposition 2 and Equation (3) we have

$$\begin{aligned}\bar{w}_{ij} = f_{\gamma^i+\beta^j} &= f_{\overline{\gamma^i}+\overline{\beta^j}} \\ &= f_{\beta^{E-i+1}+\gamma^{E-j+1}} \\ &= \bar{w}_{(E-j+1)(E-i+1)}\end{aligned}$$

If $\beta^j \cap \gamma^i = \mathbf{0}$, then $\overline{\beta^j} \cap \overline{\gamma^i} = \mathbf{0}$, i.e., $\beta^{E-i+1} \cap \gamma^{E-j+1} = \mathbf{0}$. According to Proposition 3 we have

$$\bar{w}_{(E-j+1)(E-i+1)} = \bar{w}_{ij} = f_{\gamma^i+\beta^1}.$$

If $\beta^j \nsubseteq \gamma^i$ and $\beta^j \cap \gamma^i \neq \mathbf{0}$ then $\beta^{E-i+1} \nsubseteq \gamma^{E-j+1}$ and $\beta^{E-i+1} \cap \gamma^{E-j+1} \neq \mathbf{0}$. According to Proposition 4 we have

$$\begin{aligned}\bar{w}_{ij} = f_{\gamma^i+(\gamma^i\cap\beta^j)} &= f_{\overline{\gamma^i}+(\overline{\gamma^i\cap\beta^j})} \\ &= f_{\overline{\gamma^i}+(\overline{\gamma^i}\cup\overline{\beta^j})} \\ &= f_{\beta^{E-i+1}+(\beta^{E-i+1}\cup\gamma^{E-j+1})} \\ &= f_{\gamma^{E-j+1}+(\gamma^{E-j+1}\cap\beta^{E-i+1})} \\ &= \bar{w}_{(E-j+1)(E-i+1)}\end{aligned}$$

It is clear that

$$\beta^1 \cap \gamma^{E-k+1} = \beta^k \cap \gamma^{E-k+1} = \mathbf{0}$$

holds for $1 \leq k \leq E$. Therefore $\bar{w}_{(E-k+1)1} = \bar{w}_{(E-k+1)k} = f_{\gamma^{E-k+1}+\beta^1}$ for $1 \leq k \leq E$. ■

We reverse the order of all the rows in $\bar{W}_e(f)$ then the i-th row becomes the $(E-i+1)$-th row. We denote by $M_e(f)$ the new matrix and by m_{ij} the entry on row i and column j of $M_e(f)$. According to Proposition 5, $m_{ij} = \bar{w}_{(E-i+1)j} = \bar{w}_{(E-j+1)i} = m_{ji}$, which means that $M_e(f)$ is an $E \times E$ symmetric matrix. Moreover, we have

$$m_{k1} = \bar{w}_{(E-k+1)1} = \bar{w}_{(E-k+1)k} = m_{kk}$$

and

$$m_{1k} = \bar{w}_{Ek} = \bar{w}_{(E-k+1)1},$$

i.e., $m_{k1} = m_{kk} = m_{1k}$ holds for $1 \leq k \leq E$ in $M_e(f)$.

Since $W_e(f)$ can be changed into $M_e(f)$ by applying some elementary transformations, $W_e(f)$ and $M_e(f)$ has the same rank for every integer $e = 1, 2, \cdots, \lceil \frac{n}{2} \rceil - 1$. The optimal resistance of f against FAA's can be further determined by the invertibility of a set of binary matrixes over $\mathbb{F}_2$, i.e., $M_e(f)$ with $1 \leq e \leq \lceil \frac{n}{2} \rceil$.

V. The Main Result

In this section by observing a necessary condition of matrix $M_e(f)$ to be invertible, we obtain a necessary condition of Boolean functions to have optimal resistance against FAA's.

It is well-known that the determinant of an $n \times n$ skew-symmetric matrix over a field with odd characteristic is equal to 0 if n is odd. Thus it is not hard for us to prove the following fact about the determinant of symmetric matrices over $\mathbb{F}_2$.

Proposition 6: The determinant of an $n \times n$ symmetric matrix over $\mathbb{F}_2$ is equal to 0 if n is odd and all the entries on its diagonal are zero.

With Proposition 6 we give a necessary condition of matrix $M_e(f)$ to be invertible.

Lemma 3: Let $f \in \mathbb{B}_n$, $1 \leq e \leq \lceil \frac{n}{2} \rceil - 1$ and $E = \sum_{i=0}^{e} \binom{n}{i}$. $M_e(f)$ is invertible over $\mathbb{F}_2$ only if one of the following two conditions is satisfied.

1) $m_{11} = 1$ and E is odd,
2) $m_{11} = 0$ and E is even.

Proof: If $m_{11} = 1$, we define a $E \times E$ matrix $\mathbf{A} = \{a_{ij}\}_{1 \leq i \leq E, 1 \leq j \leq E}$ with

$$a_{ij} = \begin{cases} 1 & \text{if } i = j \\ m_{1j} & \text{if } i = 1 \\ 0 & \text{otherwise} \end{cases}$$

Then

$$\mathbf{A}^{\mathrm{T}} M_e(f) \mathbf{A} =$$

$$\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & b_{11} & b_{12} & \cdots & b_{1(E-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & b_{(E-1)1} & b_{(E-1)2} & \cdots & b_{(E-1)(E-1)} \end{pmatrix}$$

where matrix $\mathbf{B} = \{b_{ij}\}_{1 \leq i \leq E-1, 1 \leq j \leq E-1}$ is an $(E-1) \times (E-1)$ matrix.

It can be verified that $b_{ij} = m_{1(i+1)} m_{1(j+1)} + m_{(i+1)(j+1)}$, which implies that $b_{ij} = b_{ji}$ and $\mathbf{B}$ is an $(E-1) \times (E-1)$ symmetric matrix. Furthermore, $b_{kk} = m_{1(k+1)} m_{1(k+1)} + m_{(k+1)(k+1)} = 0$ for $k = 1, 2, \cdots, E-1$. If E is even then $E-1$ is odd. By Proposition 6 the rank of B is less than $E-1$ over $\mathbb{F}_2$, then the rank of $M_e(f)$ is less than E, i.e., $M_e(f)$ is not invertible over $\mathbb{F}_2$.

If $m_{1k} = 0$ for $1 \leq k \leq E$, then $M_e(f)$ must not be invertible over $\mathbb{F}_2$.

We suppose that $m_{11} = 0$ but there exists k such that $m_{1k} = m_{k1} = m_{kk} = 1$. If $m_{11} = m_{12} = 0$, i.e., $k \neq 1, 2$, switching row 2 with row k and switching column 2 with column k we get a new symmetric matrix, denoted

by $\bar{M}_e(f) = \{\bar{m}_{ij}\}_{1\le i\le E, 1\le j\le E}$, such that $\bar{m}_{11} = 0$, $\bar{m}_{12} = 1$ and $\bar{m}_{1k} = \bar{m}_{k1} = \bar{m}_{kk}$ for $1 \le k \le E$.

For $\bar{M}_e(f)$ we define a $E \times E$ matrix $\mathbf{A} = \{a_{ij}\}_{1\le i\le E, 1\le j\le E}$ with [1]

$$a_{ij} = \begin{cases} 1 & \text{if } i = j \\ \bar{m}_{12}\bar{m}_{1j} & \text{if } i = 2 \\ \bar{m}_{12}\bar{m}_{2j} + \bar{m}_{22}\bar{m}_{1j} & \text{if } i = 1 \\ 0 & \text{otherwise} \end{cases}$$

Then

$$\mathbf{A}^{\mathrm{T}}\bar{M}_e(f)\mathbf{A} = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 1 & \bar{m}_{22} & 0 & \cdots & 0 \\ 0 & 0 & b_{11} & \cdots & b_{1(E-2)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & b_{(E-2)1} & \cdots & b_{(E-2)(E-2)} \end{pmatrix}$$

where matrix $\mathbf{B} = \{b_{ij}\}_{1\le i\le E-2, 1\le j\le E-2}$ is an $(E-2)\times(E-2)$ matrix.

It can be verified that

$$\begin{aligned} b_{ij} &= \bar{m}_{1(i+2)}\bar{m}_{2(j+2)} + \bar{m}_{1(j+2)}\bar{m}_{2(i+2)} \\ &+ \bar{m}_{22}\bar{m}_{1(i+2)}\bar{m}_{1(j+2)} + \bar{m}_{(i+2)(j+2)} \end{aligned}$$

which implies that $b_{ij} = b_{ji}$ and $\mathbf{B}$ is an $(E-2)\times(E-2)$ symmetric matrix. Furthermore, for $k = 1, 2, \cdots, E-2$

$$b_{kk} = \bar{m}_{22}\bar{m}_{1(k+2)}\bar{m}_{1(k+2)} + \bar{m}_{(k+2)(k+2)} = 0,$$

since $\bar{m}_{22} = \bar{m}_{12} = 1$ and $\bar{m}_{1(k+2)} = \bar{m}_{(k+2)(k+2)}$. If E is odd then $E-2$ is also odd. By Proposition 6 the rank of B is less than $E-2$ over $\mathbb{F}_2$, then the rank of $M_e(f)$ is less than E, i.e., $M_e(f)$ is not invertible over $\mathbb{F}_2$. Combining two cases above we have the desired results. ■

[1]We found such a matrix from an unpublished note '*Rank of Symmetric Matrices over Finite Fields*' given by M. Brown and R.C. Rhoades, which is available at http://math.stanford.edu/∼rhoades.

Note that $m_{11} = f_{\gamma^E+\beta^1}$ in $M_e(f)$ is equal to the coefficient of n-variable monomial $x_1x_2\cdots x_n$ in the ANF of Boolean function $f \in \mathbb{B}_n$. This implies that f be balanced only if $m_{11} = 0$.

Since balanced Boolean functions are more interesting for cryptography, firstly we consier the resistance of balanced Boolean functions against FAA's. From Lemma 3 we see that there exists an n-variable balanced Boolean function with optimal resistance against FAA's only if

$$\sum_{i=0}^{1}\binom{n}{i}, \sum_{i=0}^{2}\binom{n}{i}, \cdots, \sum_{i=0}^{\lceil\frac{n}{2}\rceil-1}\binom{n}{i}$$

are all even. Thus it is necessary to know what should n be like when all the sums above are even.

For n-variable balanced Boolean functions, a trivial observation is that n must be odd so that $\sum_{i=0}^{1}\binom{n}{i}$ is even.

Lemma 4: Let n be odd and k be the exponent of the highest power of 2 that divides integer $n-1$. Then

$$\binom{n}{2}, \binom{n}{3}, \binom{n}{4}, \cdots, \binom{n}{2^k-1}$$

are all even, but $\binom{n}{2^k}$ is odd.

Proof: Denote by $\mathrm{IntExp}_2(N)$ the exponent of the highest power of 2 that divides integer N. Let $2 \le t \le 2^k$. When t is even the parity of $\binom{n}{t}$ is determined by

$$\mathrm{IntExp}_2\left[\prod_{i=0}^{\frac{t-2}{2}}(n-1-2i)\right] - \mathrm{IntExp}_2\left[\prod_{i=1}^{\frac{t}{2}}2i\right].$$

Since $k = \mathrm{IntExp}_2(n-1)$ we have $n \equiv 1 \bmod 2^k$ and

$$\mathrm{IntExp}_2(n-1-2i) = \mathrm{IntExp}_2(2i)$$

for every $i = 1, 2, \cdots, \frac{t-2}{2}$. Then when t is even $\binom{n}{t}$ is even if and only if

$$\mathrm{IntExp}_2(n-1) - \mathrm{IntExp}_2(t) > 0.$$

For every $i = 1, 2, \cdots, \frac{2^k-2}{2}$ we have

$$\mathrm{IntExp}_2(n-1) - \mathrm{IntExp}_2(2i) > 0,$$

and for $i = 2^{k-1}$

$$\mathrm{IntExp}_2(n-1) - \mathrm{IntExp}_2(2i) = 0,$$

since $n \equiv 1 \bmod 2^k$ but $n \neq 1 \bmod 2^{k+1}$. Then

$$\binom{n}{2}, \binom{n}{4}, \binom{n}{6}, \cdots, \binom{n}{2^k - 2}$$

are all even but $\binom{n}{2^k}$ is odd. Finally, It is easy to see that $\binom{n}{t}$ is even implies $\binom{n}{t+1}$ is even. Then

$$\binom{n}{3}, \binom{n}{5}, \binom{n}{7}, \cdots, \binom{n}{2^k - 1}$$

are all even. ■

With Lemma 4 we can give a necessary condition of balanced Boolean functions to have optimal resistance against FAA's.

Theorem 2: There exists an n-variable balanced Boolean function with optimal resistance against FAA's only if $n = 2^k + 1$ and k is a positive integer.

Proof: Let $f \in \mathbb{B}_n$ be balanced. According to Theorem 1 and Lemma 3, f has optimal resistance against FAA's only if n is odd and

$$\binom{n}{2}, \binom{n}{3}, \binom{n}{4}, \cdots, \binom{n}{\lceil \frac{n}{2} \rceil - 1}$$

are all even.

Let $k = \mathrm{IntExp}_2(n-1)$ is the exponent of the highest power of 2 that divides integer $n-1$. Then $n = 2^k \cdot q + 1$ with q odd. From Lemma 4 all the binomial coefficients above are even only if

$$\lceil \frac{n}{2} \rceil - 1 \leq 2^k - 1,$$

i.e., $\frac{n+1}{2} \leq 2^k$. But $\frac{n+1}{2} = 2^{k-1} \cdot q + 1 \leq 2^k$ holds only when $q = 1$. Therefore

$$\binom{n}{2}, \binom{n}{3}, \binom{n}{4}, \cdots, \binom{n}{\lceil \frac{n}{2} \rceil - 1}$$

are all even only if $n = 2^k + 1$. This means that f has optimal resistance against FAA's only if $n = 2^k + 1$ and k is a positive integer. ■

Finally, for unbalanced Boolean functions against FAA's. we have a similar result. From Lemma 3 we see that there exists an n-variable unbalanced Boolean function with optimal resistance against FAA's only if $\sum_{i=0}^{1} \binom{n}{i}$ is odd and

$$\sum_{i=0}^{2} \binom{n}{i}, \sum_{i=0}^{3} \binom{n}{i}, \cdots, \sum_{i=0}^{\frac{n}{2}-1} \binom{n}{i}$$

are all even. A trivial observation is that n must be even so that $\sum_{i=0}^{1} \binom{n}{i}$ is odd.

From Lemma 4 and its proof we have a similar lemma as follows.

Lemma 5: Let n be even and $k = \mathrm{IntExp}_2(n)$ be the exponent of the highest power of 2 that divides integer n. Then

$$\binom{n}{2}, \binom{n}{3}, \binom{n}{4}, \cdots, \binom{n}{2^k - 1}$$

are all even, but $\binom{n}{2^k}$ is odd.

Then from Theorem 2 we can similarly prove the following result.

Theorem 3: There exists an n-variable unbalanced Boolean function with optimal resistance against FAA's only if $n = 2^k$ and $k \geq 2$ is a positive integer.

Proof: Let $f \in \mathbb{B}_n$ be unbalanced. According to Theorem 1 and Lemma 3, f has optimal resistance against FAA's only if n and

$$\binom{n}{2}, \binom{n}{3}, \binom{n}{4}, \cdots, \binom{n}{\frac{n}{2} - 1}$$

are all even.

Let $k = \mathrm{IntExp}_2(n)$ is the highest power of 2 that divides integer n. Then $n = 2^k \cdot q$ with q odd. From Lemma 5 all the binomial coefficients above are even only if $\frac{n}{2} - 1 \leq 2^k - 1$, i.e., $\frac{n}{2} \leq 2^k$. But $\frac{n}{2} = 2^{k-1} \cdot q \leq 2^k$ holds only when $q = 1$. Therefore f has optimal resistance against FAA's only if $n = 2^k$ and $k \geq 2$ is a positive integer. ■

Theorem 2 gives a necessary condition of n-variable *balanced* Boolean functions to have optimal resistance against FAA's and Theorem 3 gives a necessary condition of n-variable *unbalanced* Boolean functions to

have the optimal resistance. There exists an n-variable balanced Boolean function with optimal resistance only when $n = 3, 5, 9, 17, 33, 65, 129, \cdots$. This explains our failure to find by computer tests a number of balanced Boolean functions in larger number of variables with optimal resistance against FAA's. There does not exist an n-variable balanced Boolean function with optimal resistance against FAA's for most values of n.

VI. Conclusion

In this corresponding, we obtain a necessary of n-variable Boolean functions to have optimal resistance against FAA's. We show that there does not exist an n-variable Boolean function with optimal resistance against FAA's for most values of n. There exists an n-variable balanced Boolean function with optimal resistance against FAA's only if $n = 2^k + 1$ and k is a positive integer.

References

[1] N. Courtois, W. Meier, "Algebraic attacks on stream ciphers with linear feedback," in *Advances in Cryptology - EUROCRYPT 2003*, LNCS, 2003, vol. 2729, pp. 345-359.

[2] W. Meier, E. Pasalic, C. Carlet, "Algebraic attacks and decomposition of Boolean functions," in *Advances in Cryptology - EUROCRYPT 2004*, LNCS, 2004, vol. 3027, pp. 474-491.

[3] C. Carlet, D. K. Dalai, K. C. Gupta, S. Maitra, "Algebraic Immunity for Cryptographically Significant Boolean Functions: Analysis and Construction," *IEEE Trans. Information Theory*, 2006, 52(7):3105-3121.

[4] N. Li, W. Qi, "Boolean functions of an odd number of variables with maximum algebraic immunity," *Sci. China Ser. F-Information Sciences*, 2007, 50(3):307-317.

[5] C. Carlet, K. Feng, "An Infinite Class of Balanced Functions with Optimal Algebraic Immunity, Good Immunity to Fast Algebraic Attacks and Good Nonlinearity," in *Advances in Cryptology - ASIACRYPT 2008*, LNCS, 2008, vol. 5350, pp. 425-440.

[6] Z. Tu, Y. Deng, "A conjecture about binary strings and its applications on constructing Boolean functions with optimal algebraic immunity," Designs, Codes and Cryptography, 2011, 60(1), 1-14.

[7] N. Courtois, "Fast algebraic attacks on stream ciphers with linear feedback," in *Advances in Cryptology - CRYPTO 2003*, LNCS, 2003, vol. 2729, pp. 176-194.

[8] F. Armknecht, "Improving fast algebraic attacks," in *Fast Software Encryption 2004*, LNCS, 2004, vol. 3017, pp. 65-82.

[9] N. Courtois, "Cryptanalysis of SFINKS," in *Information Security and Cryptology - ICISC 2005*, LNCS, 2006, vol. 3935, pp. 261-269.

[10] A. Braeken, J. Lano , N. Mentens , B. Preneel, and I. Verbauwhede, "SFINKS: A Synchronous Stream Cipher for Restricted Hardware Environments," in *SKEW - Symmetric Key Encryption Workshop, 2005*.

[11] Y. Du, F. Zhang, M. Liu, "On the Resistance of Boolean Functions against Fast Algebraic Attacks," in *Information Security and Cryptology - ICISC 2011*, to appear in LNCS, 2012.

[12] F. Armknecht, C. Carlet, P. Gaborit, S. Küunzli, W. Meier, O. Ruatta, "Efficient Computation of Algebraic Immunity for Algebraic and Fast Algebraic Attacks," in *Advances in Cryptology - EUROCRYPT 2006*, LNCS 2006, vol. 4004, pp. 147-164.

[13] E. Pasalic, "Almost Fully Optimized Infinite Classes of Boolean Functions Resistant to (Fast) Algebraic Cryptanalysis," in *Information Security and Cryptology - ICISC 2008*, LNCS, 2009, vol. 5461, pp. 399-414.

[14] M. Liu, D. Lin, D. Pei, "Fast Algebraic Attacks and Decomposition of Symmetric Boolean Functions," *IEEE Trans. Information Theory*, 2011, 57(7):4817-4821.

[15] X. Zeng, C. Carlet, J. Shan, L. Hu, "More Balanced Boolean Functions With Optimal Algebraic Immunity and Good Nonlinearity and Resistance to Fast Algebraic Attacks," *IEEE Trans. Information Theory*, 2011, 57(9):6310-6320.

[16] D. K. Dalai, S. Maitra, "Reducing the Number of Homogeneous Linear Equations in Finding Annihilators," in *SETA 2006*, LNCS, 2006, vol. 4086, pp. 376-390.