On the Immunity of Rotation Symmetric Boolean Functions Against Fast Algebraic Attacks *

Yin Zhang Meicheng Liu† Dongdai Lin

The State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100190, P. R. China

Abstract

In this paper, it is shown that an n-variable rotation symmetric Boolean function f with n even but not a power of 2 admits a rotation symmetric function g of degree at most $e \leq n/3$ such that the product gf has degree at most $n - e - 1$.

Keywords: cryptography, Boolean functions, fast algebraic attacks, algebraic immunity, rotation symmetric

1 Introduction

Boolean functions are frequently used in the design of stream ciphers, block ciphers and hash functions. One of the most vital roles in cryptography of Boolean functions is to be used as filter and combination generators of stream ciphers based on linear feedback shift registers (LFSR). The study of the cryptographic criteria of Boolean functions is important because of the connections between known cryptanalytic attacks and these criteria. The class of rotation symmetric Boolean functions have been proven to be very useful in cryptography [19, 6]. This has led to many papers studying different cryptographic properties of rotation symmetric functions, e.g., [22, 12].

In recent years, algebraic and fast algebraic attacks [1, 4, 5] have been regarded as a great threat against LFSR-based stream ciphers. These attacks cleverly use over-defined systems of multi-variable nonlinear equations to recover the secret key. Algebraic attacks lower the degree of the equations by multiplying a nonzero function while fast algebraic attacks obtain equations of small degree by linear combination. Thus algebraic immunity, the minimum algebraic degree of annihilators of f or $f + 1$, was introduced in [18] to measure the ability of Boolean functions to resist algebraic attacks; while the notion of (e, d)-resistance against fast algebraic attacks of Boolean functions was proposed in [10]. It is well known that $\lceil \frac{n}{2} \rceil$

*Supported by the National 973 Program of China under Grant 2011CB302400, the National Natural Science Foundation of China under Grants 60970152, 10971246 and 61173134, the Grand Project of Institute of Software of CAS under Grant YOCX285056 and the CAS Special Grant for Postgraduate Research, Innovation and Practice.

†Corresponding author. E-mail: meicheng.liu@gmail.com.

is maximum algebraic immunity of n-variable Boolean functions. The identification and construction of Boolean functions with maximum algebraic immunity are researched in a large number of papers, e.g., [7, 8, 13, 14, 3, 15, 17]. However, it is still open what is maximum immunity to fast algebraic attacks.

It has been demonstrated that the resistance of Boolean functions against fast algebraic attacks is not fully covered by algebraic immunity [2, 16]. A preprocessing of fast algebraic attacks on LFSR-based stream ciphers, which use a Boolean function f as the filter or combination generator, is to find a function g of small degree such that the multiple gf has degree not too large. For any pair of integers (e, d) such that $e + d \geq n$, there is a nonzero function g of degree at most e such that gf has degree at most d [5]. Thus f has optimal possible resistance against fast algebraic attacks, if for any pair of integers (e, d) such that $e + d < n$ and $e < n/2$, there is no nonzero function g of degree at most e such that gf has degree at most d. Note that one can use the fast general attack by splitting the function into two $f = h + l$ with l being the linear part of f [5]. In this case, $e = 1$ and d equals the degree of the function f.

For determining the immunity against fast algebraic attacks, F. Armknecht et al. [2] introduced an effective algorithm and showed that a class of symmetric Boolean functions have poor resistance against fast algebraic attacks despite their resistance against algebraic attacks. Later M. Liu et al. [16] stated that almost all the symmetric Boolean functions behavior badly against fast algebraic attacks. Y. Du et al. [9] improved Armknecht's algorithm and got better computation complexity when deciding optimal possible resistance against fast algebraic attacks of Boolean functions. Based on univariate polynomial representation, C. Carlet and K. Feng [3] constructed a class of Boolean functions with maximum AI, and observed through computer experiments by Armknecht's algorithm that their functions also have good behavior against fast algebraic attacks. P. Rizomiliotis [20, 21] introduced a method to evaluate the behavior of Boolean functions against fast algebraic attacks using univariate polynomial representation.

Yet we still have very little knowledge about the resistance of Boolean functions to fast algebraic attacks. In this paper, we study rotation symmetric Boolean functions in terms of the immunity against fast algebraic attacks. We develop the techniques used in [2, 9] for computing the immunity against fast algebraic attacks from Boolean functions into rotation symmetric Boolean functions. It is shown that for a rotation symmetric function f, there exists a function g of degree at most e such that gf has degree at most d, if a correlative matrix, denoted by $S(f; e, d)$, has not full column rank. The size of $S(f; e, d)$ is much smaller than those of [2, 9]. Further, some properties of such matrices are presented for $e = 2^m$ with 2^m dividing n. A large number of singular matrices are then found, such as $S(f; 2^m, n - 2^m - 1)$. Consequently, for even integer n (excluding a power of 2), rotation symmetric functions on n variables always admit $e + d < n$ for some $e \leq n/3$. It states that such functions do not achieve optimal possible resistance against fast algebraic attacks.

2 Preliminary

Let $\mathbb{F}_2^n$ be the n-th dimensional vector space over the binary field $\mathbb{F}_2$ and $\mathbf{B}_n$ be the set of all n-variable Boolean functions mapping from $\mathbb{F}_2^n$ into $\mathbb{F}_2$. For convenience, we denote $(1, 1, \ldots, 1) \in \mathbb{F}_2^n$ by $\mathbf{1}_n$ and $(0, 0, \ldots, 0) \in \mathbb{F}_2^n$ by $\mathbf{0}_n$. An n-variable Boolean function f can

be uniquely represented as a truth table of length 2^n,

$$f = [f(\mathbf{0}_n), f(1, 0, \cdots, 0), \cdots, f(\mathbf{1}_n)].$$

The support of f is defined as $\mathrm{supp}(f) = \{x \mid f(x) = 1\}$ and the number of ones in the truth table of f is called the Hamming weight of f, denoted by $\mathrm{wt}(f)$. We say f is balanced if $\mathrm{wt}(f) = 2^{n-1}$.

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

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

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

For $x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$, let

$$\rho(x) = (x_2, \ldots, x_n, x_1),$$

and

$$\rho^k(x) = \rho(\rho^{k-1}(x)).$$

Definition 1. *An n-variable Boolean function is called rotation symmetric if for any $x \in \mathbb{F}_2^n$, $f(\rho(x)) = f(x)$.*

The set of all n-variable rotation symmetric Boolean functions (RSBF) is denoted by $\mathbf{RSB}_n$. The ANF of a rotation symmetric function is unchanged by any cyclic permutation ρ^k of the variables $x_1, x_2, \cdots, x_n$.

For $c \in \mathbb{F}_2^n$, we define

$$G_n(c) = \{\rho^k(c) : 0 \leq k \leq n-1\}.$$

Denoted by $\nu(c)$ the number of elements in $G_n(c)$, that is, $\nu(c) = |G_n(c)|$. We select the representative element of $G_n(c)$ as the lexicographically first element. Denoted by $\Gamma(n)$ the set of all the representative elements of $G_n(c)$ ($c \in \mathbb{F}_2^n$). Then the existence of a representative term x^c implies the existence of all the terms x^u ($u \in G_n(c)$) in the ANF of an n-variable rotation symmetric Boolean function, which means that $f \in \mathbf{RSB}_n$ can be written as

$$f(x) = \sum_{c \in \Gamma(n)} f_c \sum_{u \in G_n(c)} x^u,\ x^u = x_1^{u_1} x_2^{u_2} \cdots x_n^{u_n},\ f_c \in \mathbb{F}_2.$$

3 The immunity of Boolean functions against fast algebraic attacks

Denoted by $\mathcal{W}_e$ the set $\{x \in \mathbb{F}_2^n | \mathrm{wt}(x) \leq e\}$ and by $\overline{\mathcal{W}}_d$ the set $\{x \in \mathbb{F}_2^n | \mathrm{wt}(x) \geq d+1\}$. For $y, z \in \mathbb{F}_2^n$, let $z \subset y$ be an abbreviation for $\mathrm{supp}(z) \subset \mathrm{supp}(y)$, where $\mathrm{supp}(x) = \{i | x_i = 1\}$, and let $y \cup z = (y_1 \vee z_1, \ldots, y_n \vee z_n)$ where $\vee$ is the OR operation. Let g of algebraic degree at most e satisfy that $h = gf$ has algebraic degree at most d. Let

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

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

and

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

We have $h_y = 0$ for $y \in \overline{\mathcal{W}}_d$. Then

$$0 = h_y = \sum_{z \in \mathcal{W}_e} \sum_{c \cup z = y} f_c g_z = \sum_{z \in \mathcal{W}_e} g_z \sum_{c \cup z = y} f_c, \text{ for } y \in \overline{\mathcal{W}}_d. \tag{1}$$

The above equations on g_z's are homogeneous linear. Denote the coefficient matrix of the equations by $M(f; e, d)$, which is a $\sum_{i=0}^{n-d} \binom{n}{i} \times \sum_{i=0}^{e} \binom{n}{i}$ matrix. Then f admits no function g of algebraic degree at most e such that $h = gf$ has algebraic degree at most d if and only if the rank of the matrix $M(f; e, d)$ equals the number of g_z's which is $\sum_{i=0}^{e} \binom{n}{i}$, i.e., $M(f; e, d)$ has full column rank (see also [2, 9]).

Theorem 1. *[2, 9] Let $f \in \mathbf{B}_n$. Then there exists no function g of degree at most e such that the product gf has degree at most d if and only if the matrix $M(f; e, d)$ has full column rank.*

4 The immunity of rotation symmetric Boolean functions against fast algebraic attacks

Denoted by $\Gamma_e(n)$ the set $\{y \in \Gamma(n) | \operatorname{wt}(y) \leq e\}$ ordered by increasing weight and by $\gamma_d(n)$ the set $\{y \in \Gamma(n) | \operatorname{wt}(y) \geq d+1\}$ in reverse order as $\Gamma_e(n)$. Then $|\gamma_d(n)| \approx \sum_{i=0}^{n-d} \binom{n}{i}/n$ and $|\Gamma_e(n)| \approx \sum_{i=0}^{e} \binom{n}{i}/n$. We refer to [22] for the exact values of $|\gamma_d(n)|$ and $|\Gamma_e(n)|$. For $f \in \mathbf{RSB}_n$, let $g \in \mathbf{RSB}_n$ of algebraic degree at most e satisfy that $h = gf$ has algebraic degree at most d. Then h is also a rotation symmetric Boolean function. Let

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

$$g(x) = \sum_{z \in \Gamma_e(n)} g_z \sum_{u \in G_n(z)} x^u, \ g_z \in \mathbb{F}_2, \tag{2}$$

and

$$h(x) = \sum_{y \in \Gamma(n)} h_y \sum_{u \in G_n(y)} x^u, \ h_y \in \mathbb{F}_2.$$

Then for $y \in \gamma_d(n)$ it is derived from (1) and (2) that

$$0 = h_y = \sum_{z \in \Gamma_e(n)} \sum_{u \in G_n(z)} \sum_{c \cup u = y} g_z f_c = \sum_{z \in \Gamma_e(n)} g_z \sum_{u \in G_n(z)} \sum_{c \cup u = y} f_c. \tag{3}$$

Then the above equations on g_z's are homogeneous linear. Denote the coefficient matrix of the equations by $S(f; e, d)$, which is a $|\gamma_d(n)| \times |\Gamma_e(n)|$ matrix with the ij-th element equal to

$$s_{y,z} = \sum_{u \in G_n(z)} \sum_{c \cup u = y} f_c, \tag{4}$$

where y is the i-th element in $\gamma_d(n)$ and z is the j-th element in $\Gamma_e(n)$. The above equations have nonzero solution if and only if the matrix $S(f;e,d)$ does not have full column rank. Therefore we obtain the following result.

Theorem 2. *Let $f \in \mathbf{RSB}_n$. Then there exists a nonzero rotation symmetric function g of degree at most e such that the product gf has degree at most d if and only if the matrix $S(f;e,d)$ does not have full column rank.*

4.1 Properties of matrix $S(f;e,d)$

In this section, we present some properties of the matrix $S(f;e,d)$ for $n = 2^m t$ and $e = 2^m$.

Proposition 3. *For $y \in \Gamma(n)$, $s_{y,\mathbf{0}_n} = f_y$.*

Proof. According to (4), we have

$$s_{y,\mathbf{0}_n} = \sum_{u \in G_n(\mathbf{0}_n)} \sum_{c \cup u = y} f_c = \sum_{c \cup \mathbf{0}_n = y} f_c = f_y.$$

□

Before stating other properties of the matrix $S(f;e,d)$, we list some useful lemmas. Lemma 4 is used to prove Lemma 5, Lemma 6 and Lemma 7, which lead to Proposition 8 and Proposition 9.

Lemma 4 was implied in [22]. Here we give a proof for self-completeness.

Lemma 4. *Let $c \in \mathbb{F}_2^n$. Then*
1) $\nu(c)|n$.
2) $\frac{n}{\gcd(n,\mathrm{wt}(c))}|\nu(c)$.

Proof. 1) Recall that $\nu(c)$ is the order of $G_n(c)$, i.e., $\nu(c)$ equals the minimum integer t such that $\rho^t(c) = c$. Then the fact that $\rho^n(c) = c$ shows $\nu(c)|n$.

2) Let $k = n/\nu(c)$. Then c can be represented as

$$c = (\underbrace{b, b, \ldots, b}_{k}),\ b \in \mathbb{F}_2^{\nu(c)}.$$

Therefore $\mathrm{wt}(b) = \mathrm{wt}(c)/k$, which means that $k|\,\mathrm{wt}(c)$ and then $n|\nu(c) \cdot \mathrm{wt}(c)$. Hence the lemma is confirmed. □

Hereinafter, for $t|n$, we define

$$\eta_t = (\underbrace{1,1,\ldots,1,0}_{t}, \underbrace{1,1,\ldots,1,0}_{t}, \ldots, \underbrace{1,1,\ldots,1,0}_{t}),$$

and

$$\tilde{\eta}_t = (\underbrace{1,0,0,\ldots,0}_{t}, \underbrace{1,0,0,\ldots,0}_{t}, \ldots, \underbrace{1,0,0,\ldots,0}_{t}).$$

It is clear that $\mathrm{wt}(\eta_t) = n - n/t$, $\mathrm{wt}(\tilde{\eta}_t) = n/t$ and $\nu(\eta_t) = \nu(\tilde{\eta}_t) = t$. For $c \in \mathbb{F}_2^n$ and $t|n$, let

$$G_n^t(c) = \{c, \rho^t(c), \ldots, \rho^{(\nu_t(c)-1)t}(c)\},$$

where $\nu_t(c)$ is the smallest integer that satisfies

$$\rho^{\nu_t(c)t}(c) = c.$$

By the definitions of $\nu(c)$ and $\nu_t(c)$ we know that

$$\nu_t(c) = \frac{\nu(c)}{\gcd(\nu(c), t)}. \tag{5}$$

Lemma 5. *Let $n = 2^m t$ and $n - 2^m \leq \mathrm{wt}(c) \leq n - 1$. If $c \in G_n(\eta_t)$, then $\nu(c) = t$ and $\nu_t(c) = 1$; otherwise, both $\nu(c)$ and $\nu_t(c)$ are even.*

Proof. For $c \in G_n(\eta_t)$ it holds that $\nu(c) = t$ and therefore $\nu_t(c) = 1$ according to (5). Next we check the second half part of the lemma.

For $c \notin G_n(\eta_t)$ with $\mathrm{wt}(c) = n - 2^m$, it holds that $\nu(c) > t$. By Lemma 4(1) we have $\nu(c)|n = 2^m t$ and by Lemma 4(2) we have $t|\nu(c)$. Therefore $2t|\nu(c)$. Then $\nu(c)$ and $\nu_t(c) = \nu(c)/\gcd(\nu(c), t) = \nu(c)/t$ are both even.

For $n - 2^m + 1 \leq \mathrm{wt}(c) \leq n - 1$, it follows that $\gcd(n, \mathrm{wt}(c)) < 2^m$. From (5) we know $\nu(c)|\nu_t(c) \cdot t$, then by Lemma 4(2) we have

$$\frac{2^m t}{\gcd(2^m t, \mathrm{wt}(c))}|\nu_t(c) \cdot t,$$

and $\nu_t(c)$ is therefore even, which means that $\nu(c)$ is also even since $\nu_t(c)|\nu(c)$. □

The similar proof of Lemma 5 also applies to Lemma 6.

Lemma 6. *Let $n = 2^m t$ and $1 \leq \mathrm{wt}(c) \leq 2^m$. If $c \in G_n(\tilde{\eta}_t)$, then $\nu(c) = t$ and $\nu_t(c) = 1$; otherwise, both $\nu(c)$ and $\nu_t(c)$ are even.*

Lemma 7. *Let $n = 2^m t$ and $n - 2^{m+1} \leq \mathrm{wt}(c) \leq n - 2^m$. If $c \in G_n(\eta_t)$ or $c \in G_n(\eta_t + \rho^k(\tilde{\eta}_t))$ with $2 \leq k \leq n$, then $\nu_t(c) = 1$; otherwise, $\nu_t(c)$ is even.*

Proof. The case for $\mathrm{wt}(c) = n - 2^m$ was proved in Lemma 5.

For $c \in G_n(\eta_t + \rho^k(\tilde{\eta}_t))$ with $2 \leq k \leq n$, we have $\rho^t(c) = c$ and therefore $\nu_t(c) = 1$.

For $c \notin G_n(\eta_t + \rho^k(\tilde{\eta}_t))$ with $\mathrm{wt}(c) = n - 2^{m+1}$, it holds that $\nu(c) > t$. By Lemma 4(1) we have $\nu(c)|n = 2^m t$ and by Lemma 4(2) we have

$$\frac{2^m t}{\gcd(2^m t, \mathrm{wt}(c))} = \frac{t}{\gcd(t, 2)}|\nu(c).$$

Therefore $2t|\nu(c)$. Then $\nu_t(c) = \nu(c)/t$ is even according to (5).

For $n - 2^{m+1} + 1 \leq \mathrm{wt}(c) \leq n - 2^m - 1$, it follows that $\gcd(n, \mathrm{wt}(c)) < 2^m$. From (5) we know $\nu(c)|\nu_t(c) \cdot t$, then by Lemma 4(2) we have

$$\frac{2^m t}{\gcd(2^m t, \mathrm{wt}(c))}|\nu_t(c) \cdot t,$$

and $\nu_t(c)$ is therefore even. □

Proposition 8. *Let $n = 2^m t$. Then*

$$s_{\mathbf{1}_n,z} = \begin{cases} f_{\mathbf{1}_n} & \text{for } z = \mathbf{0}_n, \\ t(f_{\mathbf{1}_n} + f_{\eta_t}) & \text{for } z = \tilde{\eta}_t, \\ 0 & \text{for } z \in \Gamma_{2^m}(n) \setminus \{\mathbf{0}_n, \tilde{\eta}_t\}. \end{cases}$$

Proof. By Proposition 3, $s_{\mathbf{1}_n,\mathbf{0}_n} = f_{\mathbf{1}_n}$. According to (4), we have

$$\begin{aligned} s_{\mathbf{1}_n,z} &= \sum_{u \in G_n(z)} \sum_{c \cup u = \mathbf{1}_n} f_c \\ &= \sum_{k=0}^{\nu(z)-1} \sum_{c \cup \rho^k(z) = \mathbf{1}_n} f_c \\ &= \sum_{k=0}^{\nu(z)-1} \sum_{\rho^k(c) \cup \rho^k(z) = \mathbf{1}_n} f_{\rho^k(c)}. \end{aligned}$$

Since $\rho^k(c) \cup \rho^k(u) = \mathbf{1}_n$ if and only if $c \cup u = \mathbf{1}_n$, and $f_{\rho^k(c)} = f_c$ for $f \in \mathbf{RSB}_n$, we have

$$s_{\mathbf{1}_n,z} = \nu(z) \sum_{c \cup z = \mathbf{1}_n} f_c.$$

From Lemma 6, it holds that

$$s_{\mathbf{1}_n,z} = 0, \text{ for } z \in \Gamma_{2^m}(n) \setminus \{\mathbf{0}_n, \tilde{\eta}_t\},$$

and for $z = \tilde{\eta}_t$,

$$s_{1^n,\tilde{\eta}_t} = t \sum_{c \cup \tilde{\eta}_t = \mathbf{1}_n} f_c.$$

Let C be the set of all the lexicographically first elements in the sets $G_n^t(c)$ where $\mathrm{wt}(c) \geq n - \mathrm{wt}(\tilde{\eta}_t) = n - 2^m$. Then

$$s_{1^n,\tilde{\eta}_t} = t \sum_{c \in C} \sum_{\substack{0 \leq k \leq \nu_t(c)-1 \\ \rho^{kt}(c) \cup \tilde{\eta}_t = \mathbf{1}_n}} f_{\rho^{kt}(c)}.$$

Since $\rho^t(\tilde{\eta}_t) = \tilde{\eta}_t$, it follows that $\rho^t(c) \cup \tilde{\eta}_t = \mathbf{1}_n$ if and only if $c \cup \tilde{\eta}_t = \mathbf{1}_n$. Then

$$\begin{aligned} s_{1^n,\tilde{\eta}_t} &= t \sum_{\substack{c \in C \\ c \cup \tilde{\eta}_t = \mathbf{1}_n}} \nu_t(c) f_c \\ &= t(f_{\mathbf{1}_n} + f_{\eta_t}) + t \sum_{\substack{c \in C \setminus \{\mathbf{1}_n, \eta_t\} \\ c \cup \tilde{\eta}_t = \mathbf{1}_n}} \nu_t(c) f_c \\ &= t(f_{\mathbf{1}_n} + f_{\eta_t}) \text{ (by Lemma 5).} \end{aligned}$$

□

Proposition 9. *Let $n = 2^m t$. Then*

$$s_{\eta_t,z} = \begin{cases} f_{\eta_t} & \text{for } z = \mathbf{0}_n, \\ 0 & \text{for } z \in \Gamma_{2^m}(n) \setminus \{\mathbf{0}_n, \tilde{\eta}_t\}, \end{cases}$$

and

$$s_{\eta_t,\tilde{\eta}_t} = \begin{cases} 0 & \text{for odd } t, \\ f_{\eta_t} + f_{\eta_{\frac{t}{2}}} & \text{for even } t. \end{cases}$$

Proof. By Proposition 3, $s_{\eta_t,\mathbf{0}_n} = f_{\eta_t}$. According to (4), we have

$$s_{\eta_t,z} = \sum_{u \in G_n(z)} \sum_{c \cup u = \eta_t} f_c.$$

Let U be the set of all the lexicographically first elements in the sets $G_n^t(u)$ where $u \in G_n(z)$. The fact that $\rho^{kt}(c) \cup \rho^{kt}(u) = \eta_t$ if and only if $c \cup u = \eta_t$ gives

$$\begin{aligned} s_{\eta_t,z} &= \sum_{u \in U} \sum_{k=0}^{\nu_t(u)-1} \sum_{c \cup \rho^{kt}(u) = \eta_t} f_c \\ &= \sum_{u \in U} \sum_{k=0}^{\nu_t(u)-1} \sum_{\rho^{kt}(c) \cup \rho^{kt}(u) = \eta_t} f_{\rho^{kt}(c)} \\ &= \sum_{u \in U} \sum_{k=0}^{\nu_t(u)-1} \sum_{c \cup u = \eta_t} f_c \\ &= \sum_{u \in U} \nu_t(u) \sum_{c \cup u = \eta_t} f_c. \end{aligned}$$

For $z \in \Gamma_{2^m}(n) \setminus \{\mathbf{0}_n, \tilde{\eta}_t\}$, by Lemma 6 it follows that $\nu_t(u)$ with $u \in G_n(z)$ is even and therefore $s_{r,z} = 0$.

For $z = \tilde{\eta}_t$, we have

$$\begin{aligned} s_{\eta_t,\tilde{\eta}_t} &= \sum_{\substack{u \in G_n(\tilde{\eta}_t) \\ u \neq \rho(\tilde{\eta}_t)}} \sum_{c \cup u = \eta_t} f_c \\ &= \sum_{k=2}^{t} \sum_{c \cup \rho^k(\tilde{\eta}_t) = \eta_t} f_c. \end{aligned}$$

Let C be the set of the lexicographically first elements in the sets $G_n^t(c)$ where $n - 2^{m+1} \leq \mathrm{wt}(c) \leq n - 2^m$. Since $\rho^t(\eta_t) = \eta_t$ and $\rho^t(\rho^k(\tilde{\eta}_t)) = \rho^k(\tilde{\eta}_t)$, it follows that $\rho^{it}(c) \cup \rho^k(\tilde{\eta}_t) = \eta_t$

if and only if $c \cup \rho^k(\tilde{\eta}_t) = \eta_t$. Hence

$$\begin{aligned} s_{\eta_t,\tilde{\eta}_t} &= \sum_{k=2}^{t} \sum_{c\in C} \sum_{\substack{u\in G_n^t(c) \\ u\cup\rho^k(\tilde{\eta}_t)=\eta_t}} f_u \\ &= \sum_{k=2}^{t} \sum_{c\in C} \sum_{\substack{0\le i\le \nu_t(c)-1 \\ \rho^{it}(c)\cup\rho^k(\tilde{\eta}_t)=\eta_t}} f_{\rho^{it}(c)} \\ &= \sum_{k=2}^{t} \sum_{\substack{c\in C \\ c\cup\rho^k(\tilde{\eta}_t)=\eta_t}} \nu_t(c) f_c \\ &= \sum_{k=2}^{t} (f_{\eta_t} + f_{\eta_t+\rho^k(\tilde{\eta}_t)}) \text{ (by Lemma 7).} \end{aligned}$$

Note that for $2 \le k \le t$,

$$\eta_t + \rho^k(\tilde{\eta}_t) = \rho^{k-1}(\eta_t) + \rho(\tilde{\eta}_t) = \rho^{k-1}(\eta_t + \rho^{t+2-k}(\tilde{\eta}_t)).$$

Then $f_{\eta_t+\rho^k(\tilde{\eta}_t)} = f_{\eta_t+\rho^{t+2-k}(\tilde{\eta}_t)}$ and hence for odd t,

$$s_{\eta_t,\tilde{\eta}_t} = 2\sum_{k=2}^{\frac{t+1}{2}} (f_{\eta_t} + f_{\eta_t+\rho^k(\tilde{\eta}_t)}) = 0.$$

and for even t,

$$\begin{aligned} s_{\eta_t,\tilde{\eta}_t} &= f_{\eta_t} + f_{\eta_t+\rho^{\frac{t}{2}+1}(\tilde{\eta}_t)} + 2\sum_{k=2}^{\frac{t}{2}} (f_{\eta_t} + f_{\eta_t+\rho^k(\tilde{\eta}_t)}) \\ &= f_{\eta_t} + f_{\eta_{\frac{t}{2}}}. \end{aligned}$$

□

For $e = 1$ and $d = n-2$, the matrix $S(f; e, d)$ is

$$S(f; 1, n-2) = \begin{pmatrix} s_{\mathbf{1}_n,\mathbf{0}_n} & s_{\mathbf{1}_n,\tilde{\eta}_n} \\ s_{\eta_n,\mathbf{0}_n} & s_{\eta_n,\tilde{\eta}_n} \end{pmatrix}.$$

Taking $m = 0$ and $t = n$ in Proposition 8 and Proposition 9, it follows that

$$S(f; 1, n-2) = \begin{pmatrix} f_{\mathbf{1}_n} & 0 \\ f_{\eta_n} & f_{\eta_n} + f_{\eta_{\frac{n}{2}}} \end{pmatrix}, \text{ for even } n,$$

and

$$S(f; 1, n-2) = \begin{pmatrix} f_{\mathbf{1}_n} & f_{\mathbf{1}_n} + f_{\eta_n} \\ f_{\eta_n} & 0 \end{pmatrix}, \text{ for odd } n.$$

4.2 Singularity of matrix $S(f; e, n-e-1)$

If $d = n-e-1$, then $|\gamma_d(n)| = |\Gamma_e(n)|$ and therefore $S(f; e, d)$ is a square matrix. The problem of determining the existence of a rotation symmetric function g of degree at most e such that $\deg(fg) \leq n-e-1$ is converted into the problem of determining whether $S(f; e, n-e-1)$ is invertible. In this section, we concentrate on the matrix $S(f; e, n-e-1)$ for $n = 2^m t$ and $e = 2^m$. For the case that t is an odd number, from Proposition 8, the first row of the matrix is

$$(f_{\mathbf{1}_n}, 0, \ldots, 0, f_{\mathbf{1}_n} + f_{\eta_t}, 0, \ldots, 0),$$

and by Proposition 9 there is a row equal to

$$(f_{\eta_t}, 0, \ldots, 0).$$

If $f_{\mathbf{1}_n} = 1$ or $f_{\eta_t} = 0$, then the two rows are linearly dependent and the matrix is singular. Similarly, for even number t, the first row of $S(f; 2^m, n-2^m-1)$ is

$$(f_{\mathbf{1}_n}, 0, \ldots, 0),$$

and there is a row equal to

$$(f_{\eta_t}, 0, \ldots, 0, f_{\eta_t} + f_{\eta_{\frac{t}{2}}}, 0, \ldots, 0).$$

if $f_{\mathbf{1}_n} = 0$ or $f_{\eta_t} = f_{\eta_{\frac{t}{2}}}$, then the matrix is singular.

Then the theorems below follow from Theorem 2.

Theorem 10. *Let $n = 2^m t$ with t odd, and $f \in \mathbf{RSB}_n$. If $f_{\mathbf{1}_n} = 1$ or $f_{\eta_t} = 0$, then there exists a nonzero rotation symmetric function g of degree at most 2^m such that the product gf has degree at most $n - 2^m - 1$.*

Theorem 11. *Let $n = 2^m t$ with t even, and $f \in \mathbf{RSB}_n$. If $f_{\mathbf{1}_n} = 0$ or $f_{\eta_t} = f_{\eta_{\frac{t}{2}}}$, then there exists a nonzero rotation symmetric function g of degree at most 2^m such that the product gf has degree at most $n - 2^m - 1$.*

Corollary 12. *Let n be odd and $f \in \mathbf{RSB}_n$. If $\deg(f) \neq n-1$, then there exists a nonzero affine function g such that the product gf has degree at most $n-2$.*

Proof. It is obtained from Theorem 10. □

Corollary 13. *Let n be even and $f \in \mathbf{RSB}_n$. If $\deg(f) \leq n-1$ or $f_{\eta_n} = f_{\eta_{\frac{n}{2}}}$, then there exists a nonzero affine function g such that the product gf has degree at most $n-2$.*

Proof. It is derived from Theorem 11. □

Theorem 14. *Let $n = 2^m t$ with $m \geq 1$ and t odd, and $f \in \mathbf{RSB}_n$. Then there exists a positive integer $e \leq 2^m$ and a nonzero rotation symmetric function g of degree at most e such that the product gf has degree at most $n-e-1$.*

Proof. If $f_{\mathbf{1}_n} = 1$, the result is then confirmed by Theorem 10; otherwise, the result is demonstrated by Theorem 11. □

Theorem 14 states that any rotation symmetric Boolean function f on even number (but not a power of 2) of variables always admits a rotation symmetric function g of degree at most e for some $e \leq n/3$ such that $d = \deg(gf)$ satisfies $e + d < n$.

5 Conclusion

This paper uses smaller matrices to identify the immunity of rotation symmetric Boolean functions against fast algebraic attacks due to the special structure of such functions, and shows that about half of rotation symmetric Boolean functions can not achieve optimal possible resistance. The results of this paper are also useful for constructing rotation symmetric Boolean functions with good immunity against fast algebraic attacks since some necessary conditions to achieve good immunity are implied. But the sufficient conditions for rotation symmetric Boolean functions to achieve good immunity against fast algebraic attacks need further research.

References

[1] F. Armknecht. Improving fast algebraic attacks. In: B. Roy and W. Meier (eds.) FSE 2004. LNCS vol. 3017, pp. 65–82. Berlin, Heidelberg: Springer, 2004.

[2] F. Armknecht, C. Carlet, P. Gaborit, et al. Efficient computation of algebraic immunity for algebraic and fast algebraic attacks. In: S. Vaudenay (eds.) EUROCRYPT 2006. LNCS vol. 4004, pp. 147–164. Berlin, Heidelberg: Springer, 2006.

[3] C. Carlet and K. Feng. An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity. ASIACRYPT 2008, LNCS vol. 5350, 425–440. Berlin, Heidelberg: Springer, 2008.

[4] N. Courtois and W. Meier. Algebraic attacks on stream ciphers with linear feedback. Advances in Cryptology-EUROCRYPT 2003, LNCS 2656, 345–359. Berlin, Heidelberg: Springer, 2003.

[5] N. Courtois. Fast algebraic attacks on stream ciphers with linear feedback. Advances in Cryptology-CRYPTO 2003, LNCS 2729, 176–194. Berlin, Heidelberg: Springer, 2003.

[6] T. W. Cusick, P. Stanica. Cryptographic Boolean Functions and Applications. Academic Press, San Diego, 2009.

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

[8] D. K. Dalai, K. C. Gupta, and S. Maitra. Results on algebraic immunity for cryptographically significant Boolean functions. INDOCRYPT 2004, LNCS 3348, 92–106. Berlin, Heidelberg: Springer, 2005.

[9] Y. Du, F. Zhang and M. Liu. On the resistance of Boolean functions against fast algebraic attacks. To appear in ICISC 2011.

[10] G. Gong. Sequences, DFT and resistance against fast algebraic attacks. SETA 2008, LNCS, Vol.5203, pp. 197–218, 2008.

[11] P. Hawkes and G. Rose. Rewriting variables: the complexity of fast algebraic attacks on stream ciphers. CRYPTO 2004, LNCS 3152, pp. 390–406. Berlin, Heidelberg: Springer, 2004.

[12] S. Kavut, S. Maitra, M. D. Yücel. Search for Boolean functions with excellent profiles in the rotation symmetric class. IEEE Transaction on Information Theory, vol. 53, no. 5, pp. 1743–1751, 2007.

[13] N. Li, L. Qu, W. Qi, et al. On the construction of Boolean Functions with optimal algebraic immunity. IEEE Trans. Inform. Theory, vol. 54, no. 3, 1330–1334, 2008.

[14] N. Li, W. Qi. Construction and analysis of Boolean functions of $2t+1$ variables with maximum algebraic immunity. ASIACRYPT 2006, LNCS 4284, pp. 84–98. Berlin, Heidelberg: Springer, 2006.

[15] M. Liu, Y. Du, D. Pei, and D. Lin. On designated-weight Boolean functions with highest algebraic immunity. Sci China Math, vol. 53, no. 11, pp. 2847–2854, 2010.

[16] M. Liu, D. Lin, D. Pei. Fast algebraic attacks and decomposition of symmetric Boolean functions. IEEE Transaction on Information Theory, vol. 57, no. 7, pp. 4817–4821, 2011.

[17] M. Liu, D. Pei, and Y. Du. Identification and construction of Boolean functions with maximum algebraic immunity. Sci China Inf Sci, vol. 53, no. 7, pp. 1379–1396, 2010.

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

[19] J. Pieprzyk, C. X. Qu. Fast hashing and rotation-symmetric functions. Journal of Universal Computer Science, vol. 5, no. 1, pp. 20–31, 1999.

[20] P. Rizomiliotis. On the resistance of Boolean functions against algebraic attacks using univariate polynomial representation. IEEE Transaction on Information Theory, vol. 56, NO. 8, pp. 4014–4024, 2010.

[21] P. Rizomiliotis. On the security of the Feng-Liao-Yang Boolean functions with optimal algebraic immunity against fast algebraic attacks. Designs, Codes and Cryptography, vol. 57, no. 3, pp. 283-292, 2010.

[22] P. Stănică and S. Maitra. Rotation symmetric Boolean functions - count and cryptographic properties. Discrete Applied Mathematics, vol. 156, no. 10, pp. 1567–1580, 2008.