

On the Fast Algebraic Immunity of Even-Variable Rotation Symmetric Boolean Functions

Minglei ZHA*, Bin WANG*

* Shanghai Key Lab of Intelligent Information Processing, School of Computer Science, Fudan University, Shanghai, PR China.

10210240007@fudan.edu.cn, bwang@fudan.edu.cn

Abstract—An *AAR* (algebraic attack resistant) Boolean function is considered having good capability against both classical and fast algebraic attacks. However, *AAR* is too hard to achieve. This paper studies the protection against fast algebraic attacks on rotation symmetric Boolean functions by discussing their fast algebraic immunity. The result shows that all the even n -variable rotation symmetric Boolean functions of degree $(n-1)$ are not *AAR* because their fast algebraic immunity is at most $(n-1)$. Furthermore, we find that some of the even n -variable rotation symmetric Boolean functions of degree n or $(n-2)$ have fast algebraic immunity at most $(n-1)$, too.

Keywords—stream ciphers, Boolean functions, rotation symmetric Boolean functions, fast algebraic attacks, fast algebraic immunity.

I. INTRODUCTION

Boolean functions [1] are broadly used in design of ciphers, especially in stream ciphers based on LFSRs (linear feedback shift registers), in which the two basic models often used are the nonlinear combiner and the filter generator. RSBFs (rotation symmetric Boolean functions) [15-18] are an interesting class of Boolean functions studied recent years, for some of their cryptographic properties are considered good.

Recently algebraic attacks [2, 3] were studied as a threat against LFSR-based stream ciphers. Given a Boolean function f , the core of the algebraic attacks is to find minimum or low degree annihilators of f or $f+1$, i.e., to find g of minimum or low degree so that $f \cdot g = 0$ or $(f+1) \cdot g = 0$. Thus *AI* (algebraic immunity) [8-14] is regarded as the measure of the protection against algebraic attacks.

Fast algebraic attacks [4-7] are another kind of attack, in which the core of the analysis on a Boolean function f is to find a function g of low degree such that the degree of $f \cdot g$ is not too large. The notion of *FAI* (fast algebraic immunity) of a Boolean function [19, 20] is introduced to judge the capability of a Boolean function against fast algebraic attacks.

In [4] the notion of *AAR* (algebraic attack resistant) is introduced as a measure of protection against both classical and fast algebraic attacks. The full fast algebraic immunity [19] of Boolean functions is n and functions having full fast algebraic immunity are equivalent to *AAR* functions.

This paper studies the protection against fast algebraic attacks on RSBFs. The result shows that many even-variable RSBFs are not *AAR* functions because their *FAI* is at most $(n-1)$.

The reminder of this paper is organized as follows. In section 2 are some preliminaries of Boolean functions. In section 3, we discuss the composition of the *ANF* (algebraic normal form) and the *SANF* (short algebraic normal form) of RSBFs. In section 4, we give our results when n is even by two theorems. In section 5 are a few conclusions.

II. PRELIMINARIES

We denote by F_n^2 the n -dimensional vector space over the finite field F_2 . A Boolean function of n variables can be viewed as a mapping from F_n^2 into F_2 . We denote by B_n the set of all n -variable Boolean functions.

Any $f \in B_n$ can be uniquely represented as a multivariate polynomial over F_2 :

$$f(x_1, \dots, x_n) = \sum_{K \subseteq \{1, 2, \dots, n\}} a_K \prod_{k \in K} x_k,$$

which is called the *ANF*, or as a truth table:

$$f = [f(0, 0, 0, \dots, 0), f(0, 0, 0, \dots, 1), \dots, f(1, 1, 1, \dots, 1)] \in F_2^{2^n}.$$

The algebraic degree of f , denoted by $\deg(f)$, is the number of variables in the highest order terms with nonzero coefficient.

The notion of algebraic immunity which is used for analyzing the ability of a Boolean function against algebraic attacks is defined as follows.

Definition 1. A nonzero Boolean function g is called the annihilator of a Boolean function f if $f \cdot g = 0$. The algebraic immunity of f , denoted by $AI(f)$, is defined as the minimum degree of the annihilators of f or $f+1$, i.e.,

$$AI(f) = \min_{g \neq 0} \{\deg(g) \mid f \cdot g = 0 \text{ or } (f+1) \cdot g = 0\}.$$

To resist algebraic attacks, a Boolean function should have high *AI*. It is proved in [2] that for any Boolean function f , we

have $AI(f) \leq \lceil n/2 \rceil$. The notion of fast algebraic immunity, which is studied to judge the capability of a Boolean function to resist the fast algebraic attacks, is defined as follows.

Definition 2. The fast algebraic immunity of a Boolean function f , denoted by $FAI(f)$, can be defined as

$$FAI(f) = \min_{g: 1 \leq \deg(g) < AI(f)} \{ \deg(g) + \deg(f \cdot g), 2AI(f) \},$$

A Boolean function should have as high as possible FAI to resist fast algebraic attacks.

Remark 1. According to the definition of FAI , for any Boolean function f , $FAI(f)$ is at most $2 \cdot \lceil n/2 \rceil$, more precisely, n if f is even-variable and $n+1$ if f is odd-variable.

In [6], it is proved that for any integer pair (e, d) such that $e+d \geq n$, there always exists a nonzero function g of degree at most e such that the degree of $f \cdot g$ is at most d for any n -variable Boolean function f . Thus the notion of AAR introduced as a measure of capability against both classical and fast algebraic attacks in [6] can be redefined as follows.

Definition 3. An n -variable Boolean function f is called algebraic attack resistant (AAR) if both $AI(f)$ and $FAI(f)$ achieve maximum, i.e., $AI(f)$ is $\lceil n/2 \rceil$ and $FAI(f)$ is n .

However, a Boolean function is hard to achieve AAR . In section 4, we give the proofs that many even-variable RSBFs are not AAR because they have FAI at most $(n-1)$.

III. THE ANF COMPOSITION OF ROTATION SYMMETRIC BOOLEAN FUNCTIONS

The permutation ρ_n^k is defined as follows before we give the definition of RSBFs.

Definition 4.

$$\rho_n^k(x_i) = \begin{cases} x_{i+k} & \text{if } i+k \leq n \\ x_{i+k-n} & \text{if } i+k > n \end{cases}$$

Thus we can give the definition of RSBF as follows.

Definition 5. An n -variable Boolean function f is rotation symmetric Boolean function if and only if for any $(x_1, \dots, x_n) \in F_n^2$, $f(\rho_n^k(x_1, \dots, x_n)) = f(x_1, \dots, x_n)$, for any $1 \leq k \leq n$,

where $\rho_n^k(x_1, \dots, x_n) = (\rho_n^k(x_1), \dots, \rho_n^k(x_n))$.

It is known that if a term $x_{i_1}x_{i_2} \dots x_{i_l}$ is present in the ANF of a RSBF f , then the terms $\rho_n^k(x_{i_1}x_{i_2} \dots x_{i_l})$, namely $(\rho_n^k(x_{i_1}) \rho_n^k(x_{i_2}) \dots \rho_n^k(x_{i_l}))$ for any $1 \leq k \leq n$ must be also present in its ANF. For example, in a 4-variable RSBF, if the term $x_1x_2x_3$ is present in the ANF, then the terms $x_1x_2x_4$, $x_1x_3x_4$, $x_2x_3x_4$ must be also present.

Let

$$G_n(x_1, \dots, x_n) = \rho_n^k(x_1, \dots, x_n), 1 \leq k \leq n\},$$

i.e., the orbit under the permutating of ρ_n^k . We choose the lexicographically first element to represent all the elements in

the $G_n(x_{i_1}, x_{i_2}, \dots, x_{i_l})$, thus we can define the SANF of a RSBF. A RSBF f could be written as $a_0 + a_1x_1 + \sum a_{i_1}x_{i_1}x_{i_2} + \dots + \sum a_{i_1 \dots i_n}x_{i_1}x_{i_2} \dots x_{i_n}$, where the coefficients $a_0, a_1, \dots, a_{i_1 \dots i_n}$ are in $\{0, 1\}$. Note that the variable x_1 is always present in each non-constant term according to the definition, and the variable x_n is always not present in the terms having degree less than n .

Proposition 1. For n even, the $(n-2)$ -degree terms in SANF of an n -variable RSBF f can be simply divided as two classes, the first class contains only one element $x_1 \dots x_{n/2-1}x_{n/2+1} \dots x_{n-1}$, for the cardinality of the G_n it represents is $n/2$, and the second class contains other terms of degree $(n-2)$, for the cardinality of the G_n they represent is n .

Proof. The element representing a G_n in the SANF of a RSBF f is chosen lexicographically, so the variables $x_1, \dots, x_{n/2-1}$ must be present in each $(n-2)$ -degree term. It is easy to determine that only the term $x_1 \dots x_{n/2-1}x_{n/2+1} \dots x_{n-1}$ will be the same as the initial status after it is rotated $n/2$ times, while others will be same as the initial status only if after they are rotated n times. $\square$

Example 1. An example of the 4-degree terms in the SANF of a 6-variable RSBF.

TABLE1. An Example

Class	terms in SANF	terms in ANF
1	$x_1x_2x_4x_5$	$x_1x_2x_4x_5$ $x_2x_3x_5x_6$ $x_1x_3x_4x_6$
2	$x_1x_2x_3x_4$	$x_1x_2x_3x_4$ $x_2x_3x_4x_5$ $x_3x_4x_5x_6$ $x_1x_4x_5x_6$ $x_1x_2x_3x_6$
	$x_1x_2x_3x_5$	$x_1x_2x_3x_5$ $x_2x_3x_4x_6$ $x_1x_3x_4x_5$ $x_2x_4x_5x_6$ $x_1x_3x_5x_6$ $x_1x_2x_4x_6$

IV. THE FAST ALGEBRAIC IMMUNITY OF EVEN-VARIABLE ROTATION SYMMETRIC BOOLEAN FUNCTIONS

An elementary rotation symmetric Boolean function corresponding to a term X_i in the SANF of a RSBF is defined as the sum of all the terms that are represented by X_i . For example, the elementary rotation symmetric Boolean function corresponding to $x_1x_2x_4x_5$ of a 6-variable RSBF is $x_1x_2x_4x_5 + x_2x_3x_5x_6 + x_1x_3x_4x_6$.

The r -th elementary symmetric Boolean function of an n -variable Boolean function f , denoted by σ_r , is the sum of all the r -degree terms, thus σ_1 is the first elementary symmetric Boolean function, i.e., $x_1 + \dots + x_n$. Now we can get the following lemmas easily if n is even.

Lemma 1. For each elementary rotation symmetric Boolean function g corresponding to the element in the second class mentioned in proposition 1, the multiple $g \cdot \sigma_1$ is 0. And, the multiple of σ_1 and the elementary rotation symmetric

Boolean function corresponding to the term $x_1 \cdot \dots \cdot x_{n/2-1} x_{n/2+1} \cdot \dots \cdot x_{n-1}$ is the $(n-1)$ -th elementary symmetric Boolean function σ_{n-1} .

Proof. An elementary rotation symmetric Boolean function g corresponding to an element in the second class is such a function: in the function there are n terms and each term contains exactly $(n-2)$ variables, which means there will be two variables missed comparing with the term $x_1 \dots x_n$ in each term. Since the terms are created by rotating from an initial term for n times, after multiplying by σ_1 , there will be $2n$ terms in which each term has degree $(n-1)$ and is present twice. As $X_i + X_i = 0$, we have that the multiple $g \cdot \sigma_1$ is 0.

The elementary rotation symmetric Boolean function corresponding to the term $x_1 \cdot \dots \cdot x_{n/2-1} x_{n/2+1} \cdot \dots \cdot x_{n-1}$ contains $n/2$ terms that are created by rotating from the term for $n/2$ times. After multiplying by σ_1 , there will be n different terms of degree $(n-1)$, i.e., σ_{n-1} .

Lemma 2. For n even, the elementary rotation symmetric Boolean function corresponding to the term $x_1 \cdot \dots \cdot x_{n-1}$ is σ_{n-1} , and

$$\sigma_{n-1} \cdot \sigma_1 = \sigma_{n-1}.$$

Proof. Only one variable is missed comparing with the term $x_1 \cdot \dots \cdot x_n$ in each term of σ_{n-1} , as σ_{n-1} contains even different terms with degree $(n-1)$, the multiple $\sigma_{n-1} \cdot \sigma_1$ contains n n -degree terms and n different kinds of $(n-1)$ -degree terms in which each kind contains $(n-1)$ terms, as $X_i + X_i = 0$, the result contains n different kinds of $(n-1)$ -degree terms, i.e., the $(n-1)$ -th elementary symmetric Boolean function σ_{n-1} .

From Lemma 1 and Lemma 2, we can deduce the following theorems easily.

Theorem 1. The FAI of an even n -variable RSBF f with degree $(n-1)$ is at most $(n-1)$.

Proof. Choose function $g = \sigma_1$ if the term $x_1 \cdot \dots \cdot x_{n/2-1} x_{n/2+1} \cdot \dots \cdot x_{n-1}$ is present in the SANF of f , and choose $g = \sigma_1 + 1$ if not. Then the degree of the multiple $f \cdot g$ is at most $(n-2)$:

Case 1: if the term $x_1 \cdot \dots \cdot x_{n/2-1} x_{n/2+1} \cdot \dots \cdot x_{n-1}$ is present in the SANF of f , then $f \cdot g = f \cdot \sigma_1$, in which, according to lemma 2, the result of the multiple of σ_1 and the elementary rotation symmetric Boolean function with degree $(n-1)$ is σ_{n-1} , and the result of the multiple of σ_1 and elementary rotation symmetric Boolean functions with degree $(n-2)$, according to lemma 1, is σ_{n-1} , too. That means the degree of $f \cdot g = f \cdot \sigma_1$ is at most $(n-2)$.

Case 2: if the term $x_1 \cdot \dots \cdot x_{n/2-1} x_{n/2+1} \cdot \dots \cdot x_{n-1}$ is not present in the SANF of f , then we have $f \cdot g = f \cdot \sigma_1 + f$, in which, the degree

of $f \cdot \sigma_1$ is $(n-1)$ and the sum of all the terms with degree $(n-1)$ is σ_{n-1} according to lemma 2. That means the degree of $f \cdot g = f \cdot \sigma_1 + f$ is at most $(n-2)$. That is to say, the FAI of an even n -variable RSBF with degree $(n-1)$ is at most $(n-1)$.

Theorem 2. The FAI of an even n -variable RSBF f is at most $(n-1)$ if both the term $x_1 \cdot \dots \cdot x_{n/2-1} x_{n/2+1} \cdot \dots \cdot x_{n-1}$ and the term $x_1 \cdot \dots \cdot x_{n-1}$ are present or neither of them is present in the SANF of f .

Proof. According to Theorem 1, the FAI of f is at most $(n-1)$ if the degree of f is $(n-1)$.

If the degree of f is n or $(n-2)$, the degree of the multiple $f \cdot \sigma_1$ is at most $(n-2)$ according to lemma 1 and lemma 2, i.e., the FAI of f is at most $(n-1)$. $\square$

V. CONCLUSIONS

By Theorem 1, we conclude that the FAI of all the even n -variable RSBFs with degree $(n-1)$ is at most $(n-1)$, which means they are not AAR functions. Theorem 2 shows that a class of even n -variable RSBFs with degree n or $(n-2)$ are not AAR because their FAI is at most $(n-1)$, too. The method of analyzing the composition of the SANF and ANF of RSBFs described in Proposition 1 will be useful to discuss the similar problems.

REFERENCES

- [1] C. Carlet. *Boolean functions for cryptography and error correcting codes*. Boolean Methods and Models. Cambridge, U.K.: Cambridge Univ. Press, 2006.
- [2] N. T. Courtois and W. Meier. "Algebraic Attacks on Stream Ciphers with Linear Feedback" *Proceedings of EUROCRYPT 2003*, LNCS, Berlin, Germany: Springer-Verlag, vol. 2656, pp. 345-359, 2003.
- [3] X. Zhang, Q. Wang, B. Wang, and Haibin Kan. "A Constructive Method of Algebraic Attack with Less Key stream Bits Date of Evaluation". *IEICE Transactions on Fundamentals*, accepted.
- [4] E. Pasalic. "Almost Fully Optimized Infinite Classes of Boolean Functions Resistant to (Fast) Algebraic Cryptanalysis". *Proceedings of ICISC 2008*, LNCS, Berlin, Germany: Springer-Verlag, vol. 5461, pp. 399-414, 2009.
- [5] F. Armknecht, C. Carlet, P. Gaborit, S. K  nzli, W. Meier, and O. Ruatta. "Efficient Computation of Algebraic Immunity for Algebraic and Fast Algebraic Attacks". *Proceedings of EUROCRYPT 2006*, LNCS, Berlin, Germany: Springer-Verlag, vol. 4004, PP. 147-164, 2006.
- [6] N. T. Courtois. "Fast Algebraic Attacks on Stream Ciphers with Linear Feedback". *Proceedings of CRYPTO 2003*, LNCS, Berlin, Germany: Springer-Verlag, vol. 2729, pp. 176-194, 2003.
- [7] F. Armknecht. "Improving Fast Algebraic Attacks". *Proceedings of FSE 2004*, LNCS, Berlin, Germany: Springer-Verlag, vol. 3017, pp. 65-82, 2004.
- [8] J. Peng, Q. Wu, and Haibin Kan. "On Symmetric Boolean Functions with High Algebraic Immunity on Even Number of Variables". *IEEE Transactions on Information Theory*, accepted.
- [9] Q. Wang, J. Peng, Haibin Kan and X. Xue. "Constructions of cryptographically significant Boolean functions using primitive polynomials". *IEEE Transactions on Information Theory*, Vol. 56, No.6, June 2010.
- [10] Y. LI, Haibin KAN, and Kokichia Futatsugi. Note on "On the Construction of Boolean Functions with Optimal Algebraic Immunity". *IEICE Transactions on Fundamentals*, Vol.E94-A, No.9, Sep. 2011.

- [11] J. Peng and Haibin Kan. "Annihilators and algebraic immunity of symmetric Boolean functions". *IEICE Transactions on Fundamentals*, Vol.E94-A, No.6, pp. -, Jun. 2011.
- [12] Y. Li, H. Wang, Haibin Kan. "Constructing Even-Variable Symmetric Boolean Functions with High Algebraic Immunity". *IEICE Transactions on Fundamentals*, Vol.E94-A, No.1, Jan. 2011.
- [13] Q.C. Wang, X.Y. Xue and Haibin Kan. "New Balanced Boolean Functions with Good Cryptographic Properties". *IEICE Transactions on Fundamentals*, Vol.E92-A, No.10, Oct. 2009.
- [14] Y. Li, M. Yang, Haibin Kan. "Constructing and Counting Boolean Functions on Even Variables with Maximum Algebraic Immunity". *IEICE Transactions on Fundamentals*, Vol.E93-A, No.3, Mar. 2010.
- [15] J. Pieprzyk and Cheng Xin Qu. "Fast Hashing and Rotation-Symmetric Functions". *Journal of Universal Computer Science*, pages 20-31, vol 5, no. 1, 1999.
- [16] P. Stańnica and S. Maitra. "Rotation, "Symmetric Boolean Functions-Count and Cryptographic Properties". *R. C. Bose Centenary Symposium on Discrete Mathematics and Applications*, Berlin, Germany: Springer-Verlag, vol. 15. Dec. 2002.
- [17] P. Stańnica, S. Maitra, and John A. Clark. "Results on Rotation Symmetric Bent and Correlation Immune Boolean Functions". *Proceedings of FSE 2004*, LNCS, Berlin, Germany: Springer-Verlag, vol. 3017, pp. 161-177. 2004.
- [18] S. Fu, C. Li, K. Matsuura, and L. Qu. "Construction of Rotation Symmetric Boolean Functions with Maximum Algebraic Immunity". *Proceedings of CANS 2009*, LNCS, Berlin, Germany: Springer-Verlag, vol. 5888, pp. 402-412. 2009.
- [19] M. Liu, D. Lin and D. Pei. "Fast Algebraic Attacks and Decomposition of Symmetric Boolean Functions". *IEEE TRANSACTIONS ON INFORMATION THEORY*, Vol. 57, No. 7, pp. 4817-4823. JULY 2011.
- [20] Q. Wang and T. Johansson. "A Note on Fast Algebraic Attacks and Higher Order Nonlinearities". *Inscrypt 2010*, LNCS, Berlin, Germany: Springer-Verlag, vol. 6584, pp. 84-98, 2010.