Discrete Applied Mathematics 162 (2014) 17–27

Contents lists available at ScienceDirect

Discrete Applied Mathematics

journal homepage: www.elsevier.com/locate/dam

On the immunity of rotation symmetric Boolean functions against fast algebraic attacks☆

Yin Zhang, Meicheng Liu *, Dongdai Lin

State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100195, PR China

ARTICLE INFO

Article history:
Received 28 February 2012
Received in revised form 16 April 2013
Accepted 22 April 2013
Available online 18 May 2013

Keywords:
Cryptography
Boolean functions
Rotation symmetric
Fast algebraic attacks
Algebraic immunity

ABSTRACT

In this paper, an efficient algorithm is proposed to estimate the immunity of rotation symmetric Boolean functions against fast algebraic attacks. The algorithm is true-biased and almost always outputs the correct answer. Besides, 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 $n - e - 1$.

1. Introduction

Boolean functions are frequently used in the design of stream ciphers, block ciphers and hash functions. One of the key 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 significant 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 [17,7]. This has led to many papers studying different cryptographic properties of rotation symmetric functions; e.g., [20,10].

In recent years, algebraic and fast algebraic attacks [1,6,4] 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 secret keys. 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 nonzero annihilators of f and $f \oplus 1$, was introduced in [16] to measure the ability of Boolean functions to resist algebraic attacks. It is well known that $\lceil \frac{n}{2} \rceil$ is maximum algebraic immunity of n-variable Boolean functions. The identification and construction of Boolean functions with maximum algebraic immunity have been researched in a large number of papers; e.g., [8,12,11,3,14].

It has been demonstrated that the resistance of Boolean functions against fast algebraic attacks is not fully covered by algebraic immunity [5,2,13]. A preprocessing of fast algebraic attacks on LFSR-based stream ciphers, which uses a Boolean function f as the filter or combination generator, is to find a function g of small degree such that the product gf has degree

☆ Supported by the National 973 Program of China under Grant 2011CB302400, the National Natural Science Foundation of China under Grant 61173134, and the Strategic Priority Research Program of the Chinese Academy of Sciences under Grant XDA06010701.

* Corresponding author. Tel.: +86 1082546582x8090; fax: +86 1082546564.
E-mail address: meicheng.liu@gmail.com (M. Liu).

0166-218X/$ – see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.dam.2013.04.014

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 [4]. A Boolean function is said to be perfect algebraic immune ($\mathcal{PAI}$) [15], 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 $f = h \oplus l$ with l being the linear part of f [4]. In this case, $e = 1$ and d equals the algebraic degree of the function f, where the function g can be considered as the nonzero constant. Thus a $\mathcal{PAI}$ function has algebraic degree at least $n - 1$.

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. [13] stated that almost all the symmetric Boolean functions behave badly against fast algebraic attacks, and proved that no symmetric Boolean functions are $\mathcal{PAI}$. In [18,19], P. Rizomiliotis introduced a method to evaluate the behavior of Boolean functions against fast algebraic attacks using univariate polynomial representation. In [15], the authors improved both Armknecht's and Rizomiliotis's methods, showed the maximum immunity to fast algebraic attacks, and proved that there exist n-variable $\mathcal{PAI}$ functions if and only if n is one more than or equal to a power of two.

In this paper, we study rotation symmetric Boolean functions in terms of the immunity against fast algebraic attacks. We develop the techniques of [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 Boolean function f, there exists a rotation symmetric function g of degree at most e such that gf has degree at most d, if and only 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]. Based on this result, we propose a true-biased algorithm for computing the immunity of rotation symmetric Boolean functions against fast algebraic attacks, which is faster than Armknecht's algorithm by a factor of n and uses less memory by a factor of n^2. The computer investigations suggest that our algorithm almost always outputs the correct answer and in some cases, e.g., when n equals a power of two, it always outputs the correct answer.

Further, several properties of the matrix $S(f; e, d)$ are derived 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), a rotation symmetric function on n variables always admits a nonzero rotation symmetric function g of degree at most e such that gf has degree at most $n - e - 1$ for some $e \leq n/3$. The results imply that such functions are not $\mathcal{PAI}$.

This paper is organized as follows. In Section 2 some basic concepts and facts are provided. Section 3 introduces the matrix $S(f; e, d)$ and presents an algorithm for efficient computation of the immunity of rotation symmetric Boolean function against fast algebraic attacks. Section 4 derives several properties of the matrix $S(f; e, d)$ while Section 5 shows the nonexistence of rotation symmetric $\mathcal{PAI}$ functions for even $n \neq 2^m$. Section 6 concludes the paper.

2. Preliminary

2.1. Basic definitions and notations

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,

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

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 that 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 $\mathbb{F}_2$:

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

where $c = (c_1, \ldots, c_n)$ and $x = (x_1, \ldots, x_n)$, 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 $x_1, x_2, \ldots, x_n$.