Information Sciences 421 (2017) 181–203

Contents lists available at ScienceDirect

Information Sciences

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

Results on highly nonlinear Boolean functions with provably good immunity to fast algebraic attacks[☆]

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 13 March 2015
Revised 29 August 2017
Accepted 31 August 2017
Available online 7 September 2017

Keywords:
Cryptography
Boolean functions
Fast algebraic attacks
Algebraic immunity
Nonlinearity

ABSTRACT

In the last decade, algebraic and fast algebraic attacks are regarded as the most successful attacks on LFSR-based stream ciphers. Since the notion of algebraic immunity was introduced, the properties and constructions of Boolean functions with maximum algebraic immunity have been researched in a large number of papers. However, there are few results with respect to Boolean functions with provably good immunity against fast algebraic attacks. In previous literatures, only Carlet–Feng function was proven to have good immunity to fast algebraic attacks.

In this paper, we first study a large family of highly nonlinear Boolean functions in terms of the immunity to fast algebraic attacks, which includes the functions of Tu–Deng, the functions of Tang et al. and the functions of Jin et al. Based on a sufficient and necessary condition for measuring the immunity of Boolean functions against fast algebraic attacks using bivariate polynomial representation, we propose an efficient method for estimating the immunity of the functions of such family. Then we prove that a family of $2k$-variable Boolean functions, including the function recently constructed by Tang et al., are almost perfect algebraic immune for any integer $k \geq 3$. More exactly, they achieve optimal algebraic immunity and almost perfect immunity to fast algebraic attacks. The functions of such family are balanced and have optimal algebraic degree. Besides, we prove a lower bound on their nonlinearity based on the work of Tang et al. which is better than that of Carlet–Feng function. It is also checked for $3 \leq k \leq 9$ that the exact nonlinearity of such functions is very good, which is slightly smaller than that of Carlet–Feng function, and some functions of this family even have a slightly larger nonlinearity than Tang's et al. function. To sum up, among the known functions with provably good immunity against fast algebraic attacks, the functions of this family make a trade-off between the exact value and the lower bound of nonlinearity.

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

[☆] This work was partially presented as an extended abstract [20] at ISIT 2014 where all the proofs are omitted due to the page limit. This work was supported by the National Natural Science Foundation of China under Grants 61303258 and 61672516.

[*] Corresponding author.
E-mail address: meicheng.liu@gmail.com (M. Liu).

http://dx.doi.org/10.1016/j.ins.2017.08.097
0020-0255/© 2017 Elsevier Inc. All rights reserved.

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.

In recent years, algebraic and fast algebraic attacks [1,6,7] have been regarded as the most successful attacks on 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; fast algebraic attacks obtain equations of small degree by linear combination.

Thus the algebraic immunity ($\mathcal{AI}$), the minimum algebraic degree of annihilators of f or $f+1$, was introduced by Meier et al. [21] to measure the ability of Boolean functions to resist algebraic attacks. It was shown by Courtois and Meier [7] that maximum $\mathcal{AI}$ of n-variable Boolean functions is $\lceil \frac{n}{2} \rceil$. Constructions of Boolean functions with maximum $\mathcal{AI}$ were researched in a large number of papers, e.g., [4,9,12,16,17,24,27]. However, there are few results referring to constructions of Boolean functions with provable good immunity against fast algebraic attacks.

A preprocessing of fast algebraic attacks on LFSR-based stream ciphers, which use a Boolean function f: $GF(2)^n \rightarrow GF(2)$ 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. The resistance against fast algebraic attacks is not covered by algebraic immunity [2,8,18]. At Eurocrypt 2006, Armknecht et al. [2] introduced an effective algorithm for determining the immunity against fast algebraic attacks, and showed that a class of symmetric Boolean functions (the majority functions) have poor resistance against fast algebraic attacks despite their resistance against algebraic attacks. Later Liu et al. [18] stated that almost all the symmetric functions including these functions with good algebraic immunity behave badly against fast algebraic attacks.

In [6] Courtois proved that for any pair of positive 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. This result reveals an upper bound on maximum immunity to fast algebraic attacks. It implies that the function f has maximum possible resistance against fast algebraic attacks, if for any pair of positive 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. Such functions are said to be perfect algebraic immune ($\mathcal{PAI}$) [19]. 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 [6]. In this case, e equals 1 (i.e., the degree of the linear function l) and d equals the degree of h (i.e., the degree of f), where g can be considered as the nonzero constant. Thus $\mathcal{PAI}$ functions have algebraic degree at least $n-1$. A $\mathcal{PAI}$ function also achieves maximum $\mathcal{AI}$. As a consequence, a $\mathcal{PAI}$ function has perfect immunity against classical and fast algebraic attacks. Besides, it is shown that a perfect algebraic immune function behaves good against probabilistic algebraic attacks as well [19]. Although preventing classical and fast algebraic attacks is not sufficient for resisting algebraic attacks on the augmented function [11], the resistance against these attacks depends on the update function and tap positions used in a stream cipher and in actual fact it is not a property of the Boolean function. In [19] Liu et al. proved that there are n-variable $\mathcal{PAI}$ functions if and only if $n=2^s$ or 2^s+1. More precisely, there exist n-variable $\mathcal{PAI}$ functions with degree $n-1$ (balanced functions) if and only if $n=2^s+1$; there exist n-variable $\mathcal{PAI}$ functions with degree n (unbalanced functions) if and only if $n=2^s$.

It is extremely intractable to show a Boolean function to be immune to fast algebraic attacks from a mathematical point of view. Although several classes of Boolean functions, e.g., [4,22,23,27,28], are observed through computer experiments to have good behavior against fast algebraic attacks, in previous literatures only Carlet–Feng function (see [4,10]), which is affine equivalent to discrete logarithm function [13], was proven to have good immunity against fast algebraic attacks. As a matter of fact, Carlet–Feng function was shown in [19] to be optimal against fast algebraic attacks as well as algebraic attacks. The results of [19] imply that Carlet–Feng function is $\mathcal{PAI}$ for $n=2^s+1$ and is almost $\mathcal{PAI}$ for $n \neq 2^s+1$.

In this paper, we mainly study the immunity of Boolean functions against fast algebraic attacks using bivariate polynomial representation.

Based on bivariate polynomial representation, we prove that a Boolean function $f(x, y)$ admits no nonzero function $g(x, y)$ of degree at most e such that the product $g(x, y)f(x, y)$ has degree at most d if and only if a related matrix $B(f; e, d)$, whose elements are represented by the coefficients of the bivariate polynomial representation of the function f, has full column rank.

Then, we investigate the immunity against fast algebraic attacks for a large family of functions that has a form as

$$\tau(x,y) = \phi(xy^r) + (x^{2^k-1}+1)\psi(y) + (y^{2^k-1}+1)\varphi(x),$$

where ϕ, ψ and φ are Boolean functions from $\mathbb{F}_{2^k}$ into $\mathbb{F}_2$. We first present several properties of the matrix $B(\tau;\, e, d)$. Two observations on this matrix $B(\tau;\, e, d)$ are that after appropriate row transformations it can be represented by

$$\begin{pmatrix} * \\ B^*(\phi(xy^r);e,d) \end{pmatrix}, \tag{1}$$

and that after appropriate column transformations it can be represented by

$$\begin{pmatrix} *, & B_*(\phi(xy^r);e,d) \end{pmatrix}, \tag{2}$$

where $B^*(\phi(xy^r);\, e, d)$ and $B_*(\phi(xy^r);\, e, d)$ are submatrices of $B(\phi(xy^r);\, e, d)$. Our observation on the matrix $B(\phi(xy^r);\, e, d)$ is that after appropriate matrix transformations it is a quasidiagonal matrix. Then, based on these properties, we propose an efficient method to determine the immunity of $\tau(x, y)$ against fast algebraic attacks through computations of submatrices of $B(\phi(xy^r);\, e, d)$.