Advances in Mathematics of Communications
Volume 11, No. 2, 2017, 373–377
doi:10.3934/amc.2017031

FAST ALGEBRAIC IMMUNITY OF BOOLEAN FUNCTIONS

Sihem Mesnager

Department of Mathematics
University of Paris VIII and Paris XIII and Télécom ParisTech
LAGA, UMR 7539, CNRS, Sorbonne Paris Cité

Gérard Cohen

Télécom ParisTech, department INFRES/MIC2, CNRS, UMR 5441

(Communicated by Domingo Gomez-Perez)

Abstract. Since 1970, Boolean functions have been the focus of a lot of attention in cryptography. An important topic in symmetric ciphers concerns the cryptographic properties of Boolean functions and constructions of Boolean functions with good cryptographic properties, that is, good resistance to known attacks. An important progress in cryptanalysis areas made in 2003 was the introduction by Courtois and Meier of algebraic attacks and fast algebraic attacks which are very powerful analysis concepts and can be applied to almost all cryptographic algorithms. To study the resistance against algebraic attacks, the notion of algebraic immunity has been introduced. In this paper, we use a parameter introduced by Liu and al., called *fast algebraic immunity*, as a tool to measure the resistance of a cryptosystem (involving Boolean functions) to fast algebraic attacks. We prove an upper bound on the fast algebraic immunity. Using our upper bound, we establish the weakness of trace inverse functions against fast algebraic attacks confirming a recent result of Feng and Gong.

1. Introduction

Symmetric cryptosystems are commonly used for encrypting and decrypting owing to their efficiency. A classical model of symmetric cryptosystem are stream ciphers. Most of them are composed of one or several Linear Feedback Shift Register (LFSR) combined or filtered by a Boolean function. These cryptosystems have been the objects of a lot of cryptanalyses and several design criteria have been proposed concerning the filtering or combining functions. In several stream ciphers, the generation of the keystream consists of a linear part, producing a sequence with a large period, usually composed of one or several LFSR's, and a nonlinear combining or filtering function f that produces the output, given the state of the linear part. Until 2003, a list of some main classical cryptographic criteria for designing such a function f was known (see [1]) In 2003, new kinds of attacks drawn from an original idea of Shannon [13] emerged; these attacks are called *algebraic attacks* and *fast algebraic attacks* [4, 5, 9].

These attacks have changed the situation in symmetric cryptography by adding a new criterion of considerable importance to this list.They proceed by modeling

2010 *Mathematics Subject Classification:* xxxxxxxxxxxxxxx.
Key words and phrases: Boolean functions, stream cipher, algebraic immunity, algebraic attacks, fast algebraic attacks.

the problem of recovering the secret key by means of an over-defined system of multivariate nonlinear equations of algebraic degree at most $\deg(f)$. The core of algebraic attacks is to find out low degree Boolean functions $g \neq 0$ and h such that $fg = h$. It is shown in [9] that this is equivalent to the existence of low degree *annihilators* of f, that is, of n-variable Boolean functions g such that $f \cdot g = 0$ or $(1+f) \cdot g = 0$. The minimum degree of such g is called the *algebraic immunity* of f, and we denote it by $AI(f)$. It must be as high as possible (the optimum value of $AI(f)$ being equal to $\lceil \frac{n}{2} \rceil$). Fast algebraic attacks proceed in a different way but having a high algebraic immunity is not only a necessary condition for resistance to standard algebraic attacks but also for resistance to fast algebraic attacks.

Nowadays, the resistance against algebraic attacks and fast algebraic attacks, is considered as an important cryptographic property for Boolean functions used in stream ciphers. Both attacks are very powerful analysis concepts and can be applied to almost all cryptographic algorithms.

The notion of algebraic immunity has received a wide attention since it is a powerful tool to measure the resistance of standard algebraic attacks. Nevertheless, an algebraic tool to handle the resistance to fast algebraic attacks is not clearly identified in the literature. To fill the gap, we introduce in Section 3 the notion of the so-called *fast algebraic immunity* as a tool to measure the resistance of a cryptosystem (involving Boolean functions) to fast algebraic attacks. Next, in Section 4, we focus on the inverse function $x \mapsto x^{-1}$ over the finite field $\mathbb{F}_{2^n}$ which is an important multi-output Boolean function, firstly introduced by Niberg [11]. Such a function has several good cryptographic properties, including involutivity, high nonlinearity, high algebraic degree, almost optimal differential uniformity etc. It has also been used and adopted in many symmetric algorithms in stream and block ciphers. Using our tool, we demonstrate easily the weakness of trace inverse functions against fast algebraic attacks, confirming a recent result of Feng and Gong.

This paper is organized as follows. Formal definitions and necessary preliminaries are introduced in Section 2. Our main contributions described above are presented in Sections 3 and 4.

2. Preliminaries and notation

Let n be any positive integer. In this paper, we shall denote by $\mathcal{B}_n$ the set of all n-variable Boolean functions over $\mathbb{F}_2^n$. Any n-variable Boolean function f (that is an application from $\mathbb{F}_2^n$ to $\mathbb{F}_2$) admits a unique *algebraic normal form* (ANF), that is, a representation as a multivariate polynomial over $\mathbb{F}_2$

$$f(x_1, \ldots, x_n) = \bigoplus_{I \subseteq \{1,\ldots,n\}} a_I \prod_{i \in I} x_i,$$

where the a_I's are in $\mathbb{F}_2$. The terms $\prod_{i \in I} x_i$ are called *monomials*. The *algebraic degree* $\deg(f)$ of a Boolean function f equals the maximum degree of those monomials whose coefficients are nonzero in its algebraic normal form. If we identify $\mathbb{F}_2^n$ with the Galois field $\mathbb{F}_{2^n}$ of order 2^n, Boolean functions of n-variables are then the binary functions over the Galois field $\mathbb{F}_{2^n}$ (one can always endow this vector space with the structure of a field, thanks to the choice of a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$) of order 2^n. The *weight* of f, denoted by $wt(f)$, is the *Hamming weight* of the image vector of f, that is, the cardinality of its support $supp(f) := \{x \in \mathbb{F}_{2^n} \mid f(x) = 1\}$.
For any positive integer k, and r dividing k, the trace function from $\mathbb{F}_{2^k}$ to $\mathbb{F}_{2^r}$, denoted by Tr_r^k, is the mapping defined as: $\forall x \in \mathbb{F}_{2^k}$, $Tr_r^k(x) := \sum_{i=0}^{\frac{k}{r}-1} x^{2^{ir}}$.

In particular, we denote the *absolute trace* over $\mathbb{F}_2$ of an element $x \in \mathbb{F}_{2^n}$ by $Tr_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}$.
Every non-zero Boolean function f defined on $\mathbb{F}_{2^n}$ has a (unique) trace expansion of the form:

$$\forall x \in \mathbb{F}_{2^n}, \quad f(x) = \sum_{j \in \Gamma_n} Tr_1^{o(j)}(a_j x^j) + \epsilon(1 + x^{2^n-1})$$

called its polynomial form, where Γ_n is the set of integers obtained by choosing one element in each cyclotomic class of 2 modulo 2^n-1, $o(j)$ is the size of the cyclotomic coset of 2 modulo 2^n-1 containing j, $a_j \in \mathbb{F}_{2^{o(j)}}$ and, $\epsilon = wt(f)$ modulo 2. The algebraic degree of f is equal to the maximum 2-weight of an exponent j for which $a_j \neq 0$ if $\epsilon = 0$ and to n if $\epsilon = 1$. We recall that the 2-weight of an exponent j, that we denote $w_2(j)$, is the number of 1 in its binary expansion.

The algebraic immunity [9] of a Boolean function f quantifies the resistance to the standard algebraic attack of the pseudo-random generators using it as a nonlinear function. It is defined as follows.

Definition 1 (Algebraic Immunity)**.** Let f be an n-variable Boolean function. An n-variable Boolean function g is said to be an *annihilator* of f if the product $f \cdot g$ is null (that is, the support of g is included in the support of $1 \oplus f$). The algebraic immunity of f is the minimum algebraic degree of all the nonzero annihilators of f or of $f \oplus 1$. The *algebraic immunity* of f, is denoted by $AI(f)$.

Clearly, the algebraic immunity of a Boolean function f is less than or equal to its algebraic degree since $1 \oplus f$ is an annihilator of f. As shown in [5], we have $AI(f) \leq \lceil \frac{n}{2} \rceil$ as already recalled above. Obviously, we have

Proposition 2. *Let f be a Boolean function, then $AI(1 + f) = AI(f)$.*

3. Fast algebraic immunity

Let f be an n- variable Boolean function. Courtois [4](Theorem 7.2.1) has shown that there always exists g with $\deg(g) > 1$ such that $\deg(g) + \deg(f \cdot g) \leq n$. If there exists a nonzero n-variable Boolean function g with low algebraic degree with respect to n, then a fast algebraic attack (FAA) might be efficient. It was said that f has optimal resistance against fast algebraic attack if and only if there does not exist a nonzero n-variable Boolean function g of degree at most e such that $\deg(g) + \deg(f \cdot g) \leq n$ and $e < \frac{n}{2}$ ([2, 6]). In general, to study the resistance of f against FAA's, we need to determine whether $\deg(f \cdot g) \geq n - e$ holds for any nonzero n-variable Boolean function g of degree at most e ([12, 6]). To this end, it has been introduced in [8] a tool to evaluate the resistance f to FAA's that we recall below (note that in [3] (Definition 2), the authors have proposed very recently a more precise definition).

Definition 3 (Fast Algebraic Immunity)**.** Let f be an n-variable Boolean function. We call *fast algebraic immunity* of f, denoted by $FAI(f)$, the minimum value between $2AI(f)$ and the smallest value taken by $\deg(g) + \deg(f \cdot g)$ when g ranges over the set of non-constant n-variable Boolean functions of algebraic degree less than $AI(f)$. That is,

$$FAI(f) = \min\left(2AI(f), \min_{g \in \mathcal{B}_n | 1 \leq \deg g < AI(f)} (\deg g + \deg(f \cdot g))\right).$$

Fast algebraic immunity FAI is invariant under affine transformations:

Proposition 4. *Let f be an n-variable Boolean function. Let A be an affine automorphism of $\mathbb{F}_{2^n}$. Then $FAI(f \circ A) = FAI(f)$.*

Proof. Recall that the standard algebraic immunity is invariant under affine transformations: $AI(f \circ A) = AI(f)$. Now, observe that $\deg g + \deg(f \cdot g) = \deg(g \circ A) + \deg(f \circ A \cdot g \circ A)$. The result follows then straightforwardly from noting that $\{g \in \mathcal{B}_n \mid 1 \leq \deg(g) < AI(f)\} = \{g \circ A \mid g \in \mathcal{B}_n, 1 \leq \deg(g) < AI(f)\}$. □

4. Study of the resistance of Boolean power functions to FAA by means of fast algebraic immunity

The resistance of Boolean power functions has been studied in [6, 10]. In this paper, we are also interested in this topic but with a different approach. Indeed, we believe that having a parameter to study the resistance to FAA would help. A candidate is the FAI introduced in [8] and recalled in Definition 3. Boolean power functions are functions of the form $Tr_1^n(\gamma x^d)$ where $\gamma \in \mathbb{F}_{2^n}$ and d is a positive integer. Given a positive integer d, let $\mathcal{W}_d$ be the set of integers t lying between 1 and $2^n - 2$ such that $w_2(t) \leq d$.

Proposition 5. *Let f of algebraic degree d be such that $f(0) = 0$. Then*

$$FAI(f) \leq \min\Big(2AI(f), \min_{e \in \mathcal{W}_{AI(f)-1}} \big(w_2(e) + \max_{\substack{0 \leq l \leq n-1 \\ (r,t) \in \mathcal{W}_e \times \mathcal{W}_d}} w_2(r + 2^l t)\big)\Big).$$

Proof. Let $1 \leq e < AI(f)$. Let g be of algebraic degree e such that $g(0) = 0$. Write $f(x) = \sum_{t \in \mathcal{W}_d} Tr_1^n(\gamma_t x^t)$ and $g(x) = \sum_{r \in \mathcal{W}_e} Tr_1^n(\beta_r x^r)$. Then $f(x)g(x) = \sum_{l=0}^{n-1} \sum_{(r,t) \in \mathcal{W}_e \times \mathcal{W}_d} Tr_1^n\left(\beta_t \gamma_t^{2^l} x^{r+2^l t}\right)$. Thus

$$\deg(f \cdot g) \leq \max_{0 \leq l \leq n-1, (r,t) \in \mathcal{W}_e \times \mathcal{W}_d} w_2(r + 2^l t).$$

The result follows then straightforwardly. □

Let us now state a result established in [10]. For a binary string, λ consecutive 1 preceded by a zero and followed by a zero is called a *run* of ones of length λ. We are only interested in the number of runs of ones in a given binary string and not in their lengths. Furthermore the runs are considered to be cyclic. For example 1100011100001111 has two runs and not three.

Lemma 6 ([10, Lemma 1])**.** *Let $f(x) = Tr_1^n(\gamma x^d)$ where $\gamma \in \mathbb{F}_{2^n}$ and d is a positive integer. There exists g of algebraic degree $\left\lceil \frac{n}{\lfloor \sqrt{n} \rfloor} \right\rceil$ such that*

$$\deg(f \cdot g) \leq u\lfloor \sqrt{n} \rfloor + \left\lceil \frac{n}{\lfloor \sqrt{n} \rfloor} \right\rceil - 1$$

where u is the number of runs of 1 in the binary representation of d.

Collecting together Proposition 5 and Lemma 6, one gets

Proposition 7. *Let $f(x) = Tr_1^n(\gamma x^d)$ where $\gamma \in \mathbb{F}_{2^n}$ and d is a positive integer. Suppose that $AI(f) \geq \left\lceil \frac{n}{\lfloor \sqrt{n} \rfloor} \right\rceil + 1$. Then*

$$FAI(f) \leq u\lfloor \sqrt{n} \rfloor + 2\left\lceil \frac{n}{\lfloor \sqrt{n} \rfloor} \right\rceil - 1$$

where u is the number of runs of 1 in the binary representation of d.

It has been shown in [7] that the algebraic immunity AI of $Tr_1^n(\lambda x^{-1}) = Tr_1^n(\lambda x^{2^n-2})$ is equal to $\lfloor\sqrt{n}\rfloor + \left\lceil \frac{n}{\lfloor\sqrt{n}\rfloor} \right\rceil - 2 \geq \left\lceil \frac{n}{\lfloor\sqrt{n}\rfloor} \right\rceil + 1$ provided that $n \geq 4$. Now, observe that there is a single run in $2^n - 2$ proving that

Proposition 8. *Let $n \geq 4$. Then*

$$FAI(Tr_1^n(\lambda x^{-1})) \leq \min\left(2\lfloor\sqrt{n}\rfloor + 2\left\lceil \frac{n}{\lfloor\sqrt{n}\rfloor} \right\rceil - 4, \lfloor\sqrt{n}\rfloor + 2\left\lceil \frac{n}{\lfloor\sqrt{n}\rfloor} \right\rceil - 1\right).$$

Remark 9. Observe that $2\lfloor\sqrt{n}\rfloor + 2\left\lceil \frac{n}{\lfloor\sqrt{n}\rfloor} \right\rceil - 4 > \lfloor\sqrt{n}\rfloor + 2\left\lceil \frac{n}{\lfloor\sqrt{n}\rfloor} \right\rceil - 1$ whenever $n \geq 16$.

5. Concluding remarks

In this paper, we use the notion of fast algebraic immunity introduced in [8] to measure the resistance to FAA of Boolean power functions. We provide some results related to this parameter and study the case of the trace inverse function. A natural extension would be to study other important classes of Boolean functions and use it to investigate their resistance to FAA's.

References

[1] C. Carlet, Boolean functions for cryptography and error correcting codes, in *Boolean Models and Methods in Mathematics, Computer Science, and Engineering* (eds. Y. Crama and P.L. Hammer), Cambridge Univ. Press, 2010, 257–397.

[2] C. Carlet and K. Feng, An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity, in *Adv. Crypt.–ASIACRYPT 2008*, Springer, 2008, 425–440.

[3] C. Carlet and D. Tang, Enhanced Boolean functions suitable for the filter model of pseudo-random generator, *Des. Codes Crypt.*, **76** (2015), 571–587.

[4] N. Courtois, Fast algebraic attacks on stream ciphers with linear feedback, *Advances in Cryptology–CRYPTO 2003*, Springer, 2003, 177–194.

[5] N. Courtois and W. Meier, Algebraic attacks on stream ciphers with linear feedback, in *Advances in Cryptology*, Springer, 2002, 346–359.

[6] Y. Du, F. Zhang and M. Liu, On the resistance of Boolean functions against fast algebraic attacks, in *ICISC 2011*, Springer, 2012, 261–274.

[7] X. Feng and G. Gong, On algebraic immunity of trace inverse functions over finite fields with characteristic two, Cryptology ePrint Archive: Report 2013/585.

[8] M. Liu, D. Lin and D. Pei, Fast algebraic attacks and decomposition of symmetric Boolean functions, *IEEE Trans. Inf. Theory*, **57** (2011), 4817–4821.

[9] W. Meier, E. Pasalic and C. Carlet, Algebraic attacks and decomposition of Boolean functions, in *Eurocrypt 2004*, Springer, 2004, 474–491.

[10] Y. Nawaz, G. Gong and K. C. Gupta, Upper bounds on algebraic immunity of Boolean power functions, in *13th Int. Workshop Fast Softw. Encrypt.*, Springer, 2006, 375–389.

[11] K. Nyberg, Differentially uniform mappings for cryptography, in *Eurocrypt 1993*, Springer, 1994, 55–64.

[12] E. Pasalic, Almost fully optimized infinite classes of Boolean functions resistant to (fast) algebraic cryptanalysis, in *ICISC 2008*, Springer, 2008, 399–414.

[13] C. Shannon, Communication theory of secrecy systems, *Bell Syst. Techn. J.*, **28** (1949), 656–715.

Received February 2016; revised March 2016.

E-mail address: smesnager@univ-paris8.fr
E-mail address: cohen@telecom-paristech.fr