Journal of Applied Mathematics & Bioinformatics, vol.3, no.1, 2013, 57-81
ISSN: 1792-6602 (print), 1792-6939 (online)
Scienpress Ltd, 2013

Algebraic attacks on stream ciphers: recent developments and new results

Konstantinos Limniotis[1,2]

Abstract

The security of stream ciphers against algebraic attacks is studied in this paper. Emphasis is given on analysing the properties of the underlying Boolean functions that need to be satisfied, such as the algebraic and the fast algebraic immunity. We present an overview of the constructions of functions with maximum algebraic immunity discovered recently, whereas known relationships with other cryptographic criteria are also reviewed. Moreover, we investigate the link between the fast algebraic immunity and the correlation immunity of Boolean functions, where a trade-off between resistance to correlation and fast algebraic attacks is proved. It is also shown that a known construction of cryptographic functions does not behave well with respect to (fast) algebraic attacks.

Mathematics Subject Classification: 94A60
Keywords: algebraic attacks; algebraic immunity; cryptography; correlation immunity; stream ciphers

[1] Hellenic Data Protection Authority, e-mail: klimniotis@dpa.gr
[2] National and Kapodistrian University of Athens, e-mail: klimn@di.uoa.gr

Article Info: *Received* : November 1, 2012. *Revised* : January 30, 2013
Published online : March 30, 2013

1 Introduction

Stream ciphers form an important class of cipher systems. They are widely used to provide confidentiality in environments characterized by a limited computing power or memory capacity, and the need to encrypt at high speed (e.g. wireless communications). The advantages of stream ciphers rest with the fact that they require only few gates in VLSI circuitry and are easy to build, whereas they are able to provide a high security level; in addition, since they avoid error propagation, they are preferable in applications where errors may occur during the transmission. Stream ciphers are also well suited to military cryptography, since only the device generating the keystream may be subject to strict security measures; other devices which will be fed by the keystream and perform the encryption do not require such stringent environments.

In binary additive stream ciphers, a keystream $k = k_1k_2\ldots$, which is known only to the transmitter and the receiver, is xor-ed with the original message (plaintext) $m = m_1m_2\ldots$, resulting in the encrypted message (ciphertext) $c = c_1c_2\ldots$ that satisfies $c_i = m_i \oplus k_i$ for all i. In general, the security of such systems is strongly contingent on the unpredictability of the keystreams. It should be stressed that if the keystream is truly random and its length is equal to the length of the plaintext, then such a system, being called *one-time pad* and proposed by an Army Officer Joseph Mauborgne as an improvement of the so-called Vernam cipher introduced by the engineer Gilbert Vernam in 1918, has perfect secrecy as it is pointed out in Claude Shannon's pioneeiring work [45]. However, the one-time pad is of limited practical value since generation of truly random keystreams is not efficient, whereas the requirement for having a keystream of length equal to the length of the message introduces a huge key distribution problem. Hence, the design of stream ciphers strives to resemble the one-time pad, that is to construct efficient keystream generators producing pseudorandom sequences of large period which closely resemble truly random sequences.

Linear Feedback Shift registers (LFSR) are basic building blocks for keystream generators in stream ciphers, due to their appealing properties and ease of implementation. A typical diagram of a LFSR is depicted in Figure 2. Each such circuit consists of n consecutive 2-state storage units, where at each clock pulse the content of any stage (0 or 1) is shifted to the next stage; the con-

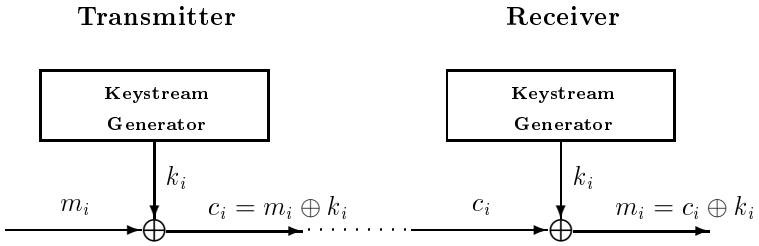

Figure 1: A typical stream cipher operation

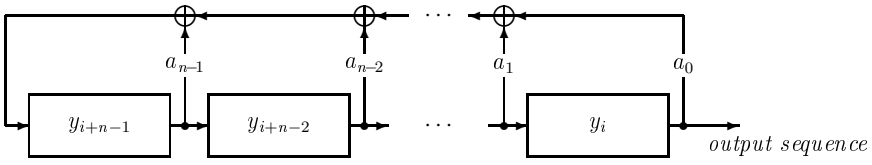

Figure 2: A diagram of a Linear Feedback Shift Register

tent of the last (leftmost) stage is computed according to a feedback function. However, the *linear complexity*, i.e. the length of the shortest LFSR generating a given sequence, is important for assessing resistance to several cryptanalytic attacks, like the *Berlekamp–Massey algorithm* [32], but also more recent type of attacks [43]; in particular, the linear complexity represents the minimum amount of the sequence required to fully specify the remainder. Hence, it is evident that any keystream should have high linear complexity and, thus, LFSRs do not suffice to provide sequences of cryptographic strength.

As a response to this, several techniques have been proposed to increase the linear complexity obtained by LFSRs, such as nonlinear filters and nonlinear combiners [36] (see Figures 3 and 4 respectively). The security of these systems is mainly attributed to the properties of the underlying Boolean functions that are used as filter/combiner functions; namely, cryptographic Boolean functions need to satisfy specific criteria, such as high algebraic degree, in order to ensure resistance against several cryptanalytic attacks [36]. As most constructions are ad-hoc, finding good keystream generators, which is strongly contigent to identifying Boolean functions with good cryptographic properties, is of great theoretical and practical value.

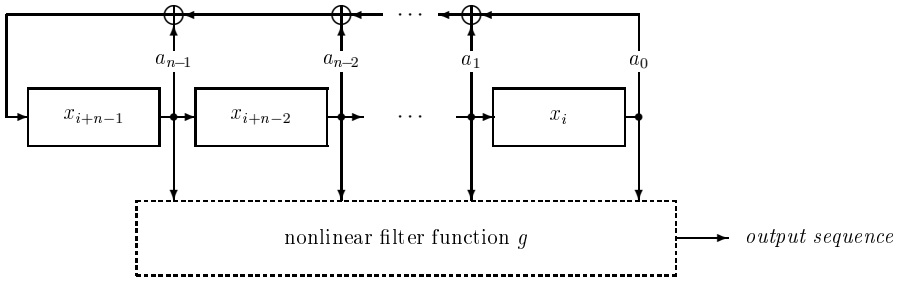

Figure 3: The diagram of a nonlinear filter generator

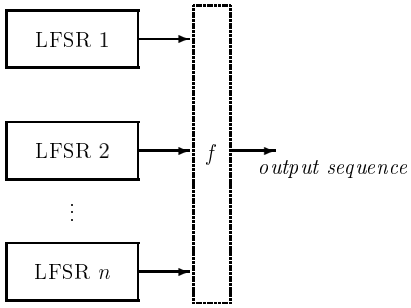

Figure 4: The diagram of a nonlinear combiner generator

Apart from its algebraic degree, the *nonlinearity* of a Boolean function is among the most significant cryptographic properties; it is defined as the minimum distance from all the affine functions, and indicates whether attacks based on linear cryptanalysis [33] and best affine approximations [16] can be prevented. With the appearance of more recent attacks, such as low order approximation attacks [22], Boolean functions need also have the property that they cannot be approximated adequately by low degree functions. Hence, their *rth order nonlinearity* [4], that is the minimum distance from all functions of degree at most r, need to be computed as a significant cryptographic measure.

Another important cryptographic criterion of a Boolean function is the so-called *correlation immunity*, which is a measure of the degree to which its outputs are uncorrelated with some subset of its inputs. A function should have high correlation immunity in order to thwart specific cryptanalytic attacks, such as correlation attacks [46, 47, 35].

A more recent attack, attracting great attention, is the so-called algebraic

attack, which exploits the structure of the underlying Boolean functions so as to construct overdefined systems of nonlinear multivariate equations to facilitate the determination of the secret key [12]. As a result of the analysis derived in [34], the following property is stated as a prerequisite for any Boolean function f of n variables in order to prevent algebraic attacks: there should not be a function g of low degree satisfying either $f * g = 0$ or $(f + 1) * g = 0$. This observation leads to the definition of the *algebraic immunity* as a significant cryptographic criterion for Boolean functions, which indicates the degree of the minimum-degree function g satisfying the foregoing condition.

Algebraic attacks may be further improved by exploiting linear relations among the keystream bits; this approach, called *fast algebraic attack*, was first proposed in [13] and has been further investigated in [1, 2, 17]. Fast algebraic attacks may be efficiently applied to cryptographic systems that are resistant to conventional algebraic attacks, although they require knowledge of consecutive keystream bits (which is not needed in algebraic attacks).

A maximum value for the algebraic immunity is also a necessary (though not sufficient) condition for withstanding such attacks [38]; the notion of *fast algebraic immunity* has been recently intoduced in [29] to assess the resistance against fast algebraic attacks. In general, constructions of functions resistant to fast algebraic attacks, as well as the characterization of such functions with respect to other cryptographic criteria, remains a challenging open problem.

In this paper, we focus on properties of cryptographic Boolean functions in terms of their resistance against both conventional and fast algebraic attacks. More precisely, the contribution of the paper is twofold. First, we present a state of the art of the constructions of Boolean functions with maximum algebraic immunity, whereas their resistance against fast algebraic attacks is also dicussed; we also survey known relationships between algebraic immunity and other cryptographic criteria, such as nonlinearity and correlation immunity. The contribution of the paper is the identification of a trade-off between resistance to correlation and fast algebraic attacks; it is the first time that such a relationship is proved, given the fact that the connection between the correlation and algebraic immunity is known to be an interesting open problem as it was recently stated in [18, p. 65]. Furthermore, we show that correlation-immune functions obtained via the well-known Siegenthaler's construction do not behave well in terms of fast algebraic attacks, whereas it is also shown that

they may also be vulnerable to low-order approximation attacks if construction parameters are not properly chosen.

The paper is organised as follows; the basic definitions and the notation used are introduced in Section 2. A survey of (fast) algebraic attacks is given in Section 3, whereas known relationships between algebraic immunity and other cryptographic measures are also described. A tradeoff between resistance to correlation and fast algebraic attack is proved in Section 4; moreover, we further investigate a known class of correlation immune functions (obtained via the Siegenthaler's construction), illustrating that this class may be vulnerable to fast algebraic attacks. Finally, concluding remarks are given in Section 5.

2 Preliminaries

Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function, where $\mathbb{F}_2 = \{0, 1\}$ is the binary field. The set of Boolean functions on n variables is denoted by $\mathbb{B}_n$. The truth table of f is the binary vector

$$\boldsymbol{f} = (f(0, 0, \ldots, 0), f(1, 0, \ldots, 0), \ldots, f(1, 1, \ldots, 1))$$

of length 2^n, also denoted by f for simplicity. The Boolean function $f \in \mathbb{B}_n$ is said to be *balanced* if $\mathrm{wt}(f) = 2^{n-1}$.

The *support* of a Boolean function $f \in \mathbb{B}_n$ is defined as $\mathrm{supp}(f) = \{\boldsymbol{b} \in \mathbb{F}_2^n : f(\boldsymbol{b}) = 1\}$.

Any n-variable Boolean function f is commonly expressed in the so-called *Algebraic Normal Form* (ANF) as

$$f(\boldsymbol{x}) = \sum_{\boldsymbol{v} \in \mathbb{F}_{2^n}} a_{\boldsymbol{v}} \boldsymbol{x}^{\boldsymbol{v}} \tag{1}$$

where the sum is taken modulo 2, $a_{\boldsymbol{v}} \in \mathbb{F}_2$ and each monomial $\boldsymbol{x}^{\boldsymbol{v}}$ is determined by $\boldsymbol{x}^{\boldsymbol{v}} = \prod_{i=1}^{n} x_i^{\boldsymbol{v}_i}$. The *degree* of f equals the degree of the highest-degree monomial in its ANF. If $\deg(f)$ is 1, then f is said to be an *affine* (or *linear* if the constant term is zero); the monomials of degree $k \leq \deg(f)$ that appear in (1) are called the *kth degree part* of $f \in \mathbb{B}_n$.

By definition, if $\deg(f) \leq r$, then the vector $\boldsymbol{f}$ is a codeword of the rth order binary Reed-Muller code $\mathsf{R}(r, n)$ [31]; we also write $f \in \mathsf{R}(r, n)$ for simplicity.

The Walsh or Hadamard transform of the Boolean function $f \in \mathbb{B}_n$ at some $\boldsymbol{b} \in \mathbb{F}_2^n$, denoted by $\chi_f(\boldsymbol{b})$, is the real-valued function given by

$$\chi_f(\boldsymbol{b}) = \sum_{\boldsymbol{x} \in \mathbb{F}_2^n} (-1)^{f(\boldsymbol{x}) + \boldsymbol{b}\boldsymbol{x}^T} = 2^n - 2\,\mathrm{wt}(f + \boldsymbol{b}\boldsymbol{x}^T). \tag{2}$$

According to (2), the Boolean function f is balanced if and only if $\chi_f(\mathbf{0}) = 0$.

Each Boolean function $f \in \mathbb{B}_n$ is decomposed as follows

$$f(\boldsymbol{x}) = (1 + x_i) f|_{x_i=0} + x_i f|_{x_i=1}$$

for any $0 \leq i \leq n-1$, where $f|_{x_i=0}, f|_{x_i=1} \in \mathbb{B}_{n-1}$ are not dependent on x_i. Such a decomposition - which can be recursively applied to the subfunctions $f|_{x_i=0} \triangleq f_{i,0}, f|_{x_i=1} \triangleq f_{i,1}$ - is also called *Shannon's expansion formula*. This decomposition may be also written as $f = f_{i,0} \parallel f_{i,1}$. If $i = n-1$, then this is the usual *concatenation* of the truth tables of the sub-functions $f|_{x_i=0}, f|_{x_i=1} \in \mathbb{B}_{n-1}$.

2.1 Correlation attacks and correlation immunity

A known type of attacks that can be applied to stream ciphers is the so-called *correlation attacks*, firstly introduced in [46] for nonlinear combiners (but can be also applied, suitably modified, to nonlinear filter generators [47]). The correlation attack exploits the existence of a statistical dependence between the keystream and the output of a single constituent LFSR; such a dependence exists if and only if the output of the corresponding Boolean function f is correlated to at least one of its inputs (*see* Figure 4). Many variations of such type of attacks occur, whereas the *fast correlation attacks* are the most powerful [35].

To thwart such type of attacks, the Boolean functions employed as nonlinear filter/combiner generators should possess certain properties (apart from having high algebraic degree); the *correlation immunity* is a measure of the degree to which the outputs of a function are uncorrelated with some subset of its inputs. More precisely, we say that $f \in \mathbb{B}_n$ is *t-th correlation immune* if it is not correlated with any t-subset of $\{x_1, \ldots, x_n\}$; namely if

$$Pr(f(\boldsymbol{x}) = 0 | x_{i_1} = b_{i_1}, \ldots, x_{i_t} = b_{it}) = Pr(f(\boldsymbol{x}) = 0)$$

for any t positions $x_{i_1}, \ldots, x_{i_t}$ and any $b_{i_1}, \ldots, b_{i_t} \in \mathbb{F}_2$. If a t-th order correlation immune function is also balanced, then it is called *t-th order resilient* [46].

An equivalent characterization of correlation-immune functions is the following.

Definition 2.1. *If $f \in \mathbb{B}_2^n$ is a k-th order correlation-immune function, then* $\mathrm{supp}(f)$ *has the following property: for any $\boldsymbol{\alpha} = (a_1, \ldots, a_k) \in \mathbb{F}_2^k$ and for any $\{j_1, j_2, \ldots, j_k\} \subseteq \{1, 2, \ldots, n\}$, it holds*

$$|\{\boldsymbol{x} = (x_1, x_2, \ldots, x_n) \in \mathrm{supp}(f), x_{j_1} = a_1, \ldots, x_{j_k} = a_k\}| = \mathrm{wt}(f)/2^k$$

In other words, when $\boldsymbol{x} \in \mathbb{F}_2^n$ passes through all the vectors of $\mathrm{supp}(f)$*, then the vector formed from any $(i_1, i_2, \ldots, i_k)$ coordinates of $\boldsymbol{x}$ will equally likely to be any vector of $\mathbb{F}_2^k$.*

It is easy to verify that if f is k-th order correlation-immune, then it is also m-th order correlation-immune for any $m < k$.

There is a known trade-off between the correlation immunity and the degree of a function [46]: if $f \in \mathbb{B}_n$ is k-th order correlation-immune, then $\deg(f) \leq n - k$. More specifically, for a resilient function f of order k, it holds $\deg(f) \leq n - k - 1$ if $1 \leq k \leq n - 2$ [46].

The following well-known result has been proved in [50].

Proposition 2.1. *A function $f \in \mathbb{B}_n$ is t-th order correlation immune if and only if*

$$\chi_f(\boldsymbol{b}) = 0, \ \forall \ \boldsymbol{b} \text{ such that } 1 \leq \mathrm{wt}(\boldsymbol{b}) \leq t.$$

Clearly, f is t-th order resilient if, additionally, it holds $\chi_f(\mathbf{0}) = 0$.

2.2 Low order approximation attacks and nonlinearity

If a high-degree cryptographic Boolean function can be adequately approximated by a low-degree function, then the corresponding cryptographic system is not secure; for instance, the linear cryptanalysis on stream ciphers [19] exploits the existence of biased linear relations between some keystream bits

and some key bits. Alternatively, the attacker may replace the corresponding Boolean function f (e.g. the combiner function) by another function g of low degree such that $\mathrm{wt}(f+g)$ is small [22] and, thus, to mount a fast correlation attack to the modified system in order to reveal a secret key which produces a slightly modified keystream (namely a noisy version of the keystream, where the noise is small). Consequently, cryptographic functions should not be well approximated by low-degree functions.

The minimum distance between f and all affine functions is the *nonlinearity* of f, and is denoted by $\mathsf{nl}(f)$; it is determined by the Walsh transform [31] via

$$\mathsf{nl}(f) = \min_{l \in \mathsf{R}(1,n)} \mathrm{wt}(f+l) = 2^{n-1} - \frac{1}{2} \max_{\boldsymbol{b} \in \mathbb{F}_2^n} |\chi_f(\boldsymbol{b})|. \tag{3}$$

The notion of the nonlinearity is readily generalized to the *rth order nonlinearity* $\mathsf{nl}_r(f)$ of the function f, which is defined as

$$\mathsf{nl}_r(f) = \min_{g \in \mathsf{R}(r,n)} \mathrm{wt}(f+g)\,. \tag{4}$$

From (4) we have $\mathsf{nl}(f) \geq \mathsf{nl}_2(f) \geq \mathsf{nl}_3(f) \geq \cdots$ and this sequence is the so-called *nonlinearity profile* of f [4].

Computing the r-th order nonlinearity of Boolean functions, as well as their best r-th order approximations, is known to be a difficult task even for small values of r (if $r=1$, then the maximum possible nonlinearity is achieved by the so-called *bent* functions, which is $2^{n-1} - 2^{n/2-1}$ for n even; if n is odd, then the value of the maximum possible achievable nonlinearity remains unknown). Some particular cases though have been recently fully solved; the following result - which will be used in the sequel - has been proved in [21].

Theorem 2.2. *Let $f \in \mathbb{B}_n$, $\deg(f) = 3$, having the form $f = (q_1 + l_1) \,\|_j\, (q_2 + l_2)$, where $q_1, q_2, l_1, l_2 \in \mathbb{B}_{n-1}$ not dependent on x_j and, moreover, $\deg(q_1) = \deg(q_2) = 2$, $\deg(l_1), \deg(l_2) \leq 1$. Then, the best quadratic approximations of f have one of the following forms*

i. $\xi_f^0 = (q_1 + l_1) \,\|_j\, (q_1 + \lambda_{q_1+q_2+l_2})$;

ii. $\xi_f^1 = (q_2 + \lambda_{q_1+q_2+l_1}) \,\|_j\, (q_2 + l_2)$.

where $\lambda_{q_1+q_2+l_i}$, $i=1,2$, is a best affine approximation of $q_1+q_2+l_i$. Moreover, it holds $\mathsf{nl}_2(f) = 2^{n-2} - 2^{n-2-h}$ for some $1 \leq h \leq \lfloor \frac{n-1}{2} \rfloor$; more precisely, $2h$

is the rank of the symplectic matrix associated with the quadratic part $q_1 + q_2$ *[31].*

3 Algebraic attacks on stream ciphers

Let us consider a pseudo-random keystream generator in either the nonlinear filter or combiner model. Both cases can be described in a unified approach by a linear permutation $L : \mathbb{F}_2^N \to \mathbb{F}_2^N$, a linear mapping $L' : \mathbb{F}_2^N \to \mathbb{F}_2^n$ and a n-variable combining or filtering Boolean function $f \in \mathbb{B}_n$ in a following way: If $s_0, s_1 \ldots, s_{N-1}$ is the secret key of the keystream generator (that is the initialisation of the linear part of the generator) and $k_0, k_1, \ldots$ is the produced keystream, then it holds

$$f(L' \circ L^i(s_0, s_1, \ldots, s_{N-1})) = k_i, \ i \geq 0$$

where each $L^i : \mathbb{F}_2^N \to \mathbb{F}_2^N$ is a linear operator, determined by the composition of L with itself i times (for instance, in the filter model, L is the function that maps each of the LFSR to the next state). Algebraic attacks try to efficienly solve the latter equation, if the number of equations is much larger than the number of unknowns (an algebraic attack is is a known-plaintext attack, that is the attacker needs to know a part of the initial message, which in turn implies knowledge of part of the keystream).

Let us assume that there exists $g \in \mathbb{B}_n$ of low degree such that $f * g = h$, where h is also of low degree. Then, from the above we get

$$k_i g(L' \circ L^i(s_0, s_1, \ldots, s_{N-1})) = h(L' \circ L^i(s_0, s_1, \ldots, s_{N-1})) \qquad (5)$$

and, thus, a system of equations of low degree is constructed by considering each i such that $k_i = 1$; this system may be solved more efficiently than the initial system (e.g. by using Groebner basis or via linearization of the system and subsequent application of Gaussian elimination).

From the analysis of [12, 34] it turned out that the aforementioned condition may be re-stated as follows: for a cryptographic Boolean function f, there should not exist a low degree function g such that it holds either $f * g = 0$ or $(f + 1) * g = 0$. These requirements are equivalent to saying that f need to have high *algebraic immunity*, defined as follows.

Definition 3.1. *The algebraic immunity of $f \in \mathbb{B}_n$ is defined as*

$$\mathsf{AI}_n(f) = \min\{\deg(g) |\ g \in \mathcal{AN}(f) \cup \mathcal{AN}(f+1),\ g \neq 0\}$$

where $\mathcal{AN}(f) = \{g \in \mathbb{B}_2^n : f * g = 0\}$, and $*$ denotes the multiplication (point-wise product) of Boolean functions.

Each element in $\mathcal{AN}(f)$ is called *annihilator* of f. Moreover, it is proved in [12] that $\mathsf{AI}_n(f) \leq \lceil \frac{n}{2} \rceil$.

There are many open problems that should be addressed in the design of cryptosystems that are immune to algebraic attacks. An important open issue is the construction of Boolean functions achieving the maximum possible algebraic immunity. Several constructions of such functions are provided in the literature. The first one is the *majority* function, described in [15], which is a symmetric function; other constructions of symmetric functions having maximum algebraic immunity are also given in [3, 40, 11] (note that when the number of the variables is odd, then the only symmetric function with maximum algebraic immunity is the majority function [39]). However, the symmetry property poses a risk from a cryptographic point of view and, thus, constructions of non-symmetric functions of maximum algebraic immunity are of high importance. Several such constructions have been given in [5, 6, 23, 44, 9]; unfortunately, most of the functions do not present high nonlinearity, whereas others are non-balanced. Further constructions, providing functions with higher nonlinearities, are given in [7, 48, 41, 51] (as is pointed out though in [10], the first construction in [48] coincides with the construction in [7]). A generic construction of functions with odd number of variables and maximum algebraic immunity is also given in [25]; however, this construction, although it covers the entire space of functions with maximum algebraic immunity, is more theoretical than practical. Finally, proper modifications on some of the above families of functions so as to provide new functions with also maximum algebraic immunity have been recently proposed in [26, 27]. More precisely, an algorithmic approach to appropriately modify the majority function with odd number of variables is proved in [26], whereas it is shown in [27] that the same approach also holds for the case of even number of variables (the even case has been also studied in [9]). The proposed unified algorithm, covering both the odd and even case, is shown next (Algorithm 1), where a partial ordering of

Algorithm 1 Generate Functions of Maximum AI via the majority function

Require: Majority function $f \in \mathbb{B}_n$

$i \leftarrow 0,\ f_0 \leftarrow f$
$S \leftarrow \mathrm{supp}(f)$
$S' \leftarrow \mathrm{supp}(1+f)$
$T \leftarrow \{\boldsymbol{v} \in \mathrm{supp}(f) : \mathrm{wt}(\boldsymbol{v}) = \lceil \frac{n}{2} \rceil\}$
$T' \leftarrow \{\boldsymbol{v} \in \mathrm{supp}(f+1) : \mathrm{wt}(\boldsymbol{v}) = \lfloor \frac{n}{2} \rfloor\}$
while $(T \neq \emptyset) \vee (T' \neq \emptyset)$ **do**
    $i \leftarrow i+1$
    $(\boldsymbol{a}_i, \boldsymbol{b}_i) \in \{S \times S' : \boldsymbol{a}_i \succ \boldsymbol{b}_i \wedge (\boldsymbol{a}_i \in T \ \vee \boldsymbol{b}_i \in T')\}$ ▷ choose randomly
    f_i: $\mathrm{supp}(f_i) \leftarrow \mathrm{supp}(f_{i-1}) \setminus \{\boldsymbol{a}_i\} \cup \{\boldsymbol{b}_i\}$
    $S \leftarrow S \setminus \{\boldsymbol{a}_i\}$
    $S' \leftarrow S' \setminus \{\boldsymbol{b}_i\}$
    $T \leftarrow T \setminus \{\boldsymbol{v} \in T : \boldsymbol{v} \succ \boldsymbol{b}_i\}$
    $T' \leftarrow T' \setminus \{\boldsymbol{u} \in T' : \boldsymbol{u} \prec \boldsymbol{a}_i\}$
end while

Ensure: functions $\{f_i\}_{i \geq 1} : \mathsf{AI}_n(f_i) = \lceil \frac{n}{2} \rceil$

Figure 5: Algorithm for constructing functions with maximum AI

vectors in $\mathbb{F}_2^n$ defined as follows

$$\boldsymbol{u} \preceq \boldsymbol{v} \Leftrightarrow u_i \leq v_i \ \forall\ 0 \leq i \leq n-1\ ,$$

has been utilized.

It should be stressed though that constructing functions with maximum algebraic immunity (without sacrificing other cryptographic criteria) still remains an active research area.

Several relationships have been proved between algebraic immunity and other cryptographic measures. For instance, it was shown in [5] that

$$\sum_{i=0}^{\mathsf{AI}_n(f)-1} \binom{n}{i} \leq \mathrm{wt}(f) \leq \sum_{i=0}^{n-\mathsf{AI}_n(f)} \binom{n}{i}\ .$$

It is also well-known that low nonlinearity implies low algebraic immunity (although high nonlinearity does not always imply high algebraic immunity). More precisely, it is proved in [5] that

$$\mathsf{nl}_r(f) \geq \sum_{i=0}^{\mathsf{AI}_n(f)-r-1} \binom{n}{i}\ .$$

Especially for the first-order nonlinearity, a better bound has been proved in [30]:

$$\mathsf{nl}(f) \geq 2 \sum_{i=0}^{\mathsf{AI}_n(f)-2} \binom{n-1}{i}, \tag{6}$$

whereas other improvements on the aforementioned bounds have been proved in [4, 37], namely

$$\mathsf{nl}_r(f) \geq 2 \sum_{i=0}^{\mathsf{AI}_n(f)-r-1} \binom{n-r}{i} \quad \text{(for most cases)},$$

and

$$\mathsf{nl}_r(f) \geq \sum_{i=0}^{\mathsf{AI}_n(f)-r-1} \binom{n}{i} + \sum_{i=\mathsf{AI}_n(f)-2r}^{\mathsf{AI}_n(f)-r-1} \binom{n-r}{i},$$

respectively. Note that the latter one, provided in [37], improves the bound in [5] and, moreover, it also improves the bound given in [4]) (for small values of r, which is the most important case in cryptography). Furthermore, for $r = 1$, the bound in [37] coincides with (6).

In addition, by also considering the notion of

$$\mathsf{AI}_n^c(f) \triangleq \max\{\min_{\deg(g)}\{f * g = 0\}, \min_{\deg(g)}\{(f+1) * g = 0\}\},$$

where clearly $\mathsf{AI}_n(f) \leq \mathsf{AI}_n^c(f)$, the following result is proved in [42]:

Proposition 3.1. *Let $f \in \mathbb{B}_n$ with $\mathsf{AI}_n(f) = k_1 \leq \mathsf{AI}_n^c(f) = k_2$ and $g \in \mathbb{B}_n$ with $\deg(g) = r$. Then, it holds:*

1. *If $k_2 \leq 2r$, then $\mathrm{wt}(f+g) \geq \sum_{i=0}^{k_1-r-1} \binom{n}{i} + \sum_{i=0}^{k_2-r-1} \binom{n}{i}$,*
2. *If $k_1 \leq 2r$ and $k_2 \geq 2r+1$, then $\mathrm{wt}(f+g) \geq \sum_{i=0}^{k_1-r-1} \binom{n}{i} + \sum_{i=0}^{k_2-r-1} \binom{n-r}{i}$,*
3. *If $k_1 \geq 2r+1$, then $\mathrm{wt}(f+g) \geq \sum_{i=0}^{k_1-r-1} \binom{n}{i} + \sum_{i=k_1-2r}^{k_2-r-1} \binom{n-r}{i}$.*

Nevertheless, there are still many open questions concerning the relationship between algebraic immunity and other cryptographic criteria of Boolean functions, such as correlation immunity.

3.1 Fast algebraic attacks on stream ciphers

The bacic idea behind fast algebraic attacks is the identification, for a given cryptographic function $f \in \mathbb{F}_2^n$, of a low-degree function g such that the function $h = f * g$ is of reasonable degree; if this is the case, then the number of the unknowns in the corresponding equations may be further reduced. Note that $g+h \in \mathcal{AN}(f)$ and, thus, the degree of $g+h$ may be greater than $\mathsf{AI}_n(f)$, thus leading to the result that maximum algebraic immunity does not imply resistance to fast algebraic attacks.

Assuming that such g, h do exist, we get (similarly to (5)):

$$k_i g(L' \circ L^i(s_0, s_1, \ldots, s_{N-1})) = h(L' \circ L^i(s_0, s_1, \ldots, s_{N-1})), \quad i = 0, 1, \ldots \quad (7)$$

Then there exists a linear combination of the first $\sum_{i=0}^{\deg(h)} \binom{N}{i}$ equations that sum the right-hand part of (7) to zero; this linear combination can be found via the well-known Berlekamp-Massey algorithm [32]. By this procedure, we get one equation of degree at most $\deg(g)$ (and, thus, the main computational effort in such attacks rests with $\deg(g)$).

It is evident from the above analysis that the core process of fast algebraic attacks is the identification of functions g, h with $\deg(g) = e$, $\deg(h) = d$ such that, for a given cryptographic function $f \in \mathbb{B}_n$, it holds $f * g = h$ and $e + d < n$. It is well-known that there always exists a pair g, h with degrees e, d respectively such that $e + d \geq n$ [13].

Pasalic in [38] introduced the following definition, to provide a unique approach for characterizing the resistance to both conventional and fast algebraic attacks:

Definition 3.2. *A Boolean function $f \in \mathbb{B}_n$ is called Algebraic Attack Resistant ($\mathcal{AAR}$) if it has maximum algebraic immunity $\lceil \frac{n}{2} \rceil$ and, moreover, for any $g \notin \mathcal{AN}(f)$ with $\deg(g) = e$, $1 \leq e \leq \lceil \frac{n}{2} \rceil - 1$, we necessarily have that $d \triangleq \deg(f * g)$ satisfies $e + d \geq n$. The latter property is referred to as High Degree Product ($\mathcal{HDP}$) of order n.*

It is proved in [38] that if $f \in \mathbb{B}_n$ satisfies $\mathcal{HDP}$ of order n, so does $f + 1$ and, furthermore, f has maximum algebraic immunity $\lceil \frac{n}{2} \rceil$.

More recently, the notion of *fast algebraic immunity* has been introduced in [29].

Definition 3.3. *The fast algebraic immunity of $f \in \mathbb{B}_n$, denoted by $\mathsf{FAI}_n(f)$, is defined as*

$$\mathsf{FAI}_n(f) = \min_{g \in \mathbb{B}_n} \{2\,\mathsf{AI}_n(f), \deg(g) + \deg(f * g)\}\ ,$$

where $1 \leq \deg(g) \leq \mathsf{AI}_n(f)$.

From the above analysis we get that $\mathsf{FAI}_n(f) \leq n$ and, thus, functions of the maximum possible fast algebraic immunity n are required to withstand fast algebraic attacks. Moreover, it is obvious that $\mathsf{FAI}_n(f) = n$ if and only if f is $\mathcal{AAR}$.

A relationship between fast algebraic immunity and r-th order nonlinearity has been recently proved in [49]:

Theorem 3.4. *Let $f \in \mathbb{B}_n$ and d a positive integer. If $\mathsf{nl}_r(f) < \sum_{i=0}^{d} \binom{n}{i}$ for some $r < \deg(f)$, then $\mathsf{FAI}_n(f) \leq r + 2d$.*

Amongst the known families of functions achieving optimal algebraic immunity, those proposed in [7, 41] seem to behave well against fast algebraic attacks. The construction given in [7] is described as follows:

Proposition 3.2. *Let n be any integer such that $n > 1$ and α a primitive element of the finite field $\mathbb{F}_{2^n}$. Let also $f \in \mathbb{B}_n$ such that*

$$\mathrm{supp}(f) = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{2^{n-1}-2}\}.$$

Then f has maximum algebraic immunity $\lceil \frac{n}{2} \rceil$.

This class of functions, apart from balancedness and high (first-order) nonlinearity, seems to have good behavior against fast algebraic attacks (according to experiments for small values of n). Modified versions of these functions are provided in [41, 51], where it is also shown that these functions seem to be resistant against fast algebraic attacks (although a mathematic proof is still missing). More precisely, the construction in [41] is as follows.

Proposition 3.3. *Let $n > 1$ be an integer and α be a primitive element of the finite field $\mathbb{F}_{2^n}$. If $f \in \mathbb{B}_n$ with $\mathrm{supp}(f) = \{1, \alpha, \alpha^2, \ldots, \alpha^{D_n - 1}\} \cup S$, where*

- $S \subset \{\alpha^{D_n}, \ldots, \alpha^{D_n+\hat{D}_n+1}\}$ *and* $|S| = 2^{n-1} - D_n$,
- $D_n = \sum_{i=0}^{\lceil \frac{n}{2} \rceil - 1} \binom{n}{i}$,
- $\hat{D}_n = \binom{n}{\lceil \frac{n}{2} \rceil}$,

then $\mathsf{AI}_n(f) = \lceil \frac{n}{2} \rceil$.

Furthermore, in [51] it is shown that specific modified versions of the above functions still have maximum algebraic immunity (and other cryptographic properties). Finally, efficient strategies to appropriately modify all the above classes of functions such as to ensure maximum algebraic immunity have been recently proposed in [27]; however, there is still room for study concerning fast algebraic immunity.

4 A trade-off between resistance to correlation and fast algebraic attacks

We next prove a trade-off between correlation immunity and the $\mathcal{HDP}$ property, which rests with the limitations occurring in the degree of a correlation-immune function.

Proposition 4.1. *If $f \in \mathbb{B}_n$ is m-th order correlation-immune Boolean function for $m > 2$, then it does not satisfy the $\mathcal{HDP}$ property and, thus, it is not $\mathcal{AAR}$.*

Proof. Due to our hypothesis, it holds $\deg(f) \leq n-m \leq n-3$. Let us consider any function $g \in \mathbb{B}_n$ with $\deg(g) = 1$. Then, for the function $h = g * f$ it holds $\deg(h) \leq 1+n-3 = n-2$. Consequently, we have $\deg(h)+\deg(g) \leq n-2+1 = n-1$ and the claim follows. □

Using the same arguments, we can also prove the following result.

Proposition 4.2. *If $f \in \mathbb{B}_n$ is m-th order resilient Boolean function for $2 \leq m \leq n-2$, then it does not satisfy the $\mathcal{HDP}$ property and, thus, it is not $\mathcal{AAR}$.*

From the above we get that, in general, correlation-immune functions are not optimal in terms of withstanding fast algebraic attacks (a possible exception being the case of low-order correlation immunity); this is attributed to the known trade-off between algebraic degree and correlation immunity. However, it is the first time that such a trade-off between resistance to correlation and fast algebraic attacks is being stated.

Next we focus on m-th order resilient functions since they are balanced and, thus, are of most cryptographic importance. Working similarly as above, we directly obtain the following.

Theorem 4.1. *If $f \in \mathbb{B}_n$ is m-th order resilient Boolean function, then $\mathsf{FAI}_n(f) \leq n - m + 1$.*

Proof. Recalling that $\deg(f) \leq n - m - 1$, the proof is straightforward by working similarly as in Proposition 4.2. □

From Theorem 4.1 we directly obtain the following result, which is an equivalent re-statement of Proposition 4.2 in terms of fast algebraic immunity.

Corollary 4.2. *Let $f \in \mathbb{B}_n$ be a m-th order resilient function, for $2 \leq m \leq n-2$. Then it holds $\mathsf{FAI}_n(f) < n$.*

4.1 The Siegenthaler's construction

A recursive procedure to construct an m-th order resilient Boolean function has been provided in Siegenthaler's seminal paper [46], based on the property that if $g, g' \in \mathbb{B}_n$ are both m-th order resilient, then $f = g' \parallel g \in \mathbb{B}_{n+1}$ is also m-th order resilient. Each step of the procedure starts with an m-th order resilient Boolean function g (obtained from the previous step), computes $g' = g \circ \pi$ by permuting the variables within g according to $\pi \in \mathcal{P}_n$ (chosen such that the highest degree terms of g, g' do not fully coincide), and then outputs $g' \parallel g$. At the first step, we start with a linear function $g \in \mathbb{B}_{m+2}$, e.g. $g(x_1, \ldots, x_{m+2}) = x_1 + \cdots + x_{m+1}$ and the transposition $\pi = (m+1, m+2)$, whilst at the final step we get an mth order resilient function $f \in \mathbb{B}_n$ of degree

$n-m-1$. Note that function f is the concatenation of 2^{n-m-2} sub-functions on $m+2$ variables.

As it is stated in [5], it is difficult to say whether the Siegenthaler's construction is good or bad in terms of algebraic immunity. In the sequel, we analyse the Siegenthaler's construction in terms of fast algebraic immunity. Clearly, Theorem 4.1 implies that for $m \geq 2$ any function obtained via this construction does not have maximum FAI; however, this result also holds for $m = 1$, as shown next.

Proposition 4.3. *For any* 1*-st order resilient function* $f \in \mathbb{B}_n$ *obtained via the Siegenthaler's construction, it holds* $\mathsf{FAI}_n(f) < n$.

Proof. Each such function f of degree $n-2$ has the form

$$f = f_1 \|_n f_2$$

where $f_1, f_2 \in \mathbb{B}_{n-1}$ have degree $n-3$ and do not depend on x_n. Consequently, this implies that the linear function $g(x_1, \ldots, x_n) = x_n$ satisfies $\deg(f * g) \leq n-2$ (since all the $(n-2)$-th degree terms of f contain x_n) and, hence, the claim follows. □

Consequently, any function obtained via the Siegenthaler's construction is bound to have fast algebraic immunity less that n - and, thus, it is not $\mathcal{AAR}$. Clearly, such a result can be similarly proved for any other function f that is constructed via concatenation of other functions (since the terms in the ANF of f with maximum degree share a common variable). Consequently, although the behavior of these functions in terms of algebraic immunity still remains an open problem, it becomes evident that they do not provide resistance against fast algebraic attacks.

4.1.1 Second–order nonlinearity

Apart from the fast algebraic immunity, it should be stressed that the functions obtained via the Siegenthaler's construction may not behave well in terms of withstanding low order approximation attacks. More precisely, the permutation of variables that takes place in the construction process has - in general - impact on the second-order nonlinearity of the derived function. For

instance, let us consider the case of a cubic function $f \in \mathbb{B}_5$ obtained via the Siegenthaler's construction; clearly, one such function is the following:

$$f = g' \parallel_5 g$$

where

$$g(x_1, \ldots, x_4) = (x_1 + x_3) \parallel_4 (x_1 + x_2) = x_2x_4 + x_3x_4 + x_1 + x_2$$

and g' is obtained by g via a permutation of the variables (such that $\deg(g + g') = 2$). It is easy to verify that any such function f satisfies the conditions implied by Theorem 2.2. Let us now assume that g' is obtained from g via the following permutation of variables:

$$\pi : (1, 2, 3, 4) \rightarrow (2, 1, 3, 4)$$

that is $g' = x_1x_4 + x_3x_4 + x_1 + x_2$. In this case, it holds (due to Theorem 2.2):

$$\mathsf{nl}_2(f) = 2^{n-2} - 2^{n-2-h}$$

where $2h$ is the rank of the symplectic matrix that is associated with the quadratic form

$$(x_2x_4 + x_3x_4) + (x_1x_4 + x_3x_4) = x_4(x_1 + x_2)$$

and, thus, $h = 1$ [31]. Consequently, the 1-th order resilient function f satisfies $\mathsf{nl}_2(f) = 4$ - that is the minimum possible (note also that, since $4 < \sum_{i=0}^{1} \binom{5}{i}$, we again get that $\mathsf{FAI}_n(f) < 5$ due to Theorem 3.4).

On the other hand, if g' is obtained from g via $\pi' = (1, 2, 3, 4) \rightarrow (2, 3, 4, 1)$, then $g' = x_1x_3 + x_1x_4 + x_2 + x_3$, and the 1-resilient function $f' = g' \parallel g$ satisfies $\mathsf{nl}_2(f') = 2^{n-2} - 2^{n-h'-2}$, where $2h'$ is the rank of the symplectic matrix that is associated with the quadratic form $x_2x_4 + x_3x_4 + x_1x_3 + x_1x_4$. Note that this quadratic form can be written as

$$y_1y_2 + y_3y_4 + y_1$$

where $y_1 = x_1$, $y_2 = x_2$, $y_3 = x_1 + x_2 + x_3$, $y_4 = x_1 + x_4$. Hence, since all y_i, $i = 1, 2, 3, 4$, are linearly independent, we get that $h' = 2$ [31], thus resulting in $\mathsf{nl}_2(f') = 6$. Concluding, the permutations at each step affect the second-order nonlinearity.

5 Conclusions

The resistance of stream ciphers against algebraic attacks was studied in this paper. More precisely, a survey of the recent findings in this area is provided, whereas new results are proved regarding tradeoffs that exist between resistance to correlation and fast algebraic attacks. The main outcome of our analysis is that functions of very low order correlation immunity should be chosen in order to thwart fast algebraic attacks, whereas it is also shown that even the first order correlation immunity (i.e. the minimum possible to provide resistance against correlation attacks) does not necessarily ensure resistance against fast algebraic attacks.

Many directions for further research are still open; for instance, an interesting challenge is to evaluate known powerful constructions of Boolean functions in terms of their fast algebraic immunity. Moreover, other algebraic-type attacks that have been recently proposed, such as the *fast selective discrete Fourier transform (DFT)* [20] attacks, need to be further explored and investigated.

References

[1] F. Armknecht: Improving fast algebraic attacks, *Fast Software Encryption, Lecture Notes in Computer Science, Springer-Heidelberg*, **3017**, (2004), 65–82.

[2] F. Armknecht, and G. Ars, Introducing a new variant of fast algebraic attacks and minimizing their successive data complexity, *Mycrypt 2005, Lecture Notes in Computer Science, Springer-Heidelberg*, **3715**, (2005), 16–32.

[3] A. Braeken and B. Preneel, On the algebraic immunity of symmetric Boolean functions, *Advances in Cryptology - Indocrypt 2005, Lecture Notes in Computer Science, Springer-Heidelberg*, **3797**, (2005), 35–48.

[4] C. Carlet, On the higher order nonlinearities of algebraic immune functions, *Advances in Cryptology - CRYPTO 2006, Lecture Notes in Computer Science, Springer-Heidelberg*, **4117**, (2006), 584–601.

[5] C. Carlet, D. K. Dalai, K. G. Gupta and S. Maitra, Algebraic immunity for cryptographically significant Boolean functions: analysis and construction, *IEEE Trans. Inf. Theory*, **52**(7), (2006), 3105–3121.

[6] C. Carlet, Constructing balanced functions with optimum algebraic immunity, *IEEE International Symposium on Information Theory (ISIT)*, (2007), 451–455.

[7] 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, Lecture Notes in Computer Science, Springer-Heidelberg*, **5350**, (2008), 425–440.

[8] C. Carlet and P. Gaborit, On the construction of balanced Boolean functions with a good algebraic immunity, *IEEE Int. Symp. Inf. Theory (ISIT)*, (2005), 1101–1105.

[9] C. Carlet, X. Zeng, C. Li and L. Hu, Further properties of several classes of Boolean functions with optimum algebraic immunity, *Des. Codes Cryptogr.*, **52**(3), (2009), 303–338.

[10] C. Carlet, Comments on "Constructions of cryptographically significant Boolean functions using primitive polynomials", *IEEE Trans. Inf. Theory*, **57**(7), (2011), 4852–4853.

[11] Y. Chen and P. Lu, Two classes of symmetric Boolean functions with optimum algebraic immunity: construction and analysis, *IEEE Trans. Inf. Theory*, **57**(4), (2011), 2522–2538.

[12] N. Courtois and W. Meier, Algebraic attacks on stream ciphers with linear feedback, *Advances in Cryptology - Eurocrypt 2003, Lecture Notes in Computer Science, Springer-Heidelberg*, **2656**, (2003), 345–359.

[13] N. Courtois, Fast algebraic attacks on stream ciphers with linear feedback, *Advances in Cryptology - Crypto 2003, Lecture Notes in Computer Science, Springer-Heidelberg*, **2729**, (2003), 176–194.

[14] D.K. Dalai, K.C. Gupta and S. Maitra, Results on algebraic immunity for cryptographically significant boolean functions, *Progress in Cryptology -*

Indocrypt 2004, Lecture Notes in Computer Science, Springer-Heidelberg, **1880**, (2004), 92–106.

[15] D.K. Dalai, S. Maitra and P. Sarkar, Basic theory in construction of Boolean functions with maximum possible annihilator immunity, *Des. Codes Cryptography*, **40**(1), (2006), 41–58.

[16] C. Ding, G. Xiao and W. Shan, The Stability Theory of Stream Ciphers, *Lecture Notes in Computer Science, Springer-Heidelberg*, **561**, (1991).

[17] P. Hawkes and G.G. Rose, Rewriting variables: the complexity of fast algebraic attacks on stream ciphers, *Advances in Cryptology - Crypto 2004, Lecture Notes in Computer Science, Springer-Heidelberg*, **3152**, (2004), 390–406.

[18] ECRYPT. D.STVL.9, Ongoing research areas in symmetric cryptography, *ECRYPT Deliverable*, (2008).

[19] J. Golić, Dj., Linear cryptanalysis of stream ciphers. *Fast software encryption FSE 1994, Lecture notes in Computer Science, Springer-Heidelberg*, **1008**, (1994), 154–169.

[20] G. Gong, R. Rønjom, T. Helleseth and H. Hu, Fast Discrete Fourier Spectra attacks on stream ciphers, *IEEE Trans. Inf. Theory*, **57**(8), (2011), 5555–5565.

[21] N. Kolokotronis, K. Limniotis and N. Kalouptsidis, Best affine and quadratic approximations of particular classes of Boolean functions, *IEEE Trans. Inf. Theory*, **55**(11), (2009), 5211–5222.

[22] K. Kurosawa, T. Iwata and T. Yoshiwara, New covering radius of Reed-Muller codes for t-resilient functions, *IEEE Trans. Inf. Theory*, **50**(3), (2004), 468–475.

[23] N. Li and W. Qi, Construction and analysis of Boolean functions of $2t+1$ variables with maximum algebraic immunity, *Advances in Cryptology - Asiacrypt 2006, Lecture Notes in Computer Science, Springer-Heidelberg*, **4284**, (2006), 84–98.

[24] N. Li and W. Qi, Symmetric Boolean functions depending on an odd number of variables with maximum algebraic immunity, *IEEE Trans. Inf. Theory*, **52**(5), (2006), 2271–2273.

[25] N. Li, L. Qu, W. Qi, G. Feng, C. Li and D. Xie, On the construction of Boolean functions with optimal algebraic immunity, *IEEE Trans. Inf. Theory*, **54**(3), (2008), 1330–1334.

[26] K. Limniotis, N. Kolokotronis and N. Kalouptsidis, Constructing Boolean functions in odd number of variables with maximum algebraic immunity, *IEEE Int. Symp. Inf. Theory*, (2011), 2686–2690.

[27] K. Limniotis, N. Kolokotronis and N. Kalouptsidis, Modifying Boolean functions to ensure maximum algebraic immunity, *Cryptology ePrint Archive*, Report 2012/046 (2012), `http://eprint.iacr.org`.

[28] F. Liu and K. Feng, Efficient computation of algebraic immunity of symmetric Boolean functions, *Theory and Applications of Models of Computation (TAMC), Lecture Notes in Computer Science, Springer-Heidelberg*, **4485**, (2007), 318–329.

[29] M. Liu and D. Lin, Fast algebraic attacks and decomposition of symmetric Boolean functions, *arXiv: 0910.4632v1 [cs.CR]*.

[30] M. Lobanov, Tight bound between nonlinearity and algebraic immunity, *Cryptology ePrint Archive*, Report 2005/441 (2005), `http://eprint.iacr.org`.

[31] F. MacWilliams and N. Sloane, *The Theory of Error Correcting Codes*, North-Holland, Amsterdam, 1977.

[32] J.L. Massey, Shift-register synthesis and BCH decoding, *IEEE Trans. Inform. Theory*, **15**(1), (1969), 122–127.

[33] M. Matsui, Linear cryptanalysis method for DES cipher, *Advances in Cryptology - EUROCRYPT '93, Lecture Notes in Computer Science, Springer-Heidelberg*, **765**, (1994), 386–397.

[34] W. Meier, E. Pasalic and C. Carlet, Algebraic attacks and decomposition of Boolean functions, *Advances in Cryptology - Eurocrypt 2004, Lecture Notes in Computer Science, Springer-Heidelberg*, **3027**, (2004), 474–491.

[35] W. Meier and O. Staffelbach, Fast correlation attacks on stream ciphers, *Advances in Cryptology - Eurocrypt '88, Lecture Notes in Computer Science, Springer-Heidelberg*, **330**, (1988), 301–314.

[36] A.J. Menezes, P.C. Van Oorschot and S.A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.

[37] S. Mesnager, Improving the lower bound on the higher order nonlinearity of Boolean functions with prescribed algebraic immunity, *IEEE Trans. Inf. Theory*, **54**(8), (2008), 3656–3662.

[38] E. Pasalic, Almost fully optimized infinitive classes of Boolean functions resistant to (fast) algebraic cryptanalysis, *ICISC 2008, Lecture Notes in Computer Science, Springer-Heidelberg*, **5461**, (2008), 399–414.

[39] L. Qu, C. Li and K. Feng, A note on symmetric Boolean functions with maximum algebraic immunity in odd number of variables, *IEEE Trans. Inf. Theory*, **53**(8), (2007), 2908–2910.

[40] L. Qu, K. Feng, F. Liu and L. Wang, Constructing symmetric Boolean functions with maximum algebraic immunity, *IEEE Trans. Inf. Theory*, **55**(5), (2009), 2406–2412.

[41] P. Rizomiliotis, On the resistance of Boolean functions against algebraic attacks using univariate polynomial representation, *IEEE Trans. Inf. Theory*, **56**(8), (2010), 4014–4024.

[42] P. Rizomiliotis, Improving the higher order nonlinearity lower bound for Boolean functions with given algebraic immunity, *Discr. Appl. Math.*, **158**(18), (2010), 2049–2055.

[43] S. Rønjom and T. Helleseth, A new attack on the filter generator, *IEEE Trans. Inform. Theory*, **53**(5), (2007), 1752–1758.

[44] S. Sarkar and S. Maitra, Construction of rotation symmetric Boolean functions on odd number of variables with maximum algebraic immunity,

AAECC 2007, Lecture Notes in Computer Science, Springer-Heidelberg, **4851**, (2007), 271–280.

[45] C.E. Shannon, Communication theory of secrecy systems, *Bell System Technical Journal*, **28**, (1949), 656–715 .

[46] T. Siegenthaler, Correlation-immunity of nonlinear combining functions for cryptographic applications, *IEEE Trans. Inf. Theory*, **30** (5), (1984), 776–780.

[47] T. Siegenthaler, Cryptanalysts representation of nonlinearly filtered m-sequences, *Advances in Cryptology–Eurocrypt '85, Lecture Notes in Computer Science, Springer-Heidelberg*, **219**, (1986), 103–110.

[48] Q. Wang, J. Peng and H. Kan, Constructions of cryptographically significant Boolean functions using primitive polynomials, *IEEE Trans. Inf. Theory*, **56**(6), (2010), 3048–3053.

[49] Q. Wang and T. Johansson, A note on fast algebraic attacks and higher order nonlinearities, *Inscrypt 2010 (Lecture Notes in Computer Science, Springer-Heidelberg)* **6584**, (2011), 404–414.

[50] G. Z. Xiao and G. L. Massey, A spectral characterization of correlation-immune combining functions, *IEEE Trans. Inf. Theory*, **34**(3), (1988), 569–571.

[51] X. Zeng, C. Carlet, J. Shan and L. Hu, More balanced Boolean functions with optimal algebraic immunity and good nonlinearity and resistance to fast algebraic attacks, *IEEE Trans. Inf. Theory*, **57**(9), (2011), 6310–6320.