UDC 519.7

Algebraic immunity of vectorial boolean functions and boolean groebner bases

A. N. Alekseychuk[1]

[1] *National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute», Institute of Special Communication and Information Security*

Abstract

The basic concepts and results related to the Boolean Groebner bases and their application for computing the algebraic immunity of vectorial Boolean functions are considered. This parameter plays an important role for the security evaluation of block ciphers against algebraic attacks. Unlike the available works, the description is carried out at the elementary level using terms of Boolean functions theory. In addition, obtained proofs are shorter than the previous ones. This allows us to achieve significant progress in building the fundamentals of the theory (for the Boolean case) using only elementary methods.

The paper can be useful for students and postgraduate students studying cryptology. It may also save time for professionals who want to get familiar with the mathematical techniques used in algebraic attacks on block ciphers.

Keywords: algebraic cryptoanalysis, vectorial Boolean function, Groebner basis, algebraic immunity.

Introduction

The security evaluation of block ciphers as well as some stream ciphers against algebraic attacks [1, 2, 3] generates a problem of finding or estimating the maximal number of linearly independent equations of lowest degree among all Boolean equations that describes a given vectorial Boolean function (an s-block). Although the solution of the problem is received in [4] but mentioned work is little known and assumes reader erudition in the field of polynomial ideals and Groebner bases, which, in turn, requires knowledge of commutative algebra basics.

The purpose of this paper is to outline the basic concepts and results related to the formulated above problem including the concepts of the (Boolean) Groebner basis and algebraic immunity of vectorial Boolean function. At present there are several definitions of algebraic immunity of vectorial Boolean functions [1, 4, 5, 6, 7], among which the definition given by Ars-Faugère [4] is the most appropriate from a practical point of view.

Section 1 summarizes the basic statements on ideals in the ring of Boolean functions. In particular, it is shown that each ideal is uniquely determined by the set of its zeros and is generated by a unique function that can be effectively constructed by the set of zeros of the ideal. A relation between the dimension of an ideal (as a subspace of the vector space of Boolean functions) and the number of its zeros is proved. The well-known Hilbert Nullstellensatz for the ring of Boolean functions (see [8], for example) directly follows from the mentioned relation.

Section 2 gives the definition of the algebraic immunity of a vectorial Boolean function and describes a method of estimating this parameter based on certain results of [9]. The proposed method allows fast solving of the decision problem (whether or not the algebraic immunity is above the specified threshold) directly by the truth table of the vectorial function using the Gaussian elimination algorithm.

Finally, Sections 3 and 4 are devoted to the basics of the Boolean Groebner bases theory and their application for computing the algebraic immunity. The main purpose is to prove the Ars-Faugère theorem [4], which makes possible to find algebraic immunity along with all equations of lowest degree. These equations result from the system of equations that describes a given vectorial Boolean function.

The results presented in the paper are essentially known. However, unlike the available works, the description is carried out with the help of elementary techniques and obtained proofs are shorter. Furthermore, in contrast to the traditional approach to Groebner bases of polynomial ideals (see [8], for example), the description in the paper is based on the terms of Boolean functions theory. This allows us to achieve significant progress in building the foundations of the theory (for the Boolean case) using only elementary methods.

To the author mind, the presented paper can be useful for students and postgraduate students studying cryptology. It may also save time for professionals who want to get familiar with the mathematical techniques used in algebraic attacks on block cipher.

1. Ideals in the ring of Boolean functions

For every positive integer n denote by V_n the set of binary vectors of the length n, and by B_n the set of Boolean functions in n variables. The set B_n is a commutative ring with respect to the standard addition

and multiplication of Boolean functions:

$$\forall f,g \in B_n\colon \quad (f\oplus g)(x) = f(x)\oplus g(x),$$
$$(fg)(x) = f(x)g(x), \qquad x \in V_n.$$

Recall that a set $I \subseteq B_n$ is called an ideal in the ring B_n if

$$\forall f \in B_n \forall g_1, g_2 \in I:\ g_1 \oplus g_2 \in I,\ fg_1 \in I.$$

The notation $I \lhd B_n$ means that I is an ideal in B_n. The ideal generated by a set $\{g_1, ..., g_m\} \subseteq B_n$ is defined as follows:

$$\langle g_1, ..., g_m\rangle = \{f_1g_1 \oplus ... \oplus f_mg_m :\ f_1, ..., f_m \in B_n\}.$$

For any $I \lhd B_n$, $M \subseteq B_n$ let

$$V(I) = \{x \in V_n |\ \forall g \in I\colon g(x) = 0\}, \quad (1)$$
$$J(M) = \{g \in B_n |\ \forall x \in M\colon g(x) = 0\}. \quad (2)$$

The set 1 is called the algebraic variety [8] or the set of zeroes of the ideal I. The set 2 is the ideal of all Boolean functions which turn into zero on M. The basic properties of ideals in the ring B_n are the following.

Statement 1 *For any $I \lhd B_n$, $M \subseteq B_n$ the following equalities hold:*

$$J(V(I)) = I,\ V(J(M)) = M.$$

In particular, there is a one-to-one correspondence between the ideals in the ring B_n and the subsets of the set V_n (such that each ideal is uniquely determined by the set of its zeros). Besides, each ideal $I \lhd B_n$ is generated by only one Boolean function χ_I defined as follows:

$$\forall x \in V_n\colon \chi_I(x) = \begin{cases} 0, & x \in V(I); \\ 1, & x \notin V(I). \end{cases} \quad (3)$$

Proof. First of all, let us prove the equality $I = \langle\chi_I\rangle$. If $I = \{0\}$, then this equality is obvious. Let $I \neq \{0\}$ and $x \notin V(I)$. Then there exists a function $f \in I$ such that $f(x) = 1$. We have

$$f = \bigoplus_{y \in V_n : f(y) = 1} \delta_y,$$

where the functions δ_y, $y \in V_n$, are defined by the rule $\delta_y(z) = 1 \Leftrightarrow z = y, z \in V_n$. Since $I \lhd B_n$ and $f \in I$ we obtain

$$\delta_x f = \bigoplus_{y \in V_n : f(y) = 1} \delta_x\delta_y = \delta_x \in I.$$

So, for any $x \notin V(I)$ we have

$$\delta_x \in I \Rightarrow \chi_I = \bigoplus_{y \notin V(I)} \delta_x \in I \Rightarrow \langle\chi_I\rangle \subseteq I.$$

Besides, for any $f \in I$ we have $f = f\chi_I$. Thus, $I \subseteq \langle\chi_I\rangle$ and, therefore, $I = \langle\chi_I\rangle$, which completes the proof.

Next, it follows from (1), (2) that for any $I \lhd B_n$ the relation $I \subseteq J(V(I))$ holds. Besides, if $f \in J(V(I))$, then $f(x) = 0$ for any $x \in V(I)$ and, hence, $f = f\chi_I$. But it follows from above that $\chi_I \in I$. Thus, $f \in I$ and, hence, $J(V(I)) \subseteq I$.

So, we get $J(V(I)) = I$. Finally, the equality $V(J(M)) = M$ follows from (1), (2), and the proven equality $J(V(I)) = I$ with $I = J(M)$. Statement is proved.

As an example, let us consider a system

$$g_i(x_1, ..., x_n) = 0,\ i = 1, 2, ...m \quad (4)$$

of m Boolean equations in n variables $x_1, ...x_n$. Let $I = \langle g_1, ...g_m\rangle$ be the ideal generated by the set $\{g_1, ..., g_m\}$. Then I consists of all functions $g \in B_n$ such that the equation $g(x_1, ..., x_n) = 0$ is a consequence of the system (4) and the set of all solutions of this system is $V(I)$. Next, the specified system is equivalent to one equation $\chi_I(x_1, ..., x_n) = 0$, where the function χ_I is defined by (3). Therefore, $I = \{f\chi_I | f \in B_n\}$.

Let I be an arbitrary ideal in the ring B_n; then the set

$$Ann(I) = \{f \in B_n | \forall g \in I\colon fg = 0\}$$

is also an ideal called the annihilator of the ideal I. The annihilator of a function $f \in B_n$ is defined as the annihilator of the ideal generated by this function: $Ann(f) = Ann(\langle f\rangle)$.

Statement 2 *For any $I \lhd B_n$ the ring B_n is a direct sum of the ideals I and $Ann(I)$. In other words, for each function f there exists a unique representation $f = g \oplus g^{\perp}$, where $g \in I$ and $g^{\perp} \in Ann(I)$. Besides, if $I = \langle g_0\rangle$, then $Ann(I) = \langle g_0 \oplus 1\rangle$.*

Proof. It is enough to observe that $V(Ann(I)) = V_n \setminus V(I)$ and use Statement 1.

To conclude this section let's describe the connection between ideals in the ring B_n and some block codes. Notice that every ideal $I \lhd B_n$ is a subspace of the vector space of all Boolean functions in n variables and, therefore, a linear code of length 2^n over the field of two elements. The code-words of this code are the value vectors of the functions belonging to

$$I = \{(g(x)\colon x \in V_n) : g \in I\} \quad (5)$$

Let's write the words of the code (5) in a $2^k \times 2^n$ table, where $k = \dim I$ denotes the dimension of the ideal I. It is clear that the set $V(I)$ coincides with the set of all zero columns in this table and the set $V_n \setminus V(I)$ is equal to the support of the code I. Next, all 2^k vectors $(g(x)\colon x \in V_n \setminus V(I))$, where $g \in I$, are pairwise different. Since their length is $|V_n \setminus V(I)|$ we have $k \leq |V_n \setminus V(I)|$. On the other hand, according to Statement 1 any function $g \in B_n$ such that $g(x) = 0$ for all $x \in V(I)$ belongs to the code I. Thus, $2^{|V_n \setminus V(I)|} \leq |I|$, that is $|V_n \setminus V(I)| \leq k$. So, we obtain the following statement establishing the relationship between the dimension of an ideal and the number of its zeros.

Statement 3 *For any $I \lhd B_n$ the following equality holds:*

$$|V(I)| = 2^n - \dim I.$$

As a consequence, we obtain the following variant of Hilbert's Nullstellensatz (see [8], for example).

Consequence 1 *The system of equations (4):*
a) is incompatible if and only if $\langle g_1, ..., g_m\rangle = B_n$;
b) has a unique solution $(a_1, ..., a_n) \in V_n$ if and only if

$$\langle g_1, ..., g_m\rangle = \langle x_1 \oplus a_1, ..., x_n \oplus a_n\rangle.$$

2. Algebraic immunity of vectorial Boolean function

Recall that each function $f \in B_n \setminus \{0\}$ has an unique representation in the form

$$f = \bigoplus_{\alpha \in V_n} c_\alpha x^\alpha,$$

where $c_\alpha \in \{0,1\}$, $x^\alpha = x_1^{\alpha_1}...x_n^{\alpha_n}$, $x = (x_1, ..., x_n)$, $\alpha = (\alpha_1, .., \alpha_n) \in V_n$. The number $|\alpha| = \alpha_1 + ... + \alpha_n$ is called the degree of monomial x^α and the number $\deg f = \max\{|\alpha| : c_\alpha = 1, \alpha \in V_n\}$ is called the degree of the function f. The minimal degree of an ideal $I \triangleleft B_n$ is defined as follows:

$$\min \deg I = \min\{\deg f \colon f \in I \setminus \{0\}\}.$$

Let's consider a vectorial Boolean function (an s-block) $s : V_n \to V_n$ with the coordinate functions $s_1, ..., s_n$ and denote by $I(s)$ the following ideal in the ring of Boolean functions in $2n$ variables $x = (x_1, ..., x_n)$ and $y = (y_1, ..., y_n)$:

$$I(s) = \langle y_1 \oplus s_1(x), ..., y_n \oplus s_n(x) \rangle.$$

By definition [4], the algebraic immunity of the vectorial function s is the number $AI(s) = \min \deg I(s)$. The following statement is a direct consequence of results from the previous section.

Statement 4 *The algebraic immunity of a vectorial function $s : V_n \to V_n$ equals:*
a) to the minimum of degrees of all functions $g \in B_{2n}$ satisfying the condition

$$\forall x, y \in V_n : s(x) = y \Rightarrow g(x, y) = 0$$

(in this case we say that the equation $g(x, y) = 0$ describes the vectorial function s);
b) to the minimal degree of the ideal $Ann(f_s)$, where the function $f_s : V_{2n} \to \{0, 1\}$ is defined as follows:

$$\forall x, y \in V_n \colon f_s(x, y) = \begin{cases} 1, & s(x) = y; \\ 0, & otherwise. \end{cases}$$

Thus, to estimate the algebraic immunity of a vectorial function s it is sufficient to construct the function f_s and find the smallest degree of nonzero Boolean functions that annihilate it. Based on the results from Sec. 5.1 in [9] let us prove the following statement, which enables to use the Gaussian elimination for finding the algebraic immunity of a vectorial function. First, let us introduce a few notation.

For any positive integer d denote

$$m(n, d) = \sum_{i=0}^{d} \binom{2n}{i}.$$

For an arbitrary vectorial function $s : V_n \to V_n$ consider the $2^n \times m(n, d)$ matrix $C_{s,d}$ whose rows are numbered by the vectors $x \in V_n$ and the columns — by the pairs (α, β), where $\alpha, \beta \in V_n$ and $|\alpha| + |\beta| \le d$. By definition, an element of the matrix $C_{s,d}$ located at the intersection of its row with the number x and the column with the number (α, β) is equal to the value of the monomial $u^\alpha v^\beta$ at the point $(u, v) = (x, s(x))$.

Statement 5 *We have*

$$AI(s) \ge d + 1 \Leftrightarrow rank(C_{s,d}) = m(n, d).$$

Proof. According to the definition of the matrix $C_{s,d}$, a non-zero function

$$f(x, y) = \bigoplus_{\alpha, \beta \in V_n \colon |\alpha| + |\beta| \le d} c_{\alpha,\beta} x^\alpha y^\beta$$

belongs to the ideal $Ann(f_s)$ if and only if the vector $(c_{\alpha,\beta} \colon \alpha, \beta \in V_n, |\alpha| + |\beta| \le d)$ is a non-zero solution of the system of linear equations $C_{s,d} z^\downarrow = 0^\downarrow$. Therefore,

$$\begin{aligned} &AI(s) \ge d + 1 \Leftrightarrow \\ &\Leftrightarrow (\forall f \in Ann(f_s) \setminus \{0\} \colon deg f \ne d + 1) \Leftrightarrow \\ &\Leftrightarrow \text{ the system of equations } C_{s,d} z^\downarrow = 0^\downarrow \\ &\qquad \text{has no non-zero solutions} \Leftrightarrow \\ &\qquad \Leftrightarrow rank(C_{s,d}) = m(n, d). \end{aligned}$$

Statement is proved.

Consequence 2 *Let d be the maximal positive integer satisfying the inequality $m(n, d) \le 2^n$. Then*
a) $AI(s) \le d + 1$;
b) $AI(s) = d + 1$ if and only if $rank(C_{s,d}) = m(n, d)$.

Thus, according to Consequence 2, to estimate the algebraic immunity of a vectorial Boolean function $s \colon V_n \to V_n$ it is sufficient:

1) to find the maximal positive integer d such that $m(n, d) \le 2^n$;

2) to construct the matrix $C_{s,d}$ and evaluate its rank using the Gaussian elimination algorithm. If $rank(C_{s,d}) = m(n, d)$, then $AI(s) = d + 1$; otherwise we have $AI(s) \le d$.

Example 1. Let $n = 8$, then $m(8, 2) = 137 < 2^8 < m(8, 3)$. Thus, $d = 2$ and the algebraic immunity of any function $s \colon V_8 \to V_8$ is not greater than 3. Further, the matrix $C_{s,2}$ has the size 256×137; hence $AI(s) = 3$ if and only if $rank(C_{s,2}) = 137$.

3. Groebner bases of ideals in the ring of Boolean functions

Let's denote by N_0^n the set of n-dimensional vectors with non-negative integer coordinates. This set is a semi-group with respect to the operation + of vector addition. The partial ordering $\le$ on the set N_0^n is defined as follows:

$$\forall \alpha = (\alpha_1, ..., \alpha_n), \beta = (\beta_1, ..., \beta_n) \in N_0^n \colon$$

$$\alpha \le \beta \Leftrightarrow (\alpha_i \le \beta_i, i = 1, 2, ..., n).$$

The number $|\alpha| = \alpha_1 + ... + \alpha_n$ is called the multidegree of the vector $\alpha = (\alpha_1, ..., \alpha_n) \in N_0^n$. A monomial ordering is a linear order $\preceq$ on the set N_0^n satisfying the conditions:

1) $\forall \alpha, \beta \in N_0^n \colon \alpha \le \beta \Rightarrow \alpha \preceq \beta$;
2) $\forall \alpha, \beta, \gamma \in N_0^n \colon \alpha \preceq \beta \Rightarrow \alpha + \gamma \preceq \beta + \gamma$,

A monomial ordering $\preceq$ is called graded if for all $\alpha, \beta \in N_0^n$ the following condition holds: $|\alpha| \le |\beta| \Rightarrow \alpha \preceq \beta$. In the sequel, the notation $\alpha \prec \beta$ ($\alpha < \beta$) means that $\alpha \preceq \beta$ ($\alpha \le \beta$) and $\alpha \ne \beta$.

Example 2. The lexicographic order on the set N_0^n is defined by

$$\alpha \prec_{lex} \beta \Leftrightarrow (\exists i \in \{1,2...,n\}: \alpha_1 = \beta_1, ..., \alpha_{i-1} = \beta_{i-1}, \alpha_i < \beta_i),$$

and is a monomial ordering on N_0^n. The relation $\alpha \prec_{drl} \beta$, where $\alpha = (\alpha_1, ..., \alpha_n), \beta = (\beta_1, ..., \beta_n) \in N_0^n$, defined by

$$\alpha \prec_{drl} \beta \Leftrightarrow |\alpha| \le |\beta| \text{ or } (|\alpha| = |\beta| \text{ and } (\beta_n, ..., \beta_1) \prec_{lex} (\alpha_n, ..., \alpha_1))$$

is a graded monomial ordering on the set N_0^n.

A monomial ordering $\preceq$ allows us to order the Boolean monomials $x^\alpha = x_1^{\alpha_1}...x_n^{\alpha_n}$ by the rule $x^\alpha \preceq x^\beta \Leftrightarrow \alpha \preceq \beta$, where $\alpha, \beta \in V_n$ (hereafter the set V_n is considered as a subset of the semi-group N_0^n). This ordering on the set of monomials allows us to define the leading monomial of any nonzero Boolean function $f(x) = \bigoplus\limits_{\alpha \in V_n} c_{\alpha,f} x^\alpha$, where $c_{\alpha,f} \in \{0,1\}$, $\alpha \in V_n$:

$$LM_\preceq(f) = max_\preceq\{x^\alpha : c_{\alpha,f} = 1\}.$$

Example 3. Let $n = 3$; then

$$(0,0,0) \prec_{lex} (0,0,1) \prec_{lex} (0,1,0) \prec_{lex} (0,1,1) \prec_{lex} \prec_{lex} (1,0,0) \prec_{lex} (1,0,1) \prec_{lex} (1,1,0) \prec_{lex} (1,1,1).$$

Therefore,

$$(0,0,0) \prec_{drl} (1,0,0) \prec_{drl} (0,1,0) \prec_{drl} (0,0,1) \prec_{drl} \prec_{drl} (1,1,0) \prec_{drl} (1,0,1) \prec_{drl} (0,1,1) \prec_{drl} (1,1,1).$$

Let $f(x_1, x_2, x_3) = x_2x_3 \oplus x_1 \oplus x_2 \oplus x_3$; then

$$LM_{\prec_{lex}}(f) = x_1,\ LM_{\prec_{drl}}(f) = x_2x_3.$$

By definition a monomial x^α is divisible by a monomial x^β, if $\alpha \ge \beta, \alpha, \beta \in V_n$.

Let I be a nonzero ideal in the ring of Boolean functions in n variables. A system $g_1, ..., g_m \in I$ is called a Groebner basis of the ideal I for the monomial ordering $\preceq$ on the set N_0^n if for any $f \in I$ there exists $i \in \{1, 2, ..., m\}$ such that $LM_\preceq(f)$ is divisible by $LM_\preceq(g_i)$. A Groebner basis $g_1, ..., g_m$ is called minimal if $LM_\preceq(g_i)$ is not divisible by $LM_\preceq(g_j)$ for all $i \ne j$.

Statement 6 *For any nonzero ideal $I \lhd B_n$ there exists a minimal Groebner basis.*

Proof. Let $I \setminus \{0\} = \{g_1, ..., g_t\}$ (where $t \le |B_n| = 2^{2^n}$), $LM_\preceq(g_i) = x^{\alpha_i}$, $i = 1, 2, ..., t$. Let's delete from the set $\{1, 2, ..., t\}$ all elements i such that x^{α_i} is divisible by some monomial x^{α_j}, where $j \ne i$. If $\{i_1, ..., i_m\}$ is the set of elements that remains after deleting, then according to the above definition the system $\{g_{i_1}, ..., g_{i_m}\}$ is a minimal Groebner basis of I. Statement is proved.

Example 4. Let $n = 3$ and $f(x_1, x_2, x_3) = x_1x_2 \oplus x_1 \oplus x_2 \oplus x_3$. Let's construct a minimal Groebner basis of ideal $I = \langle f \rangle$ for the monomial ordering $\prec_{drl}$. Observe that I contains the functions

$$\begin{aligned} f(x_1, x_2, x_3) &= x_1x_2 \oplus x_1 \oplus x_2 \oplus x_3, \\ x_1 f(x_1, x_2, x_3) &= x_1x_3 \oplus x_1, \\ x_2 f(x_1, x_2, x_3) &= x_2x_3 \oplus x_2, \end{aligned}$$

whose leading monomials form the set of all monomials of degree 2 in x_1, x_2, x_3. Next, the set $V(I)$ contains exactly 4 vectors (the zeroes of f). So, $\deg g \ge 2$ for all $g \in I \setminus \{0\}$. Indeed, if the ideal I contains a non-zero affine function, then it is balanced, turns into zero on the set $V(I)$, and, therefore, coincides with f.

Thus, the system of functions

$$f(x_1, x_2, x_3),\ x_1 f(x_1, x_2, x_3),\ x_2 f(x_1, x_2, x_3)$$

is a minimal Groebner basis of the ideal I.

4. Application of Groebner bases for constructing the lowest-degree equations describing a vectorial Boolean function and computing its algebraic immunity

The following statement solves the problem formulated at the Introduction of the paper.

Statement 7 ([4]) *Let $s: V_n \to V_n$ be a vectorial Boolean function, $\preceq$ be a graded monomial ordering on the set N_0^n, G be a minimal Groebner basis of the ideal $I(s)$ for this ordering. Let $g_1, ..., g_m$ be all functions from G with the lowest degree d. Then*

1) *$AI(S) = d$;*
2) *any function $f \in I(S)$ of degree d can be uniquely represented in the form*

$$f = c_1g_1 \oplus \cdots \oplus c_mg_m \quad (6)$$

where $c_i \in \{0,1\}$, $i = 1, 2, ..., m$. In particular, the ideal $I(S)$ contains exactly 2^m functions of degree d.

Proof. Let $f \in I(s) \setminus \{0\}, LM_\preceq(f) = x^\alpha$. Then $|\alpha| = \deg f$ because $\preceq$ is a graded ordering. According to the definition of Groebner basis, x^α is divisible by some monomial $x^\beta = LM_\preceq(g)$, where $g \in G$. Thus, $\alpha \ge \beta$ and $\deg f = |\alpha| \ge |\beta| = \deg g \ge d$, where the last inequality follows from the definition of d. So, the degree of each function $f \in I(s) \setminus \{0\}$ is at least d and, because $g_1 \in I(s)$ and $\deg g_1 = d$, we have $AI(s) = \min \deg I(s) = d$.

Let now $f \in I(s)$ and $\deg f = d$. Based on the above considerations we obtain $d = \deg f = |\alpha| \ge |\beta| = \deg g \ge d$ and $\alpha \ge \beta$, whence we have $\alpha = \beta$ and $g = g_i$ for some $i \in \{1, 2, ..., m\}$. So, the functions f and g_i have the same leading monomial x^α, where $|\alpha| = \deg f = \deg g_i = d$.

Let's consider the function $f^{(1)} = f \oplus g_i$ from the ideal $I(s)$. If $f^{(1)} = 0$, then $f = g_i$ has the form (6). Otherwise we have

$$f^{(1)} \in I \setminus \{0\}, \deg f^{(1)} = d,$$
$$LM_\preceq(f) \succ LM_\preceq(f^{(1)}),$$

and the above considerations are applicable to the function $f^{(1)}$: there exists $j \in \{1, 2, ..., m\}$ such that $LM_\preceq(f^{(1)}) = LM_\preceq(g_j)$ and, hence,

$$f^{(2)} \stackrel{def}{=} f^{(1)} \oplus g_j = 0$$

(and $f = f^{(1)} \oplus g_i = g_j \oplus g_i$ has the form (6)), or $f^{(2)} \in I \setminus \{0\}, \deg f^{(2)} = d$ and $LM_\preceq(f^{(1)}) \succ LM_\preceq(f^{(2)})$. It's

clear that after the finite number of steps the chain

$$LM_{\preceq}(f) \succ LM_{\preceq}(f^{(1)}) \succ LM_{\preceq}(f^{(2)}) \succ ...$$

will break and the representation (6) will be obtained for the function f. Finally, because G is a minimal Groebner basis of the ideal $I(s)$ the functions $g_1, ..., g_m$ are linearly independent over the field of two elements. Therefore, for each function $f \in I(s)$ of degree d there exists a unique representation (6).

Statement is proved.

Conclusion

The algebraic immunity $AI(s)$ of a vectorial Boolean function $s : V_n \to V_n$ is defined as the lowest degree of Boolean equations in $2n$ variables that describe the function s (Statement 4). To estimate the algebraic immunity the results from Section 2 can be used. They allow fast solving of the decision problem (whether or not the algebraic immunity is above the specified threshold) directly by the truth table of the vectorial function using the Gaussian elimination algorithm.

To estimate $AI(s)$ as well as to find all lowest-degree equations describing a vectorial Boolean function s it is sufficient to construct a minimal Groebner basis of the ideal $I(s)$ with respect to an arbitrary graded monomial ordering and use Statement 7. In practice, for computing a minimal Groebner basis of an ideal in the ring of Boolean functions the system of computer algebra *Magma* can be used [10]: for $n = 8$ computation takes a few seconds.

References

[1] N. T. Courtois and J. Pieprzyk, "Cryptanalysis of block ciphers with overdefined systems of equations," *ASIACRYPT 2002, volume 2501 of Lecture Notes in Computer Science. Springer-Verlag*, p. 267–287, 2002.

[2] A. Biryukov and C. de Canniere, "Block ciphers and systems of quadratic equations," *Fast Software Encryption. – FSE'03, Proceedings. – Springer-Verlag.*, p. 274 – 289, 2003.

[3] O. Billet and H. Gilbert, "Resistance of snow 2.0 against algebraic attacks," *Lecture Notes in Computer Science, vol 3376. Springer, Berlin, Heidelberg*, 2005.

[4] G. Ars and J.-C. Faugère, "Algebraic immunities of functions over finite fields," *Technical report, INRIA*, 2005.

[5] F. Armknecht and M. Krause, "Constructions single- and multi-output boolean functions with maximal algebraic immunity," *Automata, Languages and Programming, Proceedings. – LNCS 4052. – Springer-Verlag.*, p. 180 – 191, 2006.

[6] C. Carlet, "On the algebraic immunities and higher order nonlinearities of vectorial boolean functions," *Workshoop ACPTECC, Veliko Tavrono, Bulgaria*, p. 104 – 116, 2009.

[7] D. Ponkrasenko, "On the maximal component algebraic immunity of vectorial boolean functions," *Journal of Applied and Industrial Mathematics Vol. 10, № 2*, p. 257–263, 2016.

[8] D. Cox, J. Little, and D. O'Shea, "Ideals, varieties, and algorithms," *Springer-Verlag New York*, 2007.

[9] F. Armknecht, "On the existence of low-degree equations for algebraic attacks," *Cryptology ePrint Archive, Report 2004/185*, p. 267–287, 2004.

[10] J. Cannon, W. Bosma, C. Fieker, and A. Steel, "Handbook of magma functions," *Version 2.20, Sydney*, 2014.