Nonlinear Phenomena in Complex Systems, vol. **17**, no. 3 (2014), pp. 242 - 252

On Boolean Ideals and Varieties with Application to Algebraic Attacks

A. G. Rostovtsev and A. A. Mizyukin
Saint-Petersburg State Polytechnic University,
29 Politechnicheskaya Str, 195251 Saint-Petersburg, RUSSIA
(Received 21 March, 2014)

To find a symmetric cipher key is to solve the zero ideal of a specified set of polynomials. It is shown that the complexity of solutions can be reduced if the exact or approximate basis of the ideal substitution is defined by short polynomials. The accuracy of short basis polynomials can be improved by an affine change of variables. Two methods are proposed for solving systems of Boolean equations with the use of auxiliary short polynomials.

PACS numbers: 89.70.-a
Keywords: cipher, polynomial ring, ideal, variety, Groebner basis

1. Introduction

Symmetric cipher, hash function, as well as any computable function, is described by a set of polynomials in the Zhegalkin polynomial ring. Any finite set of polynomials forms an ideal. Zeroes of an ideal form a variety.

The problem of key breaking or hash function inversion is reduced to solving a system of polynomial equations. If the cipher has several cycles of encryption, the unknowns are the number of bits of key and intermediate texts. For example, if AES cipher has 10 cycles, an encryption key length and block length of 128 bits, and if the plaintext and ciphertext are known, then the number of unknowns is 1280. If the solution is unique, then the corresponding variety contains a unique point in the affine space over the original field.

To find the common zero of Zhegalkin polynomials, Faugere method is used to calculate Groebner basis [1], equivalent XL / XSL Courtois method [2], the method of resultants [3], the method of characteristic sets of Wu and Ritts [4], the Semaev method of gluing and agreeing [5], which does not operate with polynomials, but with tables of their values.

These methods are called algebraic attacks and they have a lot in common. In particular, a common feature of them is that the initial and final description of equations has a simple form, that is, polynomials are sparse. However, when making a solution, the intermediate polynomials are no longer sparse, which is time consuming and requires exponentially bigger memory size.

Since the Zhegalkin polynomial is linear in each variable, it can be represented as $f = f_0 + f_1 x$, where f_0, f_1 do not depend on the chosen variable x. If $g = g_0 + g_1 x$, then to eliminate variable x we will find $fg_1 + gf_1 = f_0 g_1 + f_1 g_0$. Therefore, equations $f = 0$, $g = 0$ imply an equation for the determinant $\begin{vmatrix} f_0 & f_1 \\ g_0 & g_1 \end{vmatrix} = 0$. It allows replacing two equations with one, and in case of k equations replace them with $k - 1$ equations. In the Zhegalkin polynomial ring every polynomial is a zero divider, and multiplication by zero divisor can lead to an increase in the number of solutions, but given replacement of two equations with one preserves uniqueness of the solution. Such method of variable elimination is reduced to an Faugere algorithm, since multiplication of polynomials reduces to multiplication of the polynomial by a monomial.

Modern ciphers use mixing transformations, described by nonlinear equations, and diffusion transformations, described by linear equations. Substitutions on short length words are generally used as a mixing transformation. The complexity of the solving system of polynomial equations is determined by properties of substitution.

Ciphers are designed so that it is difficult to specify a metric indicating how close the test key is to the searched key. Sometimes it is suitable to define this metric averaged for a large number of open texts and relevant ciphertexts, which is used, in particular, in differential and linear methods [6–8]. To disable these methods, substitutions with special properties are selected. According to papers [9, 10], special substitutions apparently have no advantages compared to random substitutions.

This paper shows that the complexity of solving systems of polynomial equations can be reduced by defining or supplementing an ideal with short polynomials that have a small number of terms. Algorithms of such ideal definition and improved algorithms for solving systems of polynomial equations are proposed.

2. Ideals and varieties of the polynomial ring

In this paper symbol + denotes the sum of elements of the ring, $\oplus$ – sum of ideals, ideals are designated with uppercase letters, vectors are denoted in bold, $\oplus_2$ – field of two elements.

Let R be a commutative associative ring with identity. Ideal $A \subseteq R$ is a set (subring) of such elements of the ring, that if $f,\ g \in A$, then $f \pm g \in A$ and $fr \in A$ for any $r \in R$. The set of ring ideals is partially ordered by inclusion. If $A \supseteq B$, then we say, that B is divisible by A. If $A = (f_1,\ \ldots,\ f_k)$, then $f_1,\ \ldots,\ f_k$ are the basis of the ideal , every element of A is a linear combination of the basis elements with coefficients in R. The main ideal is defined by a single polynomial $A = (f)$.

Commutative and associative addition $A \oplus B = (A, B)$ and multiplication operations are defined for ideals. If the product of ideals AB is generated by products of elements of $A,\ B$. If $f \in A$, then we say that f is divisible by A. The intersection of ideals $A \cap B \supseteq AB$ is the largest ideal containing A and B. Every ideal is contained in some maximal ideal M, differing of R. The prime ideal is defined as an ideal for which the residue class ring is complete. Every prime ideal is maximal, in an Artinian ring the contrary is true as well [11].

If R is Noetherian (strictly ascending chain of ideals is limited), any of its ideal has a finite basis. A ring in which any strictly ascending chain of ideals is limited called an Artinian one. The maximum chain length of ascending prime ideals of R ring is called the dimension of the ring. An Artinian ring is a Noetherian ring of dimension 0 [11].

Every ideal is characterized by a set of zeros. Ideals A and A^2 have the same set of zeros, but $A \supseteq A^2$. The highest ideal, which has the same set of zeros as A, is called radical A. The radical ideal coincides with its own radical.

Let K be a field, $K[x_1,\ \ldots,\ x_n]$ be a polynomial ring, $N^n(K)$ be an affine space. Any ideal $A \subseteq K[x_1,\ \ldots,\ x_n]$ defines variety $V(A)$ – set of points $P \in N^n(K)$, in which $A = 0$ (radical ideals bijectively correspond to varieties). A maximal ideal defines variety consisting of one point. Intersection (product) of ideals corresponds to varieties union, the sum of ideals corresponds to intersection of varieties. According to the Hilbert theorem on basis, each ideal of the ring $K[x_1,\ \ldots,\ x_n]$ is finitely generated [12] and is uniquely defined by the intersection of the powers of maximal ideals.

For an ideal $A \subseteq K[x_1,\ \ldots,\ x_n]$ with variety $V(A)$ coordinate ring $K[x_1,\ \ldots,\ x_n]/A$ is defined, whose elements are called functions on $V(A)$.

In the ring of polynomials of several variables the division of a polynomial on the ideal is actually ambiguous and depends on the order of division into elements of a basis. Groebner bases are used to resolve ambiguity.

Uniqueness of the division is obvious for monomials and is defined by the partial ordering of monomials by multidegree: $x_1^{c_1}x_2^{c_2}\ \ldots\ x_n^{c_n}$ is devisable by $x_1^{d_1}x_2^{d_2}\ \ldots\ x_n^{d_n}$, if $c_1 \geqslant d_1,\ c_2 \geqslant d_2,\ \ldots,\ c_n \geqslant d_n$. Polynomial f is devisable by monomial h, if every monomial of polynomial f is devisable by h.

To calculate the Groebner basis, ordering of monomials is introduced. Let $\mathrm{LT}(f)$, $\mathrm{LT}(g)$ be the leading terms of polynomials f, g, and $\mathrm{LCM}_{f,g}$ be

the least common multiple of relevant monomials. Buchberger algorithm for computing Groebner basis for all pairs of polynomials (f, g) of the ideal basis computes syzygies

$$S(f,g) = \frac{\mathrm{LCM}(f,g)}{\mathrm{LT}(f)} f - \frac{\mathrm{LCM}(f,g)}{\mathrm{LT}(g)} g$$

(thus leading monomials are reduced) and adds them to the basis. As the number of monomials is finite, then at some step the process stops. Basis $(g_1, \ldots, g_m)$ is a Groebner basis if for any g_i, g_j their syzygy will be devisable by some polynomial of the basis. To remove excess polynomials from the Groebner basis the algorithm of ideal reduction is used [13]. In the case of linear polynomials an algorithm for computing the Groebner basis is analogical to the Gaussian elimination algorithm.

Groebner bases can be used for solving systems of polynomial equations in the ring $K[x_1, \ldots, x_n]$, since any set of polynomials defines an ideal and the corresponding variety , and solving the system of equations means finding this variety. If the system has a unique solution $(e_1, \ldots, e_n)$, $e_i \in K$, then the Groebner basis has the form $(x_1 - e_1, \ldots, x_n - e_n)$.

3. Boolean rings, their ideals and varieties

In Boolean ring R we have the relation $a^2 = a$ for all $a \in R$. The Boolean ring has characteristic 2 by equations $a + a = (a + a)^2 = a^2 + 2a^2 + a^2 = a + a + 2a$, where $2a = 0$. Moreover, the Boolean ring is commutative by equations $a + b = (a + b)^2 = a^2 + ab + ba + b^2 = a + b + ab + ba$, from which $ab = ba$.

Elements of finite Boolean rings are Boolean functions. Every Boolean function f of n variables $\mathbf{x} = (x_1, \ldots, x_n)$ can be uniquely defined by 2^n-dimensional vector $\mathbf{f}$ of values for sets of arguments $((0, \ldots, 0), (0, \ldots, 0{,}1), (0, \ldots, 0{,}1{,}1), \ldots, (1, \ldots, 1))$. Furthermore, function f can be defined by the Zhegalkin polynomial
$f = a_0 + a_n x_n + a_{n-1} x_{n-1} + a_{n,n-1} x_n x_{n-1} + a_{n-1} x_{n-1} + \ldots + a_{n,n-1,\ldots 1} x_n x_{n-1} \ldots x_1$,
i.e. vector of coefficients $\mathbf{a} = (a_0, a_n, a_{n-1}, a_{n,n-1}, a_{n-2}, \ldots, a_{n,n-1,\ldots 1})$ length 2^n.

The Zhegalkin polynomial ring $G_n[\mathbf{x}]$, $\mathbf{x} = (x_1, \ldots, x_n)$, is defined as the residue class ring $G_n[\mathbf{x}] = \oplus_2[x_1, \ldots, x_n]/({x_1}^2 + x_1, \ldots, {x_n}^2 + x_n)$, where $\oplus_2 = \{0, 1\}$. By equation $f^2 + f = f(f + 1) = 0$ every element is a zero divisor , so the zero ideal is not simple.

Since the ring $G_n[\mathbf{x}]$ is finite, it is Artinian, so the product of their ideals coincides with their intersection, ring dimension is 0, sets of prime and maximal ideals coincide, every ideal is radical. The prime ideal corresponds to a variety, consisting of a single point. The product of all prime ideals is 0. Every ideal is uniquely represented as a product of prime ideals.

The prime ideal corresponding to the point $(e_1, \ldots, e_n)$, can be defined by one polynomial $1 + \prod_{i=1}^{n} (x_i + e_i + 1)$. Therefore, every ideal of the ring $G_n[\mathbf{x}]$ can be defined by a single polynomial, and every polynomial defines some ideal.

Unique decomposition into prime factors allows determining division of ideals. Ideal A is devisable by ideal B, if a set of zeros of ideal B is a subset of the set of zeros of A. Consequently, there is no need to use Groebner bases for division in $G_n[\mathbf{x}]$.

If $A = \prod_{i \in I} P_i$, $B = \prod_{i \in J} P_i$ is a decomposition on prime ideals, then the greatest common divisor of ideals $\mathrm{GCD}(A, B) = \prod_{i \in I \cap J} P_i$, $\mathrm{LCM}(A, B) = \prod_{i \in I \cup J} P_i$. Here, instead of the product of ideals we can use their intersection.

The sum of ideals $(A, B) = (A \oplus B)$ is an ideal which algebraic set consists of intersection of zero sets of ideal A and B: $V(A \oplus B) = V(A) \cap V(B)$. In this case we obtain for the principal ideals $(f) \oplus (g) = (f + g + fg)$.

By analogy with decomposition of the ideal into product, we can consider the decomposition of the ideal into the sum of ideals. Analogues of prime ideals are additively irreducible ideals. Additively, an indecomposable ideal has a single identity value, so if P is a prime ideal, then $1 + P$ (complement to ideal P) is an additively indecomposable ideal.

Theorem 1. *Ring $G_n[x]$ is isomorphic to ring $G(2^n)$ 2^n- dimensional binary vectors with operations of coordinate-wise multiplication and addition.*

Proof . Zero and identity element of the ring $G_n[\mathbf{x}]$ are constants 0 and 1. Zero of the ring $G(2^n)$ is a null vector, the identity element is a vector with all unit coordinates. There is a bijection between elements of the rings $G_n[\mathbf{x}]$ and G (2^n), defined as a transition from the vector of values of the Boolean function to the vector of coefficients. In this case the vector sum of the values of Boolean function will correspond to the sum of polynomials (vector sum of their coefficients), and the product of the vectors of values will correspond to the product of polynomials (convolution of coefficient vectors). Hence, these rings are isomorphic ones. ■

Lagrange's interpolation formula implies that if $\mathbf{f} \in G(2^n)$ is a vector of values of the Boolean function of n variables at points ((0, …, 0), (0, …, 0,1), (0, …, 0,1,1), …, (1, …, 1)), $\mathbf{a}$ is a coefficient vector of relevant Zhegalkin polynomial of $G_n[\mathbf{x}]$, then $\mathbf{a} = L_n\mathbf{f}$, where $L_1 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, $L_{i+1} = \begin{pmatrix} L_i & 0 \\ L_i & L_i \end{pmatrix}$. Since $L_n = {L_n}^{-1}$, then $\mathbf{f} = L_n\mathbf{a}$. Matrix L_n of size 2^n contains in each row and each column the number of nonzero elements raised to the power of 2. The complexity of calculation of the given isomorphism is $O(2^n)$. Therefore, if the number n is not large, it is not possible to differentiate between rings $G_n[\mathbf{x}]$ and $G(2^n)$.

In the ring $G_n[\mathbf{x}]$ two types of division are defined: an ordinary polynomial division (P-division) $f = gh$, $\deg(f) = \deg(g) + \deg(h)$, uniquely defined, and algebraic- geometric division (AG - division): $f = gh$, if $V(f) = V(g) \cup V(h)$, not uniquely defined. Two types of ideal division are defined respectively. In this case ideal A is devisable by B (AG-division), if $V(A) \supseteq V(B)$. Then there is ideal C, so that $A = BC$ and $V(A) = V(B) \cup V(C)$. P-division is a special case of AG-division. P-division is used in calculation of Groebner bases.

Two types of division are based on two types of analysis of ideal $F = (x_1^2 + x_1, \ldots, {x_n}^2 + x_n)$, defining the field $\oplus_2$. In the case of P-dividing this ideal is considered as external with respect to the original infinite integral ring of polynomials, and it can be added to the basic ideal, defining the desired variety (describing the set of keys to the given plaintexts and ciphertexts). In the case of AG- dividing this ideal is considered an integral part of the polynomial ring, which leads to presence of zero divisors.

Let the cipher be described by a set of polynomials in the ring $G_n[\mathbf{x}]$. This set of polynomials defines ideal A of variety $V(A)$, which in algebraic geometry is considered over an algebraically closed field. Even if the key is uniquely determined, the variety contains a large number of zeros (finite or infinite), whose power exceeds the power of the set of keys. To obtain the solution in a simple field we add to ideal A an ideal that defines field $\oplus_2$, i.e. we carry out calculations in the ideal $A \oplus F$.

To simplify the computational process Courtois and Faugere [1, 2] proposed to isolate F from common ideal $A \oplus F$, computing the Groebner basis for the ideal A and the resulting syzygy of modulo ideal F. Generalizing this approach, one can assume ideal A as sum $A = B \oplus I$, isolate from the ideal $A \oplus F = B \oplus I \oplus F$ ideal $I \oplus F$ for some opportune ideal I and compute the Groebner basis for ideal B, resulting syzygy of modulo ideal $I \oplus F$. Therefore, instead of the original polynomial ring $\oplus_2[x_1, \ldots, x_n]$ (or ring $G_n[\mathbf{x}]$) it is considered the coordinate ring of variety $V(I \oplus F)$, and syzygies are considered functions on the variety.

4. Ideal substitution and short additive decomposition

Basically, a cipher is built using substitutions on 3–8 bit words and diffusion mapping. Substitutions are described by nonlinear polynomials, diffusion mappings are usually defined by linear mappings of the form $\mathbf{y} = L\mathbf{x}$, where L is an invertible matrix. The complexity of solving the

system of equations describing the cipher is mainly determined by non-linear substitution polynomials. Any mapping is defined by a set of Zhegalkin polynomials, that is the ideal and the corresponding variety, which can be interpreted as a vector of values of ideal for all possible sets of variables.

If the substitution $\mathbf{y} = S(\mathbf{x})$ forces on n – bit words, then the polynomials from $(x_1, \ldots, x_n, y_1, \ldots, y_n)$, reverted to 0 at points, where equation $\mathbf{y} = S(\mathbf{x})$ is true, become elements of ideal substitution $\mathrm{A}_S \subset G_{2n}[\mathbf{x}, \mathbf{y}]$. Principal ideal is defined by polynomial, reverting to 0 exactly at points satisfying the equation $\mathbf{y} = S(\mathbf{x})$. The substitution variety consists of 2^n points.

To withstand cryptanalysis methods substitutions $\mathbf{y} = S(\mathbf{x})$ are selected in a special way. Let $\mathbf{x}$, $\mathbf{x}\prime$ be the pair of inputs, $\mathbf{y}$, $\mathbf{y}\prime$ be corresponding outputs. The differential substitution is the pair $(\Delta\mathbf{x}, \Delta\mathbf{y})$, where $\Delta\mathbf{x} = \mathbf{x} + \mathbf{x}\prime$, $\Delta\mathbf{y} = \mathbf{y} + \mathbf{y}\prime$, is characterized by its probability, if $\mathbf{x}$ runs through all set of inputs [14]. The most probable differential must have a minimum probability. Also, probabilities of equations $\mathbf{ax} + \mathbf{by}$ for all possible vectors $\mathbf{a}$, $\mathbf{b}$ must have a minimum deviation from 0.5.

Solution of the system of Boolean equations describing the cipher is difficult for the following reason (it is sufficient to show this for the Groebner bases). The original basis of the ideal is defined by a small number of short polynomials. The final basis for an ideal is also defined by a small number of short polynomials. However, when computing syzygies the power and length of polynomials increase. Even if the original polynomials have power 2 and lengths m_1, m_2, their syzygy already has power 3 and length $m_1 + m_2 - 2$. Thus, all syzygies of binomial ideal are binomials. Moreover, the length of the syzygy of polynomial and binomial equals to the length of the polynomial. This demonstrates the necessity of defining the ideal basis not by polynomials describing the separate bits substitution, but using as short polynomials (monomials, binomials, trinomials) as possible, even if their number is large.

We call an ideal monomial (binomial, trinomial, quadrinomial), if it is defined by monomials (binomials, trinomials, quadrinomials, respectively). If the ideal of the Boolean polynomials has a unique zero $(e_1, \ldots, e_n)$, then it is a binominal and has a form $(x_1 + e_1, \ldots, x_n + e_n)$.

Let $A = (f) = (f_1, \ldots, f_k) = (f_1) \oplus \ldots \oplus (f_k)$ be additive decomposition of the ideal. Then for the corresponding vector values we have: $\mathbf{f} = \mathbf{f}_1 \vee \ldots \vee \mathbf{f}_k$. The following assertion is true.

Theorem 2. *Every ideal is uniquely represented by the sum of additively indecomposable ideals.*

Proof If the ideal (g) is prime, then ideal $(1 + g)$ is additively indecomposable. Taking into account the equation $\mathbf{g}_1 \vee \ldots \vee \mathbf{g}_k = 1 + (1 + g_1)\ldots(1 + g_k)$ and unique decomposition of ideal on product of prime ideals we obtain the required assertion. ■

Hence, ideals under addition form a commutative monoid isomorphic to the monoid of binary vectors with the operation OR.

We are interested in additive decomposition not into irreducible polynomials, but into as short polynomials as possible. Obviously, the ideal substitution cannot be defined only by monomials. Let us consider the relationship of binomial ideals and Boolean functions in disjunctive normal form (DNF). DNF without inversions forms a commutative semi-ring.

Theorem 3. *An ideal is binomial if and only if, when it is defined by DNF in which each conjunction has no more than one inversion.*

Proof Let us prove that if DNF consists of conjunctions in which each variable has no more than one inversion, it defines a binomial ideal. Let m be a monomial. Since $m\overline{x} = m + mx$ is a binomial, then such DNF defines binomial ideal. Conversely, let $(f) = (f_1, \ldots, f_k)$ and all f_i be binomial. We will show that every binomial can be represented with DNF, in which only one variable has an inversion. It is sufficient to consider one binomial $m_1 + m_2 = m_1\overline{m}_2 \vee \overline{m}_1 m_2$, where m_1, m_2 are monomials. Due to the equation $\overline{x_1 \ldots x_l} = \overline{x}_1 \vee \ldots \vee \overline{x}_l$ we obtain the required assertion. ■

Note, that DNF in theorem 3 must be minimized.

The Boolean function is symmetric if its values do not change after an arbitrary permutation of variables. Denote $S_i(x_1, \ldots, x_n) \in G_n[\mathbf{x}]$ as i-th elementary symmetric polynomial. We define the elementary symmetric DNFs: $T_i(x_1, \ldots, x_n)$, $0 \leqslant i \leqslant n$, – disjunction of all conjunctions containing exactly i variables with inversion $0 \leqslant i \leqslant n$. For example, $T_1(x_1, x_2, x_3) = \overline{x}_1 x_2 x_3 \vee x_1 \overline{x}_2 x_3 \vee x_1 x_2 \overline{x}_3$. Here $T_i T_j = 0$ for $i \neq j$. It is true for the semi-ring DNF analogue of the theorem on symmetric polynomials in the polynomial ring.

Theorem 4. *Any symmetric DNF can be represented as a disjunction in the elementary symmetric functions.*

Proof It is sufficient to consider non-constant functions. We lexically order identity values of a Boolean function f: bigger sets of variables contain many inversions. Any symmetric function has an identity value for the higher set of variables containing m inversions. It has an identity value for all sets with m inversions, i.e. $f = T_m \vee \ldots$ Then we proceed to the succeeding sets of variables containing m_1 inversions and so on. We obtain $f = T_m \vee T_{m_1} \vee \ldots \vee T_{m_k}$. ■

Let us consider trinomial ideals.

Theorem 5. *DNF is a trinomial in ring $G_n[\boldsymbol{x}]$, if and only if DNF can be represented in the form $f = T_0(C_1, C_2, C_3) \vee T_2(C_1, C_2, C_3)$, where C_1, C_2, C_3 are conjunctions without variables inversions.*

Proof It is directly verified, that f takes on the value 1 if and only if $C_1 + C_2 + C_3 = 1$. Any trinomial can be defined in this way. ■

Corollary 6. Ideal is trinomial if and only if its defining polynomial f can be represented in DNF in following form

$$f = \vee_i (T_0(C_{1i}, C_{2i}, C_{3i}) \vee T_2(C_{1i}, C_{2i}, C_{3i})),$$

where C_{ji} are conjunctions without inversions.

The proof follows directly from Theorem 5.

Similarly, DNF is the sum of the four monomials in the Zhegalkin polynomial ring if DNF is equal to 1 if and only if one or three terms of polynomial are equal to 1. Therefore, $C_1 + C_2 + C_3 + C_4 = T_1(C_1, C_2, C_3, C_4) + T_3(C_1, C_2, C_3, C_4)$.

Let us consider some of the algebraic properties of the Boolean functions defined in such basis.

Theorem 6. *Following equalities are true.*

1. $a \vee (a + b) = a \vee b$.
2. $a_1 \vee \ldots \vee a_n = S_1(a_1, \ldots, a_n) + \ldots + S_n(a_1, \ldots, a_n)$.
3. $(a_1 + b) \vee \ldots \vee (a_n + b) = S_1(a_1, \ldots, a_n) + \ldots + S_n(a_1, \ldots, a_n) + b(1 + S_1(a_1, \ldots, a_n) + \ldots + S_{n-1}(a_1, \ldots, a_n))$.

Proof First equation and all other equalities for $n = 2$ can be verified directly. Then we use an induction method. ■

Hence follows an algorithm for the approximate calculation of the ideal basis of the shortest polynomials. The algorithm of direct verification of short polynomials of the ring $G_{2n}[\mathbf{x}, \mathbf{y}]$, lying in ideal, is complex even for 4-bit substitution. For example, for $n = 4$ the number of trinomials is $2.7 \cdot 10^6$, the number of quadrinomials $-1.75 \cdot 10^8$, for $n = 8$ the number of binomials, trinomials, quadrinomials is $2.1 \cdot 10^9$, $4.7 \cdot 10^{13}$, $7.7 \cdot 10^{17}$ respectively. It is necessary to limit the number of analyzed monomials to accelerate the algorithm. The proposed algorithm works as follows.

Algorithm 1. Computation of short polynomials, defining ideal substitution.

1. We compute a set of zero substitutions $V(S)$ and its complement , compute polynomial $f(S)$, defining the principal ideal substitution.
2. We compute the list of monomials that are 0 at points from $V(S)$, and delete monomials that are devisable by any

monomial in the list (delete excess monomials). We obtain original basis of ideal A_1. We compile set $V_1 = \overline{V(S)} \cap V(A_1)$.

3. We find $f_2 = f(S) \pmod{A_1}$, compile the list T_2 of monomials of f_2 and divisors of this monomials.

4. We compile binomials from the list T_2 that are 0 in every point of $V(S)$, and are equal to 1 in some points of V_1. We add binomials to ideal basis and assume $A_2 = A_1 \oplus \{\text{found binomials}\}$. We delete excess binomials that do not change $V(A_2)$. We compile a set $V_2 = \overline{V(S)} \cap V(A_2)$.

5. We find $f_3 = f_2 \pmod{A_2}$, compile the list T_3 of the monomials of f_3 and divisors of this monomials.

6. We compile trinomials from the list T_3, that are 0 in every point of $V(S)$, and are equal to1 in some points of V_2. We join binomials to ideal basis and assume $A_3 = A_2 \cup \{\text{found trinomials}\}$. We delete excess trinomials, that do not change $V(A_3)$. We compile a set $V_3 = \overline{V(S)} \cap V(A_3)$.

7. We repeat the procedure of two last steps to find polynomials of length 4 and etc. The algorithm stops, when V_k is null, or its power is low enough (in the second case an approximate basis of the ideal substitution will be found).

5. Affine equivalence of ideals

The set of substitutions can be divided into affine equivalence classes $S_1 \sim S_2$, if $S_1 = AS_2B$, where A, B are affine substitutions of the form $A(\mathbf{x}) = L\mathbf{x} + \mathbf{c}$, L – invertible matrix. Affine equivalence of substitutions is a cryptanalysis tool [15]. Affine equivalence does not change the probability of the most probable differentials and linear sums.

During the computation of the Groebner bases of a system of polynomial equations it does not matter which variables describe the inputs and which ones describe the outputs of the substitution. Thus, we can permute input and output bits arbitrarily. Hence, the substitution ideal may correspond to two substitutions (original and reverse) or even greater number of substitutions. Ideal of the ring $A_S \subset G_{2n}[\mathbf{x}, \mathbf{y}]$, having 2^n zeroes, is the ideal of the mapping with input $\mathbf{u}$ if we can choose n variables $\{u_1, \ldots, u_n\} \subset \{x_1, \ldots, x_n, y_1, \ldots, y_n\}$ so, that all ideal zeroes correspond to a non-repeating sets $\{u_i\}$.

Thus, an ideal substitution corresponds to at least two substitutions: original and reverse. However, this does not exclude the existence of other maps having the same ideal. For example, ideal substitution $S_0[0]$ of the DES standard (e, 4, d, 1, 2, f, b, 8, 3, a, 6, c, 5, 9, 0, 7) corresponds to 6 maps (including original and reverse substitutions).

Let us define affine equivalence of ideals of the ring $G_{2n}[\mathbf{x}, \mathbf{y}]$: $A \sim B$, if $A(\mathbf{x}, \mathbf{y}) = B(L(\mathbf{x}, \mathbf{y}) + \mathbf{c})$, where L is invertible over $\oplus_2$ square matrix of size $2n$, multiplied by the column vector $(\mathbf{x}, \mathbf{y})$ of length $2n$. Affine equivalence of ideals is a generalization of affine equivalence of substitutions, where matrix L is block-diagonal. Affine equivalence separates the set of ideals into classes. In this case, an ideal which is affinely equivalent to substitution ideal may not be an ideal mapping, but the power of its variety is preserved.

Affine equivalence of ideals allows us to generalize the notion of differential and substitution nonlinearity. It is known that the affine substitution equivalence preserves the probability of the most probable differentials and substitution nonlinearity. A differential ideal is defined in the same way as that for substitution, the differential probability is averaged over the variety ideal. We define the non-linearity of the ideal as the minimum nonlinearity of the Boolean function, lying in this ideal. Affine equivalence of ideals preserves their nonlinearity and maximums of differential probabilities.

Affine equivalence of ideals is a convenient tool for solving systems of polynomial equations. For example, we can obtain a more convenient

system of polynomials by selecting a suitable affine transformation.

The group of invertible matrices is generated by transvections − matrices with identity elements on the main diagonal and only one identity element outside the main diagonal [16]. The required affine transformation can be found by the steepest descent method with minimization of the relevant objective function using transvections and shift vectors **c**.

Replacing the ideal substitution with an affine equivalent ideal may shorten the length of polynomials that define the ideal and improve the accuracy of the approximation of the ideal by short polynomials (monomials, binomials, trinomials). To calculate the affine reversible change of variables that optimizes the ideal substitution, you can use the method of the steepest descent. For example, at first we choose shift vector **c**, then we choose vectors of matrix L. During experimental studies of affine equivalent ideals for different substitutions it was noticed that a convenient affine equivalent ideal is obtained when the length of the polynomial defining the principal ideal is minimal.

Algorithm 2. Calculation of affine change of variables that optimizes the substitution ideal.

1. We calculate the polynomial $f(S)$ that defines the principal ideal substitution.

2. We calculate vector **c** that minimizes length $f(S)$. To do this, we perform the search on the change of variables x_i, y_i for $1 + x_i$, $1 + y_i$. Now we calculate the new $f(S)$.

3. We find the linear change of variables $x_1 \leftarrow x_1 + d_2x_2 + ... + d_{2n}y_n$, which minimizes the length of $f(S)$, searching on all d_i. Now we calculate the new $f(S)$.

4. Alternately, we repeat step 3 for variables $x_2, \ldots, y_n$.

5. If the minimum is not found, we repeat steps 3 and 4. The resulting affine equivalence is defined by vector **c** and matrix product, determining a linear change of variables. The affine equivalent principal ideal is defined by a polynomial $f(S)$.

6. Preparing the system of boolean equations and its solution

The cipher that utilizes substitutions and linear diffusing transformations is described by a set of Zhegalkin polynomials. In this case, nonlinear equations are defined by substitution. Traditionally, nonlinear Boolean equations describing the substitution are simple Boolean functions describing the output bits after the input has been changed. Such polynomials are usually inconvenient for solving the system.

It is more convenient if the system of equations is overdetermined: the number of equations is greater than the number of variables. This leads to the concept of the ideal. Courtois proposed to minimize the degree of the polynomials that define the ideal [2]. So, the ideal of 8-bit AES substitution is described by 24 implicit quadratic equations.

Theoretically, polynomials of the form $x_i^2 + x_i$, defining properties of Boolean rings, may be put into the ideal, with variety to be found, or, first, we have to compute a Groebner basis in a integral polynomial ring over a field $\oplus_2$, and then perform the reduction of the found basis by ideal modulo, defining the Zhegalkin polynomial ring. In this case, the found Groebner basis should not change. However, since each polynomial is a zero divisor, symbolic computing packages, (e.g, MATHEMATICA) give the wrong result of computing the Groebner basis for both cases. Faugere suggested using polynomials $x_i^2 + x_i$ separately, without calculating their syzygy, but limiting the degree of the monomial syzygy for each variable [1].

It seems more promising to define an ideal substitution by shortest possible polynomials, rather than minimize the degree of polynomials. In this case the number of polynomials is much bigger than the number of variables. Since the solution of linear equations is simple, in order to

minimize the length of the polynomials an affine equivalence of ideals can be used, as well as an approximate definition of the ideal using short polynomials (this leads to a slight increase in the power of the ideal variety).

Therefore, the proposed changes of algebraic attacks on the cipher are performed at two stages. At the preparation stage, the substitution ideal is replaced by an affine equivalent ideal, which can be defined by short polynomials (exactly or approximately), and polynomials, corresponding to this affine variables change, are introduced into the resulting ideal, for which a variety is being found. In addition, auxiliary ideal I is compiled, consisting of polynomials ${x_i}^2 + x_i$ and monomials, binomials, trinomials of substitution ideals. In this case $\mathrm{I} \equiv 0 \pmod{\mathrm{A}}$, $V(\mathrm{I}) \supset V(\mathrm{A})$ respectively.

At the second stage the Groebner basis for the resulting ideal is computed. In this case we are searching for syzygies of nonlinear polynomials. Note, that the syzygy of polynomials defining substitution lies in the ideal substitution. To reduce the length and degree each syzygy is reduced modulo ideal I. Thus if the monomial syzygy is divisible by any monomial ideal I, it is removed. Binomial syzygies, divisible by ideal I binomials and trinomials are also removed. Besides, ideal I binomial $C_1 + C_2$, consisting of two monomials means that the monomial syzygy, devisable by C_1, can be replaced by a monomial, devisable by C_2. If the syzygy has a sum in a form $A + B + C$, where $A + B$ and $A + C$ are devisable by ideal I binomials (binomial $A + C$ is obtained before deleting binomial $A + B$), then it is obvious, that $B + C$ is devisable by ideal I binomials. That is why we obtain three comparisons $A + B + C \equiv A \equiv B \equiv C \pmod{I}$. Which of the three options (or all) reduction modulo I it is better to keep in the basis of the main ideal can be chosen on account of the further steps.

A similar argument is true for trinomials. This reduction can be parallelized or executed by computing hardware.

In fact, instead of polynomials defining ideal A, we consider functions on the variety $V(I)$. Consequently, the found basis will be determined to an accuracy of ideal I basis. To obtain the exact solution after finding a basis in the ring of residue classes modulo I we must attach ideal I basis to the main ideal and then continue the computation of the Groebner basis.

Another option for the solution of the system of Boolean equations is calculation of Groebner basis directly for auxiliary ideal I. Occurring errors could be corrected by a statistical set for the different pairs of plaintext − ciphertext, by analogy with the linear and differential cryptanalysis methods. If the error probability $p = \dfrac{\#V(J) - \#V(I)}{\#V(J)}$ is small and there are m substitutions at encryption input, then the required number of plaintexts and ciphertexts equals $(1 - p)^{-m}$. For example, for $m = 160$ and $p = 0.9$ it is required 2.10^7 texts.

Thus, in the computation of the Groebner bases, high degree terms will be abrogated with higher probability comparing to the small degree terms. If we assume that the monomials in the polynomial are distributed with equal probability, in the result of a polynomial reduction modulo I a higher probability is to keep small degree terms, and reduce high degree terms. As a result of reduction modulo I, the uniformity of the initial monomial distribution is broken. Here we have an analogy with the sieve method, where a random number has small prime divisors with a higher probability than large prime divisors (the analogue of small prime divisors is small degree monomials). The complexity of the sieve method is subexponential. Therefore, we can assume, that the complexity of the proposed algorithm would be subexponential with a corresponding increase in the amount of memory (assuming that the reduction polynomial modulo I would perform quicker than syzygy computation, which is not obvious if the elements of the ideal I basis have a length of 4 or more terms).

Obviously, the longer the polynomials defining the basis of the ideal I, the harder it is to perform reduction modulo I, but at the same time it reduces the probability of error (number of repetitions is reduced). Thus, there is an optimal

length of an auxiliary ideal I basis when the complexity of computing the Groebner basis is minimal.

We can define a requirement for the substitution selection: an ideal, defining the substitution, must not have good binomial or trinomial approximation in the class of affine equivalent ideals.

7. Examples on preparation of ideal substitution

1. Substitution S = {00, 1d, 2b, 38, 43, 56, 64, 71, 8f, 92, a5, be, ca, dc, e9, f7}. Here the first byte tetrad corresponds to the input, the second tetrad corresponds to the substitution output.

This substitution has the best cryptographic properties: differentials probability $\leqslant$0.25, the absolute predominance of linear sums $\leqslant$0.25. The ideal substitution is defined by trinomials and quadrinomials with probabilities (assuming that the approximate ideal is divisible by substituting ideal) 0.46 and 0.59 respectively.

The principal ideal substitution is defined by a polynomial of length 161. Minimizing the length of a principal ideal by affinity equivalence results in ideal with a variety {6a, 6c, 6d, 7b, 9e, b7, bd, be, d6, d7, df, e3, e6, ec, f7, fa} (first tetrad corresponds to variables $\mathbf{x}$, second tetrad corresponds to variables $\mathbf{y}$), ideal length is 17: $1 + x_2x_3y_1y_2 + x_2x_3x_4y_1y_2 + x_2x_3y_1y_3 + x_1x_2x_3y_1y_3 + x_2x_3x_4y_1y_3 + x_1x_2x_3y_2y_3 + x_1x_2x_4y_2y_3 + x_1x_4y_1y_2y_3 + x_1x_2x_3y_1y_2y_4 + x_1x_3x_4y_1y_2y_4 + x_1x_2x_3y_3y_4 + x_1x_2x_3x_4y_3y_4 + x_2x_3y_1y_3y_4 + x_1x_3x_4y_2y_3y_4 + x_2x_3y_1y_2y_3y_4 + x_1x_4y_1y_2y_3y_4$. This ideal is defined by trinomials and quadrinomials with probabilities of 0.40 and 0.84 respectively.

2. Substitution S = {09, 14, 2a, 3b, 4d, 51, 68, 75, 86, 92, a0, b3, cc, de, ef, f7} of cipher SAES (short AES, simplified version of American Encryption Standard [17]). Here, the first byte tetrad corresponds to the input, the second tetrad corresponds to the substitution output.

This substitution also has the best cryptographic properties: differentials probability $\leqslant$0.25, the absolute predominance of linear sums $\leqslant$0.25. Ideal substitution is defined by trinomials and quadrinomials with probabilities (assuming that the approximate ideal is divisible by substituting ideal) 0.52 and 0.53 respectively.

The principal ideal substitution is defined by a polynomial of length 107. Minimizing the length of a principal ideal by affinity equivalence results in an ideal with a variety {1f, 5f, 6d, 6f, 9f, af, b9, ba, be, d3, d6, db, ed, f2, f3, fd} (first tetrad corresponds to variables $\mathbf{x}$, second tetrad corresponds to variables $\mathbf{y}$), ideal length is 15: $1 + x_1x_2x_3x_4y_3 + x_1x_3x_4y_1y_3 + x_1x_2x_4y_2y_3 + x_1x_2x_4y_1y_2y_3 + x_1x_3x_4y_1y_4 + x_1x_2x_3x_4y_1y_4 + x_2x_3y_1y_2y_4 + x_1x_3x_4y_1y_2y_4 + x_2x_3x_4y_1y_2y_4 + x_1x_2x_4y_3y_4 + x_1x_2x_3x_4y_3y_4 + x_1x_3y_1y_2y_3y_4 + x_4y_1y_2y_3y_4 + x_3x_4y_1y_2y_3y_4$. This ideal is defined by trinomials and quadrinomials with probabilities of 0.76 and 0.89 respectively. Here we see that the substitution SAES is worse than the substitution of the first example.

In both examples, when searching a reversible affine change of variables the task is to minimize the length of the principal ideal that defines substitution.

References

[1] G.-C. Faugere. A new efficient algorithm for computing Groebner basis (F4). Journal of Pure and Applied Algebra. **139**, 61–88, (1999).

[2] N. Courtois, A. Klimov, J. Patarin, A. Shamir. Efficient algorithms for solving overdefined systems of multivariate polynomial equations. In: *EUROCRYPT 2000*. LNCS, vol. 1807. (Springer-Verlag, 2000). Pp. 392-407.

[3] X. Tang and Y. Feng. A New Efficient Algorithm for Solving Systems of Multivariate

Polynomial Equations. Cryptology e-print archive, report 2006/475, 2006. Available at http://e-print.iacr.org/2006/475.

[4] X.-S. Gao, Z. Huang. Efficient Characteristic Set Algorithms for Equation Solving in Finite Fields and Application in Analysis of Stream Ciphers. Cryptology e-print archive, report 2009/637, 2000. Available at http://e-print.iacr.org/2009/637.

[5] H. Raddum and I. Semaev. New technique for solving sparse equation systems. Cryptology e-print archive, report 2006/475, 2006. Available at http://e-print.iacr.org/2006/475.

[6] M. Albrecht, C. Cid. Algebraic techniques in differential cryptanalysis. Cryptology e-print archive, report 2008/177, 2008. Available at http://e-print.iacr.org/2008/177.

[7] E. Biham, A. Shamir. Differential cryptanalysis of DES-like cryptosystems. In: *Advances in Cryptology – CRYPTO '90.* LNCS, vol. 537. (Springer-Verlag, 1991). Pp. 2–21.

[8] M. Matsui. Linear cryptanalysis method for DES cipher. In: *Advances in Cryptology – EUROCRYPT '93.* LNCS, vol. 765. (Springer-Verlag, 1994). Pp. 386–397.

[9] A. Rostovtsev. Changing probabilities of differentials and linear sums via isomorphism of ciphers. Cryptology e-print archive, report 2009/117, 2009. Available at http://e-print.iacr.org/2009/117.

[10] A.G. Rostovtsev. Changing probabilities of differentials and linear sums with virtual isomorphism. Information security problems. Computer Systems. No. 3, 71-77 (2009).

[11] M. Atiyah, L. Macdonald. *Introduction to commutative algebra.* (Addison-Wesley, 1969).

[12] I.R. Shafarevich. *The fundamentals of algebraic geometry.* Vol. 2. (Nauka, Moscow, 1988).

[13] D.Cox, J.Little, O'Shea D. *Ideals, Varieties and Algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra.* (Mir, Moscow, 2000).

[14] H. Heyes, S. Tavares. Substitution–permutation networks resistant to differential and linear cryptanalysis. Journal of cryptology. **9**, 1-19 (1996).

[15] A. Biryukov, C. De Canniere, A. Braeken, B. Preneel. A toolbox for cryptanalysis: linear and affine equivalence algorithms. In: *Advances in Cryptology – EUROCRYPT 2003.* LNCS, vol. 2556. (Springer–Verlag, 2003). Pp. 33-50.

[16] M.I. Kargopolov, Y.I. Merzlyakov. *Fundamentals of group theory.* (Nauka, Moscow, 1982).

[17] M. Musa, E. F. Schaefer, S. Wedig. A Simplified AES Algorithm and its Linear and Differential Cryptanalysis, Cryptologia. **27**, 148-177 (2003).