UDC 003.26

On desynchronised multivariate algorithms of El Gamal type for stable semigroups of affine Cremona group

Vasyl Ustimenko[1]

[1]*Institute of Mathematics, Maria Curie-Sklodowska University, Lublin*
Institute of Telecommunications and Global information Space of the NAS of Ukraine, Kyiv

Abstract

Families of stable cyclic groups of nonlinear polynomial transformations of affine spaces K^n over general commutative ring K of increasing with n order can be used in the key exchange protocols and related to them El Gamal multivariate cryptosystems. To use high degree of noncommutativity of affine Cremona group correspondents have to modify multivariate El Gamal algorithm via the usage of conjugations for two polynomials of kind g^k and g^{-1} given by key holder (Alice) or giving them as elements of different transformation groups. The idea of hidden tame homomorphism and comlexity of decomposition of polynomial transwormation into word of elements of Cremona semigroup can be used. We suggest usage of new explicit constructions of infinite families of large stable subsemigroups of affine Cremona group of bounded degree as instruments of multivariate key exchange protocols. Recent results on generation of families of stable transformations of small degree and density via technique of symbolic walks on algebraic graphs are observed. Some of them used for the implementation of schemes as above with feasible computational complexity. We consider an example of a new implemented quadratic multivariate cryptosystem based on the above mentioned ideas.

Keywords: Multivariate Cryptography, stable transformations, modified multivariate El Gamal algorithm, desyncronisation diagram, tame homomorphism

1. Introduction

Post Quantum Cryptography (PQC) serves for the creation and investigation of asymmetrical cryptographical algorithms which can be potentially resistant against attacks based on the use of quantum computer. Multivariate cryptography is one of the oldest directions of PQC.

It uses as security tools a nonlinear polynomial transformations f of kind: $x_1 \to f_1(x_1, x_2, \dots, x_n)$, $x_2 \to f_2(x_1, x_2, \dots, x_n)$, $\dots$, $x_n \to f_n(x_1, x_2, \dots, x_n)$ acting on the affine space K^n over finite commutative ring K, where $f_i \in K[x_1, x_2, \dots, x_n]$, $i = 1, 2, \dots, n$ are multivariate polynomials given in a standard form, i. e. via a list of monomials in a chosen order (see [1], [2], [3]).

This direction started with attempts to build a secure public keys in this form. It means the key holder Alice has some initial data D which allows her to solve the equation $f(\mathrm{x}) = \mathrm{b}$, where b and x are known and unknown elements of the free module K^n, but a public user Bob has only f given publicly in its standard form. Asymmetry means that Alice has tools for the encryption and decryption but Bob has only encryption procedure.

Public knowledge on $f = f_n$ allows adversary to create as many pairs of kind plaintext p - ciphertext $\mathrm{c} = f(\mathrm{p})$ as he/she wants. It makes the problem of practical design of such a cryptosystem a difficult task. First examples were based on families of quadratical bijective transformation f_n (see [1], [2], [3]), such choice implies rather fast encryption process.

Various attempts to build secure multivariate public key were unsuccessful, but the research of the development of new candidates for secure multivariate public keys is going on (see for instance [4] and further references).

One of the first usage of non bijective map of multivariate cryptography was in *oil and vinegar* cryptosystem analysed in [5], [6]. Nowadays this general idea is strongly supported by publication [7] devoted to security analysis of direct attacks on modified unbalanced oil and vinegar systems. It looks like such systems and rainbow signatures schemes may lead to promising Public Key Schemes of Multivariate Encryption defined over finite fields.

The observation of the further research on non bijective multivariate cryptography a reader can find in [8] (proceedings of the International Conference DIMA 2015 in Belarus), where the new cryptosystems with non bijective multivariate encryption maps on the affine space ${Z_m}^n$ into itself was presented together with some results concerning construction of bijective stable transformations of large order of finite vector spaces. The technique of [13] is based on the usage of the embeddings of projective geometries into corresponding Lie algebra (see [9] and further references). Some other new cryptosystems based on maps generated by symbolic walks on algebraic grapha reader can find in [10], [11]. [12], [13].

The paper is devoted to other aspects of Multivariate cryptography. Everybody knows that Diffie Hellman key exchange protocol can be formally considered in general case of any finite group or semigroup G. in

case of group corresponding scheme of El Gamal cryptosystem can be investigated. Notice that security of this algorithm depends not only on abstract group G but on the way of its generation in computer memory. for instance if $G = Z^*p$ is multiplicative group of large prime field then discrete logarithm problem (DLP) is difficult one and guarantee the security of the protocol, if same abstract group is given as additive group of Z_{p-1} protocol is insecure because DLP will be given by linear equation. If G is noncommutative group correspondents can use conjugations of elements involved in prototol, some algorithms of this kind were suggested in [14], [15], [16], [17], where group G is given with usage generators and relations. Security of such algorithms is connected with Conjugacy Search Problem (CSP) and Power Conjugacy Search Problem (PCSP), which combine CSP ? and Discrete Logarithm Problem and their generalisations.

In papers [18], [19] we consider some modifications of Diffie Hellman protocol when G is given as subgroup of affine Cremona semigroup $S(K^n)$ over finite commutative ring K of all polynomial transformations. It means that each element is given in its standard form. To use semigroup operation one has to compute the composition of transformations. We assume that encryption of corresponding El Gamal cryptosystem is conducted by application of some transformation $F \in S(K^n)$ to plaintext $(p_1, p_2, \dots, p_n)$ from K^n. At first glance the idea of such Diffie Hellman protocol in affine Cremona semigroup looks as unrealistic one because of composition of two maps of degree r and s taken in "general position " will be a transformation of degree rs. So in majority of cases $\deg(F) = d$, $d \geq 1$ implies the exponential grows of function $d(r) = \deg(F^r)$. To guarantee the polynomiality of algorithm the assumption of stability of involved transformations can be used , i. e. degrees of elements from cyclic group generated by chosen element have to be bounded by independent constant. It is a motivation of the search for stable subgroups and semigroups of affine Cremona groups.

During last years several large stable subgroups were discovered. These results on the explicit constructions are observed in reprint [18] of IACR e-crypt Arxive and paper [19] together with examples of their usage in cryptographical algorithms. They use general technique of generation of walks in algebraic graphs defined via equations over finite commutative ring.

The idea of desynchronisation over diagram is used to modify El Gamal algorithm where conjugates of g^k and g^{-1} are elements of different factor groups is also presented there together with some illustrating examples. Examples of its realisation with large families of quadratic and cubic stable transformations are given in [18].

In current paper we going further in this direction. We present new protocols which are not generalisations of Diffie Hellman algorithm, their security rests on the decomposition of element of large subsemigroup of affine Cremona semigroup into composition of given generators. We keep requirement that all transformations are given in their standard forms.

In section 2 basic definitions are given and concept of tame transformation which is a generalisation of stamle maps is discusses

In section 3 for convenience of reader we present new general schemes of cryptographical protocols of [20] with the usage of a concept of a tame homomorphism of stable semigroups of affine transformations (homomorphic map which is computable in polynomial time). The idea to exploit the complexity of *word* problem for Cremona semigroup about the decomposition of a given polynomial transformation g from the semigroup into given generators is presented in this section.

Multivariate nature of collision maps allows to use these algorithms for safe exchange of multivariate transformations. Various *deformation rules* can be used for this purpose (see section 4). Correspondents may use a family of invertible generators g_n. Assume that one of them can generate inverse of g_n. Then the symbolic El Gamal type *tahoma* algorithms can be used by correspondents They can use *inverse protocol* to elaborate pairs of mutually invertible transformations. So they can conduct information exchange protected via complexity of some difficult problem. Group enveloped symbolic Diffie Hellman algorithm (DHA) given in [18] with the example of implementation of corresponding El Gamal cryptosystem. This implementation is described in section 6 in terms of symbolic chains semigroup $Ch(n, K)$ of sequences of polynomial transformations of free module K^n and its special homomorphisms onto quadratic stable subgroups of affine Cremona semigroups. Such a description motivates complexity estimates of computations by each correspondent. Section 5 presents the idea of inverse group enveloped DHA. Paper [20] is devoted to implementation of algorithm of section 3 via symbolic walks on graphs A(n, K) (see [+17+5], [!7+6]) generating cubic maps. In section presents 6 implementations of inverse protocol of section 3 in terms of homomorphisms of $Ch(n, K)$ and its quotients. New families of stable subsemigroups of Cremona group are defined there.

2. Tame families and concept of stability

Let us consider basic algebraic objects of multivariate cryptography, which are important for the choice of appropriate pairs of maps f, f^{-1} in both cases of public key approach or idea of asymmetric algorithms with protected encryption rules.

Let us consider the totality $SF_n(K)$ of all rules f of kind

$x_1 \to f_1(x_1, x_2, \dots, x_n)$, $x_2 \to f_2(x_1, x_2, \dots, x_n)$, ... , $x_n \to f_n(x_1, x_2, \dots, x_n)$,

for given parameter n and chosen commutative ring K with natural operation of composition. We refer to this semigroup as semigroup of formal transformation $SF_n(K)$ of free module K^n. In fact it is a totality of all endomorphisms of ring $K[x_1, x_2, \dots, x_n]$ with the operations of their superposition.

Each rule f from $SF_n(K)$ induces transformation $\tilde{f}$ which sends tuple $(p_1, p_2, \dots, p_n)$ into $(f_1(p_1, p_2, \dots, p_n), \quad f_2(p_1, p_2, \dots, p_n), \quad \dots,$

$f_n(p_1, p_2, \dots, p_n))$. Affine Cremona semigroup $C(K^n)$ is a totality of all transformations of kind $\tilde{f}$. The canonical homomorphism $\gamma : f \to \tilde{f}$ maps infinite semigroup $SF_n(K)$ onto finite semigroup $S(K^n)$ in the case of finite commutative ring K.

We refer to pair (f, f') of elements $SF_n(K)$ such that ff' and $f'f$ are two copies of identical rule $x_i \to x_i$, $i = 1, 2, \dots, n$ as pair of invertible elements. If (f, f') is such a pair, then product $\tilde{f}\tilde{f'}$ is an identity map. Let us consider the subgroup $CF_n(K)$ of all invertible elements of $SF_n(K)$ (group of formal maps). It means $f \in CF_n(K)$ if and only if there is f' such that ff' and $f'f$ are identity maps. It is clear that the image of a restriction of γ on $CF_n(K)$ is affine Cremona group $C_n(K)$ of all transformations of K^n onto K^n for which there exists a polynomial inverse. We say that a family of subsemigroups S_n of $SF_n(K)$ (or $S(K^n)$) is stable of degree d if maximal degree of elements from S_n is an independent constant d, $d > 2$. If K is a finite commutative ring then stable semigroup has to be a finite set. The brief observation of known families of stable groups can be found in [20] (see also [23], [24], [25], [26], [27]).

Let $f_n \in SF_n(K)$ be a family of nonlinear maps of degree bounded by constant d. We say that f_n form tame family if there is a family $g_n \in SF_n(K)$ of degree bounded by constant d' such that $f_n g_n = g_n f_n$ are identity maps. Let τ_1 and τ_2 be two elements from the group $AGL_n(K)$ of all affine bijective transformations, i. e. elements of affine Cremona group of degree 1. Then we refer to $f'_n = \tau_1 f_n \tau_2$ as linear deformation of f_n. Obviously f'_n is also tame family of transformations, degrees of maps from this family is also bounded by d. The degrees of inverses of f'_n are bounded by d'.

Let $G_n < FS_n(K)$ be a stable family of subgroups of degree d, $d \geq 2$, then nonlinear representatives f_n of G_n form tame family of maps.

3. On the concept of tame homomorphism and related algorithms

Let $G = G_n$ be a family of stable subsemigroups of $SF_n(K)$ (or $S(K^n)$) and $L = L_m$, where m depends on n, be a family of stable subsemigroups of $SF_m(R)$ (or $S(R^m)$), where K and R are commutative rings. There are tame homomorphism $\varphi = \varphi_n$ from G into L, i. e. value of φ in each point $g \in G_n$ is computable in polynomial time from n. Let us assume, that there are semigroups $B = B_n < G_n$ given by its generators $b_1, b_2, \dots, b_r$. Let us assume that Alice has families of tame transformations π_1 of K^n and π_2 of R^m. We assume that these data is known to Alice. She forms $(a_i = \pi_1 b_i {\pi_1}^{-1}, a'_i = \pi_2 \varphi(b_i) {\pi_2}^{-1})$, $i = 1, 2, \dots, r$ and sends them to Bob.

The elements of these pairs are given in their standard forms from $SF_n(K)$ or $SF_m(R)$.

PROTOCOL. The list of pairs known for Bob defines homomorphism Δ between $A =< a_1, a_2, \dots, a_r >$ and $A =< a'_1, a'_2, \dots, a'_r >$ given by its values on generators.

Bob forms a via his choice of word ${a_{i_1}}^{k_1} {a_{i_2}}^{k_2} \dots {a_{i_t}}^{k_t}$ in the alphabet of generators of A such that $a_{i_s} \neq a_{i_{s+1}}$ for $s = 1, 2, \dots, t-1$. He sends $a = {a_{i_1}}^{k_1} {a_{i_2}}^{k_2} \dots {a_{i_t}}^{k_t}$ to Alice and keeps $\Delta(a) = a' = {a'_{i_1}}^{k_1} {a'_{i_2}}^{k_2} \dots {a'_{i_t}}^{k_t}$ as collision element.

Alice knows tame homomorphism φ and easily computes a' as $\pi_2 \varphi({\pi_1}^{-1} a \pi_1) {\pi_2}^{-1}$.

COMPLEXITY REMARK. Adversary has to solve *word problem* for subsemigroup A, i. e. find decomposition of aA into generators a_i, $i = 1, 2, \dots, t$. General algorithm to solve this problem in polynomial time in variable n is unknown as well as a procedure to get its solution in terms of quantum computations.

REMARK 1. The condition of stability for semigroups G and L and the usage of tame transformations π_1 and π_2 allow us to estimate degrees of a and collision map.

If maximal degrees of $\pi_1(n)$ and ${\pi_1}^{-1}(n)$ are l_1 and l'_1, degrees of $\pi_1(n)$ and ${\pi_1}^{-1}(n)$ are bounded by l_2 and l'_2 and stable groups G and L are of degrees d and d' then degrees of a and $\Delta(a)$ are bounded by $l_1 l'_1 d$ and $s_1 s'_1 d'$.

REMARK 2. One can use other natural conditions on π_1 and π_2. Let us assume that $G < G_1$ and $L < G_2$, where G_i are stable families of subsemigroups of degree t_1, $t_1 \geq d$ and t_2, $t_2 \geq d'$ respectively. Let us consider normalisers N_1 and N_2 of G_1 and G_2 in affine Cremona semigroups $S(K^n)$ and $S(R^m)$. it means that $N_1 = \{\pi \in C(K^n) | \pi G_1 \pi^{-1} < G_1\}$ and $N_2 = \{\pi \in C(R^m) | \pi G_2 \pi^{-1} < G_2\}$. We can take π_1 of kind $\tau_1 n_1$ and π_2 of kind $\tau_2 n_2$, where $n_i \in N_i$, $i = 1, 2$, $\tau_1 \in AGL_n(K)$ and $\tau_2 \in AGL_m(R)$. Then degrees of a and $\Delta(a)$ are restricted by t_1 and t_2.

Notice that in the case $G = G_1$, $L = G_2$ degrees of a and $\Delta(a)$ are bounded by d and d'.

We refer to presented above algorithm as *tahoma word protocol*. Termin *tahoma* (name of shrift for word processing) stands for combination *tame homomorphism*.

The protocol exploits the complexity of the *world problem* for a semigroup of polynomial transformation of free module.

In the case considered in REMARK 2 we use termin *stable tahoma word protocol*.

INVERSE TAHOMA WORD PROTOCOL.

Let us modify above PROTOCOL in the case of invertible elements $\varphi(b_i)$ with an assumption that $\varphi(b_i)^{-1}$ are known to Alice.

Instead of pairs (a_i, a'_i) Alice forms $(a_i, \tilde{a}_i)$, where $\tilde{a}_i = {a'_i}^{-1}$, $i = 1, 2, \dots, r$. Assume

Bob gets from Alice the list of such pairs. Notice that A' is a group $< \tilde{a}_i | i = 1, 2, \dots, r >$. So Bob is able to compute antisomorphism σ sending z from A into $\Delta(b)^{-1}$ because he knows its values on generators $\tilde{a}_i$.

Like in previous protocol Bob forms a via his choice of word ${a_{i_1}}^{k_1} {a_{i_2}}^{k_2} \dots {a_{i_t}}^{k_t}$ in the alphabet of generators of A such that $a_{i_s} \neq a_{i_{s+1}}$ for $s = 1, 2, \dots, t-1$ and sends $a = {a_{i_1}}^{k_1} {a_{i_2}}^{k_2} \dots {a_{i_t}}^{k_t}$ to Alice.

Now he keeps $\sigma(a) = a' = \tilde{a}_{i_t}^{k_t} \tilde{a}_{i_{t-1}}^{k_{t-1}} \dots \tilde{a}_{i_1}^{k_1}$ as collision element.

Alice computes $e = {a'}^{-1}$ as $\pi_2 \varphi({\pi_1}^{-1} a \pi_1) {\pi_2}^{-1}$.

INVERSE TAHOMA WORD CRYPTOSYSTEM.

Both above protocols exploit the complexity of finding decomposition of a into product of given generating transformations.

Alice and Bob can communicate because of they have mutually inverse transformations e and a'. Alice writes her message p and sends e(p) to Bob, who decrypts via usage of a'. Bob can encrypt with a' and Alice decrypts with e.

REMARK. In the case when transformation $e = e_m$ of free module R^m form stable family of degree d' adversary has to intercept $O(m^{d'})$ messages and conduct costly linearisation attack to restore e and a'. So correspondents can safely exchange $O(m^{d'-1})$ messages. Notice that any moment Alice and Bob can start a new session of inverse tahoma word protocol.

Different usage of homomorphisms of subsemigroup of Cremona semigrouup in the cryptosystem was considered in [28], [29].

4. On safe exchange of symbolic transformations

The symbolic nature of collision map can be used for task that differs from exchange of keys. We refer to it as the usage of DH *deformed* symbolic rules.

Let Alice have a free module K^n over commutative ring K. She has a subset Ω of K^n and polynomial map $f : K^n \to K^n$ such the restriction of $f|\Omega$ is an injective map from Ω onto $f(\Omega) = \Gamma$. Additionally Alice has an algorithm to solve in polynomial time equation $f(\mathrm{x}) = \mathrm{b}$ with respect to unknown x from Ω and $\mathrm{b} \in \Gamma$.

Alice and Bob use *tahoma word protocol* or symbolic Diffie-Hellman protocol to elaborate the collision map g acting on K^n.

After this step Alice sends Ω and transformation $h = f + g$ to Bob.

Now Bob can get f as $h - g$. He writes plaintext $\mathrm{p} \in \Omega$ and sends ciphertext $\mathrm{c} = f(\mathrm{x})$. Alice uses her data for the decryption.

REMARK. Notice that new algorithm is still asymmetrical because Bob can encrypt but not decrypt. The encryption rule is known to trusted customer (Bob) but adversary has no access to it. In fact such access is protected by word problem in semigroup of transformations of K^N or discrete logarithm problem in corresponding affine Cremona semigroup.

OTHER DEFORMATIONS.

Alice and Bob agree (via open channel) on a *deformation rule* $D(f)$ for multivatiate rule f from affine Cremona semigroup. For example, it can be multiplication, i.e. f is the rule $x_i \to f_i$, $i = 1, 2, \ldots, n$, g is the rule $x_i \to g_i$, $i = 1, 2, \ldots, n$ and Alice sends tuple of polynomials $f_i g_i$, $i = 1, 2, \ldots, n$. Bob uses division to restore f.

Instead of addition deformation rule (sending of $x_i \to f_i(x_1, x_2, \ldots, x_n) + g_i(x_1, x_2, \ldots, x_n)$, $i = 1, 2, \ldots, n$) Alice can use deformation with adding an element $K[x_1, x_2, \ldots, x_n]^n$ obtained from g via the usage of s-time conducted derivation $\delta^{(s)}$, where $\delta = \mathrm{d}/\mathrm{d}x_1 + \mathrm{d}/\mathrm{d}x_2 + \cdots + \mathrm{d}/\mathrm{d}x_n$ (rule $x_i \to f_i(x_1, x_2, \ldots, x_n) + \delta^{(s)} g_i(x_1, x_2, \ldots, x_n)$, $i = 1, 2, \ldots, n$). The last deformation is interesting because in many cases we can achieve the equality of degrees for f and $D(f)$. It is easy to continue this list of possible deformation rules.

REMARK. Let us assume that $\Omega = K^n$. So $f = f_n$ is a bijection. Assume that degrees of nonlinear maps f_n are bounded by constant d. Let us assume that the adversary has option to intercept some pairs plaintext - ciphertext (leakage from Bob's data). In case of interseption of $O(n^d)$ adversary has chance for a successful linearisation attack and get the map f. For example if $d = 3$ then linearisation attack cost is $O(n^{10})$. After that adversary has to find the inverse function f^{-1} like in the case of multivariate public key. To prevent "transition to knowledge" of an encryption multivariate map Alice (or Bob) can arrange a new session with protocol and a transmission of new deformed encryption rule for which secret data for decryption is known.

REMARK. The technique of linearisation attacks on nonbijective maps or maps f_n of unbounded degree and low density is not developed yet.

5. On the inverse version of the group enveloped symbolic Diffie-Hellman key exchange protocol

Let $G = G_n$ be a family of stable subsemigroups of $SF_n(K)$ (or $S(K^n)$) and $L = L_m$, where m depends on n, be a family of stable subsemigroups of $SF_m(R)$ (or $S(R^m)$), where K and R are commutative rings. There are tame homomorphism $\varphi = \varphi_n$ from G into L, i. e. value of φ in each point $g \in G_n$ is computable in polynomial time from n. Let us assume, that there are subgroups $A = A_m < L_m$ and $B = B_n < G_n$ such that $\varphi(b)a = a\varphi(b)$ for all pairs $a \in A$, $b \in B$. Assume that two families of tame transformations $\pi = \pi(n)$ and $\mu = \mu(m)$ are chosen.

We assume that these data is known to Alice. She forms pairs $(c_i = \pi b_i \pi^{-1}$, ${c_i}^{-1} = \pi {b_i}^{-1} \pi^{-1}$ and $(d_i = \mu\varphi(b_i)\mu^{-1}, {d_i}^{-1} = \mu\varphi({b_i}^{-1})\mu^{-1})$, $i = 1, 2, \ldots, r$, where elements $b_i \in B_n$, there inverses and images are given in their standard forms from $SF_n(K)$ or $SF_m(R)$ and sends them to Bob. Let δ be a homomorphismm from $< c_1, c_2, \ldots, c_r >$ to $< d_1, d_2, \ldots, d_r >$ sending c_i to d_i.

We present briefly the protocol of symbolic computations introduced in [18] and define its inverse version. We refer to this protocols as *group enveloped Diffie-Hellman scheme* and *inversive group enveloped Diffie - Hellman scheme.*

PROTOCOL 1. Alice takes positive integer k_A, and a, a^{-1} from A_m and g' from the semigroup G. She computes $g_A = \mu\ (a\varphi(g')a^{-1}\ )\ \mu^{-1}$ and sends to Bob $g =' \pi^{-1}$ together with g_A.

Bob chooses positive integer k_B and element $c \in < c_1, c_2, \ldots, c_r >$ (via the choice of word in alphabet $\{c_1, c_2, \ldots, c_r\}$). He computes $g_B = c{g^{k_B}}c^{-1}$ in standard form of $SF_n(K)$ and sends it to Alice. Bob computes a map $\delta(c){g_A}^{k_B}\delta(c^{-1})$ because he knows the decomposition of c and c^{-1} into their generators and keeps it as the collision map.

Alice computes the collision map as $\mu a\varphi(\pi^{-1}{g_B}^{k_A}\pi)a^{-1}\mu^{-1}$.

REMARK. Adversary has to consider group $C' =< c_i | i = 1, 2, \dots, r >$ and solve GROUP ENVELOPED DISCRETE LOGARITHM PROBLEM, i. e. solve $yg^x y^{-1} = g_B$ where x is unknown integer parameter and $y \in C'$. Natural possibility is to solve decomposition problem of g_B into semigroup generators $c_1, c_2, \dots, c_r, g$ (*word problem* in affine Cremona semigroup).

INVERSE PROTOCOL. Let us assume that Alice can generate g' such that $\varphi(g')$ is invertible and the inverse $\varphi(g')^{-1}$ is computable for her.

As in previous algorithm Alice takes positive integer k_A, and element a, a^{-1} from A_m and g' from the semigroup G. Now she computes $z = \varphi(g')^{-1}$ and $g_A = \mu a z a^{-1} \mu^{-1}$ and sends to Bob $g = \pi g' \pi^{-1}$ together with g_A.

As in previous algorithm Bob chooses positive integer k_B and element $c \in < c_1, c_2, \dots, c_r >$ (via the choice of word in alphabet $\{c_1, c_2, \dots, c_r\}$. He computes $g_B = c {g^{k_B}} c^{-1}$ in standard form of $SF_n(K)$ and sends it to Alice. Bob computes a map $e = \delta(c) {g_A}^{k_B} \delta(c^{-1})$ because he knows the decomposition of c and c^{-1} into their generators and keeps it as his a result of a collision.

Alice computes the map e^{-1} as $\mu a \varphi(\pi^{-1} {g_B}^{k_A} \pi) a^{-1} \mu^{-1}$.

INVERSE GROUP ENVELOBED DH CRYPTOSYSTEM.

Alice and Bob can communicate because of they have mutually inverse transformations e^{-1} and e.

1) Alice writes her message p and sends e^{-1}(p) to Bob, who decrypts via usage of e.

2) Bob can encrypt with e and Alice decrypts with e^{-1}.

The algorithm (2) was introduced in [18] as desynchronised symbolic El Gamal Algorithm.

6. Semigroup Ech(K, k), its special quotients and cryptographical applications

Let K be a commutative ring and $x_1, x_2, \dots, x_k$, $k \geq 2$ be the list of variables. We consider the totality Ch(K, k) of chains $(P^1, P^2, \dots, P^s)$ of length s, $s \geq O$ where $P^i \in K[x_1, x_2, \dots, x_k]^k$.

Each $F = (F_1, F_2, \dots, F_k) \in K[x_1, x_2, \dots, x_k]^k$ induces the map $\tilde{F}$ of K^k into K^k given by rule $x_i \to F_i(x_1, x_2, \dots, x_k)$, $i = 1, 2, \dots, k$.

The natural product of $\tilde{P}$ and $\tilde{Q}$ is the map $\tilde{F}$ for $F = (F_1, F_2, \dots, F_k) \in K[x_1, x_2, \dots, x_k]^k$ with $F_i = (Q_i(P_1(x_1, x_2, \dots, x_k), P_2(x_1, x_2, \dots, x_k), \dots, P_k(x_1, x_2, \dots, x_k))$ $i = 1, 2, \dots, k$. We simply write $P \times Q = F$.

We define chain composition of *symbolic chains* $(P^1, P^2, \dots, P^s)$ and $(Q^1, Q^2, \dots, Q^l)$ as a sequence $(P^1, P^2, \dots, P^s, P^s \times Q^1, P^s \times Q^2, \dots, P^s \times Q^l)$.

LEMMA 1.

Chain composition defines a semigroup Ch(K, k).

An empty chain is a unity of this infinite semigroup. We consider subsemigroup Ech(K, k) of chains of even length.

Let $S(K^n)$ be a Cremona semigroup of all transformation of free module K^n of kind $x_i \to F_i(x_1, x_2, \dots, x_n)$, $F_i \in K[x_1, x_2, \dots, x_n]$, $i = 1, 2, \dots, n$. In [Ustimenko, E-crypt] a special map μ from Ech(K, k) into $S(K^{(k+1)k})$ was defined in terms of algebraic graphs. The definition is following.

We define Double Schubert Graph $DS(k, K)$ over commutative ring K as incidence structure defined as disjoint union of points from

$PS = \{(\mathrm{x}) = (x_1, x_2, \dots, x_k, x_{1,1}, x_{1,2}, \dots x_{k,k}) | \in (\mathrm{x}) \in K^{(k+1)k}\}$ and lines from $LS = \{[\mathrm{y}] = [y_1, y_2, \dots, y_k, y_{1,1}, y_{1,2}, \dots y_{k,k}] | \in (\mathrm{y}) \in K^{(k+1)k}\}$ where (x) is incident to [y] if and only if $x_{i,j} - y_{i,j} = x_i y_j$ for $i = 1, 2, \dots, k$, $j = 1, 2, \dots, k$. It is convenient to assume that indexes of kind i, j are placed in lexicographical order.

REMARK. *The term* Double Schubert Graphs *is chosen because points and lines of $DS(k, F_q)$ can be treated as subspaces of ${F_q}^{2k+1}$ of dimensions $k+1$ and k which form two largest Schubert cells. Recall that the largest Schubert cell is the largest orbit of group of unitriangular matrices acting on the variety of subsets of given dimensions.* (see [8] and further references).

We define the colour of point (x) $= (x_1, x_2, \dots, x_k, x_{1,1}, x_{1,2}, \dots x_{k,k})$ from PS as tuple $(x_1, x_2, \dots, x_k)$ and the colour of line [y] $= [y_1, y_2, \dots, y_k, y_{1,1}, y_{1,2}, \dots y_{k,k}]$ as tuple $(y_1, y_2, \dots, y_k)$. For each vertex v of $DS(k, K)$ there is a unique neighbour N_α(v) of given colour $\alpha = (a_1, a_2, \dots, a_k)$, $a_i \in K$, $i = 1, 2, \dots, k$.

The symbolic colour G from $K[x_1, x_2, \dots, x_k]^k$ of kind $G_1(x_1, x_2, \dots, x_k)$, $G_2(x_1, x_2, \dots, z_k)$, $\dots$, $G_k(x_1, x_2, \dots, x_k)$, where G_i are polynomials from $K[x_1, x_2, \dots, x_k]$ defines the neighbouring line of symbolic point (x) $= (x_1, x_2, \dots, x_k, x_{1,1}, x_{1,2}, \dots x_{k,k})$ (coordinates are variables) with colour $(G_1(x_1, x_2, , \dots, x_k), G_2(x_1, x_2, \dots, x_k), \dots,$ $G_k(x_1, x_2, \dots, x_k))$ in the graph $DS(k, K[x_1, x_2, \dots, x_k])$. Similarly we define a neighbour if symbolic line.

Let us consider a tuple of symbolic colours $(G^1, G^2, \dots, G^{2t}) \in K[x_1, x_2, \dots, x_k]^k$ and the map F of PS to itself which sends the point (x) to the end v_{2t} of the chain v_0, v_1, $\dots$, v_{2t}, where (x) $= \mathrm{v}_0$, $\mathrm{v}_i I \mathrm{v}_{i+1}$, $i = 0, 1, \dots, 2t-1$ and $\rho(\mathrm{v}_j) = G^j(x_1, x_2, \dots, x_k)$, $j = 1, 2, \dots, 2t$. We refer to F as closed point to point computation with the symbolic key $(G^1, G^2, \dots, G^{2t})$. As it follows from definitions $F = F_{G^1, G^2, \dots, G^{2t}}$ is a multivariate map of $K^{k(k+1)}$ to itself. When symbolic key is given F can be computed in a standard form via elementary operations of addition subtraction and multiplication of the ring $K[x_1, x_2, \dots, x_k, x_{11}, x_{12}, \dots, x_{kk}]$. Recall that $(x_1, x_2, \dots, x_k, x_{11}, x_{12}, \dots, x_{kk})$ is our symbolic point of the graph.

Symbolic key $G = (G^1, G^2, \dots, G^{2t})$ is an element of semigroup $Ech(k, K)$. We define $\mu(G)$ as $F = F_{G^1, G^2, \dots, G^{2t}}$. The following statements are instant corollaries from the definition of homomorphism.

In fact the idea to use algebraic graphs with special colours (linguistic graphs) and walks of them in cryptography was proposed in [30]. Some of its applications reader can find in [31].

THEOREM 1

The map $\mu = \mu_k$ is a homomorphism of $Ech(k, K)$ into $S(K^{(k+1)k})$.

LEMMA 2

An element $\mu(C)$ for $C = (P^1, P^2, \dots, P^{2m})$ is a bijection iff the map $\tilde{P}^{2m}$ is one to one correspondence.

LEMMA 3

If F is the inverse map for $P^{\tilde{2m}}$ in $S(K^k)$ then for C' given by tuple $(F \times P^{2m-1}, F \times P^{2m-2}, \dots, F \times P^1, F)$ the transformation $\mu(C \times C')$ is an identity map.

We refer to C' as *reverse chain.*

Let $Ech'(k, K)$ be a totality of symbolic chains of kind $C = (P^1, P^2, \dots, P^{2t})$ where the degrees of polynomials from the tuple P^{2t} are equal 1, i. e. its affine map. We will use $P^0 = (x_1, x_2, \dots, x_k)$. Notice that $\deg(P^0) = \deg(P^{2t}) = 1$. Totality $Ech'(k, K)$ is a subsemigroup in $Ech(k, K)$

We define $\deg(C)$ as maximum of $\deg(P^0) + \deg(P^1)$, $\deg(P^1) + \deg(P^2)$, $\deg(P^2) + \deg(P^3)$, $\dots$, $\deg(P^{2t-1}) + \deg(P^{2t})$.

THEOREM 2

For each C from $Ech'(k, K)$ the equality $\deg(\mu(C)) = \deg(C)$ *holds.*

Proof

Let us assume that $C = (G^1, G^2, \dots, G^{2t})$ with $G^i = ({h_1}^i, {h_2}^i, \dots, {h_k}^i)$, $i = 1, 2, \dots, 2t$ is the symbolic key of the closed point to point computation $F = F(k)$ of the symbolic automaton $DS(k, K)$. We set that $g_0 = ({h_1}^0, {h_2}^0, \dots, {h_k}^0) = (x_1, x_2, \dots, x_k)$.

Then $F = \mu(C)$ is a transformation of kind

$x_1 \to {G_1}^{2t}(x_1, x_2, \dots, x_k)$, $x_2 \to {G_2}^{2t}(x_1, x_2, \dots, x_k)$, $\dots$, $x_k \to {G_k}^{2t}(x_1, x_2, \dots, x_k))$

$x_{11} \to x_{11} - {G_1}^1 x_1 + {G_1}^1 {G_1}^2 - {G_1}^3 {G_1}^2 + {h_1}^3 {G_1}^4 + \dots + {G_1}^{2t-1} {G_1}^{2t}$

$x_{12} \to x_{12} - {G_1}^1 x_2 + {G_1}^1 {G_2}^2 - {G_1}^3 {G_2}^2 + {G_1}^3 {G_1}^4 + \dots + {G_2}^{2t-1} {G_1}^{2t}$.

$\dots$

$x_{kk} \to x_{kk} - {G_k}^1 x_k + {G_k}^1 {G_k}^2 - {G_k}^3 {G_k}^2 + {G_k}^3 {G_k}^4 + \dots + {G_k}^{2t-1} {G_k}^{2t}$

The statement follows from the above written closed form of the map.

We consider the totality $Ech'(d)(k, K)$ of all chains from $Ech'(k, K)$ of degree $\le d$, $d \ge 2$. This subset is closed under the operation $\times$.

LEMMA 4.

Subsemigroup $S(d, k) = \mu(Ech'(d)(k, K))$ is a stable subsemigroup of $S(K^{k(k+1)})$ of degree d, i. e. the degree of each element of $S(d, k))$ is $\le d$.

This statement is a direct corollary from Theorem 2.

We implement algorithm of computation of elements from semigroup $S(d, k)$. And use this program in case of $S(2, k)$ and various comutative rings for the implementation of the key exchange protocols and cryptosystems of multivariate cryptography.

We consider subsemigroup $Ech'(d)(r, k, K)$, $1 \le r \le k$ of $Ech'(d)(k, K)$ consisting of chains of kind $(F^1, F^2, \dots, F^t)$ such that ${F^i}_j \in K[x_1, x_2, \dots, x_r]$ for $j = 1, 2, \dots, r$ and arbitrary i.

LEMMA 5.

There is a canonical homomorphism σ_r of $Ech'(d)(r, k, K)$ onto $Ech'(d)(r, K)$ sending $(F^1, F^2, \dots, F^t)$ into $(G^1, G^2, \dots, G^t)$, where G^i is a projection of F^i onto its first r coordinates.

LEMMA 6.

Let η be natural embedding of $Ech'(d)(r, k, K)$ into $Ech(d)(k, K)$. Then there is a homomorphism φ of $S(d, k)$ onto $S(d, r)$ such that $\varphi(mu_k(\eta(Ech'(d)(r, k, K))) = \mu_r(\sigma_r(Ech'(d)(r, k, K))$.

Let $e_1, e_2, \dots, e_k, e_{11}, e_{1,2}, \dots, e_{k,k}$ be natural basis in which graph $DS(k, K)$ is defined. For each symbolic walk G transformation $\mu(G)$ preserves affine space W spanned by $e_1, e_2, \dots, e_r$ and e_{ij}, $i = 1, 2, \dots, r$, $j = 1, 2, \dots, r$, The homomorphism $\varphi = \varphi_r$ is simply restriction of $\mu(G)$ onto W.

LEMMA 7.

Let degree of chain C from $Ech'(k, K)$ is d. Then $\mu(C)$ can be computed in time $O(k^{2+2d})$.

LEMMA 8.

Let d be the degree of chain C from $\mu(Ech'(r, k, K))$. Then the value of φ in point C can be computed in time of $O(k^{d+2})$.

IMPLEMENTED ALGORITHM.

Alice selects commutative ring K and parameters k and r and symbolic chain G of even length from $Ech'(2)(r, k, K)$ of kind $(G^1, G^2, \dots, G^t)$ such that $x_1 \to G^t{}_1$, $x_2 \to G^t{}_2$, $\dots$, $x_r \to G^t{}_r$ is an invertible linear map of increasing with r order $d(r)$ (one can take a Singer cycle of order $q^r - 1$ in case of $K = F_q$). So subsemigroup generated by g has cardinality $\ge d(r)$.

Alice takes invertible chains $C_1, C_2, \dots, C_m$ from $Ech'(2)(r, k, K)$ together with their reverse chains C'_j, $j = 1, 2, \dots, m$.

She takes invertible computations C in $Ech'(2)(k, K)$ and D in $Ech'(2)(r, K)$ together with their reverses C' and D'. Alice takes elements X, X^{-1} from $AGL_{k(k+1)}(K)$ and Y, Y^{-1} from $AGL_{r(r+1)}(K)$.

She computes pairs $a_i = Y\mu_r(D\sigma_r(C_i)D')Y^{-1}$, ${a_i}^{-1} = Y\mu_r(D\sigma_r(C'_i)D')Y^{-1}$ and

$b_i = X\mu_k(C(C_i)C')X^{-1}$, ${b_i}^{-1} = X\mu_k(C(C'_i)C')X^{-1}$.

Alice forms $u = X\mu_k(CGC')X^{-1}$ and $v = Y\mu_r(D\sigma_r(G')D')Y^{-1}$.

She takes integer $k_A > 0$ and starts correspondence with Bob. Alice sends $w = v^{k_A}$ to Bob together with pairs a_i, ${a_i}^{-1}$ and b_i , ${b_i}^{-1}$, $i = 1, 2, \dots, m$ and element u.

Bob takes integer parameters k_B and $r_{i_1}, r_{i_2}, \dots, r_{i_s}$.

He forms word b as ${a_{i_1}}^{r_{i_1}} {a_{i_2}}^{r_{i_2}} \dots {a_{i_s}}^{r_{i_s}} w^{k_B} {a_{i_s}}^{-r_{i_s}} {a_{i_{s-1}}}^{-r_{i_{s-1}}} \dots {a_{i_1}}^{-r_{i_1}}$.

Bob creates the plaintext p from $K^{r(r+1)}$. He sends ciphertext $c = b(p)$ together with

$z = {b_{i_1}}^{r_{i_1}} {b_{i_2}}^{b_{i_2}} \dots {b_{i_s}}^{r_{i_s}} u^{k_B} \ {b_{i_s}}^{-r_{i_s}} \ {b_{i_{s-1}}}^{-r_{i_{s-1}}} \dots {b_{i_1}}^{-r_{i_1}}$.

DECRYPTION. Alice computes $z_1 = \mu_k(C')X^{-1}zX\mu_k(C)$. She takes $z_2 = Y\mu_r(D)(\varphi(z_1)^k_A)\mu_r(D')Y^{-1}$ and gets p as $z_2(c)$.

REMARK. *Adversary has to find a decomposition of nonbijective transformation z into generators $b_1, b_2, \dots, b_m$ and u. He/she has find also an inverse*

for v. Knowledge about $i_1, i_2, \dots i_s$ and $r_{i_1}, r_{i_2}, \dots r_{i_s}$ and k_B allows he/she to form z.

Let us consider a complexity estimates in case of constant integers m, k_A, k_B, $r_{i_1}, r_{i_2}, \dots, r_{i_s}$, symbolic chains of constant length and multivariate polynomials of degree 1. We assume additionally that r is linear expression from k.

So Alice can generate chains $G, C_1, C_2, \dots, C_m$ and their images under σ_r in time $O(k^2)$. She is able to compute their reverses for $O(k^3)$. Really if $F = (F^1, F^2, \dots, F^t) \in Ech'(2)(k, K)$ and $\tilde{F^t}^{-1}$ is known map. To form F' Alice need $k-1$ matrix multiplications. It requires time $O(k^4)$. It is easy to see that computation of $\sigma_r(G')^{k_A}$ also requires $O(k^4)$ elementary operations.

Alice needs to compute images of μ for several elements of $Ech'(k, K)$ and $Ech'(r, K)$ of degree 2. It costs her $O(k^4)$ elementary operations. Additionally she computes composition of linear map and quadratic map of density $0(k^2)$ from $k(k+1)$ variables. Alice can do this in $O(k^8)$ in assumption then pairs X, X^{-1} and Y, Y^{-1} are already created. Finally Alice has compute a composition of quadratic and linear map in $k(k+1)$ variables. It also takes $O(k^8)$ operations. It means that Alice can prepare all data to start algorithm In time $O(k^8)$.

Let us estimate the complexity of computations for Bob.

He need to create two words of finite lengths in corresponding affine Cremona semigroup via several compositions of quadratic polynomials in $k(k+1)$ variables. It takes him $O(k^{14})$ elementary ring operations. Computation of quadratic map in given point of $K^{k(k+1)}$ takes time $O(k^6)$. Thus the total complexity of computations for Bob is $O(k^{14})$. Let us estimate the complexity of decryption proces for Alice. She need computation of product of linear and quadratic maps, product of two quadratic maps of densities k^2 and k^4, product of two quadratic maps of densities k^4 and k^2. It requires $O(k^{12})$ operations.

OTHER OPTIONS for implementation.

Alice can increase the length of chains or parameter k_A. For instance she can works with chains $C_1, C_2, \dots, C_m$, X and Y of length $O(k^d)$ and take k_A of cardinality $O(k^d)$. So she can generate inverse XC_iX' and $XC_i'X'$, $Y\sigma_r(C_i)Y'$ and $Y\sigma_r(C_i)'Y'$ in time $O(k^{d+3})$. For computation of $Y\sigma_r(G')^{k_A}Y'$ Alice need also $O(k^{d+3})$ operations. To compute values of μ she need time $O(k^{4+d})$. Notice that further steps of algorithms takes same time as before.

So in case of $d = 8$ Alice requires $O(k^{12})$ to set data for Bob and decrypt his message.

REMARK.*Plainspace is K^n with $n = k(k+1)$. So in above case Alice and Bob need time $O(n^6)$ and $O(n^7)$.*

7. Quotients of semigroup $\mathbf{Ch}(K, k)$, and inverse protocols

Let $C = (P^1, P^2, \dots, P^s)$ be a chain from $Ch'(2k, K)$, $\deg(P^s) = 1$. We divide variables into two groups $x_1, x_2, \dots, x_k$ and $(x_{k+1}, x_{k+2}, \dots, x_{2k})$ and brake each $P^i = (P^i{}_1, P^i{}_2, \dots, P^i{}_{2k})$ into $U^i = (P^i{}_1, P^i{}_2, \dots, P^i{}_k)$ and $W^i = (P^i{}_{k+1}, P^i{}_{k+2}, \dots, P^i{}_{2k})$. We assume that $\tilde{U^i}$ maps $(x_1, x_2, \dots, x_k)$ onto U^i and $\tilde{W^i}$ maps $(x_{k+1}, x_{k+2}, \dots, x_{2k})$ onto W^i. It is convenient to use pair (U^0, W^0) where $U^0 = (x_1, x_2, \dots, x_k)$ and $W^0 = (x_{k+1}, x_{k+2}, \dots, x_{2k})$.

We define $\deg'(C)$ as maximum of $\deg(U^0)$+$\deg(W^0)$, $\deg(W^0) + \deg(U^1)$, $\deg(U^1) + \deg(W^1)$, $\deg(W^1) + \deg(U^2)$, $\dots$, $\deg(W^{s-1}) + \deg(U^s)$.

Let us consider symbolic flag of incidence structure $DS(k, K)$ which consist of point $(\mathrm{x}) = (x_1, x_2, \dots, x_k, x_{1,1}, x_{1,2}, \dots x_{k,k})$ with colour $(x_1, x_2, \dots, x_k)$ and neighbouring line $[\mathrm{y}] = [y_1, y_2, \dots, y_k, y_{1,1}, y_{1,2}, \dots y_{k,k}]$ with colour $(y_1, y_2, \dots, y_k) = (x_{k+1}, x_{k+2}, \dots, x_{2k})$. We assume that information of the flag is given by

(x) and colour tuple $(y_1, y_2, \dots, y_k)$, other coordinates $y_{1,1}, y_{1,2}, \dots y_{k,k}$ of the line are recomputed as symbolic expressions from the incidence condition.

We assume that a pair (U^0, W^0) is a colour of the symbolic flag. We consider a symbolic chain in $DS(k, K[x_1, x_2, \dots, x_{2k}])$ of kind (x^i), $[\mathrm{y}]^i$, $i = 0, 1, \dots, s$ where $(\mathrm{x}^0) = (\mathrm{x})$ is starting point of the initial flag, $[\mathrm{y}]^0 = [\mathrm{y}]$ is a line of the flag, $[\mathrm{y}]^i I(\mathrm{x}^{i+1})$ for $i = 0, 1, \dots, s-1$ and $[\mathrm{y}]^i I(\mathrm{x})^i$ for $i = 0, 1, \dots, s$, symbolic colours of $(\mathrm{x})^i$ and $[\mathrm{y}]^i$ are $(U_1^i, U_2^i, \dots, U_k^i)$ and $(W_1^i, W_2^i, \dots, W_k^i)$ respectively. Let us consider a tuple of symbolic colours $(P^1, P^2, \dots, P^s) \in K[x_1, x_2, \dots, x_{2k}]^{2k}$ and the map F of the flag variety of $DS(k, K)$ to itself which sends the initial flag given by point (x) and colour of the neighbouring line to the last flag given by point $(\mathrm{x})^s$ and colour W^s of the last line in the chain. As it follows from definitions $F = F_{P^1, P^2, \dots, P^s}$ is a multivariate map of $K^{(k+1)^2}$ to itself. When symbolic chain C is given F can be computed in a standard form via elementary operations of addition subtraction and multiplication of the ring $K[x_1, x_2, \dots, x_{2k}, x_{11}, x_{12}, \dots, x_{kk}]$. From the explicit construction of the map F the following statements follows.

THEOREM 3

The map $\lambda = \lambda_k$ which sends $P^1, P^2, \dots, P^s$ to $F = F_{P^1, P^2, \dots, P^s}$ is a homomorphism of $Sch'(2k, K)$ into $S(K^{(k+1)^2})$.

THEOREM 4

$\deg(\lambda(C)) = \deg'(C)$ *for C from $Sch'(2k, K)$*

LEMMA 9

An element $\lambda(C)$ for $C = (P^1, P^2, \dots, P^s)$ is a bijection iff the map $\tilde{P^s}$ is one to one correspondence.

LEMMA 10

If F is the inverse map for $\tilde{P^s}$ in $S(K^{2k})$ then for C' given by tuple $(F \times P^{s-1}, F \times P^{s-2}, \dots, F \times P^1, F)$ the transformation $\lambda(C \times C')$ is an identity map.

We refer to C' as *reverse chain.*

We consider the totality $Sch'(d)(2k, K)$ of all chains from $Sch'(2k, K)$ of for which $\deg' \leq d$, $d \geq 2$. This subset is closed under the operation $\times$.

LEMMA 11.

Subsemigroup $Se(d,k) = \lambda(Sch'(d)(2k,K))$ is a stable subsemigroup of $S(K^{(k+1)^2})$ of degree d, i. e. the degree of each element of $Se(d,k))$ is $\leq d$. Let us consider totality $Sch'(d)(r,2k,K)$, $1 \leq r \leq k$ of chains $C = (P^1, P^2, \dots, P^s)$ from $Ch'(d)(2k,K)$ such that $U^i = (P^i{}_1, P^i{}_2, \dots, P^i{}_k)$ and $W^i = (P^i{}_{k+1}, P^i{}_{k+2}, \dots, P^i{}_{2k})$. are tuples of kind F^i such that $F^i{}_j \in K[x_1, x_2, \dots, x_r]$ for $j = 1, 2, \dots, r$ and arbitrary $i = 1, 2, \dots, s$.

LEMMA 12.

There is a canonical homomorphism δ_r of $Sch'(d)(r,2k,K)$ onto $Sch'(d)(r,K)$ sending $(F^1, F^2, \dots, F^t)$ into $(G^1, G^2, \dots, G^t)$, where G^i is a projection of F^i onto its first r coordinates.

LEMMA 13.

Let η be natural embedding of $Sch'(d)(r,2k,K)$ into $Sch(d)(2k,K)$. Then there is a homomorphism φ of $Se(d,k)$ onto $Se(d,r)$ such that $\varphi(\lambda_k(\eta(Ech'(d)(r,k,K))) = \lambda_r(\delta_r(Sch'(d)(r,2k,K))$.

Let $e_1, e_2, \dots, e_k, e_{k+1}, e_{k+2}, \dots, e_{2k}, e_{11}, e_{1,2}, \dots, e_{k,k}$ be natural basis in which flag variety of graph $DS(k,K)$ is presented. For each symbolic walk G transformation $\lambda(G)$ preserves affine space W spanned by $e_1, e_2, \dots, e_r, e_{k+1}, e_{k+2}, \dots, e_{k+r}$ and e_{ij}, $i = 1, 2, \dots, r$, $j = 1, 2, \dots, r$. The homomorphism $\varphi = \varphi_r$ is simply restriction of $\mu(G)$ onto W.

IMPLEMENTED INVERSE TAHOMA ALGORITHM.

Alice selects commutative ring K and parameters k and r.

Alice takes invertible chains $C_1, C_2, \dots, C_m$ from $Ch'(2)(r,k,K)$ such that $D_i = \delta_r(C_i)$ are inverible. She also takes reverse chains D'_j, $j = 1, 2, \dots, m$.

She takes invertible computations C in $Ch'(2)(k,K)$ and D in $Ch'(2)(r,K)$ together with their reverses C' and D'. Alice takes elements X, X^{-1} from $AGL_{k(k+1)}(K)$ and Y, Y^{-1} from $AGL_{r(r+1)}(K)$. She computes pairs of elements $a_i{}^{-1} = Y\lambda_r(D(D'_i)D')Y^{-1}$ and $b_i = X\lambda_k(C(C_i)C')X^{-1}$. Alice sends pairs $(a_i,\ b_i)$, to Bob.

Bob takes integer parameters $r_{i_1}, r_{i_2}, \dots, r_{i_s}$. He forms word a as $a_{i_1}{}^{r_{i_1}} a_{i_2}{}^{r_{i_2}} \dots a_{i_s}{}^{r_{i_s}}$ and keeps it. Bob creates $z = b_{i_s}{}^{r_{i_s}}\ b_{i_{s-1}}{}^{r_{i_{s-1}}} \dots b_{i_1}{}^{r_{i_1}}$ and sends it to Alice.

RESTORATION. Alice computes $z_1 = \mu_k(C')X^{-1}zX\mu_k(C)$. She takes $z_2 = Y\lambda_r(D)(\varphi(z_1))\lambda_r(D')Y^{-1}$.

It is easy to see that the complexity estimates are similar to case of El Gamal type algorithm from previous section. *CONCLUSION.*

Conclusion

Presented key exchange protocols and cryptosystems are based on graphs $DS(k,K)$, their properties depends on the choice of commutative ring K. Their security rest on the complexity of word decomposition problem for the element of Cremona semigroup $S(K^n)$ into given generators. Under assumption that the element and generators are given by their standard forms of multivariate map the polynomial algorithm to solve it is not known. As always search for appropriate cryptoanalysis is important. We hope that method will attract attention of specialists. Other practical task is evaluation of parameters for which resistance of algorithm will reach standard level of security (for example 128 or 256 bites) in case of commutative rings Z_{2^7}, Z_{2^8},$Z_{2^{16}}$, $Z_{2^{32}}$, F_{2^7}, F_{2^8},$F_{2^{16}}$, $F_{2^{32}}$,

This research is partially supported by the grant PIRSES-GA-2013-612669 of the 7th Framework Program of European Commission.

References

[1] J. Ding, J. E. Gower, D. S. Schmidt, *Multivariate Public Key Cryptosystems*. Springer, Advances in Information Security, V. 25, 2006.

[2] N. Koblitz, *Algebraic aspects of cryptography*, Springer (1998).

[3] Louis Goubin, Jacques Patarin, Bo-Yin Yang, *Multivariate Cryptography. Encyclopedia of Cryptography and Security*, (2nd Ed.) 2011, 824-828.

[4] Gilles Macario-Rat, Jacques Patarin, *Two-Face: New Public Key Multivariate Schemes*, AFRICACRYPT, 2018: 252-265

[5] J. Patarin, *The Oil i Vinegar digital signatures*, Dagstuhl Workshop on Cryptography. 1997.

[6] A. Kipnis, A. Shamir, *Cryptanalisis of the Oil and Vinegar Signature Scheme* Advances in Cryptology - Crypto 96, Lecture Notes in Computer Science, V. 1462, 1996, P. 257–266.

[7] S. Bulygin, A. Petzoldt and J. Buchmann, *Towards provable security of the unbalanced oil and vinegar signature scheme under direct attacks*, In Guang Gong and Kishan Chand Gupta, editors, "Progress in Cryptology - INDOCRYPT", Guang Gong and Kishan Chand Gupta, editors, Lecture notes in Computer Science, V. 6498, 2010. P. 17–32.

[8] V. Ustimenko, *On Shubert cells in grassmanians and new algorithm of multivariate cryptography*, Proceedings of Institute of Mathematics, Minsk, 2015, pp 137-148.

[9] V. Ustimenko, A. Woldar, *A geometric approach to orbital recognition in Chevalley-type coherent configurations and association schemes*, Australasian Journal of Combinatorics, Volume 67(2) (2017), Pages 166-202.

[10] V. Ustimenko, *On new multivariate cryptosystems with nonlinearity gap*, Algebra and Discrete Mathematics, Volume 23 (2017), Number 2, pp. 331–348.

[11] V. Ustimenko, *On new multivariate cryptosystems based on hidden Eulerian equations*, Reports of Nath Acad of Sci, Ukraine, 2017. ? 5, pp 17-24.

[12] V.A. Ustimenko, *On the flag geometry of simple group of Lie type and Multivariate Cryptography*, Algebra and Discrete Mathematics. V. 19. No 1. 2015. P. 130-144.

[13] V. Ustimenko, *On algebraic graph theory and non-bijective maps in cryptography*, Algebra and Discrete Mathematics, Volume 20 (2015). Number 1, pp. 152-170.

[14] Dmitriy N. Moldovyan, Nikolay A. Moldovyan *A New Hard Problem over Non-commutative Finite Groups for Cryptographic Protocols*, International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security , MMM-ACNS 2010: Computer Network Security pp 183-194.

[15] L. Sakalauskas, P. Tvarijonas, A. Raulynaitis *Key Agreement Protocol (KAP) Using Conjugacy and Discrete Logarithm Problema in Group Representation Level*, INFORMATICA, 2007, vol. !8, No 1, 115-124.

[16] V. Shpilrain, A. Ushakov, 2006), *The conjugacy search problem in public key cryptography: unnecessary and insufficient*,Applicable Algebra in Engineering, Communication and Computing, August 2006, Volume 17, Issue 3–4, pp 285–289

[17] Delaram Kahrobaei, Bilal Khan, *A non-commutative generalization of ElGamal key exchange using polycyclic groups*, In IEEE GLOBECOM 2006 - 2006 Global Telecommunications Conference [4150920] DOI: 10.1109/GLOCOM.2006.

[18] V. Ustimenko, *On desynchronised multivariate El Gamal algorithm*, Cryptology ePrint Archive, 712, 2017.

[19] V. Ustimenko, *On the families of stable transformations of large order ane their cryptographical applications*, Tatra Mt. Math. Publ., 70 (2017), 107-117.

[20] V. Ustimenko, *On new symbolic key exchange protocols and cryptosystems based on hidden tame homomorphism*, Reports of Nath Acad of Sci, Ukraine, 2018 (to appear).

[21] V. Ustimenko, U. Romanczuk, *On Dynamical Systems of Large Girth or Cycle Indicator and their applications to Multivariate Cryptography*, in "Artificial Intelligence, Evolutionary Computing and Metaheuristics ", In the footsteps of Alan Turing Series: Studies in Computational Intelligence, Vol. 427, Springer, January , 2013, 257-285.

[22] V. Ustimenko, *On extremal graph theory and symbolic computations*, Dopovidi National Academy of Sci, Ukraine, 2013, N2, pp 42-49.On extremal graph theory and symbolic computations, Dopovidi National Academy of Sci, Ukraine, 2013, N2, pp 42-49.

[23] V. Ustimenko, A. Wroblewska, *On the key exchange with nonlinear polynomial maps of stable degree*, Annalles UMCS Informatica AI XI, 2 (2011), 81-93.

[24] A. Wroblewska, *On some properties of graph based public keys*, Albanian Journal of Mathematics, Volume 2, Number 3, 2008, 229-234, NATO Advanced Studies Institute: "New challenges in digital communications".

[25] V. Ustimenko, A. Wroblewska,*Dynamical systems as the main instrument for the constructions of new quadratic families and their usage in cryptography*, Annales UMCS Informatica AI, ISSN 1732-1360, vol.12, N3 (2012), 65-74.

[26] V. Ustimenko, M. Klisowski, *Graph based cubical multivariate maps and their cryptographical applications*, in ''Advances on Superelliptic curves and their Applications", IOS Press, NATO Science for Peace and Security series –D: Information and Communication Security, vol 41, 2015 , pp. 305 -327.

[27] V. Ustimenko, A. Wroblewska, *On new examples of families of multivariate stable maps and their cryptographical applications.* Annales UMCS, Informatica, 14(1):19–35, 2014.

[28] Romańczuk-Polubiec U., Ustimenko V., *On two windows multivariate cryptosystem depending on random parameters*, Algebra and Discrete Mathematics, 2015, Vol. 19, No. 1., pp. 101–129.

[29] Romanczuk-Polubiec U., Ustimenko V. A, *On new key exchange multivariate protocols based on pseudorandom walks on incidence structures*, Dopovidi NAN Ukrainy, N1, 2015, pp 41-49.

[30] V. Ustimenko, *Maximality of affine group, hidden graph cryptosystem and graph's stream ciphers*, Journal of Algebra and Discrete Mathematics, 2005, v.1, pp 51-65.

[31] V. A. Ustimenko, *Explicit constructions of extremal graphs and new multivariate cryptosystems*, Studia Scientiarum Mathematicarum Hungarica, Special issue "Proceedings of The Central European Conference, 2014, Budapest", volume 52, issue, June 2015, pp. 185-204.