On Multivariate Algorithms of Digital Signatures on Secure El Gamal Type Mode.

V. Ustimenko

University of Maria Curie Sklodowska, Lublin 20036, Poland

vasyl@hektor.umcs.lublin.pl

Abstract. The intersection of Non-commutative and Multivariate cryptography contains studies of cryptographic applications of subsemigroups and subgroups of affine Cremona semigroups defined over finite commutative ring *K* with the unit. We consider special subsemigroups (platforms) in a semigroup of all endomorphisms of $K[x_1, x_2, \dots, x_n]$.

Efficiently computed homomorphisms between such platforms can be used in Post Quantum key exchange protocols when correspondents elaborate common transformation of $(K^*)^n$. The security of these schemes is based on a complexity of decomposition problem for an element of a semigroup into a product of given generators.

We suggest three such protocols (with a group and with two semigroups as platforms) for their usage with multivariate digital signatures systems. The usage of protocols allows to convert public maps of these systems into private mode, i.e. one correspondent uses the collision map for safe transfer of selected multivariate rule to his/her partner.

The ‘’ privatisation’’ of former publicly given map allows the usage of digital signature system for which some of cryptanalytic instruments were found (estimation of different attacks on rainbow oil and vinegar system, cryptanalytic studies LUOV) with the essentially smaller size of hashed messages. Transition of basic multivariate map to safe El Gamal type mode does not allow the usage of cryptanalytic algorithms for already broken Imai - Matsumoto cryptosystem or Original Oil and Vinegar signature schemes proposed by J.Patarin.

So even broken digital signatures schemes can be used in the combination with protocol execution during some restricted ‘’trust interval’’ of polynomial size.

Minimal trust interval can be chosen as a dimension *n* of the space of hashed messages, i. e. transported safely multivariate map has to be used at most *n* times. Before the end of this interval correspondents have to start the session of multivariate protocol with modified multivariate map.

The security of such algorithms rests not on properties of quadratic multivariate maps but on the security of the protocol for the map delivery and corresponding NP hard problem.

Keywords: Noncommutative Cryptography, Multivariate Cryptography, key exchange protocols, semigroups of transformations, decomposition problem, multivariate digital signature.

1. On Post Quantum, Multivariate and Noncommutative Crytography.

Post Quantum Cryptography (PQC) is an answer to a threat coming from a full-scale quantum computer able to execute Shor's algorithm. With this algorithm implemented on a quantum computer, currently used public key schemes, such as RSA and elliptic curve cryptosystems, are no longer secure. The U.S. NIST made a step toward mitigating the risk of quantum attacks by announcing the PQC standardisation process [1] for new public key algorithm. In March 2019 NIST published a list of candidates qualified to the second round of the standardisation process. Few public key candidates are implemented, like candidate called Round 5 (see [2]) or classic Mc Eliece algorithm (see [3]).

Current candidates are developed within following directions of PQC: lattice based systems, code based cryptosystems, multivariate cryptography (see [4] and further references), hash based Cryptography, studies of isogenies for superelliptic curves. There is the following alternative approach to public key cryptography. Instead of public encryption rule correspondents can use protocol for elaboration some common information which allows to
define encryption rule for one user and decryption instrument for his/her partner. We refer to such algorithms as cryptosystem of El Gamal type. Recall that El Gamal proposed such cryptosystem based on classical Diffie-Hellman algorithm over multiplicative group F^*_p.

In this publication we continue to develop new cryptosystems within alternative approach ([5], [6], [7], [8], [9]) to multivariate public key cryptography based on the idea of modified Diffie - Hellman type protocols in terms of Noncommutative cryptography for subsemigroups of endomorphisms of $K[x_1, x_2, \ldots, x_n]$. Security of these algorithms rests on the complexity of word problem to decompose given multivariate map into generators of affine Cremona semigroup $End(K[x_1, x_2, \ldots, x_n])$ (see [10] for the first application of word problem in the case of group*)*. Thus we are working in the area of intersection of Multivariate and Non-commutative cryptographies.

Recall that Multivariate Cryptography (see [4]) uses polynomial maps of affine space K^n defined over a finite commutative ring K into itself as encryption tools. It exploits the complexity of finding a solution of a system of nonlinear equations from many variables. Multivariate cryptography uses as encryption tools nonlinear polynomial transformations of kind $x_1 \to f_1(x_1, x_2, \ldots, x_n)$, $x_2 \to f_2(x_1, x_2, \ldots, x_n)$, … , $x_n \to f_n(x_1, x_2, \ldots, x_n)$ transforming affine space K^n, where $f_i \in K[x_1, x_2, \ldots, x_n]$, $i=1,2,\ldots,n$ are multivariate polynomials usually given in a standard form, i. e. via a list of monomials in a chosen order (nonlinear endomorphisms of $K[x_1, x_2, \ldots, x_n]$.

Non-commutative cryptography is an active area of cryptology where the cryptographic primitives and systems are based on algebraic structures like groups, semigroups and noncommutative rings (see [11]-[25]). It is important that this direction is well supported by Cryptanalytic research (see [26]-[29]) Semigroup based cryptography consists of general cryptographical schemes defined in terms of wide classes of semigroups and their implementations for chosen semigroup families (so called platform semigroups).

Papers [5] , [6], [7], [8] and [9] contain 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. These papers use the assumption that each element is given in its standard form of Multivariate Cryptography. To use semigroup operation one has to compute the composition of transformations. This was an attempt to combine methods of Non Commutative Cryptography and Multivariate Cryptography.

Paper [5] , [6] suggests some usage of homomorphisms of subsemigroups of affine Cremona groups for protocols and cryptosystems which are not generalisations of Diffie-Hellman algorithm and its El Gamal type modifications. Some examples are given there. The implementations of these schemes with evaluation of densities of involved polynomial transformations are described in [7], , [8] and [9] . Elements of graph based stable subgroups used in [7] can serve as encryption tools of stream ciphers (see [30] and further references).

2. On stable subgroups of formal Cremona group and privatisation of Multivariate Public Keys based on maps of bounded degree.

Let $K[x_1, x_2, \dots , x_n]$ be commutive ring of all polynomials in variables $x_1, x_2, \dots , x_n$ defined over a commutive ring K. Each endomorphism $F \in E_n(K)$ is uniquely determined by its values on formal generators x_1, $i=1,2,\dots, n$. Symbol $End(K[x_1, x_2, \dots , x_n])=E_n(K)$ stands for semigroup of all endomorphisms of $K[x_1, x_2, \dots , x_n]$. So we can identify F with the formal rule $x_1 \to f_1(x_1, x_2, \dots , x_n)$, $x_2 \to f_2(x_1, x_2, \dots , x_n)$, …, $x_n \to f_n (x_1, x_2, \dots , x_n)$ where $f_i \in K[x_1, x_2, \dots , x_n]$. Element F naturally induces the transformation $\Delta(F)$ of affine space K^n given by the following rule $\Delta(F):(\alpha_1, \alpha_2, \dots, \alpha_n) \to (f_1 (\alpha_1, \alpha_2, \dots, \alpha_n), f_2(\alpha_1, \alpha_2, \dots, \alpha_n), \dots, f_n(\alpha_1, \alpha_2, \dots, \alpha_n))$ for each $(\alpha_1, \alpha_2, \dots, \alpha_n) \in K^n$. Luigi Cremona [31] introduced $\Delta(E_n(K))= CS(K^n)$ which is currently called *affine Cremona semigroup*. A group of all invertible transformations of $CS(K^n)$ with an inverse from $CS(K^n)$ is known as *affine Cremona group* $CG(K^n)$ (shortly *Cremona group*, see for instance [32], [33]).

We refer to infinite $E_n(K)$ as *formal affine Cremona semigroup*. Density of the map F is the total number of monomial terms in all f_i.

It is a known fact that typically the degree of iteration of the "random" multivariate polynomial transformation grows exponentially. This is due to the fact that the composition of two '"random" elements of $CS(K^n)$ of degree d in majority cases will have a degree d^2 .

In particular, this can be seen in the one-dimensional case (i.e. for $n = 1$) the exponential growth of the degree of iterations of a nonlinear polynomial is unavoidable. However, it turns out that for $n > 1$ the degree of some special transformations may grow significantly slower. There are discovered examples of transformations with a degree that may grow polynomially (see [34],

[35]) or be even not greater than some established constant d . Last fact means the existence of stable subsemigroups/ subgroups of formal Cremona groups of degree d, i.e. subsemigroups of endomorphisms of degree at least d. First example of families of stable groups were introduced in [36], [37] in terms of well known extremal graphs $D(n, q)$ and their analogs $D(n,K)$ defined over arbitrary commutative ring K. However the importance of their stability were realised later [38], [39]. The formal prove of the fact that these groups are stable of degree 3 is presented in [40]. Obviously the semigroup of transformations of degree 1 and general affine group of bijective transformations of degree 1 are examples of stable subsemigroups and subgroups of $E_n(K)$ of degree 1. Currently nonlinear families of stable semigroups and groups are known for each parameter d ≥ 2, they have various applications to Cryptography (see [8], [9], [41] and further references). All these results are obtained via studies of "symbolic walks" on algebraic graphs, i.e. graphs defined by a system of algebraic equations.The following statement follows from the results of [8].

Theorem 1. *For each natural number $n>1$ and each commutative ring K and $d \geq 2$ there is a family of non-commutative stable subgroups $G_n(K) < E_n(K)$ of degree d and stable semigroups $S_n(K)<E_n(K)$ of degree d such that $G_n(K) <S_n(K)$.*

Let ${}^iZ= \{ {}^ig_1 , {}^ig_2, \dots , {}^ig_t\}$ be a sequence of sets of elements from $E_{n(i)}(K)$, where $n(i)>1$ is an increasing sequence of positive integers. We say that ${}^iZ$ is a *noncommutative system of stable Cremona generators of degree d* and rank t if

(1) $\Delta({}^ig_k{}^ig_j) \neq \Delta({}^ig_j{}^ig_k)$ for arbitrary $k \neq j$.

(2) ${}^iSZ= <{}^ig_1, {}^ig_2, \dots , {}^ig_t>$ are stable semigroups of degree d.

Proposition 1. *For each commutative ring K, sequence $n(i)=i$,$i\geq 2$ and each value of parameters d and t there is a noncommutative system of stable Cremona generators of degree d and rank t.*

We say that $\mathbf{{}^iZ}$ is a *regular noncommutative system* of stable Cremona generators if $n(i)=i$ for each value of i.

Let $n(i), m(i), m(i) \leq n(i)$ be two increasing sequences of natural numbers and ${}^iZ$, ${}^iZ^1$ are corresponding stable systems of growing periods of degrees d and d' $(d' \leq d)$ and rank t, $t>1$.

We say that $\mathbf{{}^iZ'} = \{{}^ig'_1, {}^ig'_2, \dots , {}^ig'_t\}$ *is* a *quotient of stable Cremona system* ${}^iZ$ if the rule $\varphi({}^ig_j)= {}^ig'_j$, $j=1, 2,\dots, t$ defines computationally tame homomorphism of semigroup ${}^iSZ$ onto ${}^iSZ^1$, i. e. homomorphism computable in time $O(n_i^{\alpha})$ for some positive constant α. We refer to ${}^iZ$ as *stable cover of noncommutative system of stable Cremona generators*.

As it follows from results [41] the statement below holds.

THEOREM 2. *For each finite commutative ring K and natural* *numbers d, $d>0$ and t, $t \geq 2$ there is an increasing sequence $n(i)$ of natural numbers and noncommutative system of stable Cremona generators* ${}^{i}Z=\{{}^{i}g_1, {}^{i}g_2, \dots, {}^{i}g_t\}$ *of degree d and rank t which has a regular quotient* ${}^{i}Z'$.

We say that stable Cremona system of degree d of elements has *enveloping family* of stable subsemigroup $EZ^{i}(K)$ of degree d if $E_{(i)}(K)>EZ^{i}(K)>SZ^{i}(K)$.

2. Multivariate tahoma protocol for stable Cremona generators and its usage for Multivariate Encryption Algorithms.

Word *tahoma* stands here for the abbreviation of ‘’tame homomorphism’’. Noteworhy that Tahoma is a name of mountain in North America and popular shrift in text processing.

Let us assume that Alice selects a noncommutative system $Z(K)$ of *stable Cremona generators* of degree d and rank t with quotient $Z'(K)$ such that there is an enveloping family $EZ(K)$ of $Z(K)$ and enveloping family $EZ^{1}(K)$ of $Z'(K)$.

Alice chooses parameter i and bijective affine transformation T, $deg(T)=1$ and T', $deg(T')=1$ acting on $(K)^{n(i)}$ and $(K)^{m(i)}$. She selects elements E and ${}^{1}E$ from $EZ_{n(i)}(K)$ and $EZ'_{m(i)}(K)$. Alice takes generators g_1, $g_{2, \dots}$, g_t of $SZ_i(K)$ and corresponding images g'_1, g'_2, ..., g'_t in the $SZ'_i(K)$.

So she forms $a_j = TEg_jE^{-1}T^{-1}, j=1,2,\dots,t$ and $b_j = T'E'g'_j(E')^{-1}(T')^{-1}$, $j=1,2,\dots,t$ written in standard form of $E_{n(i)}(K)$ and $E_{m(i)}(K)$.

Alice sends (a_j, b_j) and $j=1,2,\dots,t$ to Bob. He takes alphabet $\{z_1, z_{\underline{2}},\dots, z_{\underline{t}}\}$ and selects word $w(z_1, z_2, \dots, z_t)$, $=z_{i(1)}^{\alpha(1)}z_{i(2)}^{\alpha(2)} \dots z_{2i(l)}^{\alpha(l)}$, where $\alpha(j)>0$, $j=1,2, \dots, l$, $l>1$, $i(s)\epsilon\{1,2,\dots,t\}$, $i(j)\neq i(j+1)$ for $j=1,2,\dots,t-1$.

Bob computes $b=w(b_1, b_2,\dots,b_t)$ and keeps it safely for himself. He forms $a=w(a_1, a_2, \dots a_t)$ and sends this element of $E_{n(i)}(K)$ to Alice.

She uses the following restoration process to get $w(b_1, b_2,\dots,b_t)$. Alice computes $E^{-1}T^{-1}aTE=c$. She uses tame homorphism φ corresponding to noncomutative system Z and its quotient Z^{1} and computes $\varphi(c)=c'$. Secondly she computes $b=w(b_1, b_2,\dots,b_t)$ as $T'E'c^{1}(E')^{-1}(T')^{-1}$.

REMARK 1. *Adversary* has to decompose available multivariate map $a=w(a_1, a_2)$ from $E_{n(i)}$ into word in given generators $a_1, a_2, \dots, a_t$ written in their standard form. So security rests on the *word problem* in semigroup $E_{n(i)}(K)$ (or stable semigroup $<a_1, a_{2, \dots,} a_t>$).

Noteworthy that due to this algorithm correspondents Alice and Bob can safely elaborate collision quadratic transformation of $(K)^{m(i)}$ with the chosen dimension $m(i)$. In the case of regular quotient $m(i)=i$.

So correspondents have an algorithm to elaborate safely stable collision map of selected degree d acting of free module K^{l} of arbitrarily chosen dimension. This option rises the following question.

DO WE NEED MULTIVARIATE PUBLIC KEY?

One of the directions of security research is CLASSICAL MULTIVARIATE CRYPTOGRAPHY (see books [42], [43] which present examples of old public keys in the form of a family of quadratic elements ${}^{n}F$

of $E_n(F_q)$ which induces a bijective map $\Delta({}^nF)$. The map ${}^nF$ is given publicly.

So each public user (and adversary as well)can create as many pairs $(x, y=\Delta({}^nF)(x))$ where x is choosen plaintext from the plainspace $F_q{}^n$ and get corresponding ciphertext y as he/she wants.

Thus due to above protocol there is no need to give F to public. Alice can select some family which is a current or former (already broken) candidate to a safe pubic key. So she has a private algorithm to solve equation $F(x)=b$.

She can deformate ${}^nF$ by bijective elements ${}^1T_n$ and ${}^2T_n$ from $AGL_n(F_q)$ to use elements $G_n={}^1T_n\,{}^nF\,{}^2T_n$. Secondly Alice and Bob executes MULTIVARIATE TAHOMA PROTOCOL to elaborate common element $B_n(x)$ from $E_n(F_q)$.

We assume that G_n and B_n are given in the forms of tuples $(g_1, g_2, \ldots, g_n)$ and $(b_1, b_2, \ldots, b_n)$ where g_i and b_i are elements of $F_q[x_1, x_2, \ldots, x_n]$.Finally Alice sends $(g_1+b_1, g_2+b_2, \ldots, g_n+b_n)$ to Bob. He uses his knowledge on $B(x)$ and publicly known addition rule to restore $G(x)$. So Bob uses $G(x)$ as encryption function**.** Alice uses her private algorithm of finding the reimage of $F(x)$ for the decryption.

Conclusion 1. *No need to give multivariate rule F(x) of bounded degree* for public *audience. There is a safe way to transport the rule to your partner.*
Next question is
How long correspondents are able to keep G in private mode?

REMARK 2. Assume that correspondents use Multivariate Stable Protocol and Alice transports safely quadratic multivariate encryption map G on $F_q{}^n$ (or transformation of constant degree d).

Bob sends Alice several elements of kind $G(p_i)$, $i=1,2, \ldots, l$ via open channel during their communication.

If parameter l is "large enough" ($l=O(n^2)$ for $d=2$) then ADVERSARY can use his cyberterrorist tools and intercept some *pairs* (p_i, c_i) where p_i is a plaintext and c_i is a corresponding ciphertext. *If he/she intercepts* $O(n^2)$ such pairs then he can approximate G with costly polynomial algorithm (cryptanalitic linearisation method), which requires $O(n^5)$ elementary operation for $d=2$.

Such activity allows ADVERSARY to become in the same position with user Bob. He gets G from the private storage of correspondents. Similarly to the case of having public rule adversary can compute $G(p)$ for any chosen p.

Of course Adversary has to break "public rule" G as well, i.e. to find out the way of computation of its reimage.

Alice and Bob could be smart enough to use reasonable trust interval restricting parameter l (*number of messages*) by some expression $C(n)$ such that $C(n) \leq den(G)/(2n)$ (half of the *average density of* G_i, $i=1,2,\ldots,n$**).**

At the end of trust interval Alice may select other conjugates of generators of Singer system, correspondents conduct a new session of the protocol. Alice delivers safely a new quadratic encryption rule for Bob.

Conclusion 2. *After the transportation of the encryption multivariate rule F(x) to your partner there is an option of its periodical modification. This scheme allows privatisation of multivariate public rules,i.e. transition of the rule to noncommutative El Gamal Gamal type cryptosystem which uses Protocols of noncommutative cryptography which hide the encryption algorithm from adversary.*

PRACTICAL ASPECTS: Instead of quasipublic rules Alice can create invertible quadratic multivariate map G of density $O(n)$ (density is the number of monomial terms in all G_i , $i=1,2,\dots,n$) which allows to compute its reimage for $O(n)$ elementary steps. Notice that $O(n)$ is a speed of reading of string from M^n, where M is selected finite alphabet.

Some of the presented cryptographic privatisation schemes are already implemented on the level of prototype models (see [7], [9]).

3. On multivariate digital signatures algorithms and their privatisation scheme.

It is commonly admitted that Multivariate cryptography turned out to be more successful as an approach to build signature schemes primarily because multivariate schemes provide the shortest signature among post-quantum algorithms. Such signatures use system of nonlinear polynomial equations

$$^1p(x_1,x_2 , \dots , x_n) = {}^1p_{i,j} \cdot x_ix_j+{}^1p_i \cdot x_i+ {}^1p_0$$

$$^2p(x_1, x_2, \dots , x_n) = {}^2p_{\,i,j} \cdot x_ix_j +{}^2p_i \cdot x_i +{}^2p_0$$

$$\dots$$

$$^mp(x_1,x_2 , \dots , x_n) = {}^mp_{i,j} \cdot x_ix_j+{}^m\mathrm{p}_i \cdot x_i+ {}^mp_0$$

where ${}^kp_{\,i,j}$, ${}^kp_{\,i}$ are elements of selected commutative ring K.

The quadratic multivariare cryptography map consists of two bijective affine transformations, S and T of dimensions n and m, and a quadratic element P' of kind $x_i \rightarrow {}^ip$ of formal Cremona group, where ${}^ip$ are written above elements of $K[x_1, x_2,\dots,x_n]$.We denote via $\Delta(P')^{-1}(y)$ some reimage of $y=\Delta(P(x))$. The triple $\Delta(S)^{-1}$, $\Delta(P')^{-1}$, $\Delta(T)^{-1}$ is the private keyq also known as the trapdoor.

The public key is the composition S, P' and T which is by assumption hard to invert without the knowledge of the trapdoor. Signatures are generated using the private key and are verified using the public key as follows. The message is hashed to a vector y via a known hash function. The signature is $\Delta(T)^{-}$

^{1} $(\Delta(P')^{-1})(\Delta(S)^{-1})$. The receiver of the signed document must have the public key P in posession. He computes the hash y and checks that the signature x fulfils $\Delta(P)(y)=x$.

EXAMPLE. Assume that we have two groups of variables $z_1, z_2, \ldots, z_r$ and $z'_1, z'_2, \ldots, z_{n-r}$ such that the substitution $x_1=z_1, x_2=z_2, \ldots, x_r=z_r, x_{r+1}=z'_1, x_{r+2}=z'_2, \ldots, x_n=z'_{n-r}$ converts every single element ${}^{i}p$ to expression in the form $\Sigma\gamma_{ijk}z_jz'_k + \Sigma\lambda_{ijk}z'_jz'_k + \Sigma\varsigma_{ij}z_j + \Sigma\varsigma'_{ij}z'_j + \sigma_i$. In this situation we have to sign a given message y and the result is a valid signature x .The coefficients, $\gamma_{ijk}, \lambda_{ijk}, \varsigma_{ij}, \varsigma'_{ij}$and σ_i must be chosen secretly. The vinegar variables z'_i are chosen randomly (or pseudorandomly).The resulting linear equations system gets solved for the oil variables z_i.

Described above *unbalanced oil and vinegar (UOV) scheme* is a modified version of the oil and vinegar scheme designed by J. Patarin. Both are digital signature protocols. They are algorithms of multivariate cryptography. The security of this signature scheme is based on an *NP*-hard mathematical problem. To create and validate signatures a minimal quadratic equation system must be solved. Solving m equations with n variables is *NP*-hard. While the problem is easy if m is either essentially larger or essentially smaller than n,[1] importantly for cryptographic purposes, the problem is thought to be difficult in the average case when m and n are nearly equal, even when using a quantum computer. Multiple signature schemes have been devised based on multivariate equations with the goal of achieving quantum resistance. We assume that parameter n can be selected in a free way and parameters n and m are connected via linear equation $\alpha n+\beta m+b$ where $\alpha\neq 0, \beta\neq 0$. So $m=)(n)$. We take integer k which $\geq max(n, m), k=O(n)$ and commutative ring $K[x_1,x_2,\ldots,x_n, x_{n+1}, x_{n+2}, \ldots, x_k]$ where x_i, $i=1,2,\ldots,n$ are variables of public equations ${}^{j}p(x_1,x_2, \ldots, x_n), j=1,2, \ldots,m$ and $x_{n+1}, x_{n+2},\ldots,x_k$ are formal variables. Further one of suggested below schemes can be used.

Scheme 1. Let us assume that Alice selects a noncommutative system $Z(K)$ of *stable Cremona generators* of degree d =2 and rank t, $t>1$ with regular quotient $Z'(K)$ such that there is an enveloping family $EZ(K)$ of $Z(K)$ and enveloping family $EZ^1(K)$ of $Z'(K)$. Let us assume that $Z(K)$ corresponds to the sequence of increasing integers $n(i)$ and i coincides with the number of total variables k introduced above. So Alice takes generators ${}^{k}g_1, {}^{k}g_2, \ldots, {}^{k}g_t$ and uses multivariate *tahoma protocol*. She forms $a_j \in E_{n(k)}(K)$ and $b_j \in E_k(K)$. *She* sends them to Bob. Correspondents execute the protocol and elaborate common collision element $h=(h_1, h_2, \ldots, h_k) \in E_k(K)$. Alice (or Bob) selects polynomials ^{i}p for the multivariate digital signature system (m.d.s.). She/he takes h' with coordinates $h'_1={}^{i}p+h_i$, $i=1,2,\ldots m$ and $h'_i= h_i + f_i$,

$i=m+1, m+2,\ldots,k$ where f_i are quadratic ''pseudorandom'' elements of $K[x_1, x_2, \ldots, x_k]$.

Noteworthy that users has to know formats n and m of hashed vector and a signature. So Bob (Alice) restores $({}^1p, {}^2p,\ldots,{}^mp)$ and correspondents can use the multivariate digital signature system on private El Gamal mode based on the chosen multivariate tahoma protocol.

Scheme 2. Alice (or Bob) can use described above scheme with $d=3$. For $f \in K[x_1, x_2, \ldots x_k]$ we define its quadratic restriction $r(f)$ as the sum of monomial terms of degree at most 2. Let $D=d/d_{x1}+ d/d_{x2}, \ldots + d/d_{xk}$ be differentiation operator for elements of $K[x_1, x_2, \ldots x_k]$. We define deformation $def(f)$ of f as $D(f)+r(f)$ (see [5] for the idea of deformated collision maps). So correspondents use scheme 1 to elaborate common cubical collisen map h. They continue remaining steps of scheme 1 with quadratic $def(h)$ instead of h.

5. Examples of stable cubical groups.

5.1. Simplest graph based example. The following family of stable groups is already used in some algorithms of symmetric cryptography and protocols of commutative and noncommutative cryptography (see [44], [45] and further references). Let K be a commutative ring. We define $A(n, K)$ as bipartite graph with the point set $P=K^n$and line set $L=K^n$ (two copies of a Cartesian power of K are used). We will use brackets and parenthesis to distinguish tuples from P and L. So $(p)=(p_1, p_2, \ldots , p_n)\in P_n$ and $[l]=[l_1, l_2, \ldots , l_n]\in L_n$. The incidence relation $I=A(n,K)$ (or corresponding bipartite graph I) is given by condition $pI\, l$ if and only if the equations of the following kind hold.

$p_2 - l_2=l_1p_1$, $p_3 - l_3= p_1 l_2$, $p_4 - l_4 = l_1p_3$, $p_5 - l_3 = p_1 l_4$, $\ldots$, $p_n - l_n= p_1 l_{n-1}$ for odd n and $p_n - l_n = l_1 p_{n-1}$ for even n.

Let us consider the case of finite commutative ring K, $|K|=m$. As it instantly follows from the definition the order of our bipartite graph $A(n, K)$ is $2m^n$. The graph is m-regular. In fact the neighbour of given point p is given by above equations, where parameters $p_1, p_2,\ldots, p_n$ are fixed elements of the ring and symbols $l_1, l_2,\ldots, l_n$ are variables. It is easy to see that the value for l_1 could be freely chosen. This choice uniformly establishes values for l_2, l_3, $\ldots$, l_n . So each point has precisely m neighbours. In a similar way we observe the neighbourhood of the line, which also contains m neighbours. We introduce the colour $\rho(p)$ of the point p and the colour $\rho(l)$ of line l as parameter p_1 and l_1 respectively.

Graphs $A(n, K)$ with colouring ρ belong to class of Γ *linguistic graphs* considered in [46]. Linguistic graph $\Gamma= \Gamma(K)$ is defined over commutative ring K as a bipartite graph with partition sets L=K^n and P=K^k and colour sets K^s and K^r respectively. Projection ρ of point $x=(x_1, x_2, ..., x_n)$, or line $y=[y_1, y_2, ...,y_t]$, on the tuple of their first s and r coordinates respectively defines colours of vertices. Each vertex has a unique neighbour of selected colour. So $n+r=t+s$. The incidence of linguistic graphs is given by a system of polynomial equation over the ring K.
In the case of linguistic graph $\Gamma(K)$ with $s=r=1$ the path consisting of its vertices $v_0, v_1, v_2, ...,v_k$ is uniquely defined by initial vertex v_0, and colours $\rho(v_i,), i=1, 2,..., k$ of other vertices from the path. We can consider graph $\Gamma=\Gamma'(K[x_1, x_2, ..., x_n])$ defined by the same with Γ equations but over the commutative ring $K[x_1, x_2, ..., x_n])$.
So the following symbolic computation can be defined. Take the *symbolic point* $x=(x_1, x_2, ..., x_n)$, where x_i are generic variables of $K[x_1, x_2, ..., x_n]$ and *symbolic string C* which is a tuple of polynomials $f_1,, f_2,, ... , f_k$, from $K[x_1]$ with even parameter k.. Form the path of vertices $v_0,=x$, v_1 such that v_1Iv_o and $\rho(v_1)=f_1(x_1)$, v_2 such that v_2Iv_1 and $\rho(v_2)=f_2(x_1)$, ..., v_k such that v_kIv_{k-1} and $\rho(v_k)=f_k(x_1)$. We choose parameter k as even number. So v_k is the point from the partition set $K[x_1, x_2,..., x_n]^n$ of the graph Γ'.

We notice that the computation of each coordinate of v_i depending on variables $x_1, x_2, ..., x_n$ and polynomials $f_1,, f_2,, ... , f_k$ needs only arithmetical operations of addition and multiplication. As it follows from the definition of linguistic graph final vertex v_k (point) has coordinates $(h_1(x_1), h_2(x_1,x_2), h_3(x_1,x_2,x_3),...,h_n(x_1,x_2,..., x_n))$, where $h_1(x_1)=f_k(x_1)$. Let us consider the map $H= \Gamma\char`^\eta(C)$: $x_i\rightarrow h_i(x_1, x_2,..., x_n), i=1, 2,..., n$ which corresponds to symbolic string C. Assume that the equation $b=f_k(x_1)$ has exactly one solution. Then the map $H:x_i\rightarrow h_i(x_1, x_2, ..., x_n)$, $i=1, 2,..., n$ is a bijective transformation. In the case of finite parameter k and finite densities of $f_i(x_1)$, $i=1, 2,..., n$ the map H also has finite density. If all parameters $\deg(f_i(x_1))$ are finite then the map H has a linear degree in variable n. The idea of symbolic computation (see [44] and further references) is the following one.
Let us consider the totality $St=St(K)$ of all symbolic strings with the product $(f_1, f_2,..., f_r) \cdot (g_1, g_2,..., g_s) = (f_1, f_2,..., f_s, g_1(f_r), g_2(f_r),...g_s(f_r))$. It is easy to see that $St(K)$ is a semigroup for which empty string serves as a unity.

One can check that the map ${}^{\Gamma}\eta=\eta$ *is a* homomorphism of semigroup $St(K)$ into Cremona semigroup $S(K^n)$ for each linguistic graph Γ with $r=s=1$ and point set K^n. We consider a subsemigroup $\sum=\sum(K)$ *of symbolic strings C* of kind $(x_1+a_i, x_2+ a_2 \ldots, x_t+a_t)$ where parameter t is even. In the case of a linguistic graphs with $r=s=1$ we identify a symbolic stringn C with the corresponding tuple $(a_1, a_2, \ldots, a_t)$. Natural product of two strings given by tuples $C_1=(a_1, a_2, \ldots, a_t)$ and $C_2=(b_1, b_2, \ldots, b_m)$ is a string $C=C_1 \circ C_2=(a_1, a_2, \ldots, a_t, b_1+a_t, b_2+a_t, \ldots, b_m+a_t)$. This product transforms $\sum$ to a semigroup. The map η' sending C to $\eta(C)$ is a homomorphism of $\sum$ into affine Cremona group $C(K^n)$. It is a restriction of ${}^{\Gamma}\eta$ onto $\sum(K)$. Let $C=(x_1 a_1, x_1+a_2, \ldots., x_1+a_s)$ be a symbolic string from semigroup $\Sigma(K)$. We refer to $Rev(C)=(x_1-a_s+a_{s-1}, x_1-a_s+a_{s-2}, \ldots, x_1-a_s+a_1, x_1-a_s)$ as a reversing string for C. It is easy to see that $\eta'(CRev(C))$ *is a unity* of Cremona semigroup.

In the case of linguistic graphs $\Gamma=A(n, K)$ the totality $G(n, K) = \eta'(\sum(K))$ is a stable subgroup of degree 3 (see [44] and further references). We use notation ${}^{n}\eta'$ for the restriction of ${}^{\Gamma}\eta$, $\Gamma=A(n,K)$ onto $\sum$. We assume that $a_0=0$ and say that transformation $\eta'(C)$ is irreducible if $a_i \neq a_{i+2}$, $i=1, 2,\ldots, t-2$. If $a_1 \neq a_{t-1}$, and $a_2 \neq a_t$ we say that irreducible symbolic string C and corresponding transformation $\eta'(C)$ are standard elements. We have a natural homomorphism $G(n+1, K)$ onto $G(n, K)$ induced by the homomorphism Δ from $A(n+1, K)$ onto $A(n, K)$ sending point $(x_1, x_2, \ldots, x_n, x_{n+1})$ to $(x_1, x_2, \ldots, x_n)$ and line $[x_1, x_2, \ldots, x_n, x_{n+1}]$ to $[x_1, x_2, \ldots, x_n]$. It means that there is well defined projective limit $A(K)$ of graphs $A(n, K)$ and groups $G(K)$ of groups $G(n, K)$ when n is growing to infinity. In fact in the case of $K=F_q$, $q>2$ infinite graph $A(F_q)$ is a tree.

It means that group $G(F_q)$ is a group of walks of even length on q-regular tree starting in zero point with natural addition of them. A standard symbolic string C defines transformation ${}^{n}\eta'(C)$ in each group $G(n, K)$, $n \geq 2$ and $G(K)$. An irreducible transformation $\eta'(C)$ from $G(K)$ has an infinite order.

We are going to use the family of maps introduced below.

Let $\Delta=\Delta n,k$, $n>k$ be a canonical homomorphism of $A(n,K)$ onto $A(k,K)$ corresponding to procedure of deleting of coordinates with indexes $k+1, k+2, \ldots, n$. This map defines the canonical homomorphism $M=\mu(n, k)$ of group $G(n, K)$ onto $G(k, K)$. Let us consider the diagram

$$\begin{tikzcd}
 & \sum(K) \arrow[dl, dash] \arrow[d] \\
G(k, K) & G(n, K) \arrow[l]
\end{tikzcd}$$

where vertical arrow corresponds to homomorphism ${}^{n}\eta'$ from $\sum(K)$, skew line corresponds to ${}^{k}\eta'$ and horizontal arrow stands for $M(n,k)$, $n>k$. It is easy to see that this diagram is a commutative one.

As it was noticed in [44] subgroups $G(n, K)$ of $E_n(K)$ form a family of stable cubical maps. So correspondents can take pair $G(n, K)$ and $G(k, K)$ with $n(k)=k+\gamma$ where parameter γ is a positive constant or a positive linear function in variable k.

Alice can use defined above computationally tame homomorphism $M=M(n,k)$, $n>k$ of groups $G(n,K)$ and $G(k,K)$.

She considers family of subgroups $G_k=G(n,K)$, $n=n(k)$, $k-2,3$ and family $G'_k=G(k,K), k=2,3,\ldots,n$

She selects different strings $w_1, w_2, \dots w_t$ of even length of semigroup $\sum(K)$ such that $w_i w_j \neq w_j w_i$ for different i and *f*rom $\{1,2,\dots,t\}$. This condition implies that ${}^s\eta(w_i w_j) \neq {}^s\eta(w_j w_i)$ for $s \geq 2$. After the check of noncommutativity of generators Alice takes generators ${}^ig_j={}^{n(i)}\eta\ (w_j)\ , j=1, 2, \dots, t, i \geq 2$ which form a Cremona system of stable noncommutative generators corresponding to sequence $n(2),n(3),\dots$. Let us denote this system as Z. Notice that ${}^iSZ = <{}^ig_1, {}^ig_2, \dots, {}^ig_t>$ is a subgroup of G_i. So the $G_i(K)$ form an enveloping family of Z..

Similarly Alice consider generators ${}^ig'_j = {}^i\eta\ (w_j), j=2, 3, \dots, t, i \geq 2$ of system Z'.Notice that ${}^iSZ$ '$= <{}^ig'_1, {}^ig'_2, \dots, {}^ig'_t>$ is a subgroup of $G'_i(K)$

So the $G'_i(K), i=2,3,\dots$ is an enveloping family of Z'.

It is easy to see that the system Z' is a quotient of Z defined by tame homomorphisms which move ${}^ig_j$ to ${}^ig'_{j.}$ So Alice takes $i=k$ and starts Stable Tahoma Protocol with Z and Z' and described enveloping families. So she conducts steps of the algorithm , generates pairs a_i , b_i , $i=1,2,\dots,t$ and sends them to Bob. Thus correspondents generate the collision element h in *E_k(K).* Alice (or Bob) selects multivariate map for digital signatures *(MDS)* to Bob (Alice). She/he uses *def (h)* and safely delivers the map to partner.

5.2. Other stable subgroups defined via linguistic graphs.

Let us consider more general graph based constructions of semigroups of formal Cremona semigroup $E_n(K)$.

Element $x_1 \longrightarrow f_i(x_1, x_2, \dots, f_n), i=1,2,\dots,n$ of this semigroup will be identified with the tuple of elements $(f_1, f_2, \dots, f_n)$, $\mathrm{f}_i \in K[x_1, x_2, \dots, x_n]$ when it is convenient.

Let us consider a totality ${}^sBS(K)$ of sequences of kind $u=(H_0, G_1, G_2, H_3, H_4, G_5, G_6, \dots, H_{t-1}, H_t), t=4i$, where $H_k \in E_s(K), G_j \in E_s((K)$. We refer to ${}^sBS(K)$ as a totality of free symbolic strings of rank s. We define a product of u with $u'=(H'_0, G'_1, G'_2, H'_3, H'_4, G'_5, G'_6, \dots, H'_{l-1}, H_l)$ as $w=(H_0, G_1, G_2, H_3, H_4, G_5, G_6, \dots, H_{t-1}, H'_0(H_t), G'_1(H_t), G'_2(H_t), H'_3(H_t), H'_4(H_t), G'_5(H_t), G'_6(H_t), \dots, H'_{l-1}(H_t), H'_l(H_t))$. Notice that the compositions of maps is computed in $E_s(K)$.

It is easy to see that this operation transforms ${}^sBS(K)$ into the semigroup with the unity element (H_0), where E_0 is an identity transformation from $S(K^s)$. Elements of kind $(H_0, G_1, G_2, H_3, H_4)$ are generators of the semigroup. This subsemigroup has some similarity with subsemigroup of special chains in the free product $E_s(K)$▪$E_s(K)$. We refer to ${}^sBS(K)$ as *semigroup of free regular strings of dimension s.*

Let us assume that H_t of written above $u \in {}^sBS(K)$ is a bijective map and its inverse is a polynomial map (in the case of infinite ring K). Then we can consider a reverse linguistic string $Rev(u)= (H_{t-1}(H_t^{-1}), G_{t-2}(H_t^{-1}), G_{t-3},(H_t^{-1}), H_{t-4}(H_t^{-1}),H_{t-5}^{1}(H_t), \dots,G_2(H_t^{-1}), G_1(H_t^{-1}), H_0(H_t^{-1}), H_t^{-1})$ and refer to u as reversible string. Let ${}^sBR(K)$ stand for the semigroup of reversible strings.

Let K be a finite commutative ring. We refer to an incidence structure with a point set $P=P_{s,m}=K^{s+m}$ and a line set $L=L_{r,m}=K^{r+m}$ as linguistic incidence structure I_m if point x=$(x_1, x_2, \dots, x_s, x_{s+1}, x_{s+2}, \dots, x_{s+m})$ is incident to line y=$[y_1, y_2, \dots, y_r, y_{r+1}, y_{r+2}, \dots, y_{r+m}]$ if and only if the following relations hold

$$a_1x_{s+1}+b_1y_{r+1}=f_1(x_1, x_2, \dots, x_s, y_1, y_2, \dots, y_r)$$
$$a_2x_{s+2}+b_2y_{r+2}=f_2(x_1, x_2, \dots, x_s, x_{s+1}, y_1, y_2, \dots, y_r, y_{r+1})$$
$$\dots$$
$$a_mx_{s+m}+b_my_{r+m}=f_m(x_1, x_2, \dots, x_s, x_{s+1}, \dots, x_{s+m}, y_1, y_2, \dots, y_r, y_{r+1}, \dots, y_{r+m})$$

where a_j, and b_j , $j=1,2,,,,m$ are not zero divisors, and f_j are multivariate polynomials with coefficients from K. Brackets and parenthesis allow us to distinguish points from lines (see [9]).

The colour $\rho(x)=\rho((x))$ $(\rho(y)=\rho([y]))$ of point $\mathbf{x}$ (line $[\mathbf{y}]$) is defined as projection of an element (x) (respectively $[y])$ from a free module on its initial s (relatively r) coordinates. As it follows from the definition of linguistic incidence structure for each vertex of incidence graph there exists the unique neighbour of a chosen colour.

We refer to $\rho((x))=(x_1, x_2, \dots, x_s)$ for $(x)=(x_1, x_2, \dots, x_{s+m})$ and $\rho([y])=(y_1, y_2, \dots, y_r)$ for $[y]=[y_1, y_2, \dots, y_{r+m}]$ as the colour of the point and the colour of the line respectively. For each $b\epsilon K^r$ and p=$(p_1, p_2, \dots, p_{s+m})$ there is the unique neighbour of the point $[l]=N_b(p)=N((p),b)$ with the colour b. Similarly for each $c\epsilon K^s$ and line l=$[l_1, l_2, \dots, l_{r+m}]$ there is the unique neighbour of the line $(p)= N_c([l])=N([l],b)$ with the colour c. We refer to operator of taking the neighbour of vertex accordingly chosen colour as sliding operator. On the sets P and L of points and lines of linguistic graph we define jump operators ${}^1J={}^1J_b(p)=J((p),b)=(b_1, b_2, \dots, b_s, p_1, p_2, \dots, p_{s+m})$, where $(b_1, b_2, \dots, b_s)\epsilon K^s$ and ${}^2J={}^2J_b([l])=J([l],b)=[b_1, b_2, \dots, b_r, l_1, l_2, \dots, l_{r+m}]$, where $(b_1, b_2, \dots, b_r)\epsilon K^r$. We refer to tuple (s, r, m) as type of the linguistic graph $I=I(K)$.

Notice that we can consider the same set of above equations with coedicients from K for variables x_i and y_i from the extension K' of K and define graph ${}^{K'}I={}^{K}{}'I(K)$. Let $s=r$ and $K'=K[x_1, x_2, \dots, x_n]$, $n=m+s$. We consider induced subgraph in I' of all vertices of ${}^{K'}I$ with colours from $K[x_1, x_2, \dots, x_s]$ (tuples of $K[x_1, x_2, \dots, x_s]^s$)

We form the sequence of vertices (walk with jumps) of graph $I'$with the usage of string u from free linguistic semigroupn ${}^sBS(K)$.

We take initial point (x)=$(x_1, x_2, \dots, x_s, x_{s+1}, x_{s+2}, \dots, x_{s+m})$ formed by the generic variables of K' and consider

a skating chain

$$(x),J((x),H_0)=({}^1x),N(({}^1x),G_1)=[{}^2x],J([{}^2x],G_2)=[{}^3x],N([{}^3x],H_3)=({}^4x),J(({}^4x),H_4)=({}^5x),$$
$$\dots, J([{}^{t-2}x],G_{t-2})=[{}^{t-1}x],N([{}^{t-1}x],H_{t-1})=({}^tx),J(({}^tx),H_t)=({}^tx).$$

Let $({}^tx)$ be the tuple $(H_t, F_2, F_3, \dots, F_n)$ where $F_i \epsilon K[x_1, x_2, \dots, x_n]$. We define ${}^I\Psi(u)$, $I=I(K)$ as the map $(x_1, x_2, \dots, x_n)\rightarrow(H_t, F_2, F_3, \dots, F_n)$ and refer to it *as chain transition of point variety.*

The statement written below follows from the definition of the map.

Lemma 1. *The map* $\psi={}^{I}\psi$: ${}^{s}BS(K)\rightarrow E_n(K)$ *is a homomorphism of semigroups,* $\psi({}^{s}BR(K))$*is a group* ([41]),

We refer to ${}^{I}\psi({}^{s}BS(K))={}^{I}CT(K)$ as a *chain transitions semigroup* of linguistic graph $I(K)$ and to map ψ as *linguistic compression map.* Notice that in the case of the finite commutative ring homomorphism composition $\Delta\psi$ *of homomorphism* Δ *and* ψ maps infinite semigroup into finite set of elements of $\Delta({}^{I}CT(K))$.

We define subsemigroup ${}^{s}GS(K)$ of *symbolic ground strings* as a totality of bipartite strings $u=(H_0, G_1, G_2, H_3, H_4, G_5, G_6,\dots, H_{t-1}, H_t)$ in ${}^{s}BS_r(K)$ with $H_0=E_0, G_1=G_2, H_3=H_4,G_5=G_6,\dots, H_{t-1}=H_t$ where E_0 is a unit of $E_n(K)$ and refer to ${}^{I}\psi({}^{s}GS(K))={}^{I}GCT(K)$ as *semigroup of ground chain transitions* on linguistic graph *I*.

In the case of linguistic graph $A(n,K)$ of type $(1,1,n\text{-}1)$ we can consider a subgroup $St(K)$ of elements of ${}^{1}GS(K)$ with coordinates of type $x_1+t,\ t\epsilon K$ and identify ${}^{A(n,K)}\psi\ (St(K))$ with introduced above group of cubical endomorphisms $GA(n, K)$.

We can consider a subgroup $LSt(K)$ of elements ${}^{1}BS(K)$ *with* coordinates of type $x_1+t,\ t\epsilon K$ and construct extension $Ext(GA(n,K))$ of $G(n,K)$ as ${}^{A(n,K)}\psi\ (LSt(K))$. As it was shown in the paper [47] elements of stable group $Ext(AG(n,K))$ are also cubical endomorphisms.

In fact the first family $GD(n,K)$ of stable groups of degree 3 was introduced as group of transformative of bijective stream ciphers of multivariate nature define via linguistic graphs $D(n, K)$ of type $(1,1,n\text{-}1)$ in [36] The implementation of this cipher in the case $K=F_q$ is described in [37]. Graphs $D(n, F_q)$ and their connected components were introduced in [48],[49],[50] as family of graphs of large girth of Extremal graph theory. (see also [51], [52]). Connections between graphs $D(n,K)$ and $A(n,K)$ are discussed in [44].

5.3. Special homomorphisms of linguistic graphs and corresponding semigroups.

Let $I(K)$ be linguistic graph over commutative ring K defined in section 3.1. and $M = \{m1, m2,\dots, md\}$ be a subset of $\{1, 2, \dots, m\}$ (set of indexes for equations). Assume that equations indexed by elements from M of the following kind

$a_{m1}x_{m1} - b_{m1}y_{m1}=f_{m1}(x_1, x_2 , \dots, x_s ,y_1, y_2, \dots , y_r)$

$a_{m2}x_{m2} - b_{m2}y_{m2} = f_{m2}(x_1, x_2, \dots ,x_s,x_{m1},y_1, y_2, \dots , y_{r,}, y_{m1})$

…

$a_{md}x_{md} - b_{md}y_{md} =f_{md} (x_1, x_2, \dots , x_s,x_{m1},x_{m2,\dots ,} x_{m\,d-1,} y_1, y_2, \dots , y_{r,}, y_{m1}, y_{m2,\dots ,} y_{m\,d-1,})$ define other linguistic incidence structure $I_{M.}$ Then the natural projections $\delta_{1,}$: $(x)\rightarrow(x_1, x_2, \dots , x_s,x_{m1}, x_{m2,\dots ,} x_{md})$ and δ_2: $[y]\rightarrow[y_1, y_2, \dots , y_r, y_{m1},y_{m2,\dots ,} y_{md}]$ of free modules define the natural homomorphism δ of incidence structure I onto $I_{M.}$. We will use the same symbol ρ for the colouring of linguistic graph $I_{M..}$

It is clear, that δ is colour preserving homomorphism of incidence structures (bipartite graphs). We refer to δ as symplectic homomorphism and graph I_M as symplectic quotient of linguistic graph *I.* In the case of linguistic graphs defined by infinite number of equations we may consider symplectic quotients defined by infinite subset *M* (see [30], where symplectic homomorphism was used for the cryptosystem construction).

Lemma 3. *A symplectic homomorphism $\acute{\eta}$ of linguistic graph I of type (r, s, m) onto I' defined over commutative ring K induces the semigroup homomorphism $\acute{\eta}^*$ of ${}^{I}CT(K)$ into ${}^{I'}CT(K)$ and the following diagram is commutative*

$$\begin{tikzcd}
{}^{s}BS_r(K) \arrow[r] \arrow[d] & {}^{I}CT(K) \arrow[dl, dash, "/"] \\
{}^{I'}CT(K) &
\end{tikzcd}$$

where horizontal and vertical arrows corresponds to linguistic compression homomorphisms ${}^{I}\boldsymbol{\psi}$ and ${}^{I'}\boldsymbol{\psi}$ and symbol / corresponds to η^*.

If S is a stable subsemigroup of ${}^{I}CT(K)$ (or $BCT_I(K)$) of degree d then $\acute{\eta}^*(S)$ is also a stable subsemigroup (or subgroup).The degree of $\acute{\eta}^*(S)$ is bounded above by d. We will search for subsemigroup X *of* ${}^{s}BS_r(K)$ and linguistic graphs $I(K)$ such that $\Psi(X)$ is a stable subsemigroups of ${}^{I}CT(K)$.

5.4. Example of stable subsemigroups of arbitrary degree.

We define Double Schubert Graph $DS(k,K)$ over commutative ring K as incidence structure defined as disjoint union of partition sets $PS=K^{k(k+ 1)}$ consisting of points which are tuples of kind $x =(x_1 , x_2, \dots , x_k, x_{11} , x_{12}, \dots , x_{kk})$ and $LS=K^{k(k+1)}$ consisting of lines which are tuples of kind $y =[y_1 ,y_2, \dots ,y_k, y_{11} ,y_{12}, \dots ,y_{kk}]$, where x is incident to y, if and only if $x_{ij} - y_{ij}=x_i y_j$ for $i=1, 2,\dots, k$ and $j=1, 2,\dots, k$. It is convenient to assume that the indices of kind i,j are placed for tuples of $K^{k(k+1)}$ in the lexicographical order.

The term Double Schubert Graph 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. We will consider these connection in details in the next section.

We define the colour of point $x =(x_1 , x_2, \dots , x_k, x_{11} , x_{12}, \dots , x_{kk})$ from PS as tuple$(x_1 , x_2, \dots , x_k,)$ and the colour of a line $y =[y_1 ,y_2, \dots ,y_k y_{11} ,y_{12}, \dots ,y_{kk}]$ as the tuple $(y_1 , y_2, \dots ,y_k)$. For each vertex v of $DS(k, K)$, there is the unique neighbour $y=N_a(v)$ of a given colour $a=(a_1,a_2, \dots ,a_k)$. It means the graphs $DS(k, K)$ form a family of linguistic graphs.

Let us consider the subsemigroup ${}^{k}Y(d, K)$ of ${}^{k}BS(K)$ consisting of strings $u=(H_0, G_1, G_2, H_3, H_4, G_5, G_6,\dots, H_{t-1}, H_t)$ such that maximum of parameters $deg(H_0)+deg(G_1), deg(G_2)+deg(H_3), deg(H_4)+deg(G_5),$

$deg(G_6)+deg(H_7), deg(G_{t-2})+deg(H_{t-1}), deg(H_t)=1$

equals d, $d>1$.

Theorem 2 (see [41]). *Let I(K) be an incidence relation of Double Schubert graph DS(k, K). Then ${}^{I}\psi({}^{k}Y(d, K))={}^{k}U(d,K)$ form a family of stable semigroups of degree d.*

The proof is based on the fact that the chain transition u from ${}^{k}U(d, K)$ moves $x_{i,j}$ into expression $x_{i,j}+T(u)$, where $T(u)$ is a linear combination of products $f\epsilon K[x_1, x_2,\dots, x_k]$, $g\epsilon K[y_1, y_2,\dots, y_k]$ where $deg(f)+deg(g)\leq d$.

New semigroup ${}^{k}U(d, K)$ consists of transformations of the free module K^t, $t=(k+1)k$. If $d=2$ then ${}^{k}U(d, K)$ contain semigroups of quadratic transformation defined in [9], which consists of ground chain transitions.

Let J be subset of the Cartesian square of $M=\{I,2,\dots,k\}$. We can identify its element (i,j) with the index ij of Double Schubert Graph $DS(k,K)$.

Proposition 1. *Each subset J of M^2 defines symplectic homomorphism δ_J of $DS(k, K)$ onto linguistic graph $DS_J(k,K)$.*

It is easy to see that in the case of empty set J the image of the map is a complete bipartite graph with the vertex set K^kUK^k.

Corollary 1. *Let $I(J, K))$ be an incidence relation of linguistic graph $DS_J(k, K)$. Then ${}^{I(J,K)}\psi({}^{k}Y(d, K))={}^{k}U_J(d,K)$ form a family of stable semigroups of degree d.*

Second protocol of safe delivery of MDS.

Let $f: N\rightarrow R$ be real function in natural variable and $[\ ,]'$ stands for ceiling function, i.e $[f(n)]'$ is closest to $f(n)$ parameter n' such that $n'\geq n$.

Alice consider family of ${}^{r(n)}Y(d, K))$, $d=2$ or $d=3$ where $r(i)=[i^{1/2}]'$, i=2,3,… So the point set ${}^{r(i)}DS(d, K))$ is a free module of dimension $[i^{1/2}]'+([i^{1/2}]')^2$ which is at least $[i^{1/2} + i]'$.

For each i she can select the strings $u(1)=u(1,i), u(2,i), \dots, u(t,i)$, $t\geq 2$ of kind $u(k,i)=({}^{k,i}H_0, ,{}^{k,i}G_1, {}^{k,i}G_2, {}^{k,i}H_3, {}^{k,i}H_4, {}^{k,i}G_5, {}^{k,i}G_6,\dots, {}^{k,i}H_{t-1}, {}^{k,i}H_t)$, $k=1,2,\dots,t$ such that ${}^{k,i}H_t{}^{j,i}H_t\neq{}^{ji}H_t{}^{k,i}H_t$ for distinct k and j.

Last condition insure that for ${}^{I}\psi(u(k,i))=a(k,i)$, $k=1,2,\dots,t$ conditions $a(k,i)a(j,i)\neq a(j, i)a(k,i)$ holds if $j\neq k$.

So cubical endomorphisms $a(l,i)\epsilon E_{r(i)}$, $l=1,2,\dots,t$, $i=2,3,\dots$ form stable cubical Noncommutative Cremona system Z corresponding to the sequence $r(i)$. Semigroups ${}^{r(i)}U(d, K)$ form enveloping family of Z. Alice can take ${}^{r(i)}DS(d, K))$ and subset $J(i)$ which defines an incidence system $I(J, K))$ such that $|J(i)|=i-r(i)$. So the point set of $I(J(i), K)$ is K^i.

Symplectic homomorphism of ${}^{r(i)}DS(d, K))$ onto $I(J(i),K)$ induces homomorphism $\phi(i,J(i))$ *of semigroup* ${}^{r(i)}U(d, K)$ onto ${}^{i}U_{J(i)}(d,K)$. It is easy to see that $\phi(i,J(i))(a(k,i))=a'(k,i)$ form the quotient Z' of the system Z with enveloping family ${}^{i}U_{J(i)}(d,K)$.

So Alice selects multivariate digital signatures system with parameters m and n. She takes $i=k$ which exceed $max(m, n)$ for parameters m and n of MDC. She generates $a(k,j)$, $j=1,2,\dots,t$ from ${}^{r(k)}U(d, K)$ and considers subset $J(i)$. Alice uses invertible elements of enveloping semigroups ${}^{r(k)}U(d, K)$ and ${}^{k}U_{J(k)}(d,K)$ together with bijective affine transformations of free modules $K^{r(k)}$ and K^k. So she uses multivariate tahoma protocol, generates pairs (a_i, b_i) and sends them to Bob.

Correspondents executes the protocol and generates the collision map $h=(h_1, h_2,\dots, h_k)$ from $E_k(K)$.

In the case of $d=2$ Alice *(or Bob)* uses scheme 1 of section 4. So she/he sends $h_i+ {}^ip_i$, $i=1,2,\ldots,m$ to the partner who restores ${}^ip$. If $d=3$ Alice (or Bob) uses scheme 2 of section 4 with computation of $def(h)$.

6. Conclusions.

We consider an option to keep multivariate public map of digital signature system on ''secure mode of El Gamal type". So the combination of Multivariate Tahoma Protocol based on selected platform with the multivariate digital signature defined over chosen groupf field $K=F_q$ is used. The base is in fact triple which consists on two stable subsem groups $S_1(q)$ and $S_2(q)$ of $E_{p(n)}$ and $E_n(F_q)$ and homomorphis between them Open size n gives the format of used hashed vectors. This number is known to adversary.

According to the cryptographic conventions the whole used combination has to be known up to some hidden formal parameters which form the key of the algorithm.

Thus adversary knows ground field F_q, dimensions n and $p(n)$, pairs of generators (a_i , b_i), $i=1,2$, where $a_i \in E_{p(n)}(F_q)$ and $b_i \in E_n(q)$. So he knows degree of stable subsemigroups $<a_1, a_2,\ldots,a_t>$ an $<b_1, b_2,\ldots b_t>$, can use homomorphism which moves a_i to b_i but does not know alternative efficien way of homomorphism computation.

Adversary is informed that correspondents use protocol in periodic way, the collision map is used exactly one time and multivariate map is used for signatures $\leq$ n times. From session to session correspondents can change sets of generators without change of the platform

He/she know the type of multivariate map $P=SP'T$, S and T of dimensions n and m, and a quadratic element P' of kind $x_i \to {}^ip$, $i=1,2,\ldots m$, but does not know multivariate map P itself. It means that adversary knows that correspondents are followers of one selected method. So correspondents are followers of Imai-Matsumoto method, Original Oil and Vinegar method by J. Patarin, Rainbow UOV, or Lifted UOV algorithms.

Notice that cryptanalysis for first two method is known only in the case when P is given public. Adversary knows that correspondents are able to change maps S and T and internal parameters of P' in each of these four cases. For the simplicity we assume that number of equations m is known to adversary.

Thus adversary can try to break the tahoma multivariate protocol based on known NP hard problem (work decomposition of element of formal Cremona group into a product of given generators presented in the standard form of Multivariate Cryptography). Of course if he/she breaks the protocol adversary gets the multivariate digital signature in its public form. He/she has to periodically compute such a decomposition of obtained element into generators to get the corresponding collision map. So in the case of already broken classical Imai-Matsumoto and Oil and Vinegar schemes adversary can forge the signature. In the case of Raibow and Lifted UOV adversary has to find a solution for related crypt analytic problem. Current state of the cryptanalysis of these schemes the reader can find in [53], [54], [55].

Breaking the WORD PROBLEM is currently unsolvable post quantum problem, so we discuss the remaining options for adversary. Assume that adversary intercepts all pairs of kind (hash vector/corresponding signature) during the session. These *n* pairs are not sufficient to approximate the quadratic multivariate map of the signature. So the security of the entire algorithm rests entirely on the security of the protocol.

We present 12 combined algorithm (3 families of platforms and 4 types of general digital signatures). Time execution of the combination is a sum of already investigated protocol and signature scheme.

References.

1. Post-Quantum Cryptography: Call for Proposals:https://csrc.nist.gov/Project; Post-Quantum-Cryptography-Standardization/Call-for-Proposals, Post-Quantum Cryptography: Round 2 Submissions.
2. M. Andrzejczak, The Low –Area FPGA Desighn for the Post – Quantum Cryptography Proposal Round 5, Proceedings of the Federated Conference on Computer Science and Information Systems (FedCSIS), Cryptography and Security Systems, Leipzig, 2019.
3. R. J. McEliece, A Public-Key Cryptosystem Based On Algebraic Coding Theory (1978), DSN Progress Report, 44: 114–116.
4. Jintai Ding and Albrecht Petzoldt. Current state of multivariate cryptography. *IEEE Security & Privacy*, 15(4):28–36, 2017.
5. V. Ustimenko, On new symbolic key exchange protocols and cryptosystems based on hidden tame homomorphism. Dopovidi. NAS of Ukraine, 2018, n 10, pp.26-36.
6. V. Ustimenko, On the families of stable transformations of large order and their cryptographical applications, Tatra Mt. Math. Publ., 70 (2017), 107-117.
7. V. Ustimenko, M. Klisowski , On Noncommutative Cryptography with cubical multivariate maps of predictable density, In “Intelligent Computing’’ , Proceedings of the 2019 Computing Conference, Londone, Volume 2, Part of Advances in Intelligent Systems and Computing (AISC), volume 998, Springer, pp. 654-674.
8. V. Ustimenko, On desynchronised multivariate algorithms of El Gamal type for stable semigroups of affine Cremona group, Theoretical and Applied Cybersecurity, National Technical University of Ukraine "Igor Sikorsky Kiev Polytechnic Institute", Volume 1, No. 1, pp. 22-30 (2019).
9. V. Ustimenko, On the usage of postquantum protocols defined in terms of transformation semigroups and their homomophisms, Theoretical and Applied Cybersecurity, National Technical University of Ukraine "Igor Sikorsky Kiev Polytechnic Institute", Volume 1, No. 2, pp. 32-44 (2020).
10. R. Wagner, M. R. Magyarik, ``A Public-Key Cryptosystem Based on the Word N Problem", Advances in Cryptology, Proceedings of CRYPTO '84, Santa Barbara, California, USA, August 19-22, 1984.
11. D. N. Moldovyan, N. 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.

12. 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.
13. V. Shpilrain, A. Ushakov, 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
14. 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.
15. 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.
16. Zhenfu Cao (2012). New Directions of Modern Cryptography. Boca Raton: CRC Press, Taylor & Francis Group. ISBN 978-1-4665-0140-9.
17. Benjamin Fine, et. al. "Aspects of Non abelian Group Based Cryptography: A Survey and Open Problems". arXiv:1103.4093.
18. Alexei G. Myasnikov; Vladimir Shpilrain; Alexander Ushakov. Non-commutative Cryptography and Complexity of Group-theoretic Problems. Amer. Math Soc. 2011
19. Anshel, I., Anshel, M., Goldfeld, D.: An algebraic method for public-key cryptography. Math. Res.Lett. 6(3–4), 287–291 (1999).
20. Blackburn, S.R., Galbraith, S.D.: Cryptanalysis of two cryptosystems based on group actions. In: Advances in Cryptology—ASIACRYPT '99. Lecture Notes in Computer Science, vol. 1716, pp. 52–61. Springer, Berlin (1999).
21. C Ko, K.H., Lee, S.J., Cheon, J.H., Han, J.W., Kang, J.S., Park, C.: New public-key cryptosystem using braid groups. In: Advances in Cryptology—CRYPTO 2000, Santa Barbara, CA. Lecture Notes in Computer Science, vol. 1880, pp. 166–183. Springer, Berlin (2000)
22. Maze, G., Monico, C., Rosenthal, J.: Public key cryptography based on semigroup actions. Adv.Math. Commun. **1**(4), 489–507 (2007).
23. P.H. Kropholler, S.J. Pride , W.A.M. Othman K.B. Wong, P.C. Wong, Properties of certain semigroups and their potential as platforms for cryptosystems, Semigroup Forum (2010) 81: 172–186.
24. J. A. Lopez Ramos, J. Rosenthal, D. Schipani, R. Schnyder, Group key management based on semigroup actions, Journal of Algebra and its applications, vol.16 , 2019.
25. Gautam Kumar and Hemraj Saini, Novel Noncommutative Cryptography Scheme Using Extra Special Group, Security and Communication Networks ,Volume 2017, Article ID 9036382, 21 pages, https://doi.org/10.1155/2017/9036382.
26. V. A. Roman'kov, A nonlinear decomposition attack, Groups Complex. Cryptol. 8, No. 2 (2016), 197-207.
27. V. Roman'kov, An improved version of the AAG cryptographic protocol, Groups, Complex., Cryptol, 11, No. 1 (2019), 35-42.
28. A. Ben-Zvi, A. Kalka and B. Tsaban, Cryptanalysis via algebraic span, In: Shacham H. and Boldyreva A. (eds.) Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2018, Proceedings, Part I, Vol. 10991, 255{274, Springer, Cham (2018).
29. B. Tsaban, Polynomial-time solutions of computational problems in noncommutative-algebraic cryptography, J. Cryptol. 28, No. 3 (2015), 601-622.
30. V. Ustimenko, U. Romanczuk-Polubiec, A. Wroblewska, M. Polak, E. Zhupa, On the constructions of new symmetric ciphers based on non-bijective multivariate maps of prescribed degree,Security and Communication Networks, Volume 2019, Article ID 2137561, 15pages https://doi.org/10.1155/2019/2137561
31. Max Noether, Luigi Cremona , Mathematische Annalen 59, 1904, p. 1–19.

32. I.R. Shafarevich, On some in_nite dimension groups II, Izv. Akad. Nauk SSSR Ser. Mat., Volume 45, No. 1, pp. 214-226 (1981); Mathematics of the USSR-Izvestiya, Volume 18, No. 1, pp. 185-194 (1982).
33. Yu. Bodnarchuk, Every regular automorphism of the affine Cremona group is inner, Journal of Pure and Applied Algebra, Volume 157, Issue 1, pp. 115-119 (2001).
34. A. Ostafe, I. E. Shparlinski, On the degree growth in some polynomial dynamical systems and nonlinear pseudorandom number generators, Mathematics of Computation, Volume 79, No. 269, pp. 501-511 (2010).
35. A. Ostafe, Multivariate permutation polynomial systems and nonlinear pseudorandom number generators, Finite Fields and Their Applications, Vol. 16, 2010, Is.3, pp. 144-154.
36. V. Ustimenko, Coordinatisation of Trees and their Quotients, in the Voronoj's Impact on Modern Science, Kiev, Institute of Mathematics, 1998, vol. 2, 125-152.
37. V. Ustimenko, CRYPTIM:Graphs as Tools for Symmetric Encryption, Lecture Notes in Computer Science, Springer, LNCS 2227, Proceedings of AAECC-14 Symposium on Applied Algebra, Algebraic Algorithms and Error Correction Codes, November 2001, p. 278 - 286.
38. V. Ustimenko, On the graph based cryptography and symbolic computations, Serdica Journal of Computing, Proceedings of International Conference on Application of Computer Algebra, ACA-2006, Varna, N1 (2007).
39. V. Ustimenko, On the extremal graph theory for directed graphs and its crypto-graphical applications, In:T. Shaska, W.C. Huffman, D. Joener and V. Ustimenko, Advances in Coding Theory and Cryptography, Series on Coding and Cryptology, vol. 3, 181-200 (2007).
40. A. Wroblewska, On some properties of graph based public keys, Albanian Journal of Mathematics, Volume 2, No. 3, pp. 229-234 (2008)
41. V.Ustimenko, On inverse protocols of Post Quantum Cryptography based on pairs of noncommutative multivariate platforms used in tandem, ePrint Archive, 897, 2019.
42. J. Ding., J.E. Gower and D.S. Schmidt., *Multivariate Public Key Cryptosystems*, 260. Springer, Advances in Information Security, v. 25, (2006).
43. N. Koblitz, Algebraic aspects of cryptography, Springer (1998)., 206 P.
44. V. A. Ustimenko, V. A. (2013). On the extremal graph theory and symbolic computations. Dopov. Nac. akad. Nauk Ukr., 2013, No. 2, pp. 42-49.
45. V. Ustimenko, On semigroups of multiplicative Cremona transformations and new solutions of Post Quantum Cryptography, Cryptology ePrint Archive, 133, 2019.
46. V. Ustimenko, Maximality of affine group, hidden graph cryptosystem and graph’s stream ciphers, Journal of Algebra and Discrete Mathematics, 1, 2004, v.10, pp. 51-65.
47. V. Ustimenko, U. Romanczuk-Polubiec, A.Wroblewska, Expanding graphs of the Extremal Graph Theory and expanded platforms of Post Quantum Cryptography, Position Papers of the 2019 Federated Conference on Computer Science and Information Systems, FedCSIS 2019, Leipzig, Germany, September 1-4, 2019, Annals of Computer Science and Information Systems, No. 19, pp. 41{46 (2019).
48. F. Lazebnik, V. Ustimenko, Some Algebraic Constractions of Dense Graphs of Large Girth and of Large Size, DIMACS series in Discrete Mathematics and Theoretical Computer Science , v. 10, (1993) 75 - 93.
49. F. Lazebnik, V. Ustimenko, New Examples of Graphs without Small Cycles and of Large Size, Europ. J. of Combinatorics(1993) 14, PP. 445-460..
50. F. Lazebnik, V. Ustimenko, Explicit construction of graphs with arbitrary large girth and of large size, Discrete Applied Mathematics 60 (1995), 275-28.
51. F.Lazebnik, V. Ustimenko, A.J.Woldar, A new series of dense graphs of high girth, Bulletin of the AMS 32 (1) (1995), 73-79.
52. F.Lazebnik, V. Ustimenko and A. J.Woldar, A characterisation of the components of the graphs D(k; q), Discrete Mathematics,157 (1996), 271-283.

53. Jintai Ding and Joshua Deaton and Kurt Schmidt and Vishakha and Zheng Zhang, Cryptanalysis of The Lifted Unbalanced Oil Vinegar signature scheme, Cryptology ePrint Archive: Report 2019/1490.
54. Jintai Ding and Joshua Deaton and Vishakha and Bo-Yin Yang, The Nested Subset Differential Attack: A Practical Direct Attack Against LUOV which Forges a Signature within 210 Minutes, ePrint Archive: Report 2020/967.
55. Shuhei Nakamura and Yasuhiko Ikematsu and Yacheng Wang and Jintai Ding and Tsuyoshi Takagi. Shuhei Nakamura and Yasuhiko Ikematsu and Yacheng Wang and Jintai Ding and Tsuyoshi Takagi, New Complexity Estimation on the Rainbow-Band-Separation Attack, ePrint Archive: Report 2020/703