UDC 001.8

On Multivariate Algorithms of Digital Signatures Based on Maps of Unbounded Degree Acting on Secure El Gamal Type Mode

V. O. Ustimenko

Royal Holloway University of London, UK,
Institute of Telecommunications and Global Information Space, Kyiv, Ukraine

Abstract

Multivariate cryptography studies applications of endomorphisms of $K[x_1\ x_2,\ \ldots,\ x_n]$ where K is a finite commutative ring given in the standard form $x_i \rightarrow f_1\ (x_1, x_2, \ldots, x_n),\ i=1, 2, \ldots, n.$ The importance of this direction for the constructions of multivariate digital signatures systems is well known. Close attention of researchers directed towards studies of perspectives of efficient quadratic unbalanced rainbow oil and vinegar system (RUOV) presented for NIST postquantum certification. Various cryptanalytic studies of these signature systems were completed. During Third Round of NIST standardisation projects ROUV digital signature system were rejected. Recently some options to seriously modify theses algorithms as well as all multivariate signature systems which alow to avoid already known attacks were suggested. One of the modifications is to use protocol of noncommutative multivariate cryptography based on platform of endomorphisms of degree 2 and 3. The secure protocol allows safe transfer of quadratic multivariate map from one correspondent to another. So the quadratic map developed for digital signature scheme can be used in a private mode. This scheme requires periodic usage of the protocol with the change of generators and the modification of quadratic multivariate maps. Other modification suggests combination of multivariate map of unbounded degree of size $O(n)$ and density of each f_i of size $O(1)$. The resulting map F in its standard form is given as the public rule. We suggest the usage of the last algorithm on the secure El Gamal mode. It means that correspondents use protocols of Noncommutative Cryptography with two multivariate platforms to elaborate safely a collision endomorphism $G: x_i \rightarrow g_i$ of linear unbounded degree such that densities of each g_i are of size $O(n^2)$. One of correspondents generates mentioned above F and sends $F+G$ to his/her partner.

The security of the protocol and entire digital signature scheme rests on the complexity of NP hard word problem of finding decomposition of given endomorphism G of $K[x_1,x_2,\ldots,x_n]$ into composition of given generators ${}^1G, {}^2G, \ldots {}^tG, t>1$ of the semigroup of $End(K[x_1,x_2,\ldots,x_n])$. Differently from the usage of quadratic map on El Gamal mode the case of unbounded degree allows single usage of the protocol because the task to approximate F via interception of hashed messages and corresponding signatures is unfeasible in this case.

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

Funding: This research is supported by British Academy Fellowship for Researchers under Risk 2022

1. Introduction: On Multivariate Digital Signature Schemes of Post Quantum Cryptography

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 for new public key algorithms. In March 2019 NIST published a list of candidates qualified to the second round of the standardisation process. The cryptosystems are designed for tasks of information exchange and digital signatures. In July 2020 the list of algorithms selected for the Third Round of NIST competition has been published.

In the case of digital signatures preliminary analysis indicates some advantages of algorithms based on quadratic public rules of Multivariate Cryptography. These systems provide the smallest sizes of the used hashed messages and digital signatures.

Cryptanalytic studies of perspectives of quadratic rainbow oil and vinegar systems and LUOV have their own history. Papers [1] and [2] investigates various options of attacks on the systems. These studies show some advantages of ROUV in comparison with LOUV. So the ROUV but not LOUV was selected for the Third ROUND of NIST competition. Anyway during this round due to cryptanalytical studies (see [35]) these digital signatures were regicted. In July 2022 the firs four winners of NIST competition were announced. All of them are developed in terms of Lattice based Cryptography, Noteworthy that other 4 directions of Postquantum Cryptography and Noncommutative Cryptography are still promising to bring scure instruments of PQC because they use well known NP hard problems in their foundations.

So, we start the search for the possible modifications of general multivariate digital signature schemes based on quadratic public rules such that attacks described in [1] and [2] (in the case of ROUV and LOUV) will be eliminated. Recall that classical multivariate signature system is based on public quadratic map P' of vector space F_q^m onto F_q^n of kind $P'=T_1PT_2$ where the map P is given by rule $x_i \rightarrow f_i(x_1, x_2, \dots, x_m)$, $i=1,2,\dots,n$ defined by quadratic polynomials f_i and bijective affine transformations T_1, T_2 of spaces F_q^m and F_q^n. Users Alice and Bob use selected encryption function F and hash function which creates hash vector $H(c)$ from vector space F_q^m. Alice writes the plaintext p and computes corresponding ciphertext c. The knowledge of the decomposition T_1PT_2 and private algorithm to compute value of P^{-1} in a given point allows Alice to compute some reimage $P'^{-1}(H(c))=(u_1, u_2, \dots, u_n)=u$ of $H(c)$ (so called *signature)* and to send u to Bob via an open channel. He checks the identity $P'(u)=v(c)$. This is his confirmation that ciphertext is sent by Alice. Finally he decrypts. The security of presented above algorithm rests on the complexity of the problem of computation of reimage for non-bijective P'. This is a well known general *NP* hard problem.

Noteworthy that in the case of Unbalanced Oil and Vinegar the partition of variables into two parts of ''oil'' and ''vinegar'' unknowns and special form of P allows Alice to compute element from $P^{-1}(H(c))$. She uses a specialisation of ''vinegar'' variables via substitution of pseudorandom parameters, such specialisation reduces the search for reimage to solving the system of linear equations.

We start the search for the options to modify general digital scheme of multivariate cryptography, which eliminate attacks investigated in [1] and [2]. We suggest the following three modifications.

The first of them is based on the idea that the map P' is not given publicly [3]. Correspondents execute the protocol of non-commutative cryptography based on the platform of stable multivariate transformations of degree 2 in n variables (see [5]). They elaborate the quadratic collision map G from the vector space F_q^m onto F_q^n. The security of this protocol rests on the complexity of finding the decomposition of nonlinear element of the subsemigroup of endomorphisms of $F_q[x_1, x_2, \dots, x_n]$ into the composition of its given generators. Postquantum algorithm to solve this problem in polynomial time is unknown. Secondly one of correspondents selects quadratic map P' and sends $G+P'$ to his/her partner. So correspondents can use digital signature system defined by P' which is unknown to adversary. The postquantum protocol has to be used periodically with different data. Users can change maps T_1, T_2, *internal parameters of* P keeping the class of chosen schemes as well as generators of stable semigroups of degree 2.

In the second modification the map T_1 has to be changed for a composition ST_1 of $T_1$with a bijective map S of kind $x_i \rightarrow s_i(x_1, x_2, \dots, x_n)$ of unbounded linear degree $>m$ such that each s_i has density $O(1)$ [4]. Thus $P'=ST_1PT_2$ is a map of degree $O(n)$ and density $O(n^2)$. The map P' of the second scheme is given to the public. Attacks investigated in [1] and [2] are eliminated because the degree of P' is not bounded by a small constant.

The third scheme, which is introduced in this paper, is based on the usage of multivariate

protocol of non-commutative cryptography with two distinct platforms which allows to elaborate collision map G of unbounded degree of size $O(n)$ and density of size $O(n^2)$ (see [5]). On receiving the collision map one of correspondents sends $G+P'$ to his/her partner. The protocol can be used only once because the adversary is unable to approximate unknown P' of unbounded degree via interception of hash vectors and corresponding signatures.

Several multivariate digital signature schemes (m.d.s.s.) with the usage of protocols of non-commutative cryptography as above were integrated with the state electronic management networks for the tasks of telemedicine and e-governing in Ukraine. These m.d.s.s. are used for the authentication of users. Some of them will be presented for the standardisation and certification processes conducted by the State Service of Special Communication and Information Protection of Ukraine (Kyiv).

Section 2 is dedicated to the definitions of the most important semigroups in Noncommutative Multivariate Cryptography such as formal and affine Cremona semigroups and their reduced version.

In Section 3 we consider elements of theory of linguistic graphs. Section 4 is dedicated to the usage of linguistic graphs for the construction of stable subsemigroups and elements of formal Cremona groups of linear degree and prescribed density.

We also presented the modification of quadratic m. d. s. s. based on reduced endomorphism of $F_q[x_1, x_2, \ldots, x_n]$ of linear degree and density $O(n^2)$. In Section 5 we consider the concept of Unbalanced Oil and Vinegar signature systems.

Section 6 is dedicated to the abstract schemes of protocol of multivariate non-commutative cryptography which allows correspondents to elaborate common collision multivariate endomorphism of linear degree and polynomial density. The scheme uses two platforms which are subsemigroups of formal Cremona semigroup $E_n(F_q)$ of all endomorphisms of $F_q[x_1, x_2, \ldots, x_n]$ and their homomorphic images. One of them can be a large stable subsemigroup S of degree 2, i.e subgroup formed by quadratic endomorphisms.

The second platform is a semigroup of Eulerian transformation, i. e. endomorphisms moving single variable x_i into monomial term.

Protocols based on subsemigroups of Eulerian transformations is considered in [8],[5]. 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 [9] for the first application of word problem in the case of group).

In Section 7 we consider implementation of general scheme of the protocol of Section 6. We use stable and Eulerian platforms based on special linguisti graphs defined over commutative ring and its multiplicative group. This section presents the algorithm of safe transition of public key m.d. s. s. of section 4 on the private mode.

Section 8 contains conclusive remarks and complexity estimates for m.d.s.s. of Sections 4 and 7.

Noteworthy that property of stability is very restrictive because the composition of two randomly chosen quadratic transformations has degree 4 with probability close to 1. The observation of known explicit constructions are given in [5], [6], [7], [10].

Thus we have been working in the area of intersection of Multivariate and *Non-commutative cryptography* which 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 cryptographic schemes defined in terms of wide classes of semigroups and their implementations for chosen semigroup families (so called platform semigroups.

2 On Formal Cremona Group, Reduced Multivariate Transformation of Finite Vector Spaces and Eulerian Transformations

2.1. Formal and affine Cremona groups heading

Let $K[x_1, x_2, \ldots, x_n]$ be commutive ring of all polynomials in variables $x_1, x_2, \ldots, x_n$ defined over a commutive ring K. Each endomorphism $F \in E_n(K)$ is uniquely determined by its values on formal generators x_i, $i=1,2,\ldots, n$. 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 and 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 [30] 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 [31], [32]).

We refer to infinite $E_n(K)$ as *formal affine Cremona semigroup*. Density of the map F is the maximal number of monomial terms in f_i, $i=1,2,\dots,n$.2. 1.

2.2. Reduced formal Cremona group

Let us consider the case $K=F_q$. Noteworthy that $x^q=x$ for each $x\in F_q$ and $x^{q-1}=1$ for $x\neq 0$ and $x^{q-1}=0$ for $x=0$. So $x^m=x^{m \bmod q-1}$ where m *modulo* $q-1$ is different from 0. We define $x^0=1$ for $x\neq 0$ and $x^0=0$ for $x=0$. We introduce m' as $m \bmod q-1$.

For the monomial term $ax_1^{m(1)}x_2^{m(2)}\dots x_t^{m(t)}$ we introduce its reduced form as $ax_1^{'m(1)}x_2^{'m(2)}\dots x_t^{'m(t)}$. For $f\in K[x_1, x_2,\dots, x_m]$ we define $'f$ as linear combination of reduced form of monomial terms of f.

Let us consider the totality $'E_n(F_q)$ of formal rules $'F$ of kind $x_i\to' f_i(x_1, x_2,\dots, x_n)$, $i=1,2,\dots,n$, $f_i\in K[x_1, x_2,\dots, x_n]$. We define $'F'G$ *as natural superposition* of $'F$ and $'G$. We refer to $'E_n(F_q)$ as *reduced formal Cremona semigroup of rank n.*

The map χ_n sending $x_i\to f_i$, $i=1,2,\dots n$ to $x_i\to f'_i$, $i=1,2,\dots,n$ is a homomorphism of $E_n(F_q)$ onto $'E_n(F_q)$. Noteworthy that $E_n(F_q)$ is an infinite semigroup but $'E_n(F_q)$ is the finite one. We introduce $'K[x_1, x_2,\dots,x_n]$ as totality of $'f$ such that $f\in K[x_1, x_2,\dots,x_n]$.

2.3. Eulerian semigroups

Let K be a finite commutative ring with the unit such that multiplicative group K^* of regular elemments of this ring contains at least 2 elemments. We take Cartesian power ${}^nE(K)=(K^*)^n$ and consider an Eulerian semigroup ${}^nES(K)$ of transformations of kind

$$\begin{aligned} x_1 &\to \mu_1 x_1^{a(1,1)} x_2^{a(1,2)} \dots x_m^{a(1,n)},\\ x_2 &\to \mu_2 x_1^{a(2,1)} x_2^{a(2,2)} \dots x_m^{a(2,n)}, \qquad (1)\\ &\dots\\ x_m &\to \mu_n x_1^{a(n,1)} x_2^{a(n,2)} \dots x_m^{a(n,n)}, \end{aligned}$$

where $a(i,j)$ are elements of arithmetic ring Z_d, $d=|K^*|$, $\mu_i\in K^*$.

Let ${}^nEG(K)$ stand for Eulerian group of invertible transformations from ${}^nES(K)$. Simple example of an element from ${}^nEG(K)$ is a written above transformation where $a(i,j)=1$ for $i\neq j$ or $i=j=1$, and $a(j,j)=2$ for $j\geq 2$. It is easy to see that the group of monomial linear transformations M_n is a subgroup of ${}^nEG(K)$. So semigroup ${}^nES(K)$ is a highly noncommutative algebraic system. Each element from ${}^nES(K)$ can be considered as transformation of a free module K^n.

Let π and δ be two permutations on the set $\{1,2,\dots, n\}$. Let us consider a transformation of $(K^*)^n$, $K=Z_m$ or $K=F_q$ and $d=|K^*|$. We define transformation ${}^AJG(\pi, \delta)$, where A is triangular matrix with positive integer entries $0\leq a(i,j)\leq d$, $i\geq d$ defined by the following closed formula.

$$\begin{aligned} &y_{\pi(1)}=\mu_1 x_{\delta(1)}^{a(1,1)}\\ &y_{\pi(2)}=\mu_2 x_{\delta(1)}^{a(2,1)} x_{\delta(2)}^{a(2,2)}\\ &\dots\\ &y_{\pi(n)}=\mu_n x_{\delta(1)}^{a(n,1)} x_{\delta(2)}^{a(n,2)} \dots x_{\delta(n)}^{a(n,n)} \end{aligned}$$

where $(a(1,1),d)=1$, $(a(2,2),d)=1,\dots,(a(n,n),d)=1$.

We refer to ${}^AJG(\pi, \delta)$ as Jordan - Gauss multiplicative transformation or simply JG element. It is an invertible element of ${}^nES(K)$ with the inverse of kind ${}^BJG(\delta, \pi)$ such that $a(i,i)b(i,i)=1 \pmod d$. Notice that in the case $K=Z_m$ straightforward process of computation the inverse of JG element is connected to the factorization problem of integer m. If $n=1$ and m is a product of two large primes p and q the complexity of the problem is used in RSA public key algorithm. The idea to use composition of JG elements or their generalisations with injective maps *of* K^n into K^n was used in [33] ($K=Z_m$) and [34] ($K=F_q$).

We say that τ is *a tame Eulerian element* over Z_m or F_q. if it is a composition of several Jordan Gauss multiplicative maps over commutative ring or field respectively. It is clear that τ sends variable x_i to a certain monomial term. The decomposition of τ into product of Jordan Gauss transformation allows us to find the solution of equations $\tau(x)=b$ for x from $(Z_m^*)^n$ or $(F^*_q)^m$. So tame Eulerian transformations over Z_m or F_q. are special elements of ${}^nEG(Z_m)$ or ${}^nEG(F_q)$ respectively.

We refer to elements of ${}^nES(K)$ as multiplicative Cremona element. Assume that the order of K is a constant. As it follows from the definition the computation of the value of element from ${}^nES(K)$ on the given element of K^n is estimated by $O(n^2)$. The product of two multiplicative Cremona elements can be computed in time $O(n^4)$.

We are not discussing here the complexity of computing the inverse for general element $g \epsilon {}^nEG(K)$ on Turing machine or Quantum computer and the problem of finding the inverse for computationally tame Eulerian elements.

Remark 2.1. Let G be a subgroup of ${}^nEG(K)$ generated by Jordan-Gauss elements $g_1, g_2, ..., g_t$. The *word problem* of finding the decomposition of $g \epsilon G$ into product of generator g_i is a difficult one, i. e. polynomial algorithms to solve it with Turing machine or Quantum Computer are unknown. If the word problem is solved and the inverses of g_i is computable then the inverse of g is determined. Notice that if $n=1$, $K=Z_m$, $m=pq$ where p and q are large primes and G is generated by $g_1=_M g_1^a$ the problem is unsolvable by Turing machine but it can be solved with the usage of Quantum Computer.

3. Some Subsemigroup and Subgroups Defined via Linguistic Graphs over Commutative Rings and Groups.

3.1. The case of rings.

Let us assume that $K=F_q$ and consider some graph based constructions of semigroups of formal Cremona semigroup $'E_n(K)$. Constructions of this section are very similar to schemes of [5] which define some subsemigroups of $E_n(K)$.

Element $x_1 \rightarrow 'f_i(x_1, x_2, ..., f_n)$, $i=1,2,...,n$ of $'E_n(K)$ will be identified with the tuple of elements $('f_1, 'f_2, ..., 'f_n)$, $'f_i \epsilon 'K[x_1, x_2, ..., x_n]$ when it is convenient.

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

Let us assume that H_t of written above $u \epsilon {}^sBS'(K)$ is automorphism of $K[x_1, x_2, ..., x_s]$. So its inverse is well defined. Then we can consider a reverse linguistic string $Rev(u)= (H_{t-1}(H_t^{-1}), G_{t-2}(H_t^{-1}), G_{t-3},(H_t^{-1}), H_{t-4}(H_t^{-1}),H_{t-5}^{-1}(H_t), ...,G_2(H_t^{-1}), G_1(H_t^{-1}), H_0(H_t^{-1}), H_t^{-1})$ 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 $x=(x_1, x_2, ..., x_s, x_{s+1}, x_{s+2}, ..., x_{s+m})$ is incident to line $y=[y_1, y_2, ..., y_r, y_{r+1}, y_{r+2}, ..., y_{r+m}]$ if and only if the following relations hold

$a_1x_{s+1}+b_1y_{r+1}=f_1 (x_1, x_2 ,... , x_s, y_1, y_2, ... , y_r)$

$a_2x_{s+2}+b_2y_{r+2}=f_2 (x_1, x_2 ,... , x_s, x_{s+1}, y_1, y_2, ... , y_r, y_{r+1})$

...

$a_mx_{s+m}+b_my_{r+m}=f_m (x_1, x_2 ,... , x_s, x_{s+1},..., x_{s+m}, y_1, y_2, ... , y_r, y_{r+1}, ..., y_{r+m})$

where a_j, and b_j , $j=1,2,,,,m$ are distinct from zero, and f_j are multivariate polynomials with coefficients from K. Brackets and parenthesis allow us to distinguish points from lines.

Noteworthy that polynomials f_i can be changed for $'f_i \epsilon 'K[x_1, x_2, ..., x_s]$.

The colour $\rho(x)=\rho((x))$ $(\rho(y)=\rho([y]))$ of point x (line $[y]$) 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 $\rho((x))=(x_1, x_2 ,... , x_s)$ for $(x)=(x_1, x_2 ,... , x_{s+m})$ and $\rho([y])=(y_1, y_2, ... , y_r)$ for $[y]=[y_1, y_2, ... , y_{r+m}]$ as the colour of the point and the colour of the line respectively. For each $b \epsilon K^r$ and $p=(p_1, p_2 ,... , p_{s+m})$ 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 $l=[l_1, l_2 ,... , l_{r+m}]$ there is the unique neighbour of the line $(p)= N_c([l])=N([l],b)$ with the colour c. We refer to the operator of taking the neighbour of vertex in accordance with the chosen colour as sliding operator. On the sets P

and L of points and lines of linguistic graph we define jump operators ${}^{1}J={}^{1}J_b(p)=J((p),b)=(b_1, b_2,\dots,b_s, p_1, p_2, \dots, p_{s+m})$, where $(b_1, b_2,\dots,b_s)\epsilon K^s$ and ${}^{2}J={}^{2}J_b([l])=J([l],b)=[b_1, b_2,\dots,b_r, l_1, l_2, \dots, l_{r+m}]$, 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 mentioned equations with coefficients 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 semigroup ${}^{s}BS'(K)$.

We take the 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

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

Let $({}^{t}x)$ 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 reduced 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 .*

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

3.2 The case of Linguistic Graphs over Groups.

Similarly to the case of commutative ring we introduce a linguistic graph $I=\Gamma(G)$ over abelian group G defined as a bipartite graph with a point set $P=P_{s,m}=G^{s+m}$ and a line set $L=L_{r,m}=G^{r+m}$ as a 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 an 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

$$x_{s+1}/_1 y_{r+1}= a_1 w_1 (x_1, x_2, \dots, x_s, y_1, y_2, \dots, y_r)$$

$$x_{s+2}/_2 y_{r+2}= a_2 w_2 (x_1, x_2, \dots, x_s, x_{s+1}, y_1, y_2, \dots, y_r, y_{r+1})$$

$$\dots$$

$$x_{s+m}/y_{r+m}=a_m w_m (x_1, x_2, \dots, x_s, x_{s+1},\dots, x_{s+m}, y_1, y_2, \dots, y_r, y_{r+1}, \dots, y_{r+m})$$

where a_j, $j=1,2,\dots, m$ are elements of G and w_i are words in characters x_i and y_j from G. Brackets and parenthesis allow us to distinguish points from lines similarly to the case of linguistic graphs over commutative rings.

We define *colours* $\rho((p))$ and $\rho([l])$ of the point (p) and the line $[l]$ as the tuple of their first coordinates of kind $\boldsymbol{a}=(p_1, p_2, \dots, p_s)$ or $\boldsymbol{a}=(l_1, l_2, \dots, l_r)$ and introduce well defined operator $N(v, a)$ of computing the neighbour of vertex v of colour $a\epsilon G^s$or $a\epsilon G^r$. Similarly to the case of linguistic graph over commutative *ring* we define jump operator $J(p, a)$, $a\epsilon G^s$ on partition set P and $J(l,a)$, $a\epsilon G^r$ on partion set L by conditions $J(p,a)=(a_1, a_2, \dots a_s, p_{1+s}, p_{2+s}, \dots, p_{s+n})$ and $\rho(J(l,a))=[a_1, a_2, \dots a_r, p_{1+r}, p_{2+r}, \dots, p_{r+m}]$. We also consider symplectic and linguistic homomorphisms of linguistic graphs over groups defined similarly to the case of commutative rings.

Let us use various linguistic graphs with $r=s$ over the multiplicative group $G=K^*$ and subsemigroup of monomial strings ${}^{s}BS(K^*)$ from ${}^{s}BS(K)$, $0<s<n$, $0<r<n$, $s=r$ for generation of pairs of mutually inverse elements of ${}^{n}EG(K)$. Let us consider the homomorphism of the semigroup ${}^{s}BS_r(K^*)$ into Eulerian semigroup ${}^{n}ES(K)$, $n=s+m$ defined in terms of linguistic graph $I=I(K^*)$ over K^* of type (s,r,m).

Let N_a be an operator of taking neighbour of given vertex with the colour a in the graph I. Let us consider the commutative group $K'=K^*[x_1, x_2,\dots,x_s, x_{s+1}, \dots, x_n]$ of monomial terms of $K[x_1, x_2,\dots,x_s, x_{s+1}, \dots, x_n]$ with coefficients from K^* and linguistic graphs I' over group K' defined by the same equations with I but over the larger commutative group K'. We assume that N_a and N'_a are operators of taking neighbour of given vertex with the colour a in the graph I and I' respectively. Let us consider the string of kind $v=(x_1, x_2, \dots, x_s, x_{s+1}, x_{s+2}, \dots, x_{s+m})$ from K^{s+m} *(or* $(K')^{s+m}$ *)*. We define jump operator ${}^{s}J(v, a)$, $a=(y_1, y_2, \dots, y_s)$ moving v to $(y_1, y_2, \dots, y_t, x_{s+1}, x_{s+2}, \dots, x_{s+m})$ from K^{t+m}.

We consider an infinite graph $I'(K')$, $n=m+s$ with partition sets $P'=(K')^{m+s}$ and $L'=(K')^{m+r}$. After that we take a string $u=(H_0, G_1, G_2, H_3, H_4, G_5, G_6,\dots, H_{t-1}, H_t)$ from ${}^{s}BS_r(K^*)$ and the point $(x)=(x_1, x_2,\dots, x_n)$ formed by generic elements of K'. This data defines uniquely a skating chain

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

Let $({}^tx)$be the tuple $(H_t, F_2, F_3,\ldots,F_n)$ where $F_i \epsilon K[x_1, x_2,\ldots, x_n]$. We define ${}^1\Psi(u)$ as the map $(x_1, x_2,\ldots, x_n)\rightarrow(H_t, F_2, F_3,\ldots,F_n)$ and refer to it *as chain transition of point variety*. The statement written below follows from the definition of the map.

Lemma 2. *The map* $\psi={}^I\psi$**:** ${}^sBS(K^*)\rightarrow {}^nES(K)$ *is a homomorphism of semigroups.*

We refer to ${}^I\psi({}^sBS_r(K^*))={}^ICT(K^*)$ as a *chain transitions semigroup* of linguistic graph $I(K^*)$ over K^* and to map ψ as *multiplicative linguistic compression map*.

4. Stable Subsemigroups in '$E_n(F_q)$ of Arbitrary Degree and Elements of Unbounded Degree and Bounded Density

4.1. Stable subsemihroup and graphs

We say that subsemigroup of S_n *of* $E_n(K)$ or $'E_n(F_q)$ is stable if maximal degree of elements from S_n is d, where d is some constant.

Families of stable subsemigroups of $E_n(K)$ in terms of Double Schubert Graphs are constructed in [7]. In this section we introduce similar constructions for the case of $E_n(F_q)$.

Graph $DS(k,K)$ is defined 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 $x=(x_1, x_2, \ldots, x_k, x_{11}, x_{12}, \ldots, x_{kk})$ and $LS=K^{k(k+1)}$ consisting of lines which are tuples of kind $y=[y_1, y_2, \ldots, y_k, y_{11}, y_{12}, \ldots, y_{kk}]$, where x is incident to y, if and only if $x_{ij}-y_{ij}=x_i y_j$ for $i=1, 2,\ldots, k$ and $j=1, 2,\ldots, k$. 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 define the colour of point $x=(x_1, x_2, \ldots, x_k, x_{11}, x_{12}, \ldots, x_{kk})$ from PS as a tuple$(x_1, x_2, \ldots, x_k)$ and the colour of a line $y=[y_1, y_2, \ldots, y_k, y_{11}, y_{12}, \ldots, y_{kk}]$ as a tuple $(y_1, y_2, \ldots, y_k)$. For each vertex v of $DS(k, K)$, there is the unique neighbour $y=N_a(v)$ of a given colour $a=(a_1, a_2, \ldots, a_k)$. It means that graphs $DS(k, K)$ form a family of linguistic graphs.

In the case of $K=F_q$ the subsemigroup ${}^kY'(d, K)$ of ${}^kBS'(K)$ consists of strings $u=(H_0, G_1, G_2, H_3, H_4, G_5, G_6,\ldots, H_{t-1}, H_t)$ from ${}^sBS'(K)$ such that maximum of parameters $deg(H_0)+deg(G_1)$, $deg(G_2)+deg(H_3)$, $deg(H_4)+deg(G_5)$,

$deg(G_6)+deg(H_7), \ldots, deg(G_{t-2})+deg(H_{t-1}), deg(H_t)=1$ is equal to constant d, $1<d<(q-1)n$.

Theorem 1. *Let I(K) be an incidence relation of Double Schubert graph DS(k, K) defined over finite field K. Then* ${}^I\psi({}^kY'(d, K))={}^kU'(d,K)$ *forms a family of stable semigroups of degree d in* $'E_n(K)$.

The proof is based on the fact that the chain transition u from ${}^kU'(d, K)$ moves $x_{i,j}$ into expression $x_{i,j}+T(u)$, where $T(u)$ is a linear combination of products $'f\epsilon K[x_1, x_2,\ldots, x_k]$, $g\epsilon K[y_1, y_2,\ldots, y_k]$ where $deg(f)+deg(g)\leq d$.

New semigroup ${}^kU(d, K)$ consists of transformations of a free module K^t, $t=(k+1)k$. If $d=2$ then ${}^kU(d, K)$ contains semigroups of quadratic transformations defined in [6].

Let J be subset of Cartesian square of $M=\{I,2,\ldots,k\}$. 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* $DS_J(k,K)$.

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

Remark. *If* $d<q-1$ *then groups* ${}^kU'_J(d,K)$ *and* ${}^kU'_J(d,K)$ (${}^kU(d,K)$ *and* ${}^kU'(d,K)$) *are isomorphic.*

Recall that *density* of element f of $K[x_1, x_2,\ldots, x_n]$ *(or* $'K[x_1, x_2,\ldots, x_n]$, $K=F_q$) is its number $den(f)$ of monomial terms. The *density* $den(F)$ of a map $F: x_i \rightarrow f_i(x_1, x_2,\ldots, x_n)$, $i=1,2,\ldots,n$ is a maximum of $den(f_i)$. .

Lemma 3. *Let u be the string* $(H_0, G_1, G_2, H_3, H_4, G_5, G_6,\ldots, H_{t-1}, H_t)$ *from* ${}^sBS(K)$ (*or* ${}^sBS'(K)$, $K=F_q$) *such that maximum of parameters* $deg(H_0)+deg(G_1)$, $deg(G_2)+deg(H_3)$, $deg(H_4)+deg(G_5)$, $deg(G_6)+deg(H_7), \ldots, deg(G_{t-2})+deg(H_{t-1})$, $deg(H_t)$ *is a constant d. Then degree of* ${}^{I(J,K)}\psi(u)$ *is bounded by d.*

Lemma 4. *Let u be the string* $(H_0, G_1, G_2, H_3, H_4, G_5, G_6,\ldots, H_{t-1}, H_t)$ *from* ${}^sBS(K)$ *(or* ${}^sBS'(K)$, $K=F_q$) *such that maximum of parameters* $den(H_0)den(G_1)$, $den(G_2)den(H_3)$,

$den(H_4)den(G_5)$, $den(G_6)den(H_7)$, …, $den(G_{t-2})den(H_{t-1})$, $den(H_t)$ is a constant d. Then density of ${}^{I(J,K)}\psi(u)$ is bounded by d+1.

Let u be a string from ${}^{s}BS'(K)$, $K=F_q$ satisfying Lemma 2 such that H_t is a composition DT of the map D of kind $x_i \to \lambda_i x_{i+1}^{\alpha(i)}$, $i=1,2,\ldots, s-1$, $x_s = \lambda_s x_1^{\alpha(s)}$ where $(\alpha(i), q-1)=1$, $\lambda_i \neq 0$ for $i=1,2,\ldots,s$ and element $T \in AGL_s(K)$ with the density d.Then density of invertible element ${}^{I(J,K)}\psi(u)=G$ is bounded by d and degree $\leq s(q-1)$. Let $L=\{1. 2,\ldots s\} \cup J$ be set of indices for $x_1, x_2,\ldots,x_s,, x_{ij}, , (i,j) \in J$ and π be a permutation on L. We consider an element H of $'E_m(F_q)$, $m=|J|+s$ of kind $x_i \to \mu_i x_{\pi(i)}^{\beta(i)}$, $i=1,2,\ldots s$.

Lemma 5.

An element $F_J=HG \in 'E_m(F_q)$ has the density bounded by d and the order at least s.

It is easy to choose string u and transformations D and H such that degree of G is of kind $\gamma m(q-1)$ wher γ is a constant $0<\gamma\leq 1$.

4.2. On the graph based m.d.s.s. of linear degree and density $O(n^2)$

Alice selects a finite field and sequence of pairs (s_m, J_m), $s_m>1$, $|J_m|<(s_m)^2$ such that $|s_m+|J_m|=m$ and generates defined above transformation $F_J=(d_1(x_1, x_2, \ldots, x_m), d_2(x_1, x_2, \ldots, x_m),\ldots, d_m(x_1, x_2, \ldots, x_m)) \in 'E_m(F_q)$. She selects a public rule of kind $P'=T_1PT_2$ written in the form $x_i \to Q_i(x_1, x_2,\ldots,x_m)$, $i=1,2,\ldots,n$, where $n=n(m)$. Alice computes composition F_J and P', i.e standard form of $x_i \to Q_i(d_1(x_1, x_2, \ldots, x_m), d_2(x_1, x_2, \ldots, x_m),\ldots, d_m(x_1, x_2, \ldots, x_m))=R_1(x_1, x_2, \ldots x_m)$, $i=1,2,\ldots n$. in fact she computes R_i as elements of commutative ring $'F_q[x_1, x_2,\ldots,x_m]$ of reduced multivariate polynomials.

Alice uses the nature of $F_J=HG$, where G is graph based transformations. She computes G^{m-1} as ${}^{I(J,K)}\psi(Rev(u))$ and H^{-1} in an obvious way. The knowledge of decomposition $G^{-1}H^{-1}$ for $(F_J)^{-1}$ and decomposition T_1PT_2 of P' allows Alice to create a signature efficiently.

Remark 4.2. We implement this m. d. s. s. with $s_m=[m^{1/2}]'$ where [,]' is the ceiling function.

5. On Examples of Multivariate Digital Signatures Schemes.

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

$${}^1p(x_1,x_2,\ldots,x_n) = {}^1p_{i,j}\cdot x_ix_j + {}^1p_i\cdot x_i + {}^1p_0$$
$${}^2p(x_1,x_2,\ldots,x_n) = {}^2p_{i,j}\cdot x_ix_j + {}^2p_i\cdot x_i + {}^2p_0$$
$$\ldots$$
$${}^mp(x_1,x_2,\ldots,x_n) = {}^mp_{i,j}\cdot x_ix_j + {}^mp_i\cdot x_i + {}^mp_0$$

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

The quadratic multivariate cryptography map consists of two bijective affine transformations, S and T of dimensions n and m, and a quadratic element P' of kind $x_i \to {}^ip$ of formal Cremona group, where ${}^ip$ are written above elements of $K[x_1, x_2,\ldots,x_n]$.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 key which is 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 ${}^ip$ 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, γ_{ijk}, λ_{ijk}, ς_{ij}, ς'_{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*, 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 $m=O(n)$. 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 ${}^jp(x_1,x_2 , \ldots , x_n)$, $j=1,2, \ldots,m$ and $x_{n+1}, x_{n+2},\ldots,x_k$ are formal variables.

6. Multivariate Protocol for Stable Cremona Generators and Eulerian Systems with Growing Periods.

6.1. The Case of Stable Generators.

Recall that a monogenic semigroup or a cyclic semigroup *S* is a semigroup generated by a single element, which is called a generating element of semigroup *S*. Now we shall determine the general structure of monogenic semigroups. Let $S = \{ a, a^2, a^3, \ldots\}$ be a monogenic semigroup with a generating element *a*. It is a well known fact that all infinite monogenic semigroups *S* are isomorphic to $(N; +)$. In the case of finite cardinality of *S*, there exists natural numbers *k* and *l* such that $k \neq l$ and $a^k = a^l$. Let *m* be the smallest natural number such that $a^m = a^{m=x}$ for some $x > 0$ and let *r* be the smallest natural number such that $a^m = a^{jm+r}$. Then we call *m* the index of *a* denoted by $m = ind(a)$ and *r* the *period* of *a* denoted by $r = per(a)$. All finite monogenic semigroups S are determined up to isomorphism by the height *m* and the period *r* of their generator.

Let ${}^iZ= \{ {}^ig_1 , {}^ig_2, \ldots , {}^ig_t\}$ 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) ${}^iSZ= \langle {}^ig_1, {}^ig_2, \ldots , {}^ig_t\rangle$ are stable semigroups of degree *d*.

(3) For each *j* period of elements ${}^ig_j$, $i=1,2,\ldots,t$ tends to infinity.

Proposition 2.(see [3] and further references). *For each commutative ring K, sequence n(i)=i ,i≥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 ${}^iZ$ 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 ${}^iZ' =\{ {}^ig'_1, {}^ig'_2, \ldots , {}^ig'_t\}$ *is* a *quotient of stable Cremona system* ${}^iZ$ if the rule $\varphi({}^ig_j)= {}^ig'_j$, $j=1, 2,\ldots, t$ defines computationally tame homomorphism of semigroup ${}^iSZ$ onto ${}^iSZ^1$, i. e. a 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.*

Theorem 2 (see [6] and further references**).** *For each finite commutative ring K and natural numbers d, d>0 and t, t ≥ 2 there is an increasing sequence n(i) of natural numbers and noncommutative system of stable Cremona generators* ${}^iZ =\{ {}^ig_1, {}^ig_2, \ldots , {}^ig_t\}$ *of degree d and rank t which has a regular quotient* ${}^iZ'$.

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

Word *tahoma* stands here for the abbreviation of ''tame homomorphism''.

Noteworhy that Tahoma is a name of the mountain in North America and a popular shrift in a 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 ${}^1E$ from $EZ_{n(i)}(K)$ and $EZ'_{m(i)}(K)$. Alice takes generators $g_1 , g_{2, \ldots} , g_t$ of $SZ_i(K)$ and corresponding images $g'_1, g'_2 , \ldots, g'_t$ in the $SZ'_i(K)$.

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

Alice sends (a_j, b_j) and $j=1,2,\ldots,t$ to Bob. He takes alphabet $\{z_1, z_2,\ldots , z_t\}$ 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 $\alpha(j)>0$, $j=1,2, \dots, l$, $l>1$, $i(s)\in\{1,2,\dots,t\}$, $i(j)\neq i(j+1)$ 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 homomorphism 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. Adversary has to decompose available multivariate map $a=w(a_1, a_2, \dots, a_t)$ 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 on free module K^l of an arbitrarily chosen dimension.

6.2. The Case of Toric Generators

Let ${}^iZ=\{{}^ig_1, {}^ig_2, \dots, {}^ig_t\}$ be a set of elements $ES_{n(i)}(K)$,where $n(i)$ is increasing sequence of positive integers. We say that ${}^iZ$ is a system of Eulerian generators with growing periods (SEG) and rank t if

(1) For each j, $1\leq j\leq t$ values $per(\Delta({}^ig_j))$ tends to ∞ when i grows.

(2) ${}^kg_i\,{}^kg_i \neq {}^kg_j\,{}^kg_i$ for $i\neq j$**.**

We refer to semigroups ${}^iSZ=<{}^ig_1, {}^ig_2, \dots, {}^ig_t>$ as toric subsemigroups of $ES_{n(i)}(K)$. We say that subsets ${}^iZ^1=\{{}^ig^1_1, {}^ig^1_2, \dots, {}^ig^1_t\}$ of $ES_{m(i)}$,where $m(i)$ is increasing sequence of positive integers form, a quotient of Eulerian system ${}^iZ$ with growing periods if

(1) $n(i)\geq m(i)$ **,**

(2) the rules ${}^i\varphi({}^ig_j)={}^ig^1_j$, $j=1, 2, \dots, t$ define computationally tame homomorphisms of semigroups ${}^iSZ$ onto ${}^iSZ^1=<{}^iZ^1>$, i. e. homomorphisms computable in time $O(n(i)^{\alpha})$ for some positive constant α .

(3) ${}^iZ^1$ is also Eulerian system with growing periods.

We say that ${}^iZ^1$ is a regular Eulerian quotient if $n(i)=i$ for each value of i and $n(i)$ is polynomial expressions in variable i of bounded degree**.**

In the section 7.1 we constructively prove the following statement.

Theorem 3.

*For each finite commutative ring K with unity and natural number $t\geq 2$ there is an increasing sequence n(i) of natural numbers and Eulerian system ${}^iZ=\{{}^ig_1, {}^ig_2, \dots, {}^ig_t\}$ of rank **t** with growing periods (orders**)** which has a regular quotient ${}^iZ^1$.*

Multivariate Eulerian Protocol.

Let us assume that Alice selects a noncommutative system $Z(K)$ of *Eulerian generators* of rank t with quotient $Z'(K)$.

Alice chooses parameter i and bijective transformations $T\in EG_{n(i)}(K)$ and $T'\in EG_{m(i)}(K)$ acting on $(K^*)^{n(i)}$ and $(K^*)^{m(i)}$. Alice takes generators $g_1, g_2, \dots, g_t$ of $SZ_i(K)$ and corresponding images $g'_1, g'_2, \dots, g'_t$ in the $SZ'_i(K)$.

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

Alice sends (a_j, b_j) and $j=1,2,\dots,t$ to Bob. He takes alphabet $\{z_1, z_2,\dots, z_t\}$ 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 $\alpha(j)>0$, $j=1,2, \dots, l$, $l>1$, $i(s)\in\{1,2,\dots,t\}$, $i(j)\neq i(j+1)$ 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 $ES_{n(i)}(K)$ to Alice.

She uses the following restoration process to get $w(b_1, b_2,\dots,b_t)$. Alice computes $T^{-1}aT=c$. She uses tame homomorphism φ corresponding to noncomutative Eulerian 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 $T'c^{1}(T')^{-1}$.

Tandem of Protocols.

Let us consider two protocols in a natural combination.

Assume that Alice has data to set protocols 6.1 and 6.2 in the case of regular quotients.

She has system $CZ(K)$ *of stable Cremona generators of degree d* and rank t with regular quotient $CZ'(K)$ such that there is an enveloping family $EZ(K)$ of $CZ(K)$ and enveloping family $EZ^1(K)$ of $CZ'(K)$.

Alice also has a noncommutative system $Z(K)$ of Eulerian generators of rank t with regular quotient $Z'(K)$, i. e system of Eulerian generators corresponding to the sequence $n_1=i$, $i=1,2,\dots,n$.

So Alice uses these data to execute algorithms 6.1 and 6.2 together with Bob

For the parameter i selected by Alice correspondents elaborate collision elements b_C and b_E of these protocols. Notice the b_E is an element of $E_n(K)$. Thus correspondents have element $b_E b_C$ which has density $O(n^d)$ and a linear degree.

7. Implementation of the Tandem of Protocols

7.1. Family of linguistic graphs over multiplicative group of a commutative ring and graph based multivariate Eulerian protocol

We define Eulerian Double Schubert Graph $DS(k,K^*)$ over multiplicative group 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.

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 that graphs $DS(k, K^*)$ form a family of linguistic graphs.

Let us consider the subsemigroup ${}^kY(K^*)$ of ${}^kBS(K^*)$ consisting of strings $u=(H_0, G_1, G_2, H_3, H_4, G_5, G_6, \dots, H_{t-1}, H_t)$.

Let $I^*=I(K^*)$ be an incidence relation of Eulerian Double Schubert graph $DS(k, K^*)$. Then ${}^{I^*}\psi({}^kY(K^*))={}^kU(K^*)$ form a family of stable semigroups of $ES_n(K)$, $n=k+k^2$.

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 Eulerian Double Schubert Graph $DS(k,K^*)$.

For each subset J of M^2 deleting the coordinates of points and lines with coordinates indexed by elements $M-J$ defines symplectic homomorphism δ_J of $DS(k, K^*)$ onto a linguistic quotient $DS_J(k,K^*)$.

Let $I^*(J, K))$ be an incidence relation of linguistic graph $DS_J(k, K)$. Then homomorphism δ_J induces tame homomorphism of semigroup ${}^kU(K^*)$ onto its linguistic quotient ${}^{I^*(J,K)}\psi({}^kY(K^*))={}^kU_J(K^*)$.

Let K be a commutative ring with a unity. For each pair (n, m), $n \geq m$ an element T of $ES_n(K)$ with $per(T) \geq m$ can be constructed. Let us consider a subset $\{1,2, \dots,m\}$ of $\{1,2, \dots n\}$ and transformation T such that

$T(x_j)=x_{j+1}^{\lambda(j)}$, $j=1,2,\dots m-1$, $T(x_m)=x_1^{\lambda(m)}$, $(\lambda(i)i, |K^*|)$, $i-1,2,\dots,m$. Noteworthy that elements of kind STS^{-1} where S is a monomial transformation from $ES_n(K)$ have periods $>m$.

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

Alice considers family of ${}^{r(i)}Y(K))$ where $r(i)=[i^{1/2}]'$, $i=2,3,\dots$ So the point set of $DS(r(i), K^*))$ is a variety $(K^*)^m$ of dimension $m=[i^{1/2}]' + ([i^{1/2}]')^2$ which is at least $[i^{1/2} + i]'$.

For each i she can select the strings $u(1,i)$, $u(2,i)$, $\dots$, $u(t,i)$, $t \geq 2$ with coordinates from $ES_{r(i)}(K)$ of kind $u(k,i)=({}^{k,i}H_0, {}^{k,i}G_1, {}^{k,i}G_2, {}^{k,i}H_3, {}^{k,i}H_4, {}^{k,i}G_5, {}^{k,i}G_6, \dots, {}^{k,i}H_{t(k,i)-1}, {}^{k,i}H_{t(k,i)})$, $k=1,2,\dots,t$, $t(k,i) \geq 4$ such that ${}^{k,i}H_{t(k,i)}\,{}^{j,i}H_{t(j,i)} \neq {}^{ji}H_{t(j,i)}\,{}^{k,i}H_{t(k,i)}$ for distinct k and j and period of ${}^{k,i}H_{t(k,i)}$ is $>r(i)^{\alpha}$, $0<\alpha<1$.

The last conditions insure that for ${}^I\psi(u(k,i))=a(k,i)$, $k=1,2,\dots,t$ conditions $a(k,i)a(j,i) \neq a(j,i)a(k,i)$ hold and period of $a(k,i)$, i=1,2,… tends to infinity for each k. So elements $a(l,i) \in ES_{r(i)}$, $l=1,2,\dots,t$, $i=2,3,\dots$ form Eulerian system EZ of generators of growing periods corresponding to the sequence $r(i)$. Alice can take $DS(r(i), K^*)$ 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 $DS(r(i), K^*))$ onto $I(J(i),K^*)$ induces homomorphism $\phi^*(i,J(i))$ of semigroup ${}^{r(i)}U(K^*)$ onto ${}^iU_{J(i)}(K)$. It is easy to see that $\phi^*(i,J(i))(a(k,i))=a'(k,i)$ forms the regular quotient EZ' of the system EZ.

So correspondents can use toric tahoma protocol with the System EZ ofEulerian generators with growing periods and its regular quotient EZ'.

7.2. Example of a family of linguistic graphs over commutative ring and corresponding protocol

In the second protocol we use already defined symbol [,]' and already defined graphs *DS(k, K).*

Alice considers family of ${}^{r'(n)}Y(d, K))$, where $r'(i)=[i^{1/2}]'+\gamma$, where γ is an integer constant. 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 $u(1)=u(1,i), u(2,i), \ldots, u(t,i), t \geq 2$ of kind $u(k,i)=({}^{k,i}H_0, {}^{k,i}G_1, {}^{k,i}G_2, {}^{k,i}H_3, {}^{k,i}H_4, {}^{k,i}G_5, {}^{k,i}G_6, \ldots, {}^{k,i}H_{t(k,i)-1}, {}^{k,i}H_{t(k,i)})$, $k=1,2,\ldots,t$ from ${}^{k}U(d, K)$ such that $\Delta({}^{k,i}H_{t(k,i)}\ {}^{j,i}H_{t\ (j,i)}) \neq^{ji} \Delta({}^{j,i}H_{t\ (j,i)}\ {}^{k,i}H_{t(k,i)})$ for distinct k and j and period of ${}^{k,i}H_{t(k,i)}$ from $AGL_{r'(i)}(K) > r'(i)^{\alpha}$, $0<\alpha<1$.

The last condition insures that for ${}^{I}\psi(u(k,i))=b(k,i)$, $k=1,2,\ldots,t$ conditions $b(k,i)b(j,i)\neq b(j,i)b(k,i)$ hold if $j \neq k$ and period of $b(k,i)$, i=1,2,… tends to infinity for each k.

So endomorphisms $b(l,i)\epsilon E_{r'(i)}$, $l=1,2,\ldots,t$, $i=2,3,\ldots$ form stable

Noncommutative Cremona system *CZ* of degree *d* 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 $\phi(i,J(i))(b(k,i))=b'(k,i)$ form the quotient *EZ'* of the system *EZ* with enveloping family ${}^{i}U_{J'(i)}(d,K)$.

7.3. The combination and its usage for the privatization of public rules

Correspondents select parameter *i*. They use both protocols to elaborate collision map $H\epsilon ES_i(K)$, $K=F_q$ of linear degree $s(i)$ and stable transformation G from $E_i(K)$. They compute $G'=HG$ of linear degree and density $O(i^d)$.

Assume that $d=2$. One of correspondents (Alice) consider the public rule $F=(f_1, f_2, \ldots, f_m)$ of m.d.s.s. of Section 4 with *n* variables and *m* equations. Parameter *i* is selected as maximum of *n* and *m.*. If $m<n$ we consider transformation $F'=(f_1, f_2, \ldots, f_m, x_{m+1}, x_{m+2}, \ldots, x_i)$ where x_j are generic variables of $K[x_1, x_2, \ldots, x_i]$ and sends $G'+F'$ to Bob. He restores F' and they use the m.d.s.s. scheme of Section 4.

8. Complexity Aspects

Let us assume that correspondents use m.d.s.s. based on the composition of a quadratic multivariate public rule P' with $m=O(n)$ equations in *n* variables over finite field F_q with the endomorphism *H* from $E_n(F_q)$. Bob substitutes received signature string in the $G=HP'$ given in the standard form of each equation in time $O(n^3)$. So the check of the signature takes him $O(n^4)$ time.

Let us compute the time required for the generation of *H.*

Notice that choice of string with bounded length costs $O(n^{1/2})$. The computation of the value of linguistic homomorphism takes time evaluated by $O(n^{2+1/2})$. Each coordinate of *H* has $O(1)$ monomial terms of degree bounded by $qn^{1/2}$. The generation of *D* of density 1 and degree *q* takes time $O(n)$. The computation of *D* and *H* takes $O(n^{1+1/2})$. Each coordinate of *DH* has density $O(1)$ and degree *qn.* The computation of each coordinate of *(DH)P'* takes $O(n^3)$. So the complexity of computation of new public rule is $O(n^4)$.

The knowledge of the inverse string allows to compute inverse of *H* in time $O(n^{2+1/2})$. The inverse of *D* is computable for $O(n)$. So Alice can find appropriate signature for the time required for the computation of reimage of *P'.*

Finally we evaluate the complexity of execution of each protocol.

In the case of our stable platform of degree 2 Bob has a finite set of stable quadratic tranformations. The computation of composition of several generators in stable case can be evaluated via computation of two generators. It takes $O(n^7)$ elementary operations. It means that the total time for the execution of the protocol by Bob is $O(n^7)$. It is easy to see that Alice can generate data for the first stage essentially faster than $O(n^7)$.

For the computation of the collision quadratic endomorphism she need to compute the composition of linear and quadratic elements in two different orders. It can be done in time $O(n^5)$. Additionally Alice has to compute the product of two stable quadratic elements. We already noticed that it required $O(n^7)$ elementary steps. So $O(n^7)$ is the appropriate upper bound

for time execution of the protocol by each correspondent.

Similarly we will see that in the case of Eulerian platform the protocol can be executed in time $O(n^4)$ which is necessary to compute the product of two Eulerian transformations. Correspondents has to multiply Eulerian element with quadratic transformation. It can be done in time $O(n^4)$.

Conclusions

In paper [3] the method of conversion of multivariate digital signature scheme based on quadratic public map *P'* was proposed. So instead *P'* the combination of *HP'* with bijective element $H \in E_n(K)$ of linear degree $l(n)$ and density $O(1)$ is used. We notice that in the case $K=F_q$ we can work with reduced polynomials which are linear combinations of monomial terms $x_1^{a(1)}x_2^{a(2)}...x_n^{a(n)}$ where $a(i)$, $i=1,2,..., n$ are a residue modulo $q-1$. We modify the technique [4] of construction H via walk on special graphs defined by equations (''linguistic graphs over field F_q'') and construct bijective map *'H* from the reduced Cremona semigroup.

New scheme of usage *'HP'* has better estimates for time of execution presented in Section 7. Attacks presented in [1], [2] can not be used against new schemes.

The main objective of the paper is the algorithm of safe transition of multivariate digital signature scheme of linear degree onto private El Gamal type mode.

This algorithm uses a combination of two protocols of Multivariate Noncommutative Cryptography with platform formed by a family of quadratic stable subsemigroups of formal Cremona semigroup and platform formed by a family of semigroups of Eulerian transformations. The second platform is defined via families of linguistic graphs over groups which were introduced in this paper.

The combination of protocols allows correspondents to elaborate family G_n of elements of $'E_n(F_q)$, $n=2,3,...$of linear degree and density $O(n^2)$. One correspondent selects combination *Fn=HP'* and sends *Gn+Fn* to his/her partner.

Breaking the word problem is currently unsolvable post quantum problem, so the remaining option for adversary is to intercept many pairs of kind hash vector/corresponding signature and try to approximate *Fn.* The approximation task for the non bijective map of unbounded degree and density $O(n^2)$ is unfeasible one. This section should summarize the significance of this article for the development of the scientific field.

References

[1] 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.

[2] 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.

[3] Ustimenko, On Multivariate Algorithms of Digital Signatures on Secure El Gamal Type Mode ePrint Archive: Report 2020/984.

[4] V. Ustimenko, On Multivariate Algorithms of Digital Signatures of Linear Degree and Low Density, ePrint Archive: Report 2020/1015.

[5] 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).

[6] 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).

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

[8] V. Ustimenko, On semigroups of multiplicative Cremona transformations and new solutions of Post Quantum Cryptography, Cryptology ePrint Archive, 133, 2019.

[9] 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.

[10] 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, 15 pages https://doi.org/10.1155/2019/2137561

[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.

[27] 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).
[28] B. Tsaban, Polynomial-time solutions of computational problems in noncommutative-algebraic cryptography, J. Cryptol. 28, No. 3 (2015), 601-622.
[29] Max Noether, Luigi Cremona, Mathematische Annalen 59, 1904, p. 1–19.
[30] 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).
[31] 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).
[32] V. Ustimenko, On new multivariate cryptosystems based on hidden Eulerian equations, Dopov. Nath Acad of Sci, Ukraine, 2017. № 5, pp 17-24.
[33] V. Ustimenko, On new multivariate cryptosystems based on hidden Eulerian equations over finite fields, Cryptology ePrint Archive, 093, 2017.
Anne Canteaut François-Xavier Standaert (Eds.), Eurocrypt 2021, LNCS 12696, 40th Annual International Conference on the Theoryand Applications of Cryptographic Techniques Zagreb, Croatia, October 17–21, 2021, Proceedings, Part I, Springer, 2021, 839 p.