On Noncommutative Cryptography and homomorphism of stable cubical multivariate transformation groups of infinite dimensional affine spaces

V. Ustimenko, M. Klisowski

University of Maria Curie Sklodowska, Lublin 20036, Poland
vasyl@hektor.umcs.lublin.pl, mklisow@hektor.umcs.lublin.pl

Abstract. Noncommutative cryptography is based on applications of algebraic structures like noncommutative groups, semigroups and noncommutative rings. Its intersection with Multivariate cryptography contains studies of cryptographic applications of subsemigroups and subgroups of affine Cremona semigroups defined overfinite commutative rings. Efficiently computed homomorphisms between stable subsemigroups of affine Cremona semigroups can be used in tame homomorphisms protocols schemes and their inverse versions. The implementation scheme with the sequence of subgroups of affine Cremona group, which defines projective limit was already suggested. We present the implementation of other scheme which uses two projective limits which define two different infinite groups and the homomorphism between them. The security of corresponding algorithm is based on a complexity of decomposition problem for an element of affine Cremona semigroup into product of given generators. These algorithms may be used in postquantum technologies.

Keywords: Multivariate Cryptography, stable transformation groups and semigroups, decomposition problem of nonlinear multivariate map into given generators, tame homomorphisms, key exchange protocols, cryptosystems, algebraic graphs.

1. On ideas of Noncommutative Cryptography with platforms of transformations of Multivariate Cryptography.

Post Quantum Cryptography serves for the research of asymmetrical cryptographic algorithms which can be potentially resistant against attacks with the usage of quantum computer. The security of currently popular algorithms are based on the complexity of the following well known three hard problems: integer factorisation, discrete logarithm problem, discrete logarithm for elliptic curves. Each of these problems can be solved in polynomial time by Peter Shor's algorithm for theoretical quantum computer. In fact some rather old cryptosystems which were suggested in late 70th of the 20 century potentially may have some resistance to attacks on quantum computers (see for instance Mac Eliece cryptosystem [32]).

Modern PQC is divided into several directions such as Multivariate Cryptography, Nonlinear Cryptography , Lattice based Cryptography, Hash based Cryptography, Code based Cryptography, studies of isogenies for superelliptic curves, Noncommutative cryptography and others.

The Multivariate Cryptography (see [1], [2], [3]) uses polynomial maps of affine space K^n defined over a finite commutative ring 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 $x_1 \rightarrow f_1(x_1, x_2, \ldots, x_n), x_2, \rightarrow f_2(x_1, x_2, \ldots, x_n), \ldots, x_n \rightarrow f_n(x_1, x_2, \ldots, x_n)$), transforming affine space K^n, ere$f_i: K[x_1, x_2, \ldots, x_n], i = 1,2, \ldots, n$ are multivariate polynomials usually given in a standard form, i.e. via a list of monomials in a chosen order.

Non-commutative cryptography appeared with attempts to apply Combinatorial group theory to Information Security. If G is noncom-mutative group then correspondents can use conjugations of elements involved in protocol, some algorithms of this kind were suggested in [4], [5], [6], [7], where group G is given with the usage of generators and relations. Security of such algorithms is connected to Conjugacy Search Problem (CSP) and Power Conjugacy Search Problem (PCSP), which combine CSP and Discrete Logarithm Problem and their generalizations. Currently Non-commutative cryptography is essentially wider than group based cryptography. It is an active area of cryptology, where the cryptographic primitives and systems are based on algebraic structures like groups, semigroups and noncommutative rings (see [8], [9], [10], [11], [12], [13], [14], [15], [16]). This direction of security research has very rapid development (see [17], [18] and further references in these publications).

One of the earliest applications of a non-commutative algebraic structures for cryptographic purposes was the usage of braid groups to develop cryptographic protocols. Later several other non-commutative structures like Tompson groups and Grigorchuk groups have been identified as potential candidates for cryptographic post quantum applications. The standard way of presentations of groups and semigroups is the usage of generators and relations (Combinatorial Group Theory). 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).

The paper is devoted to some research on the intersection of Non Commutative and Multivariate Cryptographies. We try to use some abstract schemes in terms of Combinatorial Semigroup Theory for the implementation with platforms which are semigroups and groups of polynomial transformations of free modules Kn where K is commutative ring.

The most popular form of Multivariate cryptosystem is the usage of a single very special map f in a public key mode. First examples were based on families of quadratic bijective transformation fn(see [1], [2], [3]), such choice implies rather fast encryption process.The paper is devoted to other aspects of Multivariate cryptography when some subsemigroup of affine Cremona semigroup of all polynomial transformations is used instead of a single transformation. Let us discuss a case of subsemigroup with single generator. Everybody knows that Diffie - Hellman key exchange protocol can be formally considered in general case of any finite group or semigroup G. In the case of group *G* corresponding El Gamal cryptosystem can be introduced. Notice that security of this algorithm depends not only on abstract group G but on the way of its generation in computers memory. For instance if $G=Z^*_p$ is multiplicative group of large prime field then discrete logarithm problem (DLP) is difficult one and guarantees the security of the protocol, if the same abstract group is given as additive group of Z_{p-1} protocol is insecure because DLP will be given by linear equation.

Notice that the implementation of the idea to use multivariate generator in its standard form has to overcome essential difficulties. At first glance Diffie - Hellman protocol in affine Cremona semigroup looks as unrealistic one because of composition of two maps of degree *r* and *s* taken in "general position " will be a transformation of degree *rs*. So in majority of cases $deg(F)=d$, $d>1$ implies very fast growth of function $d(r)=deg(F^r)$. Of course in the case of generator in common position not only degree but a density (total number of monomial terms of the map in its standard forms) grows exponentially.

So we have to find special conditions on subsemigroup of affine Cremona group which guarantee the polynomial complexity of procedurȩ to compute the composition of several elements from subsemigroup. Such conditions can define a basis of Noncommutative Multivariate Cryptography. Hopefully at least two conditions of this kind are already known [19] (see further references) and [34]. We consider them in the following section.

2. On stable subsemigroups of Affine Cremona Semigroup, Eulerian transformations and corresponding cryptographic schemes.

Stability condition demands that degree of each transformation of the subsemigroup of affine Cremona semigroup has to be bounded by independent constant d. We refer to such subsemigroup as stable subsemigroup of degree *d*. Examples of known families of stable subgroups of degree $d=3$ reader can find in [19] (see further refrences) or [33] Applications of such families to Symmetric Cryptograpjy could be found in [35]. Some examples of stable families of subgroups of degree 2 are given in [20]).

Eulerian condition demands that all transformations of subsemigroup of affine Cremona subgroup are given in a standard form $(x_1 , x_2, \dots , x_n) \to (f_1(x_1 , x_2, \dots , x_n), f_2(x_1 , x_2, \dots , x_n), \dots ,f_n(x_1 , x_2, \dots , x_n))$, where each f_i has density 1. All transformations of this kind for General Eulerian Semigroup ${}^nGES(K)$ of transformations of kind $x_1 \to \mu_1 x_1^{a(1,1)} x_2^{a(1,2)} \dots x_n^{a(1,n)}$, $x_2 \to \mu_2 x_1^{a(2,1)} x_2^{a(2,2)} \dots x_n^{a(2,n)}$,…, $x_n \to \mu_n x_1^{a(n,1)} x_2^{a(n,2)} \dots x_n^{a(n,n)}$ where $a(i,j)$ are positive integers and $\mu_i \epsilon K$.

First cryptosystems of Nonlinear Multivariate Cryptograpjy in terms of ${}^nGES(K)$ are suggested in [34].

The *discrete logarithm problem* is the special simplest *case of* the *word decomposition problem* for semigroups. Let S' be a subsemigroup of S generated by elements $g_1, g_2, \dots , g_t$. The *word problem* (WP) of finding the decomposition of $g \epsilon S$ into product of generator g_i is difficult, i. e. polynomial algorithms to solve it with Turing machine or Quantum Computer are unknown. The idea to apply this problem in Cryptography was considered in [36] where some general schemes to use WP for constructuons of algorithms of Noncommutative Cryptography were suggested. Of course the complexity of the problem depends heavily of choice of S and the way of presentation of semigroup. In the cases of families of affine Cremona semigroups or S= ${}^nGES(K)$ problem WP is computationally infeasible with a Turing machine" and with Quantum Computer.

We are working on implementations of the following formal schemes of usage the complexity of WP. Tame map means computable in polynomial time from parameter m.

TORIC TAHOMA CRYPTOSYSTEM.

Let K be a commutative ring, subgroups ${}^nG$ of ${}^nGES(K)$ act naturally on $(K^*)^n$, ${}^mS(n, K)$ is a subsemigroup of ${}^mGES(K)$ such that there is a tame homomorphisn $\Delta=\Delta(m,n)$ of ${}^mS(n, K)$ onto ${}^nG$. We assume that $m=m(n)$ where $m>n$ and consider the following *toric tahoma cryptosystem*:

Alice takes $b_1 , b_2, \dots , b_s$, s>1 from ${}^mS(n, K)$ and $a_1 , a_2, \dots , a_s$ where , $a_i=\Delta(b_i)^{-1}$. She takes $g \epsilon\, {}^mEG(K)$ and $h \epsilon\, {}^nEG(K)$ and forms pairs $(g_i, h_i) =(g^{-1} b_i g , h^{-1} a_i h)$, $i=1, 2,\dots, s$ and sends them to Bob.

He writes the word $w(z_1, z_2 ,\dots, z_s)$ in the alphabet $z_1, z_2 ,\dots, z_s$ together with the reverse word $w'(z_1, z_2 ,\dots, z_s)$ formed by characters of w written in the reverse order. He computes element $b=w(g_1, g_2 ,\dots, g_s)$ via specialization $z_i=g_i$ and $a=w'(h_1, h_2 ,\dots, h_s)$ via specialization $z_i=h_i$. Bob keeps a for himself and sends b to Alice. She computes a^{-1} as $h^{-1}\Delta(gbg^{-1})h$.

Alice writes her message $(p_1 , p_2, \dots , p_n)$ and sends ciphertext $a^{-1}(p_1 , p_2, \dots , p_n)$ to Bob. He decrypts with his function a. Symmetrically Bob sends his ciphertext $a(p_1 , p_2, \dots , p_n)$ to Alice and she decrypts with a^{-1}.

The problems of constructions of large subgroups G of ${}^nGES(K)$, pairs (g, g^{-1}), $g \epsilon G$, and tame Eulerian homomorphisms $\mu : G \to H$, i. e. computable in polynomial time $t(n)$ homomorphisms of subgroup G of ${}^nGES(K)$ onto $H< {}^mGES(K)$ are motivated by tasks of Nonlinear Cryptography.

The first platforms for this scheme and some other abstract schemes are suggested in [34].

If we change semigroup ${}^mGES(K)$ for affine Cremona semigroup $S(K^m)$ we obtain the following AFFINE TAHOMA CRYPTOSYSTEM on stable transformations.

Let K be a commutative ring, stable subgroups ${}^nG$ of $S(K^n)$ act naturally on K^n and ${}^mS(n, K)$ be a subgroup of $S(K^m)$ such that there is a tame homomorphisn $\Delta=\Delta(m,n)$ of ${}^mS(n, K)$ onto ${}^nG$. We assume that $m=m(n)$ where $m>n$.

Alice takes b_1 , $b_2, \dots$, b_s , s>1 from ${}^mS(n, K)$ and a_1 , $a_2, \dots$, a_s where , $a_i=\Delta(b_i)^{-1}$. She takes $g\epsilon C(Q^m)$ and $h\epsilon C(R^n)$ where R and Q are extensions of the commutative ring K and forms pairs $(g_i, h_i) =(g^{-1}b_i g , h^{-1} a_i h)$, $i=1, 2,..., s$ and sends them to Bob. We assume that $g=g'T$, $h=h'T'$ where semigroup $<g', {}^mS(n, K)>$ generated by g' and elements of ${}^mS(n, K)$ and group $<h' ,G>$ are stable semigroups of degree d and $T\epsilon AGL_n(R)$, $T'\epsilon AGL_m(Q)$.

As in the previous algorithm Bob writes the word $w(z_1, z_2 ,..., z_s)$ in the alphabet $z_1, z_2 ,..., z_s$ together with the reverse word $w'(z_1, z_2 ,..., z_s)$ formed by characters of w written in the reverse order. He computes element $b=w(g_1, g_2 ,..., g_s)$ via specialization $z_i=g_i$ and $a=w'(h_1, h_2 ,..., h_s)$ via specialization $z_i=h_i$. Bob keeps a for himself and sends b to Alice. She computes a^{-1} as $h^{-1}\Delta(gbg^{-1})h$.

Alice writes her message $(p_1 , p_2, \dots , p_n)$ from R^n and sends ciphertext $a^{-1}(p_1 , p_2, \dots , p_n)$ to Bob. He decrypts with his function a. Symmetrically Bob sends his ciphertext $a(p_1 , p_2, \dots , p_n)$ to Alice and she decrypts with a^{-1} (see [21]). Let ${}^nTC(K,R,Q)$ stand for affine Tahoma cryptosystem as above.

In [20] quadratic stable subsemigroups with correspondent homomorphims are suggested as platforms of this scheme. Some other schemes are also implemented there with these platforms. Some cubical platforms were suggested in [21].

Only one family of platforms were investigated via computer implementation. Paper [31] is devoted to implementations of Affine Tahoma scheme with platforms of cubical stable groups. They were defined via families of linguistic graphs which form projective limits and the standard homomorphisms between two members of this sequences. So we have pairs (G_n , Δ_n) where $G_n <S(K^n)$, Δ_n is a homomorphism of G_n onto G_m, $m=m(n)$ such that projective limits $lim (G_n)$, $n \to\infty$ and $lim(\Delta(G_n))$, $n \to\infty$ coincide with the same infinite transformation group G.

This article is devoted to another computer experiment with the new platform which uses the same groups G_n but different tame homomorphisms η_n . In the new scheme $lim(G_n)$, $n \to\infty$ equals to G, but $\lim(\eta_n(G_n))$, $n \to\infty$ coincides with the image of homomorphism of G with an infinite kernel.

We believe that option to vary tame homomorphisms in the chosen sequence of semigroup makes the task of cryptanalytic much more difficult.

We use projective limits $D(K)$ and $A(K)$ of the well known graphs $D(n, K)$ [22], [23] and $A(n,K)$ (see [24] and further references) defined *over* arbitrary finite commutative rings. Walks on the graphs D(K) and A(K) allow to define groups $GD(K)$ and $GA(K)$ of cubic transformations of infinite dimensional affine space over K. Group $GA(K)$ is a homomorphic image of $GD(K)$, both groups can be obtained as projective limits of sequences $GA_n(K)$ and $GD_n(K)$,n=1, 2,… of finite cubical stable groups. We suggest key exchange protocols based on homomorphisms of $GD_j(K)$ ontp $GA_i(K)$ for some i and j.

Computer simulations demonstrate an interesting effect of density stabilisation of generated cubical maps. The time execution tables for algorithms of generation of maps and numbers of monomial terms are given. They demonstrate the feasibility of algorithms. The method of generation allows to construct for each bijective transformation of the free module over *K its* inverse map. Multivariate nature of collision maps allows to use these algorithms for the safe exchange of multivariate transformations. Various *deformation rules* can be used for this purpose (see formal schemes of [21] and [19], [20]).

3. Some basic definitions.

Let us consider basic algebraic objects of multivariate cryptography, which are important for the choice of appropriate pairs of maps f, f^{-1} in both cases of public key approach or idea of asymmetric algorithms with protected encryption rules. Let us consider the totality $SF_n(K)$ of all rules of kind: $x_1 \rightarrow f_1(x_1, x_2, \dots, x_n)$, $x_2 \rightarrow f_2(x_1, x_2, \dots, x_n)$, ..., $x_n \rightarrow f_n(x_1, x_2, \dots, x_n)$ acting on the affine space K^n, where f_i , $i = 1, 2,\dots, n$ are elements of $K[x_1, x_2, \dots, x_n]$ with natural operation of composition. We refer to this semigroup as semigroup of formal transformation $SF_n(K)$ of free module K^n. In fact it is a totality of all endomorphisms of ring $K[x_1, x_2, \dots, x_k]$ wth the operation of their superposition. Each rule f from $SF_n(K)$ induces transformation t(f) which sends tuple $(p_1 , p_2, \dots , p_n)$ into $(f_1(p_1 , p_2, \dots , p_n), f_2(p_1 , p_2, \dots , p_n), \dots ,f_n(p_1 , p_2, \dots , p_n))$. Affine Cremona semigroup $S(K^n)$ is a totality of all transformations of kind $t(f)$. The canonical homomorphism $t \rightarrow t(f)$ maps infinite semigroup $SF_n(K)$ onto finite semigroup $S(K^n)$ in the case of finite commutative ring K.

We refer to pair (f, f') of elements $SF_n(K)$ such that ff' and $f'f$ are two copies of identical rule $x_i \rightarrow x_i$, $i = 1, 2,\dots, n$ as pair of invertible elements. If (f, f') **is** such a pair, then product $t(f)t(f')$ is an identity map. Let us consider the subgroup $CF_n(K)$ of all invertible elements of $SF_n(K)$ (group of formal maps). It means f is an element of $CF_n(K)$ if and only if there is f' such that ff' and $f' f$ are identity maps. It is clear that the image of a restriction of t on $CF_n(K)$ is affine Cremona group $C_n(K)$ of all transformations of K^n onto K^n for which there exists a polynomial inverse.

We say that a family of subsemigroups S_n of $SF_n(K)$ (or $S(K^n)$) is stable of degree d if maximal degree of elements from S_n is an independent constant d, $d > 1$. If K is a finite commutative ring then stable semigroup has to be a finite set.

Condition $d>1$ is natural because of elements from the group $AGLn(K)$ of all affine bijective transformations, i. e. elements of affine Cremona group of degree 1.

4. On linguistic graphs and related semigroups of affine transformations.

The missing definitions of graph-theoretical concepts which appear in this paper can be found in [21]. All graphs we consider are *simple* graphs, i.e. undirected without loops and multiple edges. Let $V(G)$ and $E(G)$ denote the set of vertices and the set of edges of G respectively.

When it is convenient we shall identify G with the corresponding anti-reflexive binary relation on $V(G)$, i.e. $E(G)$ is a subset of $V(G)\circ V(G)$ and write $v\ G\ u$ for the adjacent vertices u and v (or neighbours). We refer to $|\{ x \in V(G) | xGv \}|$ as degree of the vertex v.

The *incidence structure* is the set V with partition sets P *(points)* and L *(lines)* and symmetric binary relation I such that the incidence of two elements implies that one of them is a point and another one is a line. We shall identify I with the simple graph of this incidence relation or *bipartite graph*. The pair x, y , $x \in P$, $y \in L$ such that $x\ I\ y$ is called a *flag* of incidence structure I.

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 [22]. Brackets and parenthesis allow us to distinguish points from lines.

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 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 ϵK^r and p=($p_1, p_2, \dots, p_{s+m}$) there is a unique neighbour of the point $[l]=N_b(p)$ with the colour b. Similarly for each cϵK^s and line $l=[l_1, l_2, \dots, l_{r+m}]$ there is a unique neighbour of the line $(p)= N_c([l])$ with the colour c. The triples of parameters s, r, m defines *type of linguistic graph.*

We consider also linguistic incidence structures defined by infinite number of equations. Let $M = \{m1, m2, \dots, md\}$ be a subset of $\{1, 2, \dots, m\}$ (set of indexes for equations). Assume that equations indexed by elements from M of following kind

$a_{m1}x_{m1} + b_{m1}\mathbf{y}_{m1} = f_{m1} (x_1, x_2, \dots, x_s, y_1, y_2, \dots, y_r)$

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

…

$a_{md}x_{md} + b_{md}\mathbf{y}_{md} = f_{md} (x_1, x_2, \dots, x_s, x_{m1}, x_{m2,\dots,} x_{m\ d-1}, y_1, y_2, \dots, y_{r,,} y_{m1}, y_{m2}, _{,\dots,} y_{m\ d-1,})$ are define other linguistic incidence structure *IM*. Then the natural projections $\delta_{1,}: (x)\rightarrow(x_1, x_2, \dots, x_s, x_{m1}, x_{m2,\dots,} x_{md})$ and $\delta_2:[y]\rightarrow[y_1, y_2, \dots, y_r, y_{m1}, y_{m2,\dots,} y_{md}]$ of free modules define the natural homomorphism δ of incidence structure I onto $I_{M.}$. We will use 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 [23], where symplectic homomorphism was used for the cryptosystem construction).

We consider more general concept of linguistic homomorphism ξ of linguistic incidence systems P, L, $I(K)$ and induced by linear projections δ of P and δ' : of L defined via deleting of some coordinates of colour tuples

$(x_1, x_1, \dots, x_s)$ and $[y_1, y_2, \dots, y_r]$ together with simultaneous deleting of x_{i+r} and y_{i+s} for i from some subset of $\{1, 2,\dots, m\}$. The image of ξ is a linguistic graph of type s_1, r_1, m_1 where $s_1 \leq s$, $r_1 \leq r$, $m_1 \leq m$.

In the case of linguistic graph Γ the path consisting of its vertices $v_0, v_1, v_2, \dots, v_k$ is uniquely defined by initial vertex v_0, and colours $\rho(v_{i},)$, $i=1, 2,\dots, k$.

Let us concentrate on linguistic graphs of type $1,1, m$. Let $N(a,v)$ be the operator of taking neighbour of the vertex v with colour $a\epsilon K$. We refer to sequences $(f_1 , f_2 ,..., f_s)$ with $f_1 \epsilon K[x_1]$ of even length s as *symbolic strings*. On the totality $S_{1,1}$ (K) of such sequences we consider the product

$(f_1, f_2, ... , f_s)(g_1, g_2, ..., g_r)=(f_1 , f_2 ,...,f_s , g_1 (f_s(x_1)), g_2(f_s (x_1),..., g_r (f_s (x_1))).$

Proposition 1. Elements of $S_{1,1}$ *(K)* with defined product form a semigroup.

If *Q* is an extension of the ground commutative ring *K* then linguistic graph *I(Q)* and can be defined via the same set of equations. Let us take $Q=K[x_1, x_2,..., x_n]$ and consider infinite linguistic graph $I'=I(K[x_1, x_2,..., x_n])$ with partition sets *P'* and *L'* isomorphic to variety $K[x_1, x_2,..., x_n]^n$. For each symbolic string $(f_1, f_2, ... , f_s)$ from $S_{1,1}$ *(K)* and consider the symbolic computation $C(f_1, f_2, ... , f_s)$ which is a walk in *I'* with starting point $X=(x_1, x_2,..., x_n)$ are generic elements of the commutative ring $K[x_1, x_2,..., x_n]$, other elements of the walk are $X_1=N(f_1, X), X_2=N(f_2, X_1), \dots, X_s=N(f_s, X_{s-1})$. Notice that operators $N(f_i, X_{i-1})$ are computed in the graph *I'*.

It is easy to see that $X_s =(f_s(x_1), g_2(x_1, x_2), \dots, g_n(x_1, x_2, \dots, x_n))$, where $g_i \epsilon K[x_1, x_2, \dots, x_i]$. The rule $(x_1 \to f_s(x_1), x_2 \to g_2(x_1, x_2), \dots, x_n \to g_n(x_1, x_2, \dots, x_n))$ defines the map from $S(K^n)$ into itself . We denote this map as $\Delta^{I(K)}(f_1, f_2, ... , f_s)$ and refer to it as a map of symbolic computation.

Proposition 2. A map $\Delta^{I(K)}$ from $S_{1,1}(K)$ into $s(K^n)$ sending symbolic string $(f_1, f_2, ... , f_s)$ to $\Delta^{I(K)}(f_1, f_2, ... , f_s)$ is a homomorphism of $S_{1,1}(K)$ into $s(K^n)$.

We refer to the image *PS(I(K))* of homomorphism of proposition 2 as semigroup of symbolic point to point computations and refer to $\Delta^{I(K)}$ as *linguistic compression (lc) homomorphism.* We define a semigroup *LS(I(K)) of line to line computations* via simple change of points for lines in *I* and *I'*.

Proposition 3. A symplectic homomorphism δ of linguistic graphs ${}^1I(K)$ and ${}^2I(K)$ of type *(1, 1, n)* induces canonical homomorphism of $PS({}^1I(K))$ onto $PS({}^2I(K))$.

Let us consider subsemigroup $\Sigma(K)$ of $S_{1,1}(K)$ generated by *symbolic shifting strings* of kind $(x_1+a_1, x_1+a_2, ..., x_1+a_s)$, where a_i, $i=1,2,...,s$ are elements of *K*. We identify tuple $C=(x_1+a_1, x_1+a_2, ..., x_1+a_s)$ *with its code* $<a_1, a_2, ..., a_s>$.

Proposition 4. For each linguistic graph *I(K) of type (1, 1, n-1)* the image $\Sigma(I(K))$ of $\Sigma(K)$ under the linguistic compression homomorphism of onto ***PS(I(K))*** is a subgroup of affine Cremona group.

In fact for invertibility of $\Delta(f_1, f_2,\dots, f_s) \epsilon PS(I(K))$ the bijectivity of f_s is a sufficient and necessary condition. We refer to Σ *(I(K))* as *group of walks on points* of linguistic graph *I(K).*

Let $C=(x_1+a_1, x_1+a_2, ..., x_1+a_s)$ be a shifting symbolic string from the semigroup $\Sigma(K)$. We refer to *Rev*(C)=$(x_1-a_s+a_{s-1}, x_1-a_s+a_{s-2}, \dots , x_1-a_s+a_1 , x_1-a_s)$as revering string for x.

Lemma *Let* $\Delta=\Delta^{I(K)}$ *be linguistic compression map from* $S_{1,1}(K)$ *onto* $PS(I(K))$ *and* $\mathbf{x} \in \Sigma(K)$. *Then inverse map for* $\Delta(x)$ *coincides with* $\Delta(Rev(x))$.

5. Stable groups of cubical maps defined in terms of linguistic graphs and their homomorphisms.

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 $(p)=(p_1, p_2, \dots , p_n)\in P_n$ and $[l]=[l_1, l_2, \dots , l_n]\in L_n$. 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.

$p_2 - l_2=l_1p_1$, $p_3 - l_3= p_1 l_2$, $p_4 - l_4 = l_1p_3$, $p_5 - l_3 = p_1 l_4$, ... , $p_n - l_n= p_1 l_{n-1}$ 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 $p_1, p_2,\dots, p_n$ are fixed elements of the ring and symbols $l_1, l_2,\dots, l_n$ are variables. It is easy to see that the value for l_1 could be freely chosen. This choice uniformly establishes values for $l_2, l_3, \dots , l_n$. 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.

It means that graphs $A(n, K)$ with colouring ρ belong to class of Γ linguistic graphs of type $(1, 1, n-1)$.

Let $GA(n,K)=\Sigma(A(n,K))$ stands for the group of walks on points of $A(n,K)$. We have a natural homomorphism $GA(n+1, K)$ onto $GA(n, K)$ induced by symplectic homomorphism Δ from $A(n+1, K)$ onto $A(n, K)$ sending point $(x_1, x_2, \dots, x_n, x_{n+1})$ to $(x_1, x_2, \dots, x_n)$ and line $[x_1, x_2, \dots, x_n, x_{n+1}]$ to $[x_1, x_2, \dots, x_n]$. It means that there is well defined projective limit $A(K)$ of graphs $A(n, K)$ and groups $GA(K)$ of groups $G(n, K)$ when n is growing to infinity. As it stated in [25] case of $K=F_q$, $q>2$ infinite graph $A(F_q)$ is a tree. Some properties of infinite groups $GA(K)$ of transformation of infinite dimensional affine space over commutative ring K the reader can find in [24].

Other family $D(n, K)$ of linguistic graphs of type $(1,1, n-1)$ defined over the commutative ring K were defined in [23] but its definition in the case of $K=F_q$ was known earlier. In fact graphs $D(n,q)=D(n, F_q)$ are widely known due to their applications in Extremal Graph Theory, in Theory of LDPC codes and Cryptography. Graphs $D(n, K)$ are bipartite with set of vertices

$V=PUL$, $|P\cap L|=0$. A subset of the vertices P is called the set of *points* and another subset L is called the set of *lines*. Let P and L be two copies of Cartesian power K^n, where $n\geq 2$ is an integer. Two types of brackets are used in order to distinguish points from lines. It has a set of vertices (collection of points and lines), which are n-dimensional vectors over K:$(\boldsymbol{p}) = (p_1, p_2 , p_3, p_4, . . . , p_i, p_{i+1}, p_{i+2}, p_{i+3}, . . ., p_n)$, $[\boldsymbol{l}] = [l_1, l_2, l_3, l_4, . . . , l_i, l_{i+1},l_{i+2},l_{i+3}, . . ., l_n]$. The point $(\boldsymbol{p})$ is incident with the line $[\boldsymbol{l}]$, if the following relations between their coordinates hold: $l_2-p_2=l_1p_1$, $l_3-p_3=l_2\mathrm{p}_1$, $l_4-p_4=l_1p_2$, $l_i-p_i=l_1p_{i-2}$, $l_{i+1}-p_{i+1}=l_{i-1}p_1$, : $l_{i+2}-\mathrm{p}_{i+2}=l_ip_1$: $l_{i+3}-p_{i+3}=l_1p_{i+1}$ where $i\geq 5$. Connected component of edge-transitive graph $D(n,q)$ is denoted by $CD(n,q)$ [22]. Notice that all connected components of the natural projective limit $D(q)$ of graphs $D(n,q)$, $n\rightarrow\infty$ are q-regular trees. Let $D(K)$ stands for the projective limit of graphs $D(n,K)$

Let us denote as $GD(n,K)$ and $GD(K)$ the groups $\Sigma(D(n,K))$ and $\Sigma(D(K))$ of walks on points of graphs $D(n, K)$ and $D(K)$ respectively. For the description of certain symplectic quotients we will use the alternative description of graphs $D(K)$. It is based on the connections of these graphs with Kac-Moody Lie algebra with extended diagram A_1.The vertices of $D(K)$ are infinite dimensional tuples over K. We write them in the following way $(p) = (p_{0,1}, p_{1,1}, p_{1,2}, p_{21}, p_{22}, p'_{22}, p_{23}, ... , p_{i,i}, p'_{i,i} , p_{i,i+1}, p_{i+1,i}, ...)$, $[l] = [l_{1,0}, l_{1,1} ,l_{1,2,}, l_{21}, l_{22}, l'_{22}, l_{23}, ... ,l_{i,i}, l'_{i,i} ,l_{i,i+1}, l_{i+1,i}, ...]$. We assume that almost all components of points and lines are zeros. The condition of incidence of point (p) and line $[l]$ ($(p)I[l]$) can be written via the list of equations below.

$l_{i,i} - p_{i,i} =l_{1,0}\, p_{i-1,i}$; $l'_{i,i} - p'_{i,i} = l_{i,i-1}\, p_{0,1}$; $l_{i,i+1} - p_{i,i+1} =l_{i,i}\, p_{0,1}$;$l_{i+1,i} - p_{i+1,i} =l_{1,0}\, p'_{i,i}$. This four relations are defined for $i\geq 1$, $(p'_{1,1} = p_{1,1},\ l'_{1,1} = l_{1,1})$.

Similarly, we can define the projective limit $A(K)$ of graphs $A(n,K)$, $n>1$.

We can describe the bipartite infinite graph $A(K)$ on the vertex set consisting on points and lines $(p) = (p_{0,1}, p_{1,1}, p_{1,2}, p_{21}, p_{22,}, p_{23}, ..., p_{i,i} , p_{i,i+1,\dots}),$

$[l] = [l_{1,0}, l_{1,1} ,l_{1,2,}, l_{21}, l_{22}, l_{23}, ... ,l_{i,i} , l_{i,i+1, \dots}]$ such that point (p) is incident with the line $[l]$ $((p)I[l]$, if the following relations between their coordinates hold: $l_{i,i} - p_{i,i} =l_{1,0}\, p_{i-1,i}$; $l_{i,i+1} - p_{i,i+1} =l_{i,i}\, p_{0,1}$.

It is clear that the set of indices A={(1; 0), (0; 1), (1; 1), (1; 2), (2; 2), (2; 3), … , (i-1, i), (i, i) } is a subset in D={(1, 0), (0; 1), (1, 1), (1, 2), (2; 2), (2, *2)',..., (i- 1, i); (i; i - 1); (i, i); (i, i)',...)*. So graph $A(K)$ is a symplectic quotient of linguistic incidence structure $D(K)$. Let us use symbol Ψ for the corresponding symplectic homomorphism. For each positive integer $m \geq 2$ we consider subsets $M=A^m$ and $M=D^m$ containing of first m-2 elements of $A'=A-\{(1, 0), (0,1)\}$ and $D'=D-\{(1, 0), (0,1)\}$ with respect to the above orders and obtain symplectic quotients I_M of $D(K)$ and $A(K)$.One can check that corresponding quotients are isomorphic to graphs $D(m, K)$ and $A(m,K)$. The investigation of pair A^m , D^m leads to following statement [23].

Proposition 5. For each $n \geq 4$ there are a symplectic homomorphisms of $D(2n,K)$ onto $A(m, k), 2 \geq m \geq n+1$ and $D(2n+1, K)$ onto $A(m,K), 2\geq m \geq n+2$. Notice that $D(n,K)=A(n,K)$ for $n =2,3$.

Proposition 6. Groups $GD(K)$ and $GA(K)$ are stable cubical transformations of infinite dimensional affine space over commutative ring K.

Corollary. $GD(n, K)$ and $GA(n,K)$ are stable cubical subgroups of Cremona group $C(K^n)$.

6. On Three Gates Bridge diagram and algorithms of Noncommutative cryptography for stable transformation groups.

Let us consider the following Three Gates Bridge diagram.

$$\begin{tikzcd}
\Sigma(R) \arrow[d] & \Sigma(Q) \arrow[l] \arrow[d] & \Sigma(Q) \arrow[l] \arrow[r] \arrow[d] & \Sigma(K) \arrow[d] \\
GA(m,R) & GA(m,Q) \arrow[l] & GD(n, Q) \arrow[l] \arrow[r] & GD(n,K)
\end{tikzcd}$$

Commutative rings K and R are finite extensions of basic commutative ring Q. Left and rights arrows of the first row of the diagram corresponds to natural embedding of $\Sigma(Q)$ into $\Sigma(R)$ and $\Sigma(K)$. The middle row between two copies of $\Sigma(Q)$ corresponds to identity isomorphism.

Left and rights arrows of the second row of the diagram corresponds to natural embeddings of $GA(m,Q)$ into $GA(m,R)$ and $GD(n,Q)$ into $CD(n,K)$. The middle row between $GD(m,Q)$ and $GA(m,Q)$ corresponds to homomorphism of these groups induced by symplectic homomorphism of linguistic graphs $D(n, Q)$ and $A(m, Q)$ described in Proposition 5.

Vertical arrows of the diagram correspond to linguistic compression homomorphisms of $S_{1,1}(R)$ onto $PS(I(R)), I(R)=A(m,R)$ restricted onto $\Sigma(R)$, $S_{1,1}(Q)$ onto $PS(I(Q)), I(Q)=A(m,Q)$ restricted onto $\Sigma (Q)$, $S_{1,1} (Q)$ onto $PS(D(n,Q))$ restricted onto $\Sigma(Q)$, $S_{1,1}(K)$ onto $PS(D(n,K))$ restricted onto $\Sigma (K)$. As it follows from the definitions Three Gates Bridge diagram is commutative diagram.

6.1 Tahoma word protocol.

Alice sets pairs of graphs $D(n, Q)$ and its symplectic image $A(m,Q)$. She chooses ring extensions R and K . This information defines Three Bridge Diagram. She selects strings $C_i=< {}^i\alpha_1 , {}^i\alpha_2,\dots, {}^i\alpha_{t(1)}>, i=1, 2, \dots, r$ from $\Sigma(Q)$ and elements $B=<\beta_1 ,\beta_2, \dots, \beta_s>$ from $\Sigma(K)$ and $D=<\gamma_1, \gamma_2 , \dots, \gamma_k,>$ from $\Sigma(K)$. Alice computes $Rev(B)$ and $Rev\ (D)$. She takes affine transformations $T_1\ \epsilon AGL_n\ (K)$ and T_2 from $AGL_m\ (K)$.

Alice forms strings $B_i=Rev(B)C_iB$ and $D_i=Rev(D)C_iD,\ i=1,2,\ldots,r$ in $\Sigma\ (K)$ and $\Sigma\ (R)$. She computes images CB_i and CD_i of linguistic compression homomorphism $\Delta^{D(n,K)}$

and $\Delta^{A(m,K)}$ on elements B_i and D_i . Finally Alice computes elements $T_1^{-1}CB_i\ T_1\ =G_i$ and $F_i\ =T_2\ ^{-1}CD_i\ T_2$ which are elements of affine Cremona groups $C(K^n)$ and $C(R^m\ )$.

Alice keeps the pairs (G_i , F_i) and computes additionally for herself $H=T_1^{-1}\Delta^{D(n,K)}(Rev(B))$, $H^{-1}=\Delta^{D(n,K)}(B)T_1$ and $Z=T_2^{-1}\Delta^{DA(m,K)}(Rev(D))$, $Z^{-1}=\Delta^{A(m,K)}(D)T_2$.

The homomorphism δ: $GD(n,\ Q)\rightarrow GA(m,Q)$ of the diagram is tame, i.e. its image can be computed in polynomial time in variable n. The triple $(GD(n,\ Q),\ GA(m,Q),\ \delta)$ can be considered as a platform of *Tahoma protocol* introduced in [21], word *tahoma* stands for abbreviation of *tame homomorphism*.

Tahoma word prototocol exchange scheme: Alice uses (G_i , F_i) and pairs (H, H^{-1}) and (Z, Z^{-1}) from affine Cremona groups $C(K^n)$ and $C(R^m\ )$ as starting data of the following protocol (steps *S1-S4*)

S1. Alice sends pairs (G_i , F_i), $i=1,2,\ldots,r$ to Bob.

S2. Bob takes formal alphabet $A=\{\ z_1,\ z_2,\ldots,\ z_r\ \}$ and writes a word $w=u_1,u_2,\ldots,\ u_k$ where $u_i\ \epsilon A$. He computes the specializations g and f for w of kind $u_j=G_i$ and $u_j=F_i$ if u u_j coincides with $z_i,\ \ i=1,2,\ldots,r$ in groups $<G_1,\ G_2,..,G_r>\ <\ GD(n,K)$ and $<F_1,\ F_2,\ldots,F_r><\ GA(m,R)$ respectively.

S3. Bob send g to Alice and keeps f for herself.

S4. Alice computes $f_1=Hg\ H^{-1}$, $f_2=\delta(f_1)$ and gets collision map f as $Zf_2\ Z^{-1}$.

Remark. Adversary has to find the decomposition of f into Generators $G_1,\ G_2,\ldots,\ G_r$. The polynomial algorithms to solve this problem in ordinary Turing machine or Quantum computer are unknown.

6.2 Inverse Tahoma word protocol.

Alice changes F_i onto their inverses computed via elements

$*D_i=Rev(D)(Rev(C_i))D$, $*CD_i=\Delta^{A(m,K)}(*D)$ and $*F_i=\ T_2\ ^{-1}*CD_iT_2.$

Alice sends pairs (G_i , $*F_i$) to Bob.

As in previous algorithm he takes formal alphabet $A=\{\ z_1,\ z_2,\ldots,\ z_r\ \}$ and writes a word $w=u_1,u_2,\ldots,\ u_k$ where $u_i\ \epsilon A$. He computes the specializations g or w of kind $u_j=G_i$ and if u_j coincides with $z_i,\ \ i=1,2,\ldots,r$ in groups $<G_1,\ G_2,..,G_r>\ <\ GD(n,K)$. Bor forms the reverse word $*w=u_k,u_{k-1},\ldots,\ u_{.1}$ After that he substitutes $*F_i$ and computes corresponding word f in group $<F_1,\ F_2,\ldots,F_r><\ GA(m,R)$.

Bob send g to Alice. *She* computes $f_1=HgH^{-1}$, $f_2=\delta(f_1)$ and gets map f^{-1}as Zf_2 Z^{-1}.

Correspondents can exchange information in secure way. Alice writes message $(p)=(p_1, p_2,\dots,p_m)$, $p_u \in R$ computes cipherext $f^{-1}(p)=(c)$ and sends it to Bob. He decrypts with his map *f.* In his turn Bob uses *f* as encryption map and Alice decrypts with her f^{-1}.

6.3 Group enveloped Diffie Hellman protocol based on homomorphism of *GD(K)* onto *GA(K).*

Alice uses (G_i , F_i), i=1, …, r and pairs (H, H^{-1}) and (Z, Z^{-1}) from affine Cremona groups $C(K^n)$ and $C(R^m)$ as in 4.1 together with $*F_i$ considered in 6.2. She takes also $*G_i$ computed via elements $*B_i=Rev(B)(Rev(C_i))B$, $*CB_i=\Delta^{D(m,K)}(*B)$ and $*G_i= T_1^{-1}*CB_iT_{1.}$. Alice takes string C from $\Sigma(Q)$ and positive integer k_A. She computes symbolic string C^d , $d=k_A$ in $\Sigma(Q)$ and $\Delta^{D(m,K)}(Rev(B)CB)$ *and* $\Delta^{A(m,K)}(Rev(D)\ C^dD)$. Finally Alice constructs $G= T_1^{-1}\Delta^{D(m,K)}(Rev(B)CB)T_1$ and $G_A = T_2^{-1}\Delta^{A(m,K)}(Rev(D)\ C^dD)T_2$.

She sends (G_i , F_i), ($*G_i$, $*F_i$), $i=1, \dots, r$ to Bob together with G and G_A. Bob selects positive integer $l=k_B$ and word $w=u_1,u_2,\dots, u_k$ as in algorithm 6.1. He forms $*w=u_k,u_{k-1},\dots, u_{.1}$ similarly to 6.2.

Bob computes the specializations g or w of kind u_j=G$_i$ and if u_j coincides with $z_{i,}$ $i=1,2,\dots,r$ in the sub group $<G_1, G_2,..,G_r>$ of $GD(n,K)$. He computes g^{-1} as specialization of $*w$ such that u_j=*G$_i$ if u_j coincides with z_i, $i=1,2,\dots,r$ .Similarly Bob computes the specialization h of w of kind u= $u_j=F_i$ if u_j coincides with z_i and h^{-1} with appropriate specialization of $*w$.

He computes element $U=g^{-1}G^lg$ and sends it to Alice but keeps for himself $h^{-1}G^l_Ah=W$.

Alice can recover the collision map W via computations of $W_1=HUH^{-1}$, $\delta(W_1)=W_2$, $W_3= W_2^d$ and $W= ZW_3Z^{-1}$**.**

Remark. Adversary has to find the decomposition of U into generators G, $G_1, G_2,\dots, G_r$ in rhe affine Cremona group.

6.4 Inverse group enveloped Diffie - Hellman protocol.

This algorithm uses same data. Alice computes $G_A = T_2^{-1}\Delta^{A(m,K)}(Rev(D)$ $C^dD)T_2$. but instead of computation of G as $T_1^{-1}\Delta^{D(m,K)}(Rev(B)CB)T_1$ she computes G as $T_1^{-1}\Delta^{D(m,K)}(Rev(B)(Rev(C)B)T_1$, i. e. changes G for its inverse.

So Bob gets pair (G_A, G) and complete same steps as in the case of algorithm 6.3. In this new version he gets same W but new element U is an inverse of the map from previous version.

Alice computes $W_1=HUH^{-1}$, $\delta(W_1)=W_2$, $W_3= W_2^d$ and $W_4= ZW_3Z^{-1}$**,** but obtained W_4 is the inverse of W.

So in algorithm 6.4 correspondents elaborate mutually inverse maps W (Bob) and W^{-1} **(**Alice). Alice writes message $(p)=(p_1, p_2,...,p_m)$, $p_u \in R$ computes cipherext W $^{-1}(p)=(c)$ and sends it to Bob. He decrypts with his map W. In his turn Bob uses W as encryption map and Alice decrypts with her W^{-1}.

So like in the case of 6.2 Alice and Bob can exchange messages in a secure way.

6.5 General complexity estimates for the protocols.

Let us assume that Alice is going to use the homomorphism between $D(n,Q)$ and $A(m,Q)$ for $m<n$ and $m=O(n)$. Rings K and R are finite extensions of Q. So we can assume that cost of arithmetic operation in these commutative rings is $O(1)$. We will count number arithmetical operations of commutative ring K which she need to generate an element of $g=G(n, K)$ which corresponds to symbolic computation with the key of length $O(1)$.

Without loss of generality we may assume that correspondents are involved with Inverse Tahoma Protocol. Counting steps of recurrent process of maps generation via the semigroup compression homomorphisms gives us $O(n)$ operations. Alice chooses already computed affine transformations T and T^{-1}. Alice forms elements $b1, b2, \dots ,br$ from $G(n, K)$ together with their inverses and homomorphic images μ '(bi), $i=1, 2,..., r$ from $G(m, K)$ in time $O(n)$. She takes $T^{-}$and T^{-1} from $AGLn(K)$ and forms $ai= T^{-}biT^{-1}$ and $a'i= T(bi^{-1})T^{-1}$ in time $O(n^7)$.

Bob receives the list of pairs ai, $a'i$, $i=1, 2,..., r$. He computes chosen word of kind $a=a_{i1}^{k1}a_{i2}^{k2}..., a_{it}^{kt}$ for chosen finite parameter t and integers ki, $i=1, 2,...,t$ in time $O(n^{13})$ operations and sends it to Alice. Bob writes his message $p=(p_1, p_2, ,..., p_m)$. To form ciphertext he applies to p transformation a'_{it} with multiplicity k_t, a'_{it-1} with multiplicity $k_{t-1}, ..., a'_{i1}$ with multiplicity k_1 and forms ciphertext c. It takes him $O(n^3)$ elementary operations. Alice computes cubical $b=aT$ with $O(n^5)$ operations. After she gets $d= T^{-1}b$ in time $O(n^7)$. Alice easily gets μ(d) and computes $e=T_1d$ and $f=e\ T_1^{-1}$. She computes p as $f(c)$. The last step cost her $O(n^3)$ elementary ring operations.

Remark. The complexity of algorithm execution is O(n^{13}). More accurate evaluation in terms of number d of monomial terms in the standard form of cubical maps gives us complexity Cd$^4n^{-3}$, where C is independent constant.

Studies of parameter d is presented in the next section. Computer simulations demonstrate that in the case of finite fields of characteristic 2 parameter d=O(n^3) and algorithm can be executed in time O(n^9).

Simulations allow us to get similar bound in the cases of arithmetical and Boolean rings.

7. APPENDIX 1. On safe exchange of symbolic transformations

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

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

Alice and Bob use *tahoma word protocol* or symbolic Diffie-Hellman protocol to elaborate the collision map g acting on K^n. After this step Alice sends Ω and transformation $h=f+g$ to Bob. Now Bob can get f as h-g. He writes plaintext p from Ω and sends ciphertext $c=f(x)$. Alice uses her data for the decryption.

Remark 7.1.

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

Other deformations.

Alice and Bob agree (via open channel) on a deformation rule $D(f)$ for multivatiate rule f from affine Cremona semigroup. For example, it can be multiplication, i.e. f is the rule $x_i \rightarrow f_i\ (x_1, x_2, \ldots, x_n\ ), i=1, 2,\ldots, n$ and g is the rule$x_i \rightarrow g_i(x_1\ , x_2, \ldots, x_n\ ), i=1, 2,\ldots, n$ and Alice sends tuple of polynomials $f_i g_i\ , i=1, 2,\ldots, n$. Bob uses division to restore f. Instead of addition deformation rule (sending of $x_i \rightarrow f_i(x_1, x_2, \ldots, x_n\ ) +g_i\ (x_1, x_2, \ldots, x_n\ ), i=1, 2,\ldots, n$)Alice can use deformation with adding an element $K[x_1, x_2, \ldots, x_n]^n$ obtained from g via the usage of s-time conducted derivation δ^s, where $\delta = d/\ x_1 + d/d\ x_2 + \ldots + d/d\ x_n$ (rule $x_i \rightarrow f_i\ (x_1\ , x_2\ , \ldots, x_n) +\delta^s g_i\ (x_1, x_2, \ldots, x_n\ ), i=1, 2,\ldots, n$).The last deformation is interesting because in many cases we can achieve the equality of degrees for f and $D(f)$. It is easy to continue this list of possible deformation rules.

Remark 7.2.

Let us assume that $\Omega=K^n$. So $f=f(n)$ is a bijection. Assume that degrees of nonlinear maps $f(n)$ are bounded by constant d . Let us assume that the adversary has option to intercept some pairs plaintext - ciphertext (leakage from Bob's data). In case of interception of $O(n^d)$ adversary has chance for a successful linearisation attack and get the map f. For example if d=3 then linearisation attack cost is $O(n^{10})$. After that adversary has to find the inverse function for f like in the case of multivariate public key.

To prevent "transition to knowledge" of an encryption multivariate map Alice (or Bob) can arrange a new session with protocol and a transmission of new deformed encryption rule for which secret data for decryption is known.

Remark 7.3.

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

8. APPENDIX 2. Graphs *A(n,q)* and *D(n,q)*, digital condenced matters physics effect.

We can substitute graph $A(n, K)$ for other linguistic graph L of type $(1,1, n-1)$ defined over the commutative ring K and rewrite the content of section 5. We use graphs $A(n,K)$ and well known linguistic graph $D(n,K)$ of this type to implement all algorithm of previous section. Graphs $D(n, K)$ are bipartite with set of vertices $V=PUL$, $|P\cap L=0|$. A subset of the vertices P is called the set of *points* and another subset L is called the set of *lines*. Let P and L be two copies of Cartesian power K^n, where $n\geq 2$ is an integer. Two types of brackets are used in order to distinguish points from lines. It has a set of vertices (collection of points and lines), which are n-dimensional vectors over K:($\boldsymbol{p}$) = $(p_1, p_2 , p_3, p_4, . . . , p_i, p_{i+1}, p_{i+2}, p_{i+3}, . . ., p_n)$, [$\boldsymbol{l}$] = $[l_1, l_2, l_3, l_4, . . . , l_i, l_{i+1},l_{i+2},l_{i+3}, . . ., l_n]$. The point ($\boldsymbol{p}$) is incident with the line [$\boldsymbol{l}$] , if the following relations between their coordinates hold: $l_2-p_2=l_1p_1$, $l_3-p_3=l_2\mathrm{p}_1$, $l_4-p_4=l_1p_2$, $l_i-p_i=l_1p_{i-2}$, $l_{i+1}-p_{i+1}=l_{i-1}p_1$, : $l_{i+2}-\mathrm{p}_{i+2}=l_ip_1$: $l_{i+3}-p_{i+3}=l_1p_{i+1}$ where $i\geq 5$. Connected component of edge-transitive graph $D(n,q)$ is denoted by $CD(n,q)$ [22]. Notice that all connected components of the natural projective limit $D(q)$ of graphs $D(n,q)$, $n\to\infty$ infinite graph $D(q)$ are q-regular trees.

Let us denote as $G'(n,K)$ the group of elements of kind $g=\dot{\eta}(C)$ *of irreducible computation* computation $C =(a_1, a_2 , ... , a_t)$ in the case of graphs $D(n,K)$.

We present time of generation (in ms) of element g from G(n,K) and $G'(n, K)$ in the cases of graphs $A(n,K)$ and $D(n,K)$ and number $M(g)$ of monomial terms for g.

We refer to parameter t as *length of word.* We can see the ‘’condensed matters physics’’ digital effect. If t is ’’sufficiently large’’, then $M(g)$ is independent from t constant c. It means that the density of cubical collision map in all algorithm is simply c

We have written a program for generating of elements and for encrypting text using the generated public key. The program is written in C++ and compiled with the gcc compiler. We used an average PC with processor Pentium 3.00 GHz, 2GB memory RAM and system Windows 7. We have implemented three cases:

1. T and T_1 are identities,

2. T and T_1 are maps of kind $x_1 \rightarrow x_1 + a_2x_2 + \underline{a_3x_3} + \ldots + a_tx_t,$, $x_2 \rightarrow x_2$, $x_3 \rightarrow x_3$, $\ldots$, $x_t \rightarrow x_t$, $a_i \neq 0$, $i=1,2,\ldots,t$ (linear time of computing for T and T_1), where $t=n$ *and* $t=m$, respectively.
3. $T= Ax+ b$, $T_1= A_1x+ b_1$; matrices A, A_1 and
   Vectors b, b_1 have mostly nonzero elements.

The tables 1-6 present the number of monomials depending on the number of variables (n) and the password length in all three cases and both families of graphs *D(n,K)* and *A(n,K)*, where K is a finite field of characteristic 2. The tables 7-12 present the time (in milliseconds) of the generation of public key monomials depending on the number of variables *n* and the length of the word in all three cases and both families of graphs *D(n,K)* and *A(n,K)*. In [29],[30] and [31] this similar program *for* program the case when *K* is Boolean ring were used for investigation of classical Diffie - Hellman protocol for cyclic group <*g*> and corresponding El Gamal cryptosystem. Currently we expand this computer package on the case of commutative rings Z_m, where *m* is power of *2*.

Illustrative example.

Let Alice selects the graph $A(n,K), K = F_{2^{32}}$,*n=64* and its canonical homomorphism onto graph *A(32, K)*, which induces canonical homomorphism Δ <u>of </u>*G(64, K)* onto *G(32,K)*. She takes two irreducible elements of $\sum = \sum(K)$, $\alpha=(a_1, a_2, \ldots, a_{16})$ and $\beta=(b_1, b_2, \ldots, b_{16})$ of pseudorandom kind, use homomorhism $\acute{\eta}' = \acute{\eta}'_{64}$ of $\sum$ into *G(64, K)* and gets elements $a=\acute{\eta}'(\alpha)$ and $b= \acute{\eta}'(\beta)$.

Alice forms string $h=(h_1, h_2, \ldots, h_t)$. $t=16$ and the reverse string $rev(h)=(-h_t+h_{t-1}, -h_t+h_{t-2}, \ldots, -h_t+h_1, -h_t)$ for which $n= \acute{\eta}'(h)=n$ and $n'= \acute{\eta}'(rev(h))$.

She takes affine transformation *T* of the vector space F_q^{64} , $q=2^{32}$ and its inverse T^{-1} and forms elements $a^1=Tnan'T^{-1}$ and $b^1=Tnbn'T^{-1}$.

Alice takes $d=(d_1, d_2\_, \ldots, d_t)$ and the pair $m=\acute{\eta}'_{32}(d)$, $m'= \acute{\eta}'_{32}\ (rev(d))$. She forms $a^2=Sm\ \acute{\eta}'_{32}(\alpha)m'S^{-1}=Sm\ \acute{\eta}'_{32}(\alpha)m'S^{-1}$ and $b^2=Sm\ \acute{\eta}'_{32}(\beta)m'S^{-1}$ where *S* is the bijective affine transformation of 32 dimensional vector space. She sends pairs (a^1, a^2), (b^1, b^2), to Bob. Let us assume that Alice uses transformation *T* and *S* of kind 3. It means that cubical transformations a^1 and b^1 are given by lists with 399424 monomial terms and transformations a^2, b^2 are given by their 50720 monomial terms (see table 6).

Bob takes word $w= x^{s1}y^{r1}\ x^{s2}y^{r2} \ldots$ of some lengths k, $k \geq 3$ (even or odd), where *s1*, *s2*,…and *r1*, *r2*, …are positive integers.

He substitutes a^1 and b^1 instead of *x* and *y* (or *y* and *x*) and compute corresponding transformation *c* from affine Cremona semigroup of 64 dimensional vector space over finite field F_q. The cubical transformations c is presented by its 388424 monomial terms. Bob substitutes the collision map *c'* via substitution of a^2 and b^2 in word *w* instead of *x* and *y*. Collision element *c'* is given by the list of its 50720 monomials.

Bob sends the transformation c to Alice. She computes $c^1 = T^{-1}n'cnT$ which contains 1810 (monomial terms) (see table 4). Alice computes $c^2=\Delta(c^1)$ given by 770 terms. She reconstructs the collision map as $Sm\, c^2\, m'S^{-1}$.

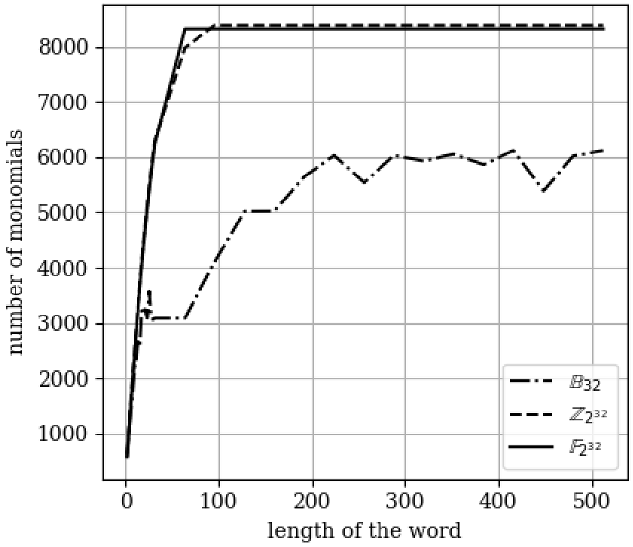

Fig. 1. Number of monomial terms of the cubic map induced by the graph ($n = 128$) (graph $D(n, K)$, $K = B(32), Z_{2^{32}}, F_{2^{32}}$), case I.

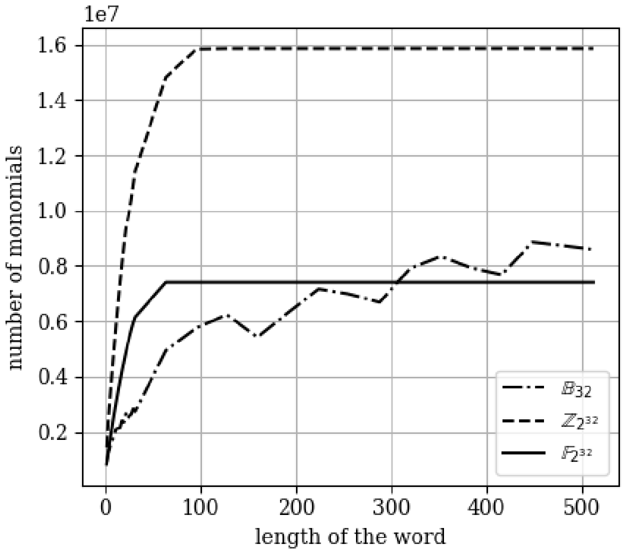

Fig. 2. Number of monomial terms of the cubic map induced by the graph ($n = 128$) (graph $D(n, K)$, $K = B(32), Z_{2^{32}}, F_{2^{32}}$), case II

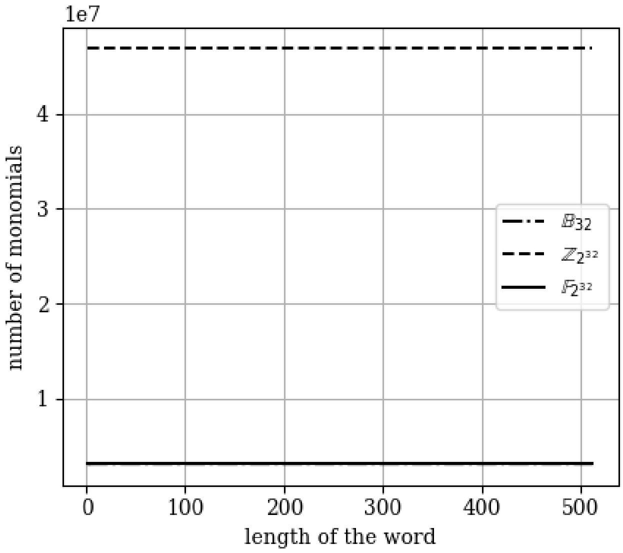

Fig. 3. Number of monomial terms of the cubic map induced by the graph ($n = 128$) (graph $D(n, K)$, $K = B(32), Z_{2^{32}}, F_{2^{32}}$), case III

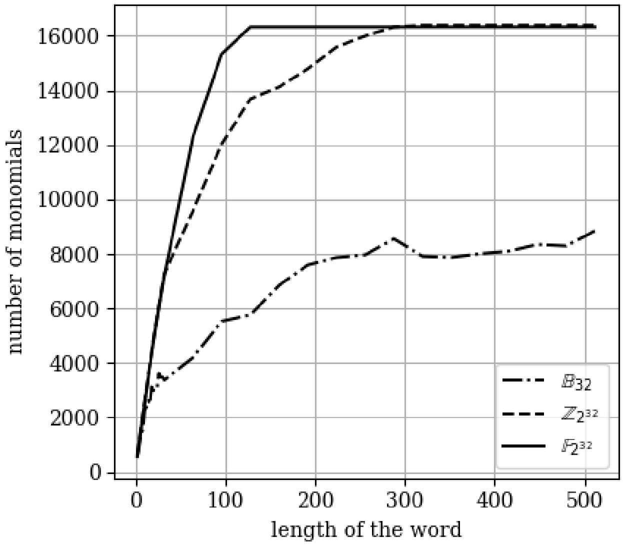

Fig. 4. Number of monomial terms of the cubic map induced by the graph ($n = 128$) (graph $A(n, K)$, $K = B(32), Z_{2^{32}}, F_{2^{32}}$), case I

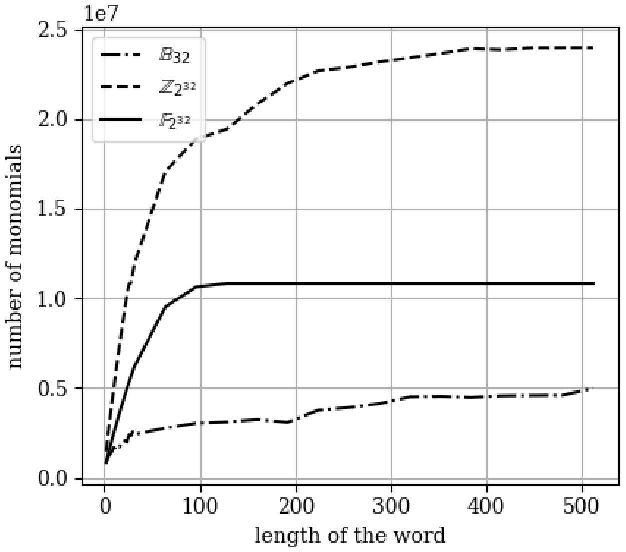

Fig. 5. Number of monomial terms of the cubic map induced by the graph ($n = 128$) (graph $A(n, K)$, $K = B(32), Z_{2^{32}}, F_{2^{32}}$), case II

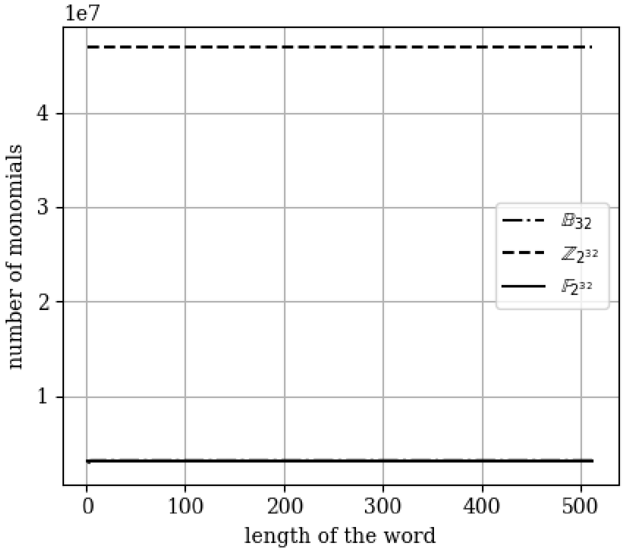

Fig. 6. Number of monomial terms of the cubic map induced by the graph ($n = 128$) (graph $A(n,K)$, $K = B(32), Z_{2^{32}}, F_{2^{32}}$), case III

Table 1. Number of monomial terms of the cubic map induced by the graph $D(n,F_{2^{32}})$, case I

	length of the word				
n	**16**	**32**	**64**	**128**	**256**
16	145	145	145	145	145
32	544	545	545	545	545
64	1584	2112	2113	2113	2113
128	3664	6240	8320	8321	8321

Table 2. Number of monomial terms of the cubic map induced by the graph $D(n,F_{2^{32}})$, case II

	length of the word				
n	**16**	**32**	**64**	**128**	**256**
16	3649	3649	3649	3649	3649
32	41355	41356	41356	41356	41356
64	440147	529052	529053	529053	529053
128	3823600	6149213	7405944	7405945	7405945

Table 3. Number of monomial terms of the cubic map induced by the graph $D(n,F_{2^{32}})$, case III

	length of the word				
n	**16**	**32**	**64**	**128**	**256**
16	6544	6544	6544	6544	6544
32	50720	50720	50720	50720	50720
64	399424	399424	399424	399424	399424
128	3170432	3170432	3170432	3170432	3170432

Table 4. Number of monomial terms of the cubic map induced by the graph $A(n,F_{2^{32}})$, case I

	length of the word				
n	**16**	**32**	**64**	**128**	**256**
16	250	250	250	250	250

32	770	1010	1010	1010	1010
64	1810	3074	4066	4066	4066
128	3890	7202	12290	16322	16322

Table 5. Number of monomial terms of the cubic map induced by the graph $A(n,F_{2^{32}})$, case II

	length of the word				
n	**16**	**32**	**64**	**128**	**256**
16	5623	5623	5623	5623	5623
32	53581	62252	62252	62252	62252
64	454375	680750	781087	781087	781087
128	3607741	6237144	9519921	10826616	10826616

Table 6. Number of monomial terms of the cubic map induced by the graph $A(n,F_{2^{32}})$, case III

	length of the word				
n	**16**	**32**	**64**	**128**	**256**
16	6544	6544	6544	6544	6544
32	50720	50720	50720	50720	50720
64	399424	399424	399424	399424	399424
128	3170432	3170432	3170432	3170432	3170432

Table 7. Generation time for the map (ms) $D(n,F_{2^{32}})$, case I

	length of the word				
n	**16**	**32**	**64**	**128**	**256**
16	12	24	32	52	100
32	64	140	292	592	1192
64	1044	2261	4833	9985	20270
128	15821	33846	74340	160213	331895

Table 8. Generation time for the map (ms) $D(n,F_{2^{32}})$, case II

	length of the word

n	16	32	64	128	256
16	28	48	100	212	420
32	284	648	1372	2816	5712
64	3229	8397	19454	41568	85783
128	55075	139366	357361	824166	1758059

Table 9. Generation time for the map (ms) $D(n,F_{2^{32}})$, case III

	length of the word				
n	**16**	**32**	**64**	**128**	**256**
16	76	140	268	524	1036
32	1224	2328	4541	8968	17828
64	21889	40417	77480	151592	299844
128	453798	812140	1526713	2946022	5792889

Table 10. Generation time for the map (ms) $A(n,F_{2^{32}})$, case I

	length of the word				
n	**16**	**32**	**64**	**128**	**256**
16	4	12	24	48	96
32	56	132	288	600	1232
64	996	2100	4644	10068	20933
128	15645	33489	74244	167454	364707

Table 11. Generation time for the map (ms) $A(n,F_{2^{32}})$, case II

	length of the word				
n	**16**	**32**	**64**	**128**	**256**
16	20	60	128	260	540
32	308	788	1776	3760	7716
64	3193	8858	23231	53196	113148
128	54031	137201	368460	950849	2164037

Table 12. Generation time for the map (ms) $A(n, F_{2^{32}})$, case III

	length of the word				
n	**16**	**32**	**64**	**128**	**256**
16	76	148	288	576	1148
32	1268	2420	4700	9268	18405
64	22144	40948	78551	153784	304240
128	460200	819498	1532277	2970743	5836938

9. Conclusion.

We propose Post Quantum Cryptography information security solutions based on the complexity of the following problem Cremona Semigroup Word Decomposition (CSWD).

Thus we hope that introduced algorithms can be considered as serious candidates to be postquantum cryptographical tools. We believe that future studies of cryptanalitics confirm that CSWD problem remains unsolvable on ordinary Turing Machine and Quantum Computer under the condition of stability of platform S. Hope that the idea of an alternative disclosure of hidden homomorphism will attract attention of cryptanalytics.

Complexity estimates for both correspondents demonstrate possibility of current usage of algorithms. Computer simulations demonstrate an interesting fase transition effect, which allow to predict the density of the collision maps of key exchange protocols and their inverse forms. This effect also demonstrates feasibility of proposed cryptographic schemes. Direct and inverse protocols to elaborate collision multivariate transformation of free module K^n of predictable density can be used together with stream cipher working with data written in alphabet K or passwords written in this alphabet.

Correspondents can use collision maps to add them to part of password orpart of plaintext or part of ciphertext. There is an option to deformate part of passwords, plaintext and ciphertext by outcomes of inverse protocols.

References.

1. J. Ding., J. E. Gower, D. S. Schmidt., Multivariate Public Key Cryptosystems, 260. Springer, Advances in Information Security, v. 25, (2006).
2. N. Koblitz, Algebraic aspects of cryptography, Springer (1998)., 206 P.
3. L. Goubin, J.Patarin, Bo-Yin Yang, Multivariate Cryptography. Encyclopedia of Cryptography and Security, (2nd Ed.) 2011, 824-828.
4. 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.

5. 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.
6. 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.
7. 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.
8. Alexei Myasnikov; Vladimir Shpilrain; Alexander Ushakov (2008). Group-based Cryptography. Berlin: Birkhäuser Verlag.
9. Zhenfu Cao (2012). New Directions of Modern Cryptography. Boca Raton: CRC Press, Taylor & Francis Group. ISBN 978-1-4665-0140-9.
10. Benjamin Fine, et. al. "Aspects of Non abelian Group Based Cryptography: A Survey and Open Problems". arXiv:1103.4093.
11. Alexei G. Myasnikov; Vladimir Shpilrain; Alexander Ushakov (2011). Non-commutative Cryptography and Complexity of Group-theoretic Problems. American Mathematical Society.
12. Anshel, I., Anshel, M., Goldfeld, D.: An algebraic method for public-key cryptography. Math. Res.Lett. 6(3–4), 287–291 (1999).
13. 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).
14. 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)
15. Maze, G., Monico, C., Rosenthal, J.: Public key cryptography based on semigroup actions. Adv.Math. Commun. **1**(4), 489–507 (2007)
16. 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
17. 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 (to appear in 2019).
18. 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
19. V. Ustimenko, On the families of stable transformations of large order and their cryptographical applications, Tatra Mt. Math. Publ., 70 (2017), 107-117.
20. V. Ustimenko, On desynchronised multivariate El Gamal algorithm, Cryptology ePrint Archive, 712, 2017.
21. V. Ustimenko, On new symbolic key exchange protocols and cryptosystems based on hidden tame homomorphism,. *Dopov. Nac. akad. nauk Ukraine,2018, n 10, pp.26-36.*
22. F. Lazebnik, V. Ustimenko and A. Woldar, New Series of Dense Graphs of High Girth, Bull (New Series) of AMS, 1995, v. 32, pp.73—79.
23. V. Ustimenko, Coordinatisation of Trees and their Quotients, in th Voronoj's Impact on Modern Science, Kiev, Institute of Mathematics, 1998, vol. 2, 125-152.

24. V. Ustimenko, U. Romanczuk, On Extremal Graph Theory, Explicit Algebraic Constructions of Extremal Graphs and Corresponding Turing Encryption Machines, in Series: Studies in Computational Intelligence, Vol. 427, Springer, January , 2013, 257-285.
25. V. Ustimenko, Maximality of affine group, hidden graph cryptosystem and graph's stream ciphers, Journal of Algebra and Discrecadete Mathematics, 2005, v.1, pp 51-65
26. V. Ustimenko, Linguistic Dynamical Systems, Graphs of Large Girth and Cryptography, Journal of Mathematical Sciences, Springer, vol.140, N3 (2007), pp. 412-434.
27. V. Ustimenko, Graphs with special arcs and cryptography , Acta Applicandae Mathematicae (Kluwer) 2002, 74,117-153.
28. V. Ustimenko. On the graph based cryptography and symbolic computations. Proceedings of International Conference on Application of Computer Algebra, ACA-2006,v1, Serdica Journal of Computing, 2007, pp 131-156.
29. M. Klisowski, Zwiększenie bezpieczeństwa kryptograficznych algorytmów wielu zmiennych bazujacych na algebraicznej teorii grafów, PhD thesis, Czestochowa, 2014.
30. M. Klisowski, V. Ustimenko, Graph based cubical multivariate maps and their cryptographical applications, in ‘’Advances on Superelliptic curves and their Applications’’, IOS Press, NATO Science for Peace and Security series –D: Information and Communication Security, vol 41, 2014, pp. 305 -327.
31. M. Klisowski, V. A. Ustimenko, On the Comparison of Cryptographical Properties of Two Different Families of Graphs with Large Cycle Indicator, Mathematics in Computer Science, 2012, Volume 6, Number 2, Pages 181-198.
32. McEliece, Robert J. (1978). "A Public-Key Cryptosystem Based On Algebraic Coding Theory" . DSN Progress Report. 44: 114–116, Bibcode:1978DSNPR..44..114M.
33. V. Ustimenko, M. Klisowski , On Noncommutative Cryptography with cubical multivariate maps of predictable density, Proceedings of ‘’Computing 2019’’ conference, London, 16-17, July, Springer, Advances in Intelligent Systems and Computing (to appear).
34. V. Ustimenko, On semigroups of multiplicative Cremona transformations and new solutions of Post Quantum Cryptography, Cryptology ePrint Archive, 133, 2019
35. 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
36. 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.