On symbolic computations over arbitrary commutative rings and cryptography with the temporal Jordan-Gauss graphs.

Vasyl Ustimenko [1,2]

[1)]Royal Holloway University of London, UK, [2)] Institute of Telecommunications and the Global Information Space, Kyiv, Ukraine, e – mail: Vasyl.Ustymenko@rhul.ac.uk

Abstract. The paper is dedicated to Multivariate Cryptography over general commutative ring K and protocols of symbolic computations for safe delivery of multivariate maps. We consider iterative algorithm of generation of multivariate maps of prescribed degree or density with the trapdoor accelerator, i.e. piece of information which allows to compute the reimage of the map in polynomial time. The concept of Jordan-Gauss temporal graphs is used for the obfuscation of known graph based public keys and constructions of new cryptosystems. We suggest use of the platforms of Noncommutative Cryptography defined in terms of Multivariate Cryptography over K for the conversion of Multivariate Public Keys into El Gamal type Cryptosystems. Some new platforms are introduced.

Keywords: Public keys of Multivariate Cryptography over general commutative ring K, Noncommutative Cryptography, key exchange protocols, semigroups of transformations.

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

1. Introduction

The paper is dedicated to the constructions of special multivariate maps on affine space K^n over finite commutative ring with the unity. We are interested in maps of prescribed bounded by constant degree or unbounded degree but prescribed density which has a trapdoor accelerator, i.e pieces of information such that its knowledge allows us to compute the reimage of the map in polynomial time.

One of the applications of these maps is the following scheme of access control to the resources of Information System. Administrator A of the Information System (IS) possesses the map F in n-variables and its trapdoor accelerator T. He/she is going to give secure access to the resources of IS to trusted user ***U.*** So A and U executes selected protocol of Noncommutative Cryptography in terms of special subsemigroup S of the affine Cremona semigroup of all multivariate maps of K^n into itself. The output of the protocol X can be used by A and U for the creation of its *deformation* $G(X)$ which is a transformation of K^n

Administrator sends $F+G(X)$ to U. User restores F. Now A is able to create pseudorandom or genuinely random password $(p_1, p_2, ..., p_n) = p$ as the condition to enter the system. Administrator solves the equation $F(x)=b$ and sends the solution $x=(d_1,$

$d_2,..., d_n)=d$ to the user together with the link for entering the password. User U gets the password as $F(d_1, d_2,...., d_n)$.

Administrator has the option to change the password several times working with the same map F with the trapdoor accelerator. He/she is able to change F via a new session of the protocol and delivery scheme.

The security of this scheme rests on the security of selected Postquantum Protocol on Noncommutative Cryptography. We describe Twisted Diffie-Helman protocol which use the complexity of Conjugation Power Problem of the semigroup ${}^nES(K)$ of Eulerian endomorphisms of $K[x_1, x_2,..., x_n]$ which sends each variable x_i, $i=1,2,..., n$ to a monomial term. Some other protocols of Noncommutative Cryptography with the platform ${}^nES(K)$ are given in [1].

For each positive integer d, $d\geq 2$ we present the multivariate map of degree d with the trapdoor accelerator. In fact we present the iterative process of expansion of initial map $\boldsymbol{F_0}$ which can be a bijective multivariate nonlinear map of degree at most d on K^n with the trapdoor accelerator T or an element of general affine group $AGL_n(K)$. The input parameters are positive integers $m(1), m(2),..., m(k), k\geq 2$. The step i, $i=1, 2,..., k$ of the algorithm produces the multivariate map G_i of degree d on the $K^{n+m(1)+m(2)+...+m(i)}$ with the trapdoor accelerator T_i.

Similarly we can take polynomial surjective map F_0 of K^n onto K^r of degree at most d with the trapdoor accelerator T and get the sequence of surjective polynomial multivariate maps of $K^{n+m(1)+m(2)+...+m(i)}$ onto $K^{r+m(1)+m(2)+...+m(i)}$ of degree d with the trapdoor accelerators.

So we can use known construction of multivariate cryptography over the general maps with trapdoor accelerators or linear maps on affine spaces for the construction of new maps together with the polynomial algorithm to compute reimage.

We define the density of the multivariate polynomial in n variables as the number of its monomial terms. The density of multivariate map $F : (x_1, x_2, ..., x_n) \rightarrow (f_1 (x_1, x_2, ..., x_n), f_2(x_1, x_2, ..., x_n),...., f_2(x_1, x_2, ..., x_n),...., f_m(x_1, x_2, ..., x_n))$ is the maximal value of densities of f_i for $i=1, 2,..., m$.

We also will work with the multivariate maps in n variable of unbounded degree and prescribed density $O(n^{\lambda})$. Let K^* stands for the multiplicative group of K. Assume that K^* is nontrivial. We say that multivariate map F of K^n to itself has multiplicative trapdoor accelerator T if the restriction of F onto $(K^*)^n$ is injective map and the knowledge of T allows to compute the reimage of the element from $F((K^*)^n)$ in a polynomial time.

For each nonnegative rational number λ we present the explicit constructions of multivariate maps of density λ with unbounded degree and multiplicative trapdoor accelerator. Additionally we present the iterative process of the expansion of the selected initial map F_0 which is a multivariate nonlinear map of density $O(1)$ on K^n

with unbounded degree and the multiplicative trapdoor accelerator *T*. The input consists of positive integers *m(1), m(2),..., m(k), k≥2* and some internal parameters which are nonnegative rational numbers.

The step *i, i=1, 2,..., k* of the algorithm produces the multivariate map G_i of polynomial density on the $K^{n+m(1)+m(2)+...+m(i)}$ with the multiplicative trapdoor accelerator T_i.. Appropriate choice of internal parameters allows us to construct G_k of prescribed density $O((n+m(1)+m(2)+...+m(k))^{\lambda})$.

We can use multivariate maps of unbounded degree and prescribed polynomial density with the multiplicative trapdoor accelerator instead of maps of bounded degree in the presented above scheme of access control. We can use the same protocol of Noncommutative Cryptography and the same platform ${}^nES(K)$ of Eulerian transformations. The modification of the deformation rule will be presented.

Let us consider the case of finite commutative ring *K* of the cardinality *O(1)* with nontrivial multiplicative group. In the case of the map *F* of unbounded by constant degree of size *O(n)* and of density *O(1)* with the multiplicative trapdoor accelerator we use term pseudolinear map. The complexity of computation of $F(p), p\epsilon(K^*)^n$ is $O(n^2)$. In the case of density $O(n^{\lambda}), \lambda<1$ we use the term of sub quadratic map. The complexity of computation of $F(p), p\epsilon (K^*)^n$ is $O(n^{2+\lambda})$.

It is better then in the case of quadratic map on the space K^n. If density is *O(n)* we say that we have pseudo quadratic map.

We hope that defined in the paper wide variety of the quadratic or cubic maps with the trapdoor accelerators and the varieties of pseudo-linear, sub quadratic and pseudo quadratic maps with the multiplicative trapdoor accelerators can be effectively used in the presented above scheme of the access control of Information System.

These varieties are defined via the symbolic computations in terms of algebraic graphs defined by the systems of nonlinear algebraic equations over the finite commutative ring *K* with unity or temporal analogue of these graphs for which generic equations are changeable with the change of time. The sequences of pseudorandom or genuinely random graphs can be used for the change of coefficients in time dependent algebraic equations.

For the design of maps we use Jordan -Gauss graphs which are bipartite graph with partition sets K^n and K^m given via quadratic equations such that the neighbourhood of the vertex is the solution set of linear system of equations written in its row-echelon form.

Subsection 2.1 of Section 2 contains basic definitions of affine Cremona semigroup and group of endomorphism of multivariate ring $K[x_1, x_2,..., x_n]$, endomorphisms with the trapdoor accelerators. It contains the discussion of the area of Multivariate Cryptography over the general finite commutative ring.

In the subsection 2. 2 we define linguistic graphs over the general commutative ring and their temporal analogue. Algorithm 1.2 allows us to construct the variety of elements of Cremona semigroup with the trapdoor accelerator defined in terms of selected linguistic graph or its temporal analogue. Simple conditions insure that the constructive map is bijective transformation of K^n. The method allows us to construct surjective maps of K^n onto K^m, $n>m\geq 2$ with the trapdoor accelerator. For practical implementation of the algorithm we need select special classes of linguistic graphs which allow us to control the degrees and densities of the outputs. We define the special class of Jordan-Gauss graphs and consider flexible families of generalised Double Schubert graphs $DS_{s,r}(K)$ *and truncated Double Schubert graphs* ${}^{Q}DS_{s,r}(K)$ which are convenient instruments for generating of families of multivariate maps of prescribed degree on the affine space K^n.

Assume that *(F, T)* stands for pair multivariate function F of degree d, $d\geq 2$ on K^n and its trapdoor accelerator. We suggest the method of construction of new pair *(F', T')* of degree d on $K^{n'}$, $n'> n$ from the known *(F, T)*. It can be used iteratively. Many constructions of pairs *(F, T)* over fields can be found in the recent papers on Classical Multivariate Cryptography [26]-[37].

In Section 3 we introduce semigroup of ${}^{n}ES(K)$ of Eulerian endomorphisms of $K[x_1, x_2,..., x_n]$ and consider iterative method of construction of multivariate maps of prescribed density $O(n^d)$ with the trapdoor accelerators or multiplicative trapdoor accelerators. These maps are constructed in terms of temporal truncated Schubert graphs.

In Section 4 we consider twisted Diffie-Hellman protocol implemented with the platform ${}^{n}ES(K)$ of Eulerian transformations. We introduce several *deformation rules* convenient for the safe delivery of multivariate maps of prescribed degree or density from one correspondent to his/her partner. We discuss the use of stable subsemigroups of Cremona semigroup ${}^{n}CS(K)$ as platform for the protocol. Stability means that the maximal degree of endomorphisms from the semigroup is a constant d.

In section 5 we consider Jordan-Gauss graphs of geometries of Chevalley groups defined over field F, their analogue defined over general commutative ring K and temporal versions of these graphs. The class of such temporal graphs and their special homomorphic images (symplectic quotients) contains temporal generalised Schubert graphs and truncated Schubert graphs.

We consider temporal geometries of Chevalley type over K defined in [2] in terms of root system with Coxeter - Dynkin diagram X_n, corresponding cryptosystems and protocol based algorithms in terms of platforms defined in terms of these temporal geometries in Section 5.

Section 6 contains conclusive remarks.

2. On the methods of constructions of multivariate transformations of K^n with the trapdoor accelerator

2.1. General remarks.

Let K be a finite commutative ring. It is possible to say that Multivariate Cryptography in a wide sense is about the use of polynomial maps F of affine spaces K^n to itself for cryptographical purposes.

In classical case $K=F_q$ the map F is an element of affine Cremona semigroup ${}^nCS(K)$ of endomorphisms of multivariate ring $K[x_1, x_2, ..., x_n]$. Endomorphism F can be given by its values $F(x_1)=f_1, F(x_2)=f_2, ..., F(x_n)=f_n$ on the variables x_i, $i=1, 2,..., n$.

We can assume that polynomials f_i are given in their standard form i.e. sum of monomial terms ordered in lexicographical order.

Endomorphism F induces the map F' : $x_1 \to f_1(x_1, x_2, ..., x_n)$, $x_2 \to f_1(x_1, x_2, ..., x_n)$,..., $x_n \to f_n(x_1, x_2, ..., x_n)$ of the affine space K^n into itself.

We define degree $deg(F)$ as maximal value of $deg\ (f_i)$. The density $den\ f_i(x_1, x_2, ..., x_n)$ is its number of monomial terms. We define density $den(F)$ of F as maximal value of $den\ (f_i)$, $i=1, 2, ..., n$ and identify endomorphism F with the tuple $(f_1(x_1, x_2, ..., x_n), f_2(x_1, x_2, ..., x_n), ..., f_m(x_1, x_2, ..., x_n))$.

The image $Im\ F'$ is isomorphic to K^m for some m, $n \geq m$. We can treat F' as surjective map of K^n onto K^m.

We say that piece of information T is *trapdoor accelerator* of surjective nonlinear polynomial map F' of K^n onto K^m, $n \geq m$ if the knowledge of T allows to compute a reimage of given element $b \in K^m$ in a polynomial time.

New multivariate cryptosystem "TUOV: Triangular Unbalanced Oil and Vinegar" was officially submitted to NIST recently see https://csrc.nist.gov/csrc/media/Projects/pqc-digsig/documents/round-1/spec-files/TUOV-spec-web.pdf). It is based on the quadratic map defined over finite fields with the trapdoor accelerator.

He hopes that this is the example of one way function, i. e the reimage of this quadratic map is not possible to compute in a polynomial time without the knowledge of given trapdoor accelerator.

As you know the existence of one way function is not proven. Anyway there is a chance of NIST certification of TOUV as first representative from the class of Multivariate Public Keys.

As you know Multivariate cryptography uses the *gap between linearity and nonlinearity*. We know that the system of linear equations written over the field F can be solved in time $O(n^3)$ via Jordan-Gauss elimination method.

The complexity of solving nonlinear system of constant degree d, $d>1$ is subexponential.

Despite the convenience of Groebner basis method for the implementation

the complexity of this algorithm is equivalent to old Gauss elimination method for solution of the system of nonlinear equation.

Recall that the standard way to transform of nonlinear system of equation of degree d, $d>2$ to equivalent quadratic system via introduction of additional variables and substitutions is well known (see [3]).

So if we have a nonlinear map F of bounded degree d in '' general position'' which has a trapdoor accelerator T then corresponding cryptosystem is secure. This status is insure the fact that F is given as one way function i. e reimage of F is impossible to compute in a polynomial time without knowledge of the secret T.

The map F is not in '' *general position''* if some additional specific information is known. For instance, if F is bijective cubic map and F^{-1} is also cubic. Then public user can generate $O(n^3)$ pairs of kind plaintext p/corresponding ciphertext c and approximate inverse map in time $O(n^{10})$.

Known computer tests and cryptanalytic methods are attempts to justify that the map F is ''in general position''. Noteworthy that the existence of one way function is not proven yet even under the *main complexity conjecture* that $P\neq NP$.

Note that the investigation of nonlinear systems of equations over the commutative ring K with *zero divisors* is essentially harder case in comparison the case of a field. Multivariate Cryptography over rings with zero divisors can be an interesting direction of cryptographic research.

2.2. Linguistic graphs and multivariate maps over commutative rings.

Below we present the method of construction of nonlinear representatives of affine Cremona semigroup $End\ K[x_1, x_2,..., x_n]$ where K is a finite commutative ring. The incidence structure is the set V with the 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 which is of course a 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 with the unity. 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 $y=[y_1, y_2, \dots, y_r, y_{r+1}, y_{r+2}, \dots, y_{r+s}]$ if and only if the following relations hold

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

where a_j, and b_j, $j=1,2,\dots,m$ are not zero divisors, and f_j are multivariate polynomials with coefficients from K (see [4], [5]). 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 $b \in K^r$ 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 $c \in K^s$ 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.*

Let $J_a(v)$ stands for the operator of change colour of vertex $\boldsymbol{v}$ (point or line) for $a=(a_1, a_2, \dots, a_t)$ where $t=s$ or $t=r$.

We consider also linguistic incidence structures defined by infinite number of equations. Let $I(K)$ and $I'(K')$ be two linguistic graphs of the same type (s, r, m) with governing polynomials f_i and f'_i written in their standard forms. We refer to them as symbolically equivalent structures if monomial terms of f_i and f'_i for each i are the same up to their nonzero coefficients.

We refer to family $I(K)^t$, $t=1, 2,\dots$ of symbolically equivalent linguistic graphs as *temporal linguistic graph.*

Algorithm 1.2. (Generation of multivariate map F with the trapdoor accelerator, see [6])

Let us consider linguistic graph graph ${}^mI_{s,r}(K)$ given by equations (1) of type s, r, m, $s \geq r$ together with graph ${}^mI_{s,r}(R)$ where R is the commutative ring of multivariate polynomials $K[z_1, z_2, \dots, z_s, z_{s+1}, z_{s+2}, \dots, z_{s+m}]$ given by the same equations (1) with coefficients from K but with variables x_i, y_j from R. So infinite graph ${}^mI_{s,r}(R)$ has the point set R^{s+m} and the line set R^{r+m}.

Let us conduct the following symbolic computation. We consider the special point $z=(z)=(z_1, z_2, \dots, z_s, z_{s+1}, z_{s+2}, \dots, z_{s+m})$ which coordinates are variables, positive integer $\boldsymbol{l}$ and colours $a(1), a(2),\dots, a(l), b(1), b(2),\dots, b(l)$ and $\boldsymbol{c}$ such that $a(1), a(3), \dots, a(l), b(2), b(4),\dots, b(l-1) \in K[z_1, z_2, \dots, z_s]^s$, elements $a(2), a(4),\dots, a(l-1), b(1), b(3),\dots,b(l) \in K[z_1, z_2, \dots, x_s]^r$.

So, we compute recurrently $v_1=J_{a(1)}(z)$, $u_1=N_{b(1)}(v_1)$, $v_2=J_{a(2)}(u_1)$, $u_2=N_{b(2)}(v_2),\dots$, $v_l=J_{a(l)}(u_{l-1})$, $u_l=N_{b(l)}(v_l)$ and finally $J_c(u_l)=v$. If l is odd then $v=(f_1, f_2, \dots, f_r, f_{1+r}, f_{2+r}, \dots, f_{m+r})$. Thus we construct the map $F=F(a(1), a(2),\dots, a(l), b(1), b(2),\dots, b(l), c)$ from K^{s+m} to K^{r+m} sending the tuple $(z_1, z_2, \dots, z_s, x_{s+1}, x_{s+2}, \dots, x_{s+m})$ to $(f_1, f_2, \dots, f_r, f_{r+1}, f_{r+2}, \dots, f_{r+m})$. In the case of even k we construct the transformation $F=F(a(1), a(2),\dots, a(l), b(1), b(2),\dots, b(l), c)$ of K^{s+m} given by the tuple $(f_1, f_2, \dots, f_s, f_{1+s}, f_{2+s}, \dots, f_{m+s})$. Note that f_i, $i=1, 2,\dots, s$ are elements of $K[z_1, z_2, \dots, z_s]$ but $f_i \in K[z_1, z_2, \dots, z_s, z_{1+s}, z_{2+s}, \dots, z_{m+s}]$.

Assume that map L_1 is an element of $AGL_{s+m}(K)$ and L_2 is taken from $AGL_{r+m}(K)$ in the case of odd l and $L_2 \in AGL_{s+m}(K)$ if l is even. The bijective polynomial maps L_1 and L_2 have degree *1*. Then we can compute the standard form of the map $G=L_1FL_2$.

Proposition 1. **2.** [6] *Assume that constant l is odd the tuple **c** defines surjective multivariate map C from K^s to K^r with trapdoor accelerator T and parameters a(i), b(i) and c have degrees of size O(1). Then polynomial surjective map G* from K^{s+m} *to* K^{r+m} *has the trapdoor accelerator T' which is the knowledge on l, a(i), b(i), i=1,2,..., l, C, T , L_1, L_2 and equations (1).*

Remark 1.2. If $K=F_q$ we can take the pair *C, T* defined by J. Ding and his team and get a new surjective map *G* from larger vector space with the trapdoor accelerator.

Proposition 2.2. [6] *Assume that l is even or r=s and the tuple **c** defines bijective multivariate map C from K^s to K^s with trapdoor accelerator T. Assume that a(i), b(i), c are of size O(1). Then the map G is bijective, it has trapdoor accelerator T' which is the knowledge on l, a(i), b(i), i=1,2,..., l, C, T , L_1 , L_2 and equations (1).*

Remark 2.2. Under the condition of Proposition 2 in the case of even **l** it could be that $r>s$.

Procedure 1.2 (reimage computation**).**

Alice gets the image $e=(e_1, e_2, ..., e_t , e_{t+1} , e_{t+2},..., e_{t+m})$, $t=r$ or $t=s$ of the map *G*. She creates intermediate vector $(z_1, z_2,.., z_s, z_{s+1}, z_{s+2}, ..., z_{s+m})$. Alice computes $(L_2)^{-1}(e)=(d_1, d_2, ..., d_t , d_{t+1} , d_{t+2},..., d_{s+m})=d$. She investigates the system of equations $c_1(z_1, z_2, ..., z_s)=d_1$, $c_2(z_1, z_2, ..., z_s)=d_2, ..., c_t(z_1, z_2, ..., z_s)=d_t$. The knowledge of *T* allows her to take some solution $z_1=\alpha_1$, $z_2=\alpha_2$, ..., $z_s=\alpha_s$. Alice calculates values $\beta(i)=b(i)(\alpha_1, \alpha_2, ..., \alpha_s)$, $\gamma(i)=a(i)(\alpha_1, \alpha_2, ..., \alpha_s)$, $i=1, 2,..., l$.

She computes $J_{\beta(l)}(d)=v_l$, $N_{a(l)}(v_l)= u_l$, $J_{\beta(l-1)}(u_l)=v_{l-1}$, $N_{a(l-1)}(v_{l-1})= u_{l-1}$, …, $J_{\beta(1)}(u_2)=v_1$, $N_{a(l)}(v_1)= u_1$, $J_a(u_1)=u$ for $a= (\alpha_1, \alpha_2, ..., \alpha_s)$.

Alice computes the reimage as $(L_1)^{-1}(u)$.

Remark. 3. 2. We can define $F=F(a(1), a(2),...., a(l), b(1), b(2),..., b(l), c)= F(a(1), a(2),...., a(l), b(1), b(2),..., b(l), c, I_1 , I_2,..., I_l)$ *in the case of temporal linguistic graph* ${}^mI_{s,r}(K)^t$ via simple assumption that operators $N_{b(j)}$ *of the algorithm* are executed in the graph I_j $(K[z_1, z_2, ..., z_s, z_{s+1}, z_{s+2}, ..., z_{s+m}])$ formed as expansion of *momentum* graph $I_j= {}^mI_{s,r}(K)^j /t=j$, $j=1, 2, ..., l$. Proposition 1.1 and 2.2 hold for temporal graphs as well.

To control the degrees and densities of $F=F(a_1, a_2,...., a_l, b_1, b_2,..., b_l, c)$ we need a special class of linguistic graphs over *K*.

Jordan-Gauss graphs are linguistic graphs given by special *quadratic* equations over the commutative ring *K* with unity such that the neighbour of each vertex is defined by the system of linear equation given in its row-echelon form (see [7], [8], [9])

Generalised Double Schubert graph $DS_{s,r}(K)$ (see [6], [10] and further references) is a bipartite graph with the points of kind $(x)=(x_1, x_2, ..., x_s, x_{11}, x_{12}, ..., x_{sr})$ and lines

$[y]=[y_1, y_2,..., y_r, y_{11},, y_{12}, ..., y_{sr}]$ such that point (x) is incident to $[y]$ if and if the conditions

$x_{ij}-y_{ij}=x_iy_j$ (1)

hold for $i=1, 2,...,s$ and $j=1, 2,..., r$.

Temporal graph $DS_{s,r}(K)^t$ is given by equations

$^{i,j}\alpha(t)x_{ij} - {}^{i,j}\beta(t)y_{ij} = {}^{i,j}\gamma(t)x_iy_j$ (1')

where $^{i,j}\alpha(t)$ and $^{i,j}\beta(t)$ are elements of multiplicative group K^* and $^{i,j}\gamma(t)$ are elements of $K-\{0\}$.

To form momentum graphs $D_1=DS_{s,r}(K)^t/\ t=1$, $D_2=DS_{s,r}(K)^t/\ t=2$, ... we can use pseudorandom or random sequences of elements from K^* or $K-\{0\}$ respectively. For the constructions genuinely random sequences Quantum Computer can be used.

Remark 4.2. Graph $DS_{s,r}(K)$, $K=F_q$ is formed by spaces of dimension s and $s+1$ from two corresponding largest Schubert cells of projective geometry $PG_{s+r}(F_q)$.

Proposition 3.2. [6] *Let us consider map introduced above map* $G=L_1F(a(1), a(2),...., a(l), b(1), b(2),..., b(l), c, D_1, D_2,..., D_l)L_2$ *in the case of the temporal graph* $DS_{s,r}(K)^t$. *Assume that deg* $a(i)+deg\ b(i)\le d$, *deg* $c=d$. Then degree of $G=G(a(1), a(2),..., a(l), b(1), b(2),..., b(l), c)$ *is* d.

In the case of $d=2, 3$ we can use this construction to obfuscate selected multivariate cryptosystem C, T. In particular we can take as C, T already mentioned quadratic cryptosystem TUOV (Triangular Unbalanced Oil and Vinegar cryptosystem). We can also introduce enveloping trapdoor accelerator for Matsumoto-Imai cryptosystem over finite fields of characteristic 2, for the Oil and Vinegar public keys over F_q. Another quadratic multivariate public keys defined over Jordan-Gauss graphs $D(n, K)$, where K is arbitrary finite commutative ring with the nontrivial multiplicative group. It gives us the option to use Proposition 3.2 in the case of arbitrary commutative ring K (see [8], [11]). We can obfuscate presented above constructions of multivariate maps of degree d with the trapdoor accelerator T below via deleting of some coordinates of points and lines with double indexes together with corresponding equations. It will give us examples of multivariate maps of prescribed degree with the trapdoor accelerator on arbitrary free module K^n .Instead of generalised Schubert graph $DS_{s,r}(K)$ with points of kind $(x)=(x_1, x_2, ..., x_s, x_{11}, x_{12}, ..., x_{sr})$ and lines $[y]=[y_1, y_2,..., y_r, y_{11},, y_{12}, ..., y_{sr}]$ we consider homomorphic image $^QDS_{s,r}(K)$ where Q is selected proper subset of Cartesian product of $\{1,2,..., s\}=N$ and $[1,2,...,r\}=M$. We assume that $r=O(s)$, the projection $(i, j)\to i$ maps Q onto N and the projection $(i, j)\to j$ maps Q onto M. Let $Q=\{\alpha(1), \alpha(2),...,\alpha(m)\}$ *where* $m=O(s^t)$, $1\le t\le 2$. Then partition sets of $^QDS_{s,r}(K)$ are affine space K^{s+m} and K^{r+m}.

We consider the map $^QF=^QF(a_1, a_2,...., a_l, b_1, b_2,..., b_l, c)$ obtained in the case of linguistic graph $^QDS_{s,r}(K)$.

We also consider ^QG as $L_1{}^QFL_2$ where L_1 and L_2 are bijective affine transformations of

partition sets of $^{Q}DS_{n,k}(K)$.We refer to graphs $^{Q}DS_{s,r}(K)$ as *Truncated Schubert Graphs* and consider their temporal analogous $^{Q}DS_{s,r}(K)^{t}$ introduced via the deletion of coordinates indexed by elements of $N\cdot M$ *-Q* and corresponding equations from the system *(1').*

Let $D_1=DS_{s,r}(K)^t/\ t=1, D_2=DS_{s,r}(K)^t/\ t=2,$ **...** stands for the *momentum graphs* of $^{Q}DS_{s,r}(K)^{t}$**.**

Proposition 3'.2. [6] *Let us consider map introduced above map* $G=L_1F(a(1), a(2),...., a(l), b(1), b(2),..., b(l), c, D_1, D_2,..., D_l)L_2$ *in the case of the temporal graph* $^{Q}DS_{s,r}(K)^{t}$. *Assume that deg a(i)+deg b(i)≤d, deg c=d.* Then degree of $G=G(a(_1, a_2,..., a_l, b_1, b_2,..., b_l, c, D_1, D_2,..., D_l)$ *is d.*

Corollary. *Formulated above proposition allows us to construct multivariate bijective map G of prescribed degree d, d≥2 with the trapdoor accelerator on arbitrary affine space* K^{n}.

We can use the construction of Proposition 3' iteratively.

Example 1.2. Let us select finite commutative ring *K* and positive numbers *s, m(1), m(2), ...* to generate the sequence of bijective maps of prescribed degree *d* on $K^{s+m(1)}$, $K^{s+m(1)+m(2)}$, ... with the trapdoor accelerators.

1 step. We use Proposition 3'.2 in the case of selected *d*, temporal Jordan-Gauss graph of type *s, r, s+m(1)* where $s+m(1)\le sr$, $l=l(1)$ is even, tuples $a(1)=a(1, i)$, $b(1)=b(1, i)$ satisfy the condition of the statement and $c=(c_1, c_2,.., c_s)$ has degree *1* and the map *C* of kind $z_i\rightarrow c_i(z_1, z_2,..., z_s)$, $i=1, 2,.., l$ *is* an element of $AGL_s(K)$. Let the standard form G_1 from $^{s+m(1)}CG(K)$ with the corresponding trapdoor accelerator T_1 be the output of the procedure.

2 step and iteration. We use Proposition 3'.2 in the case of Jordan graph of type $s+m(1), r(1), s+m(1)+m(2)$ where $s+m(1)+m(2) \le (s+m(1))r(1)$, $l=l(2)$ is even, *a(i)* and *b(i)* satisfy the condition of the statement and ***c*** coincides with the tuple $g(1)=(G_1(z_1), G_1(z_2), ..., G_1(z_{s+m(1)}))$. Let the standard form of G_2 and its trapdoor accelerator T_2 be the output of Step 2. Notice that the piece of information T_2 is an expansion of T_1**.**

We use the tuple $c=g(2)=(G_2(z_1), G_2(z_2), ..., G_2(z_{s+m(1)+m(2)}))$ and Proposition 3' to generate the transformation G_3 of affine space $K^{s+m(1)+m(2)+m(3)}$ with the trapdoor accelerator T_3 expanding T_2**.** If we use *k* as total number of steps, then the continuation of this recurrent procedure of generating tuples *g(3), g(4), ...,g(k-1)* via free selection of even parameters *l(3), l(4), ..., l(k)* gives the transformation G_k_of degree *d* on the affine space of dimension $s+m(1)+m(2)+...+m(k)$ together with the trapdoor accelerator T_k.

Procedure 2. 2 (reimage computation for (G_k, T_k)*).*

Assume that $G_j=^{j}L_1F_j\ ^{j}L_2$, $j=1,2,...., k$ and $F_j=F(a(1, j), a(2, j),...., a(l(j), j), b(1, j), b(2, j),..., b(l(j),j), g(j-1), ^{j}D_1, ^{j}D_2,..., ^{j}D_{l(j)})$ acting on the affine space ^{j}W of dimension

$s+m(1)+m(2)+...+m(j)=n(j)$.
Alice obtained the ciphertext ${}^0c=({}^0c_1, {}^0c_2,..., {}^0c_{n(k)})$. She computes ${}^kL_2^{-1}({}^0c) = {}^kc$ and takes its projection ${}^kc'$ on the first $n(k-1)$ coordinates.
Alice computes ${}^{k-1}L_2^{-1}({}^kc')={}^{k-1}c$ and takes its projection ${}^{k-1}c'$ on first $n(k-2)$ coordinates. She continue this procedure and gets the tuples
${}^1c=(b_1, b_2, ..., b_s, b_{s+1}, b_{s+2},..., b_{s+m(1)})$ and ${}^1c'=(b_1, b_2,..., b_s)$.
Alice forms the intermediate tuple $(z_1, z_2,..., z_s)$ and investigates the system of linear equations $\boldsymbol{c_1(z}_1, z_2,..., z_s)=b_1, c_2(z_1, z_2,..., z_s)=b_2, ..., c_s(z_1, z_2,..., z_s)=b_s$. She gets the solution $z_1=\alpha_1, z_2=\alpha_2, ..., z_s=\alpha_s$.. Alice computes tuples $a^*(i, 1)=a(1, 1)(\alpha_1, \alpha_2,..., \alpha_s)$, $b^*(i, 1)=b(1, 1)(\alpha_1,\alpha_2,..., \alpha_s)$, $i=1, 2,..., l(1)$ with coordinates from K.
Alice takes graph ${}^1D_{l(1)}$ and computes $d(l(1))=J_{b^*(l(1),1)}({}^1c)$. She takes the neighbour $d'(l(1)=N_{a^*(l(1)),1)}(d(l(1))$ of the point $d(l(1)$ of colour $a^*(l(1), 1)$.Alice treats the tuple $d'(l(1))$ as the line of graph ${}^1D_{l(1)}$.She computes $J_{b^*(l(1)-1),1)}(d'(l(1))=d(l(1)-1)$ and its neighbour $d'(l(1)-1)=N_{a^*(l(1)-1),1)}(d(l(1)-1)$. Alice continue this process and gets $d'(1)=N_{a^*(1,1)}(d(1))$ in the graph ${}^1D_1$. So she gets $e(1)=J_\gamma(d'(1))$, $\gamma= (\alpha_1,\alpha_2,..., \alpha_s)$.
The tuple $({}^1L_1)^{-1}(e(1))=r(1)$ is the solution of the equation $L_1F_1(z_1, z_2, z_s, z_{s+1}, ..., z_{s+m(1)})= {}^1c={}^1(L_2)^{-1}({}^2c')$ which is equivalent to $G_1(z_1, z_2, z_s, z_{s+1}, ..., z_{s+m(1)})={}^2c'$.
Alice considers the equation ${}^2L_1F_2(z_1, z_2, ..., z_s, z_{s+1}, ..., z_{s+m(1)}, z_{s+m(1)+1},..., Z_{s+m(1)+m(2)})= {}^2c={}^2L_2({}^3c')$.
The first $s+m(1)$ equations of this system are equivalent to $L_1F_1(z_1, z_2, ..., z_{s+m(1)})={}^1c$ with the solution $\gamma(1)=({}^1\alpha_1, {}^1\alpha_2, ..., {}^1\alpha_{s+m(1)})$.
Alice computes the specializations $a^*(1, 2), a^*(2, 2),..., a^*(l(2), 2), b^*(1, 2), b^*(2, 2),..., b^*(l(2), 2)$ of $a(1, 2), a(2, 2),..., a(l(2), 2), b(1, 2), b(2, 2),..., b(l(2), 2)$ under the substitution $z_1={}^1\alpha_1, z_2={}^1\alpha_2, ..., z_{s+m(1)}= {}^1\alpha_{s+m(1)}$.
She computes the point $d(l(2))=J_{b^*(2, l(2))}({}^2c)$ and line $d'(l(2))=N_{a^*(2, l(2))}(d(l(2)))$ of the graph ${}^2D_{l(2),}$ computes $d(l(2)-1)=J_{b^*(2, l(2)-1)}(d'(l(2))$ and vertex $d'(l(2)-1)=N_{a^*(2, l(2)-1)}(d(l(2)-1))$ of the graph $\boldsymbol{{}^2D_{l(2)-1}}$. Alice continue this process and gets $d'(1)=N_{a^*(2,1)}(d(1))$ in the graph ${}^2D_1$. So she gets $e(1)=J_{\gamma(1)}(d'(1))$ in this graph.
The tuple $({}^2L_1)^{-1}(e(1))=\gamma(2)$ is the solution of the equation ${}^2L_1F_2(z_1, z_2, z_s, z_{s+1}, ..., z_{s+m(1)}, z_{s+m(1)+1},..., z_{s+m(1)+m(2)})={}^2c={}^1(L_2)^{-1}({}^3c')$ which is equivalent to $G_2(z_1, z_2, z_s, z_{s+1}, ..., z_{s+m(1)+m(2)})={}^3c'$.
Alice continue this recurrent process and gets the solution $\gamma(k)$ of the equation $G_k(z_1, z_2, z_s, z_{s+1}, ..., z_{s+m(1)+m(2)+...+m(k)})= {}^0c$.

Example 2.2. Let us select finite commutative ring K and positive numbers $s, r, s\geq r, m(1), m(2),$ **....** to generate the sequence of bijective maps of prescribed degree d from $K^{s+m(1)}$ onto $K^{r+m(1)}$, from $K^{s+m(1)+m(2)}$ onto $K^{r+m(1)+m(2)}$, ... with the trapdoor accelerators. We will use Proposition 3' several times in the case of odd parameter l.

1 step. We use Proposition 3' in the case of selected d, temporal Jordan-Gauss graph of type $s, r, m(1)$ where $s \le m(1) \le sr$, $l=l(1)$ is odd, tuples $a(i), b(i)$ satisfy the condition of the statement and $c=(c_1, c_2,.., c_s)$ has degree 1 and the map $C : (z_1, z_2,..., z_s) \to (c_1(z_1, z_2,..., z_s), c_2(z_1, z_2,..., z_s), ..., c_r(z_1, z_2,..., z_s)$ is surjective. We can assume that linear expressions $c_1, c_2,..., c_r$ are written in a row echelon form.

Let the standard form the map G_1 from $K^{s+m(1)}$ onto $K^{r+m(1))}$ with the corresponding trapdoor accelerator T_1 be the output of this step.

2 step and iteration. We use Proposition 3' in the case of Jordan graph of type $s+m(1), r(1)+m(1)$, $m(1)+m(2)$ where $s+m(1)+m(2) \le (s+m(1))(r(1)+m(1)$, $l=l(2)$ is odd, $a(i)$ and $b(i)$ satisfy the condition of the statement and $\boldsymbol{c}$ coincides with the tuple $g(1)=(G_1(z_1), G_1(z_2), ..., G_1(z_{r+m(1)}))$. Let the standard form of G_2 and its trapdoor accelerator T_2 be the output of Step 2. Notice that the piece of information T_2 is an expansion of T_1.

We use the tuple $c=g(2)=(G_2(z_1), G_2(z_2), ..., G_2(z_{r+m(1)+m(2)}))$ and Proposition 3' to generate the map G_3 of affine space $K^{s+m(1)+m(2)+m(3)}$ *onto* $K^{r+m(1)+m(2)+m(3)}$ with the trapdoor accelerator T_3 expanding T_2**.** If we use k as total number of steps, then the continuation of this recurrent procedure of generating tuples $g(3), g(4), ...,g(k-1)$ via free selection of odd parameters $l(3), l(4), ..., l(k)$ gives the standard form of the map G_k_of degree d from the affine space of dimension $s+m(1)+m(2)+...+m(k)$ onto free module of dimension $r+m(1)+m(2)+...+m(k)$ together with the trapdoor accelerator T_k.

The procedure of reimage computation of G_k is similar to the case of Example 1.2.

Remark 4. 2. ***(nonlinear disturbance).*** In both examples instead of linear map C any nonlinear surjective map H of degree at most d with the trapdoor accelerator can be used. In particular one can use quadratic transformations of arbitrary free module K^n presented in [8], [11]. In the case of Example 2. In case of finite field many classical broken or unbroken multivariate cryptosystem can be used (see [12] and further references).

3. On the multivariate maps of prescribed density with the trapdoor accelerator.

Let Assume that commutative ring K contains nontrivial multiplicative group K^*. Let us consider the totality ${}^nES(K)$ of endomorphisms of $K[z_1, z_2,..., z_n]$ of kind

$$\begin{aligned} &z_1 \to q_1 z_1^{\,a(1,1)} z_2^{\,a(1,2)} \dots z_n^{\,a(1,n)}, \\ &z_2 \to q_2 z_1^{\,a(2,1)} z_2^{\,a(2,2)} \dots z_n^{\,a(2,n)}, \qquad (1.3) \\ &\dots \\ &z_n \to q_n z_1^{\,a(n,1)} z_2^{\,a(n,2)} \dots z_n^{\,a(n,n)} \end{aligned}$$

where q_i are regular elements of finite commutative ring K with the unity.

It is easy to see that the complexity of the composition of two elements of kind (1.3) is $O(n^3)$.

The semigroup ${}^nES(K)$ acts naturally on $(K^*)^n$ and contains large subgroup ${}^nEG(K)$ of bijective transformations of the variety **(s**ee [1]).

Recall that we define density *den (f)* of element f from $K[z_1, z_2,..., z_n]$ written in its standard form as its number of monomial terms. The density of the tuple $H(z_1, z_2,..., z_n)$ is defined as maximum of $den(h_i)$, $i=1,2,..., m$.

The following statements are proven in [6].

Proposition 1. 3. *Let us consider map introduced above map $F=F(a(1), a(2),...., a(l), b(1), b(2),..., b(l), c, D_1, D_2,..., D_l)$ in the case of the temporal graph ${}^QDS_{s,r}(K)^t$ where K is a commutative ring with nontrivial multiplicative group K*. Assume that the densities of a(i), b(i) and c are of size $O(s^{\alpha(i)})$, $O(s^{\beta(i)})$ and $O(s^{\gamma})$ such that $0\le\alpha(i)+\beta(i)\le d$ and $\gamma\le d$ for some d, $d\ge 0$. Then den F has size $O(s^d)$.*

Remark 1. 3. Parameter ***d*** can be selected as rational number.

Corollary 1.3. *Let s=r or l is even, $r=O(s)$, $m=O(s^{\mu})$, $1\le\mu\le 2$, H be an element of ${}^{s+m}ES(K)$ and $L\epsilon AGL_{s+m}(K)$* and *F satisfies conditions of Proposition 1. 3. Then the density of standard form of G=HFL* is $O(s^{d+\mu})=O((s+m)^{d/\mu+1})$.

Remark 2.3. We can select *L* of density *O(1)* or density $O(m^{\lambda})$, $0\le\lambda\le 1$. The simplest case is of kind $z_i\rightarrow d_{ii}\dot{z}_i+d_{ii+1}\dot{z}_{i+1}+...+d_{is+m}\dot{z}_{i+sm}$, $i=1,2,..., m+s$. Then the density of the map is $O((s+m)^{d/\mu+\lambda})$.

Corollary 2.3. *Assume that conditions of Corollary 1.3 holds and C=EN, where $E\epsilon^sEG(K)$, $N\epsilon^sCG(K)$. Then G induces injective map of $(K^*)^{s+m}$ into $(K)^{s+m}$.*

Let $M_s(K) = GL_s(K)\cap {}^sES(K)$ be the monomial group of linear transformations.

Corollary 3.3. *Assume that conditions of Proposition 1.3 hold and $H\epsilon M_{s+m}(K)$ and $C\epsilon^sCG(K)$. Then G is a bijective map of K^{s+m} onto itself.*

Formulated above statements allow us to construct element *G* of ${}^nCG(K)$ of unbounded degree and prescribed density *d*, $d\ge O(n)$ with the trapdoor accelerator.

We define *multiplicative trapdoor accelerator (F, T)* of *F* which is the map of density *d* such that its restriction *F'* on $(K^*)^n$ is injective map and the knowledge of *T* allows to compute the reimage of *F'* in a polynomial time.

Remark 3.3.

We can construct multiplicative accelerators *(F, T)* where $F\epsilon^nCS(K)$ has unbounded degree and prescribed density $O(n^d)$, $d\ge 0$.

Algorithm 1.3.

Public key with the multivariate map *G* with the multiplicative trapdoor accelerator.

Alice select even parameter ***l*** of size *O(1)* and commutative ring *K* with nontrivial multiplicative group *K**. Natural examples are finite field F_q or modular arithmetic Z_q where $q=2^s$, $s>1$.

She selects parameters *n* and $k=O(n)$ together with the subset $Q=\{\alpha(1), \alpha(2),..., \alpha(m)\}$ of Cartesian product of $\{1,2,..., n\}$ and $\{1,2,..., k\}$ of cardinality *m*, $m=O(n^{\mu})$ where $1\le\mu\le 2$. Alice will work with graph ${}^QDS_{n,k}(R)^t$, $k=O(n)$, $R=K[z_1, z_2, ..., z_n, z_{\alpha(1)}, z_{\alpha(2)}, ...,$

$z_{\alpha(m)}]$. She selects parameter d and tuples of polynomials $a(1), a(2),..., a(l), b(1), b(2), ..., b(l)$ with coordinates from $K[z_1, z_2, ..., z_n]$ satisfying conditions of Proposition 1.3, i. e. $den(a(i))$ has size $O(s^{\alpha(i)})$,

$den(b(i))$ has size $O(s^{\beta(i)})$ and $\alpha(i)+\beta(i)=d$.

Alice forms the tuples a_i, b_i , $i=1, 2,.... l$ of with coordinates of kind $q_1 z_1^{a(1,1)} z_2^{a(1,2)} \dots z_n^{a(1,s)} + q_2 z_1^{a(2,1)} z_2^{a(2,2)} \dots z_n^{a(2,n)} + \dots + q_r z_1^{a(r,1)} z_2^{a(r,2)} \dots z_n^{a(r,n)}$ where $q_i \neq 0$. She selects the pair of $E, E' \epsilon^n EG(K)$ such that $(EE', (K^*)^n)$ and $(E'E, (K^*)^s)$ are identity permutations. The procedure 1 for this step is given below. She takes N of density $O(1)$ from $AGL_n(K)$ and L from $AGL_{n+m}(K)$ together with H and H' from $^{m+n}EG(K)$ such that HH' and $H'H$ are identity transformations of $(K^*)^{s+m(1)}$. Alice computes $C=EN$ moving $(z_1, z_2, ..., z_n)$ to $c=(c(1), c(2),..., c(n))$.

She select parameters $^{i,j}\alpha(t) \epsilon K^*$, $^{i,j}\beta(t)$ and $^{i,j}\gamma(t)$ where $t=1, 2, ..., l$, $(i, j) \epsilon Q$ for construction of momentum Jordan-Gauss graphs $D_1, D_2 ,..., D_l$ of the temporary graph $^{Q}DS_{s,k}(K)^t$.

Alice will use $D_j(K[z_1, z_2, ..., z_s , z_{\alpha(1)}, z_{\alpha(2)}, ..., z_{\alpha(m(1))}])$ which are special momentum graphs of $^{Q}DS_{s,k}(R)^t$ defined by equations with coefficients from K but with the point set R^{n+m} and line set R^{k+m}.

She uses symbolic computation in the graph $^{Q}DS_{n,k}(R)^t$ to construct the transformation $F=F(a(1), a(2),...., a(l), b(1), b(2),..., b(l), c, D_1, D_2,..., D_l)$ of K^{n+m} to itself.

Alice uses Procedure 1 to form H from $^{n+m}EG(K)$. She forms L from $AGL_{n+m}(K)$ of density $O(m^{\lambda})$, $\lambda \leq l$ and the element $G=HFL$ of affine Cremona semigroup. She computes the standard form of G and announces this multivariate rule publicly.

The standard form of G will be used as encryption tool in the case of the space of plaintexts $(K^*)^{n+m}$.

Alice generates the map via special walks on the graph. The degree of the map G is $O(n+m)$.The density of the map is $O(n+m)^{\lambda+d/\mu}$.

Thus the complexity of encryption of computation of the image of $(p_1, p_2,..., p_{n+m}) \epsilon (K^*)^{m+n}$ is $O(n+m)^{\lambda+d/\mu+1}$.

Decryption procedure.

Public user Bob writes his plaintext $p=(p_1, p_2,..., p_{m+n})$ and sends the ciphertext $s=G(p)$ to Alice.

Alice decrypts via the following procedure.

She computes $L^{-1}(s)=(d_1, d_2, ..., d_n, d_{\alpha(1)}, d_{\alpha(2)},..., d_{\alpha(m)})=d$. Alice creates intermediate tuple of variables $(z_1, z_2,..., z_n, z_{\alpha(1)}, z_{\alpha(2)},..., z_{\alpha(m)})$ consider the equations. She computes $N^{-1}(d_1, d_2, ..., d_n)=(e_1, e_2, ..., e_n)$ and considers the equations

$E(z_1, z_2,..., z_n)=e_1$,

$E(z_1, z_2,..., z_n)=e_2$,

...,
$E(z_1, z_2,..., z_n)=e_n$,
Alice uses E' and gets the solution $z_1=t_1, z_2= t_2, ..., z_n= t_n$.
She computes $a(i)(t_1, t_2,..., t_n)=a^*_i$, $i=1, 2,..., l$, $b(i)(t_1, t_2,..., t_n)=b^*_i$, $i=1, 2,..., l$ and writes the system of linear equations
$F=F(a^*(1), a^*(2),...., a^*(l), b^*(1), b^*(2),..., b^*(l), d')(t_1, t_2, ..., t_n, z_{\alpha(1)}, z_{\alpha(2)},..., z_{\alpha(m)})=d$
where $d'=(d_1, d_2, ..., d_n)$.
This system is already written in row-echelon form.
So Alice gets the solution $z_{\alpha(1)}=t_{\alpha(1)}, z_{\alpha(2)}=t_{\alpha(2)},...,z_{\alpha(m)}=t_{\alpha(m)}$.
She forms $t=(t_1, t_2,..., t_n, t_{\alpha(1)}, t_{\alpha(2)},..., t_{\alpha(m)})$ and p as $H'(t)$.

Procedure 1.3.

Let K be a finite commutative ring with unity and nontrivial multiplicative group K^* of order $d>1$. Assume that parameter n is selected and we have a task of the generating of two elements E and E' of ${}^nEG(K)$ such that EE' and $E'E$ act on $(K^*)^n$ as identity transformations.

We form the transformation J_1 and J_2 from ${}^nEG(K)$ of kind

$y_1=\mu_1 x_1^{a(1,1)}$
$y_2=\mu_2 x_1^{a(2,1)} x_2^{a(2,2)}$
...
$y_n=\mu_n x_1^{a(n,1)} x_2^{a(n,2)} ... x_n^{a(n,n)}$

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

$z_1=\mu'_1 y_1^{b(1,1)} y_2^{b(1,2)} ... y_n^{b(1,n)}$
$z_2=\mu'_1 y_2^{b(2,2)} y_2^{b(2,3)} ... y_n^{b(2,n)}$

...

$z_n=\mu'_n y_n^{b(n,n)}$
where $(b(n,n), d)=1, (b(n-1, 2), d)=1,...,(b(1, n), d)=1$.

The computation of inverses J'_1 and J'_2 of the transformations J_1 and J_2 of the variety $(K^*)^n$ is straightforward. So Alice computes $E=J_1J_2$ and $E'=J'_2J'_1$.
Similarly she constructs lower triangular and upper triangular bijective transformations JG_1 and JG_2 from $({}^{m+n}ES(K), (K^*)^{m+n})$.

So Alice computes $H=GJ_1 GJ_2$ and $H'=GJ'_2 GJ'_1$.
In the case $d=0$ and $\lambda=0$ when the density of $a(i)$, $b(i)$ and L are $O(1)$
we obtain pseudolinear cryptosystem. Its complexity for the encryption is $O(n+m)^2$.

In the case of $d/\mu+\lambda<1$ we get sub quadratic cryptosystem . It has complexity better than $O(n+m)^3$.
If $d/\mu+\lambda=1$ we obtain pseudo quadratic cryptosystem.

More general methods of generation of invertible elements of ${}^nES(K)$ can be found in [1].

Corollary 4. 3. *Let K be commutative ring with nontrivial multiplicative group K*. Then for each natural n , n>2 we can construct multivariate map of prescribed density with the multiplicative trapdoor accelerator.*
Recall that $G=E^QQL$ *induces injective map of* $(K^*)^{n+m}$ *into* K^{n+m}.
The standard form of G has the trapdoor accelerator Q, E, L, H, N, a_i, b_i, $i=1, 2,..., l$, T'. *We assume that equations of DS(n, K) are known publicly.*

Remark 4.3. Note that the map with the trapdoor accelerator of polynomial density $O(n^d)$ where d, $d \geq 2$ is a natural number can be obtained as the product of J_1 and J_2 of the Procedure 1 and selected multivariate map F of degree d with the trapdoor accelerator T.

In [8] we use the special walks of odd length in the Jordan-Gauss graphs $D(n, K)$ of type $1, 1, n-1$ for the generation of quadratic multivariate map F with the trapdoor accelerator .

The point $(p)=(p_1, p_2, ..., p_n)$ of this graph is incident with the line $[l]=[l_1, l_2, ..., l_n]$, if the following relations between their coordinates hold:
$l_2-p_2=l_1p_1$, $l_3-p_3=l_2p_1$, $l_4-p_4=l_1p_2$, $l_i-p_i=l_1p_{i-2}$, $l_{i+1}-p_{i+1}=l_{i-1}p_1$, : $l_{i+2}-p_{i+2}=l_ip_1$: $l_{i+3}-p_{i+3}=l_1p_{i+1}$ where $i\geq 5$.
So the encryption scheme is the following. Let us take graph $D(n, K[x_1, x_2, ..., x_n])$, sequence of colors $d(1), d(1)+x_1, d(2), d(3)+x_1, ..., d(l-1)+x_1, d(l)$ ($d(i) \in K$) and $h=h(x_1, x_2, ..., x_n)= ax_1^t+f(x_1, x_2, ..., x_n)$ where $a \in K^*$, quadratic f has the property that $f(a_1, a_2, ..., a_n)=f(b_1, b_1, ..., b_n)$ when tuples $(a_1, a_2, ..., a_n)$ and $(b_1, b_1, ..., b_n)$ are consist of coordinates of vertexes from the same connected component of the graph $D(n, K)$, $t \in \{1, 2\}$ and $x^t=b$ has unique solution for each b from K.
Then we have to take sequence $x=(x_1, x_2, ..., x_n)$ (point from $D(n, K[x_1, x_2, ..., x_n])$), $v_1=N_{d(1)}(x)$, $N_{d(2)+x1}(v_1)=v_2$, $N_{d(l)}(v_{l-1})=v_1$, $v_{l+1}=J_h(v_k)=(u_1, u_2, ..., u_n)$.
Let F be the map $x_1 \rightarrow u_1(x_1, x_2, ..., x_n)$, $x_2 \rightarrow u_2(x_1, x_2, ..., x_n)$, …, $x_n \rightarrow u_n(x_1, x_2, ..., x_n)$.
Then $deg\ F=2$.
We consider the map of kind $G=J_1J_2L_1FL_2$ where L_1 and L_2 are elements of $AGL_n(K)$.

We generate the map G in the case when K is a finite field F_q, $q=2^8$, F_q, $q=2^{12}$ and F_q, $q=2^{16}$ for $t=2$.

Let us denote G as $G(n, l, K)$ in the case when the length of the sequence of colours $d(1), d(2), ..., d(l)$ has length l. We present time of generation (in ms) of element

G=G(n, l, K) and the total number $M(G)$ of monomial terms in all g_i (global density). We refer to parameter l as *length of word*. We can see the ''condensed matters physics'' digital effect. If l is ''sufficiently large'', then $M(g)$ is independent from l constant (c).

We have written a program for generating of elements and for encrypting a text using the generated public key. The program is written in SAGE [8]. We use an average PC with processor Pentium 3.00 GHz, 2GB memory RAM and system Windows 7.
We have implemented three cases:

1. L_1 and L_2 are identities,
2. L_1 and L_2 are maps of kind $z_1 \rightarrow z_1 + a_2z_2 + \underline{a_3}\underline{z_3} + \ldots + a_tz_t,$, $z_2 \rightarrow z_2$, $z_3 \rightarrow z_3$, $\ldots$, $z_n \rightarrow z_n$, $a_i \neq 0$, $i=1,2,\ldots,n$ (linear time of computing for L_1 and L_2).
3. $L_1 = Ax + b$, $L_2 = A_1x + b_1$; matrices A, A_1 and vectors b, b_1 have mostly non-zero elements.

Tables 1. 1, 2.1 and 3.1 presents of the global densities of the map defined over fields of order 2^8, 2^{12} and 2^{16} in the Case 1.

Tables ***1.2*** , 2.2 and 3.2 corresponds to the Case 2 over the selected finite fields.

Tables 1.3. 2.3 and 3.3 presents the global density of maps in the Case 3.

Table 1. 1

(field of order 2^8)

Number of coefficients

pass length/ n	16	32	64	128
15	123	425	1204	2740
31	123	439	1625	4716
63	123	439	1626	6364
127	122	439	1647	6367

Table 2.1.

Field of order 2^{12}.

Number of coefficients.

Pass length/n	16	32	64	128
15	123	436	1204	2740
31	123	439	1644	4716
63	123	439	1647	6364
127	123	439	1647	6367

Table 3.1.

Field of order 2^{16}.

Number of coefficients

pass length/n	16	32	64	128
15	123	436	1204	2740
31	123	439	1644	4716
63	123	439	1647	6364
127	123	439	1647	6367

Table1.2

Field of order 2^8.

Number of coefficients

pass length/n	16	32	64	128
15	783	4828	26174	120959
31	782	4833	32940	192050
63	782	4831	32951	240840
127	781	4832	32930	240840

Table 2.2

Field of order 2^{12}.

Number of coefficients

pass length/n	16	32	64	128
15	783	4832	26189	121132
31	783	4835	32967	192157
63	783	4835	32968	241034
127	783	4835	32967	241036

Table 3. 2

Field of order 2^{16}.

Number of coefficients

pass length/n	16	32	64	128
15	783	4832	26192	121135
31	783	4835	32968	192168
63	783	4835	32971	241046
127	783	4835	32971	241051

Table 1.3

Field of order 2^8.

Number of coefficients.

pass length/n	16	32	64	128
15	2439	17887	136749	1069013
31	2443	17885	136760	1069129
63	2442	17885	136725	1069034
127	2434	17884	136768	1069097

Table 2. 3

Field of order 2^{12}.

Number of coefficients.

pass length/n	16	32	64	128
15	2447	17948	137240	1073017
31	2448	17945	137247	1073002
63	2448	17949	137249	1072985
127	2448	17946	137254	1073007

Table 3.3
Field of order 2^{16}.

Number of coefficients

pass length/n	16	32	64	128
15	2448	17952	137276	1073256
31	2448	17952	137277	1073261
63	2448	17952	137280	1073261
7	2448	17952	137280	1073266

Tables confirms that in the Case 2 and 3 we have pseudocubic multivariate transformations, i. e. maps of density $O(n^2)$. In the case 3 we have a pseudoquadratic maps.

Similar cryptosystems of complexity $O(n^3)$ are proposed in [24], [25]. Similarly to the Example 1 we can use Proposition 4 iteratively.

Example 1. 3

Alice selects finite commutative ring K and positive number $\boldsymbol{s}$ and prescribed degree $\boldsymbol{d}$.

Step 1. Alice selects even parameter $l=l(1)$ of size $O(1)$ and the degree $d(1)$ of the initial map and parameter $\mu(1)$, $1\leq\mu(1)\leq 2$.

She takes parameter $k=O(s)$ together with the subset $Q=\{\alpha(1), \alpha(2),..., \alpha(m(1))\}$ of Cartesian product of $\{1,2,..., s\}$ and $\{1,2,..., k\}$ of cardinality $m(1)$, $m(1)=O(s^{\mu(1)})$

where $1 \leq \mu(1) \leq 2$. Alice will work with graph ${}^{Q}DS_{s,k}(R)^{t}$, $k=O(s)$, $R=K[z_1, z_2, ..., z_s, z_{\alpha(1),} z_{\alpha(2),} ..., z_{\alpha(m(1))}]$. She selects tuples of polynomials $a(1)=a(1, 1)$, $a(2)=a(1, 2),..., a(l)=a(1, l)$, $b(1, 1), b(1, 2), ..., b(1, l)$, $l=l(1)$ with coordinates from $K[z_1, z_2, ..., z_s]$ satisfying conditions of Proposition 4, i. e.

$deg\ (a(i))=\alpha(i)$, $deg\ b(i)=\beta(i)$ and $\alpha(i)+\beta(i)=d(1)$.

Alice forms the tuples a_i, b_i , $i=1, 2,....\ l$ of with coordinates of kind $q_1 z_1^{\ a(1,1)} z_2^{\ a(1,2)} \dots z_s^{\ a(1,s)} + q_2 z_1^{\ a(2,1)} z_2^{\ a(2,2)} \dots z_s^{\ a(2,s)} + \dots + q_r z_1^{\ a(r,1)} z_2^{\ a(r,2)} \dots z_s^{\ a(r,s)}$ where $q_i \neq 0$. She selects the pair of $E, E' \epsilon^{s} EG(K)$ such that $(EE', (K^*)^s)$ and $(E'E, (K^*)^s)$ are identity permutations. She takes N of density $O(1)$ from $AGL_s(K)$ and L of density $O(1)$ from $AGL_{s+m(1)}(K)$ together with $H=H_1$ and $H'=H'_1$ from ${}^{m(1)+s}EG(K)$ such that HH' and $H'H$ are identity transformations of $(K^*)^{s+m(1)}$. Alice computes $C=EN$ moving $(z_1, z_2, ..., z_s)$ to $c=(c(1), c(2),..., c(s))$.

She select parameters ${}^{i,j}\alpha_1(t) \epsilon K^*$, ${}^{i,j}\beta_1(t)$ and ${}^{i,j}\gamma_1(t)$ where $t=1, 2, ..., l(1)$, $(i, j) \epsilon Q$ for the construction of momentum Jordan-Gauss graphs ${}^{1}D_1, {}^{1}D_2, ..., {}^{1}D_l$ of the temporary graph ${}^{Q}DS_{s,k}(K)^{t}$.

Alice will use ${}^{1}D_j(K[z_1, z_2, ..., z_s , z_{\alpha(1),} z_{\alpha(2),} ..., z_{\alpha(m(1))}])$ which are special momentum graphs of ${}^{Q}DS_{s,k}(R)^{t}$, $R= K[z_1, z_2, ..., z_s , z_{\alpha(1),} z_{\alpha(2),} ..., z_{\alpha(m(1))}])$ defined by equations of ${}^{1}D_1, {}^{1}D_2, ..., {}^{1}D_l$ with coefficients from K but with the point set $R^{s+m(1)}$ and line set $R^{k+m(1)}$.

She uses symbolic computation in the graph ${}^{Q}DS_{s,k}(R)^{t}$ to construct the transformation $F=F_1=F(a(1, 1), a(1, 2),...., a(1, l(1)), b(1, 1), b(1, 2),..., b(1, l), c, {}^{1}D_1, {}^{1}D_2,..., {}^{1}D_{l(1)})$ of $K^{s+m(1)}$. She already formed $L=L_1$ from $AGL_{s+m(1)}(K)$ of density $O(1)$. Alice computes the element $G_1=H_1F_1L_1$ of affine Cremona semigroup. She computes the standard form of G_1. The degree of the map G_1 is $O(s+m(1))$.The density of the map is $O(s+m(1))^{d(1)/\mu(1)}$. The trapdoor accelerator T_1 consist of Q, equations of ${}^{Q}DS_{s,k}(K)$, tuples $a(1), a(2),...., a(l), b(1), b(2),..., b(l)$ and momentum graphs, transformations E , N and H_1 , L_1.

Step 2 and the iteration.

Alice selects parameter $k(1)=O(s+m(1))$ and positive integer $s+m(1) \leq m(2) \leq s+m(k)k(1)$, even parameter $l(2)$ and constants $d(2), d(2) \geq d(1)/\mu(1)$ and $\mu(2)$ where $1 \leq \mu(2) \leq 2$. She selects the subset $Q(1)=\{ \alpha(1, 1), \alpha(1, 2),..., \alpha(1, m(2))\}$ of Cartesian product of $\{1,2,..., s+m(1)\}$ and $\{1,2,..., k(1)\}$ of cardinality $m(2)$, $m(2)=O((s+m(1))^{\mu(2)})$. Alice will work with graph ${}^{Q(1)}DS_{s+m(1),k(1)}(R)^{t}$, $R=K[z_1, z_2, ..., z_{s+m(1)}, z_{\alpha(1,1),} z_{\alpha(1,2),} ..., z_{\alpha(1,m(2))}]$. She selects parameters to create momentum graphs ${}^{2}D_1, {}^{2}D_2, ..., {}^{2}D_{l(2)}$ of the temporary graph ${}^{Q(1)}DS_{s+m(1),k(1)}(K)^{t}$.

Alice will use ${}^{2}D_j(K[z_1, z_2, ..., z_{s+m(1)} , z_{\alpha(1,1),} z_{\alpha(1,2),} ..., z_{\alpha(1,m(2))}])$, $J=1, 2,..., l(2)$ which are special momentum graphs of ${}^{Q}DS_{s+m(1),k(1)}(R)^{t}$, $R= K[z_1, z_2, ..., z_s , z_{\alpha(1),} z_{\alpha(2),} ..., z_{\alpha(m(1))}])$ defined by equations of ${}^{2}D_1, {}^{2}D_2, ..., {}^{2}D_{l(2)}$ with coefficients from K but with the point set $R^{s+m(1)+m(2)}$ and line set $R^{k(1)+m(1+)m(2)}$.

She selects tuples $a(2, 1), a(2, 2),...., a(2, l(2)), b(2, 1), b(2, 2),..., b(2, l(2))$ with coordinates from $K[z_1, z_2, ..., z_{s+m(1)}]$ such that $den\ (a(2, i)b(2, i))=O((s+m(1))^{d(2)})$. Alice constructs the transformation $F_2=F(a(2, 1), a(2, 2),...., a(2, l(2)), b(2, 1), b(2, 2),..., b(2, l(2)), g(1), {}^2D_1, {}^2D_2,..., {}^2D_{l(2)})$ of $K^{s+m(1)+m(2)}$ where g_1 is the tuple $(G_1(z_1), G_1(z_2),..., G_1(z_{s+m(1)})$. She selects the pair of $H_2, H_2'\epsilon^{s+m(1)+m(2)}EG(K)$ such that $(H_2H_2', (K^*)^{s+m(1)+m(2)})$ is identity permutations.

She selects $L=L_2$ from $AGL_{s+m(1)+m(2)}(K)$ of density $O(1)$ and forms $G_2=H_2F_2L_2$.

The density of the standard form of the map G_2 will be determined as $O((s+m(1))^{d(2)})$ or $O((s+m(1)+m(2))^{d(2)/\mu(2)})$.The map G_2 has a multiplicative trapdoor accelerator T_2 which is extension of T_1 via adding $Q(1)$ of cardinality $m(2)$, parameters $k(1)$, $l(2)$ equations of ${}^{Q(1)}DS_{s+m(1),k(1)}(K)$, tuples $a(2.1), a(2, 2),...., a(2, l(2)), b(2, 1), b(2, 2),..., b(2, l(2))$, momentum graphs ${}^2D_1, {}^2D_2,..., {}^2D_{l(2)}$ and transformations H_2, H_2', L_2.

Alice takes parameters $d(3), d(3) \geq d(2)/\mu(2), \mu(3), 1 \leq \mu(3)) \leq 2, k(2)$ of size $O(s+m(1)+m(2))$ and $m(3)$ of size $O((s+m(1)+m(2))^{\mu(3)}$ such that $s+m(1)+m(2) \leq m(3) \leq (s+m(1)+m(2))k(2)$. She takes even parameter $l(3)$ and selects subset $Q(2)=\{\alpha(2, 1), \alpha(2, 2),..., \alpha(2, m(3))\}$ of Cartesian product of $\{1, 2,...., s+m(1)+m(2)\}$ and $\{1, 2, ..., k(2)\}$.

Alice will work with graph ${}^{Q(2)}DS_{s+m(1)+m(2),k(2)}(R)^t$, $R=K[z_1, z_2, ..., z_{s+m(1)+m(2)}, z_{\alpha(2,1)}, z_{\alpha(2, 2)}, ..., z_{\alpha(2, m(3))}]$. She selects parameters to create momentum graphs ${}^3D_1, {}^3D_2 ,..., {}^3D_{l(3)}$ of the temporary graph ${}^{Q(2)}DS_{s+m(1)+m(2), k(2)}(K)^t$.

Alice forms tuples $a(3, 1), a(3, 2),...., a(3, l(3)), b(3, 1), b(3, 2),..., b(3, l(3))$ with coordinates from $K[z_1, z_2, ..., z_{s+m(1)+m(2)}]$ such that $den\ (a(3, i)b(3, i))=O((s+m(1)+m(2)+m(3))^{d(3)})$. Alice constructs the transformation $F_3=F(a(3, 1), a(3, 2),...., a(3, l(3)), b(3, 1), b(3, 2),..., b(3, l(3)), g(2), {}^3D_1, {}^3D_2,..., {}^3D_{l(3)})$ of $K^{s+m(1)+m(2)+m(3)}$ where $g(2)$ is the tuple $(G_2(z_1), G_2(z_2),..., G_2(z_{s+m(1)+m(2)})$.

She selects the pair of $H_3, H_3'\epsilon^{s+m(1)+m(2)+m(3)}EG(K)$ such that $(H_3H_3', (K^*)^{s+m(1)+m(2)+m(3)})$ is identity permutation.

She selects $L=L_3$ from $AGL_{s+m(1)+m(2)+m(3)}(K)$ of density $O(1)$ and forms $G_3=H_3F_3L_3$.

The density of the standard form of the map G_3 will be determined as $O((s+m(1)+m(2)^{d(3)})$ or $O((s+m(1)+m(2)+m(3))^{d(3)/\mu(3)})$. The map G_3 has a multiplicative trapdoor accelerator T_3 which is extension of T_2 via adding $Q(2)$ of cardinality $m(3)$, parameters $k(2)$, $l(3)$, equations of ${}^{Q(2)}DS_{s+m(1)+m(2),k(2)}(K)$, tuples $a(3.1), a(3, 2),...., a(3, l(2)), b(3, 1), b(3, 2),..., b(3, l(3))$, momentum graphs ${}^3D_1, {}^3D_2,..., {}^3D_{l(3)}$ and transformations H_3, H_3', L_3.

Alice continue the iterative process**.** She creates G_4 , G_5, ..., G_r of the densities of kind $O(n(i))^{\beta(i)}$, $i=4, 5,...., r$ where $n(i)$ is the dimension of the space of ciphertexts and $\beta(i)=d(i)/\mu(i)$ with the multiplicative trapdoor accelerators T_i , $i=4,5,..., r$ respectively.

So the final map G_r of $K^{s+m(1)+m(2)+...+m(r)}$ to itself with the multiplicative trapdoor accelerator T_r has a polynomial density.

Recall that $d(i)\geq d(i-1)/\mu(i-1)$ for $i=2, 3,..., r$**.** In the case when these inequalities become equalities $d(r)/\mu(r)=d(1)/(\mu(1)\mu(2)\mu(3)...\mu(r))$

Alice can select $d(1)=0$ when G_r has density $O(1)$. Then the output will be pseudolinear map. The choice of small parameter $d(1)$ will allow her to get sub quadratic map of the density $O(n^{\lambda})$ with arbitrary selected λ, $\lambda<1$**.** Obviously Alice can create the map G_r of prescribed density $O(n^d)$ with the multiplicative trapdoor accelerator.

Note that Alice can take $G_r L$ where L has degree 1 and density $O(n)$ and use the standard form of transformation of density
$O(n^{d+1})$ with the multiplicative trapdoor accelerator.

Procedure 1.3. (reimage computation for (G_r, T_r)).

Assume that $G_j=H_jF_jL_j$, $j=1,2,...., r$ and $F_j=F(a(1, j), a(2, j),...., a(l(j), j), b(1, j), b(2, j),..., b(l(j),j), g(j-1), {}^jD_1, {}^jD_2,..., {}^jD_{l(j)})$ acting on the affine space ${}^jW$ of dimension $s+m(1)+m(2)+...+m(j)=n(j)$.

Alice obtained the ciphertext ${}^0c=({}^0c_1, {}^0c_2,..., {}^0c_{n(r)})$. She computes $L_r^{-1}({}^0c) = {}^rc$ and takes its projection ${}^rc'$ on the first $n(r-1)$ coordinates.

Alice computes $L_{r-1}^{-1}({}^rc')={}^{r-1}c$ and takes its projection ${}^{r-1}c'$ on first $n(r-2)$ coordinates. She continue this procedure and gets the tuples ${}^1c=(b_1, b_2, ..., b_s, b_{s+1}, b_{s+2},..., b_{s+m(1)})$ and ${}^1c'=(b_1, b_2,..., b_s)$.

Alice forms the intermediate tuple $(z_1, z_2,..., z_s)$ and investigates the system of linear equations $c_1(z_1, z_2,..., z_s)=b_1, c_2(z_1, z_2,..., z_s)=b_2, ..., c_s(z_1, z_2,..., z_s)=b_s$. She gets the solution $z_1=\alpha_1, z_2=\alpha_2, ..., z_s=\alpha_s$. In fact $(\alpha_1, \alpha_2, ..., \alpha_s)= E'(N^{-1}(b_1, b_2, ..., b_s))$.

Alice computes tuples $a^*(i, 1)=a(1, 1)(\alpha_1, \alpha_2,..., \alpha_s)$, $b^*(i, 1)=b(1, 1)(\alpha_1, \alpha_2,..., \alpha_s)$, $i=1, 2,..., l(1)$ with coordinates from K.

Alice takes graph ${}^1D_{l(1)}$ and computes $d(l(1))=J_{b^*(l(1),1)}({}^1c)$. She takes the neighbour $d'(l(1)=N_{a^*(l(1)),1)}(d(l(1))$ of the point $d(l(1)$ of colour $a^*(l(1), 1)$.

Alice treats the tuple $d'(l(1))$ as the line of the graph ${}^1D_{l(1)}$. She computes $J_{b^*(l(1)-1),1)}(d'(l(1))=d(l(1)-1)$ and its neighbour $d'(l(1)-1)=N_{a^*(l(1)-1),1)}(d(l(1)-1)$. Alice continue this process and gets $d'(1)=N_{a^*(1,1)}(d(1))$ in the graph ${}^1D_1$. So she gets $e(1)=J_{\gamma}(d'(1))$, $\gamma= (\alpha_1,\alpha_2,..., \alpha_s)$.

The tuple $(H_1)'(e(1))=r(1)$ is the solution of the equation $H_1F_1(z_1, z_2, z_s, z_{s+1}, ..., z_{s+m(1)})= {}^1c=(L_1)^{-1}({}^2c')$ which is equivalent to
$G_1(z_1, z_2, z_s, z_{s+1}, ..., z_{s+m(1)})={}^2c'$.
Alice considers the equation $H_2F_2(z_1, z_2, ..., z_s, z_{s+1}, ..., z_{s+m(1)}, z_{s+m(1)+1},...,z_{s+m(1)+m(2)})= {}^2c=L_2({}^3c')$.

The first $s+m(1)$ equations of this system are equivalent to $H_1F_1(z_1, z_2, ..., z_{s+m(1)})={}^1c$ with the solution $\gamma(1)=({}^1\alpha_1, {}^1\alpha_2, \ldots, {}^1\alpha_{s+m(1)})$ obtained due to the knowledge of the trapdoor accelerator.

Alice computes the specializations $a^*(1, 2), a^*(2, 2),..., a^*(l(2), 2), b^*(1, 2), b^*(2, 2),..., b^*(l(2), 2)$ of $a(1, 2), a(2, 2),..., a(l(2), 2), b(1, 2), b(2, 2),..., b(l(2), 2)$ under the substitution $z_1={}^1\alpha_1, z_2={}^1\alpha_2, \ldots, z_{s+m(1)}={}^1\alpha_{s+m(1)}$.
She computes the point $d(l(2))=J_{b^*(2, l(2))}({}^2c)$ and line $d'(l(2))=N_{a^*(2, l(2))}(d(l(2)))$ of the graph ${}^2D_{l(2),}$ computes $d(l(2)-1)=J_{b^*(2, l(2)-1)}(d'(l(2))$ and vertex $d'(l(2)-1)=N_{a^*(2, l(2)-1)}(d(l(2)-1))$ of the graph ${}^2D_{l(2)-1}$. Alice continue this process and gets $d'(1)=N_{a^*(2,1)}(d(1))$ in the graph ${}^2D_1$. So she gets $e(2)=J_{\gamma(1)}(d'(1))$ in this graph.
The tuple $(H_2)^{'}(e(2))=\gamma(2)$ is the solution of the equation $H_2F_2(z_1, z_2, z_s, z_{s+1}, \ldots, z_{s+m(1)}, z_{s+m(1)+1,\ldots,} z_{s+m(1)+m(2)})={}^2c=L_2({}^3c')$ which is equivalent to $G_2(z_1, z_2, z_s, z_{s+1}, \ldots, z_{s+m(1)+m(2)})={}^3c'$. Alice continue this recurrent process and gets the solution $\gamma(r)$ of the equation $G_r(z_1, z_2, z_s, z_{s+1}, \ldots, z_{s+m(1)+m(2)+\ldots+m(k)})={}^0c$.

Remark 5.3. ***(****nonlinear disturbance****).*** In this iterative algorithm instead of the combination EN on K^s one can take any pseudolinear map Z with the multiplicative trapdoor accelerator at most d with the trapdoor accelerator can be used.

4. On the safe delivery of multivariate maps.

4.1. On protocols of Noncommutative Cryptography.

The following protocol is one of the classical instruments of Noncommutative Cryptography.

Twisted Diffie-Hellman protocol.

Similarly Let S be an abstract group which has some invertible elements.
Alice and Bob poses common element $g \in S$ and the pair of invertible elements h, h^{-1} from this semigroup.
Alice selects natural numbers $k(A)$ and $r(A)$, she forms $h^{-r(A)}g^{k(A)}h^{r(A)}= g_A$.
Bob choses $k(B)$ and $r(B)$, he forms $h^{-r(B)}g^{k(B)}h^{r(B)}= g_B$.
They exchange g_A, g_B and compute the collision element X as ${}^Ag= h^{-r(A)}g_B{}^{k(A)}h^{r(A)}$ (Alice) and ${}^Bg= h^{-r(B)}g_A{}^{k(B)}h^{r(B)}$ (Bob) respectively.

The security of this scheme is based on the complexity of Power Conjugacy Problem, adversary has to solve the equation $h^{-x}g^yh^x=b$, where b coincides with g_B or g_A. The complexity of this problem is essentially depends on the choice of highly noncommutative platform S.

In the case of platform $S={}^nES(K)$ where $K=F_q$ or $K=Z_q$ this problem is intractable even with the use of quantum computer.

The computational complexity of this protocol is $O(n^3)$.

If we assume that the degree of transformations h and g from ${}^nES(K)$ is $O(1)$ then the complexity of the protocol is $O(n)$.

Other platforms defined in terms of multivariate cryptography and corresponding protocols reader can find in [6], [13], [16], [17] [59], [60], [61]. Foundations of Noncommutative Cryptography, description of algorithms and crypt-analytic results reader can find in [38]-[58].

4.2. Safe delivery of transformations of polynomial density $O(n^d)$.

Let F be the map from $(K^*)^n$ in K^n of density $O(n^d)$, $0 \le d \le 1$ such that its restriction on $(K^*)^n$ is injective. Assume that T is a multiplicative trapdoor accelerator of F and Alice has the pair (F, T).

Below please find an examples of the deformation.

Example 1.4. (the case of maps of unbounded degree**).**

Alice and Bob conduct Twisted Diffie-Hellman protocol based on the platform ${}^nES(K)$. Assume that the collision map C is given by formula (1). Correspondents can use subsemigroup of ${}^nES(K)$ with generators from the set $M=\{g , h, C\}$. They use open channel to agree on words $w_j(C)=({}^jg_{i(1)}, {}^jg_{i(2)}, \ldots, {}^jg_{i(s(j))})$ of length $s(j), s(j) \ge 1$ where ${}^j\boldsymbol{g}_{i(1)}, {}^j\boldsymbol{g}_{i(2)}, \ldots, {}^jg_{i(s(j))}$, $j=1, 2, \ldots, r$ is the sequence of elements of the alphabet M which contains at least one appearance of C.

Let ${}^jg(C)$ are element of ${}^nES(K)$ generated as product of characters of the $w_j(C)$. We form ${}^jh(C)$ sending x_i to ${}^jg(C)(x_i)a(i, j)$ where $a(i, j)$ are publicly known elements of $K-\{0\}$.

Let $G(C)$ be the sum ${}^1h(C)+{}^2h(C)+\ldots{}^rh(C)$.

Alice can send the tuple $(F(x_1)+G(C)(x_1), F(x_2)+G(C)(x_2), \ldots F(x_n)+G(C)(x_n))$ to Bob. He is able to restore the map F.

This ''steganographic'' way of safe delivery of the multivariate map is secure even in the case r is linear expression from n of size $O(n)$.

Example 2.4. (the case of nonlinear transformation of constant degree d).

Alice takes the collision element C and nonempty subsets of $\{1, 2, \ldots,n\}$ of kind $\{i(1), i(2), \ldots, i(m)\}$ of cardinality m, $1 \le m \le d$.

She form g_i as the linear combination of monomial terms $(q_{i(1)})^{a(i, i(1))}(q_{i(2)})^{a(i, i(2))}\ldots(q_{i(m)})^{a(i, i(m))}\ldots x_{i(1)}x_{i(2)}\ldots x_{i(m)}$ and constant $C(x_i)(q_1, q_2,\ldots, q_m)$ with known nonzero coefficients from K. Alice sends $(F(x_1)+g_1, F(x_2)+g_2,\ldots, F(x_n)+g_n)$ to Bob.

Remark 1.4. Assume that the map F of degree $O(n)$ is not given publicly, Alice and Bob use it in the protocol based secure way.

Adversary may intercept polynomial number of pairs of kind plaintext /ciphertext but even this information can be insufficient for restoration of F without the knowledge of symbolic type of Z, i. e. lists of nontrivial monomial terms of $F(x_i)$ with coefficients 1.

Remark 2. 4. It is known that polynomial system of equations of degree $d(n)$ can be rewritten as system of quadratic equations via the method of introducing extra variables. If degree is unbounded than growth of number of variables does not allow to investigate resulting quadratic system. In case when the system is not given publicly the method of degree reduction can not be used.

5. Obfuscations of the algorithms in terms of Lie Geometries and their temporal analogue.

Missing definitions on Lie and Weyl geometries theory reader can find in [18] or [19], [20].

Let $X_n(F)$ be a simple Chevalley group over the field F with the corresponding Coxeter-Dynkin diagram X_n ($A_n, B_n, C_n, D_n, E_6, E_7, E_8, F_4, G_2$) **.** We can consider the geometry $\Gamma(X_n, F)$ of this defined by the following way.

Let U^+ be the unipotent subgroup of $X_n(F)$ generated by root subgroups corresponding to positive root of the root system with the diagram X_n and U^- be the subgroup generated by root subgroups corresponding to negative roots. Assume that at P_i, $i=1, 2,..., n$ are standard maximal subgroups, i. e. maximal subgroups of $X_n(F)$ containing U^+. Geometry $\Gamma(X_n(F))$ is the disjoint union of left cosets $(X_n(F):P_i)=\Gamma_i$, $i=1, 2,..., n$ with the type function $t(gP_i)=i$ and incidence relation I two elements α and β from Γ of different type are incident if and only if the intersection of these cosets is a nonempty set.

Let S_i be the orbit (U^-, Γ_i) containing P_i. The incidence structure ${}^{i,j}S(X_n, F)$ of I restricted onto S_iUS_j, $i\neq j$ is known as cellular Schubert graph. The following statements are proved in [6].

Theorem 1.4. *Cellular Schubert graph* ${}^{i,j}S(X_n, F)$ *is a Jordan-Gauss graph.*

Let ${}^{i,j}S(X_n, K)$ be some linguistic graph over the commutative ring K symbolically equivalent to ${}^{j}S(X_n, F)$.

Proposition 1.5. *Let us consider map introduced above map* $G=L_1F(a_1, a_2,...., a_l, b_1, b_2,..., b_l, c)L_2$ *in the case of the graph* ${}^{i,j}S(A_n, K)$. *Assume that deg a(i)+deg b(i)*$\leq d$, *deg* $c=d$. Then degree of $G=G(a_1, a_2,..., a_l, b_1, b_2,..., b_l, c)$ *is d.*

Corollary 1.5. *One can take the temporal graph* ${}^{i,j}S(A_n, K)^t$ *instead of* ${}^{i,j}S(A_n, K)$. *Then the degree of the map will be also bounded by d.*

Description of the graph ${}^{i,j}S(A_n, K)$ in terms of Projective Geometry is given in [22] where public key algorithm based on the trapdoor accelerator of quadratic multivariate bijective map is presented.

The trapdoor accelerator is the knowledge on the equations of the linguistic graph ${}^{i,j}S(A_n, K)$, the tuples $a_1, a_2,...., a_l, b_1, b_2,..., b_l$, description of trapdoor accelerator of the map defined by the tuple $\boldsymbol{c}$ and two affine transformations on the space of plaintexts.

This multivariate public key is presented in [6], special case ***d=2*** is considered in [21] and [22] . These cryptosystems and their generalisation in terms of temporal Jordan-Gauss graphs can be used as inputs of iterative Algorithms of Examples 1.2 and 2.2 of Section 2.

Proposition 2.5. *Let us consider map introduced above map* $G=L_1F(a_1, a_2,...., a_l, b_1, b_2,..., b_l, c)L_2$ *in the case of the graph* ${}^{i,j}S(X_n, K)$ where $X_n \in \{B_n, C_n, D_n\}$. *Assume that* $deg\ a(i)=1$, $deg\ b(i)=1$, $deg\ c\leq 3$. Then degree of $G=G(a_1, a_2,..., a_l, b_1, b_2,..., b_l, c)$ *is 3.*

Proposition 3.5. *Let K be a commutative ring with nontrivial multiplicative group K*. Then for defined above* $F=F(a_1, a_2,...., a_l, b_1, b_2,..., b_l, c)$ *in the case of graph* ${}^{i,j}S(X_n, K)$ where $X_n \in \{B_n, C_n, D_n\}$ *and densities of* a_i, b_i *and* $\mathbf{c}$ *are of size* $O(s^{\alpha})$, $O(s^{\alpha})$ *and* $O(s^{3\alpha})$. *Then den F has size* $O(s^{3\alpha})$.

Proposition 4. 5. *Let us consider introduced above map* $F=F(a(1), a(2),...., a(l), b(1), b(2),..., b(l), c, D_1, D_2,..., D_l)$ *in the case of the graph* ${}^{i,j}S(A_n, K)^t$ *where K is a commutative ring with nontrivial multiplicative group K*. Assume that the densities of a(i), b(i) and* $\mathbf{c}$ *are of size* $\mathbf{O(s^{\alpha(i)})}$, $O(s^{\beta(i)})$ *and* $O(s^{\gamma})$ *such that* $0\leq\alpha(i)+\beta(i)\leq d$ *and* $\gamma\leq d$ *for some d,* $d\geq 0$. *Then den F has size* $O(s^d)$.

Proposition 5. 5. *Let K be a commutative ring with nontrivial multiplicative group K*. Then for defined above* $F=F(a_1, a_2,...., a_l, b_1, b_2,..., b_l, c)$ *in the case of graph* ${}^{i,j}S(X_n, K)$ where *densities of* a_i, b_i *and c are of size O(1), then den F has size O(1).*

The implementation of the public key algorithm based on the ${}^{i,j}S(A_n, K)$ based multivariate map *F* of Proposition 8 with the multiplicative trapdoor accelerator is presented in [23]. The substitution of ${}^{i,j}S(A_n, K)^t$ instead of ${}^{i,j}S(A_n, K)$ leads to essential obfuscation of the cryptosystem.

This multivariate public key can be used as input of iterative Algorithms of Example 1.3 of Section 3.

Remark 1.5. In each case of last 3 written above statements we can take temporal Jordan - Gauss graph ${}^{i,j}S(X_n, K)^t$ instead of ${}^{i,j}S(X_n, K)$ and get multivariate map with similar properties.

We define symplectic homomorphism of the linguistic graph $I_n(K)$ of type r, s, m given by equations (1) as the map obtained by deleting of some coordinates of point $(x_1, x_2, ..., x_{s+m})$, and line $[y_1, y_2, ..., y_{r+m}]$ with indexes from of kind $\{s+i(1), s+i(2), ..., s+i(l)\}$ and $\{r+i(1\}, r+i(2), ..., r+i(l)\}$ respectively, where $J=\{i(1), i(2), ..., i(l)\}$ are nonempty subset of $\{1, 2, ...,m\}$ such that deletion of equations with right hand sides $f_{i(j)}$ and and coordinates indexes $\{1, 2,..., s\}U[1, 2, \mathbf{„„} r\}$ which do not appear in remaining equations lead to a new linguistic graph.

We refer to the image of symplectic homomorphism as symplectic quotient. Truncated Schubert graph ${}^{Q}DS_{s,r}(K)$ is a symplectic quotient of Jordan-Gauss graph ${}^{Q}DS_{s,r}(K)$.

Note that the each subset $J=\{m, m-1, ...m- k\}$, $1<k<m$ defines the symplectic homomorphism of $I_n(K)$.

Note that some quotients of graphs ${}^{i,j}S(A_n, K)$ can be used in iterative algorithms of Examples *1, 2, 3* instead of graphs ${}^{Q}DS_{s,r}(K)$.

Orbits of U^- on $\Gamma(X_n, F)$ are vector spaces of kind F^k, $k\geq 0$. Invariant cosets gP_i where g is Coxeter element, i.e. the element of Weyl group with maximal length of irreducible decomposition into standard generators, can be treated as 0-dimensional subspaces. These orbits are in one to one correspondence with elements of Weyl geometry $\Gamma(W)$. Let S_α be orbit corresponding to $\alpha\epsilon\, \Gamma(W)$ of dimension $d(\alpha)$. Two elements $x \epsilon S_\alpha$ and $y \epsilon S_\beta$ can be incident only in the case when α is incident to β in Weyl geometry $\Gamma(W)$. For each flag $\{\alpha, \beta\}$ of $\Gamma(W)$ we consider $I(\alpha, \beta)$ which is the restriction of I on $S_\alpha \cup S_\beta$.

Proposition 5.5. *The incidence structure $I(\alpha, \beta)$ with point set $F^{d(\alpha)}$ and line set $F^{d(\beta)}$ is a Jordan-Gauss graph.*

Let K be a commutative ring with the unity. *Temporal geometry* $\Gamma(X_n, K)^t$, $t=1, 2,....$ is the disjoint union of $K^{d(\alpha)}$ together with the totality of temporal Jordan-Gauss graphs $I(\alpha, \beta, K)^t$. We say that $x\epsilon K^{d(\alpha)}$ and $y\epsilon K^{d(\beta)}$ are incident in momentum $t=i$ if $\alpha I\beta$ and x, y is an edge of the graph $I(\alpha, \beta, K)^t/t=i$.

Let $\{\alpha,\beta\}$ be standard flag of rank 2 , i.e $\alpha=W_i$, $\beta=W_j$ where $i\neq j$. We consider the reverse walk of kind $\alpha, \beta, \gamma(1), \gamma(2), ..., \gamma(l), \beta, \alpha$. It means that $\alpha I\beta,\ \beta I\gamma(1), \gamma(1)I\gamma(2), ..., \gamma(l)I\beta$ in the Weyl geometry $W(X_n)$.

We consider the sequence of incidence structures ${}^1I=(K^{d(\alpha)}, K^{d(\beta)}, I(\alpha, \beta, K)^t/t=1)$, ${}^2I=(K^{d(\beta)}, K^{d(\gamma(1))},\ I(\beta, \gamma(1), K)^t/t=2)$, ${}^3I=(K^{d(\gamma(1))}, K^{d(\gamma(2))},\ I(\gamma(1), \gamma(2), K)^t/t=3)$, $(K^{d(\gamma(2))}, K^{d(\gamma(3))}$, ${}^4I=(I(\gamma(2), \gamma(3), K)^t/t=4)$, ..., ${}^{l+2}I=(K^{d(\gamma(l))}, K^{d(\beta))}$, $I(\gamma(l), \gamma(\beta), K)^t/t=l+2)$, ${}^{l+3}I=(K^{d(\beta))}, K^{d(\alpha)}, I(\gamma(\beta), \gamma(\alpha), K)^t/t=l+3)$.

Let $(s(j), r(j), m(j))$ be the type of linguistic graph ${}^jI$, $j=1, 2, ,..., l+3$. The pair $a(j)\epsilon K^{s(j)}$, $b(j)\epsilon K^{r(j)}$ defines the colour of ${}^jI$. Let c be the colour of the point of ${}^1I$ (or the line in ${}^{l+3}I$).

We define the circular walk with jumps starting in $p\epsilon K^{s(j)}$ and ending in $p'\epsilon K^{s(j)}$ as the following sequence of vertices of $\Gamma(X_n, K)^t$:

$p,\ v_1=J_{a(1)}(p), u_1=N_{b(1)}(v_1), v_2=J_{a(2)}(u_1), u_2=N_{b(2)}(v_2), ..., v_{l+3}=J_{a(l+3)}(u_{l+2}), u_{l+3}=N_{b(l+3)}(v_{l+3}), u'_{l+3}=J_c(u_{l+3})$.

We denote the above presented circular walk with jumps **a**s $C(p, a(1), b(1), a(2), b(2), ..., a(l+3), b(l+3), c, I_1, I_2, ..., I_{l+3})$.

Let us consider the commutative ring $R=K[z_1, z_2,..., z_m]$, $m=d(\alpha)$ and $s=s(1)$. We consider graphs $I_1(K[z_1, z_2,..., z_m]), I_2 (K[z_1, z_2,..., z_m]), ..., I_{l+3} (K[z_1, z_2,..., z_m])$, special element $z=(z_1, z_2,..., z_m)$ from $(K[z_1, z_2,..., z_m])^{d(\alpha)}$ and colours $A(j)\epsilon K[z_1, z_2,..., z_s])^{s(j)}$, $B(j)\epsilon K[z_1, z_2,..., z_s])^{r(j)}$ and $D=(D_1, D_2, ..., D_s)\epsilon K[z_1, z_2,..., z_s])^s$

and create the sequence as $C=C(z, A(1), B(1), A(2), B(2), ..., A(l+3), B(l+3), D, I_1, I_2, ..., I_{l+3})$. Assume that

$u=(D_1(z_1, z_2,..., z_s), D_2(z_1, z_2,..., z_s), ..., D_2(z_1, z_2,..., z_s), H_{s+1}(z_1, z_2,..., z_s, z_{s+1}, z_{s+2}, ..., z_m), H_{s+2}(z_1, z_2,..., z_s, z_{s+1}, z_{s+2}, ..., z_m), ..., H_m(z_1, z_2,..., z_s, z_{s+1}, z_{s+2}, ..., z_m)$.

We consider the map $F=F(A(1), B(1), A(2), B(2), ..., A(l+3), B(l+3), D, I_1, I_2, ..., I_{l+3})$ given by

$z_1 \to D_1(z_1, z_2,..., z_s), z_2 \to D_1(z_1, z_2,..., z_s), ..., z_s \to D_s(z_1, z_2,..., z_s),$

$z_{s+1} \to H_{s+1}(z_1, z_2,..., z_s, z_{s+1}, z_{s+2}, ..., z_m), z_{s+2} \to H_{s+2}(z_1, z_2,..., z_s, z_{s+1}, z_{s+2}, ..., z_m), ...,$

$z_{s+2} \to H_{s+2}(z_1, z_2,..., z_s, z_{s+1}, z_{s+2}, ..., z_m)$.

Let $(N_1(z_1, z_2,..., z_s), N_2(z_1, z_2,..., z_s), ..., N_k(z_1, z_2,..., z_s))$ be an element from $K[z_1, z_2,..., z_s]^k$ and $\boldsymbol{G}$ is an endomorphism of $K[z_1, z_2,..., z_s]$. We assume that $N(G)$ stands for $(N_1(G(z_1), G(z_2), ... , G(z_k)), N_2(G(z_1), \boldsymbol{G(z_2)}, ... , G(z_k)), ..., (N_k(G(z_1), G(z_2), ... , G(z_k))$. Then the composition of $F=F(A(1), B(1), A(2), B(2), ..., A(l+3), B(l+3), D, I_1, I_2, ..., I_{l+3})$ and $F'=F(A'(1), B'(1), A'(2), B'(2), ..., A(l'+3), B'(l'+3), D', I'_1, I'_2, ..., I'_{l+3})$ will be written as

$FF'=F(A(1), B(1), A(2), B(2), ..., A(l+3), B(l+3), D, A'(1)(D), B'(1)(D), A'(2)(D), B'(2)(D), ..., A(l'+3)(D), B'(l'+3), D'(D)), I_1, I_2,..., I_l, I'_1, I'_2,..., I_{l'})$.

So we prove the following statement.

Proposition 5. 5. *Let S be a semigroup of ${}^sCS(K)$. Then the totality ${}^{i,j}H(X_n, S)$ of transformations of kind $F=F(A(1), B(1), A(2), B(2), ..., A(l+3), B(l+3), D, I_1, I_2, ..., I_{l+3}), D \epsilon S$ is a subsemigroup in ${}^{s+m}CS(K)$.*

Theorem 2. 5. *Assume that $X_n=A_n$ and for $F=F(A(1), B(1), A(2), B(2), ..., A(l+3), B(l+3), D, I_1, I_2, ..., I_{l+3})$ the conditions deg $A(i)$+ deg $B(i) \le d$, $i=1,2,...., l$, deg $D \le d$ hold. Then deg $F \le d$.*

Assume that $AGLS_s(K)$ be a semigroup of all endomorphisms of $K[x_1, x_2,..., x_s]$ of degree 1. So $AGL_s(K)$ is the subgroup of all invertible elements of $AGLS_s(K)$.

Corollary 2.5. *The maximal degree of elements* of ${}^{i,j}H(A_n, AGLS_s(K))$ *satisfying conditions of Theorem 1 is d.*

Let us consider the binary walk , i. e. the reverse walk $\alpha, \beta, \gamma(1), \gamma(2), ..., \gamma(l), \beta, \alpha$ of Weyl geometry where l is odd and $\gamma(j)=\alpha$ if j is odd, $\gamma(j)=\beta$ if j is even.

Let ${}^{i,j}B(X_n, S)$ be the subsemigroup in ${}^{i,j}H(X_n, S)$ consisting of elements corresponding to binary walks.

Theorem 3. 5.

The semigroup ${}^{i,j}B(X_n, AGL_s(K))$ is a subgroup of ${}^{s+m}CG(K)$.

Algorithm 1.5.

Let us consider the special cases of the implementation of twisted Diffie-Hellman protocol with the platform $H = L^{i,j}H(X_n, AGLS_s(K))(L)^{-1}$ Assume that elements g and h , $h \epsilon L^{i,j}B(X_n , AGL_s(K)) (L)^{-1}$ written in their standard forms are known publicly. Alice and Bob elaborate the collision element $\boldsymbol{Z}$ in its standard form.

Let us consider some special options in the case of $X_n=A_n$.

a) The densities of L and L^{-1} are of size $O(1)$, $s=O(n^{\alpha})$ for $\alpha<1$.

We consider the subsemigroup ${}^{i,j}H^d(A_n, AGLS_s(K))$ of semigroup ${}^{i,j}H(A_n, AGLS_s(K))$ formed by elements $F(A(1), B(1), A(2), B(2), ..., A(l+3), B(l+3), D, I_1, I_2, ..., I_{l+3})$ where $l=O(1)$, densities of $A(i)$, $B(i)$ and $D(i)$ are of size $O(1)$ and the maximal value of $\deg(A(i))+\deg(B(i))$ is the constant d, $d>1$**.** Let $B^d(A_n, AGL_s(K))={}^{i,j}B(X_n, AGL_s(K))\cap {}^{i,j}H^d(A_n, AGLS_s(K))$.

Alice and Bob take elements g and h from $L^{i,j}H^d(A_n, AGLS_s))\, L^{-1}$. where $h \in L^{i,j}B^d(A_n, AGL_s(K))\, L^{-1}$.

Additionally they assume that parameters $k(A)$, $k(B)$, $r(A)$ and $r(B)$ are of size $O(1)$. In this case the collision element Z of the protocol will have density $O(1)$ and degree d.

So Alice can take a polynomial transformation G of linear density and nonlinear degree d with the trapdoor accelerator and send $G+Z$ to Bob.

In particular Alice can take the subgroup ${}^{i,j'}B(A_n, {}^sCG(K))$ and its element of kind $F'=F(A'(1), B'(1), A'(2), B'(2), ..., A'(l'+3), B'(l'+3), D', I'_1, I'_2, ..., I'_{l'+3})$ depending from l' and tuples $A'(1), B'(1), A'(2), B'(2), ..., A'(l'+3), B'(l'+3), D'$ of density $O(1)$ and maximal degree of $\deg(A'(i))+\deg(B'(i))$ and $\deg(D')$ equals d, $d>1$.

Alice takes element $G=L_1F'L_2$ where the densities of $L_1 \in AGL_{s+m}(K)$ and ${}_2\in AGL_{s+m}(K)$ are of size $O(1)$. In this case the element G will have density $O(1)$ and degree d. Let us assume that the map defined by the tuple D has a trapdoor accelerator T. Then the knowledge on the T, the graph ${}^{i,j'}S(X_n(K))$, L_1, L_2 and $A'(1), B'(1), A'(2), B'(2), ..., A'(l'+3), B'(l'+3), D', I'_1, I'_2, ..., I'_{l'+3}$ is a trapdoor accelerator of the map G.

Remark 2. 5. We can take L_2 of density $O(n^{\alpha})$, $0<\alpha\le 1$. In this case the density of the map G will be $O(n^{\alpha})$.

Remark 3. 5. We can create the tuple D' by the following way.

We have to select positive integer p and parameter k together with the partition of number s into parts $s(1), s(2), ..., s(k)$ where $1<s(i)\le p$. So $s(1)+s(2)+...+s(k)=s$. Then we can use methods of Section 2 to construct nonlinear maps Q_i of $K^{s(i)}$ of prescribed degree $d(i), 2\le d(i)\le d$. Assume that $Q_i=Q_i(x_1, x_2, ..., x_{s(i)})$ is given by the rule $x_i \to {}^iq(x_1, x_2, ..., x_{s(i)})$, $i=1, 2,..., k$. We can take the tuple D' as $(Q_1(z_1, z_2, ..., z_{s(1)}), Q_2(z_{s(1)+1}, z_{s(1)+2}, ..., z_{s(1)+s(2)}), \ldots, Q_k(z_{s(k-1)+1}, z_{s(k-1)+2}, ..., z_{s(1)+s(2)+...+s(k)})$.

b) Let us assume that d is 2 or 3.

Then Alice can take arbitrary element L from $AGL_{s+m}(K)$. So densities of L and L^{-1} are of size $O(n)$. Assume that ${}^{i,j}H_d(A_n, AGLS_s(K))$ stands for the subsemigroup of ${}^{i,j}H(A_n, AGLS_s(K))$ formed by transformations of kind $F(A(1), B(1), A(2), B(2), ..., A(l+3), B(l+3), D, I_1, I_2, ..., I_{l+3})$ with the maximal value of $\deg A(i)+\deg B(i)$ equals d and $l=O(1)$.

Assume that $B_d(A_n, AGL_s(K))={}^{i,j}B(X_n, AGL_s(K))\cap {}^{i,j}H_d(A_n, AGLS_s(K))$.Alice selects the maps $g\epsilon {}^{i,j}H_d(A_n, AGLS_s(K))$ and $h\epsilon {}^{i,j}B_d(A_n, AGLS_s(K))$. In this case the collision element Z of the protocol will be of degree d.

After the completion of this protocol in this case Alice can take a polynomial transformation G of degree d with the trapdoor accelerator and send $G+Z$ to Bob.
In particular Alice can take the subgroup ${}^{i,j'}B(A_n, {}^sCG(K))$ and its element of kind $F'=F(A'(1), B'(1), A'(2), B'(2), ..., A'(l'+3), B'(l'+3), D', I'_1, I'_2, ..., I'_{l'+3})$ depending from l' of size $O(1)$ and maximal values of $deg\ (A'(i)) + deg\ (B'(i))$ and degree of nonlinear D' equals d.
Alice takes element $G=L_1F'L_2$ where $L_1\epsilon AGL_{s+m}(K)$ and $L_2\epsilon AGL_{s+m}(K)$. In this case the element G has degree d. Let us assume that the map defined by the tuple D which has a trapdoor accelerator T.
Then knowledge on the T, the graph ${}^{i,j'}S(A_n(K))$, L_1, L_2 and $A'(1), B'(1), A'(2), B'(2), ..., A'(l'+3), B'(l'+3), D', I'_1, I'_2, ..., I'_{l'+3}$ is a trapdoor accelerator of the map G.

Remark 4. 5. Alice can create the tuple D' of degree d with the trapdoor accelerator via methods of Section 2.

Remark 5. 5. Note that ${}^{i,j}H^d(A_n, AGLS_s(K))< {}^{i,j}H_d(A_n, AGLS_s(K))$. In the case of small parameters d correspondents can use faster protocoldescribed in *(a)* with g and h from ${}^{i,j}H^d(A_n, AGLS_s(K))$ for the safe delivery of general element of degree d with a trapdoor accelerator**.**

c) The case of $L\epsilon M(n, K)$.

We define support $sup(t)$ of monomial term $t(x_1, x_2,..., x_n)$ as its number of variables x_i in positive powers. The support $sup(F)$ of the map F written in its standard form is the maximal support of its monomial terms.

Let us consider the modification of (a) when L is a pseudorandom element from $M(n, K)$, i.e. $L(x_i)=\alpha x_{\pi(i)}$ where $\alpha\epsilon K^*$ and π is a pseudorandom permutation on $\{1, 2,..., n\}$. Assume that $s=O(n^\alpha)$ for $0<\alpha\leq 1$. We consider the semigroup ${}^{i,j}H(A_n, AGLS_s(K), \beta)$ formed by elements of kind $F(A(1), B(1), A(2), B(2), ..., A(l+3), B(l+3), D, I_1, I_2, ..., I_{l+3})$ such that $denA(1)den\ B(1), den\ A(2)den\ B(2), ..., den\ A(l+3)den\ B(l+3)$ are of size $O(n^\beta)$, D is an element of $AGLS_s(K)$ of density $O(n^r)$, $r\leq min\ (\alpha, \beta)$. Assume that Alice and Bob take generators g and h from ${}^{i,j}H(A_n, AGLS_s(K), \beta)$. In this case the collision element Z of the protocol will have density $O(n^\beta)$ and support $O(n^\alpha)$.
In this case Alice can take a polynomial transformation G of unbounded degree, density $O(n^{\beta'})$ and support $O(n^\alpha)$ with the trapdoor accelerator and send $G+Z$ to Bob.
In particular Alice can take the subgroup ${}^{i,j}B(A_n, {}^sCG(K))$ and its element of kind $F'=F(A'(1), B'(1), A'(2), B'(2), ..., A'(l'+3), B'(l'+3), D', I'_1, I'_2, ..., I'_{l'+3})$ depending from l' of size $O(1)$ and tuples $A'(1), B'(1), A'(2), B'(2), ..., A'(l'+3), B'(l'+3)$ with

denA'(i)den B'(i) of size $O(n^{\beta'})$. She takes tuple *D'* of density $O(n^{\beta'})$ defining bijective map on K^s.

Alice takes element $G=L_1F'L_2$ where $L_1 \epsilon M(n, K)$, and $L_2 \epsilon AGL_{s+m}(K)$ has the density $O(n^{\gamma})$, $0 \leq \gamma \leq 1$. In this case the element *G* will have density $O(n^{\gamma+\beta'})$ and support $O(n^{\alpha})$. Let us assume that the map defined by the tuple *D* has a trapdoor accelerator *T*. Then knowledge on the *T*, the graph ${}^{i,j}S(A_n(K))$, L_1, L_2 and *A'(1), B'(1), A'(2), B'(2), ..., A'(l'+3), B'(l'+3), D', I'1, I'2, ..., I'l'+3* is a trapdoor accelerator of the map *G*.

Remark 6. 5. Alice can create the tuple *D'* of the bijective map of density β' with the trapdoor accelerator via methods of Section 3. She can select $0<\beta'+\gamma \leq 2$ and work with the pseudo quadratic, sub quadratic or pseudolinear map.

d) Case of multiplicative trapdoor accelerator.

Alice can take the subsemigroup ${}^{i,j}B(A_n, {}^sCS(K))$ and select the map *F'=F(A'(1), B'(1), A'(2), B'(2), ..., A'(l'+3), B'(l'+3), D', I'1, I'2, ..., I'l'+3)* such that *A'(1), B'(1), A'(2), B'(2), ..., A'(l'+3), B'(l'+3)* satisfy the conditions of *(c)* and *D'* of density $O(n^{\beta'})$ defines the map with the multiplicative trapdoor accelerator *T*. She takes element $E \epsilon {}^sEG(K)$ with the multiplicative trapdoor accelerator *T'*, $L_2 \epsilon AGL_{s+m}(K)$ of density $O(n^{\gamma})$, $\gamma \leq 1$ and computes the standard form of $EF'L_2=G$ of density $O(n^{\beta'+\gamma})$. Then knowledge on the *T*, *T'* , the graph ${}^{i,j'}S(A_n(K))$, L_1, L_2 and *A'(1), B'(1), A'(2), B'(2), ..., A'(l'+3), B'(l'+3), D', I'1, I'2, ..., I'l'+3* is a multiplicative trapdoor accelerator of the map *G*.

For the secure delivery of *G* from Alice to Bob correspondents can use the protocol described in (c) with the platform ${}^{i,j'}H(A_n, AGLS_s(K), \beta)$ with the output Z_1 of density $O(n^{\beta})$ and support of size $O(n^{\alpha})$. Additionally correspondents conduct twisted Diffie-Hellman protocol with the platform ${}^{s+m}ES(K)$ with the output E_1.

After the execution of two protocols Alice sends E_1Z_1+G to Bob and he restores the standard form of *G*.

6. Conclusions.

The technique of Jordan-Gauss graphs and their temporal analogue defined over arbitrary commutative ring *K* can be used for the construction of bijective multivariate map *F* of prescribed degree *d* on free module K^n with the trapdoor accelerator *T* which allows to compute the reimage of given value in a polynomial time. In the case of $d=2$ and 3 such maps can be used for the construction of public keys.

If *d* is a constant larger than 3 we can construct sparce maps of density $O(n)$ with the trapdoor accelerator *T*. So the value of function can be computed in time $O(n^2)$. For each constant *d* we can construct the map of degree *d*, density $O(n)$ and trapdoor accelerator which allows the computation of the reimage in time $O(n^2)$. Recall that we define the density of *F* as maximal density of polynomials $F(x_i)$ for $i=1, 2,..., n$.

It is known that there is a special way to increase number of variables and rewrite the nonlinear system $F(x)=b$ as equivalent to it quadratic system in many variables. One can select ''sufficiently large'' d such that corresponding quadratic system is unfeasible for cryptanalytic investigation.

We define $sup(t)$ of monomial term $t= t(x_1, x_2, ..., x_n)$ as the number of variables x_i in positive power in the expression of t. The support of the multivariate map F is defined as maximal value of $sup(F)$ supports of its monomial terms. We can construct multivariate maps on K^n with the prescribed density $O(n^{\alpha}), , 0 \leq \alpha \leq 1$ and prescribed support $O(n^{\beta})$ with the trapdoor accelerator. We construct multivariate map F of unbounded degree with the support n and prescribed density $O(n^{\beta})$ and multiplicative trapdoor accelerator.

Mentioned above pairs of kind (F, T) can be investigate as potential public key constructions of multivariate Cryptography. Alternatively Alice can use her pair (F, T) in different way. She and her trusted partner Bob can use twisted Diffie-Hellman protocol with the platform ${}^nES(K)$, deform the output E via its transformation to polynomial transformation $D(E)$ of K^n. Alice sends $F+D(E)$ to Bob. The security of this asymmetric algorithm described in Section 1 rests on the security of the selected protocol.

Note that mentioned above pairs (F, T) can be used as stream ciphers when the knowledge of T is shared between Alice and Bob.

The Section 5 contains the description of temporal geometries of Chevalley type X_n defined over commutative ring K. In term of these geometries several subsemigroups of corresponding affine Cremona semigroup are defined. In particular large platform of Multivariate Cryptography over K is defined in terms of temporal analogue of projective geometry over the field. We suggest several schemes of use of these semigroups for the construction of public keys, protocols of Noncommutative Cryptography and asymmetric protocol based cryptosystems.

References

1. V. Ustimenko, On Eulerian semigroups of multivariate transformations and their cryptographic applications. European Journal of Mathematics 9, 93 (2023).
2. V. Ustimenko, On small world non Sunada twins and cellular Voronoi diagrams, Algebra and Discrete Mathematics, vol. 30, N1 (2020), pp. 118-142.
3. N. Koblitz, Algebraic aspects of cryptography, Springer (1998), 206 p.
4. V. Ustimenko, Maximality of affine group, hidden graph cryptosystem and graph's stream ciphers, Journal of Algebra and Discrete Mathematics, 2005, v.1, pp 51-65.
5. V. Ustimenko, Linguistic Dynamical Systems, Graphs of Large Girth and Cryptography, Journal of Mathematical Sciences, Springer, vol.140, N3 (2007) pp. 412-434.
6. V. Ustimenko, Graphs in terms of Algebraic Geometry, symbolic computations and secure communications in Post-Quantum world, UMCS Editorial House, Lublin, 2022, 198 p.
7. Vasyl Ustimenko, Oleksandr Pustovit, Jordan-Gauss graphs and quadratic public keys of Multivariate Cryptography, ITTAP 2024: 4th International Workshop on Information Technologies: Theoretical and

Applied Problems, October 23-25, 2024, Ternopil, Ukraine, Opole, Poland, https://ceur-ws.org/Vol-3896/paper11.pdf.
8. V. Ustimenko, Tymoteusz Chojecki, Aneta Wróblewska, On the Jordan-Gauss graphs andmultivariate public keys. IACR Cryptol. ePrint Arch. 2024/1793.
9. T. Chojecki, G. Erskine, J. Tuite, V. Ustimenko, On affine forestry over integral domains and families of deep Jordan–Gauss graphs. European Journal of Mathematics 11, 10 (2025). https://doi.org/10.1007/s40879-024-00798-2.
10. V. Ustimenko, On computations with Double Schubert Automaton and stable maps of Multivariate Cryptography, Interdisciplinary Studies of Complex Systems, No. 19 (2021) 18–32 ,https://doi.org/10.31392/iscs.2021.19.018.
11. Vasyl Ustimenko, Aneta Wróblewska, On extremal algebraic graphs, quadratic multivariate public keys and temporal rules, FedCSIS 2023: 1173-1178 (see also IACR,e-print archive 2023/738).
12. Ding Jintai, Petzoldt Albrecht, and Schmidt Dieter S., Multivariate Public Key Cryptosystems, Second Edition. Advances in Information Security, Springer, 2020.
13. V. Ustimenko, A. Wroblewska, On the key exchange with nonlinear polynomial maps of stable degree, Annalles UMCS Informatica AI XI, 2 (2011), 81-93.
14. V. Ustimenko, On desynchronised multivariate algorithms of El Gamal type for stable semigroups of affine Cremona group, Theoretical And Applied Cybersecurity, 2019, Vol. 1 No. 1.
15. V. Ustimenko, On new symbolic key exchange protocols and cryptosystems based on hidden tame homomorphism. Dopovidi. NAS of Ukraine, 2018, n. 10, pp.26-36.
16. V. Ustimenko, On short digital signatures with Eulerian transformations, IACR e-print archive 2024/001.
17. V. Ustimenko, On the Restoration of Historical Matsumoto-Imai Cryptosystem and Other Schemes in Terms of Noncommutative Cryptography. In: Arai, K. (eds) Proceedings of the Future Technologies Conference (FTC) 2024, Volume 2. FTC 2024. Lecture Notes in Networks and Systems, vol 1155. Springer, Cham. https://doi.org/10.1007/978-3-031-73122-8_7.
18. A. Brower, A. Cohen, A. Nuemaier, Distance regular graphs, Springer, Berlin, 1989.
19. R. W. Carter, Simple Groups of Lie Type, Wiley, New York (1972).
20. F. Buekenhout (Editor), Handbook on Incidence Geometry, North Holland,Amsterdam, 1995.
21. V. Ustimenko, On Schubert cells in Grassmanians and new algorithms of multivariate cryptography, Proceedings of the Institite of Mathematics, Minsk, 2015, Volume 23, N 2, pp. 137-148 (Proceedings of international conference “Discrete Mathematics, algebra and their applications”, Minsk, Belarus, September 14-18, 2015, dedicated to the 100th anniversary of Dmitrii Alexeevich Suprunenko).
22. V. Ustimenko, On Schubert cells of Projective Geometry and quadratic public keys of Multivariate Cryptography, IACR e-print archive, 2024/1480.
23. V. Ustimenko, O.Pustovit,On Schubert cells of projective geometry and pseudo-quadratic public keys of multivariate cryptography (short paper). CPITS-II 2024: Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, October 26, 2024, Kyiv, Ukraine, 198-205, https://ceur-ws.org/Vol-3826/short7.pdf
24. V. A. Ustimenko. On new multivariate cryptosystems based on hidden Eulerian equations, Dopovidi of National Academy of Science of Ukraine N5, 2017.
25. V. Ustimenko, On new multivariate cryptosystems based on hidden Eulerian equations over finite fields, IACR e-print archive.2017/093.
26. J. Ding, A. Petzoldt, Current State of Multivariate Cryptography. IEEE Security & Privacy, vol. 15, no. 4, pp. 28--36 (2017), doi :10.1109/MSP.2017.3151328.
27. D. Smith-Tone, 2F - A New Method for Constructing Efficient Multivariate Encryption Schemes. In: PQCrypto 2022: The Thirteenth International Conference on Post-Quantum Cryptography, virtual, DC, US (2022).

28. D. Smith-Tone, New Practical Multivariate Signatures from a Nonlinear Modifier. IACR e-print archive, 2021/419.
29. D. Smith-Tone, C. Tone, A Nonlinear Multivariate Cryptosystem Based on a Random Linear Code, https://eprint.iacr.org/2019/1355.
30. D. Jayashree, R. Dutta, Progress in Multivariate Cryptography: Systematic Review, Challenges, and Research Directions. ACM Computing Survey, vol. 55, issue 12, No. 246, pp. 1--34 (2023). \doi{10.1145/3571071}
31. F. Cabarcas, D. Cabarcas, J. Baena, Efficient public-key operation in multivariate schemes. Advances in Mathematics of Communications, vol. 13, no. 2, pp. 343--343 (2019).
32. R. Cartor, D, Smith-Tone, EFLASH: A new multivariate encryption scheme. In: Proceedings of the International Conference on Selected Areas in Cryptography, pp. 281--299. Springer, Heidelberg (2018).
33. Casanova, A., Faugere, J.-C., Macario-Rat, G., Patarin, J., Perret, L., Ryckeghem, J.: Gemss: A great multivariate short signature. Submission to NIST (2017).
34. Chen, J., Ning, J., Ling, J., Lau, T. S. C., Wang, Y.: A new encryption scheme for multivariate quadratic systems. Theoretical Computer Science, vol. 809, pp. 372--383 (2020).
35. Chen, M.-S., H\"{u}sing, A., Rijneveld, J., Samardjiska, S., Schwabe, P., SOFIA: MQ-based signatures in the QROM. In: Proceedings of the IACR International Workshop on Public Key Cryptography, pp. 3--33. Springer, Heidelberg (2018).
36. Duong, D.H., Tran, H.T.N., Susilo, W., Luyen, L.V.: An efficient multivariate threshold ring signature scheme. Computer Standards \& Interfaces, vol. 74 (2021).
37. Faugere, J.-C., Macario-Rat, G., Patarin, J., Perret, L.: A new perturbation for multivariate public key schemes such as HFE and UOV. Cryptology ePrint Archive (2022).
38. D. N. Moldovyan and 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.
39. L. Sakalauskas, P. Tvarijonas and A. Raulynaitis, Key Agreement Protocol (KAP) Using Conjugacy and Discrete Logarithm Problem in Group Representation Level, INFORMATICA, 2007, vol. 18, No 1, 115-124.
40. 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.
41. Delaram Kahrobaei and 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.
42. Alexei Myasnikov; Vladimir Shpilrain and Alexander Ushakov (2008), Group-based Cryptography, Berlin: Birkhäuser Verlag.
43. Zhenfu Cao (2012), New Directions of Modern Cryptography. Boca Raton: CRC Press, Taylor & Francis Group. ISBN 978-1-4665-0140-9.
44. Benjamin Fine, et. al. "Aspects of Non abelian Group Based Cryptography: A Survey and Open Problems", arXiv:1103.4093.
45. Alexei G. Myasnikov; Vladimir Shpilrain and Alexander Ushakov (2011), Non-commutative Cryptography and Complexity of Group-theoretic Problems, American Mathematical Society.
46. I. Anshel, M. Anshel and D. Goldfeld, An algebraic method for public-key cryptography. Math. Res.Lett. 6(3–4), 287–291 (1999).
47. S.R. Blackburn and S.D. Galbraith, 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).

48. K.H. Ko, S.J. Lee, J.H. Cheon, J.W. Han, J.S. Kang and C. Park, 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).
49. G. Maze, C. Monico and J. Rosenthal, Public key cryptography based on semigroup actions, Adv.Math. Commun. 1(4), 489–507 (2007).
50. P.H. Kropholler and 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.
51. J.A. Lopez Ramos, J. Rosenthal, D. Schipani and R. Schnyder, Group key management based on semigroup actions, Journal of Algebra and its applications, 2017, vol.16,(08):1750148.
52. 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.
53. Myasnikov A., Roman'kov V. A linear decomposition attack // Groups, Complexity, Cryptology. 2015. Vol. 7. P. 81–94.
54. Roman'kov V. A. A nonlinear decomposition attack. Groups, Complexity, Cryptology. 2017. Vol. 8, No. 2. P. 197–207.
55. Romankov V. Two general schemes of algebraic cryptography. Groups, Complexity, Cryptology. 2018. Vol. 10, No. 2. P. 83–98.
56. Roman'kov V. An improved version of the AAG cryptographic protocol. Groups, Complexity, Cryptology. 2019. Vol. 11, No. 1. 1 2.
57. Tsaban B. Polynomial time solutions of computational problems in noncommutative algebraic cryptography. Journal of Cryptology. 2015. Vol. 28, No. 3. P. 601–622.
58. Ben-Zvi A., Kalka A., Tsaban B. Cryptanalysis via algebraic spans. Advances in Cryptology – CRYPTO 2018 / eds.: H. Shachan, A. Boldyreva. Berlin: Springer, 2018. P. 1–20. (LNCS; vol. 109991).
59. V. Ustimenko, M. Klisowski , On Noncommutative Cryptography with cubical multivariate maps of predictable density, In "Intelligent Computing'' , Proceedings of the 2019 Computing Conference, Londone, Volume 2, Part of Advances in Intelligent Systems and Computing (AISC, volume 998, Springer, pp. 654-674.
60. V. Ustimenko, M. Klisowski, On new protocols of Noncommutative Cryptography in terms of homomorphism of stable multivariate transformation groups, Algebra and Discrete Mathematics, Vol 35, No 2 ,2023, p. pp. 220-250, DOI:10.12958/adm1523.
61. V. Ustimenko, On Multivariate Algorithms of Digital Signatures on Secure El Gamal-Type Mode, «Computational Methods and Mathematical Modeling in Cyberphysics and Engineering Applications 1» by Dmitri Koroliouk, Sergiy Lyashko, Nikolaos Limnious, 2024,(https://onlinelibrary.wiley.com/doi/book/10.10.