Jordan-Gauss graphs and quadratic public keys of Multivariate Cryptography

Vasyl Ustimenko[1,2,†], Oleksandr Pustovit[2,*,†]

[1] *Royal Holloway University of London, United Kingdom, Egham Hill, Egham TW20 0EX, United Kingdom*

[2] *Institute of telecommunications and global information space, NAS of Ukraine, Chokolivsky Boulevard 13, Kyiv, 02000, Ukraine*

Abstract

Jordan-Gauss graphs are bipartite graphs given by special quadratic equations over the commutative ring K with unity with partition sets K^n and K^m such that the neighbour of each vertex is defined by the system of linear equation given in its row-echelon form. We use families of this graphs for the construction of new quadratic surjective multivariate maps F of affine spaces over K with the trapdoor accelerator T which is a piece of information which allows to compute the reimage of F in polynomial time.

In particular for each quadratic automorphism F of $K[x_1, x_2,..., x_n]$ with the trapdoor accelerator T we construct the quadratic surjective map F' of K^t, $t=n^2+n$ onto K^{t-s}, $s\geq 0$ with the trapdoor accelerator T', $T'>T$.

So we can introduce enveloping trapdoor accelerator for Matsumoto-Imai cryptosystem over finite fields of characteristic 2, for the Oil and Vinegar public keys over F_q or quadratic multivariate public keys defined over Jordan-Gauss graphs $D(n, K)$,where K is arbitrary finite commutative ring with the nontrivial multiplicative group

Keywords

Multivariate Cryptography, Jordan – Gauss graphs, Projective Geometries, Largest Schubert Cells, Symbolic Computations

1. Introduction

This paper presents the generalisations of the quadratic multivariate public key given in [23] and defined via special walks on projective geometries over finite fields and their natural analogues defined over general commutative rings. Multivariate cryptography is one of the five main directions of Post-Quantum Cryptography.

The progress in the design of experimental quantum computers is speeding up lately. Expecting such development the National Institute of Standardisation Technologies of USA announced in 2017 the tender on standardisation best known quantum resistant algorithms of asymmetrical cryptography. The first round was finished in March 2019, essential part of

[1] *ITTAP'2024: 4th International Workshop on Information Technologies: Theoretical and Applied Problems, October 23-25, 2024, Ternopil, Ukraine, Opole, Poland*

[*] Corresponding author.

[†] These authors contributed equally.

🖂 Vasyl.Ustymenko@rhul.ac.uk (V. Ustimenko); sanyk_set@ukr.net (O. Pustovt)

0000-0002-2138-2357 (V. Ustimenko); 0000-0002-3232-1787 (O. Pustovit)

presented algorithms were rejected. In the same time the development of new algorithms with postquantum perspective was continued. Similar process took place during the 2, 3 and 4th rounds.

The last algebraic public key «Unbalanced Oil and Vinegar on Rainbow like digital signatures» (ROUV) constructed in terms of Multivariate Cryptography was rejected in 2021 (see [2], [3]). The first 4 winners of this competition was announced in 2022, they are developed in terms of Lattice Theory.

Noteworthy that NIST tender was designed for the selection and investigation of public key algorithms and in the area of Multivariate Cryptography only quadratic multivariate maps were investigated. We have to admit that general interest to various aspects of Multivariate Cryptography was connected with the search for secure and effective procedures of digital signature where mentioned above ROUV cryptosystem was taken as a serious candidate to make the shortest signature.

Let us summarize the outcomes of mentioned above NIST tender.

There are 5 categories that were considered by NIST in the PQC standardization (the submission date was 2017; in July 2022, the 4 winners and the 4 final candidates were proposed for the 4th round - this is the current official status. However, the current 8 final winners and candidates only belong to the following 4 different mathematical problems (not the 5 announced at the beginning):- lattice-based,- hash-based,- code-based, - supersingular elliptic curve isogeny based.

The standards are partially published in 2024.

Its interesting that new obfuscation ‘’TUOV: Triangular Unbalanced Oil and Vinegar’’ were presented to NIST (see https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/TUOV-spec-web.pdf) by principal submitter Jintaj Ding.

Further development of Classical Multivariate Cryptography which study quadratic and cubic endomorphisms of $F_q[x_1, x_2,..., x_n]$ is reflected in [14]. Current research in Postquantum Cryptography can be found in [4], [5], [6], [7], [8], [9], [10], [11], [12]. [13], [15], [16], [17], [27], [28], [29], [30]

We use the concept of quadratic accelerator of the endomorphism σ of $K[x_1, x_2,..., x_n]$ which is the piece of information T such that its knowledge allows us to compute the reimage of (σ, K^n) in time $O(n^2)$. Symbol K stands here for an arbitrary commutative ring with unity. Our suggestion is to use for public key the pairs (σ, T) such that σ has a polynomial density, i. e. number of monomial terms of $\sigma(x_i)$, $i=1,2,...,n$. Some examples of such public keys the reader can find in [1], [22]

For each pair (K, n), $n>1$ we present quadratic automorphism σ of $K[x_1, x_2,..., x_n]$ with the trapdoor accelerator T defined via totality of special bipartite Jordan-Gauss graphs with the partition sets isomorphic to K^n. We discuss the possible use of these transformation in the case of finite fields and arithmetical rings Z_q where q is a prime power.

In this paper we suggest new quadratic multivariate public rules defined in terms of Projective Geometry. Recall that multivariate public rule G has to be given in its standard form $x_i \rightarrow g_i(x_1, x_2, \ldots , x_n)$, where polynomials g_i are given via the lists of monomial terms in the lexicographical order.

We consider the bipartite induced subgraphs $\mathcal{J}(F)$ of projective geometry over the field F which partition sets are the largest Schubert cells. The incidence of points and lines of these graphs is given by the system of quadratic equations such that the neighbourhood of each vertex is a solution set of the system of linear equation written in its row-echelon form. Straightforward change of the finite field F for the general commutative ring with unity gives the definition of cellular Schubert graph *J(K)* (see [23]). We use graphs *J(K[x_1, x_2,…., x_n]))* for the construction of trapdoor accelerators, which are surjective multivariate maps *F* of K^n onto $K^{n'}$ written in their standard form together with the piece of information *T* such that the knowledge of this information allows to compute the reimage for the given value of *F*.

The first cryptosystem based on such trapdoor accelerator where proposed in 2015 (see [31]), cryptanalysis for the system is still unknown. The obfuscations of these cryptosystems was suggested in [32]. They were seriously generalized in [23] where walks on general cellular Schubert graphs were used.

In this article we suggest a wide class of generalization of previously proposed trapdoor accelerators based on Jordan-Gauss graphs. The main idea is to use algebraic temporal graphs. Such graphs are given via the system of algebraic equations which depends on the time of the computation.

In the Section 2 we define cellular Schubert graphs. These Jordan-Gauss graphs will be used in the constructions of quadratic multivariate transformations of the affine spaces together with the corresponding trapdoor accelerators for the computation of reimages of these maps (se Section 4).

Section 3 is dedicated to constructions of trapdoor accelerators for the polynomial maps defined in terms of temporal linguistic graphs, i. e. special sequences of linguistic graphs. In general case the degree of constructed maps can be essentially higher than 2.

Section 5 presents some methods of constructions of new trapdoor accelerators in terms of known ones. In Section 6 we discuss the possible impact of proposed algorithms.

2. Schubert cellular graphs over the fields commutative ring

The missing definitions of graph-theoretical concepts which appear in this paper can be found in [17], [18] or [19]. All graphs we consider are simple graphs, i.e. undirected without loops and multiple edges. Let *V(G)* and *E(G)* denote the set of vertexes and the set of edges of *G* respectively. When it is convenient, we shall identify *G* with the corresponding anti-reflexive binary relation on *V(G)*, i.e. *E(G)* is a subset of *V(G)·V(G)* and write *v G u* for the adjacent vertexes *u* and *v* (or neighbours). We refer to *|{ x ϵ V(G)| xGv }|* as degree of the vertex *v*. The incidence structure is the set *V* with partition sets *P* (points) and *L* (lines) and symmetric binary relation *I* such that the incidence of two elements implies that one of them is a point and another one is a line. We shall identify *I* with the simple graph of this incidence relation or bipartite graph. The pair *x,y, xϵP, yϵL* such that *x I y* is called a *flag* of incidence structure *I*. Projective geometry ${}^{n-1}PG(F_q)$ of dimension *n-1* over the finite field F_q, where *q* is a prime power, is a totality of proper subspaces of the vector space $V=(F_q)^n$ of nonzero dimension.

This is the incidence system with type function *t(W)=dim(W), W ϵ* ${}^{n-1}PG(F_q)$ and incidence relation *I* defined by the condition W_1IW_2 if and only if one of these subspaces is embedded in another one. We can select standard base e_1, e_2,…, e_n of *V* and identify ${}^{n-1}PG(F_q)$ with the totality of linear codes in $(F_q)^n$.The geometry ${}^{n-1}\mathbb{T}(q)={}^{n-1}PG(F_q)$ is a partition of subsets ${}^{n-1}\mathbb{T}(q)_i$ consisting of elements of selected type i, $i=1,2, \ldots, n-1$. We assume that each element of V is presented in the chosen base as column vector $(x_1, x_1, \ldots , x_n)$. Let U stands for the unipotent subgroup of automorphism group $PGL_n(F_q)$ consisting of lower unitriangular matrices. 5

Let us consider orbits of the natural action of U on the projective geometry ${}^{n-1}PG(F_q)$. They are known as large Schubert cells. Each of orbits on the set $\Gamma_m(F_q)$ contains exactly one symplectic element spanned by elements $e_{i(1)}, e_{i(2)}, \ldots, e_{i(m)}$. So the number of orbits of $(U, \Gamma_m(F_q))$ equals to binomial coefficient $C^m{}_n$ (n,m). Noteworthy that the cardinality of ${}^{n-1}$ $\Gamma_m(F_q)$ is expressed by Gaussian binomial coefficient. Unipotent subgroup U is generated by elementary transvections $x_{i,j}(t)$, $i<j$, $t\epsilon F_q$. If we select i and j then elements of kind $x_{i,j}(t)$ form root subgroup $U_{i,j}$, corresponding to the positive root e_i-e_j of root system A_{n-1}.

Let J be a proper subset of $\{1, 2, \ldots, n\}=N$, ${}^JS$ be Schubert cell containing symplectic subspace W_J spanned by e_j ϵ J, $\Delta(J)= \{ (i,j) \mid i\epsilon J, j\epsilon N-J, i<j \}$. Then a subgroup $U(J)$ generated by root subgroups $U_{i,j}$, $(i, j) \epsilon$ $\Delta(J)$ of order q^k, $k= |\Delta(J)|$ acts regularly on ${}^JS$. It means that we can identify ${}^JS$ and $U(J)$.Noteworthy that each $\Gamma_m(F_q)$ has a unique largest Schubert cell of size q ${}^{m(n-m)}$, it is ${}^JS$ for $J=\{n, n-1, n-2, \ldots , n-m+1\}$. We denote this cell as ${}^mLS(q)$. We consider the bipartite graph ${}^{m,k}I_n(F_q)$ of the restriction of I onto disjoint union ${}^mLS(F_q)$ and ${}^kLS(F_q)$. It is bipartite graph with bidegrees q^r and q^s where $r=|\Delta(\{n, n-1, n-2, \ldots, n-m+1\})- \Delta(\{n, n-1, n-2, \ldots , n-m+1\}) \cap\Delta(\{n, n-1, n-2, \ldots , n-k+1\}) \mid$ and $s=|\Delta(\{n, n-1, n-2, \ldots , n-k+1\}) - \Delta(\{n, n-1, n-2, \ldots, n-m+1\})\cap \Delta(\{n, n-1, n-2, \ldots, n-k+1\})|$. We refer to the graph of binary relation ${}^{m,k}I_n(F_q)$ as Cellular Schubert graph and denote it as ${}^{m,k}CS_n(F_q)$ graph. In particular case $n=2m+1$, $k=m$ these graphs are known as Double Schubert graphs [33].

Let K be a commutative ring. We consider group $U=U_n(K)$ of lower unitriangular n times n matrices with the entries from K. Let Δ be the totality of all entries of (i, j), $1 \leq i<j \leq n$, i. e. totality of positive roots from A_{n-1}. We identify element M from $U_n(K)$ with the function $f: \Delta\longrightarrow K$ such that $f(i,j)=m_{i,j}$. The restriction $M|_D$ of M on subset D of Δ is simply $f|_D$. For each proper nonempty subset J of $\{1, 2, \ldots, n \}$ we define $U(J)$ as totality of matrices $M=(m_{i,j})$ from U such that (i, j) $\epsilon\{\Delta$-$\Delta(J)\}$ implies that $m_{i,j}=0$. We define incidence system ${}^{n-1}PG(K)$ as a totality of pairs (J, M), M $\epsilon U(J)$ with type function t(J, M)=|J| and incidence relation given by conditions $({}^1J, {}^1M)\, I\, ({}^2J, {}^2M)$ if and only if one of subsets ${}^1J$ and ${}^2J$ is embedded in another one and ${}^1M$-${}^2M) \mid \Delta({}^1J)\cap\Delta({}^2J) ={}^1M \cdot {}^2M$-${}^2M \cdot {}^1M$. We refer to this incidence system as *projective geometry scheme* over commutative ring K. If $K=F$ is the field then ${}^{n-1}PG(F)$ coincides with $n-1$-dimensional projective geometry over F, i. e. totality of proper nonzero subspaces of the vector space F^n(see [21] and further references) where the reader can find similar interpretations of Lie geometries and their Schubert cells, their generalisations via pairs of type (irreducible root system, commutative ring K). The concept of large and small Schubert cell in the classical case of field is presented in [34], [35].

We introduce $\Gamma_m(K)$, ${}^mLS(K)$ and graphs ^{m,k} $CS_n(K)$ for $m=1, 2, \ldots, n-1$ via simple substitution of K instead F_q.

We refer to disjoint union of ${}^mLS(K)$, $m=1, 2, \ldots, n-1$ with the restriction of incidence relation I and type function t on this set as Schubert geometry scheme of type A_{n-1} over commutative ring K. We refer to elements of this incidence system as linear codes of Schubert type. We can define Schubert schemes over other Dynkin-Coxeter diagrams.

3. Linguistic graphs of type (r, s, p) and symbolic computations

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

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

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

$$\ldots$$

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

where a_j and b_j, $j=1,2, \ldots, m$ are not zero divisors, and *fj* are multivariate polynomials with coefficients from K. Brackets and parenthesis allow us to distinguish points from lines (see [20], [21] and further references).

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

We refer to $\rho((x))=(x_1, x_2, \ldots, x_s)$ for $(x)=(x_1, x_2, \ldots, x_{s+m})$ and $\rho([y])=(y_1, y_2, \ldots, y_r)$ for $[y]=[y_1, y_2, \ldots , y_{r+m}]$ as the colour of the point and the colour of the line respectively.

For each $b\in K^r$ and $p=(p_1, p_2, \ldots, p_{s+m})$ there is the unique neighbour of the point $[l]=N_b(p)$ with the colour b. Similarly, for each $c \in K^s$ and line $l=[l_1, l_2, \ldots, l_{r+m}]$ there is the unique neighbour of the line $(p)= N_c([l])$ with the colour c. We refer to operator of taking the neighbour of vertex accordingly chosen colour as *neighbourhood operator.*

On the sets P and L of points and lines of linguistic graph we define jump operators ${}^1\mathcal{J}={}^1\mathcal{J}_b(p)=(b_1, b_2, \ldots, b_s, p_{1+s}, p_{2+s}, \ldots, p_{s+m})$, where $(b_1, b_2, \ldots, b_s)\in K^s$ and ${}^2\mathcal{J}={}^2\mathcal{J}_b([l])=[b_1, b_2, \ldots, b_r, l_{1+r}, l_{2+r}, \ldots, l_{r+m}]$, where $(b_1, b_2, \ldots, b_r)\in K^r$. We refer to tuple (s, r, m) as type of the linguistic graph I. If $(p_1, p_2, \ldots., p_{s+m})$ and $[l_1, l_2, \ldots, l_{r+m}]$ are point and line of some linguistic graph $I(K)$ of the type (s, r, m) over K then the values of jump operators do not depend on the choice of linguistic graph $I(K)$.

We refer to a linguistic graph $I_m(K)$ where K is a commutative ring with the unity as Jordan-Gauss graph if each monomial term of *fi*, $i=1, 2,\ldots., m$ is of kind ax_iy_j, $a\neq 0$.

Let $L_i=L(fi)$ be the list of nonzero monomial terms of *fi* with coefficients equals 1.

We refer to the triple (s, r, m) and lists L_i, $i=1, 2,\ldots,m$ as linguistic symbolic scheme $S =S(I_m(K))$ and say that linguistic graph $I_m(K)$ with parameters a_i, b_i, $i=1,2,\ldots.m$ and polynomials *fi*, $i=1,2,\ldots, m$ is the interpretation of S. Noteworthy that linguistic scheme does not depend on the commutative ring K. We refer to linguistic graphs ${}^1I_m(K)$ and ${}^2I_m(K')$ as symbolically equivalent if $S({}^1I_m(K)) =S({}^2I_m(K'))$.

Note that commutative rings K and K' can be different.

Let K be a subring of K'. We say that the interpretation of S has type (K', K) if point sets and line set are affine spaces over K' but coefficients a_i, b_i, $i=1,2,\dots.m$ are elements of the multiplicative group K^* and coefficients of the polynomials fi, $i=1,2,\dots, m$ are elements of K.

We will use the case when $K'=K[z_1, z_2, \dots, z_{m+s}]$ for arbitrary chosen K to define the map from K^{s+m} to itself.

Assume that graph $I_m(K)$ has parameters a_i , b_i and symbolic scheme S is defined by polynomials fi. Let $I_m(K[z_1, z_2, \dots, z_l])$ be the interpretation of S of type $(K[z_1,z_2,\dots, z_l], K)$ given by same parameters a_i, b_i and monomial terms of fi.

Algorithm 1 (construction of endomorphisms of $K[z_1, z_2,\dots, z_s, z_{s+1},z_{s+2},\dots, z_{s+m}]$ via the sequence of linguistic graphs of type (s, r, m)).

We select the linguistic graph $I_m(K)$ of type (s, r, m) with symbolic scheme S and graphs ${}^1I_m(K)$ of type (r, s, m), ${}^2I_m(K)$ of type (s, r, m),..., graph ${}^{2t+1}I_m$ of type r, s, m with the symbolic schemes ${}^iS$, $i=1, 2,\dots, 2t+1$.

We consider the graphs $I_m(K[z_1, z_2, \dots, z_{s+m}])$ together with
${}^jI_m(K[z_1, z_2,\dots, z_{m+s}])$, $j \ge 1$ and select the polynomial tuples
${}^0H=({}^0h_1(z_1, z_2,\dots, z_s), {}^0h_2(z_1, z_2, \dots, z_s), \dots, {}^0h_s(z_1, z_2, \dots, z_s))$,
${}^0G=({}^0g_1(z_1, z_2, \dots, z_s), {}^0g_2(z_1, z_2, \dots, z_s),\dots, {}^0g_r(z_1, z_2, \dots, z_s))$,
${}^1H=({}^1h_1(z_1, z_2,\dots, z_s), {}^1h_2(z_1, z_2, \dots, z_s), \dots, {}^1h_r(z_1, z_2, \dots, z_s))$,
${}^1G= ({}^1g_1(z_1, z_2, \dots, z_s), {}^1g_2(z_1, z_2, \dots, z_s),\dots, {}^1g_s(z_1, z_2, \dots, z_s))$,
${}^2H=({}^2h_1(z_1, z_2,\dots, z_s),{}^2h_2(z_1, z_2, \dots, z_s), \dots, {}^2h_s(z_1, z_2, \dots, z_s))$,
${}^2G= ({}^2g_1(z_1, z_2, \dots, z_s), {}^2g_2(z_1, z_2, \dots, z_s),\dots, {}^2g_r(z_1, z_2, \dots, z_s))$,
…,
${}^{2t+1}H=({}^2h_1(z_1, z_2,\dots, z_s),{}^2h_2(z_1, z_2, \dots, z_s), \dots, {}^2h_r(z_1, z_2, \dots, z_s))$,
${}^{2t+1}G= ({}^{2t}g_1(z_1, z_2, \dots, z_s), {}^{2t}g_2(z_1, z_2, \dots, z_s),\dots, {}^{2t}g_s(z_1, z_2, \dots, z_s))$,
$H=H^{2t+2}=(h_1(z_1, z_2,\dots, z_s), h_2(z_1, z_2, \dots, z_s), \dots, h_s(z_1, z_2, \dots, z_s))$.

Let N_b be the neighbourhood operator of $I_m(K[z_1, z_2,\dots, z_{m+s}])$ and ${}^jN_b$ be the neighbourhood operator of ${}^jI_m(K[z_1, z_2,\dots, z_{m+s}])$, $j=1, 2,\dots, 2t+1$.

Let us take a special point $(z_1, z_2 , \dots, z_s, z_{s+1}, z_{s+2},\dots, z_{m+s})=(z)$ and compute
${}^1J_{b(0)} ((z)) = {}^0(z)$ in the graph $I_m(K[z_1, z_2, \dots, z_{s+m}])$ with $b(0)= {}^0H$,
$N_{c(0)} ({}^0(z))= {}^0([u])$ in $I_m(K[z_1, z_2, \dots, z_{s+m}])$ with $c(0)= {}^0G$,
${}^1J_{b(1)} ({}^0([u]))={}^1([z])$ in the graph ${}^1I_m(K[z_1, z_2,\dots, z_{m+s}])$ with $b(1)= {}^1H$,
${}^1N_{c(1)} ({}^1([z]))= {}^1(u)$ in the graph ${}^1I_m(K[z_1, z_2,\dots, z_{m+s}])$ with $c(1)= {}^1G$,
${}^1J_{b(2)} ({}^1(u))={}^2(z)$ in the graph ${}^2I_m(K[z_1, z_2,\dots, z_{m+s}])$ with $b(2)= {}^2H$,
${}^2N_{c(2)} ({}^2(z))={}^2(u)$ in the graph ${}^2I_m(K[z_1, z_2,\dots, z_{m+s}])$ with $c(2)2= {}^2G$,
…..
${}^1J_{b(2t+1)} ({}^{2t}([u]))={}^{2t+1}([z])$ in the graph ${}^{2t+1}I_m(K[z_1, z_2,\dots, z_{m+s}])$ with $b(2t+1)= {}^{2t+1}H$,
${}^1N_{c(2t+1)} ({}^{2t+1}([z]))= {}^{2t+1}(u)$ in the graph ${}^{2t+1}I_m(K[z_1, z_2,\dots, z_{m+s}])$ with $c(2t+1)= {}^{2t+1}G$.

Finally we compute u as ${}^2J_b ({}^{2t+1}(u))$ with $b=H$.

Assume that $u=(h_1(z_1, z_2,\dots, z_s), h_2(z_1, z_2,\dots,z_s),\dots, h_s(z_1, z_2,\dots., z_s), g_{s+1}(z_1, z_2,\dots, z_s, z_{s+1}, z_{s+2},\dots, z_{s+m}), g_{s+2}(z_1, z_2,\dots, z_s, z_{s+1}, z_{s+2},\dots, z_{s+m}), \dots, g_{s+m}(z_1, z_2,\dots, z_s, z_{s+1}, z_{s+2},\dots, z_{s+m}))$.

We consider the polynomial map F of K^{s+m} to itself given by the following rule.
$z_1 \longrightarrow h_1(z_1, z_2,\dots, z_s)$,
$z_2 \longrightarrow h_2(z_1, z_2,\dots, z_s)$,
…,

$z_s \rightarrow h_s(z_1, z_2, \ldots., z_s)$,

$z_{s+1} \rightarrow g_{s+1}(z_1, z_2, \ldots, z_s, z_{s+1}, z_{s+2}, \ldots, z_{s+m})$,
$z_{s+2} \rightarrow g_{s+2}(z_1, z_2, \ldots, z_s, z_{s+1}, z_{s+2}, \ldots, z_{s+m})$,
…,
$z_{s+m} \rightarrow g_{s+m}(x_1, x_2, \ldots, x_s, x_{s+1}, x_{s+2}, \ldots, x_{s+m})$.

We refer to linguistic graphs ${}^1I_m(K)$ and ${}^2I_m(K)$ of types (s, r, m) and (r, s, m) as graphs of adjacent types. Let

$I^*_m(K)$ stands for the dual graph to $I_m(K)$ obtained via the replacement of partition sets P and L.

So graphs $I_m(K)$ and $I^*_m(K)$ are isomorphic graphs of adjacent types.

The transformation F is defined via the sequence of linguistic graphs of consecutively adjacent types $I_m(K)={}^0I_m(K), {}^1I_m(K), {}^2I_m(K), \ldots, {}^{2t+1}I_m(K)$ and listed above sequences of tuples ${}^iH$, $i=0, 1, \ldots, 2t+2$ and ${}^iG$, $i=0, 1, 2, \ldots, 2t+1$ with coordinates from $K[z_1, z_2, \ldots, z_s]$ of length s or r.

Proposition 1 [22] . Let $z_1 \rightarrow h_1(z_1, z_2, \ldots, z_s)$, $z_2 \rightarrow h_2(z_1, z_2, \ldots, z_s), \ldots, z_s \rightarrow h_s(z_1, z_2, \ldots., z_s)$ be a bijective map B from K^s onto K^s. Then transformation $F=F({}^0I_m(K), {}^jG, {}^iH)$, $j=0, 1, \ldots, 2m+1$, $i=0, 1, \ldots, 2m+2$ is a bijective map of K^{s+m} to itself.

Proposition 2 [22]. Let the conditions of the Proposition 1 holds and the polynomial map B has a trapdoor accelerator. Then the standard form G of L_1FL_2 where L_1 and L_2 are affine transformations from $AGL_n(K)$, $n=s+m$ has a trapdoor accelerator.

Proof. We justify the Proposition 2 via the construction of trapdoor accelerator for G.

Assume that condition of Proposition 1 holds. We assume that Alice and Bob share the standard form of G. Alice poses the trapdoor accelerator T of B and the knowledge on graphs $I_m(K)$ and tuples ${}^jG$ and ${}^iH$.

Alice will work with the intermediate vector $u = (u_1, u_2, \ldots, u_{s+m})$. She selects affine transformation L_1 from $AGL_{s+m}(K)$ of kind

$z_1 \rightarrow L_1(z_1, z_2, \ldots, z_{m+s}) = u_1$,
$z_2 \rightarrow L_2(z_1, z_2, \ldots, z_{m+s}) = u_2$,
…,
$z_{s+m} \rightarrow L_{s+m}(z_1, z_2, \ldots, z_{m+s}) = u_{m+s}$,

Alice computes $(w_1(z_1, z_2, \ldots., z_{m+s}), w_2(z_1, z_2, \ldots., z_{m+s}), \ldots, w_{m+s}(z_1, z_2, \ldots., z_{m+s})) = w$ via the substitution of written above expressions for u_i into $F(u_1, u_2, \ldots u_{m+s})$. She selects another affine transformation L_2 from $AGL_{m+s}(K)$ and compute $L_2(w)=(g_1(z_1, z_2, \ldots, z_{m+s}), g_2(z_1, z_2, \ldots, z_{m+s}), \ldots, g_{m+s}(z_1, z_2, \ldots, z_{m+s}))$. Alice announces publicly the standard form of the map G: $z_i \rightarrow g_i$, $i=1, 2, \ldots, m+s$.

The trapdoor accelerator T for G consists of graphs $I_m(K)$ *of type* (s, r, m) , linguistic graphs ${}^jI_m(K)$, tuples ${}^iH$, $i=0, 1, \ldots, 2t+2$ and ${}^iG$, $i=0, 1, \ldots, 2t+1$ with coordinates from $K[z_1, z_2, \ldots, z_s]$ and affine transformations L_i, $i=1, 2$.

Assume that Alice gets the value $c =(c_1 , c_2 , \ldots, c_{m+s})$ *of* $G(p_1 , p_2 , \ldots, p_{m+s})$. She computes $(L_2)^{-1}(c)={}^1c=({}^1c_1 , {}^1c_2 , \ldots, {}^1c_{m+s})$. Alice works with the equations

$h_1(u_1, u_2, \ldots, u_s)= {}^1c_1$,
$h_2(u_1, u_2, \ldots, u_s)= {}^2c_1$,
…,

$h_s(u_1, u_2,\ldots, u_s)= {}^s c_1$,

She is getting the solution $u_i=t_i$, $i=1, 2,\ldots,s$ *from* K^s. *Let* $(1_1, t_2, \ldots, t_s)=(t)$.

She computes tuples ${}^{2t+1}G(t_1, t_2,\ldots, t_s)=a(2t+1)$, $H^{2t+1}(t_1, t_2,\ldots, t_s)=b(2t+1)$, ${}^{2t}G(t_1, t_2,\ldots, t_s)=a(2t)$, $H^{2t}(t_1, t_2,\ldots, t_s)=b(2t)$, …, $G^0(t_1, t_2,\ldots, t_s)=a(0)$, $H^0(t_1, t_2,\ldots, t_s)=b(0)$.

Alice works with the sequence of graphs ${}^jI_m(K)$, $,j=2t+1, 2t,\ldots, 1, 0$.

She computes ${}^2\mathcal{J}_{a(2t+1)}(c\ )={}^{2t+1}c$ and treat it as vertex of the graph ${}^{2t+1}I_m(K)$ Then Alice computes the neighbours $N_{b(2t+1)}({}^{2t+1}c)={}^{2t+1}b$ of this vertex in ${}^{2t+1}I_m(K)$ and treat it as a vertex of graph ${}^{2t}I_m(K)$. *So,* she computes the ${}^2\mathcal{J}_{a(2t)}({}^{2t+1}b)={}^{2t}c$. Then Alice computes the neighbour $N_{b(2t)}({}^{2t}c)={}^{2t}b$ in the graph ${}^{2t}\ I_m(K)$. She continue this process.

Finally Alice gets $\mathcal{J}_{a(1)}({}^2b)={}^1c$ and $N_{b(1)}({}^1c)={}^1b$ together with $\mathcal{J}_{a(0)}({}^1b)={}^0c$ and $N_{b(0)}({}^0c)={}^0b$.

So she gets (u^*) as ${}^1\mathcal{J}_{(t)}({}^0b)=(t_1, t_2, \ldots, t_s, u_{s+1}, u_{s+2},\ldots, u_{s+m})$.

Alice computes the plaintext (p) *as* $(L_1)^{-1}(u^*)$.

Remark. We can substitute elements L_1 and L_2 by surjective affine map L'_1 of affine space $K^{n'}$ onto K^n, $n'>n$ and surjective map L'_2 of affine space K^m onto $K^{m'}$, $m\geq m'$ and get surjective map $L'_1\ F\ L'_2$ of affine space $\mathrm{K}^{n'}$ onto $\mathrm{K}^{m'}$.

1) Algorithm 2.

Let us assume that s>r. We select the linguistic graph $I_m(K)$ of type (s, r, m) with symbolic scheme S and graphs ${}^1I_m(K)$ of type (r, s, m), ${}^2I_m(K)$ of type $(s, r, m),\ldots$, graph ${}^{2t}I_m$ of type r, s, m with the symbolic schemes ${}^iS$, $i=1, 2,\ldots, 2t$. Similarly to algorithm 1 we consider the graphs $I_m(K[z_1, z_2, \ldots, z_{s+m}])$ together with

${}^jI_m(K[z_1, z_2,\ldots, z_{m+s}])$, $j \geq 1$ and select the polynomial tuples

${}^0H=({}^0h_1(z_1, z_2,\ldots, z_s), {}^0h_2(z_1, z_2, \ldots, z_s), \ldots, {}^0h_s(z_1, z_2, \ldots, z_s))$,

${}^0G=({}^0g_1(z_1, z_2, \ldots, z_s), {}^0g_2(z_1, z_2, \ldots, z_s),\ldots, {}^0g_r(z_1, z_2, \ldots, z_s))$,

${}^1H=({}^1h_1(z_1, z_2,\ldots, z_s), {}^1h_2(z_1, z_2, \ldots, z_s), \ldots, {}^1h_r(z_1, z_2, \ldots, z_s))$,

${}^1G= ({}^1g_1(z_1, z_2, \ldots, z_s), {}^1g_2(z_1, z_2, \ldots, z_s),\ldots, {}^1g_s(z_1, z_2, \ldots, z_s))$,

${}^2H=({}^2h_1(z_1, z_2,\ldots, z_s),{}^2h_2(z_1, z_2, \ldots, z_s), \ldots, {}^2h_s(z_1, z_2, \ldots, z_s))$,

${}^2G= ({}^2g_1(z_1, z_2, \ldots, z_s), {}^2g_2(z_1, z_2, \ldots, z_s),\ldots, {}^2g_r(z_1, z_2, \ldots, z_s))$,

…,

${}^{2t}H=({}^2h_1(z_1, z_2,\ldots, z_s),{}^2h_2(z_1, z_2, \ldots, z_s), \ldots, {}^2h_s(z_1, z_2, \ldots, z_s))$,

${}^{2t}G= ({}^{2t}g_1(z_1, z_2, \ldots, z_s), {}^{2t}g_2(z_1, z_2, \ldots, z_s),\ldots, {}^{2t}g_r(z_1, z_2, \ldots, z_s))$,

$H=H^{2t+1}=(h_1(z_1, z_2,\ldots, z_s), h_2(z_1, z_2, \ldots, z_s), \ldots, h_r(z_1, z_2, \ldots, z_s))$.

As in the algorithm 1 we take a special point $(z_1, z_2\ , \ldots, z_s, z_{s+1}, z_{s+2},\ldots, z_{m+s})=(z)$ and compute

${}^1\mathcal{J}_{b(0)}\ ((z))\ ={}^0(z)$ in the graph $I_m(K[z_1, z_2, \ldots, z_{s+m}])$ with $b(0)= {}^0H$,

$N_{c(0)}\ ({}^0(z))={}^0([u])$ in $I_m(K[z_1, z_2, \ldots, z_{s+m}])$ with $c(0)= {}^0G$,

${}^1\mathcal{J}_{b(1)}\ ({}^0([u]))={}^1([z])$ in the graph ${}^1I_m(K[z_1, z_2,\ldots, z_{m+s}])$ with $b(1)= {}^1H$,

${}^1N_{c(1)}\ ({}^1([z]))={}^1(u)$ in the graph ${}^1I_m(K[z_1, z_2,\ldots, z_{m+s}])$ with $c(1)= {}^1G$,

${}^1\mathcal{J}_{b(2)}\ ({}^1(u))={}^2(z)$ in the graph ${}^2I_m(K[z_1, z_2,\ldots, z_{m+s}])$ with $b(2)= {}^2H$,

${}^2N_{c(2)}\ ({}^2(z))={}^2(u)$ in the graph ${}^2I_m(K[z_1, z_2,\ldots, z_{m+s}])$ with $c(2)2= {}^2G$,

…..

${}^1\mathcal{J}_{b(2t)}\ ({}^{2t-1}([u]))={}^{2t}([z])$ in the graph ${}^{2t}I_m(K[z_1, z_2,\ldots, z_{m+s}])$ with $b(2t)= {}^{2t}H$,

${}^{1}N_{c(2t)}\ ({}^{2t}([z]))={}^{2t}(u)$ in the graph ${}^{2t}I_m(K[z_1, z_2,\dots, z_{m+s}])$ with $c(2t)={}^{2t}G$.

Finally we compute u as ${}^{2}\mathfrak{J}_b\ ({}^{2t}(u))$ with $b=H$.

Assume that $u=(h_1(z_1, z_2,\dots, z_s), h_2(z_1, z_2,\dots,z_s),\dots, h_r(z_1, z_2,\dots., z_s), g_{s+1}(z_1, z_2,\dots, z_s, z_{s+1}, z_{s+2},\dots, z_{s+m}), g_{s+2}(z_1, z_2,\dots, z_s, z_{s+1}, z_{s+2},\dots, z_{s+m}), \dots, g_{s+m}(z_1, z_2,\dots, z_s, z_{s+1}, z_{s+2},\dots, z_{s+m}))$.

We consider the polynomial map F of K^{s+m} to K^{r+m} itself given by the following rule

$(z_1, z_2,\dots, z_s, z_{s+1}, z_{s+2},\dots, z_{s+m})\longrightarrow(h_1(z_1, z_2,\dots, z_s), h_2(z_1, z_2,\dots, z_s),\dots, h_s(z_1, z_2,\dots., z_r), g_{s+1}(z_1, z_2,\dots, z_s, z_{s+1}, z_{s+2},\dots, z_{s+m}),$

$g_{s+2}(z_1, z_2,\dots, z_s, z_{s+1}, z_{s+2},\dots, z_{s+m}), \dots, g_{s+m}(x_1, x_2,\dots, x_s, x_{s+1}, x_{s+2},\dots, x_{s+m})$.

The transformation F is defined via the sequence of linguistic graphs

of consecutively adjacent types $I_m(K)={}^{0}I_m(K)$, ${}^{1}I_m(K)$, ${}^{2}I_m(K)$, $\dots,{}^{2t}I_m(K)$ and listed above sequences of tuples ${}^{i}H$, $i=0, 1, \dots, 2t+1$ and ${}^{i}G$, $i=0, 1, 2, \dots, 2t$ with coordinates from $K[z_1, z_2, \dots, z_s]$ of length s or r.

Proposition 3 [22]. Let $(z_1, z_2, \dots, z_s)\longrightarrow(h_1(z_1, z_2,\dots, z_s), h_2(z_1, z_2,\dots, z_s),\dots, h_r(z_1, z_2,\dots., z_s)$ be a surjective map B from K^s onto K^r. Then transformation $F=F({}^{j}I_m(K), {}^{j}G, {}^{i}H), j=0, 1, \dots, 2m+1, i=0, 1, \dots, 2m+2$ is a surjective map of K^{s+m} to K^{r+m} .

Proposition 4 [22]. Let the conditions of the Proposition 1.1 holds and the polynomial map B has a trapdoor accelerator.

Assume that L'_1 and L'_2 are surjective affine maps of affine space $K^{n'}$ onto K^n, $n'>n$ and affine space K^m onto $K^{m'}$, $m\geq m'$ *respectively . Then* polynomial surjective map $L'_1\, F\, L'_2$ of affine space $K^{n'}$ onto $K^{m'}$ also has a trapdoor accelerator.

Below we present a modification of Algorithm 1.

Let $I_m(K)$ be a linguistic graph of type (s, r, m). We

define its digraph cover $D(I_m(K))$ as the following directed graph.

The set of vertexes of $D(I_m(K))$ is subdivided into two blocks.

3The first one $PL_m(K)$ is the totality of ordered flags of kind $((p) , [l])$ of the incidence structure $I_m(K)$ where $(p)=(p_1, p_2,\dots, p_s, p_{s+1},\dots, p_{s+2},\dots, p_{s+m})$, $[l]=[l_1, l_2,\dots, l_r, l_{r+1}, l_{r+2},\dots, l_{r+m}]$ such that $(p)I[l]$ and the totality

$LP_m\ (K)$ of ordered flags of kind $[[l], p]$ and binary relation ψ which is defined via the conditions

$((p), [l])\psi[[l'], (p')]$ *if* $[l]=[l']$ and $(p)\neq(p'), [[l],(p)]\psi((p'), [l]))$ if

$(p)=(p'), [l] \neq[l']$.

We refer to pair of tuples $<(p_1, p_2,\dots, p_s), [l_1, l_2, \dots, l_r]>$ *of* $((p), [l])$ from $PL_m(K)$ as the colour of the flag. We say that $(p_1,p_2,\dots,p_s)$ and $[l_1,l_2,\dots,l_s]$ are internal and external colours of the flag $((p), [l])$. The information on the flag can be given by the tuple $(p_1, p_2, \dots, p_s, p_{s+1}, p_{s+2},\dots, p_{s+m}, l_1, l_2, \dots, l_r)$. Dual presentation of $((p), [l])$ is $(p_1, p_2,\dots, p_s, l_1, l_{r+2},\dots, l_{r+m}, l_1, l_2,\dots, l_r)^*$ given via the coordinates of line.

Similarly we say that $[l_1, l_2,\dots,l_r]$ and $(p_1,p_2,\dots,p_s)$ are internal and external colours of $[[l],(p)]$. The information on this flag can be given by the tuple $[l_1,l_2,\dots, l_r, l_{r+1}, l_{r+2},\dots, l_{r+m}, p_1, p_2,\dots, p_s]$ or dual presentation $[l_1,l_2,\dots, l_r, p_{s+1}, p_{s+2},\dots, p_{s+m}, p_1, p_2,\dots, p_s]^*$.

We introduce operator of change the colour ${}^1\mathcal{J}C_a$, $a=(p'_1, p'_2,..., p'_s, l'_1, l'_2,..., l'_r)$ $[(p), [l])]= (p_1', p'_2, ..., p'_s, p_{s+1}, p_{s+2},..., p_{s+m}, l'_1, l'_2,..., l'_r)$ acting on $PL_m(K)$ and operator ${}^2\mathcal{J}C_a$, $a=(l_1', l'_2,...., l'_r, p'_1, p'_2,..., p'_s)$, ${}^2\mathcal{J}C_a([[l],(p)])$ $[l'_1, l'_2,..., l'_r, l_{r+1} ,l_{r+2}, ..., l_{r+m}, p'_1, p'_2 ,...p'_s]$ acting on the set $LP_m(K)$.

Algorithm 3.

Alice takes the sequence of graphs $D(I_m(K))$, $D({}^lI_m(K))$, $l=1,2,...,t$. She will work with the multivariate ring $K'=K[z_1, z_2,..., z_s, z_{s+1}, z_{s+2},..., z_{s+m}, z_{1s+m+1}, z_{s+m+2}, ..., z_{s+m+r}]$ and graphs $D(I_m(K')),D({}^lI_m (K'))$.

Alice selects the tuple ${}^0H=(h_1, h_2,..., h_s, g_1, g_2,..., g_r)$, $H'=(h'_1, h'_2,..., h'_s, g'_1, g'_2,..., g'_r)$ and ${}^iH=({}^ih_1, {}^ih_2,..., {}^ih_s, {}^ig_1, {}^ig_2,..., {}^ig_r)$ from $(K')^{s+r}$. She takes the flag $(z)=(z_1, z_2,..., z_s, z_{s+1}, z_{s+2},..., z_{s+m}, z_{s+m+1}, z_{s+m+2}, ..., z_{s+m+r})$ of $I_m(K')$.

Assume that for $((p),[l])$ from ${}^j PL(I_m(K'))$, $j=1.2,...,t-1$ symbol $((p),[l])^*$

means $([l], (p))$ from ${}^{j+1}PL(I_m(K'))$. If $((p),[l])$ is a flag from ${}^tPL(I_m(K'))$ then $((p),[l])^*$ is $([l], (p))$ from ${}^{t-1}PL(I_m(K'))$.

Alice uses operator ${}^1\mathcal{J}_a$, $a= {}^0H$ and computes ${}^1z ={}^1\mathcal{J}_a(z)=(h_1, h_2,..., h_s, z_{s+1}, z_{s+2},..., z_{s+m}, g_1, g_2,... g_r)$ in the graph $D(I_m(K))$. She computes $({}^1u)=({}^1z)^*= [g_1, g_2,... g_r, z'_{s+1}, z'_{s+2},..., z_{s'+m}, h_1, h_2,..., h_s]$ of the graph ${}^1I_m (K')$ where $[g_1, g_2,... g_r, z'_{s+1}, z'_{s+2},..., z_{s'+m}]$ is the neighbour of $(h_1, h_2,..., h_s, z_{s+1},) z_{s+2},..., z_{s+m})$ in $I_m(K')$.

2Next Alice uses ${}^1\mathcal{J}_{a(1)}$, $a(1)= {}^1H$ and computes ${}^1\mathcal{J}_{a(1)}({}^1u)= {}^2z$ in the graph ${}^1I_m (K')$ and $({}^2u)=({}^2z)^*$ from ${}^2I_m (K')$.

She continue this procedure and constructs $({}^iu)$, $i=3.4,..., t$. Alice takes $({}^tu)$ from ${}^tI_m (K')$

and uses ${}^2\mathcal{J}_b$, $b= H'$ for the computation of $u={}^1\mathcal{J}({}^tu)$ of kind $(h'_1, h'_2,..., h'_s, v_1, v_2, ..., v_m, g'_1, g'_2,..., g'_r)$ or $(g'_1, g'_2,..., g'_r, v_1, v_2, ..., v_m, h'_1, h'_2, ..., h'_s)$ dependently on $t \mod 2$.

She uses the following map $G= G=G({}^jI_m(K), {}^iH, H')$, $i=0,1,...,t$ as the output of the algorithm.

$z_1 \longrightarrow h'_1(z_1, z_2,..., z_s, z_{s+m+1}, z_{s+m+2}, ..., z_{s+m+r})$,

$z_2 \longrightarrow h'_2(z_1, z_2,..., z_s, z_{s+m+1}, z_{s+m+2}, ..., z_{s+m+r})$,

…

$z_s \longrightarrow h'_s(z_1, z_2,..., z_s, z_{s+m+1}, z_{s+m+2}, ..., z_{s+m+r})$,

$z_{s+1} \longrightarrow v_1(z_1, z_2,..., z_s, z_{s+1}, z_{s+2},..., z_{s+m}, z_{s+m+1}, z_{s+m+2}, ..., z_{s+m+r})$,

$z_{s+2} \longrightarrow v_2(z_1, z_2,..., z_s, z_{s+1}, z_{s+2},..., z_{s+m}, z_{s+m+1}, z_{s+m+2}, ..., z_{s+m+r})$,

…,

$z_{s+m} \longrightarrow v_m(z_1, z_2,..., z_s, z_{s+1}, z_{s+2},..., z_{s+m}, z_{s+m+1}, z_{s+m+2}, ..., z_{s+m+r})$,

$z_{1+s+m} \longrightarrow g'_1(z_1, z_2,..., z_s z_{s+m+1}, z_{s+m+2}, ..., z_{s+m+r})$,

$z_{2+s+m} \longrightarrow g'_2(z_1, z_2,..., z_s, z_{s+m+1}, z_{s+m+2}, ..., z_{s+m+r})$,

…

$z_{r+s+m} \longrightarrow g'_r(z_1, z_2,..., z_s,, z_{s+m+1}, z_{s+m+2}, ..., z_{s+m+r})$.

Proposition 5 [22]. Let $z_1 \longrightarrow h'_1(z_1, z_2,..., z_s z_{s+m+1}, z_{s+m+2}, ..., z_{s+m+r})$, $z_2 \longrightarrow h'_2(z_1, z_2,..., z_s , z_{s+m+1}, z_{s+m+2}, ..., z_{s+m+r})$,..., $z_s \longrightarrow h'_{s,}(z_1, z_2mz_{s,} z_{s+m+1}, z_{s+m+2}, ..., z_{s+m+r})$, $z_{1+s+m} \longrightarrow g'_1(z_1, z_2,..., z_s z_{s+m+1}, z_{s+m+2}, ..., z_{s+m+r})$, $z_{2+s+m} \longrightarrow g'_2(z_1, z_2,..., z_s z_{s+m+1}, z_{s+m+2}, ..., z_{s+m+r}), ...,)$, $z_{r+s+m} \longrightarrow g'_r(z_1, z_2,..., z_s , z_{s+m+1}, z_{s+m+2}, ..., z_{s+m+r})$

be a bijective map B from K^{s+r} onto K^{s+r}. Then transformation $G=G({}^jI_m(K), {}^iH, H')$, $j=0, 1, ..., t$ is a bijective map of K^{s+r+m} to itself.

Proposition 6 [22]. Let the conditions of the Proposition 3 holds and the polynomial map B has a trapdoor accelerator. Then the standard form F of L_1GL_2 where L_1 and L_2 are affine transformations from $AGL_n(K)$, $n=s+r+m$ has a trapdoor accelerator.

The justification of this statement can be obtained via the modification of the procedure in the proof of Proposition 2.

4. On the examples of Schubert cellular graphs, their symplectic quotients and cryptographic algorithms

Let us consider graphs ${}^{m,m-1}CS_{m+k-1}(F)$ over the field F which are induced subgraphs of projective geometry $PG_{m+k-1}(F)$ with vertices from the largest Schubert cells on the totalities of m=dimensional and $m-1$ dimensional subspaces of the vector space F^{m+k}. They can be defined as totalities of points $(x)=(x_1, x_2,\dots,x_k, x_{1,1}, x_{1,2},\dots,x_{k,m-1})$ and lines $[y]=[y_1, y_2,\dots,y_{m-1}, x_{1,1}, x_{1,2},\dots,x_{k,m-1}]$ from $F^{k(m-1)+k}$and $F^{k(m-1)+m-1}$ where indexes of coordinates of kind i,j for ` $i=1,2,\dots,k$ and $j=1,2,\dots, m-1$ are 1ordered lexicographically and the point (x) is incident to the line $[y]$ if and only if the conditions for each pair i,j.

Thesymbolic type S of this graph is the triple $(k, m-1, k(m-1))$ and the list of $L_{i,j}=\{x_i\ y_j\}$ ordered lexicographically. Let K be commutative ring with the unity then graph ${}^{m,m-1}CS_{m+k-1}(K)$ is defined via the change of F for K.

Let $I_{k(m-1)}(K)$ be the Jordan-Gauss graph over K symbolically equivalent to ${}^{m,m-1}CS_{m+k-1}(K)$ then corresponding equations are $a_{i,j}x_{i,j}- b_{ij}y_{i,j}= c_{i,j}x_iy_j$ where $a_{i,j}$ and b_{ij} are elements of multiplicative group K^* and $c_{i,j}$ are elements from $K-\{0\}$.

We can see that arbitrary nonempty subset M of $\{(11),(1,2),\dots, (m-1, m-1)\}$ is define the symplectic quotient I_M of $I_{k(m-1)}(K)$.

Other special case of cellular Schubert graph is ${}^{m,1}CS_m(F)$ of type $(m-1, m-1, 1)$ when we have points and lines of kind $(x_1, x_2,\dots, x_m)$ and $[y_1, y_2, \dots, y_m]$ and equation $x_m-y_m=x_1y_1 +x_2y_2+\dots +x_{m-1}y_{m-1}$. Symbolically equivalent to ${}^{m,1}CS_m(F)$ will be Jordan-Gauss graph of type $(m-1, m-1, 1)$ with the incidence given by an equation of kind $ax_m-by_m=c_1x_1y_1 +c_2x_2y_2+\dots+c_{m-1}x_{m-1}y_{m-1}$ with a and b from the multiplicative group K^* and c_i from $K-\{0\}$.

Let us consider special homomorphisms of linguistic graphs and corresponding semigroups. Let $I(K)$ be linguistic graph over commutative ring K defined in section and $M = \{m(1), m(2),\dots, m(d)\}$ be a subset of $\{1, 2, \dots, m\}$ (set of indexes for equations). Assume that equations indexed by elements from M of the following kind

$a_{m(1)+s}\,x_{m(1)} - b_{m(1)}y_{m(1)+r}=f_{m(1)}(x_1, x_2 , \dots, x_s ,y_1, y_2, \dots , y_r)$

$a_{m(2)}x_{m(2)+s} - b_{m(2)}y_{m(2)+r}= f_{m(2)}(x_1, x_2, \dots ,x_s,x_{m(1)+s},y_1, y_2, \dots , y_{r,}, y_{m(1)+r})$
)…
$a_{m(d)}x_{m(d)+s} - b_{m(d)}y_{m(d)+r} =f_{m(d)} (x_1, x_2, \dots , x_{s,,} ,x_{m(1)+s}, x_{m(2)+s,\dots}, x_{m (d-1)+s,} y_1, y_2, \dots , y_{r,,} y_{m(1)+r}, y_{m(2)+r},\dots, y_{m (d-1)+r})$
define other linguistic incidence structure $I_{M.}$.

Then the natural projections $\delta_{1,}: (x)\longrightarrow(x_1, x_2, \dots , x_{s,,} x_{m(1)+s}, x_{m(2)+s,\dots}, x_{m(d)+s})$ and $\delta_2: [y]\longrightarrow[y_1, y_2, \dots , y_{r,}\ y_{m(1)+r},y_{m(2)+r,\dots}, y_{m(d)+r}]$ of free modules define the natural homomorphism δ of incidence structure I onto $I'=I_{M.}$. We will use the same symbol ρ for the colouring of linguistic graph $I_{M..}$

It is clear, that δ is colour preserving homomorphism of incidence structures (bipartite graphs). We refer to δ as symplectic homomorphism and graph I_M as symplectic quotient of linguistic graph I. In the case of linguistic graphs defined by infinite number of equations we may consider symplectic quotients defined by infinite subset M (see [22] where symplectic homomorphism was used for the cryptosystem construction).

As it follows from the definition the symplectic quotient of Jordan-Gauss graph is also Jordan-Gauss graph.

For each linguistic graph I and $M=\{1, 2,\dots,d\}$, $d<m$ there is the symplectic quotient I_M.

Let us consider graphs ${}^{m,m-1}CS_{m+k-1}(F)$ over the field F which are induced subgraphs of projective geometry $PG_{m+k-1}(F)$ with vertices from the largest Schubert cells on the totalities of m=dimensional and $m-1$ dimensional subspaces of the vector space F^{m+k}. They can be defined as totalities of points $(x)=(x_1, x_2,\dots,x_k, x_{1,1}, x_{1,2},\dots,x_{k,m-1})$ and lines $[y]=[y_1, y_2,\dots,y_{m-1}, x_{1,1}, x_{1,2},\dots,x_{k,m-1}]$ from $F^{k(m-1)+k}$and $F^{k(m-1)+m-1}$ where indexes of coordinates of kind i,j for ` $i=1,2,\dots,k$ and $j=1,2,\dots, m-1$ are 1ordered lexicographically and the point (x) is incident to the line $[y]$ if and only if the conditions for each pair i,j. The symbolic type S of this graph is the triple $(k, m-1, k(m-1))$ and the list of $L_{i,j}=\{x_i\ y_j\}$ ordered lexicographically. Let K be commutative ring with the unity then graph ${}^{m,m-1}CS_{m+k-1}(K)$ is defined via the change of F for K.

Let $I_{k(m-1)}(K)$ be the Jordan-Gauss graph over K symbolically equivalent to ${}^{m,m-1}CS_{m+k-1}(K)$ then corresponding equations are $a_{i,j}x_{i,j}- b_{ij}y_{i,j}= c_{i,j}x_iy_j$ where $a_{i,j}$ and b_{ij} are elements of multiplicative group K^* and $c_{i,j}$ are elements from $K-\{0\}$.

We can see that arbitrary nonempty subset M of $\{(11),(1,2),\dots, (m-1, m-1)\}$ is define the symplectic quotient I_M of $I_{k(m-1)}(K)$.

Let us consider trapdoor accelerators defined in terms of cellular Schubert graphs.

We introduce the degree of the tuple from $K[z_1, z_2, \dots., z_p]$, $p>1$ as maximal degree of its coordinates as multivariate polynomials.

Proposition 7 [22]. Let the condition of Proposition 1 holds, graph ${}^jI_m(K)$, $j=0,1, \dots, 2t +1$ are symbolically equivalent to ${}^{l,k}CS_n(K)$ or its dual graph and $deg({}^jH)+deg({}^jG)\leq 2$, $j=1,2,\dots, 2t+1$, $deg(H)=2$. Then transformation $G=F({}^j\mathbf{I_m}(K)^j, {}^jG, {}^iH)$, $j=0, 1, \dots, 2t+1$, $i=0, 1, \dots, 2m+2$ is a bijective quadratic map of $K^{\mathbf{s+m}}$ to itself.

So under the conditions of Proposition 7 the construction of Proposition 2 is a bijective quadratic transformations with the trapdoor accelerator.

Proposition 8 [22]. Let the condition of Proposition 3 holds, graph ${}^jI_m(K)$, $j=0,1, \dots, 2t$ are symbolically equivalent to ${}^{l,k}CS_n(K)$ or its dual graph and $deg({}^jH)+deg({}^jG)\leq 2$, $j=1,2,\dots, 2t$, $deg(H')=2$. Then transformation $G=F({}^j\mathbf{I_m}(K), {}^jG, {}^iH)$, $j=0, 1, \dots, 2t$, $i=0, 1, \dots, 2m+1$ is a surjective quadratic map of $K^{\mathbf{s+m}}$ to $K^{\mathbf{r+m}}$ itself.

So under the conditions of Proposition 8 the construction of Proposition 4 is a surjective quadratic transformations with the trapdoor accelerator.

Proposition 9 [22]. Let the condition of Proposition 7 holds, graph ${}^jI_m(K)$, $j=0,1, \dots, t$ are symbolically equivalent to ${}^{l,k}CS_n(K)$ or its dual graph and $deg({}^jh_1, {}^jh_2, ,,,, {}^jh_s)+deg({}^jg_1, {}^jg_2, ,,,, {}^jg_r)\leq 2$, $j=0,1,2,\dots, t$, and $deg\ (H')=2$. Then the transformation $G=G({}^j\mathbf{I_m}(K)^j, {}^iH, H')$, $j=0, 1, \dots, t$ is a bijective quadratic map of $K^{\mathbf{s+r+m}}$ to itself.

So under the conditions of Proposition 9 the construction of Proposition 6 is a bijective quadratic transformations with the trapdoor accelerator.

Remark. We can substitute graphs ${}^jI_m(K)$ of the propositions 7, 8 and 9 for the nontrivial symplectic quotients of these Jordan-Gauss graphs.

5. On the extensions of known trapdoor accelerators

Let us discuss Algorithm 1 in the case when the conditions of Proposition 2 and Proposition 7 hold. So graph $^{j}I_m(K)$, $j=0,1, \ldots, 2t+1$ are symbolically equivalent to $^{l,k}CS_n(K)$ or its dual graph and $deg(^{j}H)+deg(^{j}G)\leq 2$, $j=1,2,\ldots, 2t+1$, and $deg(H)=2$ and the transformation B has a trapdoor accelerator T. We suggest the following two options for the construction of the pair (B, T).

1.We take the triangular transformation $Q{:}x_1\longrightarrow a_1x_1+b_1$, $x_2\longrightarrow a_2x_2+f_2(x_1)$, $x_3\longrightarrow a_3x_3+f_3(x_1, x_2),\ldots,$ $x_s\longrightarrow a_sx_s+f_s(x_1, x_2,\ldots,x_{s-1})$ where a_i, $i=1, 2,\ldots, s$ are elements from K^* and $deg\ fi=2$, $i=2,3,\ldots,s$ together with two elements D_{1wn} and D_2 from $AGL_s(K)$ and define B as D_1QD_2.

So the standard form of B and the decomposition of B into D_1QD_2 will be used as a trapdoor accelerator.

2. In [1] authors constructed multivariate quadratic cryptosystem based on Jordan-Gauss graphs $D(s, K)$, $s>4$ of type $(1, 1, s)$. Corresponding trapdoor accelerator is a standard form of automorphism of $K[z_1, z_2,\ldots, z_s]$ and trapdoor accelerator which provides1 the knowledge on the graph $D(s,K)$ and the tuple of ring elements of length $O(n^2)$. We may assume that the knowledge on the graph is publicly known.

3. We can use the procedure of Algorithm 1 under the conditions of Proposition 2 and Proposition 7 in the case of graph $^{s,k}CS_s$, $k<s$ for the construction of B. Alice can select the tuples ^{0}H, ^{0}G, ^{1}H, $^{1}G,\ldots,$ ^{2t+1}H, ^{2t+1}G and can choose ^{2t+1}H which defines the transformation from $AGL_{k-s}(K)$. This way she obtains the quadric bijective transformation F and construct B as the map D_1FD_2, D_1, $D_2 \epsilon AGL_s(K)$ on the affine space K^s.

In the case of finite fields of characteristic 2 Alice can use quadratic automorphism of $F_q[z_1, z_2,\ldots, z_s]$ from Matsumoto-Imai Cryptosystem. In the case of general finite field F_q she can use bijective encryption map of Oil and Vinegar public key or use other transformations with the trapdoor accelerators from known suggested multivariate schemes.

Remark. The simplest choice of linear transformation B is not appropriate for the construction of multivariate public key. Accordingly [22] the choice of B as the element from $AGL_s(K)$ insures the fact that the inverse map for F is also quadratic transformation. So the linearization attack will allow to construct inverse transformation in a polynomial time.

Example 1.

Let us assume that the graph $I_m(K)$ of the Algorithm 1 is $^{r,r-1}CS_{k+r-1}$ and the conditions of Proposition 7 hold.

The type of this Jordan-Gauss graph is $(k, r-1, m)$ where $m=k(r-1)$. Let us assume that $k=O(n)$ and $r=O(n)$. So $m=O(n^2)$,

The interpretation of each graph from the sequence requires $2k(r-1)$ elements of K^* and $(r-1)$ elements from K-$\{0\}$.

So Alice has to select the parameter t and form the tuple from $(K^*)^{2(2t+2)k(r-1)}$ and the tuple from $(K\text{-}\{0\})^{(2t+2)k(r-1)}$.

Let us assume A that $k\geq r-1$. She has to form the colours of the point and line as the tuples of length k and $r-1$ with coordinates from $K[z_1, z_2,\ldots, z_k]$ of degree 2, 1 and 0. In the entscase of the colour of the point of degree 2 Alice has to choose $((k(k-1)/2+k+1)k$ coefficients from K. Roughly the number of parameters is $(1/2)k^3$. In the case of degree 1 or 0 the numbers will be $(k+1)k$ and k respectively.

In the case of line we get $(k(k-1)/2+k+1)(r-1)$, $(k+1)(r-1)$ and r. Assume that the parameter t has size $O(n)$.

The construction of the chain ${}^0H$, ${}^0G$, ${}^1H$, ${}^1G$,... requires $O)(n^4)$ parameters. The trapdoor accelerator T can be thought as the sequence of $O(n^4)$ elements of the commutative ring. Alice has to keep it safely as her private key.

Recall that the dimension of the space of plaintexts is $d=k+k(r-1)$. It means that the trapdoor accelerator is a tuple of length $O(d^2)$.

The symbolic type of the graph can be given publicly.

The cost of the computation of the neighbor of vertex in the graph is $O(d)$. The computation of the walk with jumps of length $O(n)$ costs $O(d^{3/2})$ and application of the element from $AGL_d(K)$ costs $O(d^2)$.

Thus the complexity of private decryption procedure is $O(d^2)$.

The obfuscation of the algorithm.

a) Let us take permutations ${}^0\pi$, ${}^1\pi$, ${}^2\pi$, , ..., ${}^2\pi$ on the set $\{1, 2,\dots,k\}$ and ${}^0\mu$, ${}^1\mu$, ${}^2\mu$, ..., ${}^{2t+1}\mu$ on the set $\{1, 2,\dots, m-1\}$ and change the incidence equations of ${}^lI_m(K)$, $l=1, 2, \dots, 2t+1$for ${}^la_{i,j}x_{i,j}$ $-{}^lb_{i,j}y_{i,j} = {}^lc_{i,j}x_{i'}\, y_{j'}$ where $`i={}^1\pi(i)$, $j'={}^l\mu(j)$ and get the new graphs ${}^lI'_m(K)$.

It is easy to see that graphs ${}^lI'_m(K)$ *and* ${}^lI_m(K)$ have different symbolic type but they are isomorphic incidence structures.

We can change graphs ${}^lI_m(K)$ for ${}^{l'}I_m(K)$ and construct the new quadratic transformation F' with the trapdoor accelerator.

b) We can select a nontrivial subset M of the Cartesian product of $\{1, 2,\dots,k\}$ and $\{1,2\dots,m-1\}$ and consider a symplectic quotient $I_M(K)$ instead of $I_m(K)$ in the Proposition 5 The degree of a new transformation F' will be the same. The information on the choice of a subset M can be treated as part of the trapdoor accelerator. So the graph $I_M(K)$ will be unknown to public.

Example 2.

Let us assume that the graph $I_m(K)$ of the Algorithm 2 is ${}^{r,r-1}CS_{k+r-1}$ and the conditions of Proposition 6 hold. We assume that $k \geq r-1$.

In this case Alice also has a wide choice of options to create appropriate transformation $B`$ from K^s to K^r.

For instance she can use bijective transformations B on K^s in the presented above schemes 1 and 2. Alice takes affine map D from $AGL_s(K)$ and surjective affine map D_3 from K^s onto K^r and forms $B'=BD_3$.

In the case of finite fields $K=F_q$ we can use for the construction of B recently developed scheme TUOV.

In the case of the field of characteristic *2* Alice can use B of kind $(z_1, z_2,\dots, z_k)\rightarrow(l_1(z_1, z_2,\dots, z_k)^2+b_1, l_2(z_1, z_2,\dots, z_k)^2+b_2,\dots, l_{r-1}(z_1, z_2,\dots, z_k)^2+b_{r-1})$ where $(z_1, z_2,\dots, z_k)\rightarrow(l_1(z_1, z_2,\dots, z_k), l_2(z_1, z_2,\dots, z_k),\dots, l_{r-1}(z_1, z_2,\dots, z_k))$ is a linear map of rank $r-1$.

She can use $(z_1, z_2,\dots, z_k)\rightarrow(l_1(z_1^2, z_2^2,\dots, z_k^2)+b_1, l_2(z_1^2, z_2^2,\dots, z_k^2) +b_2,\dots, l_{r-1}(z_1^2, z_2^2,\dots, z_k^2)+b_{r-1})$ alternatively.

Alice will use the same graph $I_m(K)={}^{r,\,r-1}CS_{k+r-1}$ of the Algorithm 1 but under the conditions of Proposition 6.

She will select that $k=O(n)$ and $r=O(n)$. *So* $m=O(n^2)$. Recall that the interpretation, of each graph from the sequence requires $2k(r-1)$ elements of K^* and $k(r-1)$ elements from K-$\{0\}$.

Alice selects symbolically equivalent to ${}^{r,\,r-1}CS_{k+r-1}$ graphs ${}^jI_m(K)$, $m=k(r-1)$, $j=0,1, \dots, 2t$ and symbolic colours

${}^0H=({}^0h_1(z_1, z_2,\dots, z_k), {}^0h_2(z_1, z_2, \dots, z_k), \dots, {}^0h_s(z_1, z_2, \dots, z_k))$, ${}^0G=({}^0g_1(z_1, z_2, \dots, z_k), {}^0g_2(z_1, z_2, \dots, z_k),\dots, {}^0g_{r-1}(z_1, z_2, \dots, z_k))$,

${}^1H=({}^1h_1(z_1, z_2,\dots, z_k), {}^1h_2(z_1, z_2, \dots, z_k), \dots, {}^1h_{r-1}(z_1, z_2, \dots, z_k))$, ${}^1G= ({}^1g_1(z_1, z_2, \dots, z_k), {}^1g_2(z_1, z_2, \dots, z_k),\dots, {}^1g_k(z_1, z_2, \dots, z_k))$,

${}^2H=({}^2h_1(z_1, z_2,\dots, z_k),{}^2h_2(z_1, z_2, \dots, z_k), \dots, {}^2h_k(z_1, z_2, \dots, z_k))$,${}^2G= ({}^2g_1(z_1, z_2, \dots, z_k), {}^2g_2(z_1, z_2, \dots, z_k),\dots, {}^2g_{r-1}(z_1, z_2, \dots, z_k))$,

…,

${}^{2t}H=({}^2h_1(z_1, z_2,\dots, z_k),{}^2h_2(z_1, z_2, \dots, z_k), \dots, {}^2h_k(z_1, z_2, \dots, z_k))$,${}^{2t}G= ({}^{2t}g_1(z_1, z_2, \dots, z_k), {}^{2t}g_2(z_1, z_2, \dots, z_k),\dots, {}^{2t}g_{r-1}(z_1, z_2, \dots, z_k))$,

Alice chooses the tuple $H==(h_1(z_1, z_2,\dots, z_k),h_2(z_1, z_2, \dots, z_k), \dots, h_{r-1}(z_1, z_2, \dots, z_k))$. Recall that $B(z)=H$.

She follows to Algorithm 2 and creates the polynomial map F of K^{s+m} to K^{r+m-1} itself given by the following rule

$(z_1, z_2,\dots, z_k, z_{k+1}, z_{k+2},\dots, z_{k+m})\longrightarrow(h_1(z_1, z_2,\dots, z_k), h_2(z_1, z_2,\dots, z_k),\dots, h_{r-1}(z_1, z_2,\dots., z_k), g_r(z_1, z_2,\dots, z_k, z_{k+1}, z_{k+2},\dots, z_{k+m}),$
$g_{r+1}(z_1, z_2,\dots, z_k, z_{k+1}, z_{k+2},\dots, z_{k+m}), \dots, g_{r+m-1}(x_1, x_2,\dots, x_k, x_{s+1}, x_{s+2},\dots, x_{k+m}))$.

Alice forms L'_1 and L'_2 of the Proposition 2.1 which are surjective affine maps of affine space $K^{n'}$ onto K^n, $n'>n=k+m$ and the affine space K^{m+r-1} onto $K^{m'}$, $m+r-1\geq m'$ respectively. Then she computes the standard form G of polynomial surjective map $L'_1 F L'_2$ of affine space $K^{n'}$ onto $K^{m'}$ and sends it to Bob.

Assume that Alice and Bob gets the hash value $(c_1, c_2, \dots., c_{m'})$.

Alice creates the intermediate tuple of variables $u=(u_1, u_2,\dots u_{r-1}, u_r, u_{r+1}, \dots, u_{r+m-1})$ and writes the system of linear equations $L'_2\,(u)=c$. So she gets the solution ${}^*u=({}^*u_1, {}^*u_2,\dots, {}^*u_{r-1} , {}^*u_r, {}^*u_{r+1}, \dots, {}^*u_{r+m-1})$ and considers the quadratic equations $B(z_1, z_2,\dots, z_k)={}^*u =({}^*u_1, {}^*u_2,\dots, {}^*u_{r-1})$. The knowledge on the trapdoor accelerator of B allows Alice to get a solution $z^*=({}^*z_1, {}^*z_2,\dots, {}^*z_k)$.

So Alice computes ${}^{2t}G= ({}^{2t}g_1({}^*z_1, {}^*z_2, \dots, {}^*z_k), {}^{2t}g_2({}^*z_1, {}^*z_2, \dots,{}^* z_k),\dots, {}^{2t}g_{r-1}({}^*z_1, {}^*z_2, \dots, {}^*z_k))=b(2t)$,

${}^{2t}H=({}^2h_1({}^*z_1, {}^*z_2,\dots, {}^*z_k),{}^2h_2({}^*z_1, {}^*z_2, \dots, {}^*z_k), \dots, {}^2h_k({}^*z_1, {}^*z_2, \dots, {}^*z_k))=a(2t),\dots,$

${}^2G= ({}^2g_1({}^*z_1,{}^* z_2, \dots, {}^*z_k), {}^2g_2({}^*z_1, {}^*z_2, \dots, {}^*z_k),\dots, {}^2g_{r-1}({}^*z_1,{}^*z_2, \dots, {}^*z_k))=b(2)$,

${}^2H=({}^2h_1({}^*z_1, {}^*z_2,\dots, {}^*z_k),{}^2h_2({}^*z_1,{}^* z_2, \dots, {}^*z_k), \dots, {}^2h_k({}^*z_1,{}^* z_2, \dots,{}^* z_k))=a(2)$,

${}^1G=({}^1g_1({}^*z_1, {}^*z_2, \dots, {}^*z_k), {}^1g_2({}^*z_1, {}^*z_2, \dots, {}^*z_k),\dots, {}^1g_k({}^*z_1, {}^* z_2, \dots, {}^*z_k))=b(1),$

${}^1H=({}^1h_1({}^*z_1, {}^*z_2,\dots, {}^*z_k), {}^1h_2({}^*z_1, {}^*z_2, \dots, {}^*z_k), \dots, {}^1h_{r-1}({}^*z_1, {}^*z_2, \dots, {}^*z_k))=a(1),$

-

${}^0G=({}^0g_1({}^*z_1, {}^*z_2, \dots, {}^*z_k), {}^0g_2({}^*z_1, {}^*z_2, \dots, {}^*z_k),\dots, {}^0g_{r-1}({}^*z_1, {}^*z_2, \dots, {}^*z_k))=b(0),$

${}^0H=({}^0h_1({}^*z_1, {}^*z_2,\dots, {}^*z_k), {}^0h_2({}^*z_1, {}^*z_2, \dots, {}^*z_k), \dots, {}^0h_k({}^*z_1, {}^*z_2, \dots, {}^*z_k)))=a(0).$

Alice considers the graph ${}^{2t}I_m(K)$ with the line ${}^*u$ and computes ${}^2J_{b(2t)}({}^*u)=u_{2t}$. *She* takes the point $N_{a(2t)}(u_{2t})=v_{2t}$.

Alice treats v_{2t} as the line of the graph ${}^{2t-1}I_m(K)$ and computes ${}^2J_{b(2t-1)}=u_{2t-1}$. Alice forms the vertex

$N_{a(2t-1)}=v_{2t-1}$ of graph ${}^{2t-1}I_m(K)$.

She treats v_{2t-1} as vertex of ${}^{2t-2}I_m(K)$ and computes ${}^2J_{b(2t-2)}=u_{2t-2}$.

Alice takes the neighbour $N_{a(2t-2)}(u_{2t-2})=v_{2t-2}$.

She continues this process.

Alice takes the vertex v_1 of the graph ${}^1I_m(K)$. She treat it as the line of the graph ${}^0I_m(K)$.

Alice computes ${}^2J_{b(0)}((v_1)=u_0$.

She computes $N_{a(0)}(u_0)=v_0$.

Finally Alice computes $v={}^1J_{z^*}(v_0)$.

So she gets $v=(v_1, v_2,\dots, v_k, v_{k+1}, v_{k+2},\dots,v_{k+m})$.

Alice writes the system of linear equations

$L'_1(y_1, y_2, \dots, y_{n'})=v$ and gets the solution ${}^*y= ({}^*y_1, {}^*y_2, \dots, {}^*y_{n'})$.

She sends ${}^*y$ to Bob. He checks that $G({}^*y)=c$.

6. Conclusion

6.1. Some remarks

Below we present some heuristic arguments supporting the conjecture that the complexity to find the reimage of quadratic map of algorithms 1 and 2 without the knowledge of described trapdoor accelerator is nonpolynomial.

Let us consider the case when Alice does not use endomorphisms L_1 and L_2 of degree 1.

Assume that she use only one cellular Schubert graphs ${}^{s,k}CS_m(K)$ with the operator of changing colour and the operator to compute the neighbour of chosen vertex. We can consider the graph ψ of the binary relation " colours of vertexes x and y of different type can be changed to make recoloured vertexes adjacent in ${}^{s,k}CS_m(K)$. Then input x and output y vertexes of algorithm 1 or 2 will be connected by the walk in $\cdot\psi$. Dijkstra algorithm will allow us to find the walk between x and y and recover the reimage of y in time $vln\ (v)$ where v is the order of graph.

Let d , $d>3$ be the order of finite commutative ring K and n be the maximal dimension of the space of the partition sets of ψ. Then $v>d^n$ and the complexity of Dijkstra algorithm of finding the path between the input and the output of the algorithm is exponential one. We can expect that with the temporal graph defined via the sequence of Jordan-Gauss graphs ${}^j I_m(K), j=0, 1, 2,...$ the complexity of finding the path will be higher.

Temporal Jordan-Gauss graphs can be used for the constructions of new platforms of Noncommutative Cryptography (see [36], [37], [38], [39], [40], [41], [42] and new cryptanalytic results [43],[44], [45], [46], [47], [48], [49]). These platforms are special semigroups or groups of degree bounded by constant (2 or 3) of the Cremona semigroup of all endomorphisms of $K[x_1, x_2,..., x_n]$ over the selected K. Examples of such platforms can be found in [33], [22].

6.2. The summary

Multivariate Cryptography (MC) is one of the five core directions of Postquantum cryptography. It is specially important for creation of fast digital signatures procedures. Despite the fact currently announced by National Standards of Information Technology (NIST, USA) standards of postquantum cryptography are constructed in the terms of alternative to MC approaches the intensive research on new multivariate cryptosystem is continue. When it comes to digital signatures, NIST has developed two standards. The first is called Module-Lattice-Based Digital Signature Algorithm (ML-DSA for short) and defines a general digital signature algorithm.

The second one is called Stateless Hash-Based Digital Signature Algorithm (SLH-DSA for short). It is a digital signature algorithm based on the hash technique. Essentially shorter signatures can be obtained with the multivariate cryptosystem ''TUOV: Triangular Unbalanced Oil and Vinegar'' algorithm were presented to NIST (see https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/TUOV-spec-web.pdf) by principal submitter Jintaj Ding.

Our paper presents several new multivariate digital signatures. Some of them are the generalisations of schemes [31] known since 2015 for which the cryptanalysis is still unknown. Proposed methods allow us to construct obfuscations of arbitrary selected multivariate cryptosystem such as mentioned above TUOV, old Matsumoto-Imai system, various variants of Oil and Vinegar system and others. Additionally new method gives an option to create algebraic cryptosystems over the finite commutative rings K different from finite fields such as arithmetical or Boolean rings. We believe that Multivariate K-theory for which the main instrument is an element of Cremona semigroup of endomorphisms of $K[x_1, x_2,..., x_n]$ (see [25], [26]) has a capacity to provide efficient digital signatures. Suggested algorithms in case of finite fields and arithmetical rings can be already used for the protection of Information systems.

Acknowledgements

This research is supported by British Academy Fellowship for Researchers under Risk 2022 and by British Academy and partially supported by the British Academy award LTRSF\100333.

References

[1] 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).

[2] Ward Beullens, Improved Cryptanalysis of UOV and Rainbow, In Eurocrypt 2021, Part 1, pp. 348-373.

[3] Anne Canteaut, François-Xavier Standaert (Eds.), Eurocrypt 2021, LNCS 12696, 40th Annual In-ternational Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17–21, 2021, Proceedings, Part I, Springer.

[4] Ding and A. Petzoldt, "Current State of Multivariate Cryptography," in IEEE Security & Privacy, vol. 15, no. 4, pp. 28-36, 2017, doi: 10.1109/MSP.2017.3151328.

[5] Smith-Tone, D. (2022), 2F - A New Method for Constructing Efficient Multivariate Encryption Schemes, Proceedings of PQCrypto 2022: The Thirteenth International Conference on Post-Quantum Cryptography, virtual, DC, US.

[6] Daniel Smith Tone, New Practical Multivariate Signatures from a Nonlinear Modifier, IACR e-print archive, 2021/419.

[7] Daniel Smith-Tone and Cristina Tone, A Nonlinear Multivariate Cryptosystem Based on a Random Linear Code, https://eprint.iacr.org/2019/1355.pdf

[8] Jayashree, Dey, Ratna Dutta, Progress in Multivariate Cryptography: Systematic Review, Challenges, and Research Directions, ACM Computing Survey, volume 55, issue 12,No.246, pp 1-34, https://doi.org/10.1145/3571071.

[9] Cabarcas Felipe, Cabarcas Daniel, and Baena John. 2019. Efficient public-key operation in multivariate schemes. Advances in Mathematics of Communications 13, 2 (2019), 343.

[10] Cartor Ryann and Smith-Tone Daniel. 2018. EFLASH: A new multivariate encryption scheme. In Proceedings of the International Conference on Selected Areas in Cryptography. Springer, 281–299.

[11] Casanova Antoine, Faugère Jean-Charles, Macario-Rat Gilles, Patarin Jacques, Perret Ludovic, and Ryckeghem Jocelyn. 2017. Gemss: A great multivariate short signature. Submission to NIST (2017).y. Springer, Singapore, 209–229.

[12] Chen Jiahui, Ning Jianting, Ling Jie, Lau Terry Shue Chien, and Wang Yacheng. 2020. A new encryption scheme for multivariate quadratic systems. Theoretical Computer Science 809 (2020), 372–383.

[13] Chen Ming-Shing, Hülsing Andreas, Rijneveld Joost, Samardjiska Simona, and Schwabe Peter. 2018. SOFIA: MQ-based signatures in the QROM. In Proceedings of the IACR International Workshop on Public Key Cryptography. Springer, 3–33.

[14] Ding Jintai, Petzoldt Albrecht, and Schmidt Dieter S.. 2020. Multivariate Public Key Cryptosystems, Second Edition. Advances in Information Security. Springer.

[15] Dung H. Duong, Ha T. N. Tran, Willy Susilo, and Le Van Luyen. 2021. An efficient multivariate threshold ring signature scheme. Computer Standards & Interfaces 74.

[16] Jean-Charles Faugère, Gilles Macario-Rat, Jacques Patarin, and Ludovic Perret. 2022. A new perturbation for multivariate public key schemes such as HFE and UOV. Cryptology ePrint Archive (2022).

[17] N. Biggs, Algebraic graphs theory, Second Edition, Cambridge University Press, 1993.

[18] A. Brower, A. Cohen, A. Nuemaier, Distance regular graphs, Springer, Berlin, 1989.

[19] B. Bollob´as, Extremal Graph Theory, Academic Press, London, 1978

[20] 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

[21] V. Ustimenko, On small world non Sunada twins and cellular Voronoi diagams, Algebra and Discrete Mathematics, vol. 30, N1 (2020), pp. 118-142.

[22] V. Ustimenko. 2022. Graphs in terms of Algebraic Geometry, symbolic computations and secure communications in Post-Quantum world, UMCS Editorial House, Lublin, 2022, 198.

[23] V. Ustimenko, 2023, Schubert cells and quadratic public keys of Multivariate Cryptography. CEUR Workshop Proceedings ITTAP , https://ceur-ws.org/Vol-3628/.

[24] N. Bourbaki, Lie Groups and Lie Algebras, Chapters 1 - 9, Springer, 1998-2008.

[25] M. Noether,{\em Luigi Cremona}, Mathematische Annalen, 59 (1904), pp. 1-19.

[26] V. L. Popov, Roots of the affine Cremona group, in: Affine Algebraic Geometry, Seville, Spain, June 1821, 2003, Contemporary Mathematics, Vol. 369, American Mathematical Society, Providence, RI, 2005, pp. 12-13.

[27] Markku Juhani Saarinen, Daniel Tony Smith (editors), Post Quantum Cryptography, 15th International Workshop, PQCrypto 2024,Oxford, UK, June 12-14, 2024, Proceedings, Part 1.

[28] Markku Juhani Saarinen, Daniel Tony Smith (editors), Post Quantum Cryptography, 15th International Workshop, PQCrypto 2024,Oxford, UK, June 12-14, 2024, Proceedings, Part 2.

[29] Tsuyoshi Takagi, Masato Wakayama, Keisuke Tanaka, Noboru Kunihiro, Kazufumi Kimoto, Yasuhiko Ikematsu (editors), International Symposium on Mathematics, Quantum Theory, and Cryptography, Proceedings of MQC 2019, Open Access, 2021

[30] Kohei Arai (editor), Advances in Information and Communication,Proceedings of the 2024 Future of Information and Communication Conference (FICC), Volume 1-3, Lecture Notes in Networks and Systems, (LNNS, volume 919 -921) , Springer, 2024.

[31] 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).

[32] V. Ustimenko, Linear codes of Schubert type and quadratic public keys of Multivariate Cryptography,

IACR e-print archive, 2023/175.

[33] v. ustimenko, On computations with double Schubert automaton and stable maps of multivariate cryptography, Interdisciplinary Studies of Complex SystemsNo. 19 (2021) 18–32.

[34] I. Gelfand, R. MacPherson,Geometry in Grassmanians and generalisation of the dilogarithm, Adv. in Math., 44 (1982), 279-312.

[35] I. Gelfand, V. Serganova, Combinatorial geometries and torus strata on homogeneous compact manifolds, Soviet Math. Surv. 42 (1987), 133-168.

[36] 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.

[37] 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.

[38] 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.

[39] 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.

[40] Alexei Myasnikov; Vladimir Shpilrain and Alexander Ushakov (2008), Group-based Cryptography, Berlin: Birkhäuser Verlag.

[41] Zhenfu Cao (2012), New Directions of Modern Cryptography. Boca Raton: CRC Press, Taylor & Francis Group. ISBN 978-1-4665-0140-9.

[42] Benjamin Fine, et. al. "Aspects of Non abelian Group Based Cryptography: A Survey and Open Problems", arXiv:1103.4093.

[43] V. A. Roman'kov, A nonlinear decomposition attack, Groups Complex. Cryptol. 8, No. 2 (2016), 197-207.27.

[44] V. Roman'kov, An improved version of the AAG cryptographic protocol, Groups, Complex., Cryptol, 11, No. 1 (2019), 35-42.

[45] A. Ben-Zvi, A. Kalka and B. Tsaban, Cryptanalysis via algebraic span, In: Shacham H. and Boldyreva A. (eds.) Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2018, Proceedings, Part I, Vol. 10991, 255{274, Springer, Cham (2018).

[46] B. Tsaban, Polynomial-time solutions of computational problems in noncommutative-algebraic cryptography, J. Cryptol. 28, No. 3 (2015), 601-622.

[47] V. Roman’kov, Cryptanalysis of a new version of the MOR scheme, arXiv:1911.00895 [cs.CR].

[48] V. Roman’kov, Cryptanalysis of two schemes of Baba et al. by linear algebra methods. CoRR abs/1910.09480 (2019).

[49] Adi Ben-Zvi, Arkadius G. Kalka, Boaz Tsaban, Cryptanalysis via Algebraic Spans. CRYPTO (1) 2018: 255-274