On Schubert cells of projective geometry and pseudo-quadratic public keys of multivariate cryptography

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

[1] Royal Holloway University of London, TW20 0EX Egham, United Kingdom
[2] Institute of Telecommunications and Global Information Space, 13 Chokolivsky ave., 02000 Kyiv, 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, $n \geq m$ such that the neighbour of each vertex is defined by the system of the linear equation given in its row-echelon form. Assume that K is a finite multivariate commutative ring and the cardinality of multiplicative group K^* is >2. We use families of these graphs for the construction of new injective multivariate maps F of $(K^*)^n$ onto K^n of unbounded degree of size O(n) with the trapdoor accelerators T, i.e. pieces of information which allows us to compute the reimage of the given value of F in polynomial time. The number of monomial terms of multivariate rule F written in its standard form (the density) is $O(n^2)$. Thus public user can encrypt his/her message in time $O(n^3)$ similar to the case of a quadratic map. This cryptosystem can be obfuscated via the use of a temporal analogue of selected Jordan-Gauss graphs. Previously known multivariate cryptosystems of unbounded degree have density $O(n^4)$ of F allowing us to use the inform in the case of finite field it can be used for the construction of new cryptosystems from known pairs (F, T).

Keywords

multivariate cryptography, Jordan-Gauss graphs, projective geometries, temporal graphs, largest Schubert cells, symbolic computations

1. Introduction

This paper presents the modification of the quadratic multivariate public key given in [1] and defined via special walks on projective geometries over finite fields and their natural analogs defined over general commutative rings. New graph-based multivariate rules are "pseudo quadratic", i.e., they are maps of unbounded degree of size $O(n)$ but the number of monomial terms in all equations is $O(n^2)$. So, like in the case of a quadratic map the computation of the value of the map on the given tuple costs $O(n^3)$.

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 the standardisation best known quantum-resistant algorithms of asymmetrical cryptography. The first round was finished in March 2019, and essential parts of the presented algorithms were rejected. At the same time, the development of new algorithms with a postquantum perspective was continued. A 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 were announced in 1922, they were developed in terms of Lattice Theory.

Noteworthy that the 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 in 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 the 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.

CPITS-II 2024: Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, October 26, 2024, Kyiv, Ukraine
* 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)

It's interesting that the new obfuscation "TUOV: Triangular Unbalanced Oil and Vinegar" was presented to NIST by principal submitter Jintaj Ding [4].

The historical development of Classical Multivariate Cryptography which studies quadratic and cubic endomorphisms of $F_q[x_1, x_2,..., x_n]$ can be found in [5] and [6]. Current research in Postquantum Cryptography can be found in [5, 7–23].

Section 2 contains some definitions of Multivariate Cryptography over a general commutative ring.

In Section 3 we introduce the concept of linguistic graphs and Jordan-Gauss graphs defined over commutative ring K together with the examples of such graphs which appear as bipartite-induced subgraphs of the Incidence Graph of Projective Geometry or its analogue defined over K.

Equations of some graphs are given explicitly. We define the temporal analogue of linguistic graphs.

Section 4 is dedicated to the constructions of multivariate rules with trapdoor accelerators in terms of linguistic graphs. In the case of Cellular Schubert graphs or their temporal analogue we evaluate the density of constructed multivariate rules.

In Section 5 we describe the Eulerian subgroup of transformations of Affene Cremona semigroup of all endomorphisms of $K[x_1, x_2,..., x_n]$. Eulerian transformation maps each variable x_i into a monomial term.

The new cryptosystem is described in Section 6. This map is formed as the composition of Eulerian transformation J, transformation F defined in terms of special Jordan-Gauss graphs in Section 4, and element L from $AGL_n(K)$. The complexity of the decryption procedure is estimated there.

Section 7 contains concluding remarks.

2. On the tasks of multivariate cryptography over arbitrary finite commutative ring

This paper is dedicated to the construction of public maps F of multivariate cryptography transforming the tuple $(x_1, x_2, ..., x_n)$ from K^n to $(f_1(x_1, x_2, ..., x_n), f_2(x_1, x_2, ..., x_n), ..., f_k(x_1, x_2, ..., x_n))$ from K^k where K is a finite commutative ring with unity and polynomials $f_i \in K[x_1, x_2, ..., x_n]$ are written in their standard forms, i.e. lists of their monomial terms ordered lexicographically.

We say that piece of information T is a trapdoor accelerator of F if T is the piece of information such that its knowledge allows us to compute the reimage of F for given value b from K^k in a polynomial time $O(n^\alpha)$.

Classical multivariate cryptography uses surjective map F defined over finite field $K=F_q$ with the trapdoor accelerator T. Correspondents Alice and Bob use the following scheme.

Map F is announced publicly. Alice has the knowledge of T. Alice and Bob have some digest (hash value) $b=(b_1, b_2, ..., b_k) \in K^k$ of the document. To sign the document Alice solves the system of equations $f_i(x)=b_i$, $i=1, 2, ..., k$. She gets a solution $x_1=d_1, x_2=d_2, ..., x_n=d_n$ and sends the tuple $d=(d_1, d_2, ..., d_n)$. Public user Bob verifies that $F(d)=b$.

If $k=n$ then the pair (F, T) can be used as the encryption scheme. Bob writes his plaintext $p=(p_1, p_2, ..., p_n)$ and forms the ciphertext $c=F(p)$. He sends c to Alice via the open channel. Her knowledge of T allows Alice to restore p as $F^{-1}(c)$.

In both schemes, correspondents would like to use F as one way function for which reimages of b or p are impossible to compute in polynomial time without the knowledge of T.

The search for multivariate one way functions is motivated by the following 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 the Jordan-Gauss elimination method. The complexity of solving a nonlinear system of constant degree d, $d>1$ is subexponential (see [24, 25]). Despite the convenience of the Groebner-Shirshov basis method [26] for the implementation the complexity of this algorithm is equivalent to the old Gauss elimination method for the solution of the system of nonlinear equations. There is a standard way to transform of nonlinear system of equation of degree d, $d>2$ to an equivalent quadratic system via the introduction of additional variables and substitutions (see [5]).

So if we have a nonlinear map F of bounded degree d in "general position" which has a trapdoor accelerator T then the corresponding cryptosystem is secure. This status insures 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 a "general position" if some additional specific information is known. For instance, if F is the bijective cubic map and F^{-1} is also cubic. The 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 ensure that 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 $P \neq NP$.

It is well known that the investigation of nonlinear systems of equations over the commutative ring K with zero divisors is essentially a harder case in comparison to the case of a field.

Multivariate cryptography over rings with zero divisors is a brand new direction of research. Another idea is the construction of functions F of unbounded degree of size $O(n)$ with the trapdoor accelerators. As we already mentioned there is a reduction of arbitrary system of nonlinear equations to the system of quadratic equations. This method leads to the nonlinear increase of a number of variables. The change of practically used hundreds of variables for several thousands of them makes it impossible to use the Groebner basis technique as a cryptanalytical instrument. The adversary has the luck of computational resources to break the cryptosystem.

We will combine both ideas for the construction of new multivariate public keys for the task of information exchange within the following general scheme.

Let K be a commutative ring with nontrivial multiplicative group K^*.

We consider the multivariate map F of K^n into K^n given by the rule $x_i \to f_i(x_1, x_2, ..., x_n)$ such that its restriction on

$(K^*)^n$ is injective. We say that T is a multiplicative trapdoor of F if the knowledge of T allows us to solve the system of equations $F(x)=b$ for $b \epsilon F((K^*)^n)$.

Assume that the density of F is $O(n^d)$ where d is some constant. Then the public rule $x \longrightarrow F(x)$ can be used as an encryption scheme with the space of plaintexts $(K^*)^n$ and the space of ciphertexts (K^n).

Assume that Alice has a pair (F, T) and public user Bob has the standard form of F.

Then he writes his plaintext $p=(p_1, p_2, ..., p_n)$ and sends the ciphertext $c=F(p)$ to Alice. She uses the information piece T and computes the plaintext.

3. Linguistic and Jordan-Gauss graphs and their temporal analogs

The missing definitions of graph-theoretical concepts and incidence systems theory which appear in this paper can be found in each of the books [27–30].

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 Cartesian product $V(G) \cdot V(G)$ and write v G u for the adjacent vertexes u and v (or neighbours). We refer to $|\{x \epsilon V(G) | xGv\}|$ as the 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.

We define *linguistic graphs* of type (s, r, m) where $s>0$, $r>0$, $m>0$ over the commutative ring K with unity as bipartite graphs with the partition sets $P=K^{s+m}$ and

$L=K^{r+m}$ such that the point $(x_1, x_2, ..., x_s, x_{s+1}, x_{s+2}, ..., x_{s+m})$ from P is incident to the line $[y_1, y_2, ..., y_r, y_{r+1}, y_{r+2}, ..., y_{r+m}]$ from L if and only if the following equations are satisfied:

$$a_j x_{s+j} - b_j y_{s+j} = f_j(x_1, x_2, ..., x_{s+j-1}, y_1, y_2, ..., y_{t+j-1}) \quad (1)$$

where a_j and b_j are elements of the multiplicative group of K and f_j are polynomials from $K[x_1, x_2, ..., x_{s+j-1}, y_1, y_2, ..., y_{r+j-1}]$ (see [31]).

We say that a linguistic graph is a Jordan-Gauss graph if polynomials f_j have degree 2 and consist of monomial terms of kind $x_i y_k$ for $j=1, 2, ..., m$.

The neighbourhood of each vertex of a general Jordan-Gauss graph is given by the system of linear equations in its row-echelon form.

Examples of families of Jordan-Gauss graphs can be obtained as induced subgraphs of the incidence graphs of geometries of Chevalley groups (see [32]) defined over various fields (see [23], [33] and further references).

Let us consider the case of Coxeter-Dynkin diagram A_n, i.e. projective geometry $PG_n(F)$ of dimension n over the field F. This incidence system is a totality $PG_n(F)$ of proper nontrivial subspaces of the vector space F^{n+1}.

The dimension $t(W)$ of subspace defines the type of W. So the set $P_n(F)$ is a disjoint union of Grassmanians $\Gamma_i(F)=\{W: t(W)=i\}$, $i=1,2, ..., n-1$. Two elements ${}^1W$ and ${}^2W$ are incident $({}^1W\, I\, {}^2W)$ if they have different types and ${}^1W<{}^2W$ or ${}^2W<{}^1W$. We identify the binary relation I with the corresponding multipartite graph.

Let ${}^{i,j}\Gamma(F)$ be the bipartite graph of the restriction of I on the disjoint union of Grassmanians $\Gamma_i(F)$ and $\Gamma_j(F)$.

The Borel subgroup B of algebraic group $PGL_n(K)$ consists of triangular matrices $A=(a_{i,j})$: such that $a_{i,j}=0$ if $i<j$ with determinant 1.

Let us consider the orbits of group B acting on $PG_n(F)$. For the description of orbits, we select the standard basis $e_1, e_2, ..., e_n, e_{n+1}$ of the vector space F^{n+1}.

Then each orbit $O_{\mathcal{J}}$ from $\Gamma_m(F)$ contains the unique symplectic subspace of kind $e_{j(1)}, e_{j(2)}, ..., e_{j(m)}$ where $\mathcal{J}=\{i(1), i(2), ..., i(m)\}$ is a subset of $\{1, 2, ..., n, n+1\}$. There is a subgroup $U(\mathcal{J})$ of unitriangular elements from $GL_{n+1}(F)$ which consists of matrices $E+(a_{i,j})$ such that $a_{i,j} \neq 0$ if $(i \epsilon i \epsilon \mathcal{J}) \& (j \,\&N\text{-}\mathcal{J}) \& (i>j)$.

The transitive group of transformation $(U(\mathcal{J}), O_{\mathcal{J}})$ is a regular representation of abstract group $U(\mathcal{J})$, i.e. stabilisator of each representative of the orbit is the unity subgroup. Thus there are natural one-to-one correspondence between elements $U(\mathcal{J})$ and $O_{\mathcal{J}}$ and we can identify these sets.

Elements of orbits $U(\mathcal{J})$ and $U(\mathcal{J}')$ are not incident unless the condition

$$\mathcal{J} \subset \mathcal{J}' \text{ or } \mathcal{J}' \subset \mathcal{J} \text{ and } |\mathcal{J}| \neq |\mathcal{J}'| \quad (2)$$

holds, i.e. elements $\mathcal{J}$ and $\mathcal{J}'$ are incident as elements of Weyl geometry A_n.

For the description of the incidence condition of elements $M \epsilon U(\mathcal{J})$ we introduce subset $\Delta(\mathcal{J})=\{(i,j) | (i \epsilon i \epsilon \mathcal{J}) \& (j \,\&N\text{-}\mathcal{J}) \& (i>j)\}$.

We define the projection of triangular matrix $M=(m(i,j))$ on the subset A of $\{(i, j): i>j\}$ as function f from A to such that $f(i,j)=m(i,j)$ for $(i,j) \epsilon A$.

Each unit triangular matrix M from $U(\mathcal{J})$ is uniquely determined by its projection on $\Delta(\mathcal{J})$.

Let M and M' be elements of $U(\mathcal{J})$ and $U(\mathcal{J}')$ where $\mathcal{J}$ and $\mathcal{J}'$ are incident elements of Weyl geometry. Then M and M' are incident elements of projective geometry if and only if

$$(M\text{-}M')_{\Delta(\mathcal{J}) \cap \Delta(\mathcal{J}')} = (MM\text{-}M'M)_{1\Delta(\mathcal{J}) \cap \Delta(\mathcal{J}')} \quad (3)$$

It is easy to see that the bipartite graph ${}^F G(\mathcal{J}, \mathcal{J}')$ with partition sets $U(\mathcal{J})$ and $U(\mathcal{J}')$ where $\mathcal{J}$ and $\mathcal{J}'$ are incident elements of Weyl geometry and incidents of points and lines are defined by the condition (2) is a Jordan-Gauss graph.

Noteworthy that the coefficients of monomial terms in the system of equations (2) are $+1$ and -1. So we can introduce ${}^K G(\mathcal{J}, \mathcal{J})$ over arbitrary commutative ring K with unity via the direct change of F for K. We can consider unimportant subgroup $U_K(\mathcal{J})$ of the group of unitriangular matrices $U(n+1, K)$ over K and define the incidence of elements $U_K(\mathcal{J})$ and $U_K(\mathcal{J}')$ by the condition 2 in the case when $\mathcal{J}$ and $\mathcal{J}'$ satisfy (1).

In fact, we can define $PG_n(K)$ in the case of general commutative ring with unity as disjoint union of partition sets of bipartite graphs ${}^K G(\mathcal{J}, \mathcal{J}')$, type function $t(x)$ of $x \epsilon U_K(\mathcal{J})$ equals $|\mathcal{J}|$ for the incidence $x \epsilon U_K(\mathcal{J})$ and $y \epsilon U_K(\mathcal{J}')$ the condition (1) is necessary, if (1) holds then (2) is required additionally.

This approach of construction of incidence systems over commutative ring K with unity can be used in the case of other Dynkin-Coxeter diagrams, i.e. B_n, C_n, D_n, E_6, E_7, E_8, F_4, G_2 (see [28], [32]).

Each Grassmanian $\Gamma_m(K)$ is the union of affine spaces $U_K(\mathcal{J})$ where $|\mathcal{J}|=m$. These spaces are known as large

Schubert cells, small Schubert cells can be defined in the case of field K (see [34], [35]) The variety $\Gamma_m(K)$ contains the unique largest Schubert cell which is the cell of maximal dimension. It is easy to see that the largest Schubert cell of $\Gamma_m(K)$ is $U_K(\mathcal{J})$ for $\mathcal{J}=\{n+1, n, ..., n+1-m\}$.

We refer to the disjoint union $SPG_n(K)$ of largest Schubert cells as Schubert with the restriction of incidence relation I of $PG_n(K)$ on this subset as Schubert system over K. It is easy to see that for the incidence of elements x and y from distinct Schubert cells the condition *(3)* is sufficient.

Let $\Gamma(K)$ be a Jordan-Gauss graph of type (s, r, m) where $s>0$, $r>0$, $m>0$ over the commutative ring K with unity with the incidence given by conditions (1).

We refer to the list S of all nonzero monomial terms of f_j taken with coefficient 1, together with the parameters s, r, m as the symbolic type of the Jordan-Gauss graph $\Gamma(K)$. It is convenient that the symbolic type of a Jordan-Gauss graph $\Gamma(K)$ over K is independent of the choice of K. We say that two Jordan-Gauss graphs defined over commutative rings K and K' are symbolically equivalent if they have the same symbolic type.

We define a temporal (depending on time) Jordan-Gauss graph $\Gamma(K)^t$ of symbolic type $\boldsymbol{S}$ as the family of equivalent Jordan-Gauss graphs $\Gamma(K)^t$, $t=1, 2, ...$ defined by equations (1) with the same constant symbolic type S depending on time t coefficients $a_i=a_i(t)$, $b_i=b_i(t)$ and nonzero monomial terms of f_j of the form ${}^j a(i, k)x_i\, y_k$, $x_i\, y_k \in S$, ${}^j a(i, k)={}^j a(i, k)(t)\neq 0$. Some examples of temporal Jordan-Gauss graphs can be found in [36]. In contrast to the definition of time-dependent graphs of [37] we introduce Jordan-Gauss temporal graphs via time-dependent equations.

So we can introduce temporal analogue $PG_n(K)^t$ of $PG_n(K)$ and temporal analogue $SPG_n(K)^t$ of $SPG_n(K)$ via the option to change the coefficients of monomial terms of each nontrivial induced subgraph $G_K(\mathcal{J}, \mathcal{J}')$, ${}^j C_n(K)$.

Let ${}^{i,\,j}C_n(K)$ be the bipartite-induced subgraph of $SPG_n(K)$ of all elements of type i or type j. We refer to this graph as a cellular Schubert graph and use the term temporal Schubert Graph for $SPG_n(K)$.

We refer to $PG_n(K)^t$ and $SPG_n(K)^t$ as temporal projective geometry over K and say that $SPG_n(K)^t$ is temporal Schubert Geometry with the diagram A_n over the commutative ring K. Temporal geometries of Chevalley groups and corresponding Schubert geometries in the cases of various Coxeter-Dynkin diagrams are defined in [36].

Let us consider some illustration examples.

The graph ${}^{1,\,n}C_n(K)$ is a bipartite graph of points $(x_1, x_2, ..., x_n)$ and lines $[y_1, y_2, ..., y_n]$ with incidences given by equations: $x_n-y_n=x_1y_1+x_2y_2+\cdots+x_{n-1}y_{n-1}$.

This is symbolically equivalent to the ${}^{1,n}C_n(K')$ Jordan-Gauss graph over the ring K' with unity, having partition sets isomorphic to $(K')^n$ and with incidences given by equations of the form: $ax_n-by_n=a_1x_1y_1+a_2x_2y_2+\cdots+a_{n-1}y_{n-1}$, where a and b are elements of the multiplicative group of K' and $a_i\neq 0$, $i=1, 2, ..., n-1$.

Graph ${}^{1,\,n}C_n(K)^t$ has the same points and lines with ${}^{1,\,n}C_n(K)$ but the incidence is given by equations $a(t)x_n-b(t)y_n=a_1(t)x_1y_1+a_2x(t)x_2y_2+\cdots+a_{n-1}(t)x_{n-1}y_{n-1}$.

We say that ${}^{i,\,j}C_n(K)^t$ convert in fixed time moment $t=t^*$ to static Jordan-Gauss graph ${}^{i,\,j}C_n(K)^t\ |t=t^*$ via selection of values of "time-dependent" coefficients of monomial terms of equations.

In another example, the graph ${}^{s,\,s+1}C_{s+r}(K)$ can be interpreted as a bipartite graph consisting of points of the form $(x_1, x_2, ..., x_s, x_{1,1}, x_{1,2}, ..., x_{s,r})$ and lines $[y_1, y_2, ..., y_r, y_{1,1}, y_{1,2}, ..., y_{s,r}]$, with the incidence condition given by the equations:

$x_{i,j}-y_{i,j}=x_iy_j$, $i=1,2, ..., s$, $j=1,2, ..., r$.

This is symbolically equivalent to the graph ${}^{s,\,s+1}C_{s+r+1}(K)$, defined over the same commutative ring K and with an incidence relation given by the system of equations:

$a_{i,j}x_{i,j}-b_{i,j}y_{i,j}=d_{i,j}x_iy_j$, where elements $a_{i,j}$ and $b_{i,j}$ belong to K^* and $d_{i,j}$ are elements from $K\setminus\{0\}$.

These two families of graphs give us extremal cases: the incidence of points and hyperplanes from ${}^{1,\,n}C_n(K)$ is the case of the single equation, while the case of subspaces of dimension s and $s+1$ of ${}^{s,\,s+1}C_{s+r+1}(K)$ is the case when polynomials of the right-hand side have a single monomial.

4. Jordan-Gauss graphs and the maps with the trapdoor accelerator

Let us consider basic operators on the set of vertexes of the linguistic graph of type *(s, r, m)*.

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

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

On the sets P and L of points and lines of the linguistic graph we define colour jump operators $\mathcal{J}=\mathcal{J}_b(p)=(b_1, b_2, ..., b_s, p_1, p_2, ..., p_{s+m})$, where $(b_1, b_2, ..., b_s)\in K^s$ and $\mathcal{J}=\mathcal{J}_b([l])=[b_1, b_2, ..., b_r, l_1, l_2, ..., l_{r+m}]$, where $(b_1, b_2, ..., b_r)\in K^r$.

For the point (p) and odd parameter $\boldsymbol{l}$ sequence of the colours $a(1)\in K^s$, $b(1)\in K^r$, $a(2)\in K^r$, $b(2)\in K^s$, ..., $a(l)\in K^s$, $b(l)\in K^r$, $a(1+1)\in K^r$ which allows us to define the map $H: K^{m+s}\to K^{m+r}$ moving arbitrary point (v) to the line $h=h(a(1), b(1), a(2), b(2), ..., a(l), b(l), a(l+1))(v)=v_{l+1}$ defined via the following sequence of vertexes.

$v_1=\mathcal{J}_{a(1)}(v)$, $u_1=N_{b(1)}(v_1)$,

$v_2=\mathcal{J}_{a(2)}(v_1)$, $u_2=N_{b(2)}(v_2)$,

...,

$v_l=\mathcal{J}_{a(l)}(v_{l-1})$, $u_l=N_{b(l)}(v_l)$, $v_{l+1}=\mathcal{J}_{a(l+1)}(u_l)$. We refer to map H as the transition of (v) in the direction $(a(1), b(1), a(2), b(2), ..., a(l), b(l), a(l+1))$.

We can define the transition $H(a(1), b(1), a(2), b(2), ..., a(l), b(l), a(l+1))$ in the case of even $\boldsymbol{l}$ in which $v\to h(v)$ will be a transformation acting on $K^{s+m}=P$.

For eachlinguistic graph $\Gamma(K)$ we consider $\Gamma'=\Gamma(K[z_1, z_2, ..., z_{m+s}])$ given by the same equation but with the partition sets $K[z_1, z_2, ..., z_{m+s}])^{m+s}$ and $K[z_1, z_2, ..., z_{m+s}])^{m+r}$.

We take an odd parameter l, $l>2$, special point $z=(z_1, z_2, ..., z_{m+s})$ and apply the transition $H(a(1), b(1), a(2), b(2), ..., a(l), a(l+1))$ to the vertex $\boldsymbol{z}$ of the graph Γ' such that coordinates $a(i)$, $b(i)$ are elements of $K[[z_1, z_2, ..., z_s]$. The image of $\boldsymbol{z}$ will be the tuple $u=(a(l+1)_1(z_1, z_2, ..., z_s), a(l+1)_2(z_1, z_2, ..., z_s), ..., a(l+1)_r(z_1, z_2, ..., z_s), f_1(z_1, z_2, ..., z_{m+s}), f_2(z_1, z_2, ..., z_{m+s}),$

$..., f_m(z_1, z_2,..., z_{m+s}))$. Let $F=F(a(1), b(1), a(2), b(2), ..., a(l), a(l+1))$ be a polynomial map of K^{m+s} to K^{m+r} sending $(z_1, z_2, ..., z_{m+s})$ to $(u_1, u_2, ..., u_{m+s}])=u$.

We take two affine transformations L_1 and L_2 and consider the composition $G=L_1FL_2$ sending $(z_1, z_2, ..., z_{m+s})$ to $(g_1(z_1, z_2, ..., z_{m+s}), g_2(z_1, z_2, ..., z_{m+s}), ..., g_{m+r}(z_1, z_2,..., z_{m+s}))$.

Additionally, we consider the above-presented construction in the case of even parameter l Then $a(l+1)$ is an element of $K[x_1, x_2, ..., x_s]^s$, u_{l+1} and ν_{l+1} are points. We have to take L_1 and L_2 from $AGL_{m+s}(K)$ and construct the transformation $G=L_1FL_2$ of the affine space K^{m+s}.

Proposition 1 [23]. Let us assume that the surjective map $(z_1, z_2, ..., z_s)$ to $(a(l+1)_1, a(l+1)_2, ..., a(l+1)_t)$ where $t=r$ or $t=s$ has a trapdoor accelerator T.

Then the knowledge on $\Gamma(K)$ and tuples $a(1), b(1), a(2), b(2). ..., a(l), b(l)$, transformations L_1, L_2, and T is a trapdoor accelerator of the standard form of G mapping K^{m+s} on K^{m+t}.

Justification of Proposition 1'.

Let us assume that $\Gamma(K)$ is temporal graph and its static graphs Γ_i in time $i=1, 2, ..., l$ are known as well as $a(1), b(1), a(2), b(2), ..., a(l), b(l), a(l+1), T$ and L_1, L_2 of the Proposition 1. Let us consider the equation $G(z)=b$ for the given value of the tuple b.

We compute $(L_2)^{-1}(b)=c$ and introduce intermediate vector $p=(p_1, p_2, ..., p_s, p_{s+1}, p_{s+2}, ..., p_{s+m})$ of variables p_i and consider the equation $H(p)=c$ where $H=H(a(1), b(1), a(2), b(2), ..., a(l), a(l+1))=(a(l+1)_1, a(l+1)_2, ...a(l+1)_t, h_1, h_2,..., h_m)$, where $h_i \in K[x_1, x_2,..., x_{s+m}]$.

We use our knowledge of the trapdoor accelerator T to get solution $p_1=d_1, p_2=d_2, ..., p_s=d_s$. Let $d=(d_1, d_2,...,d_s)$. It gives us the opportunities to compute $a^*(1)=a(1)(d_1, d_2, ..., d_s)$, $b^*(1)=b(1)(d_1, d_2, ..., d_s)$, $a^*(2)=a(2)(d_1, d_2, ..., d_s)$, $b^*(2)=b(2)(d_1, d_2, ..., d_s)$, ..., $a^*(l)=a(l)(d_1, d_2, ..., d_s)$, $b^*(l)=b(l)(d_1, d_2, ..., d_s)$, $a^*(1)=a(1)(d_1, d_2, ..., d_s)$.

So, we compute $H(b^*(l), a^*(l), b^*(l-1), a^*(l-1), b^*(1), a^*(1), d)= (w_1, w_2, ..., w_s, w_{s+1}, w_{s+2}, ..., w_{s+m})=w$.

Thus we got a solution for $H(p)=c$. We compute the solution z^* of $G(z)=c$ as $z^*=(L_1)^{-1}(w))$.

If l is even or $r=1$ then the reimage reimage z^* is uniquely defined.

We define a density of multivariate polynomial $f(z_1, z_2, ..., z_n)$ written in its standard form as a number of monomial terms.

The density $den(b)$ of the tuple $b=(f_1, f_2, ..., f_k)$ from $K[z_1, z_2, ..., z_n]^k$ is the maximal density of f_i. The density of the map $F: x_i \to f_i$, $i=1,2, ..., k$ coincides with the density of the corresponding tuple of polynomials f_i.

Proposition 2 [23]. Let us assume that condition of the Proposition 1 hold and $\Gamma(K)$ coincides with the Jordan-Gauss graph ${}^{i,j}C_n(K)$, $den(a(i))=O(n^d)$, $den(b(i))=O(n^e)$, $d>1$, $i-j=O(n^k.)$, $0 \le k \le 1$ for $i=1,2, ..., l$. Then the density of the map $F(a(1), b(1), a(2), b(2), ..., a(l), b(l), a(l+1))$ is $O(n^{d+e+k})$.

Remark. Proposition 1 and Proposition 2 hold also for the temporal linguistic graphs and temporal cellular Schubert graphs.

5. On some subgroups of affine Cremona Semigroup

5.1. Some definitions

Let us consider the following important object of Noncommutative Cryptography. Affine Cremona Semigroup ${}^nCS(K)$ is defined as an endomorphism group of polynomial ring $K[x_1, x_2, ..., x_n]$ over the commutative ring K. It is an important object of Algebraic Geometry (see [38] about mathematics of Luigi Cremona—a prominent figure in Algebraic Geometry in XIX).

Element of the semigroup $\boldsymbol{\sigma}$ can be given via its values on variables, i.e. as the rule $x_i \to f_i(x_1, x_2, ..., x_n)$, $i=1, 2, ..., n$. This rule induces the map $\sigma': (a_1, a_2,.., a_n) \to (f_1(a_1, a_2, ..., a_n), f_2(x_1, x_2, ..., x_n), ..., f_n(x_1, x_2, ..., x_n))$ on the free module K^n. Automorphisms of $K[x_1, x_2, ..., x_n]$ form *affine Cremona Group* ${}^nCG(K)$ (see [39]).

In the case when K is a finite field or arithmetic ring Z_m of residues modulo m elements of affine Cremona Groups or Semigroups are used in algorithms of multivariate cryptography. Results about subsemigroups S of ${}^nCS(K)$ (or subgroups of ${}^nCG(K)$ such that computation of the superposition of arbitrary n elements can be completed for polynomial time can be used as so-called platforms of Noncommutative Cryptography.

One class of such objects is formed by stable subsemigroups of degree k, i.e. subsemigroup S such that the maximal degree of its representative is bounded by the constant k. We will talk about the Multiple Composition Computability (*MCC*) property. In the case of $k=1$ one can take $AGL_n(K)$, stable subsemigroups of degree k in ${}^nCG(K)$ exist for each k, $k=2, 3, ...$ *Affine Cremona semigroup* ${}^nCS(K)$ does not pose MCC. If one takes n quadratic elements randomly their product with a probability close to 1 will have degree 2^n. So the computation is not feasible.

EXAMPLE: Let us consider the totality ${}^nES(K)$ of endomorphisms of $K[x_1, x_2, ..., x_n]$ of kind

$$\begin{aligned} x_1 &\to \mu_1 x_1^{a(1,1)} x_2^{a(1,2)} \dots x_n^{a(1,n)}, \\ x_2 &\to \mu_2 x_1^{a(2,1)} x_2^{a(2,2)} \dots x_n^{a(2,n)}, \\ &\dots \\ x_m &\to \mu_n x_1^{a(n,1)} x_2^{a(n,2)} \dots x_n^{a(n,n)} \end{aligned} \quad (4)$$

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

It is easy to see that the complexity of the computation of the product of two elements of kind (4) is $O(n^3)$. So, the semigroup of Eulerian transformations ${}^nES(K)$ poses the property MCC. Semigroups with this property can serve as "platforms" of protocols of Noncommutative Cryptography.

The following examples of special elements of ${}^nES(K)$ can be found in [40].

5.2. On some bijective transformation of $(K^*)^n$

Let π and δ be two permutations on the set $\{1, 2, ..., n\}$. Let K be a commutative ring with unity which has nontrivial multiplicative group K^* of order $d=|K^*|>1$ and $n \ge 1$. We define transformation ${}^A\mathcal{J}G(\pi, \delta)$ of the variety $(K^*)^n$, where A is a triangular matrix with positive integer entries $0 \le a(i,j) \le d$, $i \ge d$ defined by the following closed formula.

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

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

We refer to ${}^A\mathcal{J}G(\pi, \delta)$ as Jordan transformations Gauss multiplicative transformation, or simply $\mathcal{J}G$ element. It is an invertible element of ${}^nES(K)$ with the inverse of kind ${}^B\mathcal{J}G(\delta,$

π) such that $a(i,i)b(i,i)=1 \pmod d$. Notice that in the case $K=Z_m$ straightforward process of computation the inverse of $\mathcal{J}G$ element is connected with the factorization problem of integer m. If $n=1$ and m is a product of two large primes p and q the complexity of the problem is used in the RSA public key algorithm. The idea to use the composition of $\mathcal{J}G$ elements or their generalisations with injective maps *of* K^n into K^n was used in [41] ($K=Z_m$) and [42] ($K=F_q$).

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

We refer to elements of ${}^nES(K)$ as multiplicative Cremona elements. Assume that the order of K is constant. As it follows from the definition the computation of the value of element from ${}^nES(K)$ on the given element of K^n is estimated by $O(n^2)$. The product of two multiplicative Cremona elements can be computed in time $O(n^3)$.

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

6. Multivariate cryptosystem

Let K be a finite commutative ring with unity and nontrivial multiplicative group K^* of order d>1. Alice selects graph

${}^{i,\ j}\mathcal{C}_{2m}(K)$, $i>j$, $i=m+\alpha$, $j=m-\beta$ where $\alpha>0$ and $\beta \geq 0$ are constants ≥ 0. We assume that parameters α and β are essentially smaller than n. She computes parameter $n=(m+\alpha)(m-\alpha+1)$ and $s=(m+\alpha-1)(\alpha+\beta)$, $r=(m-\beta)(\alpha+\beta)$ and forms the transformation $\mathcal{J}_1$ and $\mathcal{J}_2$ from ${}^nEG(K)$ of kind

$y_1=\mu_1 x_1^{a(1,1)}$

$y_2=\mu_2 x_1^{a(2,1)}\ x_2^{a(2,2)}$

...

$y_n=\mu_n x_1^{a(n,1)}\ x_2^{a(n,2)} \dots\ x_n^{a(n,n)}$

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

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

$z_2=\mu'_1 y_2^{b(2,2)}\ y_2^{b(2,3)} \dots\ y_n^{b(2,n)}$

...

$z_n=\mu'_n y_n^{b(n,n)}$

where $(b(n,n), d)=1$, $(b(n-1, 2), d)=1$, ..., $(b(1, n), d)=1$.

She computes the composition of $\mathcal{J}_1$ and $\mathcal{J}_2$ and obtains the vector $(z_1, z_2, \dots, z_s, z_{s+1}, \dots, z_n)$ and treats this tuple as a point of graph ${}^{i,\ j}\mathcal{C}_{2m}(K)$.

She selects even parameter l, $l>5$ of size $O(1)$ together with sparse tuples $a(1), b(1), a(2), b(2), \dots, a(l), b(l), a(l+1)$ of density $O(1)$ of Proposition 2.

So, $a(i)=({}^i l_1(z_1, z_2, \dots, z_s), {}^i l_2(z_1, z_2, \dots, z_s), \dots, {}^i l_s(z_1, z_2, \dots, z_s))$ for $i=1, 3, 5, \dots, l-1, l+1$,

$a(i)=({}^i l_1(z_1, z_2, \dots, z_s), {}^i l_2(z_1, z_2, \dots, z_s), \dots, {}^i l_r(z_1, z_2, \dots, z_s))$ for $i=2, 4,\dots, l$,

$b(i)=({}^i h_1(z_1, z_2, \dots, z_s), {}^i h_2(z_1, z_2, \dots, z_s), \dots, {}^i h_r(z_1, z_2, \dots, z_s))$ for $i=1, 3, \dots, l-1$,

$b(i)=({}^i h_1(z_1, z_2, \dots, z_s), {}^i h_2(z_1, z_2, \dots, z_s), \dots, {}^i h_s(z_1, z_2, \dots, z_s))$ for $i=2, 4, \dots, l$.

Alice selects $a(l+1)$ as a tuple of kind

$(\lambda_1 z_1^{e(1,1)}, \lambda_2 z_1^{e(2,1)} z_2^{e(2,2)}, \dots,$

$\lambda_s z_1^{e(s,1)} z_2^{e(s,2)} \dots\ z_s^{(s,s)})$ where $(e(1, 1), d)=1$, $e(2, 2), d)=1$, ..., $(e(s, s), d)=1$.

Alice computes $F(z_1, z_2, \dots, z_n)=(F(a(1), b(1), a(2), b(2), \dots, a(l), b(l), a(l+1))$ $(z_1, z_2, \dots, z_n)=(u_1, u_2, \dots, u_n)=u$.

She takes element L from $AGL_n(K)$ and computes $L(u)=(w_1, w_2, \dots, w_n)$. So Alice computes the composition $G=\mathcal{J}_1\mathcal{J}_2 FL$: $(x_1, x_2, \dots, x_n) \longrightarrow (w_1(x_1, x_2, \dots, x_n), w_2(x_1, x_2, \dots, x_n), \dots, w_n(x_1, x_2, \dots, x_n))$.

She sends standard forms of multivariate polynomials w_i to Bob. Alice keeps $\mathcal{J}_1$, $\mathcal{J}_2$, L and $a(1), b(1), a(2), b(2), \dots, a(l), b(l), a(l+1)$ as her private secret.

Encryption.

Bob generates his message $p=(p_1, p_2, \dots, p_n)$ from the space of plaintexts $(K^*)^n$. He creates the ciphertext $G(p_1, p_2, \dots, p_n)=c$ and sends it to Alice.

The process of generating G insures that the density of the map is $O(n)$. Each monomial can be computed in time $O(n)$. Thus the complexity of the encryption procedure is $O(n^3)$.

We have a nonlinear map of an unbounded degree such that the computation of its value has the same complexity as the computation of an image of a quadratic map.

Decryption.

Alice receives the message c from Bob. Firstly she computes $b=L^{-1}(c)$. Secondly Alice creates the intermediate tuple $(z_1, z_2, \dots, z_n)$ to study equation $F(z_1, z_2, \dots, z_n)=b$.

She writes the equation

$$\begin{aligned} \lambda_1 z_1^{e(1,1)} &= b_1, \\ \lambda_2 z_1^{e(2,1)} z_2^{e(2,2)} &= b_2, \\ &\dots \\ \lambda_s z_1^{e(s,1)}\ z_2^{e(s,2)} \dots z_s^{e(s,s)} &= b_s \end{aligned} \qquad (5)$$

Alice gets the solution $z_1=d_1$, $z_2=d_2$, ..., $z_s=d_s$.

She computes the parameters $a^*(i)=a(i)(d_1, d_2, \dots, d_s)$ and $b^*(i)=b(i)(d_1, d_2, \dots, d_s)$ for $i=1, 2,\dots, l$.

Alice takes point (b) and computes recurrently

$u_l=\mathcal{J}_{b^*(l)}(b)$, $w_l=N_{a^*(l)}(u_l)$,

$u_{l-1}=\mathcal{J}_{b^*(l-1)}(w_l)$, $w_{l-1}=N_{a^*(l-1)}(u_{l-1})$,

...,

$u_1=\mathcal{J}_{b^*(1)}(w_2)$, $w_1=N_{a^*(1)}(u_1)$,

She computes $z^*=(z^*_1, z^*_2, \dots, z^*_s, z^*_{s+1}, \dots, z^*_n)$ as $\mathcal{J}_d(w_1)$ for $d=(d_1, d_2, \dots, d_s)$.

We can see that z^* is the solution of the system (3).

Alice computes the plaintext p as $(\mathcal{J}_2)^{-1}(\mathcal{J}_l)^{-1}(z^*)$.

Alice computes the inverses of $\mathcal{J}_1$ and $\mathcal{J}_2$ *in* the group ${}^nEG(K)$ as well as the inverse of the map $z_1 \longrightarrow \lambda_1 z_1^{e(1,1)}$, $z_2 \longrightarrow \lambda_2 z_1^{e(2,1)} z_2^{e(2,2)}$, ..., $z_s \longrightarrow \lambda_s z_1^{e(s,1)} z_2^{e(s,2)} \dots\ z_s^{e(s,s)}$ in the group ${}^sEG(K)$ in advance. So the complexity of her decryption procedure can be estimated as $O(n^2)$.

Obfuscation.

Instead of graphs ${}^{i,j}C_{2m}(K)$ Alice takes temporal analogue ${}^{i,j}\mathcal{C}_{2m}(K)^t$ of them. She forms static graphs ${}^{i,j}\mathcal{C}_{2m}(K)^t|t=t^*$ for $t^*=1, 2, \dots, l$.

So she computes each N_b(i) in static graph ${}^{i,j}\mathcal{C}_{2m}(K)^t|t=i$ *during the algorithm execution.*

Illustrating example.

Let us consider the case $(\alpha=1, \beta=0)$.Then graph ${}^{m+1,m}C_{2m}(K)$ known as Double Schubert Graph which has

points $(x)=(x_1, x_2, ..., x_m, x_{1,1}, x_{1,2}, ..., x_{m,m})$ and $[y]=[y_1, y_2, ..., y_m, y_{1,1}, y_{1,2}, ..., y_{m,m}]$ and incidence given by equations $x_{i,j}$-$y_{i,j}=x_iy_j$. We assume that indexes of kind (i,j) are ordered lexicographically.

Alice takes endomorphism $\mathcal{J}_1$ and $\mathcal{J}_2$ of $K[x_1, x_2, ..., ,..., x_m, x_{1,1}, x_{1,2}, ..., x_{m,m}]$.

$\mathcal{J}_1\mathcal{J}_2(x)=(a_1(x_1, x_2, ..., x_m, x_{1,1}, x_{1,2}, ..., x_{m,m}), a_2(x_1, x_2, ..., x_m, x_{1,1}, x_{1,2}, ..., x_{m,m}), ...,$

$a_m(x_1, x_2, ..., x_m, x_{1,1}, x_{1,2}, ..., x_{m,m}),$

$a_{1,1}(x_1, x_2, ..., x_m, x_{1,1}, x_{1,2}, ..., x_{m,m}),$

$a_{1,2}(x_1, x_2, ..., x_m, x_{1,1}, x_{1,2}, ..., x_{m,m}),$

$...,$

$a_{m,m}(x_1, x_2, ..., x_m, x_{1,1}, x_{1,2}, ..., x_{m,m}))=(z_1, z_2, ..., z_m, z_{1,1}, z_{1,2}, ..., z_{m,m})=(z)$ where expressions $a_1, a_2, ..., a_m, a_{1,1}, a_{1,2}, ..., a_{m,m}$ are monomial terms with the coefficients from K^*.

Alice takes graph ${}^{m+1,m}C_{2m}(K[z_1, z_2, ..., z_m, z_{1,1}, z_{1,2}, ..., z_{m,m}])$. She selects colours $a(1), b(1), a(2), b(2), ..., a(l), b(l), a(l+1)$ where $a(i)$ and $b(i)$ are elements of $K[z_1, z_2, ..., z_m, z_{1,1}, z_{1,2}, ..., z_{m,m}]^m$. Element $a(l+1)$ will be chosen as $(\lambda_1 z_1^{e(1,1)}, \lambda_2 z_1^{e(2,1)} z_2^{e(2,2)}, ..., \lambda_s z_1^{e(s,1)} z_2^{e(s,2)} ... z_s^{e(s,s)})$. She computes the destination point of transition $H(a(1), b(1), a(2), b(2), ..., a(l), b(l), a(l+1))$ of the point (z) in the graph ${}^{m+1,m}C_{2m}(K[z_1, z_2, ..., z_m, z_{1,1}, z_{1,2}, ..., z_{m,m}])$. Alice specialise z_i as $a_i(x)$ and $z_{i,j}$ as $a_{i,j}(x)$.

So she computes the composition of $\mathcal{J}=\mathcal{J}_1\mathcal{J}_2$ moving (x) to (z) and $F(a(1), b(1), a(2), b(2), ..., a(l), b(l), a(l+1)$ moving z to $u=(u_1, u_2, ..., u_m, u_{1,1}, u_{1,2}, ..., u_{m,m})$. It is clear that the density of $\mathcal{J}F$ is $O(1)$. Finally Alice selects L from $AGL_n(K)$, $n=(m+1)m$ and computes $(\mathcal{J}F)L=G(x_1, x_2, ..., x_m, x_{1,1}, x_{1,2}, ..., x_{m,m})$ of kind

$x_1 \longrightarrow g_1(x_1, x_2, ..., x_m, x_{1,1}, x_{1,2}, ..., x_{m,m}),$

$x_2 \longrightarrow g_2(x_1, x_2, ..., x_m, x_{1,1}, x_{1,2}, ..., x_{m,m}),$

$...,$

$x_m \longrightarrow g_m(x_1, x_2, ..., x_m, x_{1,1}, x_{1,2}, ..., x_{m,m}),$

$x_{1,1} \longrightarrow g_{1,1}(x_1, x_2, ..., x_m, x_{1,1}, x_{1,2}, ..., x_{m,m}),$

$x_{1,2} \longrightarrow g_{1,2}(x_1, x_2, ..., x_m, x_{1,1}, x_{1,2}, ..., x_{m,m}),$

$...$

$x_{m,m} \longrightarrow g_{m,m}(x_1, x_2, ..., x_m, x_{1,1}, x_{1,2}, ..., x_{m,m}).$

For convenience Alice can rename variables from the list $x_1, x_2, ..., x_m, x_{1,1}, x_{1,2}, ..., x_{m,m}$ as $y_1, y_2, ..., y_m, x_{m+1}, x_{m+2}, ..., x_{m(m+1)}$.

7. Conclusions

In this paper, we present the method of construction of sparce multivariate maps of unbounded degree $O(n)$ with the trapdoor accelerators with the use of walks on algebraic graphs. It uses bipartite cellular Schubert graphs of projective geometries and their analogues defined over the general commutative ring K with the unity. These bipartite graphs can be changed for their temporal analogues defined via the option of a momentum change of the coefficients of monomial terms in the equations defining the incidence of points and lines.

The partition sets of such graphs are affine spaces K^n and K^m. The special walk on the temporal graph over $K[x_1, x_2, ..., x_n]$ can be used for the construction of a multivariate map G from K^n to K^n. The information on the temporal graph and the walk can serve as corresponding trapdoor accelerator T of G, i.e. the knowledge of T allows us to compute the reimages of G. We presented some of these procedures as Algorithm 1 and 4 in the case of graphs ${}^{s,k}C_n(K)$ in terms of Chevalley group over the diagram A_n (case of general linear group). Some other maps with trapdoor accelerators are described in [23] the cases of diagrams B_n, C_n, and D_n.

The first graph-based bijective quadratic public key where constructed in [6]. It uses special cellular Schubert graphs of Projective Geometry over the finite field of characteristics 2. The cryptanalysis for this public key is unknown.

The obfuscation of this cryptosystem is presented in [1]. Recent development in this direction is reflected in [33] where multivariate rules given by quadratic surjective maps and temporal analogues of cellular Schubert graphs can be used.

Another bijective quadratic cryptosystem which is also constructed in terms of Jordan-Gauss graphs is given in [43].

Multivariate cryptosystems with rules of unbounded degree are quite rare. We refer to cryptosystems [42] and [41] defined in terms of extremal Jordan-Gauss graphs over F_q and Z_q.

These multivariate maps have $O(n^4)$ monomial maps. Cryptanalysis for them is still unknown. Presented in this paper cryptosystem is given by multivariate rule with $O(n^2)$ monomial terms. Thus it can be implemented with hundreds of variables, The reduction of the degree of equations to 2 or 3 leads to an essential increase of variables (more than n^2). It makes it unfeasible to use standard methods of symbolic computations for cryptanalytic purposes.

For the implementation of this public key, we select cases $K=F_q$ and $K=Z_q$ where q is a prime power ≥ 128.

Acknowledgments

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

References

[1] V. Ustimenko, Linear Codes of Schubert Type and Quadratic Public Keys of Multivariate Cryptography, IACR e-print archive (2023).

[2] W. Beullens, Improved Cryptanalysis of UOV and Rainbow, Advances in Cryptology – EUROCRYPT 2021, LNCS 12696 (2021) 348–373. doi: 10.1007/978-3-030-77870-5_13.

[3] A. Canteaut, F.-X. Standaert, Eurocrypt 2021, LNCS 12696, 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques (2021). doi: 10.1007/978-3-030-77870-5.

[4] J. Ding, et al., TUOV: Triangular Unbalanced Oil and Vinegar. Algorithm Specifications and Supporting Documentation, ver. 1.0 (2023). URL: https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/TUOV-spec-web.pdf

[5] J. Ding, A. Petzoldt, D. Schmidt, Multivariate Public Key Cryptosystems, Second Edition. Advances in Information Security, Springer (2020).

[6] V. Ustimenko, On Schubert cells in Grassmanians and New Algorithms of Multivariate Cryptography, Proceedings of the Institut of Mathematics, 23(2) (2015) 137–148.

[7] J. Ding, A. Petzoldt, Current State of Multivariate Cryptography, in IEEE Security & Privacy, 15(4) (2017) 28–36. doi: 10.1109/MSP.2017.3151328.
[8] D. Smith-Tone, 2F—A New Method for Constructing Efficient Multivariate Encryption Schemes, in: Proceedings of PQCrypto 2022: The 13th International Conference on Post-Quantum Cryptography, virtual, DC, US (2022).
[9] D. Smith-Tone, New Practical Multivariate Signatures from a Nonlinear Modifier, IACR e-print archive (2021).
[10] D. Smith-Tone, C. Tone, A Nonlinear Multivariate Cryptosystem Based on a Random Linear Code (2019).
[11] J. Dey, R. Dutta, Progress in Multivariate Cryptography: Systematic Review, Challenges, and Research Directions, ACM Computing Survey, 55(12) (2023) 1–34. doi: 10.1145/3571071.
[12] F. Cabarcas, D. Cabarcas, J. Baena, Efficient Public-Key Operation in Multivariate Schemes, Advances in Mathematics of Communications 13(2) (2019).
[13] R. Cartor, D. Smith-Tone, EFLASH: A New Multivariate Encryption Scheme, International Conference on Selected Areas in Cryptography (2018) 281–299.
[14] A. Casanova, et al., Gemss: A Great Multivariate Short Signature, Submission to NIST (2017) 209–229.
[15] J. Chen, et al., A New Encryption Scheme For Multivariate Quadratic Systems, Theoretical Comput. Sci. 809 (2020) 372–383.
[16] M.-S. Chen, et al., SOFIA: MQ-based Signatures in the QROM, IACR International Workshop on Public Key Cryptography, LNCS 10770 (2018) 3–33.
[17] D. H. Duong, et al., An Efficient Multivariate Threshold Ring Signature Scheme, Computer Standards & Interfaces 74 (2021).
[18] J.-C. Faugère, et al., A New Perturbation for multivariate public key schemes such as HFE and UOV, Cryptology ePrint Archive (2022).
[19] M. J. Saarinen, Daniel Tony-Smith, Post Quantum Cryptography, in: 15th International Workshop, PQCrypto 2024, Part 1 (2024).
[20] M. J. Saarinen, DTony-Smith (eds.), Post Quantum Cryptography, 15th International Workshop, PQCrypto 2024, Part 2 (2024).
[21] T. Takagi, et al., International Symposium on Mathematics, Quantum Theory, and Cryptography, Proceedings of MQC 2019, Open Access (2021).
[22] K. Arai, Advances in Information and Communication, Future of Information and Communication Conference (FICC), 1–3 (2024).
[23] V. Ustimenko. Graphs in terms of Algebraic Geometry, Symbolic Computations and Secure Communications in Post-Quantum world, UMCS Editorial House (2022).
[24] B. Sturmfels. Solving Systems of Polynomial Equations. Providence, RI: American Mathematical Soc. (2002).
[25] J. F. Canny, E. Kaltofen, L. Yagati, Solving Systems of Nonlinear Polynomial Equations Faster, ISSAC '89: Proceedings of the ACM-SIGSAM 1989 International Symposium on Symbolic and Algebraic Computation (1989) 121–128. doi: 10.1145/74540.74556.
[26] B. Buchberger, Groebner basis: An Algorithmic Method in Polynomial Ideal Theory, in: Recent Trends in Multidimensional Systems Theory (1985) 184–232.
[27] N. Biggs, Algebraic graphs theory, Second Edition, Cambridge University Press (1993).
[28] A. Brower, A. Cohen, A. Nuemaier, Distance regular graphs, Springer (1989).
[29] B. Bollob´as', Extremal Graph Theory, Academic Press (1978).
[30] F. Buekenhout, Handbook on Incidence Geometry, North Holland (1995).
[31] V. Ustimenko, Maximality of Affine Group, Hidden Graph Cryptosystem and Graph's Stream Ciphers, Journal of Algebra and Discrete Mathematics, 1 (2005) 51–65.
[32] R. W. Carter, Simple Groups of Lie Type, Wiley (1972).
[33] V. Ustimenko, On Schubert cells of Projective Geometry and Quadratic Public Keys of Multivariate Cryptography, IACR e-print archive (2024).
[34] I. Gelfand, R. MacPherson, Geometry in Grassmanians and Generalization 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] V. Ustimenko, On Small World non Sunada Twins and Cellular Voronoi Diagams, Algebra and Discrete Mathematics, 30(1) (2020) 118–142.
[37] T. Adamo, G. Ghiani, E. Guerriero, On Path Ranking in Time-Dependent Graphs, Computers & Operations Research, 135 (2021) 105–446.
[38] M. Noether, Luigi Cremona, Mathematische Annalen, 59 (1904) 1–19.
[39] V. L. Popov, Roots of the Affine Cremona group, Contemporary Mathematics, 369 (2005) 12–13.
[40] V. Ustimenko, On Eulerian Semigroups of Multivariate Transformations and their Cryptographic applications, European J. Math. 9(93) (2023).
[41] V. A. Ustimenko, On New Multivariate Cryptosystems based on Hidden Eulerian Equations, Dopovidi of National Academy of Science of Ukraine, 5 (2017).
[42] V. Ustimenko, On New Multivariate Cryptosystems based on Hidden Eulerian Equations over Finite Fields, IACR e-print archive (2017).
[43] V. Ustimenko, A. Wróblewska, On Extremal Algebraic Graphs, Quadratic Multivariate Public Keys and Temporal Rules, FedCSIS (2023) 1173–1178.