

On Schubert cells of Projective Geometry and quadratic public keys of Multivariate Cryptography

Vasyl Ustimenko^{1,2}

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
E-mail: Vasyl.Ustymenko@rhul.ac.uk*

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 linear equation given in its row-echelon form.

We use families of this graphs for the construction of new quadratic and cubic surjective multivariate maps F of K^n onto K^m (or K^n onto K^n) with the trapdoor accelerators T , i. e. pieces of information which allows to compute the reimage of the given value of F in polynomial time. The technique allows us to use the information on the quadratic map F from K^s to K^r , $s \geq r$ with the trapdoor accelerator T for the construction of other map G from K^{s+rs} onto K^{r+rs} with trapdoor accelerator. In the case of finite field it can be used for construction of new cryptosystems from known pairs (F, 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 (TUOV in particular), for 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, Noncommutative Cryptography, Protocol based cryptosystems

1. Introduction

This paper presents the generalisations of the quadratic multivariate public key given in [1] 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 the standardisation best known quantum resistant algorithms of asymmetrical cryptography. The first round was finished in March 2019, essential part of 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 1922, 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 $F_q[x_1, x_2, \dots, x_n]$ see [14]. Current research in Postquantum Cryptography can be found in [4]-[21].

Each of mentioned above five directions is based on the complexity of selected NP-hard problem.

Multivariate cryptography uses the gap between linearity and nonlinearity. We know that the system of linear equations written over the field F can be solved in time $O(n^3)$ via Jordan-Gauss elimination method. The complexity of solving nonlinear system of constant degree d , $d > 1$ is subexponential

(see [22], [23]). Despite the convenience of Groebner-Shirshov basis method [24] for the implementation the complexity of this algorithm is equivalent to old Gauss elimination method for solution of the system of nonlinear equation. There is standard way to transform of nonlinear system of

equation of degree d , $d > 2$ to equivalent quadratic system via introduction of additional variables and substitutions (see [14]).

So if we have a nonlinear map F of bounded degree d in "general position" which has a trapdoor accelerator T then corresponding cryptosystem is secure. This status is insure the fact that F is given as one way function i. e reimage of F is impossible to compute in a polynomial time without knowledge of the secret T .

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

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

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

Multivariate Cryptography over rings with zero divisors is a brand new area of research.

We use the concept of quadratic accelerator of the endomorphism σ of $K[x_1, x_2, \dots, x_n]$ which is the piece of information T such that its knowledge allows us to compute the reimage of (σ, K^n) in polynomial time $O(n^a)$. 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 $\sigma(x_i)$, $i=1, 2, \dots, n$. Some examples of such public keys the reader can find in [21], [25], [26]. In [26] pairs (σ, T) of quadratic automorphisms σ of $K[x_1, x_2, \dots, x_n]$ and the trapdoor accelerator T where presented for each case (K, n) . These trapdoor accelerator T were defined via totality of special bipartite Jordan-Gauss graphs $D(n, K)$ with the partition sets isomorphic to K^n . We discussed 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 surjective quadratic and cubic multivariate public rules defined in terms of other Jordan-Gauss graphs defined in terms of Projective Geometry and its generalisation on the case of commutative rings K . Many of these public rules are nonbijective maps. Recall that multivariate public rule G has to be given in its standard form $(x_1, x_2, \dots, x_n) \rightarrow (g_1(x_1, x_2, \dots, x_n), g_2(x_1, x_2, \dots, x_n), \dots, g_m(x_1, x_2, \dots, x_n)), n \geq m$ where polynomials g_i are given via the lists of monomial terms in the lexicographical order.

The interest to surjective pairs (G, T) is justified by the fact that they can provide the shortest known digital signatures. The scheme is the following one.

Let us assume that Alice and Bob use some cipher for the communication. Alice use this cipher to send the ciphertext c which Bob is able to decrypt and get the corresponding plaintext p .

Alice and Bob share some hash function h . So they have common value $h(p)$. Size of $h(p)=d=(d_1, d_2, \dots, d_m)$ is m . It is essentially smaller than the size of the plaintext. Bob has the system of equations $g_i(z_1, z_2, \dots, z_n) = d_i, i=1, 2, \dots, m$. To sign the plaintext Alice has to send via open channel the solution of this system to Bob. She uses her knowledge on the trapdoor accelerator T to compute the solution $v=(v_1, v_2, \dots, v_n)$. Alice sends it via the open channel to Bob. He checks that $G(v)=d$.

In Section 2 we introduce the concept of linguistic graphs defined over commutative ring K together with the algorithm of generation of graph based polynomial map F and corresponding trapdoor accelerator T . Multivariate Cryptography requires polynomial maps which can be considered as good approximation of ‘‘map in general position’’. So instead of graphs given by equations we consider their temporal analogue for which there is an option to change the coefficients of equations in selected moment of time. For this selections some pseudorandom or genuinely random sequences can be used. We hope that special walks in temporal linguistic graphs can be used for the construction of (F, T) for which adversary is practically unable to compute the reimage of F without the knowledge of T which contains the sequence of ‘‘static’’ graphs given by the numerical values of coefficients.

In the case of special linguistic graphs of Jordan-Gauss type we can construct of corresponding to them maps of selected degree (2 or 3). In Section 2 these ideas are illustrated in the case of Jordan graphs $X^{s,r}(K)$ and $X^{s,r,k}(K)$.

In Section 3 construction of pairs (F, T) is illustrated in the case $K=F_q$ and graphs $X^{s,r,k}(K)$. Our Algorithm 1 or Algorithm 2 allows us to expand selected pair G, T where G is the polynomial map of K^n onto K^m and T and get the new pair F, T' such that F maps K^{n+k} onto K^{m+k} and T' is an expansion of T .

As example of known (G, T) one can take the cryptosystem TOUV.

This expansion operations on trapdoor accelerators can be used iteratively (see Algorithm 3 with the output defined over arbitrary commutative rings).

Section 4 is dedicated to description of Cellular Schubert Schubert graphs and corresponding digital signatures algorithms. This class of Jordan-Gauss graphs contains graphs $X^{s,r}(K)$. Algorithms 4 is able to produce interesting maps with trapdoor accelerators defined over general commutative ring K .

In Section 4 we describe some protocols of Noncommutative Cryptography based on the semigroup platform of polynomial transformations and discuss the idea of secure delivery of quadratic multivariate rule from one user to other one.

Section 5 contains conclusive remarks. We discuss heuristic arguments on security of suggested cryptosystems.

2. Linguistic and Jordan graphs, their temporal analogs and trapdoor accelerators.

Another The missing definitions of graph-theoretical concepts and incidence systems theory which appear in this paper can be found in [27], [28], [29] and [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 vGu for the adjacent vertexes u and v (or neighbours). We refer to $|\{x \in V(G) \mid xGu\}|$ 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.

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

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

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

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

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

Let $X_n(F)$ be one of the Chevalley groups over the Coxeter -Dynkin diagram X_n which coincides with $A_n, B_n, C_n, D_n, E_6, E_7, E_8, F_4, G_2$; F is the field; and B is the Borel subgroup of this group (see [28], [32]). Assume that $G_n = G(X_n(F))$ stands for the geometry of $X_n(F)$, which is the disjoint union of the totalities iG of left cosets of the standard maximal parabolic subgroups P_i , $i = 1, 2, \dots, n$ of this group with the natural incidence relations $I = I_n(F)$ (see [28], [31]). The type $t(v)$ of kind $v = gP_i$ is i . It follows immediately from the results in [33], [34], [35] that the nonempty restriction of the binary relations I on the disjoint union of two largest orbits iC and jC , $i \neq j$ of the Borel subgroup B on iG and jG respectively is isomorphic to some Jordan-Gauss graph ${}^{i,j}C_n(F)$. We refer to this graph as a cellular Schubert graph over F . Applications of some special cellular Schubert graphs to constructions of multivariate public keys and cryptosystems of Noncommutative Cryptography can be found in [36], [37], [38], [21].

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. Let ${}^{i,j}C_n^0(K)$ stand for the Jordan-Gauss graph defined over K which is equivalent to ${}^{i,j}C_n(F)$ for which $a_i = b_i = 1$ and each monomial term of f_i , $i = 1, 2, \dots, m$ has coefficient 1.

We define a temporal (depending on time) Jordan-Gauss graph $\Gamma(K)^t$ of symbolic type S as the family of equivalent Jordan-Gauss graphs $\Gamma(K)^t$, $t = 1, 2, \dots$ 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 ${}^j a(i, k) x_i y_k$,

$x_i y_k \in \mathcal{S}$ $\quad j a(i, k) = j a(i, k)(t) \neq 0$. Some examples of temporal Jordan-Gauss graphs can be found in [39]. In contrast to the definition of time dependent graphs of [40], we introduce Jordan-Gauss temporal graphs via time dependent equations.

We define walks on the temporal Jordan-Gauss graph and use them for the construction of multivariate public keys, protocols and cryptosystems. In this paper we will concentrate on the case $X_n = A_n$ where the cellular Schubert graphs ${}^{i,j}C_n(\mathcal{F})$ introduced above are symbolically equivalent to the induced subgraphs of the geometry $\mathcal{G}(A_n(F))$ over the field F , i.e. the n -dimensional projective geometry of all nonempty subspaces of F^{n+1} .

Finite projective geometries were traditionally used for the construction of algorithms of Coding Theory [41]. Their applications to other areas of Information Security have been published (see [42], [43] devoted to Network Coding). In particular, it was used in Cryptography (see [44], where projective geometry were used for authentication protocols). Nowadays finite geometries are widely used as tools for secret sharing.

Additionally they can be used for the design of some stream ciphers of multivariate nature and protocols of Noncommutative Cryptography (see [21] and further references).

In this case the graph ${}^l, n C_n^0(K)$ is a bipartite graph of points (x_1, x_2, \dots, x_n) and lines $[y_1, y_2, \dots, y_n]$ with incidences given by equations: $x_n - y_n = x_1 y_1 + x_2 y_2 + \dots + x_{n-1} y_{n-1}$.

This is symbolically equivalent to the ${}^l, n C_n(K')$ 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: $a x_n - b y_n = a_1 x_1 y_1 + a_2 x_2 y_2 + \dots + a_{n-1} y_{n-1}$, where a and b are elements of the multiplicative group of K' and $a_i \neq 0, i = 1, 2, \dots, n-1$.

In another example, the graph ${}^s, s+1 C_{s+r+1}^0(K)$ can be interpreted as a bipartite graph consisting of points of the form $(x_1, x_2, \dots, x_s, x_{1,1}, x_{1,2}, \dots, x_{s,r})$ and lines $[y_1, y_2, \dots, y_r, y_{1,1}, y_{1,2}, \dots, y_{s,r}]$, with the incidence condition given by the equations:

$$x_{i,j} - y_{i,j} = x_i y_j, \quad i = 1, 2, \dots, s, \quad j = 1, 2, \dots, r.$$

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:

$a_{i,j} x_{i,j} - b_{i,j} y_{i,j} = d_{i,j} x_i y_j$, 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 ${}^l, n C_n(K)$ 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.

We will use walks on graphs ${}^{i,k} C_n(K)$ in the general case of parameters i and k , and walks on their temporal analogues ${}^{i,k} C_n(K)^t$ for the creation of quadratic and cubic transformations of affine spaces over K and

studies of their cryptographic applications. For practical implementation, we will use cases when K is a finite field of characteristic 2 or arithmetical rings of order $2^t, t > 2$.

Let us consider basic operators on the set of vertexes of Jordan-Gauss graph of type (s, r, m) .

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

For each $b \in K^r$ and $p=(p_1, p_2, \dots, p_{s+m})$ there is the unique neighbour of the point $[l]=N_b(p)$ with the colour b . Similarly, for each $c \in K^s$ and line $l=[l_1, l_2, \dots, l_{r+m}]$ 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 colour jump operators $J=J_b(p)=(b_1, b_2, \dots, b_s, p_1, p_2, \dots, p_{s+m})$, where $(b_1, b_2, \dots, b_s) \in K^s$ and $J=J_b([l])=[b_1, b_2, \dots, b_r, l_1, l_2, \dots, l_{r+m}]$, where $(b_1, b_2, \dots, b_r) \in K^r$.

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

$$v_1=J_{a(1)}(v), u_1=N_{b(1)}(v_1),$$

$$v_2=J_{a(2)}(v_1), u_2=N_{b(2)}(v_2),$$

....,

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

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

For each Jordan-Gauss graph $\Gamma(K)$ we consider

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

We take an odd parameter $l, l > 2$, special point $z=(z_1, z_2, \dots, z_{m+s})$ and apply the transition $H(a(1), b(1), a(2), b(2), \dots, a(l), a(l+1))$ to the vertex z of the graph Γ' such that coordinates of $a(i), b(i)$ are elements of $K[[z_1, z_2, \dots, z_s]$. The image of z will be the tuple $u=(a(l+1)_1(z_1, z_2, \dots, z_s), a(l+1)_2(z_1, z_2, \dots, z_s), \dots, a(l+1)_r(z_1, z_2, \dots, z_s), f_1(z_1, z_2, \dots, z_{m+s}), f_2(z_1, z_2, \dots, z_{m+s}), \dots, f_m(z_1, z_2, \dots, z_{m+s}))$. Let F be a polynomial map of K^{m+s} to K^{m+r} sending $(z_1, z_2, \dots, z_{m+s})$ to $(u_1, u_2, \dots, u_{m+s})=u$.

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

Additionally we consider the above presented construction in the case of even parameter l . Then $a(l+1)$ is an element of $K[x_1, x_2, \dots, x_s]^s$, u_{l+1} and v_{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 [21]. Let us assume that the surjective map (z_1, z_2, \dots, z_s) to $(a(l+1)_1, a(l+1)_2, \dots, a(l+1)_t)$ where $t=r$ or $t=s$ has a trapdoor accelerator T .

Then the knowledge on $\Gamma(K)$ and tuples $a(1), b(1), a(2), b(2), \dots, a(l), b(l)$, transformations L_1, L_2 and T is a trapdoor accelerator of the standard form of G mapping

$$K^{m+s} \text{ on } K^{m+t}.$$

Proposition 2 [21]. Let us assume that condition of the Proposition 1 hold and $\Gamma(K)$ coincides with the Jordan-Gauss graph ${}^{ij}C_n(K)$, $\deg(a(i))+\deg(b(i))=d, d > l$ for

$i=1,2,\dots, l$ and $l \leq \deg(a(l+1)) \leq d$. Then map G is a surjective transformation of K^{m+s} onto K^{m+l} of degree d .

REMARK 2. 1. We can change graphs $\Gamma(K)$ and ${}^{ij}C_n(K)$ for their temporal analogues $\Gamma(K)^t$, ${}^{ij}C_n(K)^t$ and think that operators $N_b(i)$ in the procedure executes in the static graph corresponding time parameter $i, i=1, 2,\dots,l$. Then conclusions of Proposition 1 and Proposition 2 will hold.

Let Propositions 1' and 2' be analogues of two written above statements for the case of temporal graphs.

REMARK 2. 2. The case $d=2, 3$ of Proposition 2 and 2' will be used further for the construction of quadratic public keys.

Justification of Proposition 1'

Let us assume that $\Gamma(K)$ is temporal graph and its static graphs Γ_i in time $i=1, 2, \dots, l$ are known as well as $a(1), b(1), a(2), b(2), \dots, a(l), b(l), a(l+1), T$ 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 $p=(p_1, p_2, \dots, p_s, p_{s+1}, p_{s+2}, \dots, p_{s+m})$ of variables p_i and consider the equation $H(p)=c$ where $H=H(a(1), b(1), a(2), b(2), \dots, a(l), a(l+1))=(a(l+1)_1, a(l+1)_2, \dots, a(l+1)_b, h_1, h_2, \dots, h_m)$, where $h_i \in K[x_1, x_2, \dots, x_{s+m}]$.

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

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

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 $r=l$ then the reimage reimage z^* is uniquely defined.

3. Examples of multivariate cryptosystem.

Algorithm 1.

Let $K=F_q$. We take temporal analogue $X^{s,r}(K)$ of Jordan-Gauss graph

${}^{s,s+l}C_{s+r+l}(K)$ with points $(x_1, x_2, \dots, x_s, x_{1,1}, x_{1,2}, \dots, x_{s,r})$ and lines $[y_1, y_2, \dots, y_r, y_{1,1}, y_{1,2}, \dots, y_{s,r}]$, with the incidence condition given in the time interval $t=1, 2, \dots, l$ by the equations: ${}^t a_{i,j} x_{i,j} - {}^t b_{i,j} y_{i,j} = {}^t d_{i,j} x_i x_j$, where elements ${}^t a_{i,j}$, ${}^t b_{i,j}$ and ${}^t d_{i,j}$ are elements from $F_q \setminus \{0\}$.

She uses the pseudorandom sequence to generate $3l(rs)^2$ nonzero coefficients of the equations. So, Alice is able to compute the neighbour ${}^t N_b(v)$ of the selected color b from $K^s UK^r$ of the vertex v of static graph ${}^t X^{s,r}(K)$ in given time $t=t^* \in \{1, 2, \dots, l\}$.

Let us assume that l is odd. In the simplest case she selects linear tuples $a(1), b(1), a(2), b(2), \dots, a(l), b(l)$ of kind

$$\begin{aligned} a(i) &= ({}^i a_{11} z_1 + {}^i a_{12} z_2 + \dots + {}^i a_{1s} z_s, {}^i a_{21} z_1 + {}^i a_{22} z_2 + \dots + {}^i a_{2s} z_s, \dots, \\ &{}^i a_{s1} z_1 + {}^i a_{s2} z_2 + \dots + {}^i a_{ss} z_s), \quad i=1, 3, \dots, l, \\ b(i) &= ({}^i a_{11} z_1 + {}^i a_{12} z_2 + \dots + {}^i a_{1s} z_s, {}^i a_{21} z_1 + {}^i a_{22} z_2 + \dots + {}^i a_{2s} z_s, \dots, \end{aligned}$$

$$\begin{aligned}
& {}^i a_{r1z_1} + {}^i a_{r2z_2} + \dots + {}^i a_{rsz_s}, \quad i=2, 4, \dots, l-1, \\
& b(i) = ({}^i b_{11z_1} + {}^i b_{12z_2} + \dots + {}^i b_{1sz_s}, {}^i b_{21z_1} + {}^i b_{22z_2} + \dots + {}^i b_{2sz_s}, \dots, \\
& {}^i a_{r1z_1} + {}^i a_{r2z_2} + \dots + {}^i a_{rsz_s}), \quad i=1, 3, \dots, l, \\
& b(i) = ({}^i b_{11z_1} + {}^i b_{12z_2} + \dots + {}^i b_{1sz_s}, {}^i b_{1z_1} + {}^i b_{22z_2} + \dots + {}^i b_{2sz_s}, \dots, \\
& {}^i b_{s1z_1} + {}^i b_{s2z_2} + \dots + {}^i b_{ssz_s}), \quad i=2, 4, \dots, l-1.
\end{aligned}$$

Alice may use selected pseudorandom sequence to generate

Written above coefficients ${}^i a_{km}$ or ${}^i b_{km}$ from the field F_q .

She may take the public key of TUOV system of kind

$(z_1, z_2, \dots, z_s) \rightarrow (a_1, a_2, \dots, a_r)$ where a_i are quadratic polynomials from $K[z_1, z_2, \dots, z_s]$ and set $a(l+1) = (a_1, a_2, \dots, a_r)$. Alice takes this map together with corresponding trapdoor accelerator T .

Alice forms map $H = H(a(1), b(1), a(2), b(2), \dots, a(l), b(l), a(l+1))$ from K^{sr+s} onto K^{sr+r} .

She selects L_1 from $AGL_{rs+s}(F_q)$ and L_2 from $AGL_{rs+r}(F_q)$ and computes the standard form $G = L_1 H L_2$ given by polynomials $g_i, i=1, 2, \dots, rs+r$ written in their standard forms. Alice announces

$(z_1, z_2, \dots, z_{rs+s}) \rightarrow (g_1(z_1, z_2, \dots, z_{rs+s}), g_2(z_1, z_2, \dots, z_{rs+s}), \dots, g_{rs+r}(z_1, z_2, \dots, z_{rs+s}))$ as the public rule.

Let us consider the complexity estimates of the described procedures. We assume that $r=n, s=O(n), s>r$ and $l=O(n^e), 0 < e \leq 2$. Then the dimension m of the space K^{r+ms} is $O(n^2)$.

Recall that Alice and Bob use some cipher for the communication. Alice sends the ciphertext c and Bob decrypts it. So both of them have the plaintext p .

Alice and Bob share some hash function h and $h(p)$. Size of $h(p) = d = (d_1, d_2, \dots, d_{sr+r})$ is $r+m = O(n^2)$. It is essentially smaller than the size of the plaintext p . Bob has the system of equations $g_i(z_1, z_2, \dots, z_{sr+s}) = d_i, i=1, 2, \dots, sr+r$. To sign the corresponding to c plaintext Alice has to send via open channel the solution of this system to Bob.

She uses the procedure in the justification of the Proposition 1.

Alice computes $(L_2)^{-1}$ in time $O(m^2) = O(n^4)$.

She uses the trapdoor T for TUOV to solve

$a_i(z_1, z_2, \dots, z_s) = d_i, i=1, 2, \dots, r$ in time $O(n^2)$.

The computation of parameters $a^*(j), b^*(l), l=1, 2, \dots, l-1$ takes $O(n^{2+e})$.

Note that the application of jump operator J_a where $a \in K$ costs $O(n)$. The computation of the neighbour of the vertex of the static Jordan-Gauss graph ${}^{t^*}X^{s,r}(K)$ costs $O(m) = O(n^2)$. So Alice computes the value of $H(b^*(l), a^*(l), b^*(l-1), a^*(l-1), b^*(1), a^*(1), d)$ in time $O(n^{2+e})$.

Computation of the value of $(L_1)^{-1}$ costs $O(m^2)$.

It means that for $e \leq 2$ the computation of the signature Alice need $O(m^2) = O(n^4)$ elementary operations.

Bob verifies the signature of Alice in time $O(m^3)$ via substitution of the coordinates of the message into m multivariate equations from $O(m)$ variables.

REMARK 3.1. Alice can take some pairs of $(a(i), b(i))$, $i=1,2,\dots, l$ such that minimal degree of a is 0 and maximal degree of elements of the pair is 2. This modification does not affect the complexity of the execution.

Noteworthy that instead of the chosen above map $a(l+1)$ one can take other known trapdoor accelerators for which the cryptanalysis is already known. For instance in the paper [36] the case of finite fields of characteristic 2 the Imai-Matsumoto encryption scheme were selected (see [45]). The case $s=r$ was implemented in the of static Jordan-Gauss graphs $X^{s,s}(F_q)$ known as double Schubert graphs and $b(i)=a(i+1)$, $i=1, 2,\dots, l-1$.

The computer experiment justify that the density of the quadratic map, i.e. number of nonzero coefficients in the standard form with m variables is $O(m^3)$. So it is close to the case of the map in general form when we have the density of kind $1/2m^2(m-1)+O(v^2)$. The cryptanalysis of the implemented case is still unknown.

REMARK 3. 2. Instead of trapdoor accelerators one can take a quadratic map for which the procedure of reimage is obvious. For example in the case of F_q , $q>2$ of characteristic 2 one can take the map $(z_1, z_2, \dots, z_s) \rightarrow (l_1(z_1, z_2, \dots, z_s)^2, l_2(z_1, z_2, \dots, z_s)^2, \dots, l_r(z_1, z_2, \dots, z_s)^2)$ where linear forms l_i define linear map of rank r . Elements L_1 and L_2 of general form will hide the selected quadratic map. Other example can be found in [25].

The modification of the cryptosystem.

Let us consider some subset J of the Cartesian product C of $\{1,2,\dots, s\}$ times $\{1,2,\dots,r\}$ such that $C-J$ contains at least s elements.

Let us consider the deletion $\Delta(J)$ of coordinates of points

$(x_1, x_2, \dots, x_s, x_{1,1}, x_{1,2}, \dots, x_{s,r})$ and lines $[y_1, y_2, \dots, y_r, y_{1,1}, y_{1,2}, \dots, y_{s,r}]$ of $X^{s,r}(K)$ with the indexes from J

together with corresponding equations.

If the cardinality of $S-J$ is k then $\Delta(J)$ defines the homomorphism of $X^{s,r}(K)$ onto Jordan-Gauss graph $X^{s,r,k}(K)$ of type (s, r, k) .

Algorithm 2. We can consider the modification of Algorithm 1 via the use of $X^{s,r,k}(K)$ instead of $X^{s,r}(K)$.

The output will be the map G of kind $(z_1, z_2, \dots, z_{s+k}) \rightarrow (g_1(z_1, z_2, \dots, z_{s+k}), g_2(z_1, z_2, \dots, z_{s+k}), \dots, g_{r+k}(z_1, z_2, \dots, z_{s+k}))$.

If k is $O(n^2)$ then the complexity of the procedures for Alice to make the digital signature will be the same with the case of Algorithm 1.

When the size of k is $O(n)$ then the choice $e=1$ leads to the complexity $O(n^2)$.

REMARK 3. 3. We can used the Proposition 2 and 2' in the case of $d=3$ for creation of the cubical multivariate public rules instead of quadratic maps of Algorithm 1 and 2. Another option is the substitution of graphs ${}^{ij}C_n(K)$ instead of $X^{s,r}(K)$ in the case of Algorithm 1.

Linear algebra over the commutative rings K with zero divisors is heavily depending on the choice of K . So quadratic multivariate public keys over the general commutative rings are interesting.

Algorithm 3. Alice takes the temporal graph $\Gamma(0)={}^{ij}C_n(K)$ of type (s, r, m) and ${}^0a(1), {}^0b(1), {}^0a(2), {}^0b(2), \dots, {}^0a(l(0)), {}^0b(l(0))$ from $K[z_1, z_2, \dots, z_s]^s UK[z_1, z_2, \dots, z_s]^r$

satisfying conditions of Proposition 2' for $d=2$. She selects surjective map ${}^0a(l+1)$ of K^s onto K^r of degree 1 and form map $H_{\Gamma(0)}({}^0a(1), {}^0b(1), {}^0a(2), {}^0b(2), \dots, {}^0a(l(0)), {}^0b(l), {}^0a(l(0)+1))$ together with ${}^0G = {}^0L_1 H_{\Gamma(0)} {}^0L_2$ where ${}^0L_1 \in AGL_{s+m}(K)$ and ${}^0L_2 \in AGL_{r+m}(K)$. So, Alice computes the standard form of the map 0G of K^{s+m} onto K^{r+m} . She identifies 0G with the corresponding tuple $(g_1, g_2, \dots, g_{r+m})$ from $K[z_1, z_2, \dots, z_s]^r$

Alice takes temporal graphs $\Gamma(1) = X^{s+m, r+m, m(1)}(K)$, $m(1) \geq s+m$,

$\Gamma(2) = X^{s+m+m(1), r+m+m(1), m(2)}(K)$, $m(2) \geq s+m+m(1), \dots$, $\Gamma(n) = X^{s+m+m(1)+m(2)+\dots+m(n-1), r+m+m(1)+m(2)+\dots+m(n-1), m(n)}(K)$, $m(n) \geq s+m+m(1)+\dots+m(n-1)$.

She selects odd parameter $l(1), l(2), \dots, l(n)$ together with

1L_1 from $AGL_{s+m+m(1)+\dots+m(i)}(K)$ and 1L_2 from $AGL_{r+m+m(1)+\dots+m(i)}(K)$.

Alice forms ${}^1G = {}^1L_1 H_{\Gamma(1)} {}^1L_2$ where $H_{\Gamma(1)} = H_{\Gamma(1)}({}^1a(1), {}^1b(1), {}^1a(2), {}^1b(2), \dots, {}^1a(l), {}^1b(l), {}^0G)$ for ${}^1a(1), {}^1b(1), {}^1a(2), {}^1b(2), \dots, {}^1a(l), {}^1b(l)$ satisfying conditions of Proposition 2.

She computes ${}^2G = {}^2L_1 H_{\Gamma(2)} {}^2L_2$ where $H_{\Gamma(2)} = H_{\Gamma(2)}({}^2a(1), {}^2b(1), {}^2a(2), {}^2b(2), \dots, {}^2a(l), {}^2b(l), {}^1G)$ for ${}^2a(1), {}^2b(1), {}^2a(2), {}^2b(2), \dots, {}^2a(l), {}^2b(l)$ satisfying conditions of Proposition 2.

Alice continues this recurrent process and constructs

${}^nG = {}^nL_1 H_{\Gamma(n)} {}^nL_2$ where $H_{\Gamma(n)} = H_{\Gamma(n)}({}^n a(1), {}^n b(1), {}^n a(2), {}^n b(2), \dots, {}^n a(l), {}^n b(l), {}^{n-1}G)$ for ${}^n a(1), {}^n b(1), {}^n a(2), {}^n b(2), \dots, {}^n a(l), {}^n b(l)$ satisfying conditions of Proposition 2.

So she uses standard form of nG and the trapdoor accelerator T which is the information on static graphs of temporal graphs $\Gamma(j)$, $j=0, 1, 2, \dots, n$ on time intervals $I, 2, \dots, l(j)$ together with sequences ${}^0a(1), {}^0b(1), {}^0a(2), {}^0b(2), \dots, {}^0a(l(0)), {}^0b(l(0)), {}^0a(l(0)+1), {}^i a(1), {}^i b(1), {}^i a(2), {}^i b(2), \dots, {}^i a(l), {}^i b(l(i))$, $i=1, 2, \dots, n$ and affine transformations ${}^iL_1, {}^iL_2$ for $i=1, 2, \dots, n$.

REMARK 3. 4.. The construction of trapdoor accelerator for some bijective quadratic transformation G of affine space K^n is presented in [46]. It is based on well known Jordan-Gauss graph $D(n, K)$ of type $(1, 1, n-1)$. This cryptosystem is implemented in the cases $K=Z_q$ and $K=F_q$, $q=2^l$, $l=7, 8, 16$.

The map G together with the corresponding trapdoor accelerator T can be used as $\Gamma(0)$ of presented above iterative construction.

The detailed description of graphs ${}^iC_n(K)$ is given in the next section.

4. Schubert cellular graphs over the fields and commutative rings and their applications.

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 $t(W)=dim(W)$, $W \in {}^{n-1}PG(F_q)$ and incidence relation I defined by the condition $W_1 I W_2$ if and only if one of these subspaces is embedded in another one. We can select standard base e_1, e_2, \dots, e_n of V and identify ${}^{n-1}PG(F_q)$ with the totality of linear codes in $(F_q)^n$. The geometry ${}^{n-1}\Gamma(q) = {}^{n-1}PG(F_q)$ is a partition of subsets ${}^{n-1}\Gamma(q)_i$ consisting of elements of selected type i , $i=1, 2, \dots, n-1$. We assume that each element of V is presented in the chosen base as

column vector (x_1, x_1, \dots, x_n) . Let U stands for the unipotent subgroup of automorphism group $PGL_n(F_q)$ consisting of lower unitriangular matrices.

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 $e_{i(1)}, e_{i(2)}, \dots, e_{i(m)}$. So the number of orbits of $(U, \Gamma_m(F_q))$ equals to binomial coefficient C_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 $x_{i,j}(t)$, $i < j$, $t \in F_q$. 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 $\{1, 2, \dots, n\} = N$, ${}^J S$ be Schubert cell containing symplectic subspace W_J spanned by e_j , $j \in J$, $\Delta(J) = \{(i, j) \mid i \in J, j \in N - J, i < j\}$. Then a subgroup $U(J)$ generated by root subgroups $U_{i,j}$, $(i, j) \in \Delta(J)$ of order q^k , $k = |\Delta(J)|$ acts regularly on ${}^J S$. It means that we can identify ${}^J S$ and $U(J)$. Noteworthy that each $\Gamma_m(F_q)$ has a unique largest Schubert cell of size $q^{m(n-m)}$, it is ${}^J S$ for $J = \{n, n-1, n-2, \dots, n-m+1\}$. We denote this cell as ${}^m LS(F_q)$. We consider the bipartite graph ${}^{m,k} I_n(F_q)$ of the restriction of I onto disjoint union ${}^m LS(F_q)$ and ${}^k LS(F_q)$. It is bipartite graph with bidegrees q^r and q^s of type (r, s, p) where $r = |\Delta(\{n, n-1, n-2, \dots, n-m+1\}) - \Delta(\{n, n-1, n-2, \dots, n-m+1\}) \cap \Delta(\{n, n-1, n-2, \dots, n-k+1\})|$ and $s = |\Delta(\{n, n-1, n-2, \dots, n-k+1\}) - \Delta(\{n, n-1, n-2, \dots, n-m+1\}) \cap \Delta(\{n, n-1, n-2, \dots, n-k+1\})|$, $p = |\Delta(\{n, n-1, n-2, \dots, n-m+1\}) \cap \Delta(\{n, n-1, n-2, \dots, n-k+1\})|$. We refer to the graph of binary relation ${}^{m,k} I_n(F_q)$ as Cellular Schubert graph and denote it as ${}^{m,k} C_n(F_q)$ graph. In particular case $n = 2m+1$, $k = m$ these graphs are known as Double Schubert graphs [38].

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 $f: \Delta \rightarrow K$ 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 $\{1, 2, \dots, n\}$ we define $U(J)$ as totality of matrices $M = (m_{i,j})$ from U such that $(i, j) \in \Delta - \Delta(J)$ implies that $m_{i,j} = 0$. We define incidence system ${}^{n-1} PG(K)$ as a totality of pairs (J, M) , $M \in U(J)$ with type function $t(J, M) = |J|$ and incidence relation given by conditions $({}^1 J, {}^1 M) I ({}^2 J, {}^2 M)$ if and only if one of subsets ${}^1 J$ and ${}^2 J$ is embedded in another one and ${}^1 M \cdot {}^2 M \mid \Delta({}^1 J) \cap \Delta({}^2 J) = {}^1 M \cdot {}^2 M \cdot {}^1 M$. 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 [47], [48].

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

We refer to disjoint union of ${}^m LS(K)$, $m = 1, 2, \dots, n-1$ 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 .

Let $\Gamma = \Gamma(K)^l$ be the temporal linguistic graph of type (s, r, m) and $H(a(1), b(1), a(2), b(2), \dots, a(l), b(l), a(l+1))$ is its even transition i. e. parameter l is even. The composition of two even transitions is well defined. They are elements of Cremona semigroup ${}^{s+m}CS(K)$ of endomorphisms of $K[z_1, z_2, \dots, z_s, z_{s+1}, z_{s+2}, \dots, z_{s+m}]$. Each endomorphism F can be identified with the tuple of its values on variable $(F(z_1), F(z_2), \dots, F(z_{s+m}))$. We define $deg(F)$ as maximal of degrees $F(z_i)$, $i=1, 2, \dots, m+s$.

Proposition 3 [21].

Let $\Gamma = {}^{m,k}C_n(K)^l$ and d is some constant >1 . Then the totality of even transitions of kind $H(a(1), b(1), a(2), b(2), \dots, a(l), b(l), a(l+1))$ such that $deg(a(i)) + deg(b(i)) = d$, $d > 1$ for $i=1, 2, \dots, l$ and $deg(a(l+1)) = 1$ generates semigroup ${}^dS(\Gamma(K)^l)$ of nonlinear polynomial transformations of ${}^mLS(K)$ of maximal degree d .

REMARK 4.1. Elements of kind $H(a(1), b(1), a(2), b(2), \dots, a(l), b(l), a(l+1))$ satisfying conditions of Proposition 3 with the bijective $a(l+1)$ form a subgroup ${}^dG(\Gamma(K)^l)$ of ${}^dS(\Gamma(K)^l)$.

REMARK 4.2. Propositions 3 holds for the case $\Gamma = X^{s,r,k}(K)$

Subsemigroups ${}^dS(\Gamma(K)^l)$, $\Gamma(K)^l = {}^{m,k}C_n(K)^l$ are very special large subgroups of the corresponding affine Cremona semigroup ${}^pCS(K)$, $p = m(n-m)$ because of the product of two elements from ${}^pCS(K)$ of degree d in general position will have degree d^2 but the product of two elements of degree 2 from ${}^dS(\Gamma(K)^l)$ will be of degree at most d .

It means that the composition of two representatives of ${}^2S(\Gamma(K)^l)$ will be computed in time $O(p^7)$ and this noncommutative semigroup subsemigroup can be used as platform for the implementation of classical protocols of Noncommutative Cryptography (see [49]). We illustrate this fact in the case of following twisted Diffie-Hellman protocol.

Assume that correspondents Alice and Bob agree to use known noncommutative semigroup S which has invertible elements. They agree on non commuting elements h and invertible g from S via the communication through open channel. Alice chooses positive integers $k(A), r(A)$. Bob selects his $k(B), r(B)$. Alice sends $g^{r(A)}h^{k(A)}g^{-r(A)} = g_A$ to Bob. He sends $g^{r(B)}h^{k(B)}g^{-r(B)} = g_B$ to Alice. They compute the collision map G as $g^{r(A)}(g_B)^{k(A)}g^{-r(A)}$ and $g^{r(B)}(g_A)^{k(B)}g^{-r(B)}$.

The security of this scheme rests on the complexity of Conjugacy Power Problem. Adversary has to solve one of the equations $g^y h^x g^{-y} = g_A$ or $g^y h^x g^{-y} = g_B$.

In the case when S is subsemigroup of affine Cremona semigroup of endomorphisms of $K[x_1, x_2, \dots, x_p]$, $K = F_q$ or $K = Z_q$ where q is prime power >2 and elements g, h are given in their standard forms the Conjugacy Power Problem is NP-hard. So Alice can use $S = L {}^2S(\Gamma(K)^l) L^{-1}$ where $L \in AGL_p(K)$. She generates g and h as conjugates of elements of kind $H(a(1), b(1), a(2), b(2), \dots, a(l), b(l), a(l+1))$ of Prop-

osition 3. Alice computes their standard forms and sends them via open channel to Bob.

After the execution of this variant of the protocol Alice and Bob share large array of $O(p^3)$ coefficients of the standard form of G .

Alice can create multivariate rule F as output of Algorithm 1 given as tuple of polynomials $(f_1, f_2, \dots, f_{r+rs})$ where

$f_i \in K[x_1, x_2, \dots, x_{s+rs}]$ with trapdoor accelerator T .

Alice and Bob executes the twisted Diffie-Hellman protocol in the case of $S = {}^2S(\Gamma(K)^t)$, $\Gamma(K)^t = X^{r,s}(K)^t$ and elaborate

G given by the tuple $(g_1, g_2, \dots, g_{s+rs})$. Alice can deliver the map F safely via sending $(f_1 + g_1, f_2 + g_2, \dots, f_{r+rs} + g_{r+rs})$ to her partner Bob.

Alice and Bob can use session of the protocol and transmission of multivariate encryption tools periodically.

We will continue studies of symbiotic combinations of multivariate encryption tools with the various protocols of Noncommutative Cryptography with platforms which are subsemigroups of affine Cremona semigroups over various finite commutative rings. Examples of such protocols are given in [50].

In the section 2 we stated that in Algorithm 1 graph $X^{s,r}$ can be substituted by Jordan-Gauss graph ${}^{m,k}C_n(K)^t$ of type (s, r, p) .

For simplicity we assume that $K = F_q$ and the map B given by

the tuple $a(l+1)$ of quadratic multivariate polynomials has the trapdoor accelerator T which allows us to compute the reimage of B in time $O((s+p)^2)$. We assume that odd parameter l has size $O(n)$ and parameters m and k are in general position and consider this obfuscated version of Algorithm 1.

Algorithm 4.

Alice selects parameter n , constants α and β from open interval $(0, 1)$ together with constants a and b from \mathbb{Z} . For the simplicity we assume that $0 < \alpha < \beta$. She sets parameters $m = [\alpha n + a]$ and $k = [\beta n + b]$ where parenthesis denote the floor function and a and b are selected constants. Alice computes parameter s, r and p of the linguistic graph ${}^{m,k}C_n(K)^t$. Without loss of generality we assume that $s > r$. She chooses data to define static graphs of for $t = 1, 2, \dots, l$. Alice can form these field elements via selection of them as members of pseudorandom or genuinely random sequences. The number of all coefficients is $O(n^3)$.

She will generate the tuple $H(a(1), b(1), a(2), b(2), \dots, a(l), b(l), a(l+1))$ with $a(i)$ and $b(i)$ from $F_q[x_1, x_2, \dots, x_{s+p}]^{s+p} U F_q[x_1, x_2, \dots, x_{s+p}]^{r+p}$.

Recall that $\deg(a_i)$ and $\deg(b_i)$ are selected from the set $\{0, 1, 2\}$ under the condition that $\deg(a(i)) + \deg(b(i)) = 2, i = 1, 2, \dots, l$.

The number of all polynomial coefficients is $O(n^7)$.

Alice can form these tuples of polynomials via selection of their coefficients as pseudorandom parameters. Finally Alice selects bijective affine transformation L_1 and L_2 and computes standard

form of the map $L_1HL_2=G$ given by the tuple $(g_1, g_2, \dots, g_{r+p})$. She presents multivariate rule G to public users.

Let us evaluate the time to generate the digital signature.

Assume that correspondents have hash value

$h=(h_1, h_2, \dots, h_{r+p})$. Alice computes $(L_1)^{-1}(h)=(c_1, c_2, \dots, c_{r+p})$ in time $O(n^4)$.

She solves $a(l+1)(z_1, z_2, \dots, z_{m+s})=c$ in time $O(n^4)$ and gets

Some solution $(v_1, v_2, \dots, v_{m+s})=v$.

Alice computes $a(i)(v)$ and $b(i)(v)$ in time $O(n^4)$.

The operator of taking neighbour of the vertex cost $O(n^4)$.

For the construction of the signature she need $O(n)$ neighbour computations. Jump operators application does not affect the complexity. Thus the complexity to sign the document is $O(n^5)$.

REMARK 4.3. We can implement Algorithm 4 with the special pair $(a(l+1), T)$ constructed as the composition of output of the $D(s+p, K)$ based algorithm [46] of kind G, T' . Alice can take linear map L of K^{s+p} onto K^{r+p} of the rank $r+p$ take $a(l+1)$ as the composition G and L and T as the pair L, T' .

5. Conclusion

In this paper we present the method of construction of trapdoor accelerators of Multivariate Cryptography in terms of Algebraic Graph Theory. It uses bipartite cellular Schubert graphs of geometries of Chevalley groups given by equations over finite field F_q . Temporal analogues of these graphs are

defined via the option of a momentum change of the coefficients of monomial terms in these algebraic equation.

This approach allows us define cellular Schubert graphs and their temporal analogues over arbitrary commutative ring K with unity. The partition sets of such graph are affine spaces K^n and K^m . The special walk on the temporal graph over $K[x_1, x_2, \dots, x_n]$ can be used for the construction of multivariate map G from K^n to K^m (or K^n to K^n). The information on temporal graph and the walk can serve as corresponding trapdoor accelerator T of G , i. e. the knowledge on T allows 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 [22] the cases of diagrams B_n, C_n and D_n .

Presented in this paper methods has some similarity with the construction of multivariate rules with Oil and Vinegar techniques when variables of core quadratic maps over finite fields are divided into two groups of variables (oil and vinegar parameters and the specialisation of one group of variables converts the transformation into linear maps (see the description of RUOV in [2] and further references. The advantage of ${}^{s,k}C_n(K)$ based technique is the option to use the commutative ring with zero divisors for which corresponding linear algebra and Groebner basis technique are more sophisticated than in the case of a field. These graphs allow us to construct also cubic maps with the trapdoor accelerators.

Additionally we can present some heuristic arguments supporting the conjecture that the complexity to find the reimage of constructed quadratic or cubic outputs of algorithms 1 and 4 without the knowledge of described trapdoor accelerator has nonpolynomial nature.

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

Assume that she use only one cellular Schubert graphs ${}^{s,k}C_m(K)$ 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 ${}^{s,k}C_m(K)$ ”. Then input x and output y vertexes of algorithm 1 or 4 will be connected by the walk in ψ . 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 ${}^jI_m(K), j=0, 1, 2, \dots$ the complexity of finding the path will be higher.

Section 4 illustrates that temporal Jordan-Gauss graphs can be used for the constructions of new platforms of Noncommutative Cryptography which are special semigroups of Cremona semigroup of endomorphisms of $K[x_1, x_2, \dots, x_n]$ with bounded degree. These platforms are formed by elements of degree bounded by constant (2 or 3) over the selected commutative ring K . Results on the implementation of protocols based on such platforms can be found in [37], [38] and [22]. These protocols allow safe delivery of multivariate map of bounded degree from one correspondent to another one and its further usage for the digital signature procedure.

Alternatively to the approach of this paper we investigate options to use special endomorphisms of $K[x_1, x_2, \dots, x_n]$ of unbounded degree for design of protocols and cryptosystem on platforms of multivariate nature (see [51] and further references).

Noteworthy that Noncommutative Cryptography is another well established and promising area (see [52-58] and recent cryptanalytic results [59-65]).

We concentrate on the multivariate algorithms of digital signatures but bijective public keys can be used as encryption 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 already 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 procedures. Some of them are the generalisations of schemes [36] 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 instruments are elements of Cremona semigroups (see endomorphisms of $K[x_1, x_2, \dots, x_n]$ (see [66], [67]) have 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 partially supported by 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, 2023/175.
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 International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17–21, Springer 2021, Proceedings, Part I.
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 Re-view, Challenges, and Research Directions, ACM Computing Survey, volume 55, is-sue 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., *Multivariate Public Key Cryptosystems, Second Edition. Advances in Information Security*. Springer.2020.
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. *Cryp-tology ePrint Archive* (2022).
17. Markku Juhani Saarinen, Daniel Tony Smith (editors), *Post Quantum Cryptography, 15th International Workshop, PQCrypto 2024, Oxford, UK, June 12-14, 2024, Proceed-ings, Part 1*.
18. Markku Juhani Saarinen, Daniel Tony Smith (editors), *Post Quantum Cryptography, 15th International Workshop, PQCrypto 2024, Oxford, UK, June 12-14, 2024, Proceed-ings, Part 2*.
19. Tsuyoshi Takagi, Masato Wakayama, Keisuke Tanaka, Noboru Kunihiro, Kazufumi Kimoto, Yasuhiko Ikematsu (editors), *International Symposium on Mathe-matics, Quantum Theory, and Cryptography, Proceedings of MQC 2019, Open Access, 2021*.
20. Kohei Arai (editor), *Advances in Information and Communication, Proceedings of the 2024 Future of Information and Communication Conference (FICC), Volume 1-3, Lec-ture Notes in Networks and Systems, (LNNS, volume 919 -921) , Springer, 2024*.
21. V. Ustimenko. 2022. *Graphs in terms of Algebraic Geometry, symbolic computations and secure communications in Post-Quantum world, UMCS Editorial House, Lublin, 2022, 198*.
22. B. Sturmfels. *Solving systems of polynomial equations. Providence, RI: American Mathematical Soc. 2002*.
23. J. F. Canny, E. Kaltofen, L. Yagati, *ISSAC '89: Proceedings of the ACM-SIGSAM 1989 international symposium on Symbolic and algebraic computation. Pp 121 – 128*.
24. B. Buchbergers, *Groebner basis: An algorithmic method in polynomial ideal theory,” in Recent Trends in Multidimensional Systems Theory, edited by N. K.Bose; D. Reidel Publ. Comp., Dordrecht (Holland), pp. 184-232, 1985*.
25. V. Ustimenko, *On Extremal Algebraic Graphs and Multivariate Cryptosystems, IACR e-print archive, 2022/1537*.
26. 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)..*
27. N. Biggs, *Algebraic graphs theory, Second Edition, Cambridge University Press, 1993*.
28. A. Brower, A. Cohen, A. Nuemaier, *Distance regular graphs, Springer, Berlin, 1989*.
29. B. Bollobás, *Extremal Graph Theory, Academic Press, London, 1978*.
30. F. Buekenhout (Editor), *Handbook on Incidence Geometry, North Holland, Amsterdam, 1995*.
31. 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*.
32. R. W. Carter, *Simple Groups of Lie Type, Wiley, New York (1972)*.
33. V. A. Ustimenko, *On some properties of Chevalley groups and their generalisa-tions, In: Investigations in Algebraic Theory of Combinatorial objects, Moskow, Institute of System*

- Studies, 1985, in *Investigations in Algebraic Theory of Combinatorial Objects*, Kluwer, Dordrecht (1992) p. 112-119.
34. V. A. Ustimenko, Linear interpretation of Chevalley group flag geometries, *Ukraine Math. J.* 43, Nos. 7,8 (1991), pp. 1055–1060.
 35. V. Ustimenko, Small Schubert cells as subsets in Lie algebras, *Functional Analysis and Applications*, v. 25, no. 4, 1991, pp. 81–83.
 36. V. Ustimenko, On Schubert cells in Grassmanians and new algorithms of multivariate cryptography, *Proceedings of the Institute 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).
 37. V. Ustimenko, On desynchronised multivariate algorithms of El Gamal type for stable semigroups of affine Cremona group, *Theoretical and cryptographic problems of cybersecurity*, Vol. 1 No. 1 (2019).
 38. V. Ustimenko, On computations with double Schubert automaton and stable maps of multivariate cryptography, *Interdisciplinary Studies of Complex Systems*, No. 19 (2021) 18–32.
 39. V. Ustimenko, On small world non Sunada twins and cellular Voronoi diagrams, *Algebra and Discrete Mathematics*, vol. 30, N1 (2020), pp. 118-142.
 40. T. Adamo, G. Ghiani, E. Guerriero, On path ranking in time-dependent graphs, *Computers & Operations Research*, Volume 135, November 2021, 105-446.
 41. W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, 2003.
 42. Anton Betten, Michael Braun, Adalbert Kerber, Axel Kohnert, Alfred Wasserman, *Error Correcting Linear Codes Isometry and Applications*, Springer, 2006.
 43. Andreas Stephan Esenhans, Axel Kohnert, Alfred Wassermann, *Constructions of codes for Network Coding*, arXiv:1005.2839[cs].
 44. A. Beultespacher, Enciphered Geometry, Some Applications of Geometry to Cryptography, *Annals of Discrete Mathematics*, v. 37, 1988, 59-68.
 45. N. Koblitz, *Algebraic aspects of cryptography*, Springer (1998), 206 p.
 46. V. Ustimenko, T. Chojecki., M/ Klisowski, M. (2024). On Graphs Defined by Equations and Cubic Multivariate Public Keys. In: Arai, K. (eds) *Advances in Information and Communication. FICC 2024. Lecture Notes in Networks and Systems*, vol 921. Springer, Cham. https://doi.org/10.1007/978-3-031-54053-0_3
 47. I. Gelfand, R. MacPherson, Geometry in Grassmanians and generalisation of the dilogarithm, *Adv. in Math.*, 44 (1982), 279-312.
 48. I. Gelfand, V. Serganova, Combinatorial geometries and torus strata on homogeneous compact manifolds, *Soviet Math. Surv.* 42 (1987), 133-168.
 49. Alexei Myasnikov; Vladimir Shpilrain and Alexander Ushakov (2008), *Group-based Cryptography*, Berlin: Birkhäuser Verlag. 2008.
 50. Ustimenko, V.A.: On new symbolic key exchange protocols and cryptosystems based on a hidden tame homomorphism. *Dopovidi Nat. Akad. Nauk Ukr.*, 2018(10), 26–36 (2018).
 51. V. Ustimenko, On Eulerian semigroups of multivariate transformations and their cryptographic applications. *European Journal of Mathematics* 9, 93 (2023).
 52. 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.

53. J.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.
54. 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.
55. 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.
56. V. Ustimenko, On historical Multivariate Cryptosystems and their restorations as instruments of Post-Quantum Cryptography, *IACR e-print archive*, 2024/091.
57. Zhenfu Cao (2012), *New Directions of Modern Cryptography*. Boca Raton: CRC Press, Taylor & Francis Group. ISBN 978-1-4665-0140-9.
58. Benjamin Fine, et. al. "Aspects of Non abelian Group Based Cryptography: A Survey and Open Problems", arXiv:1103.4093.
59. [59] V. A. Roman'kov, A nonlinear decomposition attack, *Groups Complex. Cryptol.* 8, No. 2 (2016), 197-207.
60. V. Roman'kov, An improved version of the AAG cryptographic protocol, *Groups, Complex., Cryptol.* 11, No. 1 (2019), 35-42.
61. 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).
62. B. Tsaban, Polynomial-time solutions of computational problems in noncommutative-algebraic cryptography, *J. Cryptol.* 28, No. 3 (2015), 601-622.
63. V. Roman'kov, Cryptanalysis of a new version of the MOR scheme, arXiv:1911.00895 .
64. V. Roman'kov, Cryptanalysis of two schemes of Baba et al. by linear algebra methods. CoRR abs/1910.09480 (2019). [cs.CR].
65. V. Ustimenko On the restoration of historical Matsumoto - Imai cryptosystem and other schemes in terms of Noncommutative Cryptography, *Proceedings of Future Technology Conference*, London, November, 2024 (to appear).
66. M. Noether, Luigi Cremona} *Mathematische Annalen*, 59 (1904), pp. 1-19.
67. 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.