On the Jordan-Gauss graphs and new multivariate public keys

Vasyl Ustymenko[1,2,*,†], Tymoteusz Chojecki[3,†] and Aneta Wróblewska[3,†]

[1] Royal Holloway, University of London, Egham Hill, TW20 0EX Egham, United Kingdom
[2] Institute of Telecommunication and Global Information Space, 25 Chokolivskiy blv., 03186 Kyiv, Ukraine
[3] Maria Curie-Skłodowska University, 5 Pl. M. Curie-Skłodowskiej, 20-031 Lublin, Poland

Abstract

We suggest two families of multivariate public keys defined over arbitrary finite commutative ring K with unity. The first one has a quadratic multivariate public rule, this family is an obfuscation of previously defined cryptosystem defined in terms of well-known algebraic graphs $D(n, K)$ with the partition sets isomorphic to K_n. Another family of cryptosystems uses the combination of Eulerian transformation of $K[x_1, x_2, ..., x_n]$ sending each variable x_i to a monomial term with the quadratic encryption map of the first cryptosystem. The resulting map has an unbounded degree and the density $O(n_4)$ like the cubic multivariate map. The space of plaintexts of the second cryptosystem is the variety (K^*)n and the space of ciphertexts is the affine space K_n.

Keywords

multivariate cryptography over commutative rings, graph-based symbolic computations, quadratic public keys, multivariate public keys of unbounded degree

1. Introduction

This paper presents the generalization of the quadratic multivariate public key given in [1] with the use of quantum computing.

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 standardization 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 2nd, 3rd, and 4th rounds.

The last algebraic public key "Unbalanced Oil and Vinegar Rainbow like digital signatures" (ROUV) constructed in terms of Multivariate Cryptography was rejected in 2021 (see [2, 3]). Certain hopes of algebraists are connected with so-called Noncommutative Cryptography which is based on problems connected with the studies of algebraic objects such as groups, semigroups, noncommutative rings, and algebras. Presented on Mist tender single algorithms from this class based on braids group was broken. The first four winners of this competition were announced in 1922, they are 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. So, a large class of protocol-supported asymmetric algorithms of El Gamal type was eliminated. We were working on the design of the new algorithms from this class during our project. 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.

Five categories were considered by NIST in the PQC standardization (the submission date was 2017; in July 2022, the four winners and the four 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 four different mathematical problems (not the five announced at the beginning):

- Lattice-based
- Hash-based
- Code-based
- Supersingular elliptic curve isogeny based.

CQPC-2024: Classic, Quantum, and Post-Quantum Cryptography, August 6, 2024, Kyiv, Ukraine
*Corresponding author.
†These authors contributed equally.
vasyl.ustymenko@rhul.ac.uk (V. Ustymenko); tymoteusz.chojecki@umcs.pl (T. Chojecki); aneta.wroblewska@poczta.umcs.lublin.pl (A. Wróblewska)
0000-0002-2138-2357 (V. Ustymenko); 0000-0002-3294-2794 (T. Chojecki); 0000-0001-9724-4586 (A. Wróblewska)

The standards are to be published in 2024. But already at the end of round 3, the last candidate ("Rainbow") from the multivariate cryptography (MVC) category was out.

Its interesting obfuscation "TUOV: Triangular Unbalanced Oil and Vinegar" was presented to NIST [39] by principal submitter Jintaj Ding.

Further development of Classical Multivariate Cryptography which studies quadratic and cubic endomorphisms of $F_q[x_1, x_2, \ldots, x_n]$ see [6–18]. Current research in Postquantum Cryptography can be found in [35–38].

We use the concept of quadratic accelerator of the endomorphism σ of $K[x_1, x_2, \ldots, x_n]$ which is the piece of information T such that its knowledge allows us to compute the reimage of (σ, K^n) in time $O(n^2)$. Symbol K stands here for an arbitrary commutative ring with unity. Our suggestion is to use for public key the pairs (σ, T) such that σ has a polynomial density, i. e. number of monomial terms of $\sigma(x_i)$, $i = 1, 2, \ldots, n$. Some examples of such public keys the reader can find in [4, 5].

For each *pair* (K, n), $n > 1$ we present quadratic automorphism σ of $K[x_1, x_2, \ldots, x_n]$ with the trapdoor accelerator T defined via totality of special bipartite Jordan-Gauss graphs with the partition sets isomorphic to K^n. We discuss the possible use of these transformations in the case of finite fields and arithmetical rings Z_q where q is a prime power. Additionally, we create a public key as a composition of quadratic σ with the Eulerian transformation sending each x_1 to a monomial term. The public map has an unbounded degree and density $O(n^4)$. So the complexity of encryption is as in the case of classical cubic maps.

2. On Jordan-Gauss graphs and multivariate keys

The missing definitions of graph-theoretical concepts which appear in this paper can be found in [19–21]. All graphs we consider are simple graphs, i.e. undirected without loops and multiple edges. Let $V(G)$ and $E(G)$ denote the set of vertices and the set of edges of G respectively. When it is convenient we shall identify G with the corresponding anti-reflexive binary relation on $V(G)$, i.e. $E(G)$ is a subset of $V(G)\times V(G)$ and write $v\ G\ u$ for the adjacent vertices u and v (or neighbors).

We refer to $|\{x \in V(G) | xGv\}|$ 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. The pair $x, y, x \in P, y \in L$ such that $x\ I\ y$ is called a flag of incidence structure I.

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

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

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

$$\ldots$$

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

where a_j, and b_j, $j = 1, 2, \ldots, m$ are not zero divisors, and f_j are multivariate polynomials with coefficients from K (see [22, 23]). Brackets and parenthesis allow us to distinguish points from lines.

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

We refer to $\rho((x)) = (x_1, x_2, \ldots, x_s)$ for $(x) = (x_1, x_2, \ldots, x_{s+m})$ and $\rho([y]) = (y_1, y_2, \ldots, y_r)$ for $[y] = [y_1, y_2, \ldots, y_{r+m}]$ as the color of the point and the color of the line respectively. For each $b \in K^r$ and $p = (p_1, p_2, \ldots, p_{s+m})$ there is a unique neighbor of the point $[l] = N_b(p)$ with the color b. Similarly for each $c \in K^s$ and line $l = [l_1, l_2, \ldots, l_{r+m}]$, there is a unique neighbor of the line $(p) = N_c([l])$ with the color c. The triples of parameters $s, r, and\ m$ define the *type of linguistic graph.*

We consider also linguistic incidence structures defined by the infinite number of equations.

Linguistic graphs are defined up to isomorphism. We refer to written above equations as canonical equations of linguistic graphs. We consider also linguistic incidence structures defined by the infinite number of equations. Linguistic graphs are defined up to isomorphism. We refer to written above equations as canonical equations of linguistic graphs.

We say that linguistic graph is a Jordan-Gauss type if the map $[(x), [y]] \to (f_1 (x_1, x_2, \ldots, x_s, y_1, y_2, \ldots, y_r), f_2 (x_1, x_2, \ldots, x_s, x_{s+1}, y_1, y_2, \ldots, y_r, y_{r+1}), \ldots, f_{m-1} (x_1, x_2, \ldots, x_s, x_{s+1}, \ldots, x_{s+m-1}, y_1, y_2, \ldots, y_r, y_{r+1}, \ldots, y_{r+m-1}))$ where $(x) \in K^{s+m}$, $[y] \in K^{r+m}$ *is* a bilinear map into K^1. So all f_i are special quadratic maps. In the case of Jordan-Gauss graphs, the neighborhood of each vertex is given by the system of linear equations written in its row—echelon form.

Let I_m be a linguistic graph defined over the commutative ring K. For each $b \in K^r$ and $p = (p_1, p_2, \ldots, p_{s+m})$ there is the unique neighbor of the point $[l] = N_b(p)$ with the color b. Similarly, for each $c \in K^s$ and line $l = [l_1, l_2, \ldots, l_{r+m}]$ there is the unique neighbor of the line $(p) = N_c([l])$ with the color c. We refer to the operator of taking the

neighbor of vertex accordingly chosen color as *neighborhood operator.*

On the sets P and L of points and lines of the linguistic graph we define jump operators ${}^1\mathcal{J} = {}^1\mathcal{J}_b(p) = (b_1, b_2, \ldots, b_s, p_1, p_2, \ldots, p_{s+m})$, where $(b_1, b_2, \ldots, b_s) \in K^s$ and ${}^2\mathcal{J} = {}^2\mathcal{J}_b([l]) = [b_1, b_2, \ldots, b_r, l_1, l_2, \ldots, l_{r+m}]$, where $(b_1, b_2, \ldots, b_r) \in K^r$. We refer to tuple (s, r, m) as the type of the linguistic graph I.

We say that point (p) is a line $[l]$ adjacent in the linguistic graph I if ${}^1\mathcal{J}_b(p) I\, {}^2\mathcal{J}_c[l]$ for some colors $b \in K^s$ and $c \in K^r$. Let ψ stand for the adjacency relation of the linguistic graph. We say that the linguistic graph has degree d, $d \geq 2$ if the maximal degree of nonlinear multivariate polynomials f_i, $i = 1, 2, \ldots, m$ is d.

Noteworthy, that the path $v_0, v_1, \ldots, v_k$ in the linguistic graph $I_{m\_}$ is determined by starting vertex v_0 and colours of vertexes $v_1, v_2, \ldots, v_k$ such that $\rho(v_i) \neq \rho(v_{i+2})$ for $i = 0, 1, \ldots, k-2$.

Let us consider the sequence of colours $c(1), c(2), c(3), c(4), c(5)$ where $c(1)$ and $c(4), c(5)$ are from K^s and $c(2), c(4)$ are elements of K^r.

Let $v_0 = (x)$ be a general point of the graph I then for the vertices $v_1 = {}^1\mathcal{J}_{c(1)}(v_0)$, $v_2 = N_{c(2)}(v_1)$, $v_3 = {}^2\mathcal{J}_{c(3)},(v_2)$, $v_4 = N_{c(4)}(v_3)$, $v_5 = {}^1\mathcal{J}_{c(5)}(v_4)$ the relations $v_0 \psi v_3$, $v_2 \psi v_5$ holds.

We consider the tuple of colors $c(1), c(2)\ldots., c(t)$, $t = 1 \bmod 4$ such that $c(i) \in K^s$ for $i = 0,1 \bmod 4$ and $c(i) \in K^r$ for $i = 2,3 \bmod 4$.

We refer to the sequence of vertexes $v_1 = {}^1\mathcal{J}(v_0)$, $v_2 = N_{c(2)}(v_1)$, $v_3 = {}^2\mathcal{J}_{c(3)}$, $v_4 = N_{c(4)}(v_3)$, $v_5 = {}^1\mathcal{J}(v_4)$, $v_6 = N_{c(6)}(v_5)$, $v_7 = {}^2\mathcal{J}_{c(7)}(v_6)$, $v_8 = N_{c(8)}(v_7)$, $\ldots$, $v_{t-1} = N_{c(t-1)}(v_{t-2})$, $v_t = {}^1\mathcal{J}(v_{t-1})$ as *walk on the adjacency graph* with the starting point (x) and the colour trace $c(1), c(2), \ldots, c(t)$.

For each positive integer l, we can consider graph $I_m(K)$ together with ${}^lI_m = I_m(K[y_1, y_2, \ldots, y_l])$ defined by the same polynomials f_i, $i = 1, 2, \ldots, m$ with coefficients from K.

Assume that $l = m+s$. We can consider the walk on the adjacency graph $\psi(K[y_1, y_2, \ldots, y_l])$ of length $4t+1$ with starting point $(y_1, y_2, \ldots, y_s, y_{s+1}, y_{s+2}, \ldots, y_{m+s})$ and colours $c(1), c(2), \ldots, c(t)$ such that $c(i) \in K[y_1, y_2, \ldots, y_s]^s$ for $i = 0,1 \bmod 4$ and $c(i) \in K[y_1, y_2, \ldots, y_s]^r$ for $i = 2,3 \bmod 4$.

Assume that $c(t) = (h_1(y_1, y_2, \ldots, y_s), h_2(y_1, y_2, \ldots, y_s), \ldots, h_s(y_1, y_2, \ldots, y_s))$.

Then $v_1 = (h_1, h_2, \ldots, h_s, g_1, g_2, \ldots, g_m)$. Let us consider the polynomial map ${}^{I(K),c}$ *Pass*, $c \in K[x_1, x_2, \ldots, x_s]^{(2t+1)s+2rt}$ of K^{s+m} to itself which sends $(y_1, y_2, \ldots, y_s, y_{s+1}, \ldots, y_{s+m})$ to v_t, i. e. the map

$y_1 \longrightarrow h_1(y_1, y_2, \ldots, y_s)$, $y_2 \longrightarrow h_2(y_1, y_2, \ldots, y_s)$, $\ldots$, $y_s \longrightarrow \longrightarrow h_s(y_1, y_2, \ldots, y_s)$,

$y_{s+1} \longrightarrow g_1(y_1, y_2, \ldots, y_s, y_{s+1}, y_{s+2}, \ldots, y_{s+m})$, $y_{s+2} \longrightarrow \longrightarrow g_2(y_1, y_2, \ldots, y_s, y_{s+1}, y_{s+2}, \ldots, y_{s+m})$, $\ldots$, $y_{s+m} \longrightarrow \longrightarrow g_m(y_1, y_2, \ldots, y_s, y_{s+1}, y_{s+2}, \ldots, y_{s+m})$.

It is easy to see that this transformation is bijective if and only if the map $y_1 \longrightarrow h_1(y_1, y_2, \ldots, y_s)$, $y_2 \longrightarrow h_2(y_1, y_2, \ldots, y_s)$, $\ldots$, $y_s \longrightarrow h_s(y_1, y_2, \ldots, y_s)$, is bijective on K^s [24]. Defined above transformations form a semigroup ${}^{I(K)}S_P$ of multivariate transformation. Some basic properties of this semigroup are discussed in [24].

Of course, we can use lines instead of points and define another semigroup ${}^{I(K)}S_L$ formed by transformation of kind ${}^{I(K),c}$*Pass*, $c \in K[x_1, x_2, \ldots, x_s]^{(2t+1)r+2ts}$ acting on the variety K^{m+r}.

Remark. We may omit some operators of kind $\mathcal{J}_c(i)$ making the color $c(i)$ to be the same as $c(i-1)$.

We can treat the sequence c from $K[x_1, x_2, \ldots, x_s]^l$ as the tuple of its coordinates c_i from $K[x_1, x_2, \ldots, x_s]$ and define the degree of c as polynomials $c_i(x_1, x_2, \ldots, x_s)$.

In [25] special Jordan-Gauss graph $\mathcal{J}G(r, s, m, F_q)$, $q = 2^t$, $t>1$ was used for the construction of the public key. This linguistic graph of type (r, s, m) is obtained from the projective geometry $PG_n(F_q)$, i.e. the totality of nonzero proper subspaces of $(F_q)^{n+1}$. The corresponding bipartite graph is obtained as an induced subgraph of bipartite incidence graph with the partition sets which are largest Schubert cells, i.e. largest orbits of $UT_n(F_q)$ acting on l dimensional subspaces and subspaces of dimension t, $l \neq t$.

Cubic public keys defined in [26*U, Ch, K]* used Jordan-Gauss graphs $A(n, F_q)$ [27] and $D(n, F_q)$ [28]. These two families of graphs were used in [1] for the construction of a quadratic public key. This paper also contains the construction of trapdoor accelerator T of quadratic endomorphism σ of $K[x_1, x_2, \ldots, x_n]$ acting bijectively on K^n and defined in terms of graph $D(n, K)$ where K is an arbitrary commutative ring with unity [23].

The description of the generalization of this construction is given below.

Affine root system $\tilde{A}_1$ (A_1 with wave see [29]) is the totality of vectors in the two-dimensional Euclidean space R^2 with the standard basis $e_1 = (1, 0)$ and $e_2 = (0, 1)$ containing vectors $(1, 0), (0, 1), (i, i), (i, i+1), (i+1, i), i \geq 1$. All multiples of $(1, 1)$ are known as imaginary roots, other roots that have no multiples are known as real roots.

We modify $\tilde{A}_1$ by adding copies $(i, i)'$ for each imaginary root (i, i), $i>1$. So we obtain a set Root consisting of roots of $\tilde{A}_1$ and elements $(i, i)'$, $i>1$.

Let $R_1 = Root - \{(0,1)\}$ and $R_2 = Root - \backslash\{(1,0))\backslash\}$ and K be a commutative ring with unity. We consider sets $L_i = K^{Ri}$, $i = 1, 2$ of all functions f from R_i, $i = 0,1$ to K such that only for finite elements x from R_i the value $f(x)$ differs from zero.

We write an element $X = (x)$ from $P = L_1$ as the tuple $(x) = (x_{1,0}, x_{1,1}, x_{1,2}, x_{2,1}, x_{2,2}, x'_{2,2}, \ldots, x_{i,i+1}, x_{i+1,i}, x_{i+1,i+1}, x'_{i+1,i+1}, \ldots)$ where x_α is the value of X on the root α from $\tilde{A}_1$ and $x'_{i,i}$ is the value of X on $(i, i)'$, $i>1$.

Similarly we write an element $Y = [y]$ from $L = L_2$ as the tuple

$[y] = [y_{0,1}, y_{1,1}, y_{1,2}, y_{2,1}, y_{2,2}\, y'_{2,2}, \ldots, y_{i,i+1}, y_{i+1,i}, y_{i+1,i+1}, y'_{i+1,i+1}, \ldots]$ where y_α is the value of Y on the root α from

$\tilde{A}_1$ and $y'_{i,i}$ is the value of Y on $(i, i)'$, $i>1$. We introduce the incidence structure (P, L, I) as the following bipartite graph on $P \cup L$.

A point (x) of this incidence structure I is incident with a line $[y]$, i.e. (x)I[l], if their coordinates obey the following relations:

$$\begin{aligned} &x_{i,\,i,} - y_{i,\,I} = x_{1,0}\, y_{i-1,i}, \\ &x'_{i,i} - y'_{i,i} = x_{i,\,i-1} y_{0,1}, \\ &x_{i,i+1} - y_{i,\,i+1} = x_{i,i} y_{0,1}, \\ &x_{i+1,i} - y_{i+1,I} = x_{1,0} y'_{i,i}. \end{aligned} \qquad (1)$$

(These four relations are well defined for $i>1$, $x_{1,1} = x'_{1,1}$, $y_{1,1} = y'_{1,1}$).

We start the description of the connectivity invariants of $D(k, K)$.

To facilitate notation in the future results on "connectivity invariants" of $D(n, K)$, it will be convenient for us to define $x_{-1,0} = y_{0,-1} = y_{1,0} = = x_{0,1} = 0$, $x_{0,0} = y_{0,0} = -1$, $x'_{0,0} = y'_{0,0} = -1$, $x_{1,1} = x'_{1,1}$, $y_{1,1} = y'_{1,1}$ and to assume that our equations are defined for $i\geq 0$.

Graphs $CD(k, K)$ with $k\geq 6$ were introduced in [23], as induced subgraphs of $D(k, K)$ with vertices u satisfying special equations $a_2(u) = 0$, $a_3(u) = 0$, …, $a_t(u) = 0$, $t = [(k+2)/4]$, where $u = (u_\alpha, u_{1,1}, u_{1,2}, u_{2,1}, \ldots, u_{r,r}, u'_{r,r}, u_{r,r+1}, u_{r+1,\,r}, \ldots)$, $2\leq r\leq t$, $\alpha \in \{(1, 0), (0,1)\}$ is a vertex of $D(k, K)$ and $a_r = a_r(u) = \Sigma_{i=0,r}\, (u_{i,i} u'_{r-i,r-i} - u_{i,\,i+1}\, u_{r-i,r-1-1})$ for every r from the interval $[2,t]$.

We set $a = a(u) = (a_2, a_3, \ldots, a_t)$ and assume that $D(k, K) = CD(k, K)$ if $k = 2, 3, 4, 5$. As it was proven in [23] graphs $D(n, K)$ are edge transitive. So their connected components are isomorphic graphs.

Let ${}^{v}CD(k, K)$ be a solution set of the system of equations $a(u) = (v_2, v_3, \ldots, v_t) = v$ for certain $v\in K^{t-1}$. It is proven that each ${}^{v}CD(k, K)$ is the disjoint union of some connected components of graph $D(n, K)$.

If K is a commutative ring with unity of odd characteristic then ${}^{v}CD(k, K)$ is the actual connected component of the graph (see [30]).
If K is a finite field of even characteristics of order ≥ 8 then ${}^{v}CD(k, K)$ is the actual connected component of the graph (see [31]).

Let us consider the following graphs $D_T(k, K)$ associated with $D(n, K)$ and subset $T = \{j(1), j(2), j(s)\}$ of $\{2, 3, \ldots, [(k+2)/2]\}$ via the following procedure.

Delete coordinates of points and lines indexed by roots $(i(l), i(l))'$, $l = 1, 2, \ldots, s$ together with corresponding equations of kind $x'_{i(l),i(l)} - y'_{i(l),\,i(l)} = \ldots, = 1, 2, \ldots, s$.

Substitute equations $x_{i(l)+1,i(l)} - y_{i(l)+1,i(l)} = x_{1,0} y'_{i(l),\,i(l)}$ by $x_{i(l)+1,i(l)} - y_{i(l)+1,i(l)} = x_{1,0} y_{i(l),\,i(l)}$. the last action is just a deletion of the prime symbol on the righthand side of the equation.

Proposition. Graphs $D_T(k, K)$ are Jordan-Gauss graphs of type $(1, 1, n-m-1)$ where m is a cardinality of T.

Polynomials $a_i(v)$ where $1<i<j(1)$ are connectivity invariants of vertex v (point or line) of the vertex v from $D_T(k, K)$ or $D(k, K)$.

Let G be a t-regular simple graph and v be the vertex from $V(G)$. We say that k is the local depth of the vertex v if the induced graph of all vertices at distance $\leq k$ is a tree and the graph on vertices at the distance $k+1$ has a cycle.

The depth of G is the maximal local depth.

Computer simulation supports the conjecture that the depths of graphs $D(k, K)$ and $D_T(k, K)$ are the same. It is known that the depth of $D(k, K)$ is at least $[(k+3)/2]$.

Let us renominate the coordinates of points and line of $D_T(k, K)$ with one variable index i according to the lexicographical order on roots of $\tilde{A}_1$. So we have point $(x_1, x_2, \ldots, x_{k-m})$ and line $[y_1, y_2, \ldots, y_{k-m}]$ of linguistic graph.

We take the "symbolic" line $[y_1, y_2, \ldots, y_{k-m}]$ of this graph and consider the infinite graph $D_T(k, K[y_1, y_2, \ldots, y_{k-m}])$. We use the presented above technique to associate with this graph the polynomial transformations acting on K, but slightly modify the procedure.

Let $\Gamma(n, K)$, $n=k-m$ be one of the graphs $D_T(k, K)$. The graph $\Gamma(n, K)$ has so-called linguistic coloring ρ of the set of vertices. We assume that $\rho(x_1, x_2, \ldots, x_n) = x_1$ for the vertex $\boldsymbol{x}$ (point or line) given by the tuple with coordinates $x_1, x_2, \ldots, x_n$. We refer to $\boldsymbol{x_1}$ from K as the color of vertex x.

Recall that N_a and $\mathcal{J}_a$ are operators of taking the neighbor with color a and jump operator changing the original color of point or line for new color a from K.

Let $[y_1, y_2, \ldots, y_n]$ be the line y of $\Gamma(n, K[y_1, y_2, \ldots, y_n])$ and $(\varphi(1), \varphi(2), \ldots, \varphi(t))$ and $(\beta(1), \beta(2), \ldots, \beta(t))$ are the sequences of colours from $K[y_1]$ of the length at least 2. We consider the sequence ${}^{0}v = y$, ${}^{1}v = \mathcal{J}_{\varphi(1)}({}^{0}v)$, $= {}^{2}v = N_{\beta(1)}({}^{1}v)$, ${}^{3}v = N_{\varphi(2)}({}^{2}v)$, ${}^{4}v = N_{\beta(2)}({}^{3}v)$, ${}^{5}v = N_{\varphi(3)}({}^{4}v)$, …, ${}^{2t-2}v = N_{\beta(t-1)}({}^{2t-3}v)$, ${}^{2t-1}v = N_{\varphi(t)}({}^{2t-2}v)$, ${}^{2t}v = \mathcal{J}_{\beta(t)}({}^{2t-1}v)$.

Assume that $v = {}^{2t}v = [v_1, v_2, \ldots, v_n]$ where v_i are from $K[y_1, y_2, \ldots, y_n]$. We consider polynomial transformation $g(\varphi(1), \varphi(2), \ldots, \varphi(t), \beta(1), \beta(2), \ldots, \beta(t))$, $t \geq 2$ of affine space K^n of kind $y_1 \longrightarrow y_1+\beta(t)$, $y_2 \longrightarrow v_2(y_1, y_2)$, $y_3 \longrightarrow v_3(y_1, y_2, y_3)$, …, $y_n \longrightarrow v_n(y_1, y_2, \ldots, y_n)$.

It is easy to see that $g(\varphi(1), \varphi(2), \ldots, \varphi(t), \beta(1), \beta(2), \ldots, \beta(t))\bullet g(\gamma(1), \gamma(2), \ldots, \gamma(s), \sigma(1), \sigma(2), \ldots, \sigma(t)) = g(\varphi(1), \varphi(2), \ldots, \varphi(t), \gamma(1)(\beta(t)), \gamma(2)(\beta(t)), \ldots, \gamma(s)(\beta(t)), \beta(1), \beta(2), \ldots, \beta(s), \sigma(1)(\beta(t)), \sigma(2)(\beta(t)), \ldots, \sigma(s)(\beta(t))$.

The following statements are formulated in [1] in the case of graph $D(k, K)$ but they hold for arbitrary graph $D_T(k, K)$.

Proposition 1. *Transformations of kind $g = g(\varphi(1), \varphi(2), \ldots, \varphi(t), \beta(1), \beta(2), \ldots, \beta(t))$, $t \geq 2$ generate a semigroup $S(\Gamma(n, K))$ of transformations of K^n.*

Lemma 1. *The degree of transformation g of the Proposition 1 is at least $[\deg(\varphi(1))+\deg(\varphi(1)-\varphi(2))+\deg(\varphi(2)-\varphi(3))+\ldots +\deg((\varphi(t-1)-\varphi(t))]+[\deg(\beta(1)+(\deg(\beta(1)-\beta(2))+ +(\deg(\beta(2)-\beta(3))+\ldots(\deg(\beta(t-2)-\beta(t-1))]$.*

Lemma 2. *Transformation g as in the Proposition 1 is bijective if and only if $\beta(t)(x) = a$ has a unique solution for each a from K.*

Proposition 2. *Transformations of kind ${}^{n}g = g(\varphi(1), \varphi(2),..., \varphi(t), \beta(1), \beta(2), ..., \beta(t))$, $t \geq 2$ such that $deg(\varphi(i)) = 0$ and $\beta(i) = y_1+c(i)$, $c(i) \in K$ generate a subgroup ${}^{2}G(I\!I(n, K))$ of transformation of maximal degree 2.*

Remark 1. *The inverse element of ${}^{n}g = g(\varphi(1), \varphi(2),..., \varphi(t), \beta(1), \beta(2), ..., \beta(t))$, $t \geq 2$ as in the Proposition 2 can be written as ${}^{n}g(\varphi(t), \varphi(t-1), ..., \varphi(1), \beta(t-1)(\beta(t)^{-1}), \beta(t-2)(\beta(t)^{-1}), ..., \beta(1)(\beta(t)^{-1}), \beta(t)^{-1})$.*

Remark 2. *In the case of two quadratic transformations of K^n of "general position," their composition will have degree 4.*

We associate with the sequence $\varphi(1), \varphi(2), ..., \varphi(t), \beta(1), \beta(2), ..., \beta(t-1)$ of Proposition 2 and $\beta^*(t) = f(y_1, y_2, ..., y_n)$ of degree 2 another quadratic transformation $h = H(\varphi(1), \varphi(2), ..., \varphi(t), \beta(1), \beta(2), ..., \beta(t-1), \beta^*(t))$ constructed via the sequence of vertices ${}^{0}v, {}^{1}v, {}^{2}v, ..., {}^{2t-2}v = = N_{\beta(t-1)}({}^{2t-3}v), {}^{2t-1}v = N_{\varphi(t)}({}^{2t-2}v)$. We compute ${}^{2t}v = \mathfrak{J}_{\beta^*(t)}({}^{2t-1}v) = v$ and define h as the quadratic map $y_i \longrightarrow v_i$, $i = 1, 2, ..., n$.

Theorem 1. *Let K be the finite field F_q, $q = 2^r$, $r>1$. Then transformation $h = h(\varphi(1), \varphi(2), ..., \varphi(t), \beta(1), \beta(2), ..., \beta^*(t))$ for which deg $\varphi(i) = 0$, $i = 1, 2, ..., t$, $\beta(i) = y_1+c(i)$, $c(i) \in K$, $i = 1, 2, ... t-1$ and $\beta^*(t) = (y_1)^2$ is a bijective quadratic transformation of the vector space $(F_q)^n$, the polynomial degree of its inverse transformation is at least 2^{r-1}.*

We use the modifications of transformation Theorem 1 for the construction of quadratic public keys.

Algorithm 1. Alice selects commutative ring K with unity and K^* of order >2 together with parameters k, m. She selects $T = \{j(1), j(2),..., j(m)\}$ and works with the graph $D_T(k, K)$. Let us assume that $j(1)>3$.

Alice selects two transformations L_1 and L_2 from the group $AGL_n(K)$. She takes $t = O(n)$, $2<t<[(n+3)/2]$ and selects the parameters $\alpha_1, \alpha_2 = \alpha_1+d(1), ..., \alpha_3 = \alpha_2+d(2), ..., \alpha_t = \alpha_{t-1}+d(t-1)$ where parameters $d(i)$ are elements of K^*, $\beta_1 = y_1+c(1), \beta_2 = y_1+c(2), ..., \beta_{t-1} = y_1+c(t-1)$ where elements $c(1)-c(2), c(2)-c(3), ..., c(t-2)-c(t-1)$ are elements of K^*. Alice forms β^* as a polynomial of kind

$$d((d' y_1+\Sigma_{i=2,3,..., i(1)-1} a_i([\alpha_2, y_1, y_2, ..., y_n])\lambda_i+\lambda)^r + \Sigma_{i=2,3,..., i(1)-1} a_i([\alpha_2, y_1, y_2,..., y_n])\mu_i+ \mu)$$

where $d \in K^*$, $d' \in K^*$, $r = 2$ if the order of K^* is odd, $r = 1$ if K^* has even order, *and* elements $\lambda_i, \lambda, \mu_i$, and μ can be arbitrary elements from K.

She has to select β^* as a nontrivial multivariate polynomial of degree 2.

Alice uses the transformation $h = H(\varphi(1), \varphi(2), ..., \varphi(t), \beta(1), \beta(2), ..., \beta(t-1), \beta^*(t))$ and compute the standard form of $G = L_1 H(\varphi(1), \varphi(2), ..., \varphi(t), \beta(1), \beta(2), ..., \beta(t-1), \beta^*(t)) L_2$ of kind $y_1 \longrightarrow g_1(y_1, y_2, ..., y_n)$, $y_2 \longrightarrow g_1(y_1, y_2,..., y_n), ..., y_n \longrightarrow g_n(y_1, y_2, ..., y_n)$.

Alice sends the multivariate polynomials g_i to Bob via the open channel. He will use it to encrypt the plaintext from K^n.

Private Decryption Procedure. Let us assume that Alice gets the ciphertext c from Bob.

At the beginning, Alice forms an intermediate tuple $L_1(p) = [y_1, y_2, ..., y_n]$ and treats its coordinates as variables y_i.

She computes the vector $b = (L_2)^{-1}(c) = (b_1, b_2, ..., b_n)$.

She forms the tuple $(\varphi(t), b_2, b_3, ..., b_n) = u$ and computes invariants $a_i(u)$ for $i = 2, 3, ..., i(1)-1$. Alice computes $\Sigma_{i=2,3,..., i(1)-1} a_i(u)\lambda_i+\lambda = t(1)$ and $\Sigma_{i=2,3,..., i(1)-1} a_i(u)\mu_i+\mu = t(2)$ which coincide with the $\Sigma_{i=2,3,..., i(1)-1} a_i([\alpha_2, y_2, y_3, ..., y_n])\lambda_i+\lambda$ and $\Sigma_{i=2,3,..., i(1)-1} a_i([\alpha_2, y_2, y_3, ..., y_n])\mu_i+\mu)$ respectively.

She solves $d((d'y_1+t(1))^r+t(2) = b_1$ for y_1 and gets the solution $y_1 = y^*_1$.

She computes $\beta^*(t-1) = y^*_1+c(t-1)$, $\beta^*(t-2) = = y^*_1+c(t-2), ..., \beta^*(1) = y^*_1+c(1)$.

Alice computes $N_{\beta^*(t-1)}(u) = {}^{1}u$, $N_{\alpha(t-2)}({}^{1}u) = {}^{2}u$, $N_{\beta^*(t-2)}({}^{2}u) = {}^{3}u$,

$N_{\alpha(t-3)}({}^{3}u) = {}^{4}u, ..., N_{\beta^*(1)}({}^{2t-4}u) = {}^{2t-3}u$, $N_{\alpha(1)} = (\alpha(1), y^*_2, y^*_3, ..., y^*_n)$. So Alice gets the intermediate tuple $[y_1, y_2, ..., y_n] = y^*_1, y^*_2,..., y^*_n] = y^*$.

She computes the plaintext $[p]$ as $(L_1)^{-1}(y^*)$.

3. Special endomorphisms of $K[x_1, x_2..., x_n]$ and cryptosystems of post quantum cryptography

3.1. Some definitions

Affine Cremona Semigroup ${}^{n}CS(K)$ 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 Cremona object of Algebraic Geometry (see Max Noether paper [32] about Mathematics of Luigi Cremona who was the prominent figure in Algebraic Geometry in the XIX century, [33] and further references on papers which use the term *affine Cremona group*). Element of the semigroup σ can be given via its values on variables, i.e. as the rule $x_i \longrightarrow f_i(x_1, x_2, ..., x_n)$, $i = 1, 2,..., n$. This rule induces the map $\sigma': (a_1, a_2, ..., a_n) \longrightarrow (f_1(a_1, a_2,.., a_n), f_2(x_1, x_2, ..., x_n), ..., f_n(x_1, x_2, ..., x_n))$ on the free module K^n. Automorphisms of $K[x_1, x_2, ..., x_n]$ form affine Cremona Group ${}^{n}CG(K)$.

Let ${}^{n}ES(K)$ stands for the semigroup of all endomorphisms of $K[x_1, x_2, ..., x_n]$ of kind

$$\begin{aligned} &x_1 \longrightarrow \mu_1 x_1^{a(1,1)} x_2^{a(1,2)} ... x_n^{a(1,n)}, \\ &x_2 \longrightarrow \mu_2 x_1^{a(2,1)} x_2^{a(2,2)} ... x_n^{a(2,n)}, \\ &... \\ &x_n \longrightarrow \mu_n x_1^{a(n,1)} x_2^{a(n,2)} ... x_n^{a(n,n)}, \end{aligned} \quad (1)$$

where K is a finite commutative ring with the multiplicative group K^* of regular elements (nonzero

divisors) of the ring. $a(i, j)$ are elements of arithmetic ring Z_d, $d=|K^*|$, $M_1 \in K^*$.

We consider the natural action of Eulerian semigroup ${}^nES(K)$ on the set ${}^nE(K) = (K^*)^n$. Let ${}^nEG(K)$ stand for the Eulerian group of invertible transformations from ${}^nES(K)$. They act as bijective maps on the variety $(K^*)^n$.

We can use the following method of generating invertible elements.

Let π and δ be two permutations on the set $\{1, 2, ..., n\}$. Let us consider a transformation of $(K^*)^n$, $d = |K^*|$. (the most important cases are $K = Z_m$ or $K = F_q$). We define transformation ${}^A\mathcal{JG}(\pi, \delta)$, where A is a triangular matrix with positive integer entries $0 \le a(i,j) \le d$, $i \ge j$ defined by the following closed formula.

$y_{\pi(1)} = M_1 x_{\delta(1)}^{a(1,1)}$

$y_{\pi(2)} = M_2 x_{\delta(1)}^{a(2,1)} x_{\delta(2)}^{a(2,2)}$

...

$y_{\pi(n)} = M_n x_{\delta(1)}^{a(n,1)} x_{\delta(2)}^{a(n,2)} \dots x_{\delta(n)}^{a(n,n)}$

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

We refer to ${}^A\mathcal{JG}(\pi, \delta)$ as Jordan—Gauss multiplicative transformation or simply $\mathcal{JG}$ element. It is an invertible element of ${}^nES(K)$ with the inverse of kind ${}^B\mathcal{JG}(\delta, \pi)$ such that $a(i,i)b(i,i)=1 \pmod d$. Notice that in the case $K = Z_m$ straightforward process of computation of the inverse of the $\mathcal{JG}$ element is connected with the factorization problem of integer m.

3.2. Some algorithms

So Alice can generate the element $\mathcal{J}$ as a product of several Jordan Gauss transformations. The simplest case in the spirit of LU factorization is the composition of lower and upper triangular transformations.

The cryptosystem is the following procedure.

Alice can select several Jordan-Gauss transformations $\mathcal{J}_1, \mathcal{J}_2, ..., \mathcal{J}_d$, $d>1$ from ${}^mEG(K)$ and compute their product J. One of the options is to send J to public user Bob. It looks like the security of such a cryptosystem depends on the choice of commutative ring K (see [34]).

We suggest the following use $\mathcal{J}$ as a public rule.

Public user works with the space of plaintexts $(K^*)^m$.

The idea to use polynomial map F of bounded degree with the trapdoor accelerator T is used in *[dop], [arch]* for the construction of multivariate public key in the case of special rings $K = F_q$ and $K = Z_q$. These schemes use cubic endomorphism F of $K[x_1, x_2, ..., x_n]$ with the trapdoor accelerator T defined in terms of graphs $D(n, K)$ (or their homomorphic images $A(n, K)$). We suggest the following modification of these algorithms.

3.3. Multivariate public key of unbounded degree

Alice selects the finite commutative ring K with unity. She selects parameter n to work with the endomorphisms of $K[x_1, x_2, ..., x_n]$. Alice takes positive integer $d = O(1)$, $d>2$ and selects Jordan-Gauss multiplicative transformations $\mathcal{J}_1, \mathcal{J}_2, ..., \mathcal{J}_d$,. She computes their inverses $(\mathcal{J}_j)^{-1}$ and the composition $\mathcal{J} = \mathcal{J}_1\mathcal{J}_2, ..., \mathcal{J}_d$

Alice takes parameters m and k such that $n = m-k$. She selects graph $D_T(m, K)$ such that T contains k elements.

Alice chooses affine and transformations L_1 and L_2 from

$AGL_n(K)$. She forms $\alpha(1), \alpha(2), ..., \alpha(t), \beta(1), \beta(2), ..., \beta(t-1), \beta^*(t)$ of Algotithm 1 of section 2. Alice uses the transformation $G = L_1H(\alpha(1), \alpha(2), ..., \alpha(t), \beta(1), \beta(2), ..., \beta(t-1), \beta^*(t))\, L_2$.

She computes the standard form F of $\mathcal{JG}$ which has linear degree $O(n)$ and density $O(n^4)$.

Alice sends F to public user Bob.

Correspondents Alice and Bob use the variety $(K^*)^n$ as the space of plaintexts and a free module $(K)^n$ as the space of ciphertexts.

Bob writes the plaintexts $p = (p_1, p_2, ..., p_n)$ in the alphabet K^*. He sends the ciphertexts $c = F(p)$ to Alice.

Alice computes $u = G^{-1}(c)$ according to her private decryption procedure of Algorithm 1. Noteworthy that u is an element of $(K^*)^n$.

Alice computes consequtively

${}^du = \mathcal{J}_d(u)$,

${}^{d-1}u = \mathcal{J}_{d-1}({}^du), ..., {}^1u = \mathcal{J}_1({}^2u) = p$.

4. Conclusions

Multivariate Cryptography in a wide sense is about constructions and investigations of Public Keys in the form of nonlinear Multivariate rules defined over some finite commutative ring K.

This rule F has to be written as transformation $x_i \to f_i$, $i = 1, 2, ..., n$, $f_i \in K[x_1, x_2, ..., x_n]$ over the commutative ring K. Bijective F can be used for the encryption of tuples (plaintexts) from the affine space K^n. Multivariate rules can serve as instruments for the creation of digital signatures. In the case of bijective transformation, the decryption process can be thought of as an application of inverse rule G. The degree of G can be defined as the maximum of degrees of polynomials $G(x_i)$, $i = 1, 2, ..., n$. For the usage of given publicly, F as an efficient and secure instrument its degree of has to be bounded by some constant c (traditionally $c = 2$) but the polynomial degree of the inverse G has to be high.

The key owner (Alice) is supposed to have some additional piece S of private information about pair (F, G) to decrypt ciphertext obtained from the public user

(Bob). Recall that the family F_n, $n = 2, 3, ...$ from $K[x_1, x_2,..., x_n]$ has trapdoor accelerator ${}^nS$ if the knowledge of the piece of information ${}^nS$ allows to compute reimage x of $y = F_n(x)$ from K^n in time $O(n^2)$. Of course, the concept of trapdoor accelerator is just an instrument to search for practical trapdoor functions. As you know the existence of theoretical trapdoor functions is just a conjecture. It is closely connected to the Main Conjecture of Cryptography about the fact that $P \neq NP$.

Without the knowledge of S_n one has to solve a nonlinear system of equations which generally is an NP-hard problem. The finding of the inverse for F_n is an NP-hard problem if these maps are in the so-called "general position". In the case of specific maps additional argumentation of the complexity to find inverses G_n can be useful.

We present such heuristic arguments in the case of $D_T(n, K)$ based encryption defined for arbitrary commutative ring K with unity with at least 3 elements and presented in the previous section. Subset T can be viewed as part of the corresponding trapdoor accelerator ${}^nS$.

Graphs $D_T(n, K)$ have partition sets K^n (set of points and set of lines), and the incidence relation between points and lines is given by the system of linear equations over K.

To define the trapdoor accelerator for standard forms F_n, $n = 2, 3, ...$ we use special walks on graphs $D_T(n, K)$ and $D_T(n, K[x_1, x_2, ..., x_n])$. The constructed map F_n acts on the selected partition set K^n. In the case of trivial affine transformations L_1 and L_2 the relation $F_n(x) = y$ for $x = (x_1, x_2, ..., x_n)$ and $y = (y_1, y_2, ..., y_n)$ vertices x and y are joint in the graph $D_T(n, K)$ by the path of length $>cn$, where c is positive constant.

Finding the path will give us the trapdoor accelerator for the computation of preimages. This can be done by the Dijkstra algorithm of complexity O(v ln(v)) where v is the order of graphs. It could not be done in polynomial time because $v = 2|K|^n$ and $|K| \geq 3$. Noteworthy that the usage of nontrivial L_1 and L_2 will complicate the cryptanalysis.

Noteworthy that any nonlinear system of multivariate equations of of constant degree d over a finite field can be rewritten as a quadratic system with extra variables.

Studies of quadratic multivariate public rules over finite rings with zero divisors is an interesting task for cryptanalysts. Arithmetical rings modulo 2^s is an important practical task because several natural alphabets for the presentation of files in informatics have size which is the power of 2. We are looking for the K-theory of multivariate cryptography and presenting the public rule defined over a general finite commutative ring with unity.

We believe that studies of multivariate public rules of polynomial degree in variable n and the polynomial density are also interesting areas of research.

So we present a new cryptosystem from this area obtained via the composition of the Eulerian map of unbounded degree $O(n)$ with the constructed quadratic endomorphism of $K[x_1, x_2, ..., x_n]$ with the trapdoor accelerator.

Funding

This research is supported by the British Academy Fellowship for Researchers under Risk 2022 and by the British Academy Award LTRSF\100333 and UMCS Mini-Grants.

References

[1] V. Ustimenko, A. Wróblewska, On Extremal Algebraic Graphs, Quadratic Multivariate Public Keys and Temporal Rules, FedCSIS (2023) 1173–1178.

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

[4] V. Ustimenko, On New Multivariate Cryptosystems Based on Hidden Eulerian Equations Over Finite Fields, archive.2017/093(PDF).

[5] V. Ustimenko. On New Multivariate Cryptosystems Based on Hidden Eulerian Equations, Reports of the National Academy of Sciences of Ukraine 5 (2017). doi: 10.15407/dopovidi2017. 05.017.

[6] J. Ding, A. Petzoldt, Current State of Multivariate Cryptography, IEEE Security & Privacy 15(4) (2017) 28–36. doi: 10.1109/MSP.2017.3151328.

[7] D. Smith-Tone, 2F—A New Method for Constructing Efficient Multivariate Encryption Schemes, Proceedings of PQCrypto 2022, LNCS 13512 (2022). doi: 10.1007/978-3-031-17234-2_10.

[8] D. Smith-Tone, New Practical Multivariate Signatures from a Nonlinear Modifier, PQCrypto 2021, LNCS 12841 (2021). doi: 10.1007/978-3-030-81293-5_5.

[9] D. Smith-Tone, C. Tone, A Nonlinear Multivariate Cryptosystem Based on a Random Linear Code, URL: https://eprint.iacr.org/2019/1355.pdf

[10] 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.

[11] F. Cabarcas, D. Cabarcas, J. Baena, Efficient Public-Key Operation in Multivariate Schemes, Advances in Mathematics of Communications 13(2) (2019).

[12] R. Cartor, D. Smith-Tone, EFLASH: A New Multivariate Encryption Scheme, International Conference on Selected Areas in Cryptography, LNCS 11349 (2019) 281–299. doi: 10.1007/978-3-030-10970-7_13

[13] A. Casanova, et al., Gemss: A Great Multivariate Short Signature, Submission to NIST (2017) 209–229.

[14] J. Chen, et al., A New Encryption Scheme for Multivariate Quadratic Systems, Theoretical Comput. Sci. 809 (2020) 372–383. doi: 10.1016/j.tcs.2019.12.032.

[15] M.-S. Chen, et al., SOFIA: MQ-based Signatures in the QROM, IACR Inter-National Workshop on Public Key Cryptography. Springer (2018) 3–33. doi: 10.1007/978-3-319-76581-5_1.

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

[17] D. H. Duong, et al., An Efficient Multi-Variate Threshold Ring Signature Scheme, Comput. Stand. Interfaces 74 (2021). doi: 10.1016/J.CSI.2020. 103489.

[18] J.-C. Faugère, et al., A New Perturbation for Multivariate Public Key Schemes Such as HFE and UOV, Cryptology ePrint Archive (2022).

[19] N. Biggs, Algebraic Graphs Theory, Second Edition, Cambridge University Press (1993).

[20] A. Brower, A. Cohen, A. Nuemaier, Distance Regular Graphs, Springer (1989).

[21] B. Bollob´as, Extremal Graph Theory, Academic Press (1978).

[22] V. Ustimenko, Maximality of Affine Group, Hidden Graph Cryptosystem and Graph's Stream Ciphers, J Algebra Discrecadete Math. 1 (2005) 51–65

[23] V. A. Ustimenko, Linguistic Dynamical Systems, Graphs of Large Girth and Cryptography, J. Math. Sci. 140(3) (2007) 412–434.

[24] V. Ustimenko, Graphs in Terms of Algebraic Geometry, Symbolic Compu-tations and Secure Communications in Post-Quantum World, UMCS Editorial House (2022).

[25] V. Ustimenko, 2023, Schubert cells and quadratic public keys of Multivariate Cryptography, in: 3rd International Workshop on Information Technologies: Theoretical and Applied Problems, vol. 3628 (2023) 598–604.

[26] V. Ustimenko, T. Chojecki, M. Klisowski, On Extremal Algebraic Graphs and Implementations of New Cubic Multivariate Public Keys, FedCSIS 35 (2023) 1179–1184. doi: 10.15439/2023 F7763.

[27] V. Ustimenko, On Extremal Graph Theory and Symbolic Computations, Dopovidi National Academy of Sci. 2 (2013) 42–49.

[28] F. Lazebnik, V. Ustimenko, A. J. Woldar, A New Series of Dense Graphs of High Girth, Bulletin of the AMS 32(1) (1995), 73–79.

[29] N. Bourbaki, Lie Groups and Lie Algebras, Springer (1998).

[30] V. Ustimenko, Algebraic Groups and Small World Graphs of High Girth, Albanian J. Math. 3(1) (209) 26–33.

[31] F. Lazebnik, R. Viglione, On the Connectivity of Certain Graphs of High Girth, Discrete Math. 277 (2004) 309–319.

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

[33] V. L. Popov, Roots of the affine Cremona Group, Affine Algebraic Geometry, Seville, Contemporary Mathematics 369 (2005) 12–13.

[34] V. Ustimenko, On Eulerian Semigroups of Multivariate Transformations and Their Cryptographic Applications, European J. Math. 9(93) (2023).

[35] M.-J. Saarinen, D. Smith-Tony, Post Quantum Cryptography, 15th International Workshop, PQCrypto 2024, Part 1 (2024).

[36] M.-J. Saarinen, D. Smith-Tony, Post Quantum Cryptography, 15th International Workshop, PQCrypto 2024, Part 2 (2024).

[37] T. Takagi, et al., International Symposium on Mathematics, Quantum Theory, and Cryptography, Proceedings of MQC 2019, Open Access (2021).

[38] K. Arai, Advances in Information and Communication, Proceedings of the 2024 Future of Information and Communication Conference (FICC) 1–3, LNNS 919–921 (2024). doi: 10.1007/978-3-030-98012-2.

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