On the Jordan-Gauss graphs and new multivariate public keys

Vasyl Ustymenko^{1,2[0000-0002-2138-2357]}, Tymoteusz Chojecki^{3[0000-0002-3294-2794]}, and Aneta Wróblewska^{3[0000-0001-9724-4586]}

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

https://royalholloway.ac.uk/

² Institute of Telecommunication and Global Information Space Kyiv, Ukraine https://itgip.org/en/

³ Maria Curie-Skłodowska University, Pl. M. Curie-Skłodowskiej 5,20-031 Lublin,

Poland

www.umcs.pl

Abstract. We suggest two families of multivariate public keys defined over arbitrary finite commutative ring K with unity. The first one has 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 $K[x_1, x_2, \ldots, x_n]$ sending each variable x_i to a monomial term with the quadratic encryption map of the first cryptosystem. The resulting map has unbounded degree of size O(n) and the density $O(n^3)$ like in the case of cubic multivariate map public user need $O(n^4)$ elementary operations to encrypt. 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 \cdot Graph based symbolic computations \cdot Quadratic public keys \cdot Multivariate Public keys of unbounded degree

1 Introduction

This paper presents the generalisation 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 standardisation best known quantum-resistant algorithms of asymmetrical cryptography. The first round was finished in March 2019, essential part of presented algorithms were rejected. At the same time, the development of new algorithms with postquantum perspective was continued. Similar process took place during the 2^{nd} , 3^{rd} , and 4^{th} 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 4 winners of this competition were announced in 2022, they are developed in terms of Lattice Theory.

It is 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. Thus, a large class of protocols supported by asymmetric algorithms of the El Gamal type was eliminated. We have been working on the design of new algorithms from this class during our project. We must admit that the general interest in various aspects of Multivariate Cryptography was connected with the search for secure and effective procedures for digital signatures, where the mentioned above ROUV cryptosystem was considered a serious candidate to produce the shortest signatures.

Let us summarize the outcomes of the aforementioned NIST tender. There are five categories that 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 roundâĂŤthis is the current official status). However, the current eight final winners and candidates belong to only four different mathematical problems (not the five announced at the beginning): lattice-based, hash-based, code-based, supersingular elliptic curve isogeny-based.

The standards are to be published in 2024. However, already at the end of round 3, the last candidate ("Rainbow") from the multivariate cryptography (MVC) category was eliminated. An interesting obfuscation, "TUOV: Triangular Unbalanced Oil and Vinegar," was presented to NIST by the principal submitter Jintaj Ding [39].

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

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

For each pair (K, n) where n > 1, we present a quadratic automorphism σ of $K[x_1, x_2, \ldots, x_n]$ with a trapdoor accelerator T defined via 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 arithmetic rings \mathbb{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 unbounded degree and density $O(n^4)$. Therefore, the complexity of encryption is similar to that of a classical cubic map.

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], [20], [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 we write $v \ G \ u$ for the adjacent vertices u and v (or neighbours). 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 the other is a line. We shall identify I with the simple graph of this incidence relation or bipartite graph. The pair (x, y), where $x \in P$ and $y \in L$ such that xIy, 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 a 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:

$$a_{1}x_{s+1} - b_{1}y_{r+1} = f_{1}(x_{1}, x_{2}, \dots, x_{s}, y_{1}, y_{2}, \dots, y_{r})$$

$$a_{2}x_{s+2} - b_{2}y_{r+2} = f_{2}(x_{1}, x_{2}, \dots, x_{s}, x_{s+1}, y_{1}, y_{2}, \dots, y_{r}, y_{r+1})$$

$$\vdots$$

$$a_{m}x_{s+m} - b_{m}y_{r+m} = f_{m}(x_{1}, x_{2}, \dots, x_{s}, x_{s+1}, \dots, x_{s+m-1}, y_{1}, y_{2}, \dots, y_{r})$$

$$y_{r+1}, \dots, y_{r+m-1})$$

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

The color $\rho(x) = \rho((x))$ (and $\rho(y) = \rho([y])$) 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 incidence graph there exists a unique neighbour 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 neighbour 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 neighbour of the line $(p) = N_c([l])$ with the color c. The triples of parameters s, r, m define the type of linguistic graph.

We consider also linguistic incidence structures defined by an infinite number of equations. Linguistic graphs are defined up to isomorphism. We refer to the written above equations as canonical equations of linguistic graph. We say that a linguistic graph is of Jordan-Gauss type if the map $[(x), [y]] \rightarrow$ $(f_1(x_1, x_2, \ldots, x_s, y_1, y_2, \ldots, y_r), f_2(x_1, x_2, \ldots, x_s, x_{s+1}, y_1, y_2, \ldots, y_r, y_{r+1}), \ldots,$ $f_{m-1}(x_1, x_2, \ldots, x_s, x_{s+1}, \ldots, x_{s+m-1}, y_1, y_2, \ldots, y_r, y_{r+1}, \ldots, y_{r+m-1}))$ where $(x) \in K^{s+m}, [y] \in K^{r+m}$ is a bilinear map into K^1 . Thus, all f_i are special quadratic maps. In the case of Jordan-Gauss graphs, the neighbourhood 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 neighbour 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 neighbour of the line $(p) = N_c([l])$ with the color c. We refer to the operator of taking the neighbour of a vertex according to the chosen color as the neighbourhood operator.

On the sets P and L of points and lines of the linguistic graph, we define jump operators ${}^{1}J = {}^{1}J_{b}(p) = (b_{1}, b_{2}, \ldots, b_{s}, p_{1}, p_{2}, \ldots, p_{s+m})$, where $(b_{1}, b_{2}, \ldots, b_{s}) \in K^{s}$ and ${}^{2}J = {}^{2}J_{b}([l]) = [b_{1}, b_{2}, \ldots, b_{r}, l_{1}, l_{2}, \ldots, l_{r+m}]$, where $(b_{1}, b_{2}, \ldots, b_{r}) \in K^{r}$. We refer to the tuple (s, r, m) as the type of the linguistic graph I.

We say that point (p) and line [l] are adjacent in the linguistic graph I if ${}^{1}J_{b}(p)I^{2}J_{c}[l]$ 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 a linguistic graph has degree $d, d \geq 2$ if the maximal degree of nonlinear multivariate polynomials $f_{i}, i = 1, 2, ..., m$ is d.

Noteworthy, the path v_0, v_1, \ldots, v_k in the linguistic graph I_m is determined by the starting vertex v_0 and the colors of vertices 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 colors 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 $v_1 = {}^1J_{c(1)}(v_0), v_2 = N_{c(2)}(v_1), v_3 = {}^2J_{c(3)}(v_2), v_4 = N_{c(4)}(v_3), v_5 = {}^1J_{c(5)}(v_4)$ the relations $v_0\psi v_3, v_2\psi v_5$ hold.

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

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

For each positive integer l we can consider the graph $I_m(K)$ together with ${}^{l}J_m = I_m(K[y_1, y_2, \ldots, y_l])$ 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 $(y_1, y_2, \ldots, y_s, y_{s+1}, y_{s+2}, \ldots, y_{s+1})$

 (\dots, y_{m+s}) and colors $c(1), c(2), \dots, c(t)$ such that $c(i) \in K[y_1, y_2, \dots, y_s]^s$ for $i = 0, 1 \mod 4$ and $c(i) \in K[y_1, y_2, \dots, y_s]^r$ for $i = 2, 3 \mod 4$. Assume that $c(t) = (h_1(y_1, y_2, \dots, y_s), h_2(y_1, y_2, \dots, y_s), \dots, h_s(y_1, y_2, \dots, y_s)).$

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), cPass, $c \in K[x_1, x_2, \ldots, x_s]^{(2t+1)s+2rt}$ 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

$$y_{1} \rightarrow h_{1}(y_{1}, y_{2}, \dots, y_{s}),$$

$$y_{2} \rightarrow h_{2}(y_{1}, y_{2}, \dots, y_{s}),$$

$$\vdots$$

$$y_{s} \rightarrow h_{s}(y_{1}, y_{2}, \dots, y_{s}),$$

$$y_{s+1} \rightarrow g_{1}(y_{1}, y_{2}, \dots, y_{s}, y_{s+1}, y_{s+2}, \dots, y_{s+m}),$$

$$y_{s+2} \rightarrow g_{2}(y_{1}, y_{2}, \dots, y_{s}, y_{s+1}, y_{s+2}, \dots, y_{s+m}),$$

$$\vdots$$

$$y_{s+m} \rightarrow g_{m}(y_{1}, y_{2}, \dots, y_{s}, y_{s+1}, y_{s+2}, \dots, y_{s+m}).$$

It is easy to see that this transformation is bijective if and only if the map $y_1 \rightarrow h_1(y_1, y_2, \ldots, y_s), y_2 \rightarrow h_2(y_1, y_2, \ldots, y_s), \ldots, y_s \rightarrow h_s(y_1, y_2, \ldots, y_s)$ is bijective on K^s [24]. The defined above transformations form a semigroup $I(K)S_P$ of multivariate transformations. 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 transformations of the kind I(K),cPass, $c \in K[x_1, x_2, \ldots, x_s]^{(2t+1)r+2ts}$ acting on the variety K^{m+r} .

Remark 1. We may omit some operators of the kind $J_{c(i)}$ by making the color c(i) 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 the maximum degree of the polynomials $c_i(x_1, x_2, \ldots, x_s)$.

In [25], a special Jordan-Gauss graph $JG(r, s, m, F_q)$, where $q = 2^t, t > 1$ was used for the construction of a 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 the 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] used Jordan-Gauss graphs $A(n, F_q)$ [27] and $D(n, F_q)$ (see [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 a 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 (see [23]).

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

The affine root system \tilde{A}_1 (A_1 with a wave, see [29]) is the totality of vectors in the two-dimensional Euclidean space \mathbb{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), $i \ge 1$. All multiples of (1,1) are known as imaginary roots, while other roots which 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. Thus, we obtain a set Root consisting of roots of \tilde{A}_1 and elements (i, i)', i > 1.

Let $R_1 = \text{Root} \setminus \{(0, 1)\}$ and $R_2 = \text{Root} \setminus \{(1, 0)\}$ and let K be a commutative ring with unity. We consider sets $L_i = K^{R_i}$, i = 1, 2, of all functions f from R_i 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 $[y] = [y_{0,1}, y_{1,1}, y_{1,2}, y_{2,1}, y_{2,2}, y'_{2,2}, \dots, y_{i,i+1}, y_{i+1,i}, y_{i+1,i+1}, y'_{i+1,i+1}, \dots]$ 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:

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

(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 $i \ge 0$.

Graphs CD(k, K) with $k \ge 6$ were introduced in [23], as induced subgraphs of D(k, K) with vertices u satisfying special equations $a_2(u) = 0, a_3(u) =$ $0, \ldots, a_t(u) = 0, t = [(k+2)/4]$, where $u = (u_\alpha, u_{1,1}, u_{1,2}, u_{2,1}, \ldots, u_{r,r}, u'_{r,r}, u_{r,r+1}, u_{r+1,r}, \ldots), 2 \le r \le t, \alpha \in \{(1,0), (0,1)\}$ is a vertex of D(k, K) and $a_r = a_r(u) = \sum_{i=0}^r (u_{i,i}u'_{r-i,r-i} - u_{i,i+1}u_{r-i,r-1-1})$ 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 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 an 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 an 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 $T = \{j(1), j(2), \ldots, j(s)\}$ of $\{2, 3, \ldots, [(k+2)/2]\}$ via the following procedure:

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

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

Polynomials $a_i(v)$ where 1 < i < j(1) are connectivity invariants of vertex v (point or line) 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 rename the coordinates of points and lines of $D_T(k, K)$ with one variable index *i* accordingly 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 colouring ρ of the set of vertices. We assume that $\rho(x_1, x_2, \ldots, x_n) = x_1$ for the vertex x (point or line) given by the tuple with coordinates x_1, x_2, \ldots, x_n . We refer to x_1 from K as the colour of vertex x.

Recall that N_a and J_a are operators of taking the neighbour with colour a and jump operator changing the original colour of point or line to a new colour 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 $(\alpha(1), \alpha(2), \ldots, \alpha(t))$ and $(\beta(1), \beta(2), \ldots, \beta(t))$ are the sequences of colours from $K[y_1]$ of length

at least 2. We consider the sequence ${}^{0}\!v = y, {}^{1}\!v = J_{\alpha(1)}({}^{0}\!v), {}^{2}\!v = N_{\beta(1)}({}^{1}\!v), {}^{3}\!v = N_{\alpha(2)}({}^{2}\!v), {}^{4}\!v = N_{\beta(2)}({}^{3}\!v), {}^{5}\!v = N_{\alpha(3)}({}^{4}\!v), \dots, {}^{2t-2}\!v = N_{\beta(t-1)}({}^{2t-3}\!v), {}^{2t-1}\!v = N_{\alpha(t)}({}^{2t-2}\!v), {}^{2t}\!v = J_{\beta(t)}({}^{2t-1}\!v).$

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 the polynomial transformation $g(\alpha(1), \alpha(2), \ldots, \alpha(t), \beta(1), \beta(2), \ldots, \beta(t)),$ $t \ge 2$ of affine space K^n of kind $y_1 \to y_1 + \beta(t), y_2 \to v_2(y_1, y_2), y_3 \to v_3(y_1, y_2, y_3),$ $\ldots, y_n \to v_n(y_1, y_2, \ldots, y_n).$

It is easy to see that $g(\alpha(1), \alpha(2), \dots, \alpha(t), \beta(1), \beta(2), \dots, \beta(t)) \cdot g(\gamma(1), \gamma(2), \dots, \gamma(s), \sigma(1), \sigma(2), \dots, \sigma(t)) = g(\alpha(1), \alpha(2), \dots, \alpha(t), \gamma(1)(\beta(t)), \gamma(2)(\beta(t)), \dots, \gamma(s)(\beta(t)), \beta(1), \beta(2), \dots, \beta(s), \sigma(1)(\beta(t)), \sigma(2)(\beta(t)), \dots, \sigma(s)(\beta(t)).$

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

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

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

Proposition 3. Transformations of kind ${}^{n}g = g(\alpha(1), \alpha(2), \ldots, \alpha(t), \beta(1), \beta(2), \ldots, \beta(t)), t \geq 2$ such that $deg(\alpha(i)) = 0$ and $\beta(i) = y_1 + c(i), c(i) \in K, i = 1, 2, \ldots, t$ generate a subgroup ${}^{2}G(\Gamma(n, K))$ of transformation of maximal degree 2.

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

Remark 3. In the case of two quadratic transformations of K^n of "general position", their composition will have degree 4.

We associate with the sequence $\alpha(1), \alpha(2), \ldots, \alpha(t), \beta(1), \beta(2), \ldots, \beta(t-1)$ of Proposition 3 and $\beta^*(t) = f(y_1, y_2, \ldots, y_n)$ of degree 2 another quadratic transformation $h = H(\alpha(1), \alpha(2), \ldots, \alpha(t), \beta(1), \beta(2), \ldots, \beta(t-1), \beta^*(t))$, constructed via the sequence of vertices ${}^{0}v = y, {}^{1}v = J_{\alpha(1)}({}^{0}v), {}^{2}v = N_{\beta(1)}({}^{1}v), {}^{3}v = N_{\alpha(2)}({}^{2}v), {}^{4}v =$ $N_{\beta(2)}({}^{3}v), {}^{5}v = N_{\alpha(3)}({}^{4}v), \ldots, {}^{2t-2}v = N_{\beta(t-1)}({}^{2t-3}v), {}^{2t-1}v = N_{\alpha(t)}({}^{2t-2}v)$. We compute ${}^{2t}v = J_{\beta^*(t)}({}^{2t-1}v) = v$ and define h as the quadratic map $y_i \to v_i$, $i = 1, 2, \ldots, n$.

Theorem 1. Let K be the finite field F_q , $q = 2^r$, r > 1. Then transformation $h = h(\alpha(1), \alpha(2), \ldots, \alpha(t), \beta(1), \beta(2), \ldots, \beta^*(t))$ for which deg $\alpha(i) = 0$, $i = 1, 2, \ldots, t$, $\beta(i) = y_1 + c(i)$, $c(i) \in K$, $i = 1, 2, \ldots, t - 1$ and $\beta^*(t) = (y_1)^2$ is a bijective quadratic transformation of the vector space $(F_q)^n$, and 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 another quadratic public keys.

Let us consider the transformation $h^* = H^*(\alpha(1), \alpha(2), \ldots, \alpha(t-1), \beta(1), \beta(2), \ldots, \beta(l-1), \alpha^*(l))$ where degree $\beta(i) = 0$ for $i = 1, 2, \ldots, t-1$ and $\alpha = y_1 + c(i)$ for $i = 1, 2, \ldots, t-1$, with $\alpha^*(t)$ an element of $K[y_1, y_2, \ldots, y_n]$ of degree at most 2, constructed via the sequence of vertices:

 ${}^{0}v = y, {}^{1}v = J_{\alpha(1)}({}^{0}v), {}^{2}v = N_{\beta(1)}({}^{1}v), {}^{3}v = N_{\alpha(2)}({}^{2}v), {}^{4}v = N_{\beta(2)}({}^{3}v), {}^{5}v = N_{\alpha(3)}({}^{4}v), \dots, {}^{2t-2}v = N_{\beta(t-1)}({}^{2t-3}v), {}^{2t-1}v = J_{\alpha^{*}(t)}({}^{2t-2}v) = (f_{1}, f_{2}, \dots, f_{n}).$

We define h^* as the quadratic map $y_i \to f_i$, i = 1, 2, ..., n. Noteworthy that the walk with two jumps is taken on the graph defined over $K[y_1, y_2, ..., y_n], [y_1, y_2, ..., y_n]$ is starting line of the walk and $(f_1, f_2, ..., f_n)$.

2.1 Algorithm 1: Key Generation and Decryption

Key Generation Procedure. Alice selects a commutative ring K with unity and K^* of order greater than 2, together with parameters k and m. She selects $T = \{j(1), j(2), \ldots, j(m)\}$ 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 $\alpha_1 = c(0) + y_1$, $\alpha_2 = \alpha_1 + d(1), \ldots, \alpha_3 = \alpha_2 + d(2), \ldots, \alpha_{t-1} = \alpha_{t-2} + d(t-1)$ where parameters d(i) are elements of K^* , and $\beta_1 = c(1), \beta_2 = c(2), \ldots, \beta_{t-1} = c(t-1)$ where elements $c(1) - c(2), c(2) - c(3), \ldots, c(t-2) - c(t-1)$ are elements of K^* . Alice forms $\alpha(t)^*$ as a polynomial of the kind

$$d((d'y_1 + \lambda)^r + \sum_{i=2,3,\dots,i(1)-1} a_i([\alpha_1, y_1, y_2, \dots, y_n])\mu_i + \mu)$$

where $d \in K^*$, $d' \in K^*$, r = 2 if the order of $K = F_q$ is a finite field of characteristic 2d, r = 1 in other cases, and elements λ , μ_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 $h^* = H(\alpha(1), \alpha(2), \dots, \alpha(t-1), \beta(1), \beta(2), \dots, \beta(t-1), \alpha^*(t))$ and computes the standard form of $G = L_1 H^*(\alpha(1), \alpha(2), \dots, \alpha(t-1), \alpha(t-1))$,

$$\beta(1), \beta(2), \dots, \beta(t-1), \alpha^{*}(t))L_{2}$$
 of the kind:

 $y_1 \to g_1(y_1, y_2, \dots, y_n), y_2 \to g_2(y_1, y_2, \dots, y_n), \dots, y_n \to g_n(y_1, y_2, \dots, y_n)$

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 the intermediate tuple $L_1(p) = [y_1, y_2, \ldots, y_n]$ 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 $(\beta(t-1), b_2, b_3, \dots, b_n) = u$ and computes invariants $a_i(u)$ for $i = 2, 3, \dots, i(1) - 1$.

Alice computes $\sum_{i=2,3,\ldots,i(1)-1} a_i(u)\mu_i + \mu = t(2)$, which coincide with $\sum_{i=2,3,\ldots,i(1)-1} a_i([\alpha_2, y_2, y_3, \ldots, y_n])\mu_i + \mu)$, 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 $\alpha^*(i)$ for i = 1, 2, ..., t - 1.

 y_1^* and gets the intermediate tuple $[y_1, y_2, \dots, y_n] = [y_1^*, y_2^*, \dots, y_n^*] = y^*$. Finally 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 the endomorphism group of the polynomial ring $K[x_1, x_2, \ldots, x_n]$ over the commutative ring K. It is an important Cremona object of Algebraic Geometry (see Max Noether's paper [32] about the Mathematics of Luigi Cremona, who was a prominent figure in Algebraic Geometry in the XIX century [33] and further references on papers which use the term affine Cremona group). An element of the semigroup σ can be given via its values on variables, i.e., as the rule $x_i \to f_i(x_1, x_2, \ldots, x_n)$, $i = 1, 2, \ldots, n$. This rule induces the map $\sigma': (a_1, a_2, \ldots, a_n) \to (f_1(a_1, a_2, \ldots, a_n), f_2(a_1, a_2, \ldots, a_n), \ldots, f_n(a_1, a_2, \ldots, a_n))$ on the free module K^n . Automorphisms of $K[x_1, x_2, \ldots, x_n]$ form the affine Cremona Group ${}^nCG(K)$.

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

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

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 the arithmetic ring \mathbb{Z}_d , $d = |K^*|$, $\mu_i \in K^*$.

We consider the natural action of the Eulerian semigroup ${}^{n}ES(K)$ on the set ${}^{n}E(K) = (K^{*})^{n}$. Let ${}^{n}EG(K)$ stand for the Eulerian group of invertible transformations from ${}^{n}ES(K)$. 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 $\{1, 2, \ldots, n\}$. Let us consider a transformation of $(K^*)^n$, $d = |K^*|$ (the most important cases are $K = \mathbb{Z}_m$ or $K = \mathbb{F}_q$). We define the transformation ${}^A JG(\pi, \delta)$, 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:

$$y_{\pi(1)} = \mu_1 x_{\delta(1)}^{a(1,1)},$$

$$y_{\pi(2)} = \mu_2 x_{\delta(1)}^{a(2,1)} x_{\delta(2)}^{a(2,2)},$$

$$\vdots$$

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

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

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

3.2 Some Algorithms

Alice can generate the element 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 involves the following procedure:

Alice can select several Jordan-Gauss transformations $J_1, J_2, \ldots, J_d, d > 1$ from ${}^{m}EG(K)$ and compute their product J. One option is to send J to the public user Bob. It seems that the security of such a cryptosystem depends on the choice of the commutative ring K (see [34]).

We suggest the following use of J as a public rule. The public user works with the space of plaintexts $(K^*)^m$.

The idea of using a polynomial map F of bounded degree with the trapdoor accelerator T is used in [34] for the construction of a multivariate public key in the case of special rings $K = \mathbb{F}_q$ and $K = \mathbb{Z}_q$. These schemes use a cubic endomorphism F of $K[x_1, x_2, \ldots, x_n]$ 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 a finite commutative ring K with unity.

She takes parameters m and k such that n = m - k. Alice selects the graph $D_T(m, K)$ such that T contains k elements. She chooses affine transformations L_1 and L_2 from $AGL_n(K)$. She forms $\alpha(1), \alpha(2), \ldots, \alpha(t-1), \beta(1), \beta(2), \ldots, \beta(t-1), \alpha^*(t)$ as in Algorithm 1 of Section 2. Alice uses the transformation $G = L_1 H^*(\alpha(1), \alpha(2), \ldots, \alpha(t-1), \beta(1), \beta(2), \ldots, \beta(t-1), \alpha^*(t))L_2$.

Alice takes a positive integer d = O(1), d > 2, and selects Jordan-Gauss multiplicative transformations J_1, J_2, \ldots, J_d of $K[x_1, x_2, \ldots, x_n]$. She computes their inverses J_i^{-1} and the composition $J = J_1 J_2 \ldots J_d$.

She computes the standard form F of JG, which has a linear degree O(n) and density $O(n^3)$. Alice sends F to the 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 plaintext $p = (p_1, p_2, \ldots, p_n)$ in the alphabet K^* . He sends the ciphertext c = F(p) to Alice. (Alice computes $u = G^{-1}(c)$ according to her private decryption procedure of Algorithm 1. Noteworthy is that u is an element of $(K^*)^n$.

Alice computes consecutively:

$$du = J_d(u),$$

$$d^{-1}u = J_{d-1}(du),$$

$$\dots,$$

$$u = J_1(u) = p$$

The suggested multivariate rule of unbounded degree is pseudo cubic, i. e. The complexity of encryption procedure for public user is $O(n^4)$ like in the case of cubic multivariate rule. Note that in the cases of examples [4], [5] the procedure to encrypt costs $O(n^5)$.

4 Description of the implementation in the case of D(n,q).

After the renumeration of indexes of points and lines, we can assume that the point $(p) = (p_1, p_2, \ldots, p_n)$ is incident with the line $[l] = [l_1, l_2, \ldots, l_n]$, if the following relations between their coordinates hold:

$$l_2 - p_2 = l_1 p_1, \quad l_3 - p_3 = l_2 p_1, \quad l_4 - p_4 = l_1 p_2, \quad l_i - p_i = l_1 p_{i-2},$$

 $l_{i+1} - p_{i+1} = l_{i-1}p_1, \quad l_{i+2} - p_{i+2} = l_ip_1, \quad l_{i+3} - p_{i+3} = l_1p_{i+1} \quad \text{where} \quad i \ge 5.$

Let us denote G as G(n, l, K) in the case when the sequence of colors $b(1), b(2), \ldots, b(l)$ has length l. We present the time of generation (in ms) of element G = G(n, l, K) and the total number M(G) of monomial terms in all g_i . We refer to parameter l as the length of the word. For simplicity, subset J was always selected as a singleton. We can see the "condensed matters physics" digital effect. If t is "sufficiently large", then M(g) is independent of the constant t (c).

We have written a program for generating elements and for encrypting a text using the generated public key. The program is written in SAGE. We used an MacBook with a Intel Core 1,2 GHz processor, 8GB RAM, and the WmaxOS Sieerra operating system. We have implemented three **cases**: **1**. L_1 and L_2 are identities, **2**. L_1 and L_2 are maps of the kind $z_1 \rightarrow z_1 + a_2 z_2 + a_3 z_3 + \cdots + a_t z_t$, $z_2 \rightarrow z_2, z_3 \rightarrow z_3, \ldots, z_n \rightarrow z_n$, with $a_i \neq 0$, $i = 1, 2, \ldots, n$ (linear time of computing for L_1 and L_2), **3**. $L_1 = Ax + b$, $L_2 = A_1x + b_1$; matrices A, A_1 and vectors b, b_1 mostly have nonzero elements.

Tables 2, 4 and 6 present the generation time of the public key in the first case mentioned above. In Tables 1, 3 and 5, we describe the numbers of monomials

in case 1 for different sizes of the field. In Tables 7, 9 and 11, we describe the numbers of monomials in case 2 for different sizes of the field. Tables 8, 10 and 12 present the time of generation of multivariate rules in case 2. The number of monomial terms in the third case is given in Tables 13, 15, and 17. Tables 14, 16, and 18 present the generation time of the public rules in the third case.

A similar program was designed for the case when K is a Boolean ring B_m of size 2^m . Currently, we are expanding this computer package to the case of commutative rings \mathbb{Z}_m , where m is a power of 2.

	Vector size			
Pass length	16	32	64	128
15			1204	
31	123	439	1625	4716
63	123	439	1626	6364
127	122	439	1647	6367

Table 1. Number of coefficients, field of size 2^8 , Case 1.

Table 2. Time (ms), field of size 2^8 , Case 1.

	Vector size			
Pass length	16	32	64	128
15	10	10	12	40
31	5	13	38	113
63	8	30	95	320
127	22	61	197	826

Table 3. Number of coefficients, field of size 2^{12} , Case 1.

	Vector size				
Pass length	$16 \hspace{0.1cm} 32 \hspace{0.1cm} 64 \hspace{0.1cm} 12$				
15			1204		
31			1644		
63			1647		
127	123	439	1647	6367	

	Vector size			
Pass length	16	32	64	128
15	13	11	16	39
31	7	19	55	141
63	11	42	132	469
127	24	87	295	1167

Table 4. Time (ms), field of size 2^{12} , Case 1.

Table 5. Number of coefficients, field of size 2^{16} , Case 1.

	Vector size				
Pass length					
15				2740	
31	123	439	1644	4716	
63				6364	
127	123	439	1647	6367	

Table 6. Time (ms), field of size 2^{16} , Case 1.

	Vector size					
Pass length	16 32 64 128					
15	10	15	22	52		
31	9	24	80	174		
63	15	58	176	679		
127	34	107	407	1682		

Table 7. Number of coefficients, field of size 2^8 , Case 2.

	Vector size					
Pass length						
15				120959		
31	782	4833	32940	192050		
63				240840		
127	781	4832	32930	240840		

	Vector size				
Pass length	16	32	64	128	
15	76	112	531	3349	
31	39	288	1749	10793	
63	101	630		37036	
127	164	1277	10073	100360	

Table 8. Time (ms), field of size 2^8 , Case 2.

Table 9. Number of coefficients, field of size 2^{12} , Case 2.

	Vector size				
Pass length				128	
15				121132	
31				192157	
63	783	4835	32968	241034	
127	783	4835	32967	241036	

Table 10. Time (ms), field of size 2^{12} , Case 2.

	Vector size					
Pass length	16 32 64 128					
15	69	211	1047	8146		
31	89	565	4748	28555		
63	153	1209	13501	79965		
127	380	2482	29101	212006		

Table 11. Number of coefficients, field of size 2^{16} , Case 2.

	Vector size					
Pass length						
		1		121135		
31	783	4835	32968	192168		
63	783	4835	32971	241046		
127	783	4835	32971	241051		

15

	Vector size				
Pass length	16	32	64	128	
15	94	345	1761	9652	
31		-		32550	
63	233	1880	15304	109038	
127	520	4104	33386	277744	

Table 12. Time (ms), field of size 2^{16} , Case 2.

Table 13. Number of coefficients, field of size 2^8 , Case 3.

	Vector size			
Pass length	16	32	64	128
15				1069013
31	2443	17885	136760	1069129
63	2442	17885	136725	1069034
127	2434	17884	136768	1069097

Table 14. Time (ms), field of size 2^8 , Case 3.

	Vector size			
Pass length	16	32	64	128
15	84			212812
31				210437
63				256831
127	312	2760	31016	378571

Table 15. Number of coefficients, field of size 2^{12} , Case 3.

	Vector size			
Pass length	16	32	64	128
15	2447	17948	137240	1073017
31	2448	17945	137247	1073002
63				1072985
127	2448	17946	137254	1073007

	Vector size			
Pass length	16	32	64	128
15				343487
31		1		376482
63	332	3413	34633	464977
127	576	6319	51722	663752

Table 16. Time (ms), field of size 2^{12} , Case 3.

Table 17. Number of coefficients, field of size 2^{16} , Case 3.

	Vector size			
Pass length	16	32	64	128
15	2448	17952	137276	1073256
31	2448	17952	137277	1073261
63	2448	17952	137280	1073261
127	2448	17952	137280	1073266

Table 18. Time (ms), field of size 2^{16} , Case 3.

	Vector size			
Pass length			64	128
15				430393
31				497491
63				622781
127	815	7425	71509	883939

We recommend cases 2 and 3 for practical use in cryptographic applications.

Presented above results can be used for the evaluation of pseudo-cubic multivariate public keys presented in the Section 3. The encryptioon pseudo-cubic map JG has the same number of monomial terms with the quadratic map G. These numbers are reflected in tables 7, 9 and 11 (case 2, fields of order 2^8 , 2^{12} , 2^{16} and tables 13, 15 and 17 (case 3).

The encryption time of single plaintext p is proportional to number of monomial terms. In the case of JG we can simply multiply time of computation of the value of single monomial term on p and number of monomial terms.

5 Conclusion

Multivariate Cryptography in the broad sense involves the construction and investigation of public keys in the form of a nonlinear multivariate rule defined over

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

The key owner (Alice) is supposed to have some additional piece S of private information about the 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 a trapdoor accelerator nS if the knowledge of the piece of information nS allows one to compute the preimage x of $y = F_n(x)$ from K^n in time $O(n^2)$. Of course, the concept of a 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. In fact, 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 is generally an NP-hard problem. Finding the inverse for F_n is an NP-hard problem if these maps are in 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 an arbitrary commutative ring K with unity and at least 3 elements, as presented in the previous section. Subset T can be viewed as part of the corresponding trapdoor accelerator ${}^{n}S$.

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 a 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 $y = (y_1, y_2, ..., y_n)$ implies that vertices x and y are joined in the graph $D_T(n, K)$ by a path of length > cn, where c is a positive constant.

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

It is also noteworthy that any nonlinear system of multivariate equations 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. Arithmetic rings modulo 2^s are an important practical task because several natural alphabets for the presentation of files in informatics have sizes that are powers of 2. We are looking for a "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 polynomial density are also an interesting area of research.

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

References

- Ustimenko, V., Wróblewska, A.: On extremal algebraic graphs, quadratic multivariate public keys and temporal rules. FedCSIS 2023, pp. 1173–1178 (2023). Also available in IACR e-print archive, 2023/738.
- Beullens, W.: Improved Cryptanalysis of UOV and Rainbow. In: Eurocrypt 2021, Part 1, pp. 348–373. Springer, Heidelberg (2021).
- Canteaut, A., Standaert, F.-X. (eds.): Eurocrypt 2021, LNCS, vol. 12696, 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17âĂŞ21, 2021, Proceedings, Part I. Springer, Heidelberg (2021).
- 4. Ustimenko, V.: On new multivariate cryptosystems based on hidden Eulerian equations over finite fields. IACR e-print archive. 2017/093.
- Ustimenko, V.A.: On new multivariate cryptosystems based on hidden Eulerian equations. Dopovidi of National Academy of Science of Ukraine, No. 5, pp. 2017– 2017 (2017).
- Ding, J., Petzoldt, A.: Current State of Multivariate Cryptography. IEEE Security & Privacy, vol. 15, no. 4, pp. 28–36 (2017). https://doi.org/10.1109/MSP.2017. 3151328
- Smith-Tone, D.: 2F A New Method for Constructing Efficient Multivariate Encryption Schemes. In: PQCrypto 2022: The Thirteenth International Conference on Post-Quantum Cryptography, virtual, DC, US (2022).
- Smith-Tone, D.: New Practical Multivariate Signatures from a Nonlinear Modifier. IACR e-print archive, 2021/419.
- Smith-Tone, D., Tone, C.: A Nonlinear Multivariate Cryptosystem Based on a Random Linear Code. https://eprint.iacr.org/2019/1355.pdf, last accessed 2024/07/30.
- Jayashree, D., Dutta, R.: Progress in Multivariate Cryptography: Systematic Review, Challenges, and Research Directions. ACM Computing Survey, vol. 55, issue 12, No. 246, pp. 1–34 (2023). https://doi.org/10.1145/3571071
- Cabarcas, F., Cabarcas, D., Baena, J.: Efficient public-key operation in multivariate schemes. Advances in Mathematics of Communications, vol. 13, no. 2, pp. 343–343 (2019).
- Cartor, R., Smith-Tone, D.: EFLASH: A new multivariate encryption scheme. In: Proceedings of the International Conference on Selected Areas in Cryptography, pp. 281–299. Springer, Heidelberg (2018).

- 20 V. Ustymenko et al.
- Casanova, A., Faugere, J.-C., Macario-Rat, G., Patarin, J., Perret, L., Ryckeghem, J.: Gemss: A great multivariate short signature. Submission to NIST (2017).
- Chen, J., Ning, J., Ling, J., Lau, T. S. C., Wang, Y.: A new encryption scheme for multivariate quadratic systems. Theoretical Computer Science, vol. 809, pp. 372–383 (2020).
- Chen, M.-S., Hülsing, A., Rijneveld, J., Samardjiska, S., Schwabe, P.: SOFIA: MQ-based signatures in the QROM. In: Proceedings of the IACR International Workshop on Public Key Cryptography, pp. 3–33. Springer, Heidelberg (2018).
- Ding, J., Petzoldt, A., Schmidt, D.S.: Multivariate Public Key Cryptosystems. 2nd edn. Advances in Information Security. Springer, Heidelberg (2020).
- 17. Duong, D.H., Tran, H.T.N., Susilo, W., Luyen, L.V.: An efficient multivariate threshold ring signature scheme. Computer Standards & Interfaces, vol. 74 (2021).
- Faugere, J.-C., Macario-Rat, G., Patarin, J., Perret, L.: A new perturbation for multivariate public key schemes such as HFE and UOV. Cryptology ePrint Archive (2022).
- Biggs, N.: Algebraic Graph Theory. 2nd edn. Cambridge University Press, Cambridge (1993).
- Brower, A., Cohen, A., Nuemaier, A.: Distance Regular Graphs. Springer, Berlin (1989).
- 21. Bollobas, B.: Extremal Graph Theory. Academic Press, London (1978).
- Ustimenko, V.: Maximality of affine group, hidden graph cryptosystem and graph's stream ciphers. Journal of Algebra and Discrete Mathematics, vol. 1, pp. 51–65 (2005).
- Ustimenko, V.A.: Linguistic Dynamical Systems, Graphs of Large Girth and Cryptography. Journal of Mathematical Sciences, Springer, vol. 140, no. 3, pp. 412–434 (2007).
- Ustimenko, V.: Graphs in terms of Algebraic Geometry, symbolic computations and secure communications in Post-Quantum world. UMCS Editorial House, Lublin (2022).
- Ustimenko, V.: Schubert cells and quadratic public keys of Multivariate Cryptography. CEUR Workshop Proceedings ITTAP, https://ceur-ws.org/Vol-3628/, last accessed 2024/07/30.
- Ustimenko, V., Chojecki, T., Klisowski, M.: On Extremal Algebraic Graphs and implementations of new cubic Multivariate Public Keys. FedCSIS 2023, pp. 1179– 1184 (2023). Also available in IACR e-print archive, 2023/744.
- Ustimenko, V.: On extremal graph theory and symbolic computations. Dopovidi National Academy of Sciences, Ukraine, no. 2, pp. 42–49 (2013).
- Lazebnik, F., Ustimenko, V., Woldar, A.J.: A new series of dense graphs of high girth. Bulletin of the AMS, vol. 32, no. 1, pp. 73–79 (1995).
- Bourbaki, N.: Lie Groups and Lie Algebras, Chapters 1-9. Springer, Heidelberg (1998–2008).
- Ustimenko, V.: Algebraic groups and small world graphs of high girth. Albanian Journal of Mathematics, vol. 3, no. 1, pp. 26–33 (2009).
- Lazebnik, F., Viglione, R.: On the connectivity of certain graphs of high girth. Discrete Mathematics, vol. 277, pp. 309–319 (2004).
- 32. Noether, M.: Luigi Cremona. Mathematische Annalen, vol. 59, pp. 1-19 (1904).
- 33. Popov, V.L.: Roots of the affine Cremona group. In: Affine Algebraic Geometry, Seville, Spain, June 18-21, 2003. Contemporary Mathematics, vol. 369, American Mathematical Society, Providence, RI, pp. 12–13 (2005).

21

- Ustimenko, V.: On Eulerian semigroups of multivariate transformations and their cryptographic applications. European Journal of Mathematics, vol. 9, pp. 93–93 (2023).
- Saarinen, M.J., Smith, D.T. (eds.): Post Quantum Cryptography, 15th International Workshop, PQCrypto 2024, Oxford, UK, June 12-14, 2024, Proceedings, Part 1. Springer, Heidelberg (2024).
- Saarinen, M.J., Smith, D.T. (eds.): Post Quantum Cryptography, 15th International Workshop, PQCrypto 2024, Oxford, UK, June 12-14, 2024, Proceedings, Part 2. Springer, Heidelberg (2024).
- Takagi, T., Wakayama, M., Tanaka, K., Kunihiro, N., Kimoto, K., Ikematsu, Y. (eds.): International Symposium on Mathematics, Quantum Theory, and Cryptography, Proceedings of MQC 2019. Open Access, Springer, Heidelberg (2021).
- Arai, K. (ed.): Advances in Information and Communication, Proceedings of the 2024 Future of Information and Communication Conference (FICC), Volumes 1-3. Lecture Notes in Networks and Systems, vols. 919-921, Springer, Heidelberg (2024).
- 39. NIST PQC Digital Signature Project: TUOV Specification. https: //csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/ spec-files/TUOV-spec-web.pdf, last accessed 2024/07/30.