Algebra and Discrete Mathematics RESEARCH ARTICLE
Volume **19** (2015). Number 1, pp. 101–129

On two windows multivariate cryptosystem depending on random parameters

Urszula Romańczuk-Polubiec and Vasyl Ustimenko

Communicated by V. I. Sushchansky

Abstract. The concept of multivariate bijective map of an affine space K^n over commutative Ring K was already used in Cryptography. We consider the idea of nonbijective multivariate polynomial map F_n of K^n into K^n represented as "partially invertible decomposition" $F_n^{(1)}F_n^{(2)}\dots F_n^{(k)}$, $k = k(n)$, such that knowledge on the decomposition and given value $u = F(v)$ allow to restore a special part v' of reimage v. We combine an idea of "oil and vinegar signatures cryptosystem" with the idea of linguistic graph based map with partially invertible decomposition to introduce a new cryptosystem. The decomposition will be induced by pseudorandom walk on the linguistic graph and its special quotient (homomorphic image). We estimate the complexity of such general algorithm in case of special family of graphs with quotients, where both graphs form known families of Extremal Graph Theory. The map created by key holder (Alice) corresponds to pseudorandom sequence of ring elements. The postquantum version of the algorithm can be obtained simply by the usage of random strings instead of pseudorandom.

2010 MSC: 12Y05, 12Y99, 05C81, 05C85, 05C90, 94A60, 14G50.
Key words and phrases: Cryptosystem, Multivariate cryptography, Postquantum cryptography, Algebraic incidence structure, Pseudorandom sequences, Pseudorandom walk in graph.

1. On multivariate cryptography and special multivariate transformations

Multivariate cryptography (see [4]) is one of the directions of Postquantum Cryptography, which concerns with algorithms resistant to hypothetic attacks conducted by Quantum Computer. The encryption tools of Multivariate Cryptography are nonlinear multivariate transformations of affine space K^n, where K is a finite commutative ring. Nowadays this modern direction of research requires new examples of algorithms with theoretical arguments on their resistance to attacks conducted by ordinary computer (Turing machine) and new tasks for cryptanalists.

Essential part of known results on Multivariate Cryptography is devoted to studies of quadratic encryption maps. For instance, for many modifications of Imai - Matsumoto Cryptosystems the successful cryptanalisis was found.

The idea of the usage of nonbijective quadratic maps were proposed in "unbalanced oil and vinegar" system. Nowadays this idea is strongly supported by publication [3] devoted to security analisis of direct attacks on modified unbalanced oil and vinegar systems. It looks like such systems and rainbow signatures schemes may lead to promising Public Key Schemes of Multivariate Encryption (see [17], [18]).

In current paper we proposed different approach. The principle difference of our examples is that the degree of polynomial map is $\geqslant 3$. We will seriously modify approach of [26] for the creation of bijective map of K^n, where K is a general commutative ring, with invertible decomposition. The modifications allow us to produce *nonbijective* maps of K^n. suitable for the construction of multivariate cryptosystems. In difference with "unbalanced oil and vinegar" method the partition of variables is defined by homomorphism of algebraic graphs. We will analyze the options of direct attacks attacks in future publications.

Recall, that *Cremona group* $C(K^n)$ is a totality of invertible maps f of affine space K^n over a Commutative ring K into itself, such that the inverse map f^{-1} is also a polynomial one.

Let us refer to the sequence of general polynomial maps F_n on K^n, $n = 1, 2, \ldots$ as *a family of polynomial degree*, if the degree of each transformation is a parameter s of the size $O(n^t)$.

We say that a family F_n, $n = 1, 2, \ldots$ is *a family of linear degree* in the case $t = 1$. We refer to a family F_n as *a family of bounded degree* if $t = 0$. Assume that a transformation $F = F_n$ is written in the form:

$x_i \to f_i^n(x_1, x_2, \ldots, x_n), i = 1, 2, \ldots, n$, where each $f_i^n \in K[x_1, x_2, \ldots, x_n]$ is determined by the list of their monomial terms with respect to some chosen order.

We refer to the sequence $F_n \in C(K^n)$ as *a family of polynomial density* d if total quantity of all monomial expressions within all f_i^n is given as $O(n^d)$ for some independent constant d.

Proposition 1. *Let F_n, $n = 1, 2, \ldots$ be a family of polynomial degree s and of polynomial density d. Then the value of F_n in the point $x \in K^n$ can be computed by $O(n^{s+d})$ elementary steps.*

A family of elements $F_n \in C(K^n)$, $n > 1$ is called *stable* if each multiple iteration of F_n with itself has degree $\leqslant \deg F_n$.

We say that a family $F_n \in C(K^n)$ has an invertible decomposition of speed d if F_n can be written as a composition of elements $F_n^{(1)}, F_n^{(2)}, \ldots, F_n^{(k)}$, $k = k(n)$ and this decomposition will allow us to compute the value of $y = F_n(x)$ and the re-image of given y in time $k(n)O(n^d)$ (see [26] which partially reflects authors talk at the Central European Conference on Cryptology 2014).

The idea of usage of nonbijective polynomial transformations of K^n onto K^n is already known. For instance, well known multivariate construction of " oil and vinegar variables" were presented by J. Patarin [16]. This scheme and its modifications (unbalanced oil and vinegar system, in particular) were investigated in [5], [6], [2].

Below we introduce the simplest method of convertion of a computable bijective map with invertible decomposition into nonbijective family with partially computable decomposition.

Let us assume that K^n is presented as direct sum of affine subspaces W_1 and W_2. We say that the family of multivariate map $F_n : K^n \to K^n$ has partialy invertible decomposition $F_n = F_n^{(1)} F_n^{(2)} \ldots F_n^{(k)}$, $k = k(n)$ if the knowledge on this presentation allows to find the projection π of reimage v of $F_n(v) = u$ onto subspace W_1 in polynomial time.

Let us assume that nonlinear transformations F_n form a family of polynomial degree and density. Assume that it has partially invertible decomposition. Alice keeps this decomposition secret. She makes the map F_n, given in standard form, and the partition onto W_1 and W_2 (in chosen special basis) public. Public user Bob writes his message $\mathrm{p} = (p_1, p_2, \ldots, p_m)$, where $m = m(n) = \dim(W_1)$. He writes a pseudorandom string $(r_1, r_2, \ldots, r_t)$, $t = t(n) = \dim(W_2)$, He forms vector

$v = (p_1, p_2, \ldots, p_m, r_1, r_2, \ldots, r_t)$, $t + m = n$. Bob computes $\mathrm{c} = F_n(v)$ and sends it to Alice.

Alice uses the knowledge on decomposition (private key) to compute the plaintext $(p_1, p_2, \ldots, p_m)$.

First, we consider an affine deformation of a multivariate family $F_n : K^n \to K^n$ of polynomial density and polynomial degree: Let T_1 and T_2 be affine transformation of an K^n, i. e. polynomial maps of K^n into K^n of degree one. We refer to $G_n = T_1 F_n T_2$ as affine deformation of the family F_n. We say, that affine transformation is a regular one if the family of G_n is also a family of polynomial degree and polynomial density. In the simplest case, when degree of F_n is bounded by independent constant, an arbitrary deformation is a regular one. If T_1 is monomial map, i.e. it is a composition of diagonal and permutational linear transformation, then arbitrary affine deformation of such kind will be regular one.

Let F_n be a multivariate map of polynomial degree, polynomial density with invertible decomposition $F_n^{(1)} F_n^{(2)} \ldots F_n^{(k)}$, $k = k(n)$. Let W_1 be invariant subspace for F_n and nonbijective linear transformation T_1.

Assume, that $T_1|_{W_2}$ is nonbijective linear transformation, τ_2 is a bijective affine transformation of K^n. Let $e_1, e_2, \ldots, e_m$ be the basis of W_1 and $e_{m+1}, e_{m+2}, \ldots, e_n$ be the basis of W_2 is its completion to the basis of K^n. Then $T_1 F_n T_2$ has partially invertible decomposition $T_1 f_1 f_2 \ldots f_k T_2$. Really, if $G_n(v) = u$ is given, then the knowledge on the decomposition allows us to make the following steps.

1) Compute $T_2^{-1}(\mathrm{u}) = \mathrm{u}'$.

2) Compute the reimage z of u' for F_n for which $F_n(z) = u'$.

3) Let T^{-1} be the inverse of $T = T_1|_{W_1}$.

4) Take $z' = z|_{W_1}$ and compute $p = T^{-1}(z')$, which coincides with the projection $v|_W$.

We use the linguistic graphs and their special quotients to generate families of multivariate maps with partially invertible decomposition by the described above general scheme.

2. On linguistic graphs as tools of multivariate cryptography

The motivation of linguistic graph came from the observation that the restrictions of the incidence relation of geometry of simple group of Lie type on disjoint union of two maximal Schubert cell can be given via triangular system of algebraic equations (see [23], [24], [28]). Walks in

linguistic graphs have been used for the creation of stream ciphers since 1998. The first examples of such ciphers are given in [27],[29],[30]. For the estimation of the security level and feasibility studies for key exchange protocols the symbolic computations are very useful. After presentation of graph based bijective enciphering transformation as standard map H of kind

$$\begin{aligned} z_1 &\to h_1(z_1, z_2, \ldots, z_n), \\ z_2 &\to h_2(z_1, z_2, \ldots, z_n), \\ &\ldots, \\ z_n &\to h_n(z_1, z_2, \ldots, z_n) \end{aligned} \tag{1}$$

one can evaluate its degree (see [43], [44]). Other parameters such as order, number of fixed points, cycle structures can be investigated via numerical (non symbolic) computations.

The recent results on stream ciphers and key exchange protocols the reader can find in surveys [32, 34, 36, 41, 42] (see also [8, 10–12, 19–22, 33, 35, 38–40]).

We will use walks in incidence structures corresponding linguistic graphs and their flags as tools for generation of noninvertible transformation of flag variety. For this purpose we take a special homomorphic image Γ_1 (symplectic quotient) of linguistic graph Γ defined over commutative ring K. Flag space of Γ_2 can be identified with affine space K^n. Element π of symmetric group S_n acting naturally on K^n shifts symplectic quotient Γ_1 of Γ_2 to the symplectic quotient ${\Gamma_1}^\pi$ of "deformated" linguistic graph Γ_2^π. Pair Γ_1, Γ_2 defines the partition of flag space K^n into direct sum of $W_1 = K^{\tilde{n}}$ and $W_2 = K^{n-\tilde{n}}$.

The key owner Alice will create a public rule as a composition of the most preferable singular linear map T_1 with invariant space W_1 such that $T_1|_{W_1}$ is invertible, some permutation $\pi \in S_n$, nonlinear map N corresponding to the chosen walk on the flags of incidence structure Γ_2^π, and the "shutter" T_2, which is invertible affine transformation of K^n. Alice will use tools of Computer Algebra to generate the composition in the standard form (1).

A public user Bob will use "window" W_1 to write his plaintext m and W_2 to put pseudorandom string v of elements from K. He gets a randomised plaintext $\tilde{\mathrm{m}}$ as concatenation of m and v. He computes ciphertext $\mathrm{c} = H(\tilde{\mathrm{m}})$ and sends it to Alice.

The private key of Alice consists of symplectic pair I, I' of linguistic graphs, linear maps T_1 and π, chosen pseudorandom walk in Γ_2^π and "the shutter" T_2. It allows her to restore the plaintext m, but not a random string v.

Notice, that transformation H is a composition of linear map $T_1^{'} = T_1\pi$, nonlinear map N and affine shutter T_2. So it has similarity with Imai Matsumoto encryption map (see [9]). If $K = Q^l$ Alice can "hide" ring K and write public rule transformation Q^{nl} with the modified trick of Imai-Matsumoto algorithm.

Section 2 is devoted to the concept of the pair consisting of a linguistic graph and its symplectic quotient. In section 3 we consider a general scheme of generation of pseudo public multivariate map on variety of vertices (or flags) of general linguistic graph. We use term *pseudo public* because the complexity and level of security depends on the choice of the graph. The idea of this method of *symbolic walks on algebraic graph encryption* (shortly SWAGE) is presented in [31] together with an example for the case of known linguistic graphs of large girth $D(k, q)$ and their generalisation for the case of general commutative ring (see also [30] for the $D(k, q)$ graphs case). The final form of SWAGE on numerical level is presented in [40] together with the generalised method for special incidence structures of arbitrary rank. In section 3 the reader can find SWAGE descryption given both on symbolic and numerical methods. So, the method of generation of nonlinear map as mentioned above map N and computation of N^{-1} is given. Detailed descryption of general algorithm for the case of $K = Q^l$ is given. The section 3 is devoted to the examples of cryptosystems. We use the known graphs of large girth $D(k, q)$ ([13], [14], [15]) and extremal graphs $A(k, q)$(see [38], [20], [41], [42]) and there generalisations $D(k, K)$ and $A(k, K)$, where K is commutative ring. Incidence structure Γ_2 will correspond to representative of graphs from family $D(k, K)$, $n = 2, 3, \ldots$ and linguistic quotient Γ_1 corresponds to some graph from the family $A(k', K)$. The degrees of obtained public keys will be evaluated by some constants. The last section contains some remarks on the main results of the previous sections.

3. Linguistic graphs and their symplectic quotients

The missing definitions of graph-theoretical concepts which appear in this paper can be found in [1]. All graphs we consider are *simple* , 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. Then $|V(G)|$ is called the *order* of G, and $|E(G)|$ is called the *size* of G. 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 assume that $V(G)$ is a finite or an infinite set. The majority of examples will be *locally finite graphs* G, i.e. each vertex v has finite number of neighbours ($x \in V(G)$, such that $x\, G\, v$). We refer to $|\{x \in V(G) | x\, G\, v\}|$ as *degree of the vertex* v.

The sequence of distinct vertices $v_0, v_1, \ldots, v_t$, such that $v_i\, G\, v_{i+1}$ for $i = 1, \ldots, t-1$ is the *path* in the graph. A path in G is called *simple* if all its vertices are distinct. The graph is *connected* if each two of its vertices are joined by some path. The length of a path is a number of its edges. The *distance* between two vertices u and v of the graph, denoted by $\mathrm{dist}(u, v)$, is the length of the shortest path between them. The *diameter* of the graph, denoted by $\mathrm{diam}(G)$, is the maximal distance between two vertices u and v of the graph. Let C_m denote the cycle of length m, i.e. the sequence of distinct vertices $v_0, \ldots, v_m$ such that $v_i G v_{i+1}$, $i = 1, \ldots, m-1$ and $v_m\, G\, v_1$. The *girth* of a graph G, denoted by $g = g(G)$, is the length of the shortest cycle in G.

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 (*bipartite graph*).

We refer to a triple consisting of set V, its partition $V = P \cup L$ and symmetric and antireflexive binary relation I (incidence) on the set V, such that xIy implies x $\in P$, y $\in L$ or x $\in L$ and y $\in P$ as *incidence structure*. The pair {x, y}, x $\in P$, 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 *linguistic incidence structure* I_m if point

$$(\mathrm{x}) = (x_1, x_2, \ldots, x_s, , x_{s+1}, x_{s+2}, \ldots, x_{s+m})$$

is incident to line

$$[\mathrm{y}] = [y_1, y_2, \ldots, y_r, y_{r+1}, y_{r+2} \ldots, y_{r+m}]$$

if and only if the following relations hold

$$\begin{aligned}
\xi_1 x_{s+1} + \zeta_1 y_{r+1} &= f_1(x_1, x_2, \dots, x_s, y_1, y_2, \dots, y_r) \\
\xi_2 x_{s+2} + \zeta_2 y_{r+2} &= f_2(x_1, x_2, \dots, x_s, x_{s+1}, y_1, y_2, \dots, y_r, y_{r+1}) \\
&\dots \\
\xi_m x_{s+m} + \zeta_m y_{r+m} &= f_m(x_1, x_2, \dots, x_{s+m-1}, y_1, y_2, \dots, y_{r+m-1})
\end{aligned}$$

where ξ_j and ζ_j, $j = 1, 2, \dots, m$ are not zero divisors, and f_j are multivariate polynomials with coefficients from K. Brackets and parenthesis allow us to distinguish poins from lines (see [7]).

The colour $\rho(\mathrm{x}) = \rho((\mathrm{x}))$ ($\rho(\mathrm{y}) = \rho([\mathrm{y}])$) of point (x) (line [y]) is defined as projection of an element (x) ([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 unique neighbour of a chosen colour. We also consider a linguistic incidence structures defined by infinite number of equations.

Let $M = \{m_1, m_2, \dots, m_d\}$ be a subset of $\{1, 2, \dots m\}$ (set of indexes for equations), $d \leqslant m$ with the standard order. Assume that equations indexed by elements from M of following kind

$$\begin{aligned}
\xi_{m_1} x_{m_1} + \zeta_{m_1} y_{m_1} &= f_{m_1}(x_1, x_2, \dots, x_s, y_1, y_2, \dots, y_r) \\
\xi_{m_2} x_{m_2} + \zeta_{m_2} y_{m_2} &= f_{m_2}(x_1, x_2, \dots, x_s, x_{m_1} y_1, y_2, \dots, y_r, y_{m_1}) \\
&\dots \\
\xi_{m_d} x_{m_d} + \zeta_{m_d} y_{m_d} &= f_{m_d}(x_1, \dots, x_s, x_{m_1}, \dots, x_{m_{d-1}}, y_1, \dots, y_r, y_{m_1}, \dots, y_{m_{d-1}})
\end{aligned}$$

define another linguistic incidence structure I_M. Then the natural projections

$$\begin{aligned}
\pi_1 &: (\mathrm{x}) \to (x_1, x_2, \dots, x_s, x_{m_1}, x_{m_2}, \dots, x_{m_d}), \\
\pi_2 &: [\mathrm{y}] \to [y_1, y_2, \dots, y_r, y_{m_1}, y_{m_2}, \dots, y_{m_d}]
\end{aligned}$$

of free modules define the natural homomorphism ϕ of incidence structure I_m onto I_M. We will use the same symbol ρ for the colouring of linguistic graph I_M. It is clear, that $\rho(\mathrm{x}) = \rho(\phi(\mathrm{x}))$ and $\rho(\mathrm{y}) = \rho(\phi(\mathrm{y}))$. So, ϕ is a colour preserving homomorphism of incidence structure(bipartite graph) onto the other one. We refer to ϕ as *symplectic homomorphism* and graph $I_M = \phi(I_m)$ as *symplectic quotient of linguistic graph* I_m. In the case of linguistic graphs defined by infinite number of equations we may consider cases of symplectic quotients defined by the infinite subset M.

The triangular structure of the system of equations insures existence of many symplectic quotients. Let us consider an example of symplectic quotient which is not connected with a general triangular structure of a linguistic incidence system.

Let I be a graph of a linguistic incidence structure with a set of a vertex set $V = P \cup L$ over a commutative ring K. We introduce the adjacency relation ${}^{\mathcal{F}}I$ on the set of flags $\mathcal{F}(V)$ of incidence structure I as a *flag relation* (or *flag linguistic graph*): the intersection of two distinct flags is a non empty set (singleton). All vertices forming two flags $F_1 = \{(x_1), [y_1]\}$ and $F_2 = \{(x_2), [y_2]\}$ could be located at the same connected component of I, or all of them are from distinct connected components of I. Assume that system of equations

$$\begin{aligned} G_1(\mathrm{x}) &= g_1, \\ G_2(\mathrm{x}) &= g_2, \\ &\dots, \\ G_t(\mathrm{x}) &= g_t, \end{aligned}$$

where $g_i \in K$ are some constants, defines the *connectivity invariants* specified for points $(\mathrm{x}) \in P$ in linguistic incidence structure I. For elements $(\mathrm{x}_1), (\mathrm{x}_2) \in P$ from the same connectivity component in grpah I the following relations hold

$$G_i(\mathrm{x}_1) = G_i(\mathrm{x}_2), \quad i = 1, 2, \dots, t.$$

The existence of i such that $G_i(\mathrm{x}_1) \neq G_i(\mathrm{x}_2)$ implies that (x_1) and (x_2) are points from different connected components of graph I.

4. Symbolic keys and pseudorandom walks on flag space

Let $V_{s,r,m} = P_{s,m} \cup L_{r,m}$, $I_m = I_m(K)$, $m = 2, 3, \dots$ be a family of linguistic incidence structures with the point set $P_{s,m} = K^{s+m}$ and the line set $L_{s,m} = K^{r+m}$, where parameters s and r are constants and K is a fixed commutative ring. The sets of colours for points and lines are K^s and K^r, respectively. We assume that subset $M = \{i_1, i_2, \dots, i_d\}$, $d = d(m) \leqslant m$ defines the symplectic quotient I_M for each linguistic structure $I_m = I_m(K)$. Let G_1, G_2, $\dots$, G_t be connectivity invariants of incidence structures I_m.

Let ${}^{\mathcal{F}}I_m$ be the flag relation and $\mathcal{F}(V_{s,r,m}) = \mathcal{F}(V_m(K))$ be the variety of flags for incidence structure I_m. The information on the flag $\{(x), [y]\}$ can be given by the pair $(x) \in K^{s+m}$, $\rho(y) \in K^r$ or, alternatively, by the pair $[y] \in K^{r+m}$ and $\rho(x) \in K^s$. So, $\mathcal{F}(V_{s,r,m})$ is isomorphic to K^{m+r+s}.

Let $N_{P,a}$, $a \in K^s$ be the operator of a change of the point of the flag $F = \{(x), [y]\}$ defined by the rule

$$N_{P,a}(\{(\mathrm{x}), [\mathrm{y}]\}) = \{(\mathrm{x}'), [\mathrm{y}]\},$$

where $(\mathrm{x}')I_m[\mathrm{y}]$ and $\rho(\mathrm{x}') = a$. Similarly, $N_{L,a}$, $a \in K^s$ is the operator of a change of the line of the flag $F = \{(x), [y]\}$ specified by the rule

$$N_{L,b}(\{(\mathrm{x}), [\mathrm{y}]\}) = \{(\mathrm{x}), [\mathrm{y}']\},$$

where $[\mathrm{y}']I_m(\mathrm{x})$ and $\rho(\mathrm{y}') = b$. It is clear that application of the composition of N_{P,a_1}, N_{L,b_1}, N_{P,a_2}, N_{L,b_2}, $\ldots$, N_{P,a_k}, N_{L,b_k} to the flag F corresponds to the walk in our linguistic graph with the starting point (p) or the walk in the graph ${}^{\mathcal{F}}I_m$ with starting vertex $\{(x), [y]\}$.

Let $F = \{(\mathrm{x}), [\mathrm{y}]\}$ be a general flag of our linguistic structure I_m, i.e.

$$\begin{aligned}(\mathrm{x}) &= (x_1, x_2, \ldots, x_s, x_{s+1}, x_{s+2}, \ldots, x_{s+m}),\\ [\mathrm{y}] &= [y_1, y_2, \ldots, y_r, y_{r+1}, y_{r+2} \ldots, y_{r+m}]\end{aligned}$$

are incident. It is convenient for us to shift indeces and write points and lines as

$$\begin{aligned}(\mathrm{x}) &= (x_1, x_2, \ldots, x_s, x_{s+r+1}, x_{s+r+2}, \ldots, x_{s+r+m}),\\ [\mathrm{y}] &= [y_{s+1}, y_{s+2}, \ldots, y_{r+s}, y_{r+s+1}, \ldots, y_{s+r+m}].\end{aligned}$$

We assume that our incidence structure has the symplectic quotient I_M corresponding to subset $M = \{j_{s+r+i_1}, j_{s+r+i_2}, \ldots, j_{s+r+i_d}\}$. Let π be a permutation on $\{1, 2, \ldots, s, s+1, s+2, \ldots, s+r, s+r+1, s+r+2, \ldots, s+r+m\}$. Then we can consider deformated incidence structures I_m^{π} with points

$$\pi(\mathrm{x}) = (x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(s)}, x_{\pi(s+r+1)}, x_{\pi(s+r+2)}, \ldots, x_{\pi(s+r+m)})$$

and lines of kind

$$\pi(\mathrm{y}) = [y_{\pi(s+1)}, y_{\pi(s+2)}, \ldots, y_{\pi(s+r)}, y_{\pi(s+r+1)}, y_{\pi(s+r+2)}, \ldots, y_{\pi(s+r+m)}]$$

with the incidence conditions

$$\begin{aligned}
\xi_1 x_{\pi(s+r+1)} + \zeta_1 y_{\pi(s+r+1)} &= f_1(x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(s)}, y_{\pi(s+1)}, \ldots, y_{\pi(s+r)}) \\
\xi_2 x_{\pi(s+r+2)} + \zeta_2 y_{\pi(s+r+2)} &= f_2(x_{\pi(1)}, \ldots, x_{\pi(s)}, x_{\pi(s+r+1)}, y_{\pi(s+1)}, \ldots, \\
&\quad y_{\pi(s+r)}, y_{\pi(s+r+1)}) \\
&\ldots \\
\xi_m x_{\pi(s+r+m)} + \zeta_m y_{\pi(s+r+m)} &= f_m(x_{\pi(1)}, \ldots, x_{\pi(s)}, x_{\pi(s+r+1)}, \ldots x_{\pi(s+r+m-1)}, \\
&\quad y_{\pi(s+1)}, \ldots, y_{\pi(s+r)}, y_{\pi(s+r+1)}, \ldots, y_{\pi(s+r+m-1)})
\end{aligned}$$

Obviously linguistic incidence structure I_m is isomorphic to I_m^π and symplectic quotient I_M of graph I_m corresponding to subset

$$M = \{r+s+i_1, r+s+i_2, \ldots, r+s+i_d\}$$

is isomorphic to symplectic quotient I_M^π of graph I_m^π related to the subset

$$\pi(M) = \{\pi(r+s+i_1), \pi(r+s+i_2), \ldots, \pi(r+s+i_d)\}.$$

The above mentioned action of symmetric group on linguistic structure allows us without a loss of generality assume that symplectic quotient I_M of I_m corresponds to subset $M = \{r+s+1, r+s+2, \ldots, r+s+d\}$ with natural order of elements. So, the canonical homomorphism of I_m onto I_M is given by

$$\begin{aligned}
(x_1, \ldots, x_s, x_{r+s}, x_{r+s+1}, \ldots, x_{r+s+m}) &\to (x_1, \ldots, x_s, x_{r+s}, x_{r+s+1}, \ldots, x_{r+s+d}) \\
(y_{s+1}, \ldots, y_{r+s}, y_{r+s+1}, \ldots, y_{r+s+m}) &\to (y_{s+1}, \ldots, y_{r+s}, y_{r+s+1}, \ldots, y_{r+s+d})
\end{aligned}$$

We assume that x_1, x_2, …, x_s, y_{s+1}, y_{s+2}, …, y_{s+r}, x_{s+r+1}, x_{s+r+2}, …, x_{s+r+m} is the list of independent variables which gives us the entire information on the flag F of incidence structure I_m. We assume that connectivity invariants $G_1, G_2, \ldots, G_t$ are written in terms of coordinates of the point (x). We refer to a tuple

$$\mathrm{Tr}(F) = \langle x_1, x_2, \ldots, x_s, y_{s+1}, y_{s+2}, \ldots, y_{s+r}, G_1(\mathrm{x}), G_2(\mathrm{x}), \ldots, G_t(\mathrm{x}) \rangle$$

as a *trace of a flag* $F = \{(\mathrm{x}), [\mathrm{y}]\}$ i.e.

$$\mathrm{Tr}(F) = \langle \rho(\mathrm{x}), \rho(\mathrm{y}), G_1(\mathrm{x}), G_2(\mathrm{x}), \ldots, G_t(\mathrm{x}) \rangle .$$

Let Q be a subring of K, such that K is isomorphic to free module Q^l. We introduce parameter n by equality $n = (r+s+t)l$ (the dimension of flag variety over commutative ring Q). Assume that $Q[z_1, z_2, \ldots, z_n]^l$ is a to-

tality of all polynomials over Q maps from Q^n into K. We choose the fixed basis in $K = Q^l$ and identify a map P from $Q[z_1, z_2, \ldots, z_n]^l$ with the set of polynomials $p_1(z_1, z_2, \ldots, z_n)$, $p_2(z_1, z_2, \ldots, z_n)$, $\ldots$, $p_l(z_1, z_2, \ldots, z_n)$, where p_i are multivariate polynomials from $Q[z_1, z_2, \ldots, z_n]$.

Let $D_1, D_2, \ldots, D_h, D_{h+1}$ and $E_1, E_2, \ldots, E_h$ be two lists of elements where $D_i, E_j \in Q[z_1, z_2, \ldots, z_n]^l$, $i = 1, 2, \ldots, h+1$, $j = 1, 2, \ldots, h$. We refer to concatenation of both lists (writing second list after the first one) as a *symbolic key*.

We take the flag $F = \{(\mathrm{x}), [\mathrm{y}]\}$ specified by parameters of kind x_1, x_2, $\ldots$, x_s, y_{s+1}, y_{s+2}, $\ldots$, y_{s+r}, x_{s+r+1}, x_{s+r+2}, $\ldots$, x_{s+r+m} with spectrum

$$\mathrm{Tr}(F) = \langle x_1, x_2, \ldots, x_s, y_{s+1}, y_{s+2}, \ldots, y_{s+r}, G_1(\mathrm{x}), G_2(\mathrm{x}), \ldots, G_t(\mathrm{x}) \rangle .$$

Each coordinate of the flag F is a tuple of kind $(\alpha_1, \alpha_2, \ldots \alpha_l) \in Q^l$. We concatenate all these tuples with the preservation of order and form a string of parameters $\beta_1, \beta_2, \ldots, \beta_n$ from Q. After that we compute specializations of coordinates

$$d_i = D_i(\beta_1, \beta_2, \ldots, \beta_n),$$

where $i = 1, 2, \ldots, h, h+1$ and

$$e_j = E_j(\beta_1, \beta_2, \ldots, \beta_n),$$

where $j = 1, 2, \ldots, h$ of our symbolic key. Chosen base of $Q^l = K$ allows us to treat coordinates of the string $d_1, d_2, \ldots, d_h, d_{h+1}$ as elements of K^s and coordinates of $e_1, e_2, \ldots, e_h$ as string from K^r. String $(d_1, d_2, \ldots, d_h, d_{h+1}, e_1, e_2, \ldots, e_h)$ is our *numerical key*.

Finally, we compute decomposition N of operators N_{P,d_1}, F_{L,e_1}, N_{P,d_2}, N_{L,e_2}, $\ldots$, N_{P,d_h}, N_{L,e_h}, $N_{P,e_{d+1}}$.

The application of N to the flag F corresponds to the walk in graph ${}^{\mathcal{F}}I_m$ with the starting point F and the final point $N(F)$.

Notice, that the colours of the point and the line forming $F' = N(F) = \{(\mathrm{x}'), [\mathrm{y}']\}$ are $d_{h+1} \in K^s$ and $e_h \in K^r$, respectively. Under certain conditions we may restore the trace of the flag F from given F'. We have

$$G_i(\mathrm{x}) = G_i(\mathrm{x}')$$

because both flags are from the same connected component. Additionally,

$$(x'_1, x'_2, \ldots, x'_s) = D_{h+1}(x_1, \ldots, x_s, y_{s+1}, \ldots, y_{s+r}, G_1(\mathrm{x}'), \ldots, G_t(\mathrm{x}')),$$

$$(y'_{s+1}, y'_{s+2}, \ldots, y'_{s+r}) = E_h(x_1, \ldots, x_s, y_{s+1}, \ldots, y_{s+r}, G_1(\mathrm{x}'), \ldots, G_t(\mathrm{x}')).$$

We may choose function D_{h+1} and E_h such that the above written system of equations has a unique solution independently from values $G_i(\mathrm{x}')$, $i = 1, 2, \ldots, t$.

Obviously the first choice here is a linear in variables x_1, x_2, …, x_s, y_{s+1}, y_{s+2}, …, y_{s+r} system of equations. Then we can reconstruct our walk in reverse order corresponding to the composition of $N_{P,e_{h-1}}$, $N_{L,d_{h-1}}$, $N_{P,e_{h-2}}$, …, N_{L,e_1}, N_{P,d_1}.

4.1. Multivariate transformations based on symbolic keys

The above mentioned map defined by symbolic key has multivariate nature. The plainspace is the totality of tuples

$$(x_1, x_2, \ldots, x_s, y_1, y_2, \ldots, y_r, x_{s+r+1}, x_{s+r+2}, \ldots, x_{s+r+m}).$$

For each function $D_i(z_1,z_2,\ldots,z_s,z_{s+1},z_{s+2},\ldots,z_{s+r},z_{s+r+1},\ldots,z_{s+r+t})$ we consider the specialization of variables $z_1 = x_1$, $z_2 = x_2$, …, $z_s = x_s$, $z_{s+1} = y_1$, $z_{s+2} = y_2$, …, $z_{s+r} = y_r$, $z_{s+r+1} = G_1(\mathrm{x})$, $z_{s+r+2} = G_2(\mathrm{x})$, …, $z_{s+r+t} = G_t(\mathrm{x})$. In such way we construct function D'_i depending on the general tuple $(x_1, x_2, \ldots, x_s, y_1, y_2, \ldots, y_r, x_{r+s+1}, x_{s+r+2}, \ldots, x_{s+r+m})$ of the plainspace. Similarly we apply the same specialisation to each E_i and get transformation E'_i. Transformations N_{P,D'_i} and N_{L,E'_j} are multivariate bijections on K^{r+s+m}. The formal composition of N_{P,D'_1}, N_{L,E'_1}, N_{P,D'_2}, N_{L,E'_2}, …, N_{P,D'_h}, N_{L,E'_h}, $N_{P,D'_{h+1}}$ is a symbolic presentation of the map N.

5. The general algorithms of the two windows multivariate cryptosystem depending on random variables

Suppose that two users Alice and Bob want to communicate securely over an open channel in which all messages are potentially overheard. Suppose that Alice and Bob for secure communication the two windows multivariate cryprosystem depending of random parameters; so, Alice generates a couple of keys (public and private ones). We show that lack of knowledge of the private key prevents Bob or possible intruders to decrypt intercepted messages.

5.1. The key generation algorithm

Let us assume that Alice has a flag linguistic graph ${}^{\mathcal{F}}I_m$ and flag symplectic quotient ${}^{\mathcal{F}}I_M$ corresponding to $M = \{s+r+1, s+r+2, \ldots, s+r+d\}$ with natural order of elements.. So, the windows space $W = W_1 \oplus W_2$ of flags can be identified with tuples

$$F = (x_1, x_2, \ldots, x_s, y_{s+1}, y_{s+2}, \ldots, y_{s+r}, x_{s+r+1}, x_{s+r+2}, \ldots, x_{s+r+d}, x_{s+r+d+1} x_{s+r+d+2}, \ldots, x_{s+r+m}).$$

It is convenient for Alice to partite K^{r+s+m} into direct sum $W_1 = K^{s+r+d}$ and $W_2 = K^{m-d}$. She fixes the basis and identifies "*two windows spaces*" W_1 (*window for plaintext*) and W_2 (*window for random extention of plaintext*) with totalities of tuples of kind

$$(x_1, x_2, \ldots, x_s, y_{s+1}, y_{s+2}, \ldots, y_{s+r}, x_{s+r+1}, x_{s+r+2}, \ldots, x_{s+r+d}) \in W_1,$$
$$(x_{s+r+d+1}, x_{s+r+d+2}, \ldots, x_{s+r+m}) \in W_2.$$

She will choose the permutation π to deformate the flag linguistic graph ${}^{\mathcal{F}}I_m$ and its flag symplectic quotient ${}^{\mathcal{F}}I_M$. Alice will use the fact that $K = Q^l$. So, she can work with fixed base of $K = Q^l$ and identify W, W_1 and W_2 with free modules over Q of dimensions $(s + r + m)l$, $(s + r + d)l$ and $(m - d)l$, respectively.

We can now discribe an algorithm of key generation for our two windows multivariate cryptosystem depending on random variables.

Key generation. Alice should do the following steps:

1) Choose the comutative ring Q and their extention $K = Q^l$.
2) Define space $W = Q^k$, where $k = (s + r + m)l$ and fixe the base and consider the decomposition $W = W_1 \otimes W_2$, where $W_1 = Q^{k_1}$, $W_2 = Q^{k_2}$, $k_1 = (s + r + d)l$ and $k_2 = (m - d)l$.
3) Choose the most preferable singular linear transformation $T_1 : W \to W$ such that $T_1|_{W_1} = T$ is not singular.
4) Take the tuple $z = (z_1, z_2, \ldots, z_k) \in W$ an compute $w = T_1(z)$.
5) Treat tuple $w \in W$ as a flag F_1 in linguistic graph ${}^{\mathcal{F}}I_m$ of kind
$$F_1 = (x_1, \ldots, x_s, y_{s+1}, \ldots, y_{s+r}, x_{s+r+1}, x_{s+r+2}, \ldots, x_{s+r+m})$$
6) Take permutation π defined on set of indexes $\{1, 2, \ldots, s + r + m\}$ to deformate linguistic graph ${}^{\mathcal{F}}I_m$.

7) Compute flag $F_2 \in^{\mathcal{F}} I_m^{\pi}$ with the trace x'_1, x'_2, ..., x'_s, y'_{s+1}, ..., y'_{s+r}, $G_1(F_2)$, $G_2(F_2)$, ..., $G_t(F_2)$ i.e.

$$F_2 = \pi(F_1) = (x'_1, x'_2 \ldots, x'_s, y'_{s+1}, \ldots, y'_{s+r}, x'_{s+r+1}, x'_{s+r+2}, \ldots, x'_{s+r+m})$$

8) Choose the symbolic key corresponding to the symbolic way in linguistic graph ${}^{\mathcal{F}}I_m^{\pi}$ i.e. list of polynomial functions $D_i(v_1,v_2,\ldots,v_{r+s+t})$, $i = 1, 2, \ldots, h+1$, $E_j(v_1, v_2, \ldots, v_{r+s+t})$, $j = 1, 2, \ldots, h$.

9) Compute specializations
$D'_i(F_2) = D_i(x'_1, \ldots, x'_s, y'_{s+1}, \ldots, y'_{s+r}, G_1(F_2), \ldots, G_t(F_2))$,
$i = 1, 2, \ldots, h+1$,
$E'_j(F_2) = E_j(x'_1, \ldots, x'_s, y'_{s+1}, \ldots, y'_{s+r}, G_1(F_2), \ldots, G_t(F_2))$,
$j = 1, 2, \ldots, h$.
corresponding to the substitution $v_i = x'_i$, $i+1, 2, \ldots, s$, $v_{s+j} = y'_{s+j}$, $j = 1, 2, \ldots, r$, $v_{s+r+e} = G_i(F_2)$, $e = 1, 2, \ldots, t$.

10) Determine multivariate transformation N corresponding to chosen symbolic key, i.e.

$$N = N_{P,D'_1} N_{L,E'_1} \ldots N_{P,D'_h} N_{L,E'_h} N_{P,D'_{h+1}}.$$

11) Compute flag $F_3 = N(F_2)$ of the graph ${}^{\mathcal{F}}I_m^{\pi}$.

12) Treat the flag F_3 as a tuple $u \in Q^k$.

13) Choose a invartible affine transformation $T_2 : Q^k \to Q^k$ and compute $c = T_2(u)$.

14) Using symbolic computation determine a multivariate transformations $H : W \to W$ as a composition of T, N and T_2. It is clear that the transformation $H : W \to W$ is polynomial over Q of kind

$$\begin{aligned} &z_1 \to h_1(z_1, z_2, \ldots, z_k), \\ &z_2 \to h_2(z_1, z_2, \ldots, z_k), \\ &\quad \ldots, \\ &z_k \to h_k(z_1, z_2, \ldots, z_k), \quad \text{where } h_i \in Q[z_1, z_2, \ldots, z_k]. \end{aligned}$$

It implies that the *public key* of presented cryptosystem includes the following:

(1) The commutative ring Q including its additive and multiplicative structure.

(2) The subdivision of the text space $W = Q^k$ into the direct sum of $W_1 = Q^{k_1}$ as *window plaintext* and $W_2 = Q^{k_2}$ as *window random extention of plaintext.*

(3) The transformation $H : W \to W$ defined by the list of multivariate polynomials h_1,h_2,..., $h_k \in Q[z_1, z_2, \ldots, z_k]$.

The *private key* includes:

(1) Information about the structures of ring K isomorphic to free module Q^l and the fact that $k = (s + r + m)l$, $k_1 = (s + r + d)l$, $k_2 = (m - d)l$.
(2) Singular linear transformation $T_1 : W \to W$ such that $T_1|_{W_1} = T$ is not singular.
(3) Flag linguistic graph ${}^{\mathcal{F}}I_m$ and its symplectic quotient ${}^{\mathcal{F}}I_M$ corresponding to subset $M = \{j_{s+r+i_1}, j_{s+r+i_2}, \ldots, j_{s+r+i_d}\}$.
(4) Permutation π defined on $\{1, 2, \ldots, s + r + m\}$
(5) Deformed linguistic incidence structure ${}^{\mathcal{F}}I^{\pi}_m$ of ${}^{\mathcal{F}}I_m$ and deformed symplectic quotient ${}^{\mathcal{F}}I^{\pi}_M$ of graph ${}^{\mathcal{F}}I_M$, where

$$M = \{r + s + i_1, r + s + i_2, \ldots, r + s + i_d\}$$

and

$$\pi(M) = \{\pi(r + s + i_1), \pi(r + s + i_2), \ldots, \pi(r + s + i_d)\}.$$

(6) Symbolic key as list of transformations D_1, D_2, D_{h+1}, E_1, E_2, ..., E_h and its specializations D'_1, D'_2, D'_{h+1}, E'_1, E'_2, ..., E'_h determines multivariate transformation N corresponding to way in graph ${}^{\mathcal{F}}I^{\pi}_m$ i.e.

$$N = N_{P,D'_1} N_{L,E'_1} \ldots N_{P,D'_h} N_{L,E'_h} N_{P,D'_{h+1}}.$$

(7) An invariable affine transformation $T_2 : W \to W$.

5.2. Encryption and decryption algorithm

Suppose that Bob encrypts a message (plaintext) m for Alice, which Alice decrypt.

Encryption. Bob should do the following steps:

1) Obtain Alice's authentical public key (Q, k, k_1, k_2, H).
2) Represent the message m as a tuple from the window plaintext $W_1 = Q^{k_1}$.

3) Choose a random extention v of plaintext m form $W_2 = Q^{k_2}$ and make concatenation m and v i.e. $\tilde{\mathrm{m}} = \mathrm{m}||\mathrm{v}$.
4) Compute $H(\tilde{\mathrm{m}}) = \mathrm{c}$.
5) Send the ciphertext c to Alice.

Decryption. To restore the plaintext m from the ciphertext c, Alice should do the following steps:

1) Use the invertible affine transformation T_2 to compute $T_2^{-1}(\mathrm{c}) = u$.
2) Write u as a flag F_3 from graph ${}^{\mathcal{F}}I_m^{\pi}$.
3) Use symbolic key and trace of flag F_3 to determine a numerical key as list of elements $d_1, d_2, \ldots, d_h, d_{h+1}, e_1, e_2, \ldots, e_h$ from K.
4) Compute $N^{-1}(F_3) = F_2$ via computation of reverse walk in ${}^{\mathcal{F}}I_m^{\pi}$ determined by numerical key.
5) Compute $F_1 = \pi^{-1}(F_2)$ as flag from ${}^{\mathcal{F}}I_m$.
6) Get projections of flag F_1 onto flag F from symplectic quotient ${}^{\mathcal{F}}I_M$ of flag linguistic graph ${}^{\mathcal{F}}I_m$.
7) Write flag F as a tuple z from $W_1 = Q^{k_1}$.
8) Compute plaintext $\mathrm{m} = T^{-1}(z)$.

We will show the existence of families of linguistic graphs, for which we can estimate polynomial complexity of the algorithms for both correspondents and present certain arguments on security.

6. On the family of graphs of large girth with special symplectic quotients

Let P_D and L_D be two copies of Cartesian power $\mathbb{K}^{\mathbb{N}}$, where $\mathbb{K}$ is the commutative ring and $\mathbb{N}$ is the set of positive integer numbers. Elements of P_D will be called *points* and those of L_D *lines*.

To distinguish points from lines we use parentheses and brackets. If $x \in V$, then $(x) \in P_D$ and $[x] \in L_D$. It will be also advantageous to adopt the notation for co-ordinates of points and lines introduced in [30] for the case of general commutative ring $\mathbb{K}$:

$$(p) = (p_{0,1}, p_{1,1}, p_{1,2}, p_{2,1}, p_{2,2}, p'_{2,2}, p_{2,3}, \ldots, p_{i,i}, p'_{i,i}, p_{i,i+1}, p_{i+1,i}, \ldots),$$
$$[l] = [l_{1,0}, l_{1,1}, l_{1,2}, l_{2,1}, l_{2,2}, l'_{2,2}, l_{2,3}, \ldots, l_{i,i}, l'_{i,i}, l_{i,i+1}, l_{i+1,i}, \ldots].$$

The elements of P and L can be thought as infinite ordered tuples of elements from $\mathbb{K}$, such that only finite number of components are different from zero.

Now we define a linguistic incidence structure (P_D, L_D, I_D) defined by infinite system of equations as follows. We say that the point (p) is incident with the line $[l]$, and we write $(p)I[l]$, if the following relations between their co-ordinates hold:

$$\begin{aligned} l_{i,i} - p_{i,i} &= l_{1,0}p_{i-1,i}, \\ l'_{i,i} - p'_{i,i} &= l_{i,i-1}p_{0,1}, \\ l_{i,i+1} - p_{i,i+1} &= l_{i,i}p_{0,1}, \\ l_{i+1,i} - p_{i+1,i} &= l_{1,0}p'_{i,i} \end{aligned} \tag{2}$$

(These four relations are defined for $i \geqslant 1$, $p'_{1,1} = p_{1,1}$, $l'_{1,1} = l_{1,1}$). The incidence structure (P_D, L_D, I_D) we denote as $D(\mathbb{K})$. Now we speak of the *incidence graph* of (P_D, L_D, I_D), which has the vertex set $P_D \cup L_D$ and edge set consisting of all pairs $\{(p), [l]\}$ for which $(p)I[l]$.

For each positive integer $k \geqslant 2$ we obtain a symplectic quotient $(P_{D,k}, L_{D,k}, I_{D,k})$ as follows. First, $P_{D,k}$ and $L_{D,k}$ are obtained from P_D and L_D, respectively, by simply projecting each vector into its k initial coordinates. The incidence $I_{D,k}$ is then defined by imposing the first $k-1$ incidence relations and ignoring all others. The incidence graph corresponding to the structure $(P_{D,k}, L_{D,k}, I_{D,k})$ is denoted by $D(k, \mathbb{K})$.

To facilitate notation in the future results on "connectivity invariants", it will be convenient for us to define $p_{-1,0} = l_{0,-1} = p_{1,0} = l_{0,1} = 0$, $p_{0,0} = l_{0,0} = -1$, $p'_{0,0} = l'_{0,0} = -1$, $p'_{1,1} = p_{1,1}, l'_{1,1} = l_{1,1}$) and to assume that our equations are defined for $i \geqslant 0$.

Notice, that for $i = 0$, the written above four conditions are satisfied by every point and line, and for $i = 1$ the first two equations coincide and give $l_{1,1} - p_{1,1} = l_{1,0}p_{0,1}$.

Let $k \geqslant 6$, $t = [(k+2)/4]$, and let $u = (u_\alpha, u_{11}, \cdots, u_{tt}, u'_{tt}, u_{t,t+1}, u_{t+1,t}, \cdots)$ be a vertex of $\mathrm{D}(k, \mathbb{K})$ ($\alpha \in \{(1,0),(0,1)\}$, it does not matter whether u is a point or a line). For every r, $2 \leqslant r \leqslant t$, let

$$a_r = a_r(u) = \sum_{i=0,r} (u_{ii}u'_{r-i,r-i} - u_{i,i+1}u_{r-i,r-i-1}),$$

and $a = a(u) = (a_2, a_3, \cdots, a_t)$. Similarly, we assume $a = a(u) = (a_2, a_3, \cdots, a_t, \dots)$ for the vertex u of infinite graph $D(\mathbb{K})$.

Let η_k (η) be the equivalence relation:

$$u\eta_k v \Leftrightarrow a(u) = a(v) \quad (u\eta v \Leftrightarrow a(u) = a(v))$$

on the vertex set of graph $D(k, \mathbb{K})$ ($D(\mathbb{K})$), respectively .

Proposition 2 ([37]). *Let K be the commutative ring.*

(i) *For any $t' - 1$ ring elements $x_i \in \mathbb{K}$, $2 \leqslant t' \leqslant [(k+2)/4]$, there exists a vertex v of $\mathrm{D}(k, \mathbb{K})$ for which $a(v) = (x_2, \ldots, x_{t'}) = (x)$.*

(ii) *The equivalence class C_k for the equivalence relation η_k on the set $\mathbb{K}^k \cup \mathbb{K}^k$ is isomorphic to the affine variety $\mathbb{K}^t \cup \mathbb{K}^t$, $t = [4/3k] + 1$ for $k = 0, 2, 3 \bmod 4$, $k = [4/3n] + 2$ for $k = 1 \bmod 4$.*

(iii) *the vertex set C_k is the union of several connected components of $\mathrm{D}(k, \mathbb{K})$.*

Let C be the equivalence class on η on the vertex set $\mathrm{D}(\mathbb{K})$, then the induced subgraph with the vertex set C is the union of several connected components of $\mathrm{D}(\mathbb{K})$.

We shall use notation $C(t, \mathbb{K})$ ($C(\mathbb{K})$) for the induced subgraph of $D(k, \mathbb{K})$ ($D(\mathbb{K})$) with the vertex set C_k (vertex set C, respectively).

The graph $C(t, \mathbb{K})$ in the case of $\mathbb{K} = \mathbb{F}_q$, q is odd, coincides with $CD(k, q)$ which was introduced in [15].

The following statement was proven in [39].

Theorem 1. *Let $\mathbb{K}$ be commutative ring with unity of characteristic d, $d \neq 2$. Then graphs $C(t, \mathbb{K})$, $t \geqslant 2$ and $C(\mathbb{K})$ are connected.*

If $\mathbb{K} = \mathbb{F}_q$, q is odd, then the graph $C(\mathbb{F}_q)$ is a q-regular tree. In cases $\mathrm{char}(\mathbb{K}) = 2$ the questions of the description of connected components of $C(t, \mathbb{K})$ and $C(\mathbb{K})$ are open.

Below we consider the family of infinite linguistic graphs $A(\mathbb{K})$ formed by quotients of $D(\mathbb{K})$ where $\mathbb{K}$ is a commutative ring.

Let P_A and L_A be two copies of Cartesian power $\mathbb{K}^{\mathbb{N}}$, where $\mathbb{K}$ is the commutative ring and $\mathbb{N}$ is the set of positive integer numbers. Elements of P_A will be called *points* and those of L_A *lines*.

To distinguish points from lines we use parentheses and brackets. If $x \in V$, then $(x) \in P_A$ and $[x] \in L_A$. It will be also advantageous to adopt the notation for co-ordinates of points and lines introduced in [23] for the case of a general commutative ring $\mathbb{K}$:

$$(p) = (p_{0,1}, p_{1,1}, p_{1,2}, p_{2,2}, p_{2,3}, \ldots, p_{i,i}, p_{i,i+1}, \ldots),$$
$$[l] = [l_{1,0}, l_{1,1}, l_{1,2}, l_{2,2}, l_{2,3}, \ldots, l_{i,i}, l_{i,i+1}, \ldots].$$

The elements of P_A and L_A can be thought of as infinite ordered tuples of elements from $\mathbb{K}$, such that only a finite number of components are different from zero.

Now we define an incidence structure (P_A, L_A, I_A) as follows. We say that the point (p) is incident with the line $[l]$, and we write $(p)I_A[l]$, if the following relations between their co-ordinates hold:

$$l_{i,i} - p_{i,i} = l_{1,0}p_{i-1,i},$$
$$l_{i,i+1} - p_{i,i+1} = l_{i,i}p_{0,1}$$

The incidence structure (P_A, L_A, I_A) we denote as $A(\mathbb{K})$. It is clear that the set od indices $\{(1,0),(0,1),(1,1),(1,2),(2,2),(2,3),\ldots,(i-1,i),(i,i),\ldots\}$ is a subset in $\{(1,0),(0,1),(1,1),(1,2),(2,2),(2,2)',\ldots,(i-1,i),(i,i-1),(i,i),(i,i)',\ldots)\}$. So graph $A(\mathbb{K})$ is a symplectic quotient of linguistic incidence structure $D(\mathbb{K})$.

For each positive integer $k \geqslant 2$ we obtain a symplectic quotient $(P_{A,k}, L_{A,k}, I_{A,k})$ as follows. First, $P_{A,k}$ and $L_{A,k}$ are obtained from P_A and L_A respectively by simply projecting each vector into its k initial coordinates with the respect to the above order. The incidence $I_{A,k}$ is then defined by imposing the first k–1 incidence equations and ignoring all others. The incidence graph corresponding to the structure $(P_{A,k}, L_{A,k}, I_{A,k})$ is denoted by $A(k, \mathbb{K})$.

For each positive integer $k \geqslant 2$ we consider the *standard* symplectic projection $\phi_{A,k}$ of $(P_{A,k}, L_{A,k}, I_{A,k})$ onto $(P_{A,k-1}, L_{A,k-1}, I_{A,k-1})$ defined as simple projection of each vector from $P_{A,k}$ and $L_{A,k}$ onto its $k-1$ initial coordinates with respect to the above order. It is clear that $A(2,K)$ and $A(3,K)$ coincides with the $D(2,K)$ and $D(3,K)$, respectively.

Proposition 3. *Graph $A(2n+2,K)$ is a symplectic quotient of the linguistic graph $D(4n+1,K)$, $n \geqslant 2$, and $A(2n+3,K)$ is a symplectic quotient of $D(4n+3)$.*

Proof. We can arrange indices for points and lines of $D(4n+3,K)$, as $\{(1,0),(0,1),(1,1),(1,2),(2,2),(2,3),\ldots,(n+1,n+1),(n+1,n+2),(2,1),(2,2)',(3,2),(3,3)',\ldots(n+1,n),(n+1,n+1)'\}$. So the projection of a point and a line onto the first $2m+3$ coordinates is the symplectic homomorphism. In the case of $k = 4n+1$ one can partite the set of indices into disjoint union of $\{(1,0),(0,1),(1,1),(1,2),(2,2),\ldots,(n,n+1),(n+1,n+1)\}$ and $\{(2,1),(2,2)',(3,2),\ldots,(n,n)',(n+1,n)\}$. So, the projection of the point and the line onto first set contains $2n+2$ coordinates is a symplectic homomorphism. □

Notice, that graphs of kind $D(4n+3, K)$ have n connectivity invariants a_2, a_3, …, a_n, a_{n+1} and graphs $D(4n+1, K)$ have $n-1$ connectivity invariants a_2, a_3, …, a_n.

The free module K^{4n+2} (totality of flags for $D(4n+1, K)$) can be identified with the totality of functions $\{f : \Omega_{D,4n+1} \to K\}$. The natural base is formed by functions e_h, $h \in \Omega_{D,4n+1}$ such that $e_h(x) = 1$ for $x = h$ and $e_h(x) = 0$ otherwise. Tuple $(z_{0,1}, z_{1,0}, \ldots, z_{n+1,n+1})$ is a linear combination of e_h, $h \in \Omega_{D,4n+1}$, where $\Omega_{D,4n+1}$ is set of indexes with an order given in the following way

$$((1,0),(0,1),(1,1),(1,2),(2,1),(2,2),(2,2)',(2,3),(3,2),(3,3),\ldots,$$
$$(n,n)',(n,n+1),(n+1,n),(n+1,n+1))$$

7. The examples of cryptosystems with complexity estimates

We give examples of linguistic graphs and related symbolic keys, which can be used in above described cryptosystem. More specifically, in our examples we will use a pair of graphs $D(4n+1, K)$ and $A(2n+2, K)$ corresponding to the incidence structures $(P_{D,4n+1}, L_{D,4n+1}, I_{D,4n+1})$ and $(P_{A,2n+1}, L_{A,2n+2}, I_{A,2n+2})$ defined over a commutative ring K (case of pair $D(4n+3)$, $A(2n+3)$ is very similar). Recall, that graph $D(4n+1, K)$ have a connectivity invariants $G_1 = a_2$, $G_2 = a_3$, …, $G_t = a_n$, where $t = n-1$. The deformated graph has same connectivity invariants.

We assume, that we deal with the deformated linguistic graphs of kind $I = I^{\psi}_{D,4n+1}$, where permutation ψ change the standard order on the set $\Omega_{D,4n+1}$ in the definition of graph $D(4n+1, K)$ determines new set Ω of elements of $\Omega_{D,4n+1}$ with the order of elements $(0,1)$, $(1,0)$, $(1,1)$, $(1,2)$, $(2,2)$, …, $(n,n+1)$, $(n+1,n+1)$, $(2,1)$, $(2,2)'$, $(3,2)$, …, $(n,n)'$, $(n+1,n)$. The homomorphism of deformated flag systems for $D(4n+1, K)$ and $A(2n+2, K)$ is just projections of tuples of length $4n+2$ onto their initial $2n+3$ coordinates.

More specifically, at the beginning we work with flag linguistic graphs ${}^{\mathcal{F}}I^{\psi}_{D,4n+1}$ and ${}^{\mathcal{F}}I^{\psi}_{A,2n+2}$ and next we deal with ${}^{\mathcal{F}}I_{D,4n+1}$ and ${}^{\mathcal{F}}I^{\psi}_{A,2n+2}$.

First, Alice works with flag $F_1 \in^{\mathcal{F}} I^{\psi}_{D,4n+1}$, which corresponds to concatenation of tuples

$$\mathrm{m}' = (y_{1,0}, x_{0,1}, x_{1,1}, x_{1,2}, x_{2,2}, \ldots, x_{n,n+1}, x_{n+1,n+1}) \in^{\mathcal{F}} I^{\psi}_{A,M}$$

(it corresponds to plaintext m) and

$$\mathrm{v}' = (x_{2,1}, x'_{2,2}, x_{2,3}, \ldots, x'_{n,n}, x'_{n+1,n+1})$$

(it corresponds to random extention of plaintext v).

Next, she works with flag $F_2 = \{(\mathrm{x}), [\mathrm{y}]\} \in^{\mathcal{F}} I_{D,4n+1}$, where $\rho(\mathrm{x}) = x_{0,1}$, $\rho(\mathrm{y}) = y_{1,0}$ and

$$(\mathrm{x}) = (x_{0,1}, x_{1,1}, x_{1,2}, x_{2,1}, x_{2,2}, \ldots, x'_{n,n}, x_{n,n+1}, x_{n+1,n}, x_{n+1,n+1}).$$

i.e. F_2 corresponds to the tuple

$$(x_{0,1}, y_{1,0}, x_{1,1}, x_{1,2}, x_{2,1}, x_{2,2}, \ldots, x'_{n,n}, x_{n,n+1}, x_{n+1,n}, x_{n+1,n+1}).$$

Moreover, in this case we have $W = K^{4n+1}, W_1 = K^{2n+2}\, W_2 = K^{2n-1}$ and the permutation $\pi = \psi^{-1}$ on the set of indices Ω defines $\pi(\Omega) = \Omega_{D,4n+1}$.

Example 1. For the simplicity, we assume that $K = Q^l$ and $l = 1$. Alice chooses two pseudorandom sequences of ring elements $\alpha_1, \alpha_2, \ldots, \alpha_{h+1}$ and $\beta_1, \beta_2, \ldots, \beta_h$. She forms the symbolic key as $D_i(z_1, z_2, \ldots, z_{t+1}) = z_1 + \alpha_i,\ i = 1, 2, \ldots, h+1$, and $E_i(z_1, z_2, \ldots, z_{t+1}) = z_2 + \beta_i,\ i = 1, 2, \ldots, h+1$. Next, she computes its specializations $D'_i(x_{0,1}) = x_{0,1} + \alpha_i, i = 1, 2, \ldots, h+1$, $E'_j(y_{1,0}) = y_{1,0} + \beta_j, j = 1, 2, \ldots, h$, corresponding to the substitution $z_1 = x_{0,1}$, $z_2 = y_{1,0}$ and determines the transformation

$$N = N_{P,D'_1} N_{L,E'_1} N_{P,D'_2} N_{L,E'_2} \ldots N_{P,D'_h} N_{L,E'_h} N_{P,D'_{h+1}}$$

for the flag incidence system ${}^{\mathcal{F}}I_{D,4n+2}$. She executes by the tools of Computer Algebra the following transformation on K^{4n+2}. She computes H as a composition of maps T, ψ^{-1}, N and T_2, where W_1 is invariant subspace of T. Recall that W_1 is a totality of w such that $w_{2,1} = 0, w'_{2,2} = 0, w_{3,2} = 0, \ldots, w'_{n,n} = 0, w_{n+1,n} = 0$. It means that T_1 is a linear transformation of kind

$$\begin{aligned}
z_{0,1} &\to t_{0,1}(z_{0,1}, z_{1,0}, z_{1,1}, z_{1,2}, z_{2,2} \ldots, z_{n,n+1}, z_{n+1,n+1}) \\
z_{1,0} &\to t_{0,1}(z_{0,1}, z_{1,0}, z_{1,1}, z_{1,2}, z_{2,2} \ldots, z_{n,n+1}, z_{n+1,n+1}) \\
z_{1,1} &\to t_{1,1}(z_{0,1}, z_{1,0}, z_{1,1}, z_{1,2}, z_{2,2} \ldots, z_{n,n+1}, z_{n+1,n+1}) \\
z_{1,2} &\to t_{1,2}(z_{0,1}, z_{1,0}, z_{1,1}, z_{1,2}, z_{2,2} \ldots, z_{n,n+1}, z_{n+1,n+1}) \\
z_{2,2} &\to t_{2,2}(z_{0,1}, z_{1,0}, z_{1,1}, z_{1,2}, z_{2,2} \ldots, z_{n,n+1}, z_{n+1,n+1}) \\
&\ldots \\
z_{n,n+1} &\to t_{n,n+1}(z_{0,1}, z_{1,0}, z_{1,1}, z_{1,2}, z_{2,2} \ldots, z_{n,n+1} z_{n+1,n+1})
\end{aligned}$$

$$
\begin{aligned}
z_{n+1,n+1} &\to t_{n+1,n+1}(z_{0,1}, z_{1,0}, z_{1,1}, z_{1,2}, z_{2,2} \ldots, z_{n,n+1}z_{n+1,n+1}) \\
z_{2,1} &\to t_{2,1}(z_{0,1}, z_{1,0}, z_{1,1}, \ldots, z_{n,n+1}z_{n+1,n+1}z_{2,1}, z'_{2,2}, \ldots, z'_{n,n}, z_{n+1,n}) \\
z'_{2,2} &\to t'_{2,2}(z_{0,1}, z_{1,0}, z_{1,1}, \ldots, z_{n,n+1}z_{n+1,n+1}z_{2,1}, z'_{2,2}, \ldots, z'_{n,n}, z_{n+1,n}) \\
z_{3,2} &\to t_{3,2}(z_{0,1}, z_{1,0}, z_{1,1}, \ldots, z_{n,n+1}z_{n+1,n+1}z_{2,1}, z'_{2,2}, \ldots, z'_{n,n}, z_{n+1,n}) \\
&\ldots \\
z'_{n,n} &\to t_{n,n}(z_{0,1}, z_{1,0}, z_{1,1}, \ldots, z_{n,n+1}z_{n+1,n+1}z_{2,1}, z'_{2,2}, \ldots, z'_{n,n}, z_{n+1,n}) \\
z_{n+1,n} &\to t_{n+1,n}(z_{0,1}, z_{1,0}, z_{1,1}, \ldots, z_{n,n+1}z_{n+1,n+1}z_{2,1}, z'_{2,2}, \ldots, z'_{n,n}, z_{n+1,n})
\end{aligned}
$$

where t_β, $\beta \in \Omega$ are linear forms.

After the multiplication of vector z from the right on permutational matrix corresponding to $\psi^{-1} = \pi$ Alice gets the string of expressions $t_{\psi(\beta)}$, written in accordance with the initial order on Ω (see the definition of graph $D(4n+1, K)$). So, new tuple can be treated in natural way as a flag of $D(4n+1, K)$. After the application of N acting on flags of $D(4n+1, K)$ tuple t_β will be transformed in

$$f_\beta(z_{0,1}, z_{1,0}, z_{1,1}, \ldots, z_{n,n+1}z_{n+1,n+1}z_{2,1}, z'_{2,2}, \ldots, z'_{n,n}, z_{n+1,n}).$$

So, Alice will get the transformation in the form

$$z_\alpha \to f_\pi(\alpha)(z_{0,1}, z_{1,0}, z_{1,1}, \ldots, z_{n,n+1}z_{n+1,n+1}z_{2,1}, z'_{2,2}, \ldots, z'_{n,n}, z_{n+1,n}),$$

where $\alpha \in \{(1,0), (0,1), (1,1), (1,2), (2,1), (2,2), (2,2)', (2,3), (3,2), (3,3), \ldots, (n,n)', (n,n+1), (n+1,n), (n+1,n+1)\}$. The final transformation will change z_α on certain linear combination of z_β, $\beta \in \Omega$ and we get the list of public rules

$$
\begin{aligned}
z_{0,1} &\to h_{0,1}(z_{0,1}, z_{1,0}, z_{1,1}, \ldots, z_{n,n+1}z_{n+1,n+1}z_{2,1}, z'_{2,2}, \ldots, z'_{n,n}, z_{n+1,n}) \\
z_{1,0} &\to h_{0,1}(z_{0,1}, z_{1,0}, z_{1,1}, \ldots, z_{n,n+1}z_{n+1,n+1}z_{2,1}, z'_{2,2}, \ldots, z'_{n,n}, z_{n+1,n}) \\
z_{1,1} &\to h_{1,1}(z_{0,1}, z_{1,0}, z_{1,1}, \ldots, z_{n,n+1}z_{n+1,n+1}z_{2,1}, z'_{2,2}, \ldots, z'_{n,n}, z_{n+1,n}) \\
&\ldots \\
z_{n,n+1} &\to h_{n,n+1}(z_{0,1}, z_{1,0}, z_{1,1}, \ldots, z_{n,n+1}z_{n+1,n+1}z_{2,1}, z'_{2,2}, \ldots, z'_{n,n}, z_{n+1,n}) \\
z_{n+1,n+1} &\to h_{n+1,n+1}(z_{0,1}, z_{1,0}, z_{1,1}, \ldots, z_{n,n+1}z_{n+1,n+1}z_{2,1}, z'_{2,2}, \ldots, z'_{n,n}, z_{n+1,n}) \\
z_{2,1} &\to h_{2,1}(z_{0,1}, z_{1,0}, z_{1,1}, \ldots, z_{n,n+1}z_{n+1,n+1}z_{2,1}, z'_{2,2}, \ldots, z'_{n,n}, z_{n+1,n}) \\
&\ldots \\
z'_{n,n} &\to h_{n,n}(z_{0,1}, z_{1,0}, z_{1,1}, \ldots, z_{n,n+1}z_{n+1,n+1}z_{2,1}, z'_{2,2}, \ldots, z'_{n,n}, z_{n+1,n}) \\
z_{n+1,n} &\to h_{n+1,n}(z_{0,1}, z_{1,0}, z_{1,1}, \ldots, z_{n,n+1}z_{n+1,n+1}z_{2,1}, z'_{2,2}, \ldots, z'_{n,n}, z_{n+1,n})
\end{aligned}
$$

We can prove that the transformation is a cubical map.

Notice that complexity of the use of this multivariate encryption H for Bob can be estimated via complexity of computation of the value of general cubical map in $4n+2$ variables in given point of affine space K^{4n+2}. So, it equals $(4n+2)^4$ (or $O(n^4)$).

The complexity of decryption for Alice is different. We assume that Alice has already computed invertible matrices. She needs to compute the value of two linear maps in given vector. It takes $O(n^2)$ elementary steps. The computation of N^{-1} takes $O(nh)$, where $2h+1$ is the length of the walk on the graph. In practical case when $h = O(m)$ the complexity of decryption procedure is $O(n^2)$. Notice, that if matrices are sparse (number of nonzero parameters for each row or column as well as parameter h are bounded by independent constant) the complexity of decryption is $O(n)$.

Example 2. We generalise the previous example in the following way. Let $a_2(\mathrm{x}), a_3(\mathrm{x}), \ldots, a_{n-1}(\mathrm{x})$ be the list of invariants of the graph $D(4n+1, K)$. Alice chooses function $f(z_1, z_2, z_3, \ldots, z_n) \in K[z_1, z_2, z_3, \ldots, z_n]$ with the property: for all tuples $(b_2, \ldots, b_{n+1}) \in K^{n+1}$ the equation

$$f(z_1, b_2, b_3, \ldots, b_{n+1}) = a$$

has a unique solution $z_1 = \alpha \in K$ (the free module K^{4n+2} can be substituted for submanifold M isomorphic to $\mathrm{Reg(K)})K^{4n+1}$ consisting of tuples such that $y_{1,0}$ belongs to the totality Reg(K) of all invertible elements of finite commutative ring K).

Alice computes $f(x_{0,1}, y_{1,0}, a_2(\mathrm{x}), a_3(\mathrm{x}), \ldots, a_{n-1}(\mathrm{x})) = g(\mathrm{x}, y_{1,0})$,

She chooses pseudorandom parameters $\alpha_1, \alpha_2, \ldots, \alpha_{h+1}$ and $\beta_1, \beta_2, \ldots, \beta_h$ (or two random tuples generated by Quantum Computer) and generates the specialised symbolic key as $D'_i(x_{0,1}, y_{1,0}, a_2(\mathrm{x}), a_3(\mathrm{x}), \ldots, a_{n-1}(\mathrm{x})) = g(\mathrm{x}, y_{1,0}) + \alpha_i, i = 1, 2, \ldots, h+1$, $E'_j(y_{1,0}) = y_{1,0} + \beta_j, j = 1, 2, \ldots, h$, and determines multivariate transformation N.

We can evaluate degree of N as 3deg $(g(\mathrm{x}, y_{1,0}))$.

Examples of some functions g of small degree:

(a) $g(\mathrm{x}, y_{1,0}) = x_{0,1}y_{1,0} + \lambda_2 a_2(\mathrm{x}) + \lambda_3 a_3(\mathrm{x}) + \cdots + \lambda_{n-1}a_{n-1}(\mathrm{x})$. Recall, that we may use manifold M of all tuples, where $y_{1,0}$ is a regular element of ring K. Alice can use the pseudorandom (or even random) sequence λ_i for construction of the map.

(b) $g(\mathrm{x}, y_{1,0}) = x_{0,1}^3 + y_{1,0}(\lambda_2 a_2(\mathrm{x}) + \lambda_3 a_3(\mathrm{x}) + \ldots \lambda_{n-1}a_{n-1}(\mathrm{x})) + \alpha y_{1,0}^2 + \beta y_{1,0} + \gamma$. We assume that the ring K is chosen such that the equation $z^3 = a$ has a unique solution in variable z.

Let us assume that $deg(g(\mathrm{x}, y_{1,0})) = d$. Then Bob can encrypt for polynomial time $O(m^{3d+1})$. The complexity of decryption for Alice now is maximum of complexities of computation of $g(\mathrm{x}, y_{1,0})$ and $O(n^2)$. Let us take a "sparse" polynomial expression $g(\mathrm{x}, y_{1,0})$, i.e. the multivariate polynomial, which can be computed for $O(n^2)$ elementary steps. Then the complexity of decryption for Alice will be still $O(n^2)$.

It is easy to generalise above written examples for the case $K = Q^l$ with $l \geqslant 1$.

Example 3. Let us consider the case $K = Q^l$, where Q is some subring K. We fix the base and write ring element as $(x_1, x_2, \ldots, x_l)$. Assume that the product of two $(x_1, x_2, \ldots, x_l)$ and $(y_1, y_2, \ldots, y_l)$ is given by quadratic polynomial map $h : K^l \times K^l \to K^l$ like in case $K = Q[x]/m(x)$, where $m(x)$ is a polynomial map from $Q[x]$ of degree l.

So, we choose polynomial $g(z_1^1, z_1^2, \ldots z_1^l, z_2^1, z_2^2, \ldots z_2^l, \ldots, z_{t+1}^1, z_{t+1}^2, \ldots z_{t+1}^l)$ in $l(t+2)$ variables over Q instead of function f as in the previous algorithm.

A nice example can be obtained as

$$g(\mathrm{x}, \rho(\mathrm{y})) = (\rho(\mathrm{x})A - \rho(\mathrm{x})) \times \rho(\mathrm{y}) + a_2(\mathrm{x})A_2 + a_3(\mathrm{x})A_3 + \ldots a_{n-1}(\mathrm{x})A_{n-1} + \mathrm{d},$$

where A is a matrix without eigenvalue 1, $\rho(x) = (x_{0,1}^1, x_{0,1}^2, \ldots x_{0,1}^l) \in Q^l$, $\rho(y) = (y_{1,0}^1, y_{1,0}^2, \ldots, y_{1,0}^l) \in Q^l$, $a_i(\mathrm{x}) \in Q^l$, matrices A_i,$i \geqslant 2$ correspond to arbitrary maps of Q^l into itself, $\mathrm{d} \in Q^l$.

In that case Bob can also encrypt for polynomial time from parameter n and Alice can decrypt essentially faster.

8. Remarks and Conclusion

The idea of the usage of *symbolic keys* in the case of $D(n, q)$ based encryption was considered in [30]. General multivariate maps based on symbolic key for a linguistic graph as cryptographical tools was proposed in [31]. Degree estimates of multivariate maps on the flag space of $D(n, K)$ corresponding to symbolic key of kind $x_{0,1} + \alpha_i, y_{1,0} + \beta_i$, $i = 1, 2, \ldots k$, where α_i and β_i are constants from K were obtained in [44] (see also [43]). Discussions of computer simulations of $D(n, K)$ or $A(n, K)$ based algorithms for different cases of rings on the symbolic level or private keys algorithms the reader can find in [7], [8], [10], [11], [12]. Time evaluation of public rule generation, time execution of private key decryption, mixing

properties of encryption, results of order evaluation for bijection encryption maps can be found there. The descryption of connectivity invariants a_i, $i = 2, 3 \dots$ of $D(n, q)$, the reader can find in [15], their generalisation for arbitrary commutative ring are given in [27], [35]. In the case of odd characteristics connectivity invariants give a full descryption of actual connected components. This fact is proven in [37]. If charK $= 2$ then a_i does not give us complete list of invariants (counterexample for $K = \mathbb{F}_2$ is discussed in [29]).

The generalisation of private key algorithm on Schubert incidence structures of arbitrary rank is presented in [40].

The main topic of current paper is a presentation of graph based multivariate cryptosystems which use nonbijective maps. So straight forward linearisation attacks are not formally applicable there.

Authors were the participants of the International Algebraic Conference dedicated to 100-th anniversary of l. A. Kaluzhnin (July 7-12, 2014, Kyiv, Ukraine). Our paper is dedicated to the memory of Lev Kaluznin and his achievements in Mathematics.

References

[1] Bollobás B.: Extremal Graph Theory, Academic Press, London (1978).

[2] Braeken A., Wolf C., Prenel B.: A study of the security of Unbalanced Oil and Vinegar Signature Schemes, ESAT-COSIC (2004).

[3] Bulygin S., Petzoldt A., Buchmann J.: Towards provable security of the unbalanced oil and vinegar signature scheme under direct attacks. In Guang Gong and Kishan Chand Gupta, editors, Progress in Cryptology - INDOCRYPT 2010, volume 6498 of Lecture Notes in Computer Science, 17-32 (2010).

[4] Ding J., Gower J. E., Schmidt D. S.: Multivariate Public Key Cryptosystems, 260. Springer, Advances in Information Security, v. 25, (2006).

[5] Kipnis A., Shamir A.: Cryptanalisis of the Oil and Vinegar Signature Scheme, Advances in Cryptology - Crypto 96, Lecture Notes in Computer Science, v. 1462, 257-266 (1996).

[6] Kipnis. A. Unbalanced Oil and Vinegar Signature Scheme - extended version, Euro-Crypt (1999).

[7] Klisowski M., Ustimenko V.: On the Comparison of Cryptographical Properties of Two Different Families of Graphs with Large Cycle Indicator, Mathematics in Computer Science, Volume 6, Number 2, 181-198 (2012).

[8] Klisowski M., Romańczuk U., Ustimenko V.: On the implementation of cubic public keys based on new family of algebraic graphs, Annales UMCS Informatica, AI XI, Number 2, 127-14 (2011).

[9] Koblitz N.: Algebraic aspects of cryptography. Algorithms and Computation in Mathematics, vol. 3, Springer (1998).

[10] Kotorowicz J. S., Ustimenko V.: On the properties of stream ciphers based on extremal directed graphs, Cryptography Research Perspective (Roland E. Chen, ed.), Nova Science Publishers, 125-141 (2009).

[11] Kotorowicz, S., Ustimenko V.: On the implementation of cryptoalgorithms based on algebraic graphs over some commutative rings, Condens. Matter Phys. 11, no. 2(54), 347–360 (2008).

[12] Kotorowicz J. S., Romańczuk U., Ustimenko V.: On the implementation of stream ciphers based on a new family of algebraic graphs, IEEE Computer Society Press, Proceedings of the Conference CANA, FedSCIS, 485-490 (2011).

[13] Lazebnik F., Ustimenko V.: Explicit construction of graphs with an arbitrary large girth and of large size, Discrete Appl. Math. , 60, 275-284 (1995).

[14] Lazebnik F., Ustimenko V. A., A. J. Woldar A. J.: New Series of Dense Graphs of High Girth, Bull (New Series) of AMS, v.32, N1, 73-79 (1995).

[15] Lazebnik F., Ustimenko V. A., Woldar A. J.: A Characterization of the Components of the graphs $D(k, q)$, Discrete Mathematics, 157, 271-283 (1996).

[16] Patarn J.: The Oil i Vinegar digital signatures, Presented at Dagstuhl Workshop on Cryptography (1997).

[17] Petzoldt A., Bulygin S., Buchmann J.: Cyclicrainbow - a multivariate signature scheme with a partially cyclic public key. In Guang Gong and KishanChand Gupta, editors, Progress in Cryptology - INDOCRYPT 2010, volume 6498 of Lecture Notes in Computer Science, 33-48 (2010).

[18] Petzoldt A., Bulygin S., Buchmann J.: Fast verification for improved versions of the uov and rainbow signature schemes. In Philippe Gaborit, editor, Post-Quantum Cryptography, volume 7932 of Lecture Notes in Computer Science, 188-202 (2014).

[19] Romańczuk U., Ustimenko V.:, On the key exchange with matrices of large order and graph based nonlinear maps, Proceedings of the conference Applications of Computer Algebra, Vlora, Special Issue, Vol .4, N 4, 203-211 (2010)

[20] Romańczuk U., Ustimenko V.: On the family of cubical multivariate cryptosystems based on the algebraic graph over finite commutative rings of characteristic 2, Annales UMCS Informatica AI XII,N 3, 89-106 (2012).

[21] Romańczuk U., Ustimenko V.: On the key exchange with new cubical maps based on graphs, Annales UMCS Informatica, vol. 4, N 11, 11-19 (2011).

[22] Romańczuk U., Ustimenko V.: On regular forests given in terms of algebraic geometry, new families of expanding graphs with large girth and Multivariate cryptographical algorithms, Proceedings of International conference “Applications of Computer Algebra”, Malaga, 144-147 (2013).

[23] Romańczuk U., Ustimenko V. A.: On the family of cubical multivariate cryptosystemsbased on exceptional extremal graphs, Third International Conference on Symbolic Computations and Cryptography, Castro Urdiales, Extended Abstracts, 169-175 (2012).

[24] Romańczuk U., Ustimenko V.: On families of large cycle matroids, matrices of large order and key exchange protocols with nonlinear polynomial maps of small degree, Mathematics in Computer Science, Volume 6, Number 2, 167-180 (2012).

[25] Romańczuk-Polubiec U., Ustimenko V.: On new key exchange multivariate protocols based on pseudorandom walks on incidence structures, Dopovidi National Academy of Sciences of Ukraine, 41-49 (2015).

[26] Ustimenko V.: On Multivariate Cryptosystems Based on Computable Maps with Invertible Decomposition, Annales UMCS, Informatica. Volume 14, Issue 1, Pages 7-17, (2014).

[27] Ustimenko V.: Linear interpretations for flag geometries of Chevalley groups, Ukr. Math. J., v. 42, no. 3, (in Russian) 383-387 (1990).

[28] Ustimenko V.: Small Schubert cells as subsets in Lie algebras, Functional Analysis and Applications, v. 25, no. 4, 81-83 (1991).

[29] Ustimenko V.: Coordinatisation of Trees and their Quotients, The "Voronoj's Impact on Modern Science", Kiev, Institute of Mathematics, vol. 2, 125-152 (1998).

[30] Ustimenko V.: On the varieties of parabolic subgroups, their generalisations and combinatorial applications, Acta Applicandae Mathematicae, 52, 223-238 (1998).

[31] Ustimenko V.: CRYPTIM: Graphs as Tools for Symmetric Encryption, Lecture Notes in Computer Science, Springer, v. 2227, 278-287 (2001).

[32] Ustimenko V.: Graphs with Special Arcs and Cryptography, Acta Applicandae Mathematicae, vol. 74, N2, 117-153 (2002).

[33] Ustimenko V. : Maximality of affine group and hidden graph cryptosystems, J. Algebra Discrete Math., No 1, 133-150 (2005).

[34] Ustimenko V.: On the cryptographical properties of extreme algebraic graphs, Algebraic Aspects of Digital Communications, IOS Press (Lectures of Advanced NATO Institute, NATO Science for Peace and Security Series - D: Information and Communication Security), Volume 24, July, 296 pp. (2009).

[35] Ustimenko V.: Schubert cells in Lie geometries and key exchange via symbolic computations, Proceedings of the International Conference "Applications of Computer Algebra", Vlora, Albanian Journal of Mathematics, Special Issue, vol .4 n 4, 135- 145 (2010).

[36] Ustimenko V.: On the extremal graph theory for directed graphs and its cryptographical applications, In: T. Shaska, W.C. Huffman, D. Joener and V.Ustimenko, Advances in Coding Theory and Cryptography, Series on Coding and Cryptology, vol. 3, 181-200 (2007).

[37] Ustimenko V. A.: Linguistic Dynamical Systems, Graphs of Large Girth and Cryptography, Journal of Mathematical Sciences, Springer, vol.140, N3, 412-434 (2007).

[38] Ustimenko V. A.: On the graph based cryptography and symbolic computations, Serdica Journal of Computing, Proceedings of International Conference on Application of Computer Algebra, ACA-2006, Varna, N1 (2007).

[39] Ustimenko V. A., Algebraic groups and small world graphs of high girth, Albanian J. Math., 3 , No. 1, 25-33 (2009).

[40] Ustimenko V. A.: On extremal graph theory and symbolic computations, Dopovidi National Academy of Sciences of Ukraine, N2 (in Russian), 42-49 (2013).

[41] Ustimenko V. A.: On K-theory of dynamical system, corresponding to graphs and its applications, Dopovidi National Academy of Sciences of Ukraine, N8 (in Russian), 44-51 (2013).

[42] Ustimenko V.: On walks of variable length in the Schubert systems and multivariate stream ciphers, Dopovidi National Academy of Sciences of Ukraine, N 3, 55-63 (2014).

[43] Ustimenko V., Romańczuk U.: On Dynamical Systems of Large Girth or Cycle Indicator and their applications to Multivariate Cryptography, Artificial Intelligence, Evolutionary Computing and Metaheuristics, In the footsteps of Alan Turing Series: Studies in Computational Intelligence, Vol. 427, Springer, 257-285 (2013).

[44] Ustimenko V., Romańczuk U.: On Extremal Graph Theory, Explicit Algebraic Constructions of Extremal Graphs and Corresponding Turing Encryption Machines, Artificial Intelligence, Evolutionary Computing and Metaheuristics, In the footsteps of Alan Turing Series: Studies in Computational Intelligence, Vol. 427, Springer, 231-256 (2013).

[45] Ustimenko V., Wróblewska A.: On the key exchange with nonlinear polynomial maps of stable degree, Annalles UMCS Informatica AI X1, 2, 81-93 (2011).

[46] Wróblewska A.: On some properties of graph based public keys, Albanian Journal of Mathematics, Volume 2, Number 3, NATO Advanced Studies Institute: New challenges in digital communications, 229-234 (2008).

Contact information

U. Romańczuk-Polubiec ul. Ogrodowa 5/19, 17-100 Bielsk Podlaski, Poland
E-Mail(*s*): urszula_romanczuk@yahoo.pl

V. Ustimenko University of Maria Curie Skłodowska, Pl. Maria Curie Skłodowska 1, pok. 323, 20-931, Lublin, Poland
E-Mail(*s*): vasyl@hektor.umcs.lublin.pl

Received by the editors: 12.03.2015
and in final form 12.03.2015.