Algebra and Discrete Mathematics
Volume **20** (2015). Number 1, pp. 152–170

RESEARCH ARTICLE

On algebraic graph theory and non-bijective multivariate maps in cryptography

Vasyl Ustimenko

Communicated by R. I. Grigorchuk

This paper is dedicated to the glorious 60-th anniversary of Efim Zelmanov whose research is an inspirational example of continuous fruitful serving to Algebra

Abstract. Special family of non-bijective multivariate maps F_n of ${Z_m}^n$ into itself is constructed for $n = 2, 3, \ldots$ and composite m. The map F_n is injective on $\Omega_n = \{\mathrm{x} | x_1 + x_2 + \ldots x_n \in {Z_m}^*\}$ and solution of the equation $F_n(\mathrm{x}) = \mathrm{b}, \mathrm{x} \in \Omega_n$ can be reduced to the solution of equation $z^r = \alpha$, $z \in {Z_m}^*$, $(r, \phi(m)) = 1$. The "hidden RSA cryptosystem" is proposed.

Similar construction is suggested for the case $\Omega_n = {Z_m}^{*n}$.

1. Introduction

The RSA is one of the most popular cryptosystems. It is based on a number factorisation problem and Euler Theorem. Peter Shor discovered that factorisation problem can be effectively solved with the usage of theoretical quantum computer. It means that RSA could not be a security tool in the future postquantum era. One of the research directions which can lead to a postquantum secure public key is the Multivariate Cryptography which uses polynomial maps of affine space K^n defined over a finite commutative ring into itself as encryption tools (see [1]). This is a young promising research area with the current lack of known cryptosystems

Key words and phrases: multivariate cryptography, linguistic graphs, hidden Eulerian equation, hidden discrete logarithm problem.

with the proven resistence against attacks with the use of Turing machines. Other important direction of Postquantum Cryptography is a study of Super-elliptic Curves cryptosystems.

Applications of Algebraic Graph Theory to Multivariate Cryptography were observed in my talk at Central European Conference on Cryptology 2014 (Alfred Renyi Institute, Budapest) [2]. This talk was dedicated to algorithms based on bijective maps of affine spaces into themselves. Applications of algebraic graphs to cryptography started from symmetric algorithms based on explicit constructions of extremal graph theory and their directed analogs (see survey [3], [4]). The main idea is to convert an algebraic graph in finite automaton and use the preudorandom walks on the graph as encryption tools. This approach can be also used for the key exchange protocols. Nowadays the idea of "symbolic walks" on algebraic graphs when the walk on the graph depends on parameters given as special multivariate polynomials in variables depending on plainspace vector brings several public key cryptosystems. Other source of graphs suitable for cryptography is connected with finite geometries and their flag system (see [3], [5], [6] and further references).

This paper presents new cryptoalgorithm in terms of Algebraic Combinatorics which use non-bijective transformations of K^n.

Multivariate cryptography started from studies of potential for the special quadratic encryption multivariate bijective map of K^n, where K is an extention of finite field F_q of characteristic 2. One of the first such cryptosystems was proposed by Imai and Matsumoto, cryptanalysis for this system was invented by J. Patarin [1], [7]. The survey on various modifications of this algorithm and corresponding cryptanalysis the reader can find in [1]. Bijective multivariate sparse encryption maps of rather high degree based on walks in algebraic graphs were proposed in [8].

One of the first usage of non bijective map of multivariate cryptography was in *oil and vinegar* crptosystem proposed in [9] and analysed in [10]. Nowadays this general idea is strongly supported by the publication [11] dedicated to security analysis 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 defined over finite fields. Non bijective multivariate sparse encryption maps of degree 3 and $\geqslant 3$ based on walks on algebraic graphs $D(n, K)$ defined over general commutative ring and their homomorphic images were proposed in [12].

The paper is dedicated to other constructions of non bijective maps. We introduce the concept of family of multivariate maps $F = F_n$ of

the free modules K^n onto itself decomposed into transition functions $F^1, F^2, \ldots, F^{s(n)}$ of special symbolic vertex automata of linguistic graphs. In case $K = Z_m$, where m is composite, it allows us to construct partially invertible F_n respectively to subsets Ω_n of ${Z_m}^n$. It means that the restriction of F on Ω_n is injective and the decomposition above allows us to solve the equation $F(\mathrm{x})) = \mathrm{b}$ for unknown $(\mathrm{x}) \in \Omega_n$ and $\mathrm{b} \in F(\Omega_n)$ in polynomial time. We are interested in the case of Eulerian maps F_n when the solution of the equation can be reduced to the study of equations of kind $z^r = d$, where z in ${Z_m}^*$ and $(r, \phi(m)) = 1$. We construct infinite families of maps of kind $H_n = \tau_1 F_n \tau_2$, where τ_i are bijective affine transformations of ${Z_m}^n$, with Eulerian F_n of bounded degree such that H_n is partially invertible for $\Omega_n = {Z_m}^{*n}$ and $\Omega_n = \{\mathrm{x} \in {Z_m}^n | x_1 + x_2 + \ldots x_n \in {Z_m}^*\}$.

So the following scheme of a cryptosystem can be used. Alice (the public key owner) uses special linguistic graph $L_n(Z_m)$, its symbolic automaton with a special symbolic key to generate the Eulerian map F_n and the list of transition functions $F^1, F^2, \ldots, F^{s(n)}$ of the symbolic computation. She chooses appropriate bijective affine transformations τ_1 and τ_2 and creates a deformation $H_n = \tau_1 F_n \tau_2$ which is partially invertible for Ω_n as above. Alice writes the following standard form for H_n:

$$x_1 \to h_1(x_1, x_2, \ldots, x_n), \quad x_2 \to h_2(x_1, x_2, \ldots, x_n), \quad \ldots,$$
$$x_n \to h_n(x_1, x_2, \ldots, x_n)$$

where polynomials $h_i(x_1, x_2, \ldots, x_n)$, $i = 1, 2, \ldots, n$ are given by their lists of monomial terms with respect to the chosen order.

She announces the form and the plainspace Ω_n in public way.

Notice that Alice keeps the transition functions generating F_n and *deformation rule* $H_n = \tau_1 F_n \tau_2$ in secret. Cryptanalytic knows only the list of h_i and the graph $L_n(Z_m)$.

Public user (Bob) writes his message $(p_1, p_2, \ldots, p_n)$ from the plainspace Ω_n. He computes the ciphertext $\mathrm{c} = (c_1, c_2, \ldots, c_n)$, $c_i = h_i(p_1, p_2, \ldots, p_n)$, $i = 1, 2, \ldots, n$ and sends it to Alice.

Alice solves the equation $F_n(x_1, x_2, \ldots, x_n) = (c_1, c_2, \ldots, c_n)$ due to her knowledge of symbolic key of the automaton. So she reads the plaintext.

Notice that to make this scheme feasible we need to care about polynomiality of generation time, bound for the degree of H_n, Eulerian nature of the map F_n. We achieve it via special choice of linguistic graph (well known graphs $D(n, K)$) and some restriction on symbolic keys.

Section 2 is dedicated to linguistic graphs and related to them automata. In Section 3 the reader can find information on chosen linguistic

graph $D(n,K)$. The properties af chosen computation of vertex automaton for graph $D(n,Z_m)$ are justified in section 4. Last section gives precise descryption of cryptosystem.

2. Linguistic graphs and their vertex automata

The missing definitions of graph-theoretical concepts which appear in this paper can be found in [13]. 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 neighbours). 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 $v_0,v_1,\dots,v_t$, such that $v_i\,G\,v_{i+1}$ for $i=1,\dots,t-1$ is a *path* in the graph. The 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 the 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 $v_0,\dots,v_m$ such that $v_i\,G\,v_{i+1}$, $i=1,\dots,m-1$ 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 $\mathrm{x}\in P$, $\mathrm{y}\in L$ or $\mathrm{x}\in L$ and $\mathrm{y}\in P$ as *incidence structure*. The pair $\{\mathrm{x},\mathrm{y}\}$, $\mathrm{x}\in P$, $\mathrm{y}\in L$ 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

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

where ξ_j and ζ_j, $j = 1, 2, \ldots, m$ are not zero divisors, and f_j are multivariate polynomials with coefficients from K. Brackets and parenthesis allow us to distinguish points from lines (see [14]).

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.

We refer to $\rho((\mathrm{x})) = (x_1, x_2, \ldots, x_s)$ for $(\mathrm{x}) = (x_1, x_2, \ldots, x_{s+m})$ and $\rho([\mathrm{y}]) = (y_1, y_2, \ldots, y_r)$ for $[y_1, y_2, \ldots, y_{s+m}]$ as the colour of the point and the colour of the line respectively. For each $\mathrm{b} \in K^r$ and $(\mathrm{p}) = (p_1, p_2, \ldots, p_{s+m})$ there is a unique neighbour of the point $[\mathrm{l}] = N_{\mathrm{b}}(\mathrm{p})$ with the colour b. Similarly for each $\mathrm{b} \in K^s$ and $[\mathrm{l}] = [l_1, l_2, \ldots, l_{r+m}]$ there is a unique neighbour of the line $[\mathrm{p}] = N_{\mathrm{b}}([\mathrm{l}])$ with the colour b. Let $S(K^n)$ be the semigroup of all polynomial maps from K^n into K^n, where K is a commutative ring.

Assume that the transformation $F(n) \in S(K^n)$ is written in the form $x_j \to f(n)_j(x_1, x_2, \ldots, x_n)$ where each $f(n)_j$, $j = 1, 2, \ldots, n$ is determined by the list of all monomial terms with the respect to some chosen order.

Let us refer to the sequence of maps $F(n)$ from $S(K^n)$, $n = 2, 3, \ldots$ as a family of bounded degree, if the degree of each transformation $F(n)$ is bounded by some constant d, $d > 0$.

Let $\tau(n)_L$ and $\tau(n)_R$ be affine transformations of kind $\mathrm{x} \to \mathrm{x}A + \mathrm{b}$, where $\mathrm{x} \in K^n$, $\mathrm{b} \in K^n$, $A = (a_{ij})$, $1 \leqslant i, j \leqslant n$.

We assume, that the transformations $\tau_L(i)$ and $\tau_R(i)$ are invertible.

We refer to the sequence of $G(n) = \tau_L(n)F(n)\tau_R(n)$ as the deformation of the family $F(n)$, $n = 2, 3, \ldots$.

Notice that $\deg g(n) = \deg f(n)$, but densities of the maps can be different. In fact densities of $g(n)$ heavily depend on the choices of an affine transformation τ_L.

Let us convert the bipartite graph of incidence relation $I = I_m$ to vertex automaton $VA(I_m)$ in the following way. We announce that vertices of the graph are states of $VA(I_m)$. If $(\mathrm{p})I[\mathrm{l})]$ and $[\mathrm{l}] = N_{\mathrm{b}}(\mathrm{p})$ then we draw an arrow from (p) to [l] with the weight $\mathrm{b} \in K^r$. If $(\mathrm{p})I[\mathrm{l})]$ and $[\mathrm{p}] = N_{\mathrm{b}}(\mathrm{p})$ then we draw an arrow from [l] to (p) with the weight $\mathrm{b} \in K^s$. We assume that all vertices of the bipartite graph are accepting states.

Let us assume that $r = s = 1$ in all further considerations. We assume that graph I_m has connectivity invariants $d_1(\mathrm{x}), d_2(\mathrm{x}), \ldots, d_t(\mathrm{x})$ which are multivariate functions from K^{s+m} into K such that for two vertices v_1 and v_2 (points or lines) from the same connected component of the graph equalities $d_i(\mathrm{v}_2) = d_i(\mathrm{v}_1)$, $i = 1, 2, \ldots, t$ hold.

We consider symbolic vertex automaton $SV(I_m)$ corresponding to I_m defined in the following way. Its states are divided into points $(f_1, f_2, \ldots, f_{m+1})$ and lines $[g_1, g_2, \ldots, g_{m+1}]$ where $f_i \in K[x_1, x_2, \ldots, x_{1+m}]$ and $g_i \in K[x_1, x_2, \ldots, x_{1+m}]$, $i = 1, 2, \ldots, m+1$. There are two options for an by initial state: symbolic point $(x_1, x_2, \ldots, x_{1+m})$ or symbolic line $[x_1, x_2, \ldots, x_{1+m}]$. The computation of $SV(I_m)$ is given by its symbolic key $\mathrm{h}_j \in K[z_1, z_2, \ldots, z_{1+t}]$, $j = 1, 2, \ldots, k$ and its initial state (point for example) in the following way. One has to form the specialisation of a symbolic key $\tilde{h}_j = h(x_1, d_1(\mathrm{x}), d_2(\mathrm{x}), \ldots, d_t(\mathrm{x})) \in K[x_1, x_2, \ldots x_{1+m}]$ and compute the chain $(x_1, x_2, \ldots, x_{1+m})$,

$$
\begin{aligned}
N_{\tilde{h}_1(x_1,x_2,\ldots,x_{1+m})}(\mathrm{x}) &= \mathrm{v}_1,\\
N_{\tilde{h}_2(x_1,x_2,\ldots,x_{1+m})}(\mathrm{v}_1) &= \mathrm{v}_2,\\
N_{\tilde{h}_3(x_1,x_2,\ldots,x_{1+m})}(\mathrm{v}_2) &= \mathrm{v}_3,\\
&\ldots,\\
N_{\tilde{h}_k(x_1,x_2,\ldots,x_{1+m})}(\mathrm{v}_{k-1}) &= \mathrm{v}_k
\end{aligned}
$$

via symbolic computations. We refer to $F = \mathrm{v}_k$ as a result of symbolic computation with the given symbolic key and refer to a chain (x), v_j, $j = 1, 2, \ldots, k$ as decomposition of v_k into transition function of symbolic automaton $SV(I_m)$. We identify v_k with the corresponding multivariate map from $S(K^{m+1})$.

We refer to the deformation rule $G = \tau_L \mathrm{v}_k \tau_R$ and the chain v_i, $i = 1, 2, \ldots, k$ as decomposition of G of rank k into transition function of symbolic vertex automaton of the graph I_m. We say that G is symbolically decomposed via linguistic graph I_m.

Notice that for $F = (f_1, f_2, \ldots, f_{m+1})$ polynomial f_1 coincides with $h_k(x_1, d_1(\mathrm{x}), d_2(\mathrm{x}), \ldots, d_t(\mathrm{x})$. Let us investigate the equation

$$F(p_1, p_2, \ldots, p_{m+1}) = (b_1, b_2, \ldots, b_{m+1}).$$

Assume that $(b_1, b_2, \ldots, b_{m+1})$ is an element of image of F and p_i are variables. Then $h_k(p_1, d_1(\mathrm{p}), d_2(\mathrm{p}), \ldots, d_t(\mathrm{p})) = b_1$. We can rewrite it as $h_k(p_1, d_1(\mathrm{b}), d_2(\mathrm{b}), \ldots, d_t(\mathrm{b})) = b_1$. Notice that here we use the fact that vertices $(p_1, p_2, \ldots, p_{m+1})$ and $(b_1, b_2, \ldots, b_{m+1})$ (points or lines) are in the same connected component of the graph. Let us assume that for the subset Ω of K the equation $h_k(p_1, d_1(\mathrm{b}), d_2(\mathrm{b}), \ldots, d_t(\mathrm{b})) = b_1$, $p_1 \in \Omega$ has at most one solution. If $\mathrm{b} \in F(\Omega \times K^m)$ then we can find the solution $p_1 = p_1^*$. After that we can compute

$$\begin{aligned}
\beta_{k-1} &= h_{k-1}(p_1^*, d_1(\mathrm{b}), d_2(\mathrm{b}), \ldots, d_t(\mathrm{b})),\\
\beta_{k-2} &= h_{k-2}(p_1^*, d_1(\mathrm{b}), d_2(\mathrm{b}), \ldots, d_t(\mathrm{b})),\\
&\ldots\\
\beta_1 &= h_{k-2}(p_1^*, d_1(\mathrm{b}), d_2(\mathrm{b}), \ldots, d_t(\mathrm{b})).
\end{aligned}$$

It allows us to compute

$$\begin{aligned}
\mathrm{u}_{k-1} &= N_{\beta_{k-1}}(b_1, b_2, \ldots, b_{m+1}),\\
\mathrm{u}_{k-2} &= N_{\beta_{k-2}}(\mathrm{u}_{k-1}),\\
&\ldots\\
\mathrm{u}_1 &= N_{\beta_{k-2}}(\mathrm{u}_2),\\
(p_1^*, p_2^*, \ldots, p_{m+1}^*) &= N_{p_1^*}(\mathrm{u}_1).
\end{aligned}$$

So the restriction of the map F on $\Omega \times K^m$ is injective. The equation $F(\mathrm{x}) = \mathrm{b}$, where $\mathrm{x} \in \Omega \times K^m$, $\mathrm{b} \in F(\Omega \times K^m)$ has a unique solution.

Let $F' = \tau_L F \tau_R$ be the deformation of F and $T = {\tau_L}^{-1}(\Omega \times K^m)$. Then the equation $F'(\mathrm{x}) = \mathrm{b}$ for $\mathrm{x} \in T$ and $\mathrm{b} \in F'(T)$ has a unique solution. We say that the multivariate transformation F' of K^{m+1} is partially invertible on T. Such maps F' together with deformation rule $\tau_L F \tau_R$ and decomposition of F via transition functions of symbolic vertex automaton of linguistic graph can be used in symmetric cryptography. Let us consider two general examples in case $K = Z_l$, $l \geqslant 2$.

Example. Correspondents (Alice and Bob) take a linguistic graph I_m in cases $r = s = 1$ as above. Assume that they know the list of connectivity invariants $d_i(x_1, x_2, \dots, x_{m+1})$, $i = 1, 2, \dots, t$. They choose the type of an initial state. Without loss of generality we can take point $(x_1, x_2, \dots, x_{m+1})$. They set the length of computation of vertex symbolic automaton k and symbolic key

$$h_1(z_1, z_2, \dots, z_{t+1}), h_2(z_1, z_2, \dots, z_{t+1}), \dots h_k(z_1, z_2, \dots, z_{t+1}),$$

where $h_k = ax^r + f(z_2, z_3, \dots, z_{t+1})$, $a \in {Z_l}^*$, $(r, \phi(l)) = 1$. They choose affine transformation τ_L of kind

$$x_1 \to x_1 + x_2 + \dots x_{m+1}, x_j \to l_j(x_1, x_2, \dots, x_{m+1}),$$

where $l_j(x_1, x_2, \dots, x_{m+1})$ are general linear transformation of ${Z_l}^{m+1}$ into Z_l for $j = 2, 3, \dots, m+1$, and general bijective affine transformation τ_R.

We assume that the graph I_m, its connectivity invariants, and the plainspace $T = \{(x_1, x_2, \dots, x_{m+1}) \in {Z_l}^{m+1} | x_1 + x_2 + \dots + x_n \in {Z_l}^*\}$ are known to public. Cryptanalytic knows the general algorithm which depends on some unknown τ_L, τ_R and some symbolic key. Correspondents share the symbolic key $h_i(x_1, x_2, \dots, x_{t+1})$, $i = 1, 2, \dots, k$ and affine transformations τ_L and τ_R as above. Alice writes her plaintext $\mathrm{p} = (p_1, p_2, \dots, p_{m+1})$. She computes the tuple $\tau_L(\mathrm{p}) = (u_1, u_2, \dots, u_{m+1}) = \mathrm{u}$. She computes values of connectivity invariants $\beta_i = d_i(u_1, u_2, \dots, u_{m+1})$, $i = 1, 2, \dots, t$. After that Alice gets the values of symbolic keys

$$\begin{aligned} \gamma_1 &= h_1(u_1, \beta_1, \beta_2, \dots, \beta_t), \\ \gamma_2 &= h_2(u_1, \beta_1, \beta_2, \dots, \beta_t), \\ &\dots, \\ \gamma_k &= h_k(u_1, \beta_1, \beta_2, \dots, \beta_t). \end{aligned}$$

If chosen k is odd she takes the chain (u), $N_{\gamma_1}(\mathrm{u}) = [\mathrm{u}^1]$, $N_{\gamma_2}([\mathrm{u}^1]) = (\mathrm{u}^2)$, $\dots$, $N_{\gamma_k}((\mathrm{u}^{k-1})) = [\mathrm{u}^k]$. She takes $\tau_R(\mathrm{u}^k) = \mathrm{c}$ as ciphertext. Notice that in case of even K Alice gets $N_{\gamma_k}([\mathrm{u}^{k-1}]) = (\mathrm{u}^k)$.

Let us consider the decryption process. For simplicity we take the case when k is odd. Bob takes c. He computes ${\tau_R}^{-1}(\mathrm{c}) = \mathrm{u}^k$. He takes $[\mathrm{u}^k] = [b_1, b_2, \dots, b_n]$. Bob computes parameters β_i as $d_i([b_1, b_2, \dots, b_n])$ for $i = 1, 2, \dots, t$.

Bob looks at expression $ax^r + f(z_2, z_3, \dots, z_{t+1})$ and writes the equation $ax^r + f(\beta_1, \beta_2, \dots, \beta_t) = b_1$. So he computes $x^r =$

$(b_1 - f(\beta_1, \beta_2, \ldots, \beta_t))a^{-1} = \alpha$. So Bob gets u_1 as $\alpha^{r'}$ where r' is a multiplicative inverse in $Z_{\phi(l)}$.

Now, Bob computes $\gamma_i = h_i(u_1, \beta_1, \beta_2, \ldots, \beta_t)$, $i = 1, 2, \ldots, k-1$. So he gets

$$N_{\gamma_{k-1}}([\mathrm{u}^k]) = (\mathrm{u}^{k-1}), \quad N_{\gamma_{k-2}}((\mathrm{u}^{k-1})) = [\mathrm{u}^{k-2}], \ldots,$$
$$N_{\gamma_1}((\mathrm{u}^2)) = [\mathrm{u}^1], \quad N_{u_1}([\mathrm{u}^1]) = (\mathrm{u}).$$

Finally Bob obtains ${\tau_L}^{-1}(\mathrm{u}) = (p_1, p_2, \ldots, p_s)$.

Remark 1. It is easy to see that the scheme above can be easily modified in various ways. For instance, correspondents can use $T = {Z_l}^{*m+1}$ and take τ_L as linear monomial transformation $(x_1, x_2, \ldots, x_{m+1}) \to (\lambda_1 x_1, \lambda_2 x_2, \ldots, \lambda_{m+1} x_{m+1})$, where $(\lambda_1, \lambda_2, \ldots, \lambda_{m+1}) \in {Z_l}^{*m+1}$.

Remark 2. The above scheme can produce rather fast symmetric encryption algorithm in case of various linguistic graphs. It is easy to define linguistic graph I_m such that the neighbour of each vertex can be computed in time $O(m)$. We can take an empty list of connectivity invariants (parameter t is zero). Assume that we work with sparse affine transformation τ_L and τ_R which can be completed in $O(m)$ elementary steps. Then the encryption algorithm above takes $O(m)$ operations.

Towards public key algorithm. Alice can take a linguistic graph I_m in case $r = s = 1$ as above. She knows the list of connectivity invariants $d_i(x_1, x_2, \ldots, x_{m+1})$, $i = 1, 2, \ldots, t$. She chooses the type of initial state. Without loss of generality we can take point $(x_1, x_2, \ldots, x_{m+1})$. Alice chooses the length k of computation of vertex symbolic automaton k and symbolic key

$$h_1(z_1, z_2, \ldots, z_{t+1}), h_2(z_1, z_2, \ldots, z_{t+1}), \ldots, h_k(z_1, z_2, \ldots, z_{t+1}),$$

where $h_k = ax^r + f(z_2, z_3, \ldots, z_{t+1})$, $a \in {Z_l}^*$, $(r, \phi(l)) = 1$. She chooses affine transformation τ_L of kind

$$x_1 \to x_1 + x_2 + \ldots x_{m+1}, x_j \to l_j(x_1, x_2, \ldots, x_{m+1}),$$

where $l_j(x_1, x_2, \ldots, x_{m+1})$ are general linear transformation of ${Z_l}^{m+1}$ into Z_l for $j = 2, 3, \ldots, m+1$, and general bijective affine transformation τ_R.

Alice takes the initial state $\mathrm{x} = (x_1, x_2, \ldots, x_{m+1})$. She computes the tuple $\tau_L(\mathrm{x}) = (v_1, v_2, \ldots, v_{m+1}) = \mathrm{v}$, where v_i are linear expressions in variables $x_1, x_2, \ldots, x_{m+1}$. Notice that $v_1 = x_1 + x_2 + \cdots + x_{m+1}$. After that

Alice takes computation of symbolic vertex automaton with symbolic key $h_i, i = 1, 2, \ldots, k$ starting in a new initial state $(v_1, v_2, \ldots, v_{m+1})$. It means that Alice uses symbolic computations for the constructions of multivariate invariants $d_t(v_1, v_2, \ldots, v_{m+1}) = d'_t(x_1, x_2, \ldots, x_{m+1})$, $i = 1, 2, \ldots, t$.

She computes $\tilde{h_1} = h_1(v_1, d'_2, \ldots, d'_{t+1})$, $\tilde{h_2} = h_2(v_1, d'_2, \ldots, d'_{t+1})$, $\ldots$ $\tilde{h_k} = h_k(v_1, d'_2, \ldots, d'_{t+1})$.

Alice computes the chain of elements from $Z_l[x_1, x_2, \ldots, x_{m+1}]^{m+1}$ (vertices of symbolic automaton, points and lines). The point $\mathrm{v} = (v_1, v_2, \ldots, v_{m+1})$, line $[\mathrm{v}_1] = N_{\tilde{h_1}}(\mathrm{v})$, point $(\mathrm{v}_2) = N_{\tilde{h_2}}([\mathrm{v}_1])$, $\ldots$, $(\mathrm{v}_{k-1}) = N_{\tilde{h_{k-1}}}((\mathrm{v}_{k-2}))$, $[\mathrm{v}_k] = N_{\tilde{h_k}}(\mathrm{v}_{k-1})$. For simplicity we take odd k. Alice treats $F = \mathrm{v}_k$ as multivariate map and computes $G = F\tau_R$ (composition of two maps).

Assume that Alice can complete all steps as above in polynomial time and get a resulting map G of finite degree. Then she can write the standard form of G: $x_1 \to g_1(x_1, x_2, \ldots, x_{m+1})$, $x_2 \to g_2(x_1, x_2, \ldots, x_{m+1})$, $\ldots$, $x_{m+1} \to g_{m+1}(x_1, x_2, \ldots, x_{m+1})$, where g_i, $i = 1, 2, \ldots, m+1$ are given by the lists of their monomial terms with respect to some standard order.

Then Alice can announce the public rules $g_i \in Z_l[x_1, x_2, \ldots, x_{m+1}]$, $i = 1, 2, \ldots, m+1$ to all of her correspondents together with the plainspace $\Omega_{m+1} = \{\mathrm{x} \in {Z_l}^{m+1} | x_1 + x_2 + \cdots + x_m \in {Z_l}^*\}$.

Public user (Bob) writes a message $(p_1, p_2, \ldots, p_{m+1}) \in \Omega_{m+1}$ and computes the ciphertext $(c_1, c_2, \ldots, c_{m+1})$ where $c_i = g_i(p_1, p_2, \ldots, p_{m+1})$, $i = 1, 2, \ldots, m+1$ and sends it to Alice.

Alice knows the deformation rule $G = \tau_L F \tau_R$ and the symbolic key which gives the decomposition of F into transition functions of the symbolic vertex automaton of the graph. So she can use the decryption process of symmetric encryption algorithm above and restore the plaintext $(p_1, p_2, \ldots, p_{m+1})$.

Remark 3. Similarly to symmetric algorithm Alice can change Ω_{m+1} for $T = {Z_l}^{*m+1}$ and take τ_L as linear monomial transformation

$$(x_1, x_2, \ldots, x_{m+1}) \to (\lambda_1 x_1, \lambda_2 x_2, \ldots, \lambda_{m+1} x_{m+1}),$$

where $(\lambda_1, \lambda_2, \ldots, \lambda_{m+1}) \in {Z_l}^{*m+1}$.

Remark 4. One can assume that cryptanalytic knows the family of graphs I_m defined over Z_l, where l is known composite number.

We introduce free symbolic computation of odd case k for the general linguistic graph I_m over commutative ring K in case $r = s = 1$ as the

sequence $\mathrm{x} = (x_1, x_2, \ldots, x_{m+1})$ (initial state), line

$$\begin{aligned} N_{z_1}(\mathrm{x}) &= [\mathrm{u}_1], \quad \mathrm{u}_1 \in K[z_1, x_1, x_2, \ldots, x_{m+1}]^{m+1}, \\ N_{z_2}([\mathrm{u}_1]) &= (\mathrm{u}_2), \quad \mathrm{u}_2 \in K[z_1, z_2, x_1, x_2, \ldots, x_{m+1}]^{m+1}, \\ &\ldots \\ N_{z_k}((\mathrm{u}_{k-1})) &= [\mathrm{u}_k)], \quad \mathrm{u}_k \in K[z_1, z_2, \ldots, z_k, x_1, x_2, \ldots, x_{m+1}]^{m+1}. \end{aligned}$$

3. On some extremal algebraic graphs

Recall that the girth is the length of minimal cycle in the simple graph. Studies of maximal size $ex(C_3, C_4, \ldots, C_{2m}, v)$ of the simple graph on v vertices without cycles of length $3, 4, \ldots, 2m$, i. e. graphs of girth $> 2m$, form an important direction of Extremal Graph Theory.

As it follows from the famous Even Circuit Theorem by P. Erdős' we have inequality

$$ex(C_3, C_4, \ldots, C_{2n}, v) \leqslant cv^{1+1/n},$$

where c is a certain constant. The bound is known to be sharp only for $2n = 4, 6, 8$. The first general lower bounds of kind $ex(v, C_3, C_4, \ldots C_n) = \Omega(v^{1+c/n})$, where c is some constant $< 1/2$ were obtained in the 50th by Erdős' via studies of *families of graphs of a large girth*, i.e. infinite families of simple regular graphs Γ_i of degree k_i and order v_i such that $g(\Gamma_i) \geqslant c\log_{k_i} v_i$, where c is the independent of i constant. Erdős' proved the existence of such a family with arbitrary large but bounded degree $k_i = k$ with $c = 1/4$ by his famous probabilistic method.

One of the first examples of the family of graphs of large girth is the family of algebraic graphs $CD(n, q)$ (see [15] and further references). Graphs $CD(n, q)$ appear as connected components of graphs $D(n, q)$ defined via system of quadratic equations [16].

Graphs $D(n, q)$ and $CD(n, q)$ have been used in symmetric cryptography together with their natural analogs $D(n, K)$ and $CD(n, K)$ over general finite commutative rings K since 1998 (see [17]). The theory of directed graphs and language of dynamical system were very useful for studies of public key and private key algorithms based on graphs $D(n, K)$, $CD(n, K)$ (see [18–25] and further references).

There are several implementations of symmetric algorithms for cases of fields ([26], [27], [30]) and arithmetical rings ([28], [29]). Some comparison of bijective multivariate maps based on $D(n, K)$ and other graphs $A(n, K)$ are considered in [31].

4. Graphs $D(n, K)$ and new algorithms related to them

Let P and L 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 will be called *points* and these of L *lines*.

To distinguish points from lines we use parentheses and brackets. If $x \in V$, then $(x) \in P$ and $[x] \in L$. It will also be advantageous to adopt the notation for co-ordinates of points and lines introduced in [16] 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.

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

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

(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, L, I) we denote as $D(\mathbb{K})$. We speak now of the *incidence graph* of (P, L, I), which has the vertex set $P \cup L$ 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_k, L_k, I_k) as follows. Firstly, P_k and L_k are obtained from P and L, respectively, by simply projecting each vector into its k initial coordinates. The incidence I_k is then defined by imposing the first $k-1$ incidence relations and ignoring all others. The incidence graph corresponding to the structure (P_k, L_k, I_k) is denoted by $D(k, \mathbb{K})$ (see [17]).

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 (1) are defined for $i \geqslant 0$.

Notice, that for $i = 0$, the four conditions (6) 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_n (η) be the equivalence relation:

$$u\eta_n v \Leftrightarrow a(u) = a(v) \quad (u\tau v \Leftrightarrow a(u) = a(v))$$

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

Proposition 1 (see [19] and further references)**.**

(i) *For any $t-1$ ring elements $x_t \in \mathbb{K}$, $2 \leqslant t \leqslant [(k+2)/4]$, there exists a vertex v of $\mathrm{D}(n, \mathbb{K})$ for which $a(v) = (x_2, \dots, x_t) = (x)$.*

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

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

Let C be the equivalence class on τ 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 $D(n, \mathbb{K})$ ($D(\mathbb{K})$) with the vertex set C_n (vertex set C respectively).

The graph $C(t, \mathbb{K})$ in the case of $\mathbb{K} = \mathbb{F}_q$ coincides with $CD(n, q)$ which was introduced in [17].

The following statement was proven in [32].

Theorem 1. *Let $\mathbb{K}$ be commutative ring with unity of characteristic d, $d \neq 2$. Then graphs $C(t, \mathbb{K})$, $t \geqslant 6$ and $C(\mathbb{K})$ are connected.*

If $\mathbb{K} = \mathbb{F}_q$, q is odd, then 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.

5. The cryptosystem

We can rewrite result of [33] in the following form.

Proposition 2. *Let F_n be a regular computation of free symbolic automaton of linguistic graph $D(n, Z_l)$ and $\alpha_1, \alpha_2, \ldots, \alpha_k$, where k is even, are fixed elements of Z_l. Then the map $\tilde{F}_n$ corresponding to a specialisation of $z_2 = y+\alpha_1$, $z_3 = z_1+\alpha_1$, $z_4 = y+\alpha_3$, $z_5 = z_1+\alpha_5$, $\ldots$, $z_{k-1} = z_1+\alpha_{k-1}$, $z_k = y + \alpha_k$ is cubical multivariate map from $K[z_1, y, x_1, x_2, \ldots, x_n]^{m+1}$.*

Remark 5. Similar proposition is true for odd k. The map $\tilde{F}_n$ corresponding to a specialisation of $z_2 = y + \alpha_1$, $z_3 = z_1 + \alpha_1$, $z_4 = y + \alpha_3$, $z_5 = z_1 + \alpha_5$, $\ldots$, $z_{k-1} = y + \alpha_{k-1}$, $z_k = z_1 + \alpha_k$ is cubical transformation of ${Z_l}^n$.

Proposition 3. *Let F_n be a regular computation of an odd length s of a symbolic vertex automaton of $D(n.K)$ corresponding to symbolic key $h(z_1, z_2, \ldots, z_t)+\alpha_1$, $z_1+\alpha_2$, $h(z_1, z_2, \ldots, z_t)+\alpha_3$, $z_1+\alpha_4$. $\ldots$, $z_1+\alpha_{s-1}$, $h(z_1, z_2, \ldots, z_t) + \alpha_s$, where $h \in K[z_1, z_2, \ldots, z_t]$ has finite degree and α_i, $i = 1, 2, \ldots, s$ are constants from K. Then the degree of F_n is bounded by $3 \deg h(x_{01}, a_2(\mathrm{x}), a_3(\mathrm{x}), \ldots, a_t(\mathrm{x}))$.*

We say that the map F_n of ${Z_l}^n$ to itself is Eulerian partially invertible map on the domain $\Omega_n = \{\mathrm{x} | \lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_n x_n + \alpha_{n+1} \in {Z_l}^*\}$ if it is partially invertible on Ω_n and solution of equation $F_n(\mathrm{x}) = \mathrm{b}$, $\mathrm{x} \in \Omega$ and $\mathrm{b} \in F_n(\Omega_n)$ can be reduced to a solution of $z^r = a$, $z \in {Z_l}^*$, $r \neq 1$, $(r, \phi(l)) = 1$.

Theorem 2. *Let $K = Z_l$, n be a natural number $\geqslant 2$, s is an odd number $\geqslant 3$. For each domain of kind $\Omega_n = \{\mathrm{x} | \lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_n x_n + \lambda_{n+1} \in {Z_l}^*\}$ in ${Z_l}^n$, where $\lambda_i \neq 0$, $i = 1, 2, \ldots, n$ there is Eulerian map F_n of finite degree which has a symbolic decomposition of rank s. If l is a prime number, then Eulerian map F_n is a bijection.*

Proof. Let us consider a symbolic vertex automaton constructed for the family of graphs $D(n, Z_l)$. Let $a_2(\mathrm{x})$, $a_3(\mathrm{x})$, $\ldots$, $a_t(\mathrm{x})$, $t = [(n + 2)/4]$ be the list of quadratic connectivity invariants of the graph. We shall use polynomials from $Z_l[u_1, u_2, \ldots, u_t]$ to form special symbolic key. For $f \in Z_l[u_1, u_2, \ldots, u_t]$ we define $\tilde{f}$ as $f(z_1, a_2(\mathrm{z}), a_3(\mathrm{z}), \ldots, a_t(\mathrm{z}))$, where $(\mathrm{z}) = (z_1, z_2, \ldots, z_n)$ is initial point of the symbolic vertex automaton of graph $D(n, Z_l)$. We avoid double indexes for points and lines here. We have a free choice to take $H \in Z_l[u_1, u_2, \ldots, u_t]$ to form a sequence of

weights $\alpha_1(\mathrm{z}) = \tilde{H} + \beta_1$, $\alpha_2(\mathrm{z}) = z_1 + \beta_2$, $\alpha_3(\mathrm{z}) = \tilde{H} + \beta_3$, $\alpha_4(\mathrm{z}) = z_1 + \beta_4$, $\ldots$, $\alpha_{s-1}(\mathrm{z}) = z_1 + \beta_{s-1}$, $\alpha_s(\mathrm{z}) = \tilde{H} + \beta_s$, where β_i, $i = 1, 2, \ldots, s$ are fixed elements of Z_l. Let $F = F_n : {Z_l}^n \to {Z_l}^n$ be the multivariate map generated by symbolic computation above. We assume that $H(u_1, u_2, \ldots, u_t)$ is written in the form ${u_1}^r + S(u_2, u_3, \ldots, u_t)$, where S is arbitrary element of $Z_l[u_2, u_3, \ldots, u_t]$ and $r, r \neq 1$ is a parameter such that $(r, \phi(m)) = 1$. Symbol ϕ standardly stands for Euler function. Let us consider non-singular linear transformation $\tau_L : {Z_l}^n \to {Z_l}^n$ of kind

$$\begin{aligned} z_1 &\to \lambda_1 z_1 + \lambda_2 z_2 + \cdots + \lambda_n z_n + \lambda_{n+1}, \\ z_2 &\to l_2(z_1, z_2, \ldots, z_n), \\ z_3 &\to l_3(z_1, z_2, \ldots, z_n), \\ &\cdots \\ z_n &\to l_n(z_1, z_2, \ldots, z_n), \end{aligned}$$

where l_i are linear expressions from $Z_l[z_1, z_2, \ldots, z_n]$ of general kind. We form a composition $G_n = \tau_L F_n$.

Assume that $\mathrm{z} = (z_1, z_2, \ldots, z_n)$ is an element of Ω_n. Let us identify $\tau_L(\mathrm{z}) = (y_1, y_2, \ldots, y_n)$ with the point of the graph $D(n, Z_l)$. Notice that $y_1 \in {Z_l}^*$. Let us show that the reimage of $G_n(\mathrm{z})$ is uniquely determined. We write the equation $G_n(\mathrm{z}) = (b_1, b_2, \ldots, b_n)$. It is clear that $b_1 = {y_1}^r + S(u_2, u_3, \ldots, u_t) + \beta_s$. Notice that tuples y (point) and b (line) are located in the same connected component of the graph. So we have $a_i(\mathrm{y}) = a_i(\mathrm{b}) = \gamma_i$, $i = 2, 3, \ldots, t$. Thus ${y_1}^r + S(\gamma_2, \gamma_3, \ldots, \gamma_t) + \beta_s = b_1$.

Ler r' be the multiplicative inverse of r in $Z_{\phi(l)}$. We have $y_1 = (b_1 - S(\gamma_2, \gamma_3, \ldots, \gamma_t) - \beta_s)^{r'} = \alpha$.

The knowledge of parameter α allows us to compute all coordinates of tuple y. Really, we can compute values $\alpha_{s-1} = \alpha + \beta_{s-1}$, $\alpha_{s-2} = H(\alpha, \gamma_2, \gamma_3, \ldots, \gamma_t) + \beta_{s-2}, \alpha_{s-3} = \alpha + \beta_{s-3}, \ldots, \alpha_1 = H(\alpha, \gamma_2, \gamma_3, \ldots, \gamma_t) + \beta_1$, $\alpha_0 = \alpha$.

The value of y can be computed recursively $y^{s-1} = N_{\alpha_{s-1}}([\mathrm{b}])$, $y^{s-2} = N_{\alpha_{s-2}}((y^{s-1}))$, $\ldots$ $y^1 = N_{\alpha_1}((y^2))$, $y^0 = N_\alpha((y^1)) = (y_1, y_2, \ldots, y_n)$. The tuple z equals ${\tau_l}^{-1}(y^0)$.

The Proposition 3 establishes that the degree of G_n or F_n is bounded by $3\deg(\tilde{H}(\mathrm{z}))$. If $d = \deg(\tilde{S}) > r$ then the degree of G_n is bounded by $3d$. Notice, that in case of prime l the equation ${y_1}^r + S(\gamma_2, \gamma_3, \ldots, \gamma_t) + \beta_s = b_1$, $r \neq 0 \bmod p-1$ is always solvable for y_1. So maps F_n and G_n are bijections. □

Remark 6. In the theorem above we can change domain Ω_n for ${Z_l}^{*n}$.

Really we have to change a transformation τ_L in the proof for a linear monomial map $(x_1, x_2, \ldots, x_n) \to (\lambda_1 x_{\pi(1)}, \lambda_2 x_{\pi(2)}, \ldots, \lambda_n x_{\pi(n)})$, where λ_i, $i = 1, 2, \ldots, n$ are elements of $Z_l{}^*$ and π is a permutation from S_n.

The cryptosystem. Assume that Alice is the holder of a public key based on the family of maps used in the constructive proof of the previous theorem. So she takes l, $l \geqslant 2$ and parameter r, such that $(r, \phi(l)) = 1$. She chooses the odd length s, $s \geqslant 3$ of symbolic key for practical use we set size $O(n)$ for value of s. For example, Alice chooses the area $\Omega_n = \{\mathrm{x}|\mathrm{x}_1 + \mathrm{x}_2 + \cdots + \mathrm{x}_\mathrm{n} \in \mathrm{Z}_\mathrm{l}{}^*\}$ which will be a domain for Eulerian map of $G = Z_l{}^n$. Alice has a rather wide choice to pick the function $S \in Z_l[u_2, u_3, \ldots, u_t]$, $t = [(n+2)/4]$ and parameters $\beta_1, \beta_2, \ldots, \beta_s$ to form the symbolic key. She has set $l_1 = x_1 + x_2 + \ldots, x_n$ and may choose various linear functions $l_i \in Z_l[x_1, x_3, \ldots, x_n]$, $i = 2, 3, \ldots, n$ to form bijective affine map τ_l of $Z_l{}^n$ to itself. Finally, she has a free choice for another affine map τ_R.

So in polynomial time Alice generates map F_n via computation of symbolic vertex automaton of linguistic graph $D(n, Z_l)$ with the symbolic key: $\alpha_1(\mathrm{z}) = \tilde{H} + \beta_1$, $\alpha_2(\mathrm{z}) = z_1 + \beta_2$, $\alpha_3(\mathrm{z}) = \tilde{H} + \beta_3$, $\alpha_4(\mathrm{z}) = z_1 + \beta_4$, $\ldots$, $\alpha_{s-1}(\mathrm{z}) = z_1 + \beta_{s-1}$, $\alpha_s(\mathrm{z}) = \tilde{H} + \beta_s$, where β_i, $i = 1, 2, \ldots, s$ are fixed elements of Z_l. She computes the deformation $G_n = \tau_L F_n \tau_R$ in standard form $x_1 \to g_1(x_1, x_2, \ldots, x_n)$, $x_2 \to g_2(x_1, x_2, \ldots, x_n)$, $\ldots$, $x_n \to g_n(x_1, x_2, \ldots, x_n)$, where g_i, $i = 1, 2, \ldots, n$ are given by list of their monomial terms in some chosen order. Notice, that the degree of G_n is bounded by constant.

Alice announces the public the standard form of G_n and keeps data described above in secret. Cryptanalytic knows used graph and general form of a symbolic key.

Assume that a public user (Bob) creates an open text $\mathrm{p} = (p_1, p_2, \ldots, p_n)$. He computes $G_n((p_1, p_2, \ldots, p_n)) = (c_1, c_2, \ldots, c_n)$. Bounded degree of G_n insures that the computation of ciphertext can be computed in a polynomial time $O(n^c)$ for some positive constant c.

The knowledge of deformation rule $G_n = \tau_L F_n \tau_R$ and the docomposition of F_n into transition functions of symbolic vertex automaton of $D(n, Z_l)$ allows her to decrypt in polynomial time with the algorithm described in a previous section.

Remark 7. Alice can use $Z_l{}^{*n}$ instead of $\Omega_n = \{\mathrm{x}|\mathrm{x}_1 + \mathrm{x}_2 + \cdots + \mathrm{x}_\mathrm{n} \in \mathrm{Z}_\mathrm{l}{}^*\}$. In this case τ_L has to be chosen as monomial transformation.

Remark 8. In case of prime l we can change function $H + b_s$ for much more sophisticated expression. For instance $Z(x_2, x_3, \ldots, x_t) f(x_1) +$

$S(x_2, x_3, \ldots, x_t)$ where $Z(x_2, x_3, \ldots, x_t) = 0$ has no solution but $f(x_1) = d$ has exactly one solution in variable x_1 for each d.

Let $h(x) \in Z_p[x]$ has no linear divisors. Then $Z(x_2, x_3, \ldots, x_t) = h(M(x_2, x_3, \ldots, x_t)))$ is always different from zero for each $M \in K[x_2, x_3, \ldots, x_t]$.

The simplest case where we can use $M(x_2, x_3, \ldots, x_t)({x_1}^r) + S(x_2, x_3, \ldots, x_t)$, where $(r, p-1) = 1$ and the equation $M(x_2, x_3, \ldots, x_t) = 0$ has no solution. We say that such a cryptosystem is based on *hidden discrete logarithm problem*. For general parameter l we use the term hidden Eulerian equation. We can use recurrent expressions

$$M_k(\ldots(M_2(M_1(x_2, x_3, \ldots, x_t)({x_1}^{r_1}) + S_1(x_2, x_3, \ldots, x_t))^{r_2} + S_2(x_2, x_3, \ldots, x_t)) + \ldots M_{k-1}(x_2, x_3, \ldots, x_t)({x_1}^{r_{k-1}}) + S_{k-1}(x_2, x_3, \ldots, x_t))^{r_k} + S_k(x_2, x_3, \ldots, x_t)),$$

where $M_i(x_2, x_3, \ldots, x_t) = 0$ have no solutions for each $i = 1, 2, \ldots, k$.

References

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

[2] V. A. Ustimenko, *Explicit constructions of extremal graphs and new multivariate cryptosystems*, Studia Scientiarum Mathematicarum Hungarica, Special issue "Proceedings of The Central European Conference, 2014, Budapest",volume 52, issue, June 2015, pp. 185-204.

[3] V. A. Ustimenko, *Graphs with Special Arcs and Cryptography*, Acta Applicandae Mathematicae, vol. 71, N2, November 2002, 117-153.

[4] V. Ustimenko, *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, V. 3, 2007, P. 181–200.

[5] V. A. Ustimenko, *On the flag geometry of simple group of Lie type and Multivariate Cryptography*, Algebra and Discrete Mathematics. V. 19. No 1. 2015. P. 130-144.

[6] V. Ustimenko, *On walks of variable length in Schubert incidence systems and multivariate flow ciphers*, Dopovidi of Nathional Acad. Sci. of Ukraine, 2014, No 3, P. 55 - 150.

[7] N. Koblitz, Algebraic aspects of cryptography, Springer (1998).

[8] V. Ustimenko, *On Multivariate Cryptosystems Based on Computable Maps with Invertible Decompositions*, Annales of UMCS, Informatica, volume 14 (2014) , Special issue "Proceedings of International Conference Cryptography and Security Systems", pp. 7-18.

[9] J. Patarin, *The Oil and Vinegar digital signatures*, Dagstuhl Workshop on Cryptography. 1997.

[10] Kipnis A., Shamir A., *Cryptanalisis of the Oil and Vinegar Signature Scheme*, Advances in Cryptology - Crypto 96, Lecture Notes in Computer Science, V. 1462, 1996, P. 257–266.

[11] S. Bulygin, A. Petzoldt, and J. Buchmann, *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", Guang Gong and Kishan Chand Gupta, editors, Lecture notes in Computer Science, V. 6498, 2010. P. 17–32.

[12] U. Romanczuk-Polubiec, V. Ustimenko, *On two windows multivariate cryptosystem depending on random parameters*, Algebra and Discrete Mathematics, 2015, V. 19. No. 1. P. 101–129.

[13] F. Harary, *Graph Theory*, Addison-Wesley Publishing Co, Reading, MA (1966).

[14] V. Ustimenko, *Maximality of affine group, hidden graph cryptosystem and graph's stream ciphers*, Journal of Algebra and Discrete Mathematics, 2005, v.1, pp 51-65.

[15] F.Lazebnik , V. Ustimenko and A.J.Woldar, *A new series of dense graphs of high girth*, Bulletin of the AMS 32 (1) (1995), 73-79.

[16] F. Lazebnik, V. Ustimenko, *Explicit construction of graphs with arbitrary large girth and of large size*, Discrete Applied Mathematics 60 (1995), 275-284.

[17] V. Ustimenko, *Coordinatisation of Trees and their Quotients*, in the Voronoj's Impact on Modern Science, Kiev, Institute of Mathematics, 1998, vol. 2, 125-152.

[18] V. Ustimenko, *CRYPTIM: Graphs as Tools for Symmetric Encryption*, Lecture Notes in Computer Science, Springer, LNCS 2227, Proceedings of AAECC-14 Symposium on Applied Algebra, Algebraic Algorithms and Error Correction Codes, November 2001, p. 278-286.

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

[20] V. Ustimenko, *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).

[21] V. Ustimenko, U. Romanczuk, *On Extremal Graph Theory, Explicit Algebraic Constructions of Extremal Graphs and Corresponding Turing Encryption Machines*, in "Artificial Intelligence, Evolutionary Computing and Metaheuristics ", In the footsteps of Alan Turing Series: Studies in Computational Intelligence, Vol. 427, Springer, January, 2013, 257-285.

[22] V. Ustimenko, U. Romanczuk, *On Dynamical Systems of Large Girth or Cycle Indicator and their applications to Multivariate Cryptography*, in "Artificial Intelligence, Evolutionary Computing and Metaheuristics ", In the footsteps of Alan Turing Series: Studies in Computational Intelligence, Volume 427/2012, 257-285.

[23] V. Ustimenko, *On the cryptographical properties of extreme algebraic graphs*, in "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 2009, 296 pp.

[24] U. Romanczuk-Polubiec, V. Ustimenko, *On Multivariate Cryptosystems Based on Polynomially Compressed Maps with Invertible Decompositions*, Cryptography and Security Systems, Third International Conference, CSS 2014, Lublin,

Poland, September 22-24, 2014. Proceedings, Communications in Computer and Information Science, 448, p. 23-37.

[25] M. Klisowski, V. Ustimenko, *Graph based cubical multivariate maps and their cryptographical applications*, in "Advances on Superelliptic curves and their Applicationsions", IOS Press, NATO Science for Peace and Security series –D: Information and Communication Security, 2015, v. 41, 201, pp. 305-327.

[26] A. Tousene, V. Ustimenko, *CRYPTALL - a System to Encrypt All types of Data*, Notices of Kiev-Mohyla Academy, v. 23, 2004, pp. 12-15.

[27] A. Touzene, V. Ustimenko, *Graph Based Private Key Crypto System*, International Journal on Computer Research, Nova Science Publisher, v. 13 (2006), issue 4, 12pp.

[28] J. Kotorowicz, V. Ustimenko, *On the implementation of cryptoalgorithms based on algebraic graphs over some commutative rings*, Condenced Matters Physics, Special Issue: Proceedings of the international conferences "Infinite particle systems, Complex systems theory and its application", Kazimerz Dolny, Poland, 2006, 11 (no. 2(54)) (2008) 347–360.

[29] V. Ustimenko, S. Kotorowicz, *On the properties of Stream Ciphers Based on Extremal Directed graphs*, In "Cryptography Research Perspectives", Nova Publishers, Ronald E. Chen (the editor), 2008.

[30] , A. Touzene, V. Ustimenko, Marwa AlRaisi, Imene Boudelioua, *Performance of Algebraic Graphs Based Stream-Ciphers Using Large Finite Fields*, Annalles UMCS Informatica AI X1, 2 (2011), 81-93.

[31] V. A. Ustimenko, M. Klisowski, *On the Comparison of Cryptographical Properties of Two Different Families of Graphs with Large Cycle Indicator*, Mathematics in Computer Science, 2012, V. 6, Number 2, pp. 181-198.

[32] V. A. Ustimenko, *Algebraic groups and small world graphs of high girth*, Albanian J. Math, vol3, N1 (2009), 25-33.

[33] V. A. Ustimenko, A. Wroblevska, *On the key exchange with nonlinear polynomial map of stable degree*, arXiv:1304, 2920, v.1.

Contact information

V. Ustimenko University of Maria Curie Skłodowska in Lublin
E-Mail(*s*): vasyl@hektor.umcs.lublin.pl

Received by the editors: 30.09.2015
and in final form 30.09.2015.