DOI: 10.15439/2014F269
ACSIS, Vol. 2

On multivariate cryptosystems based on maps with logarithmically invertible decomposition corresponding to walk on graph

Vasyl Ustimenko
Maria Curie-Skłodowska University,
Institute of Mathematics,
pl. M. Curie-Skłodowskiej 1, 20-031 Lublin, Poland
Email: vasyl@hektor.umcs.lublin.pl

***Abstract*—The paper illustrates the concept of the map with logarithmically invertible decomposition. We introduce families of multivariate cryptosystems such that there security level is connected with discrete logarithm problem in Cremona group. The private key of such cryptosystem is a modification of graph based stream ciphers which use stable multivariate maps. Modified version corresponds to a stable map with single disturbance. If the disturbance (or initial condition) allows fast computation then modified version is almost as robust as original one. Methods of modification improve the resistance of such stream ciphers implemented on numerical level to straightforward linearisation attacks.**

I. Introduction

THE FORMAL concepts of multivariate map with logarithmically invertible decomposition is introduced by the author in Extended Abstracts Of Central European Conference on Cryptology, 2014. In this paper the examples of a cryptosystem based on this idea will be presented. The complexity estimates of an encryption and a decryption procedures are given. The construction uses walks on graphs $D(n, K)$ or $A(n, K)$ for purpose of Multivariate Cryptography. Such walks firstly used for the constructions of fast stream ciphers. The multivariate maps induced by such walks turn out to be fast cubical transformations of the plainspace (variety of vertices or variety of flags (see [1], [2]). It makes them useful for a design of stream ciphers and key exchange protocols. It was shown [3], [4] that the inverses of encryption maps are also cubical transformations. This fact restricts their use in public key cryptography. In [5] more general idea of multivariate map corresponding to *symbolic walk* on the graph has been introduced. Paper [6] suggests the deformation of such nonlinear map by two affine transformations and the use of deformated transformation in Multivariate Cryptography, but important questions of estimation of degrees, orders, densities are still under investigation.

Currently symbolic walks are used for the development of stream ciphers with high resistance to plaintext - ciphertext attacks of the adversary.

Current paper contains description of algorithms which allows a repetition of chosen walks on the graph $D(n, K)$ and $A(n, K)$. This rout makes the bridges towards discrete logarithm problem for cyclic subgroups of Cremona group.

Preliminaries on Multivariate Cryptography are collected in the section 2 which contains definitions of special multivariate maps. Section 3 is devoted to information on problems of Extremal Graph Theory which leads to discovery of graphs $D(n, F_q)$ and $A(n, q)$. The descriptions of graphs $D(n, K)$ and their connected components together with cryptographical applications are given in section 4. The graph based explicit construction of requested multivariate transformations is given in section 5. It comes together with the decryption of multivariate public key based on graphs $D(n, K)$.

The last section is the conclusion.

II. On multivariate cryptography and special multivariate transformations

Multivariate cryptography (see [7]) 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.

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 maps $f(n)$ from $C(K^n)$, $n = 1, 2, \ldots$ as *the family of bounded degree*, if the degree of each transformation is bounded by the finite parameter s.

Assume that a transformation $f = f(n)$ is written in the form: $x_i \to f_i(x_1, x_2, \ldots, x_n)$, $i = 1, 2, \ldots, n$, where each $f_i \in K^n$ is determined by the list of their monomial terms with respect to some chosen order.

A family of elements $f(n) \in C(K^n)$, $n > 1$ is called stable if each nonidentity multiple iteration of $f(n)$ with itself has the same degree with $f(n)$. Let $|g|$ be the order of $g \in C(K^n)$.

978-83-60810-58-3/$25.00 © 2014, IEEE

We say, that $f(n)$ is a family of increasing order if $|f(n)|$ for n.

Let us consider the discrete logarithm problem for a stable family f^n of increasing order. We have to solve the equation $f(n)^y = b(n)$ with respect to an integer unknown y. Notice, that $\deg(f(n)) = \deg(b(n))$. It means, that studies of degrees $(f(n))^k$, $k = 1, 2, \ldots$ do not bring us any new information for the task execution. If the order of an element $f(n)$ is growing fast with the growth of n, then discrete logarithm problem can be NP - hard.

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 $f^1(n), f^2(n), \ldots, f^{k(n)}(n)$ and this decomposition will allow us to compute the value of $y = f(x)$ and the re-image of given y in time $k(n)O(n^d)$ (see the authors extended abstract for Central European Conference on Cryptology 2014).

In the case $d = 1$ we say that invertible decomposition is of linear speed. The complexity of computation of the value of each $f^i(n)$ in a given point x is $O(n^d)$. We refer to the family of multivariate maps $h_{n+1} : K^{n+1} \to K^{n+1}$ as a family with logarithmically invertible decomposition of speed t with the initial function $f(x_1, x_2, \ldots, x_n)$ if there exists decomposition $h_{n+1} = h_{n+1,1}h_{n+1,2}\ldots h_{n+1,k(n)}$ such that the knowledge about it allows us to solve the equation $h_{n+1}{}^{\alpha}(x_1, x_2, \ldots, x_n, f(x_1, x_2, \ldots, x_n)) = (b_1, b_2, \ldots, b_{n+1})$ for unknowns $\alpha, x_1, x_2, \ldots, x_n$ in time $k(n)O(n^t)$.

We say that function $u : Z^+ \to Z^+$ is computationally equivalent to n^s, $s \geq 0$ and write $u(n^s$ if $C_1 n^s \leq u(n) \leq C_2 n^s$ for some positive constants C_1 and C_2.

Examples of stable families $f(n) \in C(K^n)$ of bounded degree and increasing order defined in terms of algebraic graph theory are given in [4], [8], [9], [11]. An example of stable transformations of linear degree and increasing order is proposed in [12] (see also survey [10], [13] and 14] for extra examples).

III. Extremal algebraic graphs corresponding to special families of multivariate maps and their usage in symmetric cryptography

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 (see [15]).

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

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

where c is a certain constant. The bound is known to be sharp only for $n = 4, 6, 10$. 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 large girth*, i.e. infinite families of simple regular graphs Γ_i of degree k_i and order v_i such that $g(\Gamma_i) \geq c\log_{k_i} v_i$, 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.

First two explicit families of regular simple graphs of large girth with unbounded girth and arbitrarily large k appeared in 90th: the family $X(p, q)$ of Cayley graphs for $PSL_2(p)$, where p and q are primes, which has been defined by G. Margulis [10] and investigated by A. Lubotzky, Sarnak and Phillips [17] and the family of algebraic graphs $CD(n, q)$ [18]. Graphs $CD(n, q)$ appear as connected components of graphs $D(n, q)$ defined via a system of quadratic equations [19]. The best known lower bound for $d \neq 2, 3, 5$ has been deduced from the existence of above mentioned families of graphs $ex(v, C_3, C_4, \ldots, C_{2d}) \geq cv^{1+2/(3d-3+e)}$ where $e = 0$ if d is odd, and $e = 1$ if d is even.

Recall, that family of regular graphs Γ_i of degree k_i and increasing order v_i is a *family of graphs of small world* if $\mathrm{diam}(\Gamma_i) \leq c\log_{\mathrm{k_i}}(v_i)$ for some independent constant c, $c > 0$, where $\mathrm{diam}(\Gamma_i)$ is a diameter of graph G_i. The graphs $X(p.q)$ form a unique known family of large girth which is a family of small world graphs at the same time. There is a conjecture known since 1995 that family of graphs $CD(n, q)$ for odd q is an other example of such kind. Currently, it is proved that the diameter of $CD(n, q)$ is bounded from above by polynomial function $d(n)$, which does not dependent from q. Expanding properties of $X(p, q)$ and $D(n, q)$ can be used in Coding Theory (magnifiers, superconcentrators, etc). The absence of short cycles and high girth property of both families can be used for the construction of LDPC codes [20]. This class of error correcting codes is an important tool of security for satellite communications. The usage of $CD(n, q)$ as Tanner graphs producing LDPC codes leads to better properties of corresponding codes in the comparison to the usage of Cayley - Ramanujan graphs (see [21]).

Both families $X(p, q)$ and $CD(n, q)$ consist of edge transitive graphs. Their expansion properties and the property to be graphs of large girth also hold for random graphs, which have no automorphisms at all. To make better deterministic approximation of random graph we can look at regular expanding graphs of large girth without edge transitive automorphism group.

Below We consider an optimization problem for simple graphs which is similar to the problem of finding maximal size for graph on v vertices with the girth $\geq d$.

Let us refer to the minimal length of a cycle, through the vertex of the given vertex of the simple graph Γ as a *cycle indicator of the vertex*. The *cycle indicator of the graph* $\mathrm{Cind}(\Gamma)$ will be defined as a maximal cycle indicator of its vertices. Regular graph will be called a *cycle irregular graph* if its indicator differs from the girth (the length of minimal cycle). The solution of the optimization problem of computation of maximal size $e = e(v, d)$ of the graph of an order v with the size greater than d, $d > 2$ has been found very recently.

It turns out that

$$e(v,d) \Leftrightarrow O(v^{1+[2/d]})$$

and this bound is always sharp (see [22] or [23] and further references).

We refer to the family of regular simple graphs Γ_i of degree k_i and order v_i as a *family of graphs of large cycle indicator*, if

$$\mathrm{Cind}(\Gamma_i) \geq c\log_{\mathrm{k_i}}(v_i)$$

for some independent constant c, $c > 0$. We refer to the maximal value of c satisfying the above inequality as *speed of growth* of the cycle indicator for a family of graphs Γ_i. As it follows from the written above evaluation of $e(v,d)$ the speed of growth of the cycle indicator for the family of graphs of constant but arbitrarily large degree is bounded above by 2.

We refer to such a family as a *family of cyclically irregular graphs of large cycle indicator* if almost all graphs from the family are cycle irregular graphs.

The following theorem was proved in [23]:

There is a family of almost Ramanujan cyclically irregular graphs of large cycle indicator with the speed of cycle indicator 2, which is a family of graphs of small word graphs.

The explicit construction of the family $A(n,q)$ like in previous statement is given in [22], [23]. Notice, that members of the family of cyclically irregular graphs are not edge transitive graphs. The LDPC codes related to new families are presented in [24], computer simulations demonstrate essential advantages of new codes in comparison to those related to $CD(n,q)$ and $D(n,q)$.

A. On the stream ciphers corresponding to special families of multivariate maps

Graphs $D(n,q)$, $A(n,q)$ and $CD(n,q)$ have been used in symmetric cryptography together with their natural analogs $D(n,K)$, $A(n,K)$ and $CD(n,K)$ over general finite commutative rings K since 1998 (see [1]). The theory of directed graphs and language of dynamical system have been very useful for studies of public key and private key algorithms based on graphs $D(n,K)$, $CD(n,K)$ and $A(n,K)$ (see [10], [25], and further references).

There are several implementations of symmetric algorithms for cases of fields (starting from [7]) and arithmetical rings ([19], in particular). Some comparison of public keys based on $D(n,K)$ and $A(n,K)$ are considered in [21].

The general scheme is the following one. We can use a family of elements $f(n)$ with invertible decomposition of speed d of increasing order for purposes of symmetric cryptography. We assume that the variety K^n is a plainspace of the encryption algorithm, the list of $(f(n,i)$, $i=1,2,\dots,k(n)$, is a password. Then the computation of the value c of encryption function $f(n,1)f(n,2)\dots f(n,k(n))$ in the given plaintext $\mathrm{p} \in K^n$ and the reimage of the ciphertext c require time $O(n^d)$. Usually the parameter $k(n)$ can be chosen free. In fact, in practical cases $k(n)$ is either constant or linear function in variable n (see surveys [20]. [23], [25] on the use graph based multivariate functions as symmetric encryption functions). To hide the graph nature of $f(n)$ correspondents (Alice and Bob) can create a new encryption map $h(n)$ as a conjugation of $f(n)$ with special invertible affine transformation $\tau = \tau(n)$ (degree equals 1) of K^n. In case of private keys both correspondents know the invertible decompositions and family $\tau(n)$ of affine transformation as part of the key.

IV. On the explicit constructions

A. Description of graphs $A(n,K)$

The graph $A(n,K)$, where K is a finite commutative ring, is defined by the following way. This is a bipartite graph with the point set $P = \{x_1,x_2,\dots,x_n)|x_i \in K\} = K^n$ and the line set $L = \{[y_1,y_2,\dots,y_n]|y_i \in K|\} = K^n$ and such that a point $\mathrm{x} = (x_1,x_2,\dots,x_n)$ is incident to a line $\mathrm{y} = [y_1,y_2,\dots,y_n]$ if and only if equations $x_i - y_i = y_1x_1$ hold for even i and relations $x_j - y_j = x_1y_j$ hold for an odd j, $j \geq 3$. We identify such an incidence relation with the corresponding bipartite graph $I = A(n,K)$. We refer to the first coordinate $x_1 = \rho(\mathrm{x})$ of a point x and the first coordinate $y_1 = \rho(\mathrm{y})$ of a line y of the line as the colour of the vertex (point or line). The following property holds for the graph: there exists a unique neighbour $N_t(v)$ of a given vertex v of a given colour $t \in K$.

As it follows from the definition the projective limit of $A(n,K)$, $n \to \infty$ is well defined. The points $\mathrm{p} = (p_1,p_2,\dots,p_n,\dots)$ and lines $\mathrm{l} = [l_1,l_2,\dots,l_n,\dots]$ are tuples with finite number of nonzero coordinates. A point and a line are incident when infinite number of equations $p_2 - y_l = l_1p_1, p_3 - l_3 = p_1l_2,\dots$ hold.

B. Description of graphs $D(n.K)$ and their connected components

We define the family of graphs $D(k,K)$, where $k > 2$ is positive integer and K is a commutative ring, such graphs have been considered in [15] for the case $K = F_q$.

Let P_D and L_D be two copies of Cartesian power K^N, where K is the commutative ring and 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 K:

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

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

Now, we introduce 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:

$$\begin{aligned} l_{i,i} - p_{i,i} &= l_{1,0}p_{i-1,i} \\ l'_{i,i} - p'_{i,i} &= l_{i,i-1}p_{0,1} \\ l_{i,i+1} - p_{i,i+1} &= l_{i,i}p_{0,1} \\ l_{i+1,i} - p_{i+1,i} &= l_{1,0}p'_{i,i} \end{aligned} \tag{6}$$

(These four relations are defined for $i \geq 1$, $p'_{1,1} = p_{1,1}$, $l'_{1,1} = l_{1,1}$). The incidence structure (P_D, L_D, I_D) we denote as $D(K)$. 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 $k \geq 2$ we obtain a symplectic quotient $(P_{D,k}, L_{D,k}, I_{D,k})$ as follows. Firstly, $P_{D,k}$ 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 $D(k, K)$.

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 $i \geq 0$.

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 $k \geq 6$, $t = [(k+2)/4]$, 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 D(k, K) ($\alpha \in \{(1,0),(0,1)\}$, it does not matter whether u is a point or a line). For every r, $2 \leq r \leq t$, 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 that $a = a(u) = (a_2, a_3, \cdots, a_t, \dots)$ for the vertex u of infinite graph $D(K)$.

Proposition 4.1: Let u and v be vertices from the same component of $D(k, K)$. Then $a(u) = a(v)$. Moreover, for any $t-1$ field elements $x_i \in F_q$, $2 \leq t \leq [(k+2)/4]$, there exists a vertex v of $D(k, K)$ for which

$a(v) = (x_2, \dots, x_t) = (x)$.

V. On flag systems of graphs $A(n, K)$ and $D(n.K)$, walks on them and multivariate maps

Graphs $D(n, K)$ and $A(n, K)$ have somme common properties. We refer to the first coordinate $x_{1,0} = \rho(\mathrm{x})$ ($x_1 = \rho(\mathrm{x})$ of a point x from graph $D(n, K)$ (graph $A(n, K)$, respectively) and the first coordinate $y_{1,0} = \rho(\mathrm{y})$ ($y_1 = \rho(\mathrm{y})$) of a line y as the colour of the vertex (point or line). The following property holds for the graph: there exists a unique neighbour $N_t(v)$ of a given vertex v of a given colour $t \in K$.

A flag of the incidence system $D(n, K)$ or $D(K)$ ($A(n, K)$ or $A(K)$) is an unordered pair $\{(\mathrm{x}), [\mathrm{y}]\}$ such that $(\mathrm{x})I[\mathrm{y}]$. Obviously, the totalities of flags $FD(n, K)$ or $(FA(n, K))$ of the bipartite flag $D(n, K)$ (or $A(n, K)$, respectively) are isomorphic to the variety K^{n+1}. So, flag $\{(\mathrm{x}), [\mathrm{y}]\}$ of $D(n, K)$ is defined by the tuple $(x_{10}, x_{11}, \dots, y_{01})$. Notice, that $N_{y_1}(\{\mathrm{x}\}) = [\mathrm{y}]$.

We consider an operator $NP_\alpha(\{(\mathrm{x}), [\mathrm{y}]\})$, $\alpha \in K$ mapping flag $\{(\mathrm{x}), [\mathrm{y}]\}$ of the incidence structure $G(n, K)$ (where G is D or A)) into its image $\{(\mathrm{x}'), [\mathrm{y}]\}$, where $\mathrm{x}') = N_\alpha([\mathrm{y}])$.

Similarly, an operator $NL_\alpha(\{(\mathrm{x}), [\mathrm{y}]\})$ maps $\{(\mathrm{x}), [\mathrm{y}]\}$ into $\{(\mathrm{x}), N_\alpha(\mathrm{x})\}$).

Let $\alpha_1, \alpha_2, \dots, \alpha_k$ and $\beta_1, \beta_2, \dots, \beta_k$ be chosen sequences of elements from the commutative ring K. The composition

$$E = NP_{\alpha_1}NL_{\beta_1}NP_{\alpha_2}NL_{\beta_2} \dots NP_{\alpha_k}NL_{\beta_k}$$

transforms flag $\{(\mathrm{x}), [\mathrm{y}]\}$ into the new flag $\{(\mathrm{x}'), [\mathrm{y}']\}$. The process of recurrent computations of $E(\{(\mathrm{x}), [\mathrm{y}]\} = \{(\mathrm{x}'), [\mathrm{y}']\}$ corresponds to the walk in a graph $G(n, K)$ with the original vertex (x) and the final point (x$'$). Notice, that $[\mathrm{y}'] = N_\alpha(\mathrm{x}')$.

Let us assume now that we have two finite families of polynomials of $K[z_1, z_2]$: $\phi_1(z_1, z_2), \phi_2(z_1, z_2), \dots, \phi_{k+1}(z_1, z_2)$ and $\psi_1(z_1, z_2), \psi_2(z_1, z_2), \dots, \psi_k(z_1, z_2)$. We assume that their density is restricted by independent constant d and their degree is bounded by the linear function $\alpha n + \beta$.

The transformation $\tilde{E}$ shifts a flag $\{(\mathrm{x}), [\mathrm{y}]\}$ into its image for the map

$$\begin{aligned} &NP_{\phi_1(x_1,y_1)}NL_{\psi_1(x_1,y_1)}NP_{\phi_2(x_1,y_1)}NL_{\psi_2(x_1,y_1)} \cdots \\ &\dots NP_{\phi_k(x_1,y_1)}NL_{\psi_k(x_1,y_1)}. \end{aligned}$$

Additionally, we assume that the system of equations $\phi_k(z_1, z_2) = a$, $\psi_k(z_1, z_2) = b$ has exactly one solution independently from the choice of a and b (boundary requirement). The written above condition insure that the reimage of $\{\mathrm{x}', [\mathrm{y}']$ for $\tilde{E}$ is uniquely determined. Really, parameters x_1 and y_1 are determined by the system of equations.

It allows us to compute each expression of kind $\phi_i(x_1, y_1)$ and $\psi_j(x_1, y_1)$ and to obtain the reverse walk in the graph with the origin x$'$ and final point x. So, we get the original flag (x), [y] with $[\mathrm{y}] = N_{y_1}(\mathrm{x})$. The code of our flag is $(x_1, x_2, \dots, x_n, y_1)$.

Let $f = f_n$ be the transformation of affine space K^{n+1} into itself which maps flag $(x_1, x_2, \dots, x_n, y_1)$ into the image for $\tilde{E}$ defined by the family of bivariate polynomials from $K[z_1, z_2]$. Assume that f_n is written in a standard form $x_i \to f_i(x_1, x_2, \dots, x_n, y_1)$, $i = 1, 2, \dots, n$, $y_1 = f_{n+1}(x_1, x_2, \dots, x_n, y_1)$.

Let ${g_n}^i : K^{n+1} \to K^{n+1}$ be the transformation moving $\mathrm{z} = (z_1, z_2, \dots, z_n, u_1)$ into $NP_{\phi_{i\,z_1,u_1}}(\mathrm{z})$ and ${h_n}^j$ be the transformation moving z into $NL_{\psi_{j\,z_1,u_1}}(\mathrm{z})$. Obviously, $f = {g_n}^1{h_n}^2{g_n}^2{h_n}^2 \dots {g_n}^k{h_n}^k$ is the invertible decomposition of f of speed $O(n)$. Notice, that generally speaking it is not true that each ${g_n}^i$ or ${h_n}^i$ is invertible. The following statement is a direct corollary of results [3] in the case $G(n,K)=D(n,K)$, and results of [4] in the case of $G(n,k)=A(n,K)$.

Theorem 5.1: The $G(n,K)$ graph based transformations $f_n : K^{n+1} \to K^{n+1}$ defined above for $\phi_j(z_1,z_2)=z_1+a_j$ and $\psi_j(z_1,z_2)=z_2+b_j$ where $a_j,b_j\in K$, $j=1,2,\dots,k$ are stable cubical maps.

It means that we always have $O(n^4)$ monomial terms for the map f_n. Notice that f_n is given by its invertible decomposition. The following statement is a direct corollary from the theorem.

Proposition 5.1: Let us consider the specialization $\tilde{f}_n$ of f_n given by relations $y_{0,1}=h(x_{1,0})$ ($y_1=h(x_1$ in case of graphs $A(n,K)$, respectively), where $h(x)\in K[x]$ is a polynomial expression of degree t, such that equation of kind $h(x_{1,0})=b$, $b\in K$ ($h(x_1)=b$) has no more than one solution. Then degree of $\tilde{f}_n$ is bounded by t^3.

Remark 5.1:

We can change variables $x_{1,0}$ and x_1 of the proposition for y_{01} and y_1, respectively.

Recall, that M is a multiplicative subset of commutative ring K if it is closed under multiplication and does not contain zero. Let us consider the following special choice of coefficients a_j and b_j. The following statement is proved in [23] (see also [13], [14]).

Theorem 5.2: Let $f_n : K^{n+1}\to K^{n+1}$ be $G(n,K)$ graph based transformation $f_n : K^{n+1}\to K^{n+1}$ defined for $\phi_j(z_1,z_2)=z_1+a_j$ and $\psi_j(z_1,z_2)=z_2+b_j$, where $a_j,b_j\in K$, $j=1,2,\dots,k$ in theorem 1.

Let M be a multiplicative set of K and $a_1,b_1\in M$, $a_{i+1}-a_i\in M$, $b_{i+1}-b_i\in M$ for $i=1,2,\dots,k-1$. Then the order of a transformation f_n is going to infinity with the growth of n.

Remark 5.2: In the case of graph $D(n,K)$ we can change polynomial $h(x_{1,0}$ for the $h(x_{1,0},a_2(\mathrm{x}),a_3(\mathrm{x}),\dots,a_t(\mathrm{x}))$, where $h(z_1,z_2,\dots z_t)\in K[(z_1,z_2,\dots z_t]$, $t=[(n+2)/4]$.

We can look at f_n as function with invertible decomposition with initial relation $y_{0,1}=h(x_{1,0}$ (case of $D(n,K)$) or $y_1=h(x_1)$ (case of $A(n,K)$. Really, invertible decomposition of f_n allows to solve

$(f_n)^s(x_{1,0},h(x_{1,0},x_{1,1},\dots,))=(c_{1,0},c_{0,1},c_{1,1},c_{2,1},\dots)$ or

$(f_n)^s(x_1,h(x_1,x_2,\dots,x_n))=(c_1,c_1',c_2,\dots,c_n)$ can be solved fast in some special simple cases.

For simplicity of writing we assume that $G(n,K)=D(n,K)$. Let us consider the system of equation $(*)$: $x_{10}+\alpha_k s=c_{1,0}$, $h(x_{1,0})+\beta_k s=c_{0,1}$

We can eliminate parameter s: $\beta_k x_{1,0}+\alpha_k\beta_k s=\beta_k c_{1,0}$

$h(x_{1,0})\alpha_k+\alpha_k\beta_k s=c_{1,0}\alpha_k$.

So, we get an equation of kind $c_{0,1}\alpha_k-\beta_k c_{1,0}=h(x_{1,0})\alpha_k x_{1,0}\beta_k$ (*)

Let us assume that $h(x_{1,0})\alpha_k x_{1,0}\beta_k=c$ has not more than one solution for each $c\in K$.

Under this condition we can solve (*) for x_1. So, if α_k or β_k differs from 0 we can find parameter s.

Assume that characteristics of ring K is a large prime p. Let us consider the following two simple cases:

(a) $\alpha_k=0$ but β_k is a regular ring element. It is clear that in this case $x_{1,0}$ is known and we can find parameter s with arbitrarily chosen function $h(x)$.

(b) $\beta_k=0$ and equation $h(x_{1,0})=c$ has no more than one solution. In this case one can find $x_{1,0}$ and find parameter s from the first equation.

We say that multivariate map $g_n : K^{n+1}=K^{n+1}$ is symmetrical if $\deg(g_n)=\deg(g_n)^{-1}$. Obviously, each stable transformation is symmetrical. It is clear that in the case (a) we get a stable transformation of K^n into itself. In case of $\deg(g_n)\neq\deg(g_n)^{-1}$ we refer to g_n as assymetrical map.

The following cryptosystem can be used.

Alice chooses a function $h(x_{1,0},a_2(\mathrm{x}),a_3(\mathrm{x}),\dots,a_t(\mathrm{x}))$ of finite degree t and invertible affine transformation: $\tau_1 : K^n\to K^n$, which sends x onto xA+b. Assume that it will be extended till K^{n+1} via the rule $\tau_1 : z\to az+l(\tau_1(\mathrm{x}))=z'$, where l is some linear function from x. Let τ be an expanded linear transformation.

Alice takes the symbolic tuple $(x_{1,0},x_{1,1},\dots,z)$ applies τ and gets the vector $u_{1,0},u_{1,1},\dots,z'=\mathrm{u}$. She will treat this tuple as a flag from $FD(n,K)$.

She writes the equation $z'=h(x_1,x_2)$ and rewrites it in the form $z=h'(x_1,x_2)$.

Alice choses the pseudorandom strings $\alpha_1,\alpha_2,\dots\alpha_k$ and $\beta_1,\beta_2,\dots,\beta_k$ of ring elements.

She generates defined above transformation $f_n : K^{n+1}\to K^{n+1}$. Alice computes symbolically $f_n(\mathrm{u})=\mathrm{w}$ and applies τ^{-1} to w.

She forms a stable cubical transformations $E=g_n=\tau f_n\tau^{-1}$ and writes it in standard form

$$
\begin{aligned}
x_{10} \to& x'_{1,0}=g_{1,0}(x_{1,0},x_{1,1},\dots,z)\\
x_{11} \to& x'_{1,1}=g_{1,1}(x_{1,0},x_{1,1},\dots,z)\\
&\vdots\\
z \to& z'=g_{0,1}(x_{1,0},x_{1,1},\dots,z)
\end{aligned}
$$

In the case of the first n rules Alice uses the specialisation $z=h'(\mathrm{x})$ and writes $\tilde{g}'_{1,0}(\mathrm{x})=g_{1,0}(h'(\mathrm{x},x_{1,0},x_{1,1}\dots)$, $\tilde{g}'_{1,1}(\mathrm{x})=g_{1,1}(h'(\mathrm{x}),x_{1,0},x_{1,1},\dots)$, $\dots$, in a standard form. The specialisetion gives us a restriction E' of our encryption map on the point set isomorphic to K^n.

Bob gets these n rules from Alice together with initial condition $z=h'(x_{1,0},x_{1,1},\dots)$.

He takes his plaintext $(\mathrm{x})=(p_{1,0},p_{1,1},\dots)$ and applies the restricted map E' iteratively s times.

Thus, he gets consecutively $E'^i(\mathrm{p})$, $i=1,2,\dots,s$ and computes recursively

$$
\begin{aligned}
z_1 =& g_{0,1}(p_{1,0},p_{1,1},\dots,h'(\mathrm{p}),\\
z_2 =& g_{0,1}(E(\mathrm{p},z_1)),\\
&\vdots\\
z_s =& g_{0,1}(E^{s-1}\mathrm{p},z_{s-1}).
\end{aligned}
$$

He sends Alice his expanded ciphertext as a pair $\mathrm{c}=E'^s(\mathrm{p})$ and parameter z_s.

For the decryption Alice applies transformation τ to the c concateneted with z_s and gets c_1. She computes $E^{-1}(\mathrm{c}_1) = c_2$. Computation $\tau^{-1}(\mathrm{c}_2)$ gives her the plaintext p.

Let us consider some obvious properties of defined above cryptosystem in special cases (a) and (b).

(a) We can see that our encryption is of symmetrical degree. Let deq$h = t$, then our map f_n has a degree bounded by t^3. If parameter t is a constant then the map E' is computable in polynomial time. Notice, that linearisation attacks are possible, they allow to compute ${E'}^{-1}$. This fact is not yet a breaking of the system, because E' is a stable map which order is growing with the growth of parameter n.

Thus, finding the solution for ${E'}^s = H(\mathrm{x})$ can be a difficult task. The discrete logarithm problem for cyclic subgroup of Cremona group of increasing order appears there. Notice, that only one value of $H(\mathrm{x})$ can be given for chosen by Bob parameter s. Algorithm can be used in dynamical mode: every session Alice changes encryption base and every time Bob changes parameter s.

Notice, that $s = s(n)$ can be a function from parameter n. Bob can encrypt for polynomia time $s(n)O(n^{t^3})$. Alice can decrypt because of the logarithmical invertibility of the map.

(b) Let us just consider a simple example

$$h(x_{1,0}, a_2(\mathrm{x}), \ldots, a_t(\mathrm{x})) = (d(a_2(\mathrm{x}), a_3(\mathrm{x}), \ldots, a_t(\mathrm{x}))x_{1,0}+ \\ + b(a_2(\mathrm{x}), \ldots, a_t(\mathrm{x}))^r + c(a_2(\mathrm{x}), a_3(\mathrm{x}), \ldots, (a_t\mathrm{x})),$$

d, b, c are multivariate functions, r is odd and equation $x^r = \alpha$ in K has not more than one solution for each parameter α. If we skip degenerate cases, our encryption function E' will be assymetric. It means that even finding the inverse E' can be a hard task in this case.

We presnt here a well known case of the pair (r, K) which satisfies to written above property (see the description of Imai-Matsumoto method in [26]). Let $K = F_{q^n}$ be an extention of the field F_q of characteristic 2. We take r as a parameter of kind $q^\beta + 1$ for some parameter β, such that the greatest common divisor of $q^\beta + 1$ and $q^n - 1$ is 1. Then map $x \to x^r$ is one to one correspondence and equation $x^r = \alpha$ has a unique solution.

VI. Conclusions

Known methods of symmetric encryption according to chosen walks on flags of bipartite graphs $A(n, K)$ and $D(n, K)$ use special colouring of their points and lines. The increasing girth and good expansion properties of these graphs lead to good mixing properties of the stream cipher based on stable transformation. The weakness of such method is an option of cubical linearisation attacks based on the fact that decryption map is also cubical (complexity of the attack is $O(n^{10})$, so its costly, but possible. There were several implementations of such algorithms for practical use in academic networks and ORACLE based university management systems for various cases of fields and rings: [2], [27], [28] devoted to ciphers used in The University of South Pacific (Fiji), [30], [31], [35] discussed algorithms used at Sultan Qaboos University (Oman), [31], [32], [35] were used in University of Maria Curie - Sklodovska (Poland), algorithm of [29] and [34] were used in teaching process of Kiev Mohyla Academy (Ukraine) and University of British Columbia (Canada), respectively.

Private key algorithm, presented in this paper allows to modificate discussed above programs with essential increase of resistence to linearisation attack without damage of theoretical speed ($O(n)$ in the case of keys of constant length and $O(n^2)$ for passwords of length $O(n)$). We can create encryption maps of large symmetric degree or assymetrical maps with inverses of high degree.

In a public mode we introduce the multivariate cryptosystems such that their security is connected with discrete logarithm problem for large cyclic subgroups of Cremona group. We hope that a new class of multivariate cryptosystems can be an interesting objects for cryptanalitical studies.

References

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

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

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

[4] Vasyl Ustimenko, Aneta Wróblevska, *On the key exchange with nonlinear polynomial maps of degree 4*, Proceedings of the conference "Applications of Computer Algebra", Vlora, Albanian Journal of Mathematics, Special Issue, December, 2010, vol .4 n 4, 161-170.

[5] Ustimenko V., Graphs with special arcs and cryptography, Acta Applicandae Mathematicae (Kluwer) 2002, 74,117-153.

[6] Ustimenko V. *Maximality of affine group and hidden graph cryptosystems*// J. Algebra Discrete Math. -2005 ., No 1,-P. 133–150.

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

[8] Vasyl 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).

[9] 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, vol. 3, 181-200 (2007).

[10] V. A. 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.

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

[12] Vasyl Ustimenko, Aneta Wróblewska, *On some algebraic aspects of data security in cloud computing*, Proceedings of International conference "Applications of Computer Algebra", Malaga, 2013, p. 144-147.

[13] V. A. Ustimenko, U. Romańczuk, *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/January 2013, 257-285.

[14] V. A. Ustimenko, U. Romańczuk *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, 237-256.

[15] B. Bollobás, *Extremal Graph Theory*, Academic Press, London, 1978.

[16] G. Margulis, *Explicit group-theoretical constructions of combinatorial schemes and their application to desighn of expanders and concentrators*, Probl. Peredachi Informatsii., 24, N1, 51-60. English translation publ. Journal of Problems of Information transmission (1988), 39-46.

[17] A. Lubotsky, R. Philips, P. Sarnak, *Ramanujan graphs*, J. Comb. Theory., 115, N 2., (1989), 62-89.

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

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

[20] P. Guinand, J. Lodge, *Tanner type codes arising from large girth graphs*, Canadian Workshop on Information Theory CWIT '97, Toronto, Ontario, Canada (June 3-6 1997):5–7.

[21] D. MacKay and M. Postol, *Weakness of Margulis and Ramanujan - Margulis Low Dencity Parity Check Codes*, Electronic Notes in Theoretical Computer Science, 74 (2003), 8pp.

[22] V. Ustimenko, *On some optimisation problems for graphs and multivariate cryptography* (in Russian), In Topics in Graph Theory: A tribute to A.A. and T. E. Zykova on the ocassion of A. A. Zykov birthday, pp 15-25, 2013, www.math.uiuc.edu/kostochka.

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

[24] M. Polak, V. A. Ustimenko, *On LDPC Codes Corresponding to Infinite Family of Graphs A(n,K)*, Proceedings of the Federated Conference on Computer Science and Information Systems (FedCSIS), CANA, Wroclaw, September, 2012 , pp 11-23.

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

[26] N. Koblitz, *Algebraic Cryptography*. Springer, 1998.

[27] Y. Khmelevsky, V. Ustimenko, *Walks on graphs as symmetric and asymmetric tools for encryption*, South Pacific Journal of Natural Studies, 2002, vol. 20, 23-41.

[28] Y. Khmelevsky, V. Ustimenko, *Practical aspects of the Informational Systems reengineering*, The South Pacific Journal of Natural Science, volume 21, 2003, p.75-21.

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

[30] A. Touzene, V. Ustimenko, *Graph Based Private KeyCrypto System*, International Journal on Computer Research, Nova Science Publisher, volume 13 (2006), issue 4, 12p.

[31] A. Touzene, V. Ustimenko, *Private and Public Key Systems Using Graphs of High Girth*, In "Cryptography Research Perspectives", Nova Publishers, Ronald E. Chen (the editor), 2008, pp.205-216

[32] J. Kotorowicz, V. Ustimenko, *On the implementation of cryptoalgorithms based on algebraic graphs over some commutative rings*, Condenced Matters Physics, 2006, 11 (no. 2(54)) (2008) 347–360.

[33] 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, 12pp.

[34] Y. Khmelevsky, Gaetan Hains, E. Ozan, Chris Kluka, D. Syrotovsky, V. Ustimenko, *International Cooperation in SW Engineering Research Projects*, Proceedings of Western Canadien Conference on Computing Education, University of Northen British Columbia, Prince George BC, May 6-7, 2011, 14pp.

[35] 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.

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