Annales UMCS Informatica AI XIV, 1 (2014) 7–18
DOI: 10.2478/umcsinfo-2014-0001

Annales UMCS
Informatica
Lublin-Polonia
Sectio AI

http://www.annales.umcs.lublin.pl/

On Multivariate Cryptosystems Based on Computable Maps with Invertible Decomposition

Vasyl Ustimenko[1]*

[1] *Institute of Computer Science, Maria Curie-Sklodowska University, pl. M. Curie-Sklodowskiej 5, 20-031 Lublin, Poland*

Abstract – Let K be a commutative ring and K^n be an affine space over K of dimension n. We introduce the concept of a family of multivariate maps $f(n)$ of K^n into itself with invertible decomposition. If $f(n)$ is computable in polynomial time then it can be used as the public rule and the invertible decomposition provides a private key in $f(n)$ based public key infrastructure. Requirements of polynomial ity of degree and density for $f(n)$ allow to estimate the complexity of encryption procedure for a public user. The concepts of a stable family and a family of increasing order are motivated by the studies of discrete logarithm problem in the Cremona group. The statement on the existence of families of multivariate maps of polynomial degree and polynomial density of increasing order with the invertible decomposition is proved. The proof is supported by explicite construction which can be used as a new cryptosystem. The presented multivariate encryption maps are induced by special walks in the algebraically defined extremal graphs $A(n, K)$ and $D(n, K)$ of increasing girth.

1 On Multivariate Cryptography and Special Multivariate Transformations

Multivariate cryptography (see [**1**]) is one of the directions of Postquantum Cryptography, which concerns 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.

*vasyl@hektor.umcs.lublin.pl

Recall that the *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 *a family of polynomial degree*, if the degree of each transformation is a parameter s of the size $O(n^t)$.

We say that a family $f(n)$ is *a family of linear degree* in the case $t = 1$. We refer to a family $f(n)$ as *a family of bounded degree* if $t = 0$. Let us 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 a chosen order.

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

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

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

Let us consider the discrete logarithm problem for a stable family f^n of the 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 new information for the task execution. If the order of element $f(n)$ grows fast with the growth of n, then the 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 a given y in time $k(n)O(n^d)$ (see the author's 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 say that the 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.

In section 4 we prove that for each commutative ring K, $\mathrm{char}(K) \neq 2$ and each $s \geq o$ there exists a family of multivariate polynomials of the increasing degree with the polynomial invertible decomposition, such that members of the family are unstable maps of the polynomial degree d, $d(n^s)$ and the polynomial density.

The proof of this theorem is obtained via studies of multivariate maps related to explicite construction of Extremal Graph Theory (see [**2, 3, 4, 5**]) given in terms of nonlinear equations over finite fields F_q and their analogas defined over general commutative ring.

The examples of stable families $f(n) \in C(K^n)$ of the constant degree and the increasing order defined in terms of algebraic graph theory are given in [**6, 7, 8, 9**]. An example of stable transformations of linear degree and increasing order is proposed in [**10**], the idea of usage of stable maps with compression is considered in [**11**].

2 Extremal Algebraic Graphs Corresponding to Special Families of Multivariate Maps

Recall that the girth is the length of minimal cycle in the simple graph. The 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:

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

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 the 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 fifties by Erdős' via the 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 the arbitrary large but bounded degree $k_i = k$ with $c = 1/4$ by his famous probabilistic method.

Only two explicit families of regular simple graphs of large girth with unbounded girth and arbitrarily large k are known: the family $X(p, q)$ of Cayley graphs for $PSL_2(p)$, where p and q are the defined primes by G. Margulis [**12**] and investigated by A. Lubotzky, Sarnak [**13**] and Phillips and the family of algebraic graphs, $CD(n, q)$ [**14**]. The graphs CD(n,q) appear as connected components of the graphs $D(n, q)$ defined via the system of quadratic equations. The best known lower bound for $d \neq 2, 3, 5$ was deduced from the existence of the 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 the family of regular graphs Γ_i of degree k_i and the increasing order v_i is a *family of graphs of small world* if $\mathrm{diam}(\Gamma_i) \leq c\log_{k_i}(v_i)$ for an independent constant c, $c > 0$, where $\mathrm{diam}(\Gamma_i)$ is 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 from 1995 that the family of graphs $CD(n, q)$ for odd q is another example of such kind. Currently. it is proven that the diameter of $CD(n, q)$ is bounded from the above by the polynomial function $d(n)$, which does not depend on 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 [**15**]. This class of error correcting codes is an important tool of security for satellite communications. The usage of $CD(n,q)$ as the Tanner graphs producing LDPC codes leads to better properties of the corresponding codes compared to the usage of Cayley - Ramanujan graphs (see [**16**]).

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 hold also 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 the edge transitive automorphism group.

We consider below the optimization problem for simple graphs which is similar to 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 a given vertex of the simple graph Γ as *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 *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 the order v with the size larger than d, $d > 2$ has been found very recently.

It turns out that:

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

and this bound is always sharp (see [**15**] or [**16**] and further references).

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

$$\mathrm{Cind}(\Gamma_i) \geq c\log_{\mathrm{k_i}}(v_i) \tag{3}$$

for an 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 the family of graphs Γ_i. As it follows from the above written 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 proven in [**16**]:

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 the previous statement is given in [**15, 16**]. 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 [**19**], computer simulations demonstrate essential advantages of new codes in comparison to those related to $CD(n,q)$ and $D(n,q)$.

The 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 [**6**]). The theory of directed graphs and language of dynamical system were very useful for the studies of public key and private key algorithms based on graphs $D(n,K)$, $CD(n,K)$ and $A(n,K)$ (see [**16**], [**17**], [**15**], [**19**] and further references).

There are several implementations of symmetric algorithms for cases of fields (starting from [**7**]) and arithmetical rings ([**19**], in particular). Comparison of public keys based on $D(n,K)$ and $A(n,K)$ are considered in [**18**].

3 On the Cryptosystems Corresponding to Special Families of Multivariate Maps

(1) We can use families of elements $f(n)$ with invertible decomposition of speed d of the 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 a constant or linear function invariable n (see surveys [**17**]. [**20**], [**22**] on the use of the graph based on 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 the case of private keys both correspondents know the invertible decompositions and family $\tau(n)$ of affine transformation as part of the key.

(2) Let $f(n)\in C(K^n))$ be a family of transformations of polynomial degree s and polynomial density d with an invertible decomposition of speed t. The following public key can be implemented.

Alice chooses a parameter n. She knows the decomposition $f(n)=f(n,1)$

$f(n,2)\dots f(n,k(n))$. Notice that transformations $f(n,i)$ can not be a bijective. Additionally, she chooses an invertible monomial linear transformations τ_L of the kind $x_i\to\lambda_i x_\pi(i)$, where π is a permutation on the set $\{1,2,\dots,n\}$. Alice takes also an affine transformation τ_R of the kind $\mathrm{x}\to \mathrm{x}A+\mathrm{b}$, where A is a non-singular matrix.

She computes the transformation $G=\tau_L f(n)\tau_R$ in the *Cremona* group and writes it in the standard form $\mathrm{x}_i\to g_i(x_1,x_2,\dots,x_n)$, $i=1,2,\dots,n$.

Let us assume that public rules g_i are governed by the lists of monomial terms, written in a chosen order.

Notice that the applications of the transformations τ_L and τ_R from the left and right , respectively, do not change the degree: $\deg(G) = \deg f(n)$. The left application of τ_L does not change the number of monomial terms. The right application of τ_R can increase number of monomial terms in n times. So, the density $\mathrm{den}(\tau_L f(n)\tau_R)$ is $O(n^{d+1})$.

A public user (Bob) gets symbolic transformation $G = G(n)$ in the form of the public rule $\mathrm{x}_i \to g_i(x_1, x_2, \ldots, x_n)$. He can encrypt for $O(n^{s+d+1})$ by computation of the value of G on his plaintext $(x_1, x_2, \ldots, x_n)$.

Alice keeps the decomposition $f(n) = f(n,1)f(n,2)\ldots f(n,k(n))$ as deep secret. It allows her to decrypt Bob's ciphertext for $k(n)O(n^t)$. If Bob does not have additional information on the transformation G, then he can only use general algorithm of computation G^{-1}. The complexity of such efforts is $O(n^{sn})$.

Remark 1. Let $f(n) \in C(K^n)$ be a family of transformations of the increasing order and $\tau_L = {\tau_R}^{-1}$. Then the transformations $G(n)$ also form the family of the increasing order.

Remark 2. Let $f(n)$ be a stable family of transformations of the restricted degree r. Let us assume that the information on stability is known to one of public users. He or she can use the fact that $\deg(\mathrm{G}) = \deg(\mathrm{G})^{-1}$ and conduct linearisation attacks, which allow to break a system for $O(n^{2r+1})$

It means that for the generation of public key we have to use families of stable transformations of non-stable degree or stable families with linear or superlinear degree.

4 On the Explicit Constructions

The graph $A(n, K)$, where K is a finite commutative ring, is defined in the following way. This is a bipartite graph with the point set $P = \{x_1, x_2, \ldots, x_n) | x_i \in K\} = K^n$ and the line set $L = \{[y_1, y_2, \ldots, y_n] | y_i \in K|\} = K^n$ and such that a point $\mathrm{x} = (x_1, x_2, \ldots, x_n)$ is incident to a line $\mathrm{y} = [y_1, y_2, \ldots, y_n]$ if and only if the equations $x_i - y_i = y_1 x_1$ hold for even i and the relations $x_j - y_j = x_1 y_j$ hold for an odd j, $j \geq 3$. We identified 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 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 follows from the definition the projective limit of $A(n, K)$, $n \to \infty$ is well defined. The points $\mathrm{p} = (p_1, p_2, \ldots, p_n, \ldots)$ and the lines $\mathrm{l} = [l_1, l_2, \ldots, l_n, \ldots]$ are tuples with a finite number of non-zero coordinates. A point and a line are incident when the infinite number of equations $p_2 - y_l = l_1 p_1, p_3 - l_3 = p_1 l_2, \ldots$ hold.

A flag of the incidence system $A(n,K)$ (or $A(K)$)is an unordered pair $\{(\mathrm{x}),[\mathrm{y}]\}$ such that $(\mathrm{x})I[\mathrm{y}]$. Obviously, the totality of flags $FA(n,K)$ $(FA(K))$of the bipartite flag $A(n,K)$ $(A(K)$, respectively) is isomorphic to the variety K^{n+1}. So, the flag $\{(\mathrm{x}),[\mathrm{y}]\}$ is defined by the tuple $(x_1,x_2,\ldots,x_n,y_1)$. 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 $A(n,K)$ (or $A(K)$) 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 $\alpha_1,\alpha_2,\ldots,\alpha_k$ and $\beta_1,\beta_2,\ldots,\beta_k$ be chosen sequences of elements from the commutative ring K. The composition:

$$E=NP_{\alpha_1}NL_{\beta_1}NP_{\alpha_2}NL_{\beta_2}\ldots NP_{\alpha_k}NL_{\beta_k} \tag{4}$$

transforms the 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 $A(n,K)$ 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 $K[z_1,z_2]$: $\phi_1(z_1,z_2),\phi_2(z_1,z_2),\ldots,\phi_{k+1}(z_1,z_2)$ and $\psi_1(z_1,z_2),\psi_2(z_1,z_2),\ldots,\psi_k(z_1,z_2)$. We assume that their density is restricted by an independent constant d and their degree is bounded by the linear function $\alpha n+\beta$.

The transformation $\tilde{E}$ which shifts a flag $\{(\mathrm{x}),[\mathrm{y}]\}$ into its image for the map $NP_{\phi_1(x_1,y_1)}NL_{\psi_1(x_1,y_1)}NP_{\phi_2(x_1,y_1)}NL_{\psi_2(x_1,y_1)}\ldots NP_{\phi_k(x_1,y_1)}NL_{\psi_k(x_1,y_1)}$.

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 independent of the choice of a and b (boundary requirement). The above written condition ensures that the reimage of $\{\mathrm{x}',[\mathrm{y}']$ for $\tilde{E}$ is uniquely determined. In fact, the parameters x_1 and y_1 are determined by the system of equations.

The simplest example for which the boundary requirements hold is a linear system of equations, i. e. the case of $\phi_k=d_1z_1+d_2z_2$ and

$\psi_k=c_1z_1+c_2z_2$ such that the matrix formed by the rows (d_1,d_2) and (c_1,c_2) is invertible over the commutative ring K. Notice that ϕ_j and ψ_j for $j<k$ can be non-linear expressions from $K[z_1,z_2]$. If the equation of the kind $y^3=a$ has a unique solution in K, we can change the linear phi_k and ψ_k for the expressions $d_{z_1}^3+d_2z_2$ and $c_1{z_1}^3+c_2z_2$, respectively. The other option corresponds to the pair $(d_{z_1}^3+d_2{z_2}^3$, $c_{z_1}^3+c_2{z_2}^3)$.

It allows us to compute each expression of the 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 the final point x. So, we get the original flag $(\mathrm{x}),[\mathrm{y}]$ with $[\mathrm{y}]=N_{y_1}(\mathrm{x})$. The code of our flag is $(x_1,x_2,\ldots,x_n,y_1)$.

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

Let ${g_n}^i:K^{n+1}\to K^{n+1}$ be the transformation moving $\mathrm{z}=(z_1,z_2,\ldots,z_n,u_1)$ 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.

It is known that if $\phi_j(z_1, z_2) = z_1 + a_j$ and $\psi_j(z_1, z_2) = z_2 + b_j$ for some constants a_j, b_j, then the transformation $f_n : K^{n+1} \to K^{n+1}$ is cubical (see [**19**]). It means that we have $O(n^4)$ monomial terms for the map.

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. If $a_{i+1} - a_i \in M$, $b_{i+1} - b_i \in M$ for $i = 1, 2, \dots, k-1$ and $a_1 \in M$, $b_1 \in M$ for some multiplicative subset of K, the transformation $\tilde{E}, FA(K)$ is a cubical map of an infinite order. The cycle C containing flag $\{(0, 0, \dots), [0, 0, \dots, 0]\}$ contains infinitely many elements. So, $(\tilde{E}, FA(K))$ has an infinite order and the order of finite permutation $(\tilde{E}, FA(n, K))$ is going to infinity with the growth of parameter n (see [**17**] or [**19**]).

Let us deformate the functions ϕ_i and ψ_i as above in the following way $\phi'(z_1, z_2) = \alpha_j {z_1}^{s(j,n)}{z_2}^{s'(j,n)} + a_j$, $\psi_j = \beta {z_1}^{r(j,n)}{z_2}^{r'(j,n)} = b_j$, where $s(j, n)$ and $s'(j, n)$ are the polynomials in variable n with the highest terms $t_1(j)n^{c_j}$ and $t'_1(j)n^{c'_j}$, $r(j, n)$ and $r'(j, n)$ are the polynomials with the highest terms $t_2(j)n^{d_j}$ and $t'_2(j)n^{d'_j}$ with non-negative values of the parameters $t_1(j)$, $t_2(j)$, c_j d_j and $t'_1(j), t'_2(j)$, c'_j d'_j. Recall that we have to care about the boundary.

The transformation $\tilde{E}_1$ corresponding to the "deformatedśpecialization $z_1 = x_1, z_2 = y_1$ has also density $O(n^4)$. It acts on elements of the cycle C in the same way as $\tilde{E}$. So, $\tilde{E}_1|C = \tilde{E}|C$. It means that $(\tilde{E}_1, FA(K)$ is an infinite transformation and the order of finite permutation $(\tilde{E}_1, FA(n, K))$ is increases with the increase of n.

The degree of transformation $(\tilde{E}_1, FA(n, K))$ can be estimated as 3 plus sum of values $\deg(\phi'_j - \phi'_{j-1})$, $j = 1, 2, \dots, k$ and $\deg(\psi'_j - \psi'_{j-1})$, $j = 1, 2, \dots, k$. We assume that $\mathrm{char}(K) \neq 2$, $M = \{1, -1\}$, $\alpha_i - \alpha_{j-1} \neq 0$ and $\beta_j \neq \beta_{j-1} \neq 0$ for each j. So, our explicit construction supports the following statement.

Theorem 1. Let K be a commutative ring of $\mathrm{char}(K) \neq 2$. For each non-negative integer parameter s there exists a family $f_n \in C(K^n)$ of unstable multivatiate maps of polynomial density $O(n^4)$ and polynomial degree d, $d <=> n^s$ of the increasing order. □

We say that the multivariate maps g_n form a symmetrically invertible family id $\deg {f_n}^{-1} = \deg f_n$.

Remark 3. If we chose $\phi_k(z_1, z_2)$ and $\psi_k(z_1, z_2)$ as expressions of the kind $az_1 + b$ and $cz_2 + d$, where a and b are regular elements of the ring, then the above constructed map f_n is symmetrically invertible.

Other boundary conditions can give us an example of the family which is not a symmetrically invertible:

Example 1. Let K be a commutative ring such that for some odd t, $t > 1$ the equations $z^t = a$ do not have more than one solution. Then boundary conditions of the kind $\phi_k(z_1, z_2) = z_1 + b$, $\psi_k(z_1, z_2) = {z_2}^t + d$ (or $\phi_k(z_1, z_2) = {z_1}^t + b$, $\psi_k(z_1, z_2) = z_2 + d$) lead to maps which are not symmetrical.

Remark 4. We can change the graphs $A(n, K)$ for $D(n, K)$ in the above written construction and obtain another explicit construction of multivariate maps of polynomial density and degree.

5 Conclusions

The known methods of symmetric encryption according to chosen walks on the flags of bipartite graphs $A(n, K)$ and $D(n, K)$ use special colouring of their points and lines. The composition of operators changing flag $F = \{v_1, v_2\}$ for the adjacent flag $F' = \{v_2, v_3\}$ such that the colours $\rho(v_3)$ of v_3 and $\rho(v_1)$ of v_1 differ for a chosen constant α is a stable cubical encryption map on the flag space K^{n+1}. The increasing girth and good expansion properties of these graphs lead to good mixing properties of the stream cipher. The weakness of such method is an option of cubical linearisation attacks based on the fact that the decryption map is also cubical (complexity of the attack is $O(n^{10})$.

We introduce a modified method such that seed maps shifting flag $F = \{v_1, v_2\}$ into $F' = \{v_2, v_3\}$ where $\rho(V_3)$ is a monomial term for variables $x_1 = \rho(v_1)$ and $y_1 = \rho(v_2)$ plus the parameter $\alpha \in K$.

The new method can produce symmetrically invertible multivariate encryption maps of unbounded polynomial degree and density $O(n^4)$ of the increasing order or multivariate maps of increasing order, polynomial degree, density $O(n^4)$ and with an unknown degree for the inverse maps.

It means that straightforward linearisation attacks are not applicable to such encryption maps. We may compute the standard form of these maps (list of monomial terms in some order) and use it as a public rule. We hope that a new class of multivariate cryptosystems can be an interesting subject of cryptanalytical studies.

In the case of $\psi_j = z_1 + c_j$ and $\phi_j = z_2 + c_j$ the algorithm of generation of the multivariate map has been implemented (see [**21**]). Let us assume that τ_L and τ_R are monomial transformations. Then change of z_i, $i = 1, 2$ for ${z_i}^3$ in a few cases of parameter j practically does not change the execution type. So, in my opinion, in the cases of sparce expressions ψ_j and ϕ_j and special sparce affine transformations the algorithm can be practically implemented.

Literatura

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

[2] Bollobás B., Extremal Graph Theory, Academic Press, London (1978).
[3] Erdös' P., R'enyi A. and S'oc V. T., On a problem of graph theory, Studia. Sci. Math. Hungar 1 (1966): 215-235.
[4] Erdös' P., Simonovits M., Compactness results in extremal graph theory, Combinatorica 2(3) (1982): 275-288.
[5] Simonovitz M., Extermal Graph Theory , In "Selected Topics in Graph Theory", 2, edited by Beineke L. W. and Wilson R. J., Academic Press, London (1983): 161-200.
[6] Ustimenko V., Coordinatisation of Trees and their Quotients, In the "Voronoj's Impact on Modern Science", Kiev, Institute of Mathematics 2 (1998): 125-152.
[7] Ustimenko V., CRYPTIM: Graphs as Tools for Symmetric Encryption, Lecture Notes in Computer Science, Springer 2227 (2001): 278–287.
[8] Ustimenko V. Maximality of affine group and hidden graph cryptosystems J. Algebra Discrete Math 1 (2005): 133–150.
[9] Wróblewska A., On some properties of graph based public keys, Albanian Journal of Mathematics, NATO Advanced Studies Institute: Ńew challenges in digital communications"2(3) (2008) : 229–234.
[10] Ustimenko V., Wróblewska A., On some algebraic aspects of data security in cloud computing, Proceedings of International conference Applications of Computer Algebra", Malaga (2013): 144–147.
[11] Romańczuk U., Ustimenko V., On regular forests given in terms of algebraic geometry, new families of expanding graphs with large girth and new multivariate cryptographical algorithms, Proceedings of International conference Applications of Computer Algebra", Malaga (2013): 135–139.
[12] Margulis G., 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.
[13] Lubotsky A., Philips R., Sarnak P., Ramanujan graphs, J. Comb. Theory 115(2) (1989): 62–89.
[14] Lazebnik F., Ustimenko V., Woldar A. J., A New Series of Dense Graphs of High Girth, Bull (New Series) of AMS, 32 (1995): 73–79.
[15] Ustimenko V., 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, 2013): 15–25, www.math.uiuc.edu/kostochka.
[16] Ustimenko V., On extremal graph theory and symbolic computations, Dopovidi National Academy of Sci of Ukraine, N2 (in Russian) (2013): 42–49.
[17] Ustimenko V., On the extremal graph theory for directed graphs and its cryptographical applications In: T. Shaska, W.C. Huffman, D. Joener and V. Ustimenko, Advances in Coding Theory and Cryptography, Series on Coding and Cryptology 3 (2007): 181–200.
[18] Kotorowicz J., Ustimenko V., 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 2(54) (2008): 347–360.
[19] Ustimenko V., Romańczuk U., 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, Springer, 427 (2013): 257–285.
[20] Ustimenko V., Romańczuk U., 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 427 (2013): 257–285.

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

[22] Ustimenko V., 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 24 (2009): 296.