On new multivariate cryptosystems based on hidden Eulerian equations over finite fields

Vasyl Ustimenko

Abstract

We propose new multivariate cryptosystems over n-dimensional vector space over a finite field F_q based on idea of hidden discrete logarithm problem for $F^*{}_q$. These cryptosystems are based on hidden eulerian equations $x^\alpha = a$, $(\alpha, q-1) = 1$. The method is based on the idea of Eulerian transformations, which allow us to use asymmetric algorithms based on families of nonlinear multiplicatively injective maps of prescribed polynomial density and flexible degree.

Mathematics Subject Classification (2010): 12Y05 12Y99 05C81 05C85 05C90 94A60 14G50

key words: Multivariate Cryptography, Finite Filds, Eulerian equations, Eulerian transformations, Linguistic Graphs, Multivariate Maps of Low Density

1 On Post Quantum and Multivariate Cryptography

Post Quantum Cryptography serves for the research on asymmetrical cryptographical algorithms which can be potentially resistant against attacks based on the use of a quantum computer.

The security of currently popular algorithms are based on the complexity of the following 3 known hard problems: integer factorisation, discrete logarithm problem, discrete logarithm for elliptic curves.

Each of these problems can be solved in polynomial time by Peter Shor's algorithm for theoretical quantum computer.

Despite that the known nowadays small experimental examples of quantum computer are not able to attack currently used cryptographical algorithm, cryptographers have already started research on postquantum security. They have also count on the new results of general complexity theory.

The history of international conferences on Post Quantum Cryptography (PQC) started in 2006.

We have to notice that Post Quantum Cryptography differs from Quantum Cryptography, which is based on the idea of usage of quantum phenomena to reach better security.

Modern PQC is divided into several directions such as Multivariate Cryptography, Lattice base Cryptography, Hash based Cryptography, Code based Cryptography, studies of isogenies for superelliptic curves.

The oldest direction is Multivariate Cryptography (see [1]) which uses polynomial maps of affine space K^n defined over a finite commutative ring into itself as encryption tools. It exploits the complexity of finding a solution of a system of nonlinear equations from many variables. Multivariate cryptography uses as security tools a nonlinear polynomial transformations of kind $x_1 \to f_1(x_1, x_2, \ldots, x_n)$, $x_2 \to f_2(x_1, x_2, \ldots, x_n)$, $\ldots$, $x_n \to f_n(x_1, x_2, \ldots, x_n)$ acting on the affine space K^n, where $f_i \in K[x_1, x_2, \ldots, x_n]$, $i = 1, 2, \ldots, n$ are multivariate polynomials given in standard form, i. e. via a list of monomials in a chosen order. Important ideas in this direction are observed in [2]. The density of map F is the maximal number $\mathrm{den}(F)$ of monomial terma of f_i, $i = 1, 2, \ldots, n$. We say that $\mathrm{den}(F)$ is polynomial if this parameter has size $O(n^d)$ for some positive constant d. The degree $\deg(F)$ of map F is the maximal value of degrees f_i, $i = 1, 2, \ldots, n$.

Let F be the map of K^n to itself which has polynomial density of size $C_1 n^{d_1}$ and polynomial degree of size $C_2 n^{d_2}$. Then the value of F on tuple $(b_1, b_2, \ldots, b_n)$ can be computed by $O(n^{d_1+d_2+1})$ basic operation of the ring.

Current task is a search for algorithm with resistance to cryptoanalytic attacks based on ordinary Turing machine. Multivariate cryptography has to demonstrate practical security algorithm which can compete with RSA, Diffie -Hellman protocols popular methods of elliptic curve cryptography (see [1], [2]).

This is still a young promising research area with the current lack of known cryptosystems with the proven resistance against attacks with the use of ordinary Turing machines. Studies of attacks based on Turing mashine and Quantum computer have to be investigated separately because of different nature of two machines, deterministic and probabilistic respectively.

Let K be a commutative ring. $S(K^n)$ stands for the affine Cremona semigroup of all polynomial transformations of affine space 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 were proposed by Imai and Matsumoto, cryptanalysis for this system was invented by J. Patarin. The survey on various modifications of this algorithm and corresponding cryptanalysis the reader can find in [1]. Various attempts to build secure multivariate public key were unsuccessful, but the research of the development of new candidates for secure multivariate public keys is going on (see for instance [3] and further references).

Applications of Algebraic Graph Theory to Multivariate Cryptography were recently observed in [4]. This survey is devoted to algorithms based on bijective maps of affine spaces into itself. Applications of algebraic graphs to cryptography started from symmetric algorithms based on explicit constructions of extremal graph theory and their directed analogue. The main idea is to convert an algebraic graph in finite automaton and to 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 from plainspace vector brings several public key cryptosystems. Other source of graphs suitable for cryptography is connected with finite geometries

and their flag system. Bijective multivariate sparse encryption maps of rather high degree based on walks in algebraic graphs were proposed in [5].

One of the first usage of non bijective map of multivariate cryptography was in *oil and vinegar* cryptosystem proposed in [6] and analysed in [7]. Nowadays this general idea is strongly supported by publication [8] devoted to security analysis of direct attacks on modified unbalanced oil and vinegar systems. This algorithm was patented. 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 ≥ 3 based on walks on algebraic graphs $D(n, K)$ defined over general commutative ring and their homomorphic images were proposed in [9].

The new cryptosystems with non bijective multivariate encryption maps on the affine space ${Z_m}^n$ into itself was presented at the international conference DIMA 2015 (Discrete Mathematics and its applications, Minsk, 2015). It uses the plainspace ${Z_m^*}^n$, where $n = k(k-1)/2$, $k \geq 2$ can be arbitrary natural number. The private key space is formed by sequence of general multivariate polynomials from $Z_m[x_1, x_2, \ldots, x_{k-1}]$ and sequence of parameters l_i, $i = 1, 2, \ldots, k-1$ which are mutually prime with $\phi(m)$. The properties of the encryption map depends heavily on the prime factorisation of m. This non bijective encryption map is the deformation of special computation generated by Schubert automaton of "$k-1$ dimensional projective geometry" over Z_m. This method does not use the partition of variables into groups, non bijective nature of the map caused by zero devisors of composite integer m. In fact the idea of multiple "hidden RSA" is used in [10].

Other algorithm exploits "hidden RSA" idea is described in [11].

In section 2 we introduce a concept of multiplicatively injective maps, Eulerian diagonal maps and an idea of their use for the construction of cryptosystems.

2 On Eulerian public key schemes

We refer to the equation $x^\alpha = b$ in the field F_q as *Eulerian equation* if $(\alpha, q-1) = 1$. It is well known that this equation has a unique solution.

We say that multivariate map $F : {F_q}^n \to {F_q}^n$ is *Eulerian map* over field if F is injective on $\Omega = {F_q}^*)^n$ and equation $F((\mathrm{x}) = \mathrm{b}, \mathrm{x} \in \Omega$ has exactly one solution.

Similar idea of Eulerian map over Z_m is presented in [10] and [11].

In this paper we suggest encryption scheme based on the following idea of diagonal Eulerian transformation of the affine space over F_q. We say that the polynomial map G of ${F_q}^n$ to ${F_q}^n$ is multiplicatively injective if its restriction on ${F_q}^{*n}$ is injective. So bijective polynomial maps and Eulerian maps are multiplicatively injective.

Let us consider a transformation $\tau_{A,i_1,i_2,\ldots,i_n}$ of ${F^*}_q^n$ to itself of kind $x_i \to y_i$, where

$y_{i_1} = {x_{i_1}}^{a_{11}}$,

$y_{i_2} = {x_{i_1}}^{a_{21}} {x_{i_2}}^{a_{22}}$,

$\ldots$

$y_{i_n} = {x_{i_1}}^{a_{n1}} {x_{i_2}}^{a_{n2}} \dots {x_{i_n}}^{a_{nn}}$,

where $(a_{ii}, q-1) = 1$ for $i = 1, 2, \dots, n$, $0 \le a_{i,j} < q-1$ and sequence L of elements $i_1, i_2, \dots, i_n$ is a permutation on $\{1, 2, \dots, n\}$. Let A be a triangular matrix with entries $a_{i,j}$ as above. We refer to a map of kind $\tau_{A,L}S$, where S is a monomial linear transformation $x_i \to \lambda_i x_{\pi(i)}$ for which $\lambda_i \in {F_q}^*$, $i = 1, 2, \dots, n$ and π is a permutation on $\{1, 2, \dots, n\}$ as monomial Eulerian map $E_{\tau_{A,L},S}$. We say that τ is Eulerian element if it is a composition of several monomial Eulerian maps. It is clear that τ sends variable x_i to a certain monomial term. The decomposition of τ into product of Eulerian monomial transformations $\tau_1 = \tau_{A_1,L_1}, S_1$, $\tau_2 = \tau_{A_2,L_2}, S_2$, $\dots$, $\tau_k = \tau_{A_k,L_k}, S_k$ allows us to find the solution of equations $\tau(\mathrm{x}) = \mathrm{b}$ for $\mathrm{x} \in {F^*_q}^n$. Really we have to find $\mathrm{b_k}$ from the condition $\tau_k(\mathrm{b}_k) = \mathrm{b}$, compute b_{k-1} from the condition $\tau_{k-1}(\mathrm{b}_{k-1}) = \mathrm{b_k}$, $\dots$, $\mathrm{x} = \mathrm{b}_1$ from the condition $\tau_1(\mathrm{b}_1) = \mathrm{b}_2$. Assume that a polynomial transformation F of ${F_q}^n$ written in standard form has a polynomial degree d (maximal degree of monomial terms) and polynomial density. We can take a bijective affine map T of ${F_q}^n$ to itself and form the map $G = \tau F T$ of finite degree bounded by some linear function in variable n. We refer to G as Eulerian deformation of F. If F has density of size $O(n^t)$ then the density of G is $O(n^{t+1})$.

It is clear that the Eulerian deformation of multiplicatively injective map over the finite field is also multiplicatively injective transformation.

Let us consider the asymmetrical encryption scheme based on the pair F, D, where F is multiplicatively injective transformation of ${F_q}^n$ and D is the data (private key) which allows to solve the equation $F(\mathrm{x}) = b$ for $\mathrm{x} \in \Omega$ in polynomial time.

As usually key holder Alice has (F, D) and public user Bob has only the map F in standard form. So Bob forms plaintext $\mathrm{p} \in \Omega$ and sends the ciphertext $\mathrm{c} = F(\mathrm{p})$ to Alice. Alice uses D and solves $F(\mathrm{x}) = \mathrm{c}$ for unknown tuple x for the decryption.

Let us consider the modification of the above scheme via Eulerian deformation $G = \tau F T$, Alice will use new data D' obtained by adding maps τ, S, T to D. Alice sends the encryption rule G to public user Bob. Bob sends $\mathrm{c} = G(\mathrm{p})$. Alice computes $\mathrm{d} = T^{-1}\mathrm{c}$. She forms tuple of unknowns $\mathrm{y} = (\mathrm{y}_1, \mathrm{y}_2, \dots, \mathrm{y_n})$. She uses data D to get the solution b of $F(\mathrm{y}) = \mathrm{d}$. Finally, she computes the b' as $S^{-1}(\mathrm{b})$ and gets the plaintext as a solution of Eulerian system $\tau \mathrm{x} = \mathrm{b}'$. This scheme can be applied to various known pairs (F, D), where F is bijective map. For instance we can take stable cubical transformation of K^n into itself defined into [12] or [13] in case when $K = F_q$ for chosen parameter q or nonstable maps of [6].

In this paper we concentrate on Eulerian maps, when D contains information on triangular system of Eulerian equations over F_q of kind

$h_1(x_{i_1}) = a_1 {x_{i_1}}^{\alpha_{11}} + b_1 = c_1$

$h_2(x_{i_1}, x_{i_2}) = a_2 {x_{i_1}}^{\alpha_{21}} {x_{i_2}}^{\alpha_{22}} + b_2(x_{i_1}) = c_2$

$\dots$

$h_s(x_{i_1}, x_{i_2}, \dots, x_{i_s}) = a_s {x_{i_1}}^{\alpha_{s1}} {x_{i_2}}^{\alpha_{s2}} \dots {x_{i_s}}^{\alpha_{ss}} + b_s(x_{i_1}, x_{i_2}, \dots, x_{i_{s-1}}) = c_s$,

where $b_1 \in F_q$, $b_2 \in F_q[x_1]$, $\dots$, $b_s \in F_q[x_1, x_2, \dots, x_{s-1}]$, a_j, $j = 1, 2, \dots, s$ are nonzero elements of F_q, $i_1, i_2, \dots, i_s$ is a permutation on $\{1, 2, \dots, s\}$, $(\alpha_{ii}, q-1) = 1$, $i = 1, 2, \dots, s$.

We refer to the map $F : x_j \to h_j(x_{i_1}, x_{i_2}, \ldots, x_{i_s})$, $j = 1, 2, \ldots, s$ as triangular Eulerian map.

Assume that α_{ii}, $i = 1, 2, \ldots, s$ are unknown. Other coefficients are available together with the solution $d_1, d_2, \ldots, d_s$. Then finding α_{ii}, $i = 1, 2, \ldots, s$ can be done via consequtive solution of discrete logarithm problem:

${d_1}^x = (c_1 - b_1)/a_1$ and $x = \alpha_{11}$, ${d_2}^x = (c_2 - b_2(d_1))/(a_2 {d_1}^{\alpha_{11}})$ and $x = \alpha_{22}$, ..., ${d_s}^x = (c_s - b_s(d_1, d_2, \ldots, d_{s-1}))/(a_s {d_1}^{\alpha_{11}} {d_2}^{\alpha_{22}} \ldots d_{s-1}^{\alpha_{s-1,s-1}})$.

In the case when parameter q is large the determination of discrete logarithm is a known hard problem.

Notice that parameters $\alpha_{i,j}$ (as well as $a_{i,j}$ of the diagonal affine transformation) will be unknown for the public user Bob in the described above cryptosystem. So we can talk about hidden discrete logarithm.

EXAMPLE 1.

Let us consider a cryptosystem based on the deformation of written above Eulerian triangular map F of ${F_q}^n$. The map F is defined by parameters $a_1, a_2, \ldots, a_n$ from ${F_q}^*$, triangular matrices A and a list of elements $b_1 \in F_q$,$b_2(z_1) \in F_q[z_1]$, $b_3(z_1, z_2) \in F_q[z_1, z_2]$, ..., $b_n(z_1, z_2, \ldots, z_{n-1}) \in F_q[z_1, z_2, \ldots, z_{n-1}]$. Polynomials b_i of constant degrees t_i can be specially chosen to make the density of F of prescribed size $O(n^d)$ for certain constant d. We can choose matrix A to make the degree of F bounded by some constant t.

Alice takes sequence of triangular matrices A_1, A_2, ..., A_k and linear orders $L_1, L_2, \ldots, L_k$ on $\{1, 2, \ldots, n\}$ to form Eulerian diagonal transformations τ_{A_i,L_i} of constant degree t_i.

She takes strings ${\lambda_1}^i$, ${\lambda_2}^i$, ..., ${\lambda_n}^i$ and permutations π_i to form monomial linear transformations S_i, $i = 1, 2, \ldots, k$. Alice chooses matrix B and vector c to form bijective affine transformation T sending $\mathrm{x} = (x_1, x_2, \ldots, x_n)$ into $\mathrm{x}B + \mathrm{c}$.

Alice computes the polynomial map $G = \tau_{A_1,L_1} S_1 \tau_{A_2,L_2} S_2 \ldots \tau_{A_k,L_k} S_k F T$ and writes G in standard form. The degree of G is bounded by $t_1 t_2 \ldots t_k t$ and its density is of size $O(n^{t+1})$. Alice sends the standard form of G to public user Bob.

Bob writes a plaintext $\mathrm{p} = (p_1, p_2, \ldots, p_n) \in {F_q}^{*n}$. He computes the ciphertext $G(\mathrm{p})$ and sends it to Alice.

Alice uses her knowledge on the decomposition $G = \tau_{A_1,L_1} S_1 \tau_{A_2,L_2} S_2 \ldots \tau_{A_k,L_k} S_k F T$. So she computes $\mathrm{c}_0 = T^{-1}(\mathrm{c})$. She solves the equation $\mathrm{F(z)}= \mathrm{c}_0$ for z. Notice that the solution c_k is an element of ${F^*}_q$. Alice gets the solution c_{k-1} of the equation $\tau_{A_k,L_k}(\mathrm{z}) = {S_k}^{-1}(\mathrm{c}_k)$. She creates inductively c_{k-j} as a solution of $\tau_{A_{k-j+1},L_{k-j+1}}(\mathrm{z}) = {S_{k-j+1}}^{-1}(\mathrm{c}_{k-j+1})$ for $j = 2, 3, \ldots, k-1$. We can see that c_1 is the plaintext.

EXAMPLE 2. Let K be a commutative ring. We define $A(n, K)$ as bipartite graph with the point set $P = K^n$ and line set $L = K^n$ (two copies of a Cartesian power of K are used).

We will use brackets and parenthesis to distinguish tuples from P and L. So $(\mathrm{p}) = (p_1, p_2, \ldots, p_n) \in P_n$ and $[\mathrm{l}] = l_1, l_2, \ldots, l_n) \in L_n$. The incidence relation $I = A(n, K)$ (or corresponding bipartite graph I) is given by condition $\mathrm{p}I\mathrm{l}$ if and only if the equations of the following kind hold.

$p_2 - l_2 = l_1 p_1$

$p_3 - l_3 = p_1 l_2$
$p_4 - l_4 = l_1 p_3$
$p_5 - l_5 = p_1 l_4$
...
$p_n - l_n = p_1 l_{n-1}$ for odd n
$p_n - l_n = l_1 p_{n-1}$ for even n

Let us consider the case of finite commutative ring K, $|K| = m$.

As it instantly follows from definition the order of our bipartite graph $A(n, K)$ is $2m^n$. The graph is m-regular. Really, the neighbour of given point p is given by above equations, where parameters $p_1, p_2, \ldots, p_n$ are fixed elements of the ring and symbols $l_1, l_2, \ldots, l_n$ are variables. It is easy to see that the value for l_1 could be freely chosen. This choice uniformly establishes values for $l_2, l_3 \ldots, l_n$. So each point has precisely m neighbours. In similar way we observe the neighbourhood of the line, which also contains m neighbours. We introduce the colour ρ(p) of the point p and the colour ρ(l) of line l as parameter p_1 and l_1 respectively. Graphs $A(n, K)$ with colouring belong to class of linguistic graphs defined in [14]. In the case of linguistic graph Γ the path consisting of its vertices v_0, v_1, v_2, ..., v_k is uniquely defined by initial vertex v_0 and colours $\rho(v_i)$, $i = 1, 2, \ldots, k$ of other vertices from the path.

So the following symbolic computation can be defined. Take the symbolic point x $= (x_1, x_2, \ldots, x_n)$ where x_i are variables and symbolic key which is a string of polynomials $f_1(x)$, $f_2(x)$, ..., $f_s(x)$ from $K[x]$. Form the path of vertices $v_0 =$ x, v_1 such that $v_0 I v_1$ and $\rho(v_1) = f_1(x_1)$, v_2 such that $v_1 I v_2$ and $\rho(v_2) = f_2(x_1)$, ..., v_s such that $v_{s-1} I v_s$ and $\rho(v_s) = f_s(x_1)$. We use term *symbolic point to point computation* in the case of even k and talk on *symbolic point to line* computation in the case of odd k. We notice that the computation of each coordinate of v_i via variables $x_1, x_2, \ldots, x_n$ and polynomials $f_1(x)$, $f_2(x)$, ..., $f_i(x)$ needs only arithmetical operations of addition and multiplication. Final vertex v_s (point or line) has coordinates $(h_1(x_1), h_2(x_1, x_2), h_3(x_1, x_2, x_3), \ldots, h_n(x_1, x_2, \ldots, x_n))$, where $h_1(x_1) = f_s(x_1)$.

Assume that $K = F_q$ (m=q) and the equation of kind $f_s(x) = b$ has at most one solution under condition that $x \in F^*{}_q$. Then the map $H : x_i \to h(x_1, x_2, \ldots, x_i)$, $i = 1, 2, \ldots, n$ is a multiplicatively injective map. If the equation of kind $f_s(x) = b$, $x \in F^*{}_q$ has the unique solution then H is bijection.

In the case of finite parameter s and finite densities of $f_i(x)$, $i = 1, 2, \ldots, s$ the map H also have finite density. If all parameters $\deg(f_i(x))$ are finite then the map H has a linear degree. For simplicity we set $f_s(x) = ax^r + b$, where $(r, q-1)) = 1$. It means that we can substitute kernel map F in the case of example 1 by map H. The map $G = \tau_{A_1,L_1} S_1 \tau_{A_2,L_2} S_2 \ldots \tau_{A_s,L_s} S_k H T$ written in standard form has linear density and constant degree.

Let $N_{g(x)}$ be the operator on $P \cup L$ be the operator sending vertex $(x_1, x_2, \ldots, x_n)$ (point or line) to its neighbour of colour $g(x_1)$. In the case of symbolic key defined via choice of $f_1(x)$ and recurrent relations of kind $f_{i+1}(x) = g_i(f_i(x))$, $i = 1, 2, \ldots, s-1$ the map H is a composition of $N_1 = N_{f_1(x)}$, $N_2 = N_{g_1}$, $N_3 = N_{g_2}$, ..., $N_s = N_{g_{s-1}}$. So in the case of bijective map $N_1 N_{2s}$ is an example of invertible decomposition of H in sense of [4].

The following cases of maps with prescribed density can be also used for the implementations.

1) Let in the case of even s we have $f_i(x) = h(x) + b_i$ for odd $i = 1, 3, \ldots, s-1$ where $h(x)$ has a chosen degree α. For even $i = 2, 4, \ldots, s$ we set $f_i(x) = x + c_i$. From results of [15] we can deduce that degree of H is $2\alpha + 1$. It is easy to see that H is bijective. Let T_1 be bijective affine transformation of the free module ${F_q}^n$. One can take the composition $H_1 = T_1 H$. Independently from the size of $s = l(n)$ the degree of H_1 is $t = 2\alpha + 1$. So its density is $O(n^t)$.

It means that we can substitute kernel map F in the case of example 1 by map $T_1 H$. The map $G = \tau_{A_1,L_1} S_1 \tau_{A_2,L_2} S_2 \ldots \tau_{A_s,L_s} S_s H_1 T$ written in standard form density $\mathrm{O(n}^{t+1})$.

2) Let us choose odd parameter s. As in the case above $f_i(x) = h(x)+b_i$ for odd $i = 1, 3, \ldots, s$ and for even $i = 2, 4, \ldots, s-1$ equalities $f_i(x) = x+c_i$ hold. We set $h(x) = ax^r+b$, , $a \in {F_q}^*$. So the map H is multiplicatively injective. We can check that the degree of H is $t = \alpha+2$. Let T_2 be a bijective affine transformation of ${F_q}^n$ of kind $x_1 \to \lambda x_1$, $x_2 = l_2(x_1, x_2, \ldots, x_n)$, $x_3 = l_3(x_1, x_2, \ldots, x_n)$, $\ldots$, $x_n = l_n(x_1, x_2, \ldots, x_n)$, where $\lambda \in {F_q}^*$ and $l_i \in F_q[x_1, x_2, \ldots, x_m]$ are of degree 1. We set $H_2 = T_2 H$. The encryption map $G = \tau_{A_1,L_1} S_1 \tau_{A_2,L_2} S_2 \ldots \tau_{A_s,L_s} S_s H_2 T$ has density $O(n^{\alpha+3})$.

MODIFIED EXAMPLES 1 and 2.

One can change the field F_q in examples 1 and 2 for ring Z_m, where m is some composite number. It leads to change of ${F^*}_q$ for Z_m^*, integer $q-1$ for $\phi(m)$, where ϕ is Euler function, graph $A(n, F_q)$ for $A(n, Z_m)$. Detailed description is in [16].

[1] Ding J. , Gower J.E., Schmidt D. S., Multivariate Public Key Cryptosystems, - Springer, Advances in Information Security, V. 25, 2006, - 259 p.

[2] Goubin L., Patarin J., Bo-Yin Yang, Multivariate Cryptography. Encyclopedia of Cryptography and Security, (2nd Ed.) 2011, pp. 824-828.

[3] Porras J., Baena J., Ding J., New Candidates for Multivariate Trapdoor Functions // Revista Colombiana de Matematicas, 2015 (November), vol. 49, No 1, pp 57-76 .

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

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

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

[7] Kipnis A., Shamir A., Cryptanalisis of the Oil and Vinegar Signature Scheme // Advances in Cryptology - Crypto 96, Lecture Notes in Computer Science, Vol. 1462, 1996, pp 257–266.

[8] Bulygin S., Petzoldt A. and Buchmann J., Towards provable security of the unbalanced oil and vinegar signature scheme under direct attacks, In Guang Gong and Kishan Chand Gupta, editors, "Progress in Cryptology - INDOCRYPT", Lecture notes in Computer Science, Vol. 6498, 2010. pp. 1732.

[9] Romaczuk-Polubiec U., Ustimenko V., On two windows multivariate cryptosystem depending on random parameters // Algebra and Discrete Mathematics, 2015, Vol. 19, No. 1., pp. 101–129.

[10] Ustimenko V., On Shubert cells in grassmanians and new algorithm of multivariate cryptography // Proceedings of Institute of Mathematics, Minsk, 2015, Vol. 23, no 2, pp 137-148.

[11] Ustimenko V., On algebraic graph theory and nonbijective maps in cryptography // Algebra and Discrete Mathematics, 2015, Vol. 20, no 1, pp. 152170.

[12] Ustimenko V., Wroblewska A., On the key exchange with nonlinear polynomial maps of stable degree // Annalles UMCS Informatica, 2011, AI XI, no 2, pp. 81-93.

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

[14] Wroblewska A., On some properties of graph based public keys // Albanian Journal of Mathematics, 2008 Vol. 2, no 3, pp. 229-234 (proceedings of NATO Advanced Studies Institute: "New challenges in digital communications").

[15] Ustimenko V. A., Maximality of affine group and hidden graph cryptosystems // J. Algebra and Discrete Math., 2005, no 1, pp. 133-150.

[16] Ustimenko V. A., On new multivariate cryptosystems based on hidden Eulerian equations // Dopovidi National Academy of Sci of Ukraine, N2 (in English, to appear in N5, 2017)