Algebra and Discrete Mathematics RESEARCH ARTICLE
Volume **23** (2017). Number 2, pp. 331–348

On new multivariate cryptosystems with nonlinearity gap*

Vasyl Ustimenko

Communicated by V. Nekrashevych

This paper is dedicated to the memory of V. I. Sushchansky whose research and teaching contributed greatly to the development of Group Theory in Ukraine and Poland

Abstract. The pair of families of bijective multivariate maps of kind F_n and ${F_n}^{-1}$ on affine space K^n over finite commutative ring K given in their standard forms has a nonlinearity gap if the degree of F_n is bounded from above by independent constant d and degree of F^{-1} is bounded from below by c^n, $c > 1$. We introduce examples of such pairs with invertible decomposition $F_n = {G^1}_n {G^2}_n \dots {G^k}_n$, i.e. the decomposition which allows to compute the value of F^{n-1} in given point $\mathrm{p} = (p_1, p_2, \dots, p_n)$ in a polynomial time $O(n^2)$.

The pair of families F_n, F'_n of nonbijective polynomial maps of affine space K^n such that composition $F_n F'_n$ leaves each element of ${K^*}^n$ unchanged such that $\deg(F_n)$ is bounded by independent constant but $\deg(F'_n)$ is of an exponential size and there is a decomposition ${G^1}_n {G^2}_n \dots {G^k}_n$ of F_n which allows to compute the reimage of vector from $F({K^*}^n)$ in time $0(n^2)$. We introduce examples of such families in cases of rings $K = F_q$ and $K = Z_m$.

*This research is partially supported by the grant PIRSES-GA-2013-612669 of the 7th Framework Programme of European Commission.

2010 MSC: 12Y05, 12Y99, 05C81, 05C85, 05C90, 94A60, 14G50.

Key words and phrases: multivariate cryptography, linguistic graphs, multivariate stable maps.

1. Foreword

Professor Sushchansky was well respected member of the community of algebraists in the former Soviet Union. His impact on the development of infinite group theory and permutation group theory in Ukraine and Poland is a very valuable one. It is difficult to overestimate his educational and research influence on students and graduate students of the Department of Mechanics and Mathematics of Kiev State Taras Shevchenko University. Many of them chose to work in Mathematics as their future profession because ofa friendly and efficient help of V. Sushchansky during their first individual research projects. During his work in Kiev State Taras Shevchenko University and Silesian Technical University professor V. Suschansky supervised many PhD theses, conducted joint research with colleagues, organised work of Research Seminars, Workshops and Conferences

I have a privilege to know V. Suschansky as my University lecturer, supervisor of research seminar and a colleague. In 1970 L. A. Kaluzhnin and V. I Sushchansky organized research seminar for undergraduate students at the department of mathematics and mechanics of Kiev State Taras Shevchenko University. The topic was algebraic combinatorics and permutation group theory. Supervisors of this seminar thought that the combination of individual students research with studies of modern mathematics has to be started at the first year of university program. It was informal seminar not listed in the official schedule of studies. V. A. Vyshensky quite often join the supervisors and assisted them in the discussion of student presentations.

Students refereed shapters or smaler units from Marshall Hall's "Combinatorics" on classical results on block design. The manuscript of P. Delsart "Algebraic Approach to Association Schemes of Coding Theory" was used together with well known books "Permutation groups", and "Permutation groups through invariant relations". Time to time students refereed some chapters of "Group Theory" by Otto Shmidt. In fact the seminar was a continuation of research studies started by O. J. Schmidt in Kiev.

Due to V. I. Sushchansky seminar participants got skills of professional work in mathematics, such as step by step check of proofs, construction of their own mathematical arguments, construction of counterexamples, break of research tasks into natural chain of subtasks. I would rather say that L. A. Kaluzhnin was responsible for seminar ideology but the working engine was V. I. Sushchansky.

Rather large group of students participators later finished their PhD theses. Sergij Ovsienko made a valuable contributed to the development of the Department of Algebra as a professor of Kiev University. Olexander Ganushkin continued his service at this department. Felix Lazebnik is a profesor of Delaware University (USA), Michiel Musychuk is a professor of Bar Ilan University (Israel). Not all participants became algebraists. Julia Mishura is a Head of Probability Department of Kiev University, Juriy Kondratiev is a Professor of Bielefeld University. Part of seminarists chose Computer Science: Platon Beletsky is a leading specialist of Quick Turn Corporation (Silicon Valley, California), Volodymir Medvedev works in Canada, V. Zdan-Poushkin and Ju. Dmitruk are working in Kiev as specialists in Applied Informatics. Irina Pankratova is a Teacher and Administrator of specialised High Schools in Physics and Mathematics (Specialised Boarder School in Physics and Mathematics and Sliceum N39).

All of them are grateful to Vitaliy Ivanovich Sushchansky as their devoted teacher.

Activity of above mentioned research seminar was closely connected with applied research project in Computer Science of Science Research Division of Kiev University conducted by L.A. Kaluzhnin and V.I. Sushchansky for the collaboration with Institute of Cybernetics (National Academy of Science of Ukraine, Department of Anatoliy Oleksandrovich Stogniy). The title of this Project was “Algebraic theory of combinatorial objects and its applications”. Since the middle of 70-th till the completion of the project in 1986 Vitaliy Suschansky was the Principal Investigator of the program. From the very beginning the project was conducted in cooperation with All Union Institute of System Studies (Moskow). This cooperation was coordinated by V. I. Suschanskiy (Kiev University group), Mykola Myhailovych Glazunov (Institute of Cybernetics in Kiev) and Igor Oleksandrovich Faradjev (Head of Department at the Institute of System Studies). The valuable contribution to the project was added by Myhailo Haimovich Klin who was a PhD student of L.A. Kaluzhnin and enthusiastic developer of Algebraic Combinatorics. In the framework of the project various methods of presentation of finite distance regular metrics and corresponding permutation groups in the computer memory, various methods of generation of permutation groups were investigated.

The project was completed in 1985, but the continuation of this research and further steps in this direction were implemented by a research school created by Vital Ivanovich Sushchanskiy. Some results of the above mentioned project reflected in volume [17] published by Institute of Cybernetics of National Academy of Science, two volumes published by Institute of System Studies (Moscow), some papers in Ukrainian Mathematical Journals and Cybernetics Journal. I have to mention that in the Soviet Union only one handbook for students on Permutation Group Theory written by L. A. Kaluzhnin and V. I. Sushchansky titled as "Transformation and Permutation" was published. The research of our department of Algebra and Discrete Mathematics is mainly directed to applications of the Permutation Group Theory and Algebraic Combinatorics to develop cryptographic algorithms. We together with many other colleagues from Ukraine, Poland, USA and other countries continue research started in Kiev by L.A. Kaluzhnin and V. I. Sushchansky.

2. On post quantum and multivariate cryptography and algebraic graph theory

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 take into account 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 based 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 an algorithm with a resistance to cryptoanalytic attacks based on an 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 the 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 was 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 a 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 pseudorandom 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 a 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 $\geqslant 3$ 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 $n = k(k-1)/2$, $k \geqslant 2$ 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 which exploits ”hidden RSA” idea is described in [11].

3. 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 a field if F is an injective on $\Omega = {F_q}^{*n}$ and equation $F(\mathrm{x}) = b$, $\mathrm{x} \in \Omega$ has exactly one solution.

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

In this paper we suggest an 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

$$
\begin{aligned}
y_{i_1} &= {x_{i_1}}^{a_{11}},\\
y_{i_2} &= {x_{i_1}}^{a_{21}}{x_{i_2}}^{a_{22}},\\
&\ldots\\
y_{i_n} &= {x_{i_1}}^{a_{n1}}{x_{i_2}}^{a_{n2}}\ldots{x_{i_n}}^{a_{nn}},
\end{aligned}
$$

where $(a_{ii}, q-1) = 1$ for $i = 1, 2, \ldots, n$, $0 \leqslant a_{i,j} < q-1$ and sequence L of elements $i_1, i_2, \ldots, i_n$ is a permutation on $\{1, 2, \ldots, n\}$. 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 $\lambda_i \in {F_q}^*$, $i = 1, 2, \ldots, n$ and π is a permutation on $\{1, 2, \ldots, n\}$ 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 $\tau_1 = \tau_{A_1,L_1,S_1}$, $\tau_2 = \tau_{A_2,L_2,S_2}, \ldots, \tau_k = \tau_{A_k,L_k,S_k}$ 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 $\tau_{k-1}(\mathrm{b}_{k-1}) = \mathrm{b_k}, \ldots, \mathrm{x} = \mathrm{b}_1$ 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 a density of a 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 a polynomial time.

As usual 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 $\mathrm{y} = (\mathrm{y}_1, \mathrm{y}_2, \ldots, \mathrm{y}_\mathrm{n})$. 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 a bijective map. For instance we can take a 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

$$
\begin{aligned}
h_1(x_{i_1}) &= a_1 {x_{i_1}}^{\alpha_{11}} + b_1 = c_1,\\
h_2(x_{i_1}, x_{i_2}) &= a_2 {x_{i_1}}^{\alpha_{21}} {x_{i_2}}^{\alpha_{22}} + b_2(x_{i_1}) = c_2,\\
&\ldots\\
h_s(x_{i_1}, x_{i_2}, \ldots, x_{i_s}) &= a_s {x_{i_1}}^{\alpha_{s1}} {x_{i_2}}^{\alpha_{s2}} \ldots {x_{i_s}}^{\alpha_{ss}} + b_s(x_{i_1}, x_{i_2}, \ldots, x_{i_{s-1}}) = c_s,
\end{aligned}
$$

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

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:

$$
{d_1}^x = (c_1 - b_1)/a_1 \quad \text{and} \quad x = \alpha_{11},
$$

$$d_2{}^x = (c_2 - b_2(d_1))/(a_2 d_1{}^{\alpha_{11}})$$

and

$$x = \alpha_{22}, \dots, d_s{}^x = (c_s - b_s(d_1, d_2, \dots, d_{s-1}))/(a_s d_1{}^{\alpha_{11}} d_2{}^{\alpha_{22}} \dots d_{s-1}^{\alpha_{s-1,s-1}}).$$

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 $a_1, a_2, \dots, a_n$ from $F_q{}^*$, triangular matrices A and a list of elements $b_1 \in F_q$,$b_2(z_1) \in F_q[z_1]$, $b_3(z_1, z_2) \in F_q[z_1, z_2]$, $\dots$, $b_n(z_1, z_2, \dots, z_{n-1}) \in F_q[z_1, z_2, \dots, z_{n-1}]$. 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, $\dots$, A_k and linear orders $L_1, L_2, \dots, L_k$ on $\{1, 2, \dots, n\}$ to form Eulerian diagonal transformations τ_{A_i,L_i} of constant degree t_i.

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

Alice computes the polynomial map

$$G = \tau_{A_1,L_1} S_1 \tau_{A_2,L_2} S_2 \dots \tau_{A_k,L_k} S_k F T$$

and writes G in standard form. The degree of G is bounded by $t_1 t_2 \dots t_k t$ 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 $\mathrm{p} = (p_1, p_2, \dots, p_n) \in F_q{}^{*n}$. He computes the ciphertext $G(\mathrm{p})$ and sends it to Alice.

Alice uses her knowledge on the decomposition

$$G = \tau_{A_1,L_1} S_1 \tau_{A_2,L_2} S_2 \dots \tau_{A_k,L_k} S_k F T.$$

So she computes $\mathrm{c}_0 = T^{-1}(\mathrm{c})$. She solves the equation $F(\mathrm{z}) = c_0$ 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.

$$\begin{aligned} p_2 - l_2 &= l_1 p_1 \\ p_3 - l_3 &= p_1 l_2 \\ p_4 - l_4 &= l_1 p_3 \\ p_5 - l_5 &= p_1 l_4 \\ &\ldots \\ p_n - l_n &= \begin{cases} p_1 l_{n-1} & \text{for odd } n \\ l_1 p_{n-1} & \text{for even } n \end{cases} \end{aligned}$$

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 a 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 a similar way we observe the neighbourhood of the line, which also contains m neighbours. We introduce the colour $\rho(\mathrm{p})$ of the point p and the colour $\rho(\mathrm{l})$ of line l as parameters p_1 and l_1 respectively. Graphs $A(n, K)$ with colouring ρ belong to the class of linguistic graphs defined in [14]. In the case of a 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 $\mathrm{x} = (x_1, x_2, \ldots, x_n)$ 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 $v_0 = \mathrm{x}$, v_1 such that $v_0 I v_1$ and $\rho(v_1) = f_1(x_1)$, v_2 such that

v_1Iv_2 and $\rho(v_2) = f_2(x_1)$, ..., v_s such that $v_{s-1}Iv_s$ 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 $x_1, x_2, \dots, x_n$ 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 $(h_1(x_1), h_2(x_1, x_2), h_3(x_1, x_2, x_3), \dots, h_n(x_1, x_2, \dots, x_n))$, 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 $H : x_i \to h(x_1, x_2, \dots, x_i)$, $i = 1, 2, \dots, n$ is a multiplicatively injective map. If the equation of a 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 $f_i(x)$, $i = 1, 2, \dots, s$ the map H also has 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 $G = \tau_{A_1,L_1}S_1\tau_{A_2,L_2}S_2 \dots \tau_{A_s,L_s}S_kHT$ written in standard form has a linear density and a constant degree.

Let $N_{g(x)}$ be the operator on $P \cup L$ be the operator sending vertex $(x_1, x_2, \dots, x_n)$ (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 $f_{i+1}(x) = g_i(f_i(x))$, $i = 1, 2, \dots, s-1$ 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 $N_1N_2 \dots N_s$ is an example of invertible decomposition of H in a 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 $i = 1, 3, \dots, s-1$ where $h(x)$ has a chosen degree α. For even $i = 2, 4, \dots, s$ 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 $H_1 = T_1H$. 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_1H. The map $G = \tau_{A_1,L_1}S_1\tau_{A_2,L_2}S_2 \dots \tau_{A_s,L_s}S_sH_1T$ written in a standard form has density $O(n^{t+1})$.

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 $H_2 = T_2H$. The encryption map $G = \tau_{A_1,L_1}S_1\tau_{A_2,L_2}S_2\ldots\tau_{A_s,L_s}S_sH_2T$ 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 the 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].

Example 3 (From Eulerian deformation to Eulerian disturbance)**.** Let F be a triangular Eulerian map as in Example 1, τ is Eulerian Element which is a composition of Eulerian monomial maps $\tau_1, \tau_2, \ldots, \tau_k$ let S be some permutational map and G be a general multiplicatively injective map.

We refer to a transformation $G' = \tau FSG$ as Eulerian disturbance of G. Notice that G' is also multiplicatively injective map. Assume that parameter q is of polynomial size $O(n^d)$. Notice that one can form $H = \tau FS$ as the map of prescribed polynomial density and prescribed polynomial degree. If degree of G is bounded by constant then G' is a map of polynomial degree and density.

Let us investigate degree of H^{-1} in the case of bijective H. In this case H sends $(x_1, x_2, \ldots, x_l)$ to $(y_1, y_2, \ldots, y_l)$ given by rules

$$\begin{aligned} b_1{x_{(i_1)}}^{\alpha_1} + r_1 &= y_{j_1}, \\ b_2{x_{i_2}}^{\alpha_2} + r_2(x_{i_1}) &= y_{j_2}, \\ b_3{x_{i_3}}^{\alpha_3} + r_3(x_{i_1}, x_{i_2}) &= y_{j_3}, \\ &\ldots \\ b_l{x_{i_3}}^{\alpha_l} + r_l(x_{i_1}, x_{i_2}, \ldots, x_{i_{l-1}}) &= y_{j_l}, \end{aligned}$$

where α_i are mutually prime with $q^m - 1$, $r_1 \in F_{q^m}$, r_i, $i \geqslant 1$ are polynomial expressions, i_1, i_2, $\ldots$, i_l and j_1, j_2, $\ldots$, j_l form permutation of symbols from $M = \{1, 2, \ldots, l\}$ and $b_i \neq 0$ for $i = 1, 2, \ldots, l$.

Let us assume that $r_{i+1} = R(x_i)R'(x_i, x_{i-1}, \ldots, x_1)$, where $R \in F_q[x_i]$ are polynomials of degree $\geqslant 1$. The inverse map for H is defined by recurrent rules

$$\begin{aligned}(b_1{}^{-1}yj_1-r_1)^{\beta_1}&=x_{i_1}\\(b_2{}^{-1}yi_2-r_2(x_{i_1}))^{\beta_2}&=x_{i_2}\\&\dots\\(b_n{}^{-1}yj_l-r_l(x_{i_1},x_{i_2},\dots,x_{i_{l-1}})^{\beta_l}&=x_{i_l}.\end{aligned}$$

where $\beta_i\alpha_i=1\mathrm{mod}(q^m-1)$ for $i=1,2,\dots,n$.

Notice that elimination of x_{i_1} from the second equation gives us x_{i_2} written as polynomial variables $y_1,y_2,\dots,y_n$ of degree $\geqslant\beta_1\beta_2$. Elimination of x_{i_2} produces polynomial expression of x_{i_3} of degree $\geqslant\beta_1\beta_2\beta_3$. The continuation of this process produces the standard form for H^{-1} of degree $\geqslant\beta_1\beta_2\dots\beta_l$. If all parameters of β_i are $\geqslant 2$ then elimination process gives H^{-1} as a map of exponentially large degree. Of course presentation of permutation H^{-1} in polynomial form is not unique, but we have serious ground to believe that even in the case of existence of alternative presentation of this map as polynomial map of polynomial degree and density it is very hard to find such a presentation explicitly.

Notice that the degree of H^{-1} obtained via natural non linear Jordan Gauss elimination can be exponential even in the case when all parameters α_i equal 1. We just present the following example $y_n=ax_n+b$, $a\neq 0$, $y_{n-1}=x_{n-1}+x_n{}^2$, $y_{n-2}=x_{n-2}+x_{n-1}^2$, …, $y_2=x_2+x_3{}^2$, $y_1=x_1+x_2{}^2$. It is easy to see that in the written above case x_n is a linear expression from y_n, x_{n-1} is a quadratic expression from y_n and y_{n-1}, x_{n-2} is an expression of degree 4 from y_n, y_{n-1}, y_{n-2}, …, x_1 is an expression of degree 2^{n-1} from y_n, y_{n-1}, …, y_1. So in this case the degree of H^{-1} is 2^{n-1}.

Implemented examples

I1. We suggest the cryptosystem with the usage of map H given by relations $y_n=ax_n+b, a\neq 0, y_{n-1}=x_{n-1}+x_n{}^2, y_{n-2}=x_{n-2}+x_{n-1}^2+x_n{}^2$, $\dots, y_2=x_2+x_3{}^2+x_4{}^2+\dots+x_n{}^2, y_1=x_1+x_2{}^2+x_3^2+\dots+x_n{}^2$ in the case of arbitrary commutative rings K. It is implemented for rings Z_{2^7}, Z_{2^8}, F_{2^7} and F_{2^8}. These choices of ring allow to use one to one correspondence of ASCEE alphabet or binary alphabet of sizes 2^7 and 2^8 and elements of chosen ring and encrypt files with extensions .txt, .doc, .jpg and etc. It is easy to see that the degree of H^{-1} is 2^{n-1}. The cryptosystem uses operators $N_{g(x)}=N^\alpha$ on the set of vertices $P\cup L$ of graph $A(n,K)$ sending vertex $(x_1,x_2,\dots,x_n)$ (point or line) to its neighbour of colour $g(x_1)=x_1+\alpha$. Alice has to choose string $\alpha_1,\alpha_2,\dots,\alpha_s$ for some even parameter s, $s \leqslant n$ such that $\alpha_i + \alpha_{i+1}$ are regular ring elements for $i = 1, 2, \dots, s-1$ and form the composition N of N^{α_1}, N^{α_2}, $\dots$, N^{α_s}. Additionally she chooses affine transformation τ of $P = K^n$. She computes the map $G = HN\tau$ of degree $\leqslant 6$ and sends it to Bob. The density of H is bounded by n, cubical map $N\tau$ has density $O(n^3)$. It means that the density of G is $0(n^4)$.

Assume that Bob writes message (p) $= (p_1, p_2, \dots, p_n)$ computes the ciphertext (c) $= G$(p) and sends it to Alice. She computes c$'$ $= \tau^{-1}$(c). Alice can do it in time $T_1 = O(n^2)$. Secondly Alice computes recursively $N^{-\alpha_s}(\mathrm{c}') = \mathrm{c}_1$, $N^{-\alpha_{s-1}}(\mathrm{c}_1) = \mathrm{c}_2$, $\dots$, $N^{-\alpha_1}(\mathrm{c}) = \mathrm{c}_s = \mathrm{r}$. It takes her time $T_2 = 2ns$ elementary operations. We can assume that $s \leqslant n$. Alice uses equations of the definition of H and computes $\mathrm{p} = H^{-1}(\mathrm{r})$ recursively with $T_3 = O(n^2)$ operations of addition and multiplications. Decryption time is evaluated by $T_1 + T_2 + T_3$ and takes Alice $O(n^2)$ elementary operations.

I2. Other algorithm for general commutative ring $K$is the following. Alice uses transformation H given by relations $y_n = ax_n$, $a \neq 0$, $y_{n-1} = x_{n-1}x_n$, $y_{n-2} = x_{n-2}x_{n-1}x_n$, $\dots$, $y_2 = x_2x_3x_4\dots x_n$, $y_1 = x_1x_2x_3\dots x_n$ in the cases of commutative ring $K = F_{2^8}$. The cryptosystem uses the transformations N and τ from previous example (I1). The plain space here will be K^{*n}. Notice that there is natural map H' given by relations $x_n = a^{-1}y_n - b$, $x_{n-1} = y_{n-1}{x_n}^{q-2}$, $x_{n-2} = y_{n-2}x_{n-1}^{q-2}{x_n}^{q-2}$, $\dots$, $x_1 = y_1{x_2}^{q-1}{x_3}^{q-2}{x_4}^{q-2}\dots{x_n}^{q-2}$. It is easy to see that degree of H' has exponential size.

Alice chooses string $\alpha_1, \alpha_2, \dots, \alpha_s$ for some even parameter s, $s \leqslant n$ such that $\alpha_i + \alpha_{i+1} \neq 0$ for $i = 1, 2, \dots, s$ and takes transformation $N = N^{\alpha_1}N^{\alpha_2}\dots N^{\alpha_s}$ together with affine transformation τ. She forms "tame chaotical map" $G = HN\tau$ of degree $O(n)$ and of the density $O(n^3)$. Notice that $G' = \tau^{-1}N^{-1}H'$ has exponential degree. The composition GG' acts identically on K^{*n}.

Alice computes the map $HN\tau$ in its standard form and sends this map to Bob. He writes plaintext $\mathrm{p} \in K^{*n}$ and computes the ciphertext $\mathrm{c} = G(\mathrm{p})$ in polynomial time $O(n^5)$ and sends it back to Alice.

The decryption process is the following. Firstly Alice applies τ^{-1} to ciphertext c. It takes $O(n^2)$ operations. After that she computes $N^{-\alpha_s}$, $N^{-\alpha_{s-1}}$, $\dots$, $N^{-\alpha_1}$. Incidence equations allows her to make each of these s steps with $2n$ elementary transformations. Finally Alice takes vector $\mathrm{c}' = \tau^{-1}N^{-1}(\mathrm{c}) \in K^{*n}$ uses equations for H an computes the value p of H' in c$'$ with the usage of division together with addition and multiplication. This step takes less than n^2 elementary operations. We can see that recursive decryption takes time $O(n^2)$. It is implemented in the cases of fields from $\{F_{2^n}|n = 7, 8\}$ and various arithmetical rings Z_m.

Remark 1. Decryption algorithm of Alice in examples I1 and I2 can be used in a symmetric mode as a stream cipher. Users can take constant parameter s and sparce affine transformation τ which takes time $O(n)$ in execution. Transformation N can be modified as $y_n = ax_n$, $a \neq 0$, $y_{n-1} = x_{n-1}x_n$, $y_{n-2} = x_{n-2}x_{n-1}$, $\ldots$, $y_2 = x_2x_3$, $y_1 = x_1x_2x_3 \ldots x_n$ (case of I2) and $y_n = ax_n+b, a \neq 0, y_{n-1} = x_{n-1}+{x_n}^2, y_{n-2} = x_{n-2}+x_{n-1}^2$, $\ldots$, $y_2 = x_2 + {x_3}^2$, $y_1 = x_1 + {x_2}^2 + x_3 \ldots {x_n}^2$ (in the case of I1). In these forms total cipher execution takes time $O(n)$. Computer simulation demonstrates good mixing properties.

Modifications of I2 and I1 in cases of rings Z_m and F_q. One can take H given by equations

$$y_n = a_1{x_n}^{\beta_n}, \quad y_{n-1} = a_2x_{n-1}^{\beta_{n-1}}{x_n}^{\delta_n},$$
$$y_{n-2} = a_3x_{n-2}^{\beta_{n-2}}{x_{n-1}}^{\delta_{n-1}}, \quad \ldots, \quad y_2 = a_{n-1}{x_2}^{\beta_2}{x_3}^{\delta_3},$$
$$y_1 = a_nx_1^{\beta_1}{x_2}^{\delta_2}(x_3x_4 \ldots x_n)^{\delta_1},$$

where $(\beta_i, q-1) = 1$, $1 \leqslant \beta_i \leqslant q-1$, $0 \leqslant \delta_i \leqslant q-1$, $i = 1, 2, \ldots, n$ in the case of finite field F_q and $(\beta_i, \phi(m)) - 1$, $1 \leqslant \beta_i \leqslant \phi(m) - 1$, $0 \leqslant \delta_i \leqslant \phi(m) - 1$, $i = 1, 2, \ldots, n$ in the case of commutative ring Z_m.

Let us assume that parameters q and m are constants. If $\delta_1 = 0$, then degree of H is constant bounded by $2q$ and $2m$ in the case of a field and a ring respectively. In the case of field degree of the map H' has exponential size in the case of $\beta_i > 1$ for $i = 1, 2, \ldots, n$.

4. Regular valued functions and bijective encryption aps with Eulerian disturbance

We refer to a polynomial function $f(x_1, x_2, \ldots, x_r) \in K[x_1, x_2, \ldots, x_r]$, $r \geqslant 0$, where K is a commutative ring, as regular valued function if the value $f(a_1, a_2, \ldots, a_n)$ is a regular element from K^*. We say that regular valued f is separable if $f = f(x_1)f(x_2) \ldots f((x_r)$. Natural example of regular valued function in the case of $K = Z_{2^n}$ is a function of kind $f = 2g + a$, where g is an arbitrary element of $K[x_1, x_2, \ldots, x_r$.

We consider mor general totality of biregular valued functions F such that $f(a_1, a_2, \ldots, a_n) \in K*$ for $(a_1, a_2, \ldots, a_n) \in {K^*}^n$.

In this section we generalise the concept of Eulerian triangular map. We define standard regular (biregular) Jordan-Eulerian map H sending a tuple $(x_1, x_2, \dots x_n)$ to

$$(y_1, y_2, \dots, y_n) = (h_1(x_1), h_2(x_1, x_2), \dots, h_n(x_1, x_2, \dots, x_n)),$$

where

$$\begin{aligned} h_1(x_1) &= {x_1}^{\alpha_1} r_0 + b_0, \\ h_2(x_1, x_2) &= a_2(x_1){x_{i_2}}^{\alpha_2} r_1(x_1) + b_1(x_1), \\ &\dots \\ h_n(x_1, x_2, \dots, x_n) &= (x_1, x_2, \dots, x_{n-1}, {x_n}^{\alpha_n}) r_{n-1}(x_1, x_2, \dots, x_{n-1}) \\ &\quad + b_{n-1}(x_1, x_2, \dots, x_{i_{n-1}}), \end{aligned}$$

where $b_0, r_0 \in K$, $b_1, r_1 \in K[x_1]$, $\dots$, $b_{n-1}, r_{n-1} \in K[x_1, x_2, \dots, x_{n-1}]$, r_j, $j = 0, 1, 2, \dots, n-1$ are regular (biregular) valued functions $(\alpha_{ii}, q-1) = 1$, $i = 1, 2, \dots, s$.

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

We refer to $F = \pi_1 H \pi_2$, where π_1 and π_2 are permutational linear maps on K^n as regular (biregular) Jordan-Eulerian map. We say that F is homogeneous if all b_i are 0 constant functions.

Notice that regular homogeneous Jordan-Eulerian function defines a map from K^n to K^{*n}, the restriction of biregular homogeneous Jordan - Euler function on K^{*n} is a transformation of this set.

Example. Let us consider homogeneous separable regular valued map G over Z_{2^m} of kind

$$\begin{gathered} y_{j_n} = x_{i_n}, \quad y_{j_{n-1}} = x_{i_{n-1}}(2x_{i_n} + 1), \quad y_{j_{n-2}} = x_{i_{n-2}}(2x_{i_{n-1}} + 1), \\ y_{j_{n-3}} = x_{i_{n-3}}(2x_{i_{n-2}} + 1), \quad \dots, \quad y_{j_2} = x_{i_2}(2x_{i_3} + 1), \\ y_{j_1} = x_1(2x_{i_2} + 1), \end{gathered}$$

where $i_1, i_2, \dots, i_n$ and $j_1, j_2, \dots, j_n$ are two permutations of symbols $1, 2, \dots, n$.

This map is quadratic. It is clear that $\phi(2^m) = 2^{m-1}$ and the inverse to regular $a \in Z_{2^m}$ is $a^{2^{m-1}-1}$. The inverse map G^{-1} is a map of kind $x_{i_n} = y_{j_n}$, $x_{i_{n-1}} = (2y_{j_n}+1)^{2^{m-1}-1} y_{j_{n-1}}$, $x_{i_{n-2}} = (2(2y_{j_n}+1)^{2^{m-1}-1} y_{j_{n-1}}+1)^{2^{m-1}-1} y_{j_{n-2}}$, ... Recurrent computations gives us x_{i_1} as expression of kind $f(y_{j_1}, y_{j_2}, \dots, y_{j_n})$ of exponential degree $\geqslant 2^{n(m-1)}$ and large density.

References

[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 on Cryptology, 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. 17-32.

[9] Romańczuk-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 non-bijective maps in cryptography*, Algebra and Discrete Mathematics, 2015, Vol. 20, no 1, pp. 152-170.

[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).

[17] V. I. Sushchansky, V. A. Ustimenko, *On the characterization of types of Boolean functions*, in Calculations in Algebra and Combinatorics, Kiev, Inst.Cyb., NAN U, 1979, pp. 44–51.

[18] L. A. Kaluznin, V.I. Sushchansky, V. A. Ustimenko, *Exponentiation in permutation group theory and its applications*, Proceedings of the Sixth Soviet Union Conference on the group theory, Kiev, IM Ukr. Acad. Sci., 1979, pp. 135–145.

[19] L. A. Kaluznin, V. I. Sushchansky, V. A. Ustimenko, *On the system of computer programs for studies of permutation groups*, Proceedings of the Conference on Interactive Systems, Borjomi, March 1981, Tbilisi, Georgia, USSR, pp. 32–37.

[20] L. A. Kaluznin, V.I. Sushchansky, V. Ustimenko, *Computer science and its applications to the theory of permutation groups*, Kibernetika, 1982, no. 6, pp. 63–84.

Contact information

V. Ustimenko
Institute of Mathematics,
Maria Curie-Sklodowska University,
Plac Marii Curie-Skłłodowskiej 5,
20-031 Lublin, Poland
E-Mail(s): vasylustimenko@yahoo.pl
Web-page(s): umcs.pl

Received by the editors: 11.06.2017.