ДОПОВІДІ
НАЦІОНАЛЬНОЇ
АКАДЕМІЇ НАУК
УКРАЇНИ

doi: https://doi.org/10.15407/dopovidi2017.05.017
UDC 519.1, 514.128

V.A. Ustimenko

Institute of Telecommunications and Global Information Space of the NAS of Ukraine, Kiev
Maria Curie-Sklodowska University, Lublin, Poland
E-mail: vasylustimenko@yahoo.pl

On new multivariate cryptosystems based on hidden Eulerian equations

Presented by Corresponding Member of the NAS of Ukraine O.M. Trofimchuk

We propose new multivariate cryptosystems over an n-dimensional free module over the arithmetical ring Z_m based on the idea of hidden discrete logarithm for Z_m^*. These cryptosystems are based on the hidden Eulerian equations. If m is a "sufficiently large" product of at least two large primes, then the solution of the equation is hard without knowledge of the decomposition of m. In the Postquantum Era, one can solve the factorization problem for m and the discrete logarithm problem for Z_m^*. However, it does not lead to the straightforward break of such cryptosystem, because of the parameter α is unknown. Some examples of such cryptosystems were already proposed. We define their modifications and generalizations based on the idea of Eulerian transformations, which allow us to use asymmetric algorithms based on families of nonlinear multiplicatively injective maps with prescribed polynomial density and degree bounded by constant.

Keywords: *postquantum cryptography, multivariate cryptography, public keys, hidden discrete logarithm problem, hidden Eulerian equations, algebraic graphs, complexity estimates.*

1. On Post Quantum and Multivariate Cryptographies. Post Quantum Cryptography serves for the research of asymmetric cryptographical algorithms which can be potentially resistant against attacks based on the use of a quantum computer. The security of currently popular algorithms is based on the complexity of three following known hard problems: integer factorization, discrete logarithm problem, and discrete logarithm problem for elliptic curves. Each of these problems can be solved for the polynomial time by Peter Shor's algorithm for a theoretical quantum computer. Though the known nowadays experimental examples of a quantum computer are not able to attack the currently used cryptographical algorithm, cryptographers already started researches of the postquantum security. They have also count on the new results of general complexity theory.

The history of the international conferences on Post Quantum Cryptography (PQC) started in 2006. We have to note that Post Quantum Cryptography differs from Quantum Cryptography, which is based on the idea of usage of quantum phenomena to reach a better security.

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

The oldest direction is Multivariate Cryptography (see [1]), which uses a polynomial map of the 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 for many variables. Multivariate cryptography uses, as security tools, nonlinear polynomial transformations $x_1 \to f_1(x_1, x_2, ..., x_n), x_2 \to f_2(x_1, x_2, ..., x_n), ..., x_n \to f_n(x_1, x_2, ..., x_n)$ acting on the affine space K^n, where $f_i : K[x_1, x_2, ..., x_n], i = 1, 2, ..., n$ are multivariate polynomials given in the standard form, i. e., via the list of monomials in a chosen order. Important ideas in this direction are given in [2]. The density of a map F is the maximal number den(F) of monomial terms of $f_i, i = 1, 2, ..., n$. We say that den(F) is polynomial, if this parameter has size $O(n^d)$ for some positive constant d. The degree deg(F) of the map F is the maximal value of degrees $f_i, i = 1, 2, ..., n$.

Let F be a map of K^n to itself, which has the polynomial density of size $C_1 n^{d_1}$ and the polynomial degree of size $C_2 n^{d_2}$. Then the value of F on the tuple $(b_1, b_2, ..., b_n)$ can be computed by $O(n^{d_1+d_2+1})$ basic operations of the ring. The current task is the search for an algorithm with resistance to cryptoanalytic attacks based on the ordinary Turing machine. Multivariate cryptography has to demonstrate the practical security algorithm, which can compete with RSA and Diffie—Hellman protocols, which are popular methods of elliptic curve cryptography (see [1, 2]).

It is a still 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 a Turing machine and a 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 the affine space K^n. Multivariate cryptography started from studies of the potential for a special quadratic encryption multivariate bijective map of K^n, where K is an extension of a finite field F_q of characteristic 2. One of the first such cryptosystems was proposed by Imai and Matsumoto, and the cryptanalysis for this system was invented by J. Patarin. The survey on various modifications of this algorithm and corresponding cryptanalysis can be found 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, e. g., [3] and references therein).

Applications of Algebraic Graph Theory to Multivariate Cryptography were recently presented in [4]. This survey is devoted to algorithms based on bijective maps of affine spaces into ourselves. Applications of algebraic graphs to cryptography started from symmetric algorithms based on explicit constructions of the extremal graph theory and their directed analogs (see surveys [4, 5]). The main idea is to convert an algebraic graph in a finite automaton and to use pseudorandom walks on a 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 a graph depends on parameters given as special multivariate polynomials in variables depending on a 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 a rather high degree based on walks in algebraic graphs were proposed in [5].

One of the first usages of a nonbijective map of multivariate cryptography in the *oil and vinegar* cryptosystem was proposed in [6] and analyzed in [7]. Nowadays, this general idea is strongly supported by work [8] devoted to the security analysis of direct attacks on modified unbalanced oil and vinegar systems. This algorithm was patented. It seems that such systems and schemes of rainbow signatures may lead to promising Public Key Schemes of Multivariate Encryption defined over finite fields. Nonbijective multivariate sparse encryption maps of degrees of at least 3, which are based on walks on algebraic graphs $D(n, K)$ defined over general commutative rings, and their homomorphic images were proposed in [9]. A new cryptosystem with nonbijective multivariate encryption maps of the affine space Z_m^n into itself was presented at the international conference DIMA 2015. It uses the plainspace $(Z_m^*)^n$, where $n = k(k-1)/2$, $k > 1$, can be any natural number.

The private key space is formed by a sequence of general multivariate polynomials from $Z_m[x_1, x_2, ..., x_{(k-1)}]$ and a sequence of parameters $l_i, i = 1, 2, ..., k-1$, which are mutually prime with $\varphi(m)$. The properties of the encryption map depend strongly on the prime factorization of m. This nonbijective encryption map is the deformation of a special computation generated by the Schubert automaton of "$k-1$ dimensional projective geometry" over Z_m. This method does not use the partition of variables into groups, and the nonbijective nature of the map is caused by zero devisors of a composite integer m. In fact, the idea of multiple "hidden RSA" is used (see [10]). The other algorithm exploited the "hidden RSA" idea is described in [11]. In Section 2, we introduce a concept of multiplicatively injective maps, Eulerian diagonal maps, and the 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 arithmetical ring Z_m as an *Eulerian equation*, if $(\alpha, m) = 1$. We say that the multivariate map $F: Z_m^n \to Z_m^n$ is an *Eulerian map* of rank r, if F is injective on $\omega = (Z_m^*)^r Z_m^{n-r}$, the parameter r is minimal with this property, and each equation $F(\mathrm{x}) = b$ is reducible to the solution of r Eulerian equations. The first examples of such maps can be found in [11] (rank 1) and [10] (case of arbitrarily large rank).

In this paper, we suggest a scheme based on the following idea of a diagonal Eulerian transformation of the affine space over Z_m. We say that the polynomial map G of Z_m^n to Z_m^n is multiplicatively injective, if its restriction on $(Z_m^*)^n$ is injective. So, bijective polynomial maps and Eulerian maps of rank > 0 are multiplicatively injective. Let us consider a transformation $\tau_{A(i_1, i_2, ..., i_n)}$ of Z_m^n to itself of kind $x_i \to y_i$, where

$$y_{i_1} = x_{i_1}^{a_{11}},$$
$$y_{i_2} = x_{i_1}^{a_{21}} x_{i_2}^{a_{22}},$$
$$\dots\dots\dots\dots\dots$$
$$y_{i_n} = x_{i_1}^{a_{n1}} x_{i_2}^{a_{n2}} \dots x_{i_n}^{a_{nn}},$$

where $(a_{ii}, \varphi(m)) = 1$ for $i = 1, 2, ..., n; a_{i,j} \leqslant \varphi(m)$, and the sequence L of elements $i_1, i_2, ..., i_n$ is a permutation of $1, 2, ..., n$. 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 λ_i is an element of Z_m^*, $i = 1, 2, ..., n$, and π is a permutation of $(1, 2, ..., n)$, as a monomial Eulerian map $E_{\tau_{(A,L)S}}$.

We say that τ is an Eulerian element, if it is a composition of several monomial Eulerian maps. It is clear that τ sends the variable x_i to a certain monomial term. The decomposition of τ

into a product of Eulerian monomial transformations allows us to find a solution of the equations $\tau(x)=b$ for x from $(Z_m^*)^n$. Really, we have to find b_k from the condition $\tau_k(b_k)=b$ and to compute b_{k-1} from the condition $\tau_{k-1}(b_{k-1})=b_k$, ..., $x=b_1$ from the condition $\tau_1(b_1)=b_2$.

Assume that a polynomial transformation F of Z_m^n written in the standard form has a polynomial degree d (maximal degree of monomial terms) and a polynomial density. We can take a bijective affine map T of Z_m^n onto itself and form the map $G=\tau FT$ of a finite degree bounded by some linear function of the variable n.

We refer to G as an Eulerian deformation of F. If F has the density of size $O(n^t)$, then the density of G is $O(n^{t+1})$. It is clear that the Eulerian deformation of a multiplicatively injective map is also a multiplicatively injective transformation.

Let us consider the asymmetric encryption scheme based on the pair F, D, where F is a multiplicatively injective transformation of $(Z_m^*)^n$ into Z_m^n and D is the data (private key), which allows one to solve the equation $F(x)=b$ for x from $\Omega = (Z_m^*)^n$ for the polynomial time. As usual, Alice has (F, D) and the public user Bob has only a map F in the standard form. So, Bob forms the plaintext p from Ω and sends the ciphertext $c=F(p)$ to Alice. She uses D and solves $F(x)=c$ for the unknown tuple x for the decryption.

Let us consider a modification of the above scheme via the Eulerian deformation $G=\tau FT$. Alice will use new data D' obtained by adding the maps τ, S, T to D. Alice sends the encryption rule G to the public user Bob. He sends $c=G(p)$. Alice computes $d=T^{-1}(c)$. She forms the tuple of unknowns $y=(y_1, y_2, ..., yn)$. She uses the data D to get the solution b of $F(y)=d$. Finally, she computes b' as $S^{-1}(b)$ and gets the plaintext as a solution of the Eulerian system $\tau(x)=b'$.

This scheme can be applied to various known pairs (F, D), where F is a bijective map. For instance, we can take a stable cubic transformation of K^n into itself defined in [12] or [13] in the case where $K=Z_m$ for the chosen parameter m or nonstable maps [6].

Here, we concentrate on the Eulerian maps of rank s, when D contains information on the triangular system of Eulerian equations

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

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

$$\cdots\cdots\cdots$$

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

$b_1 \in Z_m, b_2 \in Z_{m[x_1]}, ..., b_s \in Z_{m[x_1, x_2, ..., x_{s-1}]}, a_j, j=1,2,...,s$, are regular elements of Z_m, $i_1, i_2, ..., i_s$ is a permutation of $\{1, 2, ..., s\}$, $(\alpha_{11}, \varphi(m))=1, i=1,2,...,s$.

We refer to the map $F: x_j \to h_j(x_{i_1}, x_{i_2}, ..., x_{i_s}), j=1,2,...,s$, as a triangular Eulerian map. Assume that $\alpha_{ii}, i=1,2,...,s$, are unknown. Other coefficients are available together with the solution d_1, d_2, ..., d_s. Then finding $\alpha_{ii}, i=1,2,...,s$, can be done via the consecutive solution of the discrete logarithm problem:

$$d_1^x=(c_1-b_1)/a_1 \text{ and } x=\alpha_{11}, d_2^x=(c_2-b_2 d_1)/a_{2_{d_1}}^{\alpha_{11}} \text{ and}$$

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

In the case where m is a large prime integer, the determination of a discrete logarithm is the known hard problem. In the case where m is a product of at least two large primes, the solution of a triangular Eulerian system is hard without knowledge of the factorization problem for integer m.

Note that the 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 above-described cryptosystem. So, we can talk on the hidden discrete logarithm problem and the hidden factorization problem for integer m.

Example 1. Let us consider a cryptosystem based on the deformation of the above-written Eulerian triangular map F of Z_m^n.

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

Alice takes a sequence of triangular matrices A_1, A_2, A_k and linear orders L_1, L_2, ..., L_k on 1, 2, ..., 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, $i = 1, 2, ..., k$. Alice chooses a matrix B and a vector c to form a bijective affine transformation T sending $x = (x_1, x_2, ..., x_n)$ into $xB + c$.

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

Alice sends the standard form of G to the public user Bob.

He writes a plaintext $p = (p_1, p_2, ..., p_n)$ from $(Z_m)^n$. He computes the ciphertext $G(p)$ and sends to Alice. She uses her knowledge on the decomposition $G = \tau_{A_1, L_1} S_1, \tau_{A_2, L_2} S_2, ..., \tau_{A_k, L_k} S_k FT$. So, she computes $c_0 = T^{-1}(c)$. She solves the equation $F(z) = c_0$ for z. Note that the solution c_k is an element of Z_m^*. Alice gets the solution c_{k-1} of the equation $\tau_{A_k, L_k} = S_k^{-1}(c_k)$. She creates inductively c_{k-j} as a solution $\tau_{A_{k-j+1}, L_{k-j+1}} = S_{k-j+1}^{-1}(c_{k-j+1})$ for $j = 2, 3, ..., k-1$. We can see that c_1 is a plaintext.

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

We will use brackets and parentheses to distinguish tuples from P and L. $S_o(p) = (p_1, p_2, ..., p_n)$ from P_n and $[l] = [l_1, l_2, ..., l_n]$ from L_n. The incidence relation $I = A(n, K)$ (or corresponding bipartite graph I) is given by condition (p) I [l] if and only if the following equations hold:

$$p_2 - l_2 = l_1 p_1,$$
$$p_3 - l_3 = p_1 l_2,$$
$$p_4 - l_4 = l_1 p_3,$$
$$p_5 - l_5 = p_1 l_4,$$
$$\ldots\ldots\ldots\ldots$$
$$p_n - l_n = p_1 l_{n-1} \text{ for odd } n,$$
$$p_n - l_n = l_1 p_{n-1} \text{ for even } n.$$

Let us consider the case of finite commutative ring K, $|K| = m$. It instantly follows from the definition that the order of our bipartite graph $A(n, K)$ is $2m^n$. The graph is m-regular. Really, the neighbor of a given point (p) is given by the above equations, where the parameters $p_1, p_2, ..., p_n$ are fixed elements of the ring, and the symbols $l_1, l_2, ..., l_n$ are variables. It is easy to see that the value for l_1 could be freely chosen. This choice uniformly establishes values for $l_2, l_3, ..., l_n$. So, each point has precisely m neighbors. In a similar way, we observe the neighborhood of the line, which also contains m neighbors. We introduce the color $\rho(p)$ of the point (p) and the color $\rho[l]$ of the line [l] as the parameters p_1 and l_1, respectively.

Graphs $A(n, K)$ with coloring ρ belong to the 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 the initial vertex v_0 and colors $\rho(v_i)$, $i = 1, 2, ..., k$, of other vertices from the path. So, the following symbolic computation can be defined. Take the *symbolic point* $(\mathrm{x}) = (x_1, x_2, ..., x_n)$, where x_i are variables, and the *symbolic key* 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 the term *symbolic point-to-point computation* in the case of even k and talk on the *symbolic point-to-line* computation in the case of odd k. We note that the computation of each coordinate of v_i via the variables $x_1, x_2, ..., x_n$ and polynomials $f_1(x), f_2(x), ..., f_s(x)$ needs only the arithmetical operations of addition and multiplication. The final vertex v_s (point or line) has coordinates $(g_1(x_1), g_2(x_1, x_2), g_3(x_1, x_2, x_3), ..., g_n(x_1, x_2, ..., x_n))$, where $g_1(x_1) = f_s(x_1)$ $g_1(x_1) = f_s(x_1)$.

Assume that the equation $f_s(x) = b$ has at most one solution under the condition that $x \in t \mid (t,m) = 1$. Then the map $H: x_i \to h(x_1, x_2, ..., x_i)$ is a multiplicatively injective map. If the equation $f_s(x) = b$, $x \in Z_m$ has the unique solution, then H is a bijection.

In the case of a finite parameter s and finite densities of $f_{i(x)}$, $i = 1, 2, ..., s$, 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 $(r, \varphi(m)) = 1$ and $(a, m) = 1$. This means that we can substitute the kernel of a map F in the case of Example 1 by the map H. The map $G = \tau_{A_1, L_1} S_1 \tau_{A_2, L_2} S_2 ... \tau_{A_s, L_s} S_{kHT}$ written in the standard form has linear density and constant degree.

Let $N_{g(x)}$ be the operator on P, and L be the operator sending the vertex $(x_1, x_2, ..., x_n)$ (point or line) to its neighbor of color $g(x_1)$. In the case of symbolic key defined via the choice of $f_1(x)$ and the recurrent relations $f_{\{i+1\}}(x) = g_i(f_i(x))$, $i = 1, 2, ..., s-1$, the map H is a composition of $N_1 = N_{f_1(x)}$, $N_2 = N_{g_1(x)}$, $N_3 = N_{g_2(x)}$, ..., $N_s = N_{g_{s-1}(x)}$. So, in the case of bijective map, $N_1 N_2 ... N_s$ is an example of the 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 $i = 1, 3, ..., s-1$, where $h(x)$ has chosen degree α. For even $i = 2, 4, ..., s$, we set $f_i(x) = x + c_i$. From results of [15], we can deduce that the degree of H is $2\alpha + 1$. It is easy to see that H is bijective. Let T_1 be a bijective affine transformation of the free module Z_m^n. One can take the composition $H_1 = T_1 H$. Independently of the size of $s = l(n)$, the degree of H_1 is $t = 2\alpha + 1$. So, its density is $O(n^t)$.

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

2) Let us choose the odd parameter s. As in the case above, $f_i(x) = h(x) + b_i$ for odd $i = 1, 3, ...,$ s, and, for even $i = 2, 4, ..., s-1$, the equalities $f_i(x) = x + c_i$ hold. We set $h(x) = ax^r + b$, and a is from

Z_m^*. So the map H is multiplicatively injective. We can check that the degree of H is $t = 2\alpha + 1$. Let T_2 be a bijective affine transformation of Z_m^n of kind $x_1 \to \lambda x_1$, $x_2 = l_2(x_1, x_2, ..., x_n)$, $x_3 = l_3(x_1, x_2, ..., x_n)$, ..., $x_n = l_n(x_1, x_2, ..., x_n)$, where $\lambda \in Z_m^*$ and l_i from $Z_m[x_1, x_2, ..., x_m]$ are of degree 1. We set $H_2 = T_2H$. The encryption map $G = \tau_{A_1, L_1} S_1 \tau_{A_2, L_2} S_2 \dots \tau_{A_s, L_s} S_s H_2 T$ has density $O(n^{\alpha+3})$.

The paper is dedicated to the memory of V.I. Sushchansky, whose research and teaching gave the outstanding contribution to the development of Group Theory in Ukraine and Poland.

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

REFERENCES

1. Ding, J., Gower, J. E. & Schmidt, D. S. (2006). Multivariate Public Key Cryptosystems, Advances in Information Security. Vol. 25. Berlin: Springer.
2. Goubin, L., Patarin, J. & Yang, Bo-Yin (2011). Multivariate Cryptography. Encyclopedia of Cryptography and Security. Berlin: Springer, pp. 824-828.
3. Porras, J., Baena, J.B. & Ding, J. (2015). New Candidates for Multivariate Trapdoor Functions. Rev. Colomb. Mat., 49, No. 1, pp. 57-76.
4. Ustimenko, V. (2015). Explicit constructions of extremal graphs and new multivariate cryptosystems. Stud. Sci. Math. Hung., 52, Iss. 2, pp. 185-204. doi: https://doi.org/10.1556/012.2015.52.2.1312.
5. Ustimenko, V. (2014). On Multivariate Cryptosystems Based on Computable Maps with Invertible Decomposition. Annales of UMCS, Informatica, 14, No. 1, pp. 7-18.
6. Patarin, J. (1997). The Oil and Vinegar digital signatures, Dagstuhl Workshop on Cryptography. Wadern.
7. Kipnis, A. & Shamir, A. (1998). Cryptanalysis of the Oil and Vinegar Signature Scheme. Advances in Cryptology-Crypto 98. Lecture Notes in Computer Science. Vol. 1462. Berlin: Springer, pp. 257-266.
8. Bulygin, S., Petzoldt, A. & Buchmann, J. (2010). G. Gong, K.C. Gupta (Ed.). Progress in Cryptology — INDOCRYPT. Lecture notes in Computer Science. Vol. 6498. Berlin: Springer, pp. 17-32.
9. Romańczuk-Polubiec, U. & Ustimenko, V. (2015). On two windows multivariate cryptosystem depending on random parameters. Algebra Discrete Math., 19, No. 1, pp. 101-129.
10. Ustimenko, V. A. (2015). On Schubert cells in Grassmanians and new algorithms of multivariate cryptography. Tr. Inst. Mat., Minsk, 23, No. 2, pp. 137-148.
11. Ustimenko, V. (2015). On algebraic graph theory and non-bijective multivariate maps in cryptography. Algebra Discrete Math., 20, No. 1, pp. 152-170.
12. Ustimenko, V. & Wroblewska, A. (2011). Performance of algebraic graphs based stream-ciphers using large finite fields. Annales of UMCS, Informatica, 11, No. 2, pp. 81-93.
13. Ustimenko, V. & Romanczuk, U. (2013). On Dynamical Systems of Large Girth or Cycle Indicator and their applications to Multivariate Cryptography. Artif. Intell., Evol. Comput. and Metaheuristics, Studies in Computational Intelligence. Vol. 427. Berlin: Springer, pp. 231-256.
14. Wroblewska, A. (2008). On some properties of graph based public keys. Albanian J. Math., 2, No. 3, pp. 229-234.
15. Ustimenko, V. A. (2005). Maximality of affine group, and hidden graph cryptosystem. Algebra Discrete Math., No. 1, pp. 133-150.

Received 16.11.2016

В.О. Устименко

Інститут телекомунікацій і глобального інформаційного простору НАН України, Київ
Університет Марії Кюрі-Склодовської, Люблін, Польща
E-mail: vasylustimenko@yahoo.pl

ПРО КРИПТОСИСТЕМИ ВІД БАГАТЬОХ ЗМІННИХ, ЩО ГРУНТУЮТЬСЯ НА ПРИХОВАНИХ РІВНЯННЯХ ЕЙЛЕРА

Подано нові криптосистеми від багатьох змінних, визначені на n-вимірному вільному модулі над арифметичним кільцем лишків Z_m, що грунтується на ідеї прихованого дискретного логарифма. Такі криптосистеми базуються на прихованих рівняннях Ейлера $x^{\alpha} = a, (\alpha, m) = 1$. Якщо m є достатньо великим добутком щонайменше двох великих простих чисел, то розв'язок рівняння являє собою важкорозв'язну задачу за умови, що розклад числа m на дільники невідомий. У постквантову епоху задача факторизації розв'язується за поліноміальний час. Цей факт не призводить до безпосереднього зламу такої криптосистеми, тому що параметр α невідомий. Деякі приклади таких криптосистем розглядалися раніше. Запропоновано їх модифікації та узагальнення, які дають можливість використовувати асиметричні алгоритми, що базуються на родинах мультиплікативно ін'єктивних відображень із наперед заданою поліноміальною щільністю та степенем, обмеженим сталою.

Ключові слова: *постквантова криптографія, криптографія від багатьох змінних, публічні ключі, прихований дискретний логарифм, приховані рівняння Ейлера, алгебраїчні графи, оцінки складності.*

В.А. Устименко

Институт телекоммуникаций и глобального информационного пространства НАН Украины, Киев
Университет Марии Кюри-Склодовской, Люблин, Польша
E-mail: vasylustimenko@yahoo.pl

О КРИПТОСИСТЕМАХ ОТ МНОГИХ ПЕРЕМЕННЫХ, ОСНОВАННЫХ НА СКРЫТЫХ УРАВНЕНИЯХ ЭЙЛЕРА

Представлены новые криптосистемы от многих переменных, определенные на n-мерном свободном модуле над арифметическим кольцом вычетов Z_m, основанном на идее скрытого дискретного логарифма. Эти криптосистемы основываются на скрытых уравнениях Эйлера $x^{\alpha} = a, (\alpha, m) = 1$. Если m является достаточно большим произведением двух или более больших простых чисел, то решение уравнения составляет труднорешаемую задачу при условии, что разложение числа m на делители неизвестно. В постквантовую эру задачу факторизации можно решить за полиномиальное время. Этот факт не приводит к непосредственному взлому такой криптосистемы, так как параметр α неизвестен. Некоторые примеры таких криптосистем рассматривались раньше. Предложены их модификации и обобщения, которые позволяют использовать асимметричные алгоритмы, базирующиеся на семьях мультипликативно инъективных отображений с наперед заданной полиномиальной плотностью и степенью, ограниченной константой.

Ключевые слова: *постквантовая криптография, криптография от многих переменных, публичные ключи, скрытый дискретный логарифм, скрытые уравнения Эйлера, алгебраические графы, оценки сложности.*