doi: https://doi.org/10.15407/dopovidi2018.09.021
UDC 519.1, 514.128

V.A. Ustimenko

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

On multivariate public keys based on a pair of transformations with density gap

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

We propose an algorithm of generation of the stable families of bijective polynomial maps $f(n)$ of the n-dimensional affine space over a commutative ring K together with their inverse transformations. All maps are given in a standard basis, in which their degrees and densities are calculated. The method allows us to generate transformations $f(n)$ of the linear density with degree given by the prescribed linear function $d(n)$ and with exponential density for $f(n)^{-1}$. In the case of $K = F_q$, we can select $f(n)$ of the exponential order. The scheme of generation of public keys of multivariate cryptography of the form $g(n) = T_1 f(n) T_2$, where T_1 is a monomial linear transformation of K^n, and the degree of T_2 is equal to 1, is proposed. The estimates of complexity show that the time of execution of the encryption rule coincides with the time of computation of the value of a quadratic multivariate map. The decryption procedure based on the knowledge of a generation algorithm is even faster. The security rests on the idea of the insufficiency of adversary's computational resources to restore the inverse map with exponential density and unbounded degree and on the absence of the known general polynomial algorithms to solve this task.

Keywords: *post-quantum cryptography, multivariate cryptography, public keys, algebraic graphs, estimates of complexity.*

1. On the affine Cremona semigroup. Let K be a commutative ring. Let us consider the totality $SF_n(K)$ of all rules f of kind

$$x_1 \to f_1(x_1, x_2, ..., x_n), x_2 \to f_2(x_1, x_2, ..., x_n), ..., x_n \to f_n(x_1, x_2, ..., x_n)$$

for the given parameter n and a chosen commutative ring K with the natural operation of composition. We assume that each rule is written in its standard form, i.e., each polynomial f_i is given by the list of its monomials written in the chosen order. We refer to this semigroup as a semigroup of formal transformations $SF_n(K)$ of the free module K^n. In fact, it is a totality of all endomorphisms of the ring $K[x_1, x_2, ..., x_n]$ with the operations of their superposition.

Each rule f from $SF_n(K)$ induces a transformation $t(f)$ which sends the tuple $(p_1, p_2, ..., p_n)$ into $(f_1(p_1, p_2, ..., p_n), f_2(p_1, p_2, ..., p_n), ..., f_n(p_1, p_2, ..., p_n))$. The affine Cremona semigroup $S(K^n)$ is the totality of all transformations of kind $t(f)$. The canonical homomorphism h: $f \to t(f)$

maps the infinite semigroup $SF_n(K)$ onto a finite semigroup $S(K^n)$ in the case of finite commutative ring K.

We refer to the pair (f, f') of elements $SF_n(K)$ such that f, f' and f' f are two copies of the identical rule

$$x_1 \to x_1, x_2 \to x_2, ..., x_n \to x_n$$

as a pair of invertible elements. If (f, f') is such a pair, then the product $t(f)$ $t(f')$ is an identity map. Let us consider the subgroup $CF_n(K)$ of all invertible elements of $SF_n(K)$ (group of formal maps). It is clear that the image of a restriction of h on $CF_n(K)$ is the affine Cremona group $C(K^n)$ of all transformations of K^n onto K^n, for which there exists a polynomial inverse.

The semigroup $SF_n(K)$ is an important object of the theory of symbolic computation or the so-called Computer Algebra (see [1]), which is a powerful instrument of Multivariate Cryptography [2, 3]. We will assume that each element f of this semigroup is written in the same basis in its standard form. The degree $\deg(f)$ is the maximal degree of polynomials f_i, $i = 1, 2, ..., n$. The density $\mathrm{den}(f)$ of f is the maximal number of monomial terms in $f_i(x_1, x_2, ..., x_n)$.

We say that a family of subsemigroups S_n of $SF_n(K)$ (or $S(K^n)$) is *stable* of degree d, if the maximal degree of elements from S_n is an independent constant d, $d > 2$. If K is a finite commutative ring, then the stable semigroup has to be a finite set. The brief observation of the known families of stable groups and their cryptographical applications can be found in [4].

Let $f(n)$ be a family of nonlinear maps from $SF_n(K)$ of a degree bounded by the constant d. We say that $f(n)$ form a *tame* family, if, in $SF_n(K)$, there is a family $g(n)$ of a degree bounded by the constant d' such that $f(n)g(n) = g(n)f(n)$ is an identity map. Let $T_1(n)$ and $T_2(n)$ be two families of elements from the group $AGL_n(K)$ of all affine bijective transformations, i.e., elements of the affine Cremona group of degree 1. Then we refer to $f'(n) = T_1(n)f(n)\ T_2(n)$ as a linear deformation of $f(n)$. Obviously, $f'(n)$ is also a tame family of transformations, and the degrees of maps from this family are also bounded by d. The degrees of the inverses for $f'(n)$ are bounded by d'.

Let $G_n < CF_n(K)$ be a stable family of subgroups of degree d, $d > 1$, then the nonlinear representatives $f(n)$ of G_n form a tame family of maps. It is easy to see that the densities of $f(n)$ and its linear deformations $f'(n)$ can be very different. We refer to a pair of mutually invertible elements $f(n), f(n)^{-1}$ from $CF_n(K)$ as a pair with a density gap, if the density of $f(n)$ is a polynomial expression in the variable n, and the density of $f(n)^{-1}$ is bounded from below by an exponential function a^n with base $a > 1$.

Similarly, we refer to a pair of mutually invertible elements $f(n), f(n)^{-1}$ from $CF_n(K)$ as a pair with a degree, if the degree of $f(n)$ is a polynomial expression in the variable n, and the degree of $f(n)^{-1}$ is bounded from below by an exponential function a^n with base $a > 1$.

2. On the explicit construction of stable maps of the prescribed degree and large order. We define the Double Schubert Graph $DS(k,K)$ over a commutative ring K as the incidence structure defined as a disjoint union of partition sets $PS = K^{k(k+1)}$ consisting of points, which are tuples of kind $x = (x_1, x_2, \dots, x_{k,} x_{11}, x_{12}, \dots, x_{kk})$ and $LS = K^{k(k+1)}$ consisting of lines, which are tuples of kind $y = [y_1, y_2, \dots, y_{k,} y_{11}, y_{12}, \dots, y_{kk}]$, where x is incident to y, if and only if $x_{ij} - y_{ij} = x_i y_j$ for $i = 1, 2, ..., k$ and $j = 1, 2, ..., k$. It is convenient to assume that the indices of kind i, j are placed for tuples of $K^{k(k+1)}$ in the lexicographical order.

Remark. The term Double Schubert Graph is chosen, because the points and lines of $DS(k,F_q)$ can be treated as subspaces of $F_q^{(2k+1)}$ of dimensions $k+1$ and k, which form two largest Schubert cells. Recall that the largest Schubert cell is the largest orbit of the group of unitriangular matrices acting on the variety of subsets of given dimensions (see [5] and references therein or [6]).

We define the color of a point $x = (x_1, x_2, \dots, x_k, x_1, x_{12}, \dots, x_{kk})$ from PS as the tuple $(x_1, x_2, \dots, x_k)$ and the color of a line $y = [y_1, y_2, \dots, y_k, y_{11}, y_{12}, \dots, y_{kk}]$ as the tuple $(y_1, y_2, \dots, y_k)$. For each vertex v of $DS(k,K)$, there is the unique neighbor $y = N_a(v)$ of a given color $a = (a_1 a_2, \dots, a_k)$.

The *symbolic color* g from $K[x_1, x_2, ..., x_k]^k$ of v of kind $(f_1(x_1, x_2, ..., x_k), f_2(x_1, x_2, ..., x_k), \dots f_k(x_1, x_2, ..., x_k))$, where f_i are polynomials from $K[x_1, x_2, ..., x_k]$, defines the neighboring line of the general point $x = (x_1, x_2, \dots, x_k, x_{11}, x_{12}, \dots, x_{kk})$ with color kind $(f_1(x_1, x_2, ..., x_k), f_2(x_1, x_2, ..., x_k), \dots f_k(x_1, x_2, ..., x_k))$. Similarly, we can compute the neighboring point of the general line $[x] = [x_1, x_2, \dots, x_k, x_{11}, x_{12}, \dots, x_{kk}]$ of color g.

Let us consider a tuple of symbolic colors $g^1, g^2, ..., g^{2t}$ from $(K[x_1, x_2, ..., x_k]^k)^{2t}$ and the map f of PS to itself, which sends the point $x = (x_1, x_2, \dots, x_k, x_{11}, x_{12}, \dots, x_{kk})$ to the end v_{2t} of the chaina $v_0, v_1, v_2, \dots, v_{2t}$, where $x = v_0$, v_i I v_{i+1}, $i = 0, 1, 2, ..., 2t-1$, and the color of v_i is the tuple g_i, of elements from $K[x_1, x_2, ..., x_k]$. We refer to f as the map of the closed point-to-point computation with the symbolic key $g^1, g^2, ..., g^{2t}$ or simply the symbolic computation. As follows from the definitions, $f = f_{g^1, g^2, \dots, g^{2t}}$ is a multivariate map of $K^{k(k+1)}$ to itself. When the symbolic key is given, f can be computed in the standard form via the elementary operations of addition and multiplication of the ring $K[x_1, x_2, \dots, x_k, x_{11}, x_{12}, \dots, x_{kk}]$. Recall that $(x_1, x_2, ..., x_k, x_{11}, x_{12}, \dots, x_{kk})$ is our symbolic point of the graph.

We refer to expression $f_{g^1, g^2, \dots, g^{2t}}$ as the automaton presentation of f with a symbolic key $g^1, g^2, \dots, g^{2t}$. Note that if $t(g^{2t})$ is an element of the affine Cremona group $C(K^k)$, then $f_{g^1, g^2, \dots, g^{2t}}$ is invertible, and the automaton presentation of its inverse has a symbolic key $g^{-2t} g^{2t-1}, g^{-2t} g^{2t-2}, g^{-2t} g^{2t-3}, ..., g^{-2t} g^1, g^{-2t}$, where g^{-2t} is the inverse of the element g^{2t}.

The restrictions on degrees and densities of multivariate maps $t(g^i)$ of K^k to K^k and the size of the parameter t allow us to define a polynomial map f with polynomial degree and density.

Let $g^i = (h_1^i, h_2^i, \dots, h_k^i)$, $i = 1, 2, ..., 2t$, be the symbolic key of the closed point-to-point computation $f = f(n)$ of the symbolic automaton $DS(k,K)$). We refer to elements g^i as the governing functions of the symbolic key. We set that $g^0 = (h_1^0, h_2^0, \dots, h_k^0) = (x_1, x_2, \dots, x_k)$. Then f is a transformation of kind

$$x_1 \to h_1^{2t}(x_1, x_2, ..., x_k), x_2 \to h_2^{2t}(x_1, x_2, ..., x_k), ..., x_k \to h_n^{2t}(x_1, x_2, ..., x_k),$$
$$x_{11} \to x_{11} - h_1^1 x_1 + h_1^1 h_1^2 - h_1^2 h_1^3 + h_1^3 h_1^4 + ... + h_1^{2t-1} h_1^{2t},$$
$$x_{12} \to x_{12} - h_1^1 x_2 + h_1^1 h_2^2 - h_2^2 h_1^3 + h_1^3 h_2^4 + ... + h_2^{2t-1} h_1^{2t},$$
$$x_{kk} \to x_{kk} - h_k^1 x_k + h_k^1 h_k^2 - h_k^2 h_k^3 + h_k^3 h_k^4 + ... + h_k^{2t-1} h_k^{2t}.$$

We say that the map f of the closed point-to-point computation is affine, if all elements g^i of the symbolic key are elements of degree < 2. We refer to a subsemigroup G in $S(K^n)$ as a semigroup of degree d, if the maximal degree for a representative g equals d.

Let $AGL_n(K)$ be the group of affine transformations of K^n, i.e., the group of all bijective transformations of degree 1.

Let us consider a semigroup $E_k(K)$ introduced in [7], which consists of all transformations $f_{h^1,h^2,\ldots,h^l,g}$, where degrees of h^i for $i = 1, 2, \ldots, l$ and g are bounded by 1, and l is an odd number. It is clear that $E_k(K)$ is a stable subsemigroup of degree 2.

The group $GL_n(F_q)$ contains Singer cycles, i.e., elements of order $q^n - 1$ (see [8, 9]).

Lemma 1. *Let $K = F_q$, let f be the map of the closed point-to-point computation $h^1, h^2, \ldots, h^l, h$, and let h defines a Singer Cycle from $GL_n(F_q)$. Then the order of f is at least $q^k - 1$.*

Lemma 2. *Let $K = F_q$ and let $f_{h^1,h^2,\ldots,h^l,h}$ be an element of the semigroup $E_k(K)$ such that h defines the map from $GL_k(F_q)$ has an invariant subspace W of dimension m, and the resriction of h onto W is a Singer cycle. Then the stable semigroup $\langle f \rangle$ generated by f contains at least $q^m - 1$ elements.*

We consider two symbolic computations C_1 and C_2 with governing functions $f^1, f^2, \ldots, f^t$ and $g^1, g^2, \ldots, g^s$ and corresponding maps $m_1 = m(C_1)$ and $m_2 = m(C_2)$. We refer to the symbolic computation C_1 with governing functions $f^1, f^2, \ldots, f^t$ and $g^1(f^t), g^2(f^t), \ldots, g^s(f^t)$ as the concatenation of C_1 and C_2. It is easy to see that the map corresponding to C is $m_2(m_1)$. So, $C \to m(C)$ is homomorphism of two monoids.

Let us consider the totality $PL = PL(k,K)$ of all point-to-point computations C with governing functions $f^1, f^2, \ldots, f^t$ with the last, f^t from $K[x_1, x_2, \ldots, x_k]^k$ of kind $(l_1(x_1, x_2, \ldots, x_k), l_2(x_1, x_2, \ldots, x_k), \ldots l_k(x_1, x_2, \ldots, x_k))$, where all expressions l_i are of degree 1. It is easy to see that PL is a closed set with respect to the concatenation operation. We add the empty computation as a formal neutral element. This means that the maps of kind $m(C)$ from PL form a subsemigroup S^{PL} of the affine Cremona semigroup $S(K^{k(k+1)})$.

Note that a map $m(C)$ induced by a point-to-point computation C with governing functions $f^1, f^2, \ldots, f^t$, where f^t has coordinates, $f_1^t(x_1, x_2, \ldots, x_k), f_2^t(x_1, x_2, \ldots, x_k), \ldots, \ldots, f_k^t(x_1, x_2, \ldots, x_k)$, is an invertible transformation of $K^{k(k+1)}$, if and only if the map

$$x_1 \to f_1^t(x_1, x_2, \ldots, x_k), x_2 \to f_2^t(x_1, x_2, \ldots, x_k), \ldots, x_k \to f_k^t(x_1, x_2, \ldots, x_k),$$

is a bijection. It is clear that the invertible map $m(C)^{-1}$ from S^{PL} is also an element of S^{PL}.

Let G^{PL} be the group of all invertible elements from PL. We define the degree of the governing function f^i given by a tuple with coordinates $f_1^i(x_1, x_2, \ldots, x_k), f_2^i(x_1, x_2, \ldots, x_k), \ldots, f_k^i(x_1, x_2, \ldots, x_k)$ as the maximal degree of f_j^i for various i and j. Note that $m(C)$ from G^{PL} can be an element with very large order. In fact, in the case of $K = F_q$ and an arbitrary list of governing functions $f^1, f^2, \ldots, f^{t-1}$ and f^t for the given bilinear map

$$x_1 \to f_1^t(x_1, x_2, \ldots, x_k), x_2 \to f_2^t(x_1, x_2, \ldots, x_k), \ldots, x_k \to f_k^t(x_1, x_2, \ldots, x_k),$$

which is a Singer cycle, i.e., its order is at least $q^k - 1$, the order of $m(C)$ is also bounded from below by $q^k - 1$.

We can easily construct nonbijective maps of kind $m(C)$ from S^{PL} such that the subgroup generated by this element consists of more than q^{k-c} elements for some constant $c > 1$. In fact, one can take f^t with the invariant subspace W of dimension $k - c$ such that the restriction of f^t on W is a Singer cycle. It is convenient to consider the tuple $(x_1, x_2, \ldots, x_k)$ as a governing function f^0

of the symbolic computation C. For the polynomials f^{2i}, $i = 1, 2, ..., t/2$ which are colors of the points from $DS(k,K[x_1, x_2, ..., x_k])$, we consider their maximal degree d_e. Let d_o be the maximal degree of f^{2i+1}, $i = 1, 2, ..., t/2$. Note that the degree of the polynomial map $m(C)$ is bounded from above by $d_e + d_o$. In fact, the degree of this map is the maximum of products of coordinates of f^i and f^{i+1}, $i = 1, 2, ..., t - 1$.

Let us consider the totality $S^{rs}(PL)$ of maps $m(C)$ for the symbolic computations with d_e equals at most r and d_o equals at most s.

Theorem. *The totality* $S^{rs}(PL(k,K))$ *is a stable subsemigroup of the affine Cremona semigroup* $S(K^{k(k+1)})$ *of degree* $r + s$.

It is clear that the intersection $G^{rs}(PL(k,K))$ of $G(PL)$ and $S^{rs}(PL(k,K))$ is a stable subgroup of $C(K^{k(k+1)})$ of degree $r + s$. Note that $E_k(K)$ presented in [7] coincides with $S^{11}(PL(k, K))$.

3. On the pairs of transformations with density gap and the corresponding public key. Let us consider a point-to-point computation of the Schubert symbolic automaton from the semigroup $S^{m1}(PL(n,K))$ with $m = d(n)$ of kind $an = b$, $a > 1$ corresponding to the symbolic key f^1, $f^2, ..., f^t$ or some even parameter t with elements f^i, i is odd, with degree linearly increasing in the variable n and finite density.

Then the corresponding transformation F will be of degree $O(n)$ and linear density. Let us assume that f^t is a bijective map. Then, in majority cases, the inverse map F^{-1} given by the symbolic key formed by elements $f^{t-1}(f^{-t}), f^{t-2}(f^{-t}), ..., f^1(f^{-t}), f^{-t}$, where f^{-t} is the inverse for f^t, will be of density $O(n^n)$. So, the pair F, F^{-1} is a pair with density gap.

We propose the following public key algorithm.

Alice chooses a finite commutative ring K, positive integer n, and a linear expression $m = d(n)$. She works with the Double Schubert graph $DS(n,K)$ and the related symbolic automaton. Alice selects an odd parameter t and a symbolic key $f^1, f^2, ..., f^t$ for an invertible element of $S^{m1}(PL(n,K))$. She generates the polynomial map F corresponding to the computation with a chosen symbolic key. The standard form of this transformation can be computed with $O(n^4)$ elementary operations (quadratic in the number of variables).

Alice selects the bijective monomial transformation T of $V = K^{n(n+1)}$given by a monomial matrix of size $n(n + 1)$ times $n(n + 1)$ with $n(n + 1)$ nonzero regular entries from K^* (each column and each row contains exactly one nonzero element). She takes the affine bijective transformation T' of V and forms $G = TFT'$. For the construction of G, Alice has to compute n^2 linear combinations of the polynomial expression of n^2 multivariate polynomials of density and degree $O(n)$. So, the total cost to form G is $O(n^6)$ (cubic in the number of variables).

Alice sends the standard form of G to Bob. Note that G has degree $O(n)$ and density $O(n^3)$.

Bob writes his plaintext p from V and computes the ciphertext $c = G(p)$ in the time $O(n^4)$ (quadratic time in the number of variables).

Decryption process. Assume that Alice keeps the already computed transformation $T_1 = T^{-1}$ and $T_2 = T^{-1}$. Firstly, she computes $T_1(c) = b$. It takes $O(n^4)$ elementary operations.

Now, she has the color $t = (b_1, b_2, ..., b_n)$ of point (b). Alice is looking for an intermediate vector v formed by the coordinates of point (v) such that $F(v) = c$. Let $(r) = (v_1, v_2, ..., v_n)$ be the color of point (v). Alice has the inverse f^{-t} of the bijective affine map f^t. So, she computes $(r) = f^{-t}(r)$ in the time $O(n^2)$. Now, Alice can compute values of $f^1, f^2, ..., f^{t-1}$ on the tuple (r). This costs $O(n)$ operations. After that, she computes v as the final element of the walk of length

t with starting point (b) and the prescribed colors of vertices. This costs $O(n^2)$ elementary operations to Alice.

Finally, she gets the plaintext via the application $T_2 = T^{-1}$ also in the time $O(n^2)$.

Other ideas of the usage of algebraic graphs for the construction of multivariate cryptosystems can be found in [13—15].

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

REFERENCES

1. Machi, A. (2012). Algebra for symbolic computation. Springer.
2. Ding, J., Gower, J. E. & Schmidt, D. S. (2006). Multivariate public key cryptosystems. Advances in Information Security, Vol. 25. Springer.
3. Goubin, L., Patarin, J. & Yang, Bo-Yin. (2011). Multivariate cryptography. In Encyclopedia of Cryptography and Security. 2nd ed. (pp. 824-828). Springer.
4. Ustimenko, V. (2017). On the families of stable multivariate transformations of large order and their cryptographical applications. Tatra Mt. Math. Publ., 70, pp. 107-117.
5. Ustimenko, V. A. (2015). On Schubert cells in Grassmannians and new algorithm of multivariate cryptography. Tr. Inst. Mat., 23, No. 2, pp. 137-148.
6. Ustimenko, V. A. (1998). On the varieties of parabolic subgroups, their generalizations and combinatorial applications. Acta Appl. Math., 52, pp. 223-238.
7. Ustimenko, V. (2017). On desynchronised multivariate El Gamal algorithm. Retrieved from https://eprint.iacr.org/2017/712.pdf
8. Cossidente, A. & de Ressmine, M. J. (2004). Remarks on Singer cycle groups and their normalizers. Designs Codes Cryptogr., 32, pp. 97-102.
9. Kantor, W. (1982). Linear groups containing a Singer cycle. J. Algebra, 62, pp. 232-234.
10. Ustimenko, V. (2015). On algebraic graph theory and non–bijective maps in cryptography. Algebra Discrete Math., 20, No. 1, pp. 152-170.
11. Ustimenko, V. (2017). On new multivariate cryptosystems with nonlinearity gap. Algebra Discrete Math., 23, No. 2, pp. 331-348.
12. Ustimenko, V. (2017). On new multivariate cryptosystems based on hidden Eulerian equations. Dopov. Nac. akad. nauk Ukr., No. 5, pp. 17-24. doi: https://doi.org/10.15407/dopovidi2017.05.017
13. Romańczuk-Polubiec, U. & Ustimenko, V. (2015). On two windows multivariate cryptosystem depending on random parameters. Algebra Discrete Math., 19, No. 1, pp. 101-129.
14. Ustimenko, V. & Romańczuk, U. (2013). On dynamical systems of large girth or cycle indicator and their applications to multivariate cryptography. In Artificial Intelligence, Evolutionary Computing and Metaheuristics (pp. 257-285). Berlin: Springer.
15. Polak, M., Romańczuk, U., Ustimenko, V. & Wróblewska, A. (2013). On the applications of extremal graph theory to coding theory and cryptography. Electron. Notes Discrete Math., 43, pp. 329-342.

Received 13.03.2018

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 ҐРУНТУЮТЬСЯ НА ПАРІ ПЕРЕТВОРЕНЬ З ПРОВАЛОМ У ЩІЛЬНОСТІ

Пропонується алгоритм породження стабільних родин взаємно однозначних відображень $f(n)$ у n-вимірному афінному просторі над комутативним кільцем K разом з оберненими до них перетвореннями. Всі відображення подані у стандартному базисі, в якому обчислюються їх степінь та щільність. Метод дозво-

ляє генерувати перетворення $f(n)$ лінійної щільності зі степенем, заданим обраною лінійною функцією $d(n)$ та зі щільністю експоненціального розміру для $f(n)^{-1}$. У випадку $K = F_q$ ми можемо обрати $f(n)$ експоненціального порядку. Пропонується схема генерування публічних ключів поліноміальної криптографії від багатьох змінних вигляду $g(n) = T_1 f(n) T_2$, де T_1 є мономіальним лінійним перетворенням, а степінь T_2 дорівнює 1. Оцінки складності показують, що час виконання правила шифрування збігається з часом обчислення значення квадратичного поліноміального відображення. Процедура декодування, що базується на знанні алгоритму генерації, є ще більш швидкою. Безпека ґрунтується на ідеї недостатності обчислювальних ресурсів у опонента для відновлення оберненого відображення експоненціальної щільності і необмеженого степеня та відсутності відомих поліноміальних алгоритмів для розв'язання цієї задачі.

Ключові слова: *постквантова криптографія, криптографія від багатьох змінних, публічні ключі, 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 ПАРЕ ПРЕОБРАЗОВАНИЙ С ПРОВАЛОМ В ПЛОТНОСТИ

Предлагается алгоритм порождения стабильных семейств взаимно однозначных отображений $f(n)$ в n-мерном аффинном пространстве над коммутативным кольцом K вместе с обратными к ним преобразованиями. Все отображения заданы в стандартном базисе, в котором вычисляются их степени и плотности. Метод позволяет генерировать преобразование $f(n)$ линейной плотности со степенью, заданной выбранной линейной функцией $d(n)$ и с плотностью экспоненциального размера для $f(n)^{-1}$. В случае $K = F_q$ мы можем выбрать $f(n)$ экспоненциального порядка. Предлагается схема генерации публичных ключей полиномиальной криптографии от многих переменных вида $g(n) = T_1 f(n) T_2$, где T_1 является мономиальным линейным преобразованием, а степень T_2 равна единице. Оценки сложности показывают, что время выполнения правила шифрования совпадает с временем вычисления значения квадратичного полиномиального отображения. Процедура декодирования, основывающаяся на знании алгоритма генерации, является еще более быстрой. Безопасность основывается на недостатке вычислительных ресурсов у оппонента для восстановления обратного отображения экспоненциальной плотности и неограниченной степени и на отсутствии эффективных алгоритмов для решения этой задачи.

Ключевые слова: *постквантовая криптография, криптография от многих переменных, публичные ключи, алгебраические графы, оценки сложности.*