doi: https://doi.org/10.15407/dopovidi2018.10.026
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 new symbolic key exchange protocols and cryptosystems based on a hidden tame homomorphism

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

Multivariate cryptosystems are divided into public rules, for which tools of encryption are open for users and systems of the El Gamal type, for which the encryption function is not given in public, and, for its generation, the opponent has to solve a discrete logarithm problem in the affine Cremona group. Infinite families of transformations of a free module K^n over a finite commutative ring K such that the degrees of their members are not growing with iteration are called stable families of transformations. Such families are needed for practical implementations of multivariate cryptosystems of the El Gamal type. New explicit constructions of such families and families of stable groups and semigroups of transformations of free modules are given. New methods of creation of cryptosystems, which use stable transformation groups and semigroups and homomorphisms between them, are suggested. The security of these schemes is based on a complexity of the decomposition problem for an element of the affine Cremona semigroup into a product of given generators. Proposed schemes can be used for the exchange of messages in a form of elements of a free module and for a secure delivery of multivariate maps, which could be encryption tools and instruments for digital signatures.

Keywords: *Multivariate Cryptography, stable transformation groups and semigroups, problem of decomposition of a nonlinear multivariate map into given generators, wild and tame families of transformations, tame homomorphisms, key exchange protocols, cryptosystems, algebraic graphs.*

1. On Post Quantum and Multivariate Cryptography, public key schemes approach. Post Quantum Cryptography (PQC) serves for the research of asymmetric cryptographic algorithms, which can be potentially resistant against attacks based on the use of a quantum computer. Multivariate cryptography is one of the oldest directions of PQC. It uses, as security tools, a nonlinear polynomial transformations f of kind:

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

acting on the affine space K^n, where f_i, $i = 1, 2, ..., n$, from $K[x_1, x_2, ..., x_k]$ are multivariate polynomials given in a standard form, i. e. via a list of monomials in a chosen order (see [1]).

The most popular form is the usage of a very special map f in a *public key mode*. It means the key holder Alice has some initial data D, which allow her to solve the equation $f(x) = b$, where b

and x are known and unknown elements of the free module K^n, but a public user Bob has only f given publicly in its standard form. Asymmetry means that Alice has tools for the encryption and decryption, but Bob has only an encryption procedure.

Public knowledge on $f = f_n$ (allows the adversary to create as many pairs of kind plaintext p-ciphertext $c = f(p)$ as he/she wants. It makes the problem of practical design of such a cryptosystem to be a difficult task. First examples were based on families of quadratical bijective transformations f_n (see [1—3]), such choice implies a rather fast encryption process.

In [4], the idea of a multivariate Diffie—Hellman (DH) protocol was modified in various ways. It uses recent constructions of large families of stable subsemigroups of small degree in affine Cremona semigroups containing large cyclic semigroups.

In Section 2, we introduce new cryptographical protocols with the usage of the concept of a tame homomorphism of stable semigroups of affine transformations (homomorphic map, which is computable in polynomial time). The idea to exploit the complexity of *word problem* for the Cremona semigroup about the decomposition of a given polynomial transformation g from the semigroup into given generators is presented in Section 3.

The multivariate nature of collision maps allows us to use these algorithms for the safe exchange of multivariate transformations. Various *deformation rules* can be used for this purpose (see Section 4). Correspondents may use a family of invertible generators g_n. Assume that one of them can generate the inverse of g_n. Then the symbolic El Gamal type *tahoma* algorithms can be used by correspondents. They can use the *inverse protocol* to elaborate pairs of mutually invertible transformations. So, they can conduct the information exchange protected via the complexity of some difficult problem. Section 5 introduces the inverse of the *group enveloped symbolic Diffie—Hellman algorithm* described in [4, 5].

The last section is devoted to the implementation of the algorithm of Section 3 via symbolic walks on graphs $A(n, K)$ (see [6, 7]).

In all realizations of algorithms, we use stable subsemigroups S of the affine Cremona semigroup $S(K^n)$ generated by special symbolic automata defined in terms of special algebraic graphs. The method of generation allows us to construct, for each bijective transformation of S, its inverse element. In fact, we use linguistic graphs defined in [8]. They are bipartite graphs with a special coloring of vertices such that, for each vertex, there is a unique neighbor of the selected color. We did not use the terminology and general technique of symbolic walks on linguistic graphs. In fact, for each family of graphs considered in the paper, an algorithm of generation of the corresponding stable semigroup was given in independent way.

2. Tame families and concept of stability. Let us consider basic algebraic objects of multivariate cryptography, which are important for the choice of appropriate pairs of maps f, f^{-1} in both cases of public key approach or idea of asymmetric algorithms with protected encryption rules.

Let us consider the totality $SF_n(K)$ of all rules f of kind:

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

acting on the affine space K^n, where f_i, $i = 1, 2, ..., n$, for the given parameter n and a chosen commutative ring K with the natural operation of composition. We refer to this semigroup as a semigroup of formal transformations $SF_n(K)$ of free module K^n. In fact, it is a totality of all endo-

morphisms of the ring $K[x_1, x_2, ..., x_k]$ with the operation 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 $(f_1(p_1, p_2, ..., p_n), f_2(p, p_2, ..., p_n), ..., f_n(p_1, p_2, ..., p_n))$. The affine Cremona semigroup $C(K^n)$ is a totality of all transformations of kind $t(f)$. The canonical homomorphism $t: \to t(f)$ 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 ff' and $f'f$ are two copies of the identical rule $x_i \to x_i$, $i = 1, 2, ..., n$, 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 $CF_n(K)$-invertible elements of $SF_n(K)$ (group of formal maps). It means f is an element of $CF_n(K)$ if and only if there is f' such that ff' and $f'f$ are identity maps. It is clear that the image of a restriction of t on $CF_n(K)$ is the affine Cremona group $C_n(K)$ of all transformations of K^n onto K^n, for which there exists a polynomial inverse.

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 stable semigroup has to be a finite set. The brief observation of the known families of stable groups can be found in [4, 5] (see also [9—12]).

Let f_n from $SF_n(K)$ be a family of nonlinear maps of degree bounded by constant d. We say that f_n form a tame family, if there is a family g_n from $SF_n(K)$ of degree bounded by constant d' such that $f_n g_n = g_n f_n$ are identity maps. Let T_1 and T_2 be two 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 $f'_n = T_1 f_n T_2$ as 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 inverses of f'_n are bounded by d'. Let $G_n < SF_n(K)$ be a stable family of subgroups of degree d, $d \geqslant 2$. Then the nonlinear representatives f_n of G_n form a tame family of maps.

3. On the concept of tame homomorphism and related algorithms. Let $G = G_n$ be a family of stable subsemigroups of $SF_n(K)$ (or $S(K^n)$), and let $L = L_m$, where m depends on n, be a family of stable subsemigroups of $SF_m(R)$ (or $S(R^m)$), where K and R are commutative rings. There are tame homomorphisms $\phi = \phi_n$ from G into L, i. e. the value of ϕ at each point g from G_n is computable in polynomial time from n. Let us assume that there are semigroups $B = B_n < G_n$ given by their generators $b_1, b_2, ..., b_r$. Let us assume that Alice has families of tame transformations π_1 of K^n and of π_2 of R^m. We assume that these data are known to Alice. She forms $(a_i = \pi_1 b_i \pi_1^{-1}, a'_i = \pi_2 \phi(b_i) \pi_2^{-1})$, $i = 1, 2, ..., r$ and sends them to Bob. The elements of these pairs are given in their standard forms for representatives of $SF_n(K)$ or $SF_m(R)$.

3.1. Key exchange protocol. The list of pairs known for Bob defines a homomorphism Δ between the subsemigroups $A = \langle a_1, a_2, ..., a_r \rangle$ and $A' = \langle a'_1, a'_2, , ..., a'_r \rangle$ given by its values on generators $\Delta(a_i) = \Delta(a'_i)$ for $i = 1, 2, ..., r$. Bob forms a via his choice of word $(a_{i_1})^{k_1}(a_{i_2})^{k_2} \ldots (a_{i_t})^{k_t}$ in the alphabet of generators of A such that $a_{i_s} \neq a_{i_{s+1}}$ for $s = 1, 2, ..., t-1$. He sends a to Alice and keeps $\Delta(a) = a' = (a'_{i_1})^{k_1}(a'_{i_2})^{k_2} \ldots (a'_{i_t})^{k_t}$ as a collision element.

Alice knows the tame homomorphism ϕ and easily computes a' as $\pi_2 \phi(\pi_1^{-1} a \pi_1)\pi_2^{-1}$.

Complexity remark. The adversary has to solve the *word problem* for the subsemigroup A, i. e., find the decomposition of a from A into generators a_1, $i = 1, 2, ..., t$. The general algorithm to solve this problem in polynomial time in the variable n is unknown, as well as a procedure to get its solution in terms of quantum computations.

Remark 1. The condition of stability for the semigroups G and L and the usage of the tame transformations π_1 and π_2 allow us to estimate degrees of a and a collision map. If the maximal degrees of $\pi_1(n)$ and π_1^{-1}(n) are l_1 and l_1', the degrees of $\pi_1(n)$ and π_1^{-1}(n) are bounded by l_2 and l_2, and the stable groups G and L are of degrees d and d', then the degrees of a and $\Delta(a)$ are bounded by $l_1 l_1' d$ and $l_2 l_2' d'$.

*Remark 2***.** One can use other natural conditions on π_1 and π_2. Let us assume that $G < G_1$ and $L < G_2$, where G_i are stable families of subsemigroups of degree t_1, $t_1 \leqslant d$ and, $t_2\ t_2 \leqslant d'$, respectively. Let us consider normalizers N_1 and N_2 of G_1 and G_2 in the affine Cremona semigroups $S(K^n)$ and $S(R^m)$. It means that N_1 and N_2 are the totalities of transformations π from $C(K^n)$ and $C(R^m)$ such that $\pi_i G_i \pi_i^{-1}$, $i = 1, 2$, coincide with G_1 and G_2. We can take π_1 of kind $T_1 n_1$ and π_2 of kind $T_2 n_2$, where π_1 of kind n_i are elements of N_i, $i = 1, 2$, transformations T_1 and T_2 are elements of groups $AGL_n(K)$ and $AGLm(R)$ Then the degrees of a and $\Delta(a)$ are restricted by t_1 and t_2.

Note that, in the case $G = G_1$, $L = G_2$, the degrees of a and $\Delta(a)$ are bounded by d and d'. We refer to the presented above algorithm as the *tahoma word* protocol. The term *tahoma* (name of shrift for word processing) stands for a *tame homomorphism*.

The protocol exploits the complexity of the *word problem* for a semigroup of polynomial transformation of a free module. In the case considered in *Remark 2*, we use the term *stable tahoma word* protocol.

3.2. Inverse tahoma word protocol. Let us modify protocol 3.1 in the case of invertible elements $\phi(a_i)$ with an assumption that their inverses are known to Alice. Instead of pairs (a_i, a_i'), Alice forms $(a_{i'}, a_i^*)$, where $a_i^* = (a_i')^{-1}$, $i = 1, 2, ..., r$. Assume Bob gets the list of such pairs from Alice. Note that A' is a group $\langle a_i^* \mid i = 1, 2, ..., r\rangle$. So, Bob is able to compute the antiisomorphism δ sending z from A into $\phi(z)^{-1}$, because he knows the values of δ on generators. Like in the previous protocol, Bob forms a via his choice of word $(a_{i_1})^{k_1}(a_{i_2})^{k_2} \dots (a_{i_t})^{k_t}$ in the alphabet of generators of A such that $(a_{i_s}) \neq (a_{i_{s+1}})$ for $s = 1, 2, ..., t-1$ and sends a to Alice. Now he keeps $\delta(a) = (a_{i_t}^*)^{k_t}(a_{i_{t-1}}^*)^{k_{t-1}}(a_{i_2}^*)^{k_2}(a_{i_1}^*)^{k_1}$ as an element of the collision pair. Alice computes her part of collision pair $e = \delta(a)^{-1}$ as $\pi_2\phi(\pi_1^{-1}a\pi_1)\pi_2^{-1}$.

3.3. Inverse tahoma cryptosystem. Both above-written protocols exploit the complexity of finding the decomposition of a into a product of given generating transformations. In the case of 3.2, Alice and Bob can securely communicate, because they are able to use mutually inverse transformations e and e^{-1} as encryption tools. Alice writes her message p and sends $e(p)$ to Bob, who decrypts via the usage of $\delta(a)$. Bob can encrypt with $\delta(a)$ and Alice decrypts with e.

Remark 3. In the case where the transformation $e = e_m$ of a free module R^m forms a stable family of degree d', the adversary has to intercept $O(m^{d'})$ messages and conduct costly the linearization attack to restore e and $\delta(a)$. So, the correspondents can safely exchange $O(m^{d'-1})$ messages. Note that, at any moment, Alice and Bob can start a new session of the inverse tahoma word protocol.

A different usage of homomorphisms of a subsemigroup of the Cremona semigroup in the cryptosystem was considered in [13, 14].

4. On the safe exchange of symbolic transformations. The symbolic nature of the collision map can be used for a task that differs from the exchange of keys. We refer to it as the usage of DH *deformation symbolic rules*.

Let Alice have a free module K^n over a commutative ring K. She has a subset Ω of K^n and a polynomial map $f: K^n \to K^n$ such restriction of $f|\Omega$ is an injective map from Ω onto $f(\Omega) = \Gamma$. Additionally, Alice has an algorithm to solve, in polynomial time, the equation $x = b$ with respect to the unknown x from Ω and b from Ω.

Alice and Bob use the *tahoma word protocol* or symbolic Diffie—Hellman protocol to elaborate the collision map g acting on K^n. After this step, Alice sends Ω and the transformation $h = f + g$ to Bob.

Now Bob can get f as $h—g$. He writes a plaintext p from Ω and sends the ciphertext $c = f(x)$. Alice uses her data for the decryption.

Remark 4. Note that a new algorithm is still asymmetric because Bob can encrypt, but not decrypt. The encryption rule is known a to trusted customer (Bob) but the adversary has no access to it. In fact, such access is protected by the word problem in a semigroup of transformations of K^n or the discrete logarithm problem in the corresponding affine Cremona semigroup.

Other deformations. Alice and Bob agree (via the open channel) on a deformation rule $D(f)$ for a multivatiate rule f from the affine Cremona semigroup. For example, it can be the multiplication, i. e. f is the rule $x_i \to f_i(x_1, x_2, ..., x_n)$, $i = 1, 2, ..., n$, and g is the rule $x_i \to g_i (x_1, x_2, ..., x_n)$, $i = 1, 2, ..., n$, and Alice sends a tuple of polynomials $f_i g_i$, $i = 1, 2, ..., n$. Bob uses the division to restore f. Instead of the addition deformation rule (sending $x_i \to f_n(x_1, x_2, ..., x_n) + g_n(x_1, x_2, ..., x_n)$, $i = 1, 2, ..., n$), Alice can use a deformation with adding an element $K[x_1, x_2, ..., x_k]^n$ obtained from g via the usage of an s-time conducted derivation δ^s, where $\delta = d/dx_1 + d/dx_2 + ... + d/d_{x_n}$ (rule $x_i \to f_n(x_1, x_2, ..., x_n) + \delta^s g_n(x_1, x_2, ..., x_n)$, $i = 1, 2, ..., n$). The last deformation is interesting, because, in many cases, we can achieve the equality of degrees for f and $D(f)$. It is easy to continue this list of possible deformation rules.

Remark 5. Let us assume that $\Omega = K^n$. So, $f = f_n$ is a bijection. Assume that the degrees of nonlinear maps f_n are bounded by constant d. Let us assume that the adversary has option to intercept some pairs plaintext-ciphertext (leakage from Bob's data). In the case of interception of $O(n^d)$, the adversary has chance for a successful linearization attack and get the map f. For example, if $d = 3$, then the linearization attack cost is $O(n^{10})$. After that, the adversary has to find the inverse function for f like in the case of multivariate public key.

To prevent "transition to knowledge" of an encryption multivariate map, Alice (or Bob) can arrange a new session with the protocol and a transmission of a new deformed encryption rule, for which secret data for the decryption are known.

Remark 6. The technique of linearization attacks on nonbijective maps or maps f_n of unbounded degree and a low density is not developed yet.

5. On the inverse version of the group enveloped symbolic Diffie—Hellman key exchange protocol. Let $G = G_n$ be a family of stable subsemigroups of $SF_n(K)$ (or $S(K^n)$) and $L = L_m$, where m depends on n, be a family of stable subsemigroups of $SF_m(R)$ (or $S(R^m)$), where K and R are commutative rings. There is a tame homomorphism $\phi = \phi_n$ from G into L, i. e., the value of ϕ at each point g from G_n is computable in polynomial time from n. Let us assume that there are subgroups $A = A_m < L_m$ and $B = B_n < G_n$ such that $\phi(b)a = a\phi(b)$ for all elements a from A, b from B. Assume that two families of tame transformations $\pi = \pi(n)$ and $\mu = \mu(m)$ are chosen.

We assume that these data are known to Alice. She forms pairs $(c_i = \pi\, b_i\, \pi^{-1}, c_i^{-1} = \pi\, b_i^{-1} \pi^{-1})$ and $(d_i = \mu\phi(b_i)\mu^{-1}, d_i^{-1} = \mu\phi(b_i^{-1})\mu^{-1})$, $i = 1, 2, ..., r$, where elements b_i are from B_n, and they, in-

verses, and images are given in their standard form $SF_n(K)$ or $SF_m(R)$. She sends them to Bob. Let Δ be a homomorphism from $\langle c_1, c_2, ..., c_r\rangle$ to $\langle d_1, d_2, ..., d_r\rangle$ sending c_i to d_i.

We present briefly the protocol of symbolic computations introduced in [4] and define its inverse version. We refer to this protocol as the *group enveloped Diffie—Hellman scheme* and *inverse group enveloped Diffie—Hellman scheme*.

5.1. Protocol. Alice takes a positive integer k_A and a, a^{-1} from A_m and g' from the semigroup G. She computes $g_A = \mu a\phi(g')a^{-1}\mu^{-1}$ and sends to Bob $g = \pi g'\pi^{-1}$ together with g_A.

Bob chooses a positive integer k_B and an element c from R^m in $\langle c_1, c_2, ..., c_r\rangle$ (via the choice of a word in the alphabet $c_1, c_2, ..., c_r$. He computes $g_B = cg^t c^{-1}$ with $t = k_B$ in standard form for elements of $SF_n(K)$ and sends it to Alice.

Bob computes a map $\Delta(c)\ g_A^{\ t}\ \Delta\ (c^{-1})$, because he knows the decomposition of c and c^{-1} into their generators and keeps it as the collision map.

Alice computes the collision map as $\mu a\phi(\pi^{-1}g_B^s\pi)a^{-1}\mu^{-1}$ with $s = k_A$.

Remark 7. The adversary has to consider the group $C' = \langle\, c_i \mid i = 1, 2, ..., r\rangle$ and solve the *group enveloped discrete logarithm problem*, i. e., to solve $yg^x y^{-1} = g_B$, where x is the unknown integer parameter and y from C' (possibly, via solving the decomposition problem of g_B into semigroup generators $c_1, c_2, ..., c_r, g$ (decomposition of elements into Cremona semigroup generators, the *word problem in affine Cremona semigroup*).

5.2. Inverse protocol. Let us assume that Alice can generate g' such that $\phi(g')$ is invertible and the inverse $\phi(g')^{-1}$ is computable for her.

As in the previous algorithm, Alice takes a positive integer k_A, elements a, a^{-1} from A_m, and g' from the semigroup G. Now, she computes $z = \phi(g')^{-1}$ and $g_A = \mu aza^{-1}\mu^{-1}$ and sends to Bob $g = \pi g'\pi^{-1}$ together with g_A.

As in the previous algorithm, Bob chooses a positive integer k_B and an element c from in $\langle c_1, c_2, ..., c_r\rangle$ via the choice of a word in the alphabet of generators. He computes $g_B = cg^t c^{-1}$ with $t = k_B$ in standard form of $SF_n(K)$ and sends it to Alice.

Bob computes a map $e = \Delta(c)(g_A)^t\Delta(c)^{-1}$, $t = k_B$, because he knows the decomposition of c and c^{-1} into their generators and keeps e as his outcome of a collision.

Alice computes the map e^{-1} as $\mu a\ \phi(\pi^{-1}(g_B)^s\pi)a^{-1}\mu^{-1}$, $s = k_A$.

5.3. Inverse group enveloped cryptosystem. Alice and Bob can communicate, because they have mutually inverse transformations e^{-1} and e.

1) Alice writes her message p and sends $e^{-1}(p)$ to Bob, who decrypts via the usage of e.

2) Bob can encrypt with e, and Alice decrypts with e^{-1}.

Algorithm (5.3) was introduced in [4] as a *desynchronized symbolic El Gamal* algorithm.

6. Stable groups of cubical maps and a protocol based on the Cremona word problem. The following family of stable groups was considered in [4]. 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. So, $(p) = (p_1, p_2, ..., p_n) \in P_n$ and $[l] = [l_1, l_2, ..., l_n] \in L_n$. The incidence relation $I = A(n, K)$ (or corresponding bipartite graph I) is given by the condition $p\ I\ l$ if and only if the equations of the following kind hold:

$$p_2 - l_2 = l_1 p_1,\ p_3 - l_3 = p_1 l_2,\ p_4 - l_4 = l_1 p_3,\ p_5 - l_3 = p_1 l_4,\ ...,$$

$p_n - l_n = p_1\, l_{n-1}$ for odd n,
$p_n - l_n = l_1 p_{n-1}$ for even n.

Let us consider the case of finite commutative ring K, $|K| = m$. As it instantly follows from the definition, the order of our bipartite graph $A(n, K)$ is $2m^n$. The graph is m-regular. In fact, the neighbour 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 the 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 a point p and the color $\rho(l)$ of a line l as parameters p_1 and l_1 respectively.

Graphs $A(n, K)$ with coloring ρ belong to the class of Γ *linguistic graphs* considered in [8] (see also [15], which observes cryptographical applications of linguistic graphs). The linguistic graph Γ defined over a commutative ring K is a bipartite graph with partition sets K^n and K^m that have color set $L = K^s$ and $L = K^r$, respectively. The projection ρ of a point $x = (x_1, x_2, ..., x_n)$, or line $y = [y_1, y_2, ..., y_m]$, on the tuple of their first s and r coordinates respectively, defines the colors of vertices. Each vertex has a unique neighbor with selected color. So, $n + r = m + s$. The incidence of linguistic graphs is given by a system of polynomial equations over the ring K.

In the case of a linguistic graph Γ with $s = r = 1$, the path consisting of its vertices $v_0, v_1, v_2, ..., v_k$ is uniquely defined by the initial vertex v_0, and colours $\rho(v_i)$, $i = 1, 2, ..., k$ of other vertices from the path. So, the following symbolic computation can be defined. Take the *symbolic point* $x = (x_1, x_2, ..., x_n)$, where x_i are variables and the *symbolic key*, which is a string of polynomials $f_1, f_2, ..., f_k$, from $K[x_1]$. Form the path of vertices $v_0 = x$, v_1 such that $v_1 I v_0$ and $\rho(v_1) = f_1(x_1)$, v_2 such that $v_2 I v_1$ and $\rho(v_2) = f_2(x_1)$, ..., v_k such that $v_k I v_{k-1}$ and $\rho(v_k) = f_k(x_1)$.

We use term *symbolic point-to-point computation* in the case of even k and talk about *symbolic point-to-line computation* in the case of odd k. We note that the computation C of each coordinate of v_i via the variables $x_1, x_2, ..., x_n$ and polynomials $f_1, f_2, ..., f_k$ needs only arithmetical operations of addition and multiplication. As it follows from the definition of linguistic graph the final vertex v_k (point or line) has coordinates $(h_1(x_1), h_2(x_1, x_2), h_3(x_1, x_2, x_3), ..., h_n(x_1, x_2, ..., x_n))$, where $h_1(x_1) = f_k(x_1)$. Let us consider the map $H = \eta(C)$: $x_i \to h_i(x_1, x_2, ..., x_n)$, $i = 1, 2, ..., n$, which corresponds to the computation C. Assume that the equation $b = f_k(x_1)$ has exactly one solution. Then the map $H : x_i \to h_i(x_1, x_2, ..., x_n)$, $i = 1, 2, ..., n$, is a bijective transformation. In the case of finite parameter k and finite densities of $f_i(x_1)$, $i = 1, 2, ..., n$, the map H also has finite density. If all parameters $\deg(f_i(x_1))$ are finite, then the map H has a linear degree in the variable n. Let us consider the totality $\sum = \sum(n, K)$ of point-to-point computations C with the symbolic key of kind $f_i(x_1) = x_1 + a_i$, $i = 1, 2, ..., t$, where the parameter t is even. In case of a linguistic graph with $r = s = 1$, we identify a computation C with the corresponding string $(a_1, a_2, ..., a_t)$. We assume that the empty string is also an element of $\sum$. The natural product of two strings given by tuples $C_1 = (a_1, a_2, ..., a_t)$ and $C_2 = (b_1, b_2, ..., b_m)$ is a string $C = C_1 \circ C_2 = (a_1, a_2, ..., a_t, b_1 + a_t, b_2 + a_t, ..., b_m + a_t)$. This product transforms $\sum$ to a semigroup. The map η' sending C to $\eta(C)$ is a homomorphism of $\sum$ into the affine Cremona group $C(K^n)$. In the case of linguistic graphs $A(n, K)$, we can prove that the totality $G(n, K) = \eta'(\sum(n, K))$ is a stable subgroup of degree 3 (see [5]).

We assume that $a_0 = 0$ and say that a transformation $\eta(C)$ is irreducible, if $a_i \neq a_{i+2}$, $i = 1, 2, ..., t-2$. If $a_1 \neq a_{t-1}$, and $a_2 \neq a_t$, we say that the irreducible computation C and the corresponding transformation $\eta(C)$ are standard elements.

We have a natural homomorphism $G(n + 1, K)$ onto $G(n, K)$ induced by the homomorphism Δ from $A(n + 1, K)$ onto $A(n, K)$ sending a point $(x_1, x_2, ..., x_n, x_{n+1})$ to $(x_1, x_2, ..., x_n)$ and a line $[x_1, x_2, ..., x_n, x_{n+1}]$ to $[x_1, x_2, ..., x_n]$. It means that there is the well-defined projective limit $A(K)$ of graphs $A(n, K)$ and groups $G(K)$ of groups $G(n, K)$, when n is growing to infinity. As stated in [6] in the case of $K = F_q$, $q > 2$, the infinite graph $A(F_q)$ is a tree.

It means that the group $G(F_q)$ is a group of walks of even length on a q regular tree starting at the zero point with natural addition of them. A standard computation C defines a transformation $\eta(C)$ in each group $G(n, K)$, $n \geqslant 2$ and $G(K)$. An irreducible transformation $\eta(C)$ from $G(K)$ has an infinite order.

Some examples of a tame homomorphism were considered in [4]. We are going to use the family of maps introduced below.

Let $\Delta_{n, m,}$, $n > m$ be a canonical homomorphism of $A(n, K)$ onto $A(m, K)$ corresponding to the procedure of deleting of the coordinates with indices $m + 1, m + 2, ..., n$. This map defines the canonical homomorphism $\mu(n, m)$ of the group $G(n, K)$ onto $G(m, K)$.

Let R and K be finite extensions of a finite ring Q. Let us consider the diagram $S(R^m) > > G(m, R) > G(m, Q) \leftarrow G(n, Q) < G(n, K) < S(K^n)$ with extreme nodes $S(R^m)$ and $S(K^n)$, where $n > m$, and the arrow corresponds to a canonical homomorphism $\mu = \mu(n, m)$, $n > m$. Alice is going to use the *stable tahoma word protocol* with $G = G(n, Q)$, $G_1 = G(n, K)$, $L = G(m, K)$, $L_1 = G(m, R)$ (see Remark 2).

She can use the subgroups $H_1 = G_1$ and $H_2 = L_1$ of invertible elements instead of the whole normalizers $N_1 = N(G_1)$ of a subgroup G_1 in the affine Cremona group $S(K^n)$, and $N_2 = N(L_1)$ of subgroup in the Cremona group $S(R^m)$. She also works with the affine subgroups $AGL_n(K)$ and $AGL_m(R)$.

Alice forms $\pi_1 = T_1 n_1$, where $T_1 \in AGL_{1n}(K)$, $n_1 \in H_1$, and $\pi_2 = T_2 n_2$, where $T_2 \in AGL_{1m}(R)$, $n_2 \in H_2$. She takes a subgroup, where $G1\ pt = \pi_1 G \pi_1^{-1}$, $L' = \pi_2 L\, \pi_2^{-1}$, and a homomorphism $\mu' : x \to \to \pi_2(\mu\ (\pi_1 x \pi_1^{-1}))\pi_2^{-1}$ between these semigroups. Alice will work with G', L' and μ' instead of G, L, μ. The map μ' is tame for her, because she knows the decomposition of μ' into the conjugation with π_2, μ and the conjugation with π_1.

6.1. Example of the stable tahoma word protocol. Alice takes a subgroup B of G' given by the generators $b_1, b_2, ..., b_r$ and sends these generators to Bob together with a string $\mu'(b_i)$, $i = 1, 2, ..., r$. So, Bob knows just the restriction of μ' on B given by its values on generators. He does not know the triple G', L' and μ' with its decomposition into 3 maps. So, Bob selects $a_1, a_2, ..., a_s$, where a_i are elements of the alphabet $\{b_1, b_2, ..., b_r\}$. He computes the composition b of selected powers of a transformation a_i from $S(K^n)$ and sends the standard form of b to Alice. He keeps a composition b' of elements $\mu'(a_i)$ according to the selected order. Alice gets b' as $\mu'(b)$.

6.2. General complexity estimates for the cryptosystem in the case $K = R = Q$. Let us assume that Alice is going to use the homomorphism between $A(n, K)$ and $A(m, K)$ for $m < n$ and $m = O(n)$. We will count the number of arithmetical operations of the commutative ring K, which she needs to generate an element of $g = G(n, K)$, which corresponds to the symbolic computation with the key of length $O(1)$.

Counting steps of the recurrent process of creation g via the symbolic automaton gives us $O(n)$ operations. Alice chooses affine transformations T and T^{-1}. The computation T^{-1} costs $O(n^2)$ elementary operations. This means that Alice can create $T^{-}gT^{-1}$ for $O(n^5)$ operations. Alice forms elements $b_1, b_2, ..., b_r$ from $G(n, K)$ together with their inverses and homomorphic images $\mu'(b_i)$, $i = 1, 2, ..., r$, from $G(m, K)$ in time $O(n)$. She takes T^{-} and T^{-1} from $AGL_n(K)$ and forms $a_i = T^{-}b_iT^{-1}$ and $a_i' = T(b_i^{-1})T^{-1}$ in time $O(n^5)$.

Bob receives the list of pairs a_i, a_i', $i = 1, 2, ..., r$. He computes a chosen word of the kind $a = a_{i1}^{k1}a_{i2}^{k2}..., a_{it}^{kt}$ for the chosen finite parameter t and integers k_i, $i = 1, 2, ..., t$, in time $O(n^{13})$ operations and sends it to Alice. Bob writes his message $p = (p_1, p_2, ..., p_m)$. To form the ciphertext, he applies the transformation a_{i_t}' with multiplicity k_t, a_{i_t}' with multiplicity k_{t-1}, ..., $a_{i_{t-1}}'$ with multiplicity k_1 to p and forms the ciphertext c. It takes him $O(n^3)$ elementary operations. Alice computes a cubical $b = aT$ with $O(n^4)$ operations. After she gets $d = T^{-1}\ b$ in time $O(n^4)$. Alice easily gets $\mu(d)$ and computes $e = T_1\ d$ and $f = eT_1^{-1}$. She computes p as $f(c)$. The last step costs her $O(n^3)$ elementary ring operations.

6.3. Special implementations. Let us consider an implementation of the above cryptosystem in the case of a choice of maps T and T_1 as linear maps of finite density. Natural examples of such maps are monomial transformations or elements of direct sum of groups of kind $GL_d(K)$, where d is a finite constant.

Alice chooses the affine transformations T and T^{-1}. The computation $g\ T^{-1}$ costs $O(n)$ elementary operations. This means that Alice can create $T\ g\ T^{-1}$ for $O(n)$ operations. Alice forms elements $b_1, b_2, ..., b_r$ from $G(n, K)$ together with their inverses and homomorphic images $\mu(b_i)$, $i = 1, 2, ..., r$, from $G(m, K)$ in time $O(n)$. She takes T, T^{-1}, T_1, and T_1^{-1} from $GL_{1n}(K)$ and forms $a_i = T\ b_i T^{-1}$ and $a'_i = T_1\ \mu(\ bi^{-1})T_1^{-1}$ in time $O(n)$.

Bob receives the list of pairs a_i, a'_i, $i = 1, 2, ..., r$, of cubical elements of density $O(n)$. He computes a chosen word of kind $a = a_{i_1}^{k_1}a_{i_2}^{k_2}\ \ldots,\ a_{i_t}^{k_t}$ for the chosen finite parameter t and the integers k_i, $i = 1, 2, ..., t$, in time $O(n^5)$ operations and sends it to Alice. Bob writes his message $(p) = (p_1, p_2, ..., p_m)$. To form the ciphertext, he applies the transformation a_{i_t}' with multiplicity k_t, $a_{i_{t-1}}'$ with multiplicity k_{t-1}, ..., a_{i_1}' with multiplicity k_1 to p and forms the ciphertext c. It takes him $O(n)$ elementary operations. Alice computes a cubical $b = aT$ with $O(n^2)$ operations. After that, she gets $d = T^{-1}b$ in time $O(n^2)$. Alice easily gets $\mu(d)$ and computes $e = T_1d$ and $f = eT_1^{-1}$. She computes p as $f(c)$. The last step cost her $O(n^2)$ elementary ring operations.

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

REFERENCES

1. Ding, J., Gower, J. E. & Schmidt, D. S. (2006). Multivariate public key cryptosystems. Advances in Information Security, Vol. 25, Springer.
2. Koblitz, N. (1998). Algebraic aspects of cryptography. 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 desynchronised multivariate El Gamal algorithm. Retrieved from https://eprint.iacr. org./2017/712.pdf.
5. 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.

6. 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.
7. Ustimenko, V. A. (2013). On the extremal graph theory and symbolic computations. Dopov. Nac. akad. nauk Ukr. No. 2, pp. 42-49 (in Russian).
8. Ustimenko, V. A. (2005). Maximality of affine group, and hidden graph cryptosystem. Algebra Discrete Math., No. 1, pp. 133-150.
9. Ustimenko, V. & Wróblewska, A. (2013). On the key exchange and multivariate encryption with nonlinear polynomial maps of stable degree. Annalles UMCS, Informatica, 13, No.1, pp. 63-80.
10. Wróblewska, A. (2008). On some properties of graph based public keys. Albanian J. Math., 2, No. 3, pp. 229-234.
11. Klisowski, M. & Ustimenko, V. (2015). Graph based cubical multivariate maps and their cryptographical applications. In Advances on superelliptic curves and their applications (pp. 305-327). Amsterdam etc.: IOS Press.
12. Wróblewska, A. & Ustimenko, V. (2014). On new examples of families of multivariate stable maps and their cryptographical applications. Annales UMCS, Informatica. 14, No. 1, pp. 19-36.
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. Romańczuk-Polubiec, U. & Ustimenko, V. A. (2015). On new key exchange multivariate protocols based on pseudorandom walks on incidence structures. Dopov. Nac. akad. nauk Ukr., No. 1, pp. 41-49. doi: htpps://doi.org/10.15407/dopovidi2015.01.041
15. Ustimenko, V. A. (2015). Explicit constructions of extremal graphs and new multivariate cryptosystems. Stud. Sci. Math. Hung. Spec. iss. Proceedings of The Central European Conference, 2014, Budapest. 52, No. 2, pp. 185-204.

Received 14.03.2018

В.О. Устименко

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

ПРО НОВІ СИМВОЛІЧНІ ПРОТОКОЛИ ОБМІНУ КЛЮЧІВ ТА КРИПТОСИСТЕМИ, ЩО ОПИРАЮТЬСЯ НА ПРИХОВАНІ РУЧНІ ГОМОМОРФІЗМИ

Криптосистеми від багатьох змінних поділяються на публічні ключі, для яких засіб шифрування відкритий для всіх користувачів, та криптосистеми типу Ель Гамаля з функцією шифрування, що не надається публічно, для її генерування опонент повинен розв'язати проблему дискретного логарифма в афінній групі Кремони. Нескінченні родини перетворень вільних модулів K^n над скінченним комутативним кільцем K такі, що степені їх представників не зростають при ітерації, називають стабільними родинами перетворень. Такі родини необхідні для практичних реалізацій криптосистем типу Ель Гамаля. Наведено нові конструкції таких родин та родин стабільних напівгруп перетворень вільних модулів. Запропоновано нові методи створення криптосистем, які використовують стабільні групи та напівгрупи разом з гомоморфізмами між ними. Безпека таких схем ґрунтується на складності проблеми розкладу елемента афінної напівгрупи Кремони в добуток заданих твірних. Схеми можуть використовуватися як для обміну повідомленнями у вигляді елементів вільного модуля, так і для безпечного узгодження поліноміальних перетворень від багатьох змінних, які можуть бути знаряддям шифрування або інструментом для цифрового підпису.

Ключові слова: *криптографія від багатьох змінних, стабільні групи та напівгрупи, проблема декомпозиції нелінійного перетворення від багатьох змінних за заданими твірними, дикі та ручні перетворення, ручні гомоморфізми, протоколи обміну ключів, криптосистеми, алгебраїчні графи.*

В.А. Устименко

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

О НОВЫХ СИМВОЛИЧЕСКИХ ПРОТОКОЛАХ ОБМЕНА КЛЮЧЕЙ И КРИПТОСИСТЕМЫ, ОСНОВЫВАЮЩИХСЯ НА СКРЫТЫХ РУЧНЫХ ГОМОМОРФИЗМАХ

Криптосистемы от многих переменных подразделяются на публичные ключи, для которых способ шифрования открыт для всех пользователей, и криптосистемы типа Эль Гамаля с функцией шифрования, не заданной публично, для ее генерации оппонент должен решить проблему дискретного логарифма в афинной группе Кремоны. Бесконечные семейства преобразований свободного модуля K^n над конечным коммутативным кольцом K такие, что степени их представителей не возрастают при итерации, называют стабильными семействами преобразований. Такие семейства необходимы для практических реализаций криптосистем типа Эль Гамаля. Приведены новые конструктивные построения таких семейств и семейств стабильных полугрупп преобразований свободных модулей. Предложены новые способы построения криптосистем, использующие стабильные группы и полугруппы вместе с гомоморфизмами между ними. Безопасность таких схем опирается на сложность проблемы разложения элемента афинной полугруппы Кремоны в произведение заданных образующих. Схемы могут использоваться как для обмена сообщениями в виде элементов свободного модуля, так и для безопасного согласования полиномиальных преобразований от многих переменных, которые могут быть средствами шифрования или инструментами цифровой подписи.

Ключевые слова: *криптография от многих переменных, стабильные группы и подгруппы, проблема декомпозиции нелинейного преобразования от многих переменных по заданным образующим, дикие и ручные преобразования, ручные гомоморфизмы, протоколы обмена ключей, криптосистемы, алгебраические графы.*