ALBANIAN JOURNAL
OF MATHEMATICS
Volume 4, Number 4, Pages 161–170
ISSN 1930-1235: (2010)

ON THE KEY EXCHANGE WITH NONLINEAR POLYNOMIAL MAPS OF DEGREE 4

V. USTIMENKO AND A. WROBLEWSKA

The project is co-funded from the sources of the European Union
within the limit of the European Social Fund.

Human - The Best Inwestment

Abstract. We say that the sequence g_n, $n \geq 3$, $n \to \infty$ of polynomial transformation bijective maps of free module K^n over commutative ring K is a sequence of stable degree if the order of g_n is growing with n and the degree of each nonidentical polynomial map of kind ${g_n}^k$ is an independent constant c. A transformation $b = \tau {g_n}^k \tau^{-1}$, where τ is affine bijection, n is large and "k" is relatively small, can be used as a base of group theoretical Diffie-Hellman key exchange algorithm for the Cremona group $C(K^n)$ of all regular automorphisms of K^n. The specific feature of this method is that the order of the base may be unknown for the adversary because of the complexity of its computation. The exchange can be implemented by tools of Computer Algebra (symbolic computations). The adversary can not use the degree of righthand-side in $b^x = d$ to evaluate unknown x in this form for the discrete logarithm problem.

In the paper we introduce the explicit constructions of sequences of elements of stable degree for cases $c = 4$ for each commutative ring K containing at least 3 regular elements and discuss the implementation of related key exchange and public key algorithms.

1. Introduction

Discrete logarithm problem can be formulated for general finite group G. Find a positive integer x satisfying condition $g^x = b$ where $g \in G$ and $b \in G$. The problem has reputation to be a difficult one. But even the case of cyclic group Z_n there are many open questions. If $n = p - 1$ or $n = \phi(pq)$ where p and q are sufficiently large prime then the complexity of discrete logarithm problem justify classical Diffie-Hellman key exchange algorithm and RSA public key encryption, respectively. In most of other cases complexity of discrete logarithm problem is not

Received by the editors December 15, 2010.

Key words and phrases. Key exchange, public key cryptography, symbolic computations, graphs and digraphs of large girth .

Research supported by a project "Human - The Best Inwestment". The project is co-funded from the sources of the European Union within the European Social Fund.

investigated properly. The problem is very dependent on the choice of the base g and the way of presentation the data on the group. Group can be defined via generators and relations, as automorphism group of algebraic variety, as matrix group, as permutation group etc. In this paper we assume that G is a subgroup of S_{p^n} which is a group of polynomial bijective transformation of vector space ${F_p}^n$ into itself. Obviously $|S_{p^n}| = n!$, it is known that each permutation π can be written in the form $x_1 \to f_1(x_1, x_2, \dots x_n), x_2 \to f_2(x_1, x_2, \dots x_n), \dots, x_n \to f_n(x_1, x_2, \dots x_n)$, where f_i are multivariable polynomials from $F_p[x_1, x_2, \dots, x_n]$. The presentation of G as a subgroup of S_{p^n} is chosen because the Diffie Hellman algorithm here will be implemented by the tools of symbolic computations. Other reason is universality, as it follows from classical Cayley results each finite group G can be embedded in S_{p^n} for appropriate p and n in various ways.

Let F_p, where p is prime, be a finite field. Affine transformations $\mathrm{x} \to Ax + b$, where A is invertible matrix and $b \in (F_p)^n$, form an affine group $AGL_n(F_p)$ acting on ${F_p}^n$.

Affine transformations form an affine group $AGL_n(F_p)$ of order $(p^n - 1)(p^n - p) \dots (p^n - p^{n-1})$ in the symmetric group S_{p^n} of order $(p^n)!$. In [15] the maximality of $AGL_n(F_p)$ in S_{p^n} was proven. So we can present each permutation π as a composition of several "seed" maps of kind $\tau_1 g \tau_2$, where $\tau_1, \tau_2 \in AGL_n(F_p)$ and g is a fixed map of degree ≥ 2.

We can choose the base of ${F_p}^n$ and write each permutation $g \in S_{p^n}$ as a "public rule":

$x_1 \to g_1(x_1, x_2, \dots, x_n), x_2 \to g_2(x_1, x_2, \dots, x_n), \dots, x_n \to g_n(x_1, x_2, \dots, x_n)$.

Let $g^k \in S_{p^n}$ be the new public rule obtained via iteration of g. We consider Diffie - Hellman algorithm for S_{p^n} for the key exchange in the case of group. Correspondents Alice and Bob establish $g \in S_{p^n}$ via open communication channel, they choose positive integers n_A and n_B, respectively. They exchange public rules $h_A = g^{n_A}$ and $h_B = g^{n_B}$ via open channel. Finally, Alice and Bob compute common transformation T as ${h_B}^{n_A}$ and ${h_A}^{n_B}$, respectively.

In practice they can establish common vector $v = (v_1, v_2, \dots, v_n)$, $v_i \in F_p$ via open channel and use the collision vector $T(v)$ as a password for their private key encryption algorithm.

This scheme of "symbolic Diffie - Hellman algorithm" can be secure, if the order of g is "sufficiently large" and adversary is not able to compute number n_A (or n_B) as functions from degrees for g and h_A. Obvious bad example is the following: g sends x_i into ${x_i}^t$ for each i. In this case n_A is just a ratio of $\deg h_A$ and $\deg g$.

To avoid such trouble one can look at family of subgroups G_n of S_{p^n}, $n \to \infty$ such that maximal degree of its elements equal c, where c is small independent constant (groups of degree c or groups of stable degree). Our paper is devoted to explicit constructions of such families.

We refer to a sequence of elements $g_n \in G_n$ such that all its nonidentical powers are of degree c as element of stable degree. This is equivalent to stability of families of cyclic groups generated by g_n. Of course, cyclic groups are important for the Diffie- Hellman type protocols.

It is clear that affine groups $AGL_n(p)$, $n \to \infty$ form a family of subgroups of stable degree for $c = 1$ and all nonidentical affine transformations are of stable degree. Notice that if g is a linear diagonalisable element of $AGL_n(p)$, then discrete logarithm problem for base g is equivalent to the classical number theoretical problem. Obviously, in this case we are loosing the flavor of symbolic computations.

General problem of construction an infinite families of stable subgroups G_n of S_{p^n} of degree c satisfying some additional conditions (unbounded growth of minimal order of nonidentical group elements, existence of well defined projective limit, etc) can be also interesting because of possible applications in cryptography.

Notice that even we conjugate nonlinear C with invertible linear transformation $\tau \in AGL_n(F_p)$, some of important cryptographical parameters of C and $C' = \tau^{-1}C\tau$ can be different. Of course conjugate generators g and g' have the same number of fixed points, same cyclic structure as permutations, but counting of equal coordinates for pairs $(x, g(x))$ and $(x\ , g'(x))$ may bring very different results.

So two conjugate families of stable degree are not quite equivalent because corresponding cryptoanalitical problems may have different complexity.

We generalize the above problem for the case of Cremona group of the free module K^n, where K is arbitrary commutative ring K. For the cryptography case of finite rings is the most important. Finite field F_{p^n}, $n \geq 1$ and cyclic rings Z_m (especially $m = 27$ (ASCII codes), $m = 28$ (binary codes), $m = 216$ (arithmetic), $m = 232$ (double precision arithmetic)) are especially popular. Case of infinite rings K of characteristic zero (especially Z or C) is an interesting as well because of Matijasevich multivariable prime approximation polynomials can be defined there (see, for instance [24] and further references).

So it is natural to change a vector space ${F_p}^n$ for free module K^n (Cartesian power of K) and the family and symmetric group S_{p^n} for Cremona group $C_n(K)$ of all polynomial automorphisms of K^n.

We repeat our definition for more general situation of commutative ring.

Let G_n, $n \geq 3$, $n \to \infty$ be a sequence of subgroups of $C_n(K)$. We say that G_n is a family of groups of stable degree (or subgroup of degree c) if the maximal degree of representative $g \in G_n$ is some independent constant c.

The first family of stable subgroups of $C_n(F_q)$, $K = F_q$ with degree 3 was practically established in [25], where the degrees of polynomial graph based public key maps were evaluated. But group theoretical language was not used there and the problem of the key exchange was not considered.

Those results are based on the construction of the family $D(n, q)$ of graphs with large girth and the descryption of their connected components $CD(n, q)$. The existence of infinite families of graphs of large girth had been proven by Paul Erdös' (see [2]). Together with famous Ramanujan graphs introduced by G. Margulis [14] and investigated in [13] graphs $CD(n, q)$ is one of the first explicit constructions of such a families with unbounded degree. Graphs $D(n, q)$ had been used for the construction of LDPS codes and turbocodes which were used in real satellite communications (see [5], [6], [7]), for the development of private key encryption algorithms [21],[22], [17],[9], the option to use them for public key cryptography was considered in [20], [19] and in [18] , where the related dynamical system had been introduced (see also surveys [23], [24]).

The computer simulation show that stable subgroups related to $D(n, q)$ contain elements of very large order but our theoretical linear bounds on the order are relatively weak. We hope to improve this gap in future and justify the use of $D(n, q)$ for the key exchange.

First family of stable groups were obtained via studies of simple algebraic graphs defined over F_q. For new constructions of stable groups over commutative ring K we use directed graphs with the special colouring. The main result of the paper is the following statement.

Theorem 1. *For each commutative ring K with at least 3 regular elements there are families Q_n of Cremona group $C(K^n)$ of degrees 4 such that the projective limit Q of Q_n, $n \to \infty$ is well defined, the group Q is of infinite order, it contains elements g of infinite order, such that there exists a sequence $g_n \in Q_n$ $n \to \infty$ of stable elements such that* $\lim g_n = g$.

The family Q_n is obtained via explicit constructions. So we may use in the finite ring K with at least 3 regular elements the sequence equivalent to g_n for the key exchange. We show that the growth of the order of g_n when n is growing can be bounded from below by some linear function $\alpha \times n + \beta$. In case of such a sequences of groups $G_n = Q_n$ or $G_n = T_n$ we can modify a sequence g_i of elements of stable degree by conjugation with $h_i \in G_i$. New sequence $d_i = {h_i}^{-1} g_i h_i$ can be also a sequence of elements of stable degree.

Let us discuss the asymmetry of our modified Diffie-Hellman algorithms of the key exchange in details. Correspondents Alice and Bob are in different shoes. Alice chooses dimension n, element g_n as in theorem above, element $h \in Q_n$ and affine transformation $\tau \in AGL_n(K)$. So she obtains the base $b = \tau^{-1} h^{-1} g_n h \tau$ and sends it in the form of standard polynomial map to Bob.

Our groups Q_n are defined by the set of their generators and Alice can compute words $h^{-1} g_n h$, b and its powers very fast. So Alice chooses rather large number n_A computes $c_A = b^{n_A}$ and sends it to Bob. At his turn Bob chooses own key n_B computes $c_B = b^{n_B}$. He and Alice are getting the collision map c as ${c_A}^{n_B}$ and ${c_B}^{n_A}$, respectively.

Remark Notice that the adversary is in the same shoes with public user Bob. He (or she) need to solve one of the equations $b^x = c_B$ or $b^x = c_A$. The algorithm is implemented in the cases of finite fields and rings Z_m for family of groups Q_n. We present its time evaluation (generation of b and b_A^n by Alice and computation of b_B^c by Bob) in the last section of paper. We continue studies of orders of g_i theoretically and by computer simulation.

The computer simulation show that the number of monomial expressions of kind $x^{i_1} x^{i_2} x^{i_3} x^{i_4}$ with nonzero coefficient is rather close to binomial coefficient C_n^3. So the time of computation b^{n_B}, ${c_B}^{n_A}$ and ${c_A}^{n_B}$ can be evaluated via the complexity of computation of the composition of several general cubical polynomial maps in n variable.

2. Walks on infinite forest $D(q)$ and corresponding groups

2.1. **Graphs and incidence system.** The missing definitions of graph-theoretical concepts which appears in this paper can be found in [2]. All graphs we consider are simple, i.e. undirected without loops and multiple edges. Let $V(G)$ and $E(G)$ denote the set of vertices and the set of edges of G, respectively. Then $|V(G)|$ is called the *order* of G, and $|E(G)|$ is called the *size* of G. A path in G is called *simple* if all its vertices are distinct. When it is convenient, we shall identify G with the corresponding anti-reflexive binary relation on $V(G)$, i.e. $E(G)$ is a subset of $V(G) \times V(G)$ and write vGu for the adjacent vertices u and v (or neighbors). The sequence of distinct vertices $v_0, v_1, \ldots, v_t$, such that $v_i G v_{i+1}$ for $i = 1, \ldots, t-1$ is the pass in the graph. The length of a pass is a number of its edges. The distance $\mathrm{dist}(u, v)$ between two vertices is the length of the shortest pass between them. The diameter of the graph is the maximal distance between two vertices u and v of the graph. Let C_m denote the cycle of length m i.e. the sequence of distinct vertices

$v_0, \ldots, v_m$ such that $v_i G v_{i+1}$, $i = 1, \ldots, m-1$ and $v_m G v_1$. The girth of a graph G, denoted by $g = g(G)$, is the length of the shortest cycle in G. The degree of vertex v is the number of its neighbors (see [1] or [2]).

The incidence structure is the set V with partition sets P (points) and L (lines) and symmetric binary relation I such that the incidence of two elements implies that one of them is a point and another is a line. We shall identify I with the simple graph of this incidence relation (bipartite graph). If number of neighbours of each element is finite and depends only from its type (point or line), then the incidence structure is a tactical configuration in the sense of Moore (see [15]). The graph is k-regular if each of its vertex has degree k, where k is a constant. In this section we reformulate results of [10], [11] where the q-regular tree was described in terms of equations over finite field F_q.

Let q be a prime power, and let P and L be two countably infinite dimensional vector spaces over $GF(q)$. Elements of P will be called *points* and those of L *lines*. To distinguish points from lines we use parentheses and brackets: If $x \in V$, then $(x) \in P$ and $[x] \in L$. It will also be advantageous to adopt the notation for coordinates of points and lines introduced in [14]:

$$(p) = (p_1, p_{11}, p_{12}, p_{21}, p_{22}, p'_{22}, p_{23}, \ldots, p_{ii}, p'_{ii}, p_{i,i+1}, p_{i+1,i}, \ldots),$$
$$[l] = [l_1, l_{11}, l_{12}, l_{21}, l_{22}, l'_{22}, l_{23}, \ldots, l_{ii}, l'_{ii}, l_{i,i+1}, l_{i+1,i}, \ldots).$$

We now define an incidence structure (P, L, I) as follows. We say the point (p) is incident with the line $[l]$, and we write $(p)I[l]$, if the following relations between their coordinates hold:

$$\begin{aligned} l_{11} - p_{11} &= l_1 p_1 \\ l_{12} - p_{12} &= l_{11} p_1 \\ l_{21} - p_{21} &= l_1 p_{11} \\ l_{ii} - p_{ii} &= l_1 p_{i-1,i} \\ l'_{ii} - p'_{ii} &= l_{i,i-1} p_1 \\ l_{i,i+1} - p_{i,i+1} &= l_{ii} p_1 \\ l_{i+1,i} - p_{i+1,i} &= l_1 p'_{ii} \end{aligned} \tag{1}$$

(The last four relations are defined for $i \geq 2$.) This incidence structure (P, L, I) we denote as $D(q)$. We speak now of the *incidence graph* of (P, L, I), which has the vertex set $P \cup L$ and edge set consisting of all pairs $\{(p), [l]\}$ for which $(p)I[l]$.

To facilitate notation in future results, it will be convenient for us to define $p_{-1,0} = l_{0,-1} = p_{1,0} = l_{0,1} = 0$, $p_{0,0} = l_{0,0} = -1$, $p'_{0,0} = l'_{0,0} = 1$, $p_{0,1} = p_2$, $l_{1,0} = l_1$, $l'_{1,1} = l_{1,1}$, $p'_{1,1} = p_{1,1}$, and to rewrite (1) in the form :

$$\begin{aligned} l_{ii} - p_{ii} &= l_1 p_{i-1,i} \\ l'_{ii} - p'_{ii} &= l_{i,i-1} p_1 \\ l_{i,i+1} - p_{i,i+1} &= l_{ii} p_1 \\ l_{i+1,i} - p_{i+1,i} &= l_1 p'_{ii} \end{aligned}$$

for $i = 0, 1, 2, \ldots$

Notice that for $i = 0$, the four conditions (1) are satisfied by every point and line, and, for $i = 1$, the first two equations coincide and give $l_{1,1} - p_{1,1} = l_1 p_1$.

For each positive integer $k \geq 2$ we obtain an incidence structure (P_k, L_k, I_k) as follows. First, P_k and L_k are obtained from P and L, respectively, by simply projecting each vector onto its k initial coordinates. The incidence I_k is then defined by imposing the first k–1 incidence relations and ignoring all others. For fixed q, the incidence graph corresponding to the structure (P_k, L_k, I_k) is denoted by $D(k, q)$. It is convenient to define $D(1, q)$ to be equal to $D(2, q)$. The properties of the graphs $D(k, q)$ that we are concerned with described in the following proposition.

Theorem 2 (11)**.** *Let q be a prime power, and $k \geq 2$. Then*
(i) $D(k, q)$ is a q-regular edge-transitive bipartite graph of order $2q^k$;
(ii) for odd k, $g(D(k, q)) \geq k + 5$, for even k, $g(D(k, q)) \geq k + 4$.

We have a natural one to one correspondence between the coordinates $2, 3, \ldots, n, \ldots$ of tuples (points or lines) and equations. It is convenient for us to rename by $i + 2$ the coordinate which corresponds to the equation with the number i and write $[l] = [l_1, l_3, \ldots, l_n, \ldots]$ and $(p) = (p_1, p_3, \ldots, p_n, \ldots)$ (line and point in "natural coordinates").

Let η_i be the map "deleting all coordinates with numbers $> i$" from $D(q)$ to $D(i, q)$, and $\eta_{i,j}$ be map "deleting all coordinates with numbers $> i$ " from $D(j, q)$, $j > i$ into $D(i, q)$.

The following statement follows directly from the definitions:

Proposition 1. *([11]) The projective limit of $D(i, q), \eta_{i,j}$, $i \to \infty$ is an an infinite forest $D(q)$.*

Let us consider the description of connected components of the graphs.

Let $k \geq 6$, $t = [(k + 2)/4]$, and let $u = (u_i, u_{11}, \cdots, u_{tt}, u'_{tt}, u_{t,t+1}, u_{t+1,t}, \cdots)$ be a vertex of $D(k, q)$. (It does not matter whether u is a point or a line). For every r, $2 \leq r \leq t$, let

$a_r = a_r(u) = \sum_{i=0,m} (u_{ii} u'_{r-i,r-i} - u_{i,i+1} u_{r-i,r-i-1})$,

and $a = a(u) = (a_2, a_3, \cdots, a_t)$. (Here we define

$p_{0,-1} = l_{0,-1} = p_{1,0} = l_{0,1} = 0$, $p_{00} = l_{00} = -1$, $p_{0,1} = p_1$, $l_{1,0} = l_1$, $l'_{11} = l_{11}$, $p'_{1,1} = p_{1,1}$).

In [10] the following statement was proved.

Proposition 2. *. Let u and v be vertices from the same component of $D(k, q)$. Then $a(u) = a(v)$. Moreover, for any $t-1$ field elements $x_i \in GF(q)$, $2 \leq it \geq [(k+2)/4]$, there exists a vertex v of $D(k, q)$ for which*
$a(v) = (x_2, \ldots, x_t) = (x)$.

Let us consider the following equivalence relation $\tau : u\tau v$ iff $a(u) = a(v)$ on the set $P \cup L$ of vertices of $D(k, q)$ $(D(q))$. The equivalence class of τ containing the vertex v satisfying $a(v) = (x)$ can be considered as the set of vertices for the induced subgraph $EQ_{(x)}(k, q)$ $(EQ_{(x)}(q))$ of the graph $D(k, q)$ (respectively, $D(q)$). When $(x) = (0, \ldots, 0)$, we will omit the index v and write simply $EQ(k, q)$.

Let $CD(q)$ be the connected component of $D(q)$ which contains $(0, 0, \ldots)$. Let τ' be an equivalence relation on $V(D(k, K))$ $(D(q))$ such that the equivalences classes are the totality of connected components of this graph. Obviously $u\tau v$ implies $u\tau' v$. If char $GF(q)$ is an odd number, the converse of the last proposition is true (see [24] and further references).

Proposition 3. *Let q be an odd number. Vertices u and v of $D(q)$ $(D(k,q))$ belong to the same connected component iff $a(u) = a(v)$, i.e., $\tau = \tau'$ and $EQ(q) = CD(q)$ $(EQ(k,q) = CD(k,q))$.*

The condition $charGF(q) \neq 2$ in the last proposition is essential. For instance, the graph $EQ(k,4))$, $k > 3$, contains 2 isomorphic connected components. Clearly $EQ(k,2)$ is a union of cycles $CD(k,2)$. Thus neither $EQ(k,2)$ nor $CD(k,2)$ is an interesting family of graphs of high girth. But the case of graphs $EQ(k,q)$, q is a power of 2, $q > 2$ is very important for coding theory.

Corollary 1. *Let us consider a general vertex*

$$x = (x_j, x_{1,1}, x_{2,1}, x_{1,2} \ldots, x_{i,i}, x_{i,i}^{'}, x_{i+1,i}, x_{i,i+1}, \ldots),$$

$j = 1$ or 2, $i = 2, 3, \ldots$ of the connected component $CD(k,F)$, which contains a chosen vertex v. Then coordinates $x_{i,i}$, $x_{i,i+1}$, $x_{i+1,i}$ can be chosen independently as "free parameters" from F and $x'_{i,i}$ could be computed consequently as the unique solutions of the equations $a_i(x) = a_i(v)$, $i = 1, \ldots$.

3. On the regular directed graph with special colouring

Directed graph - an irreflexive binary relation $\phi \subset V \times V$, where V is the set of vertices.

Let introduce two sets

$$id(v) = \{x \in V | (a,x) \in \phi\},$$
$$od(v) = \{x \in V | (x,a) \in \phi\}$$

as sets of inputs and outputs of vertex v. Regularity means the cardinality of these two sets (input or output degree) are the same for each vertex.

Let Γ be regular directed graph, $E(\Gamma)$ be the set of arrows of graph Γ. Let us assume that additionally we have a colouring function i.e. the map $\pi : E \to M$ onto set of colours M such that for each vertex $v \in V$ and $\alpha \in M$ there exist unique neighbor $u \in V$ with property $\pi((v,u)) = \alpha$ and the operator $N_a(v) := N(a,v)$ of taking the neighbor u of a vertex v within the arrow $v \to u$ of colour α i a bijection. In this case we refer to Γ as *rainbow like graph.*

For each string of colours $(\alpha_1, \alpha_2, \ldots, \alpha_m)$, $\alpha_i \in M$ we can generate a permutation π which is a composition $N_{\alpha_1} \times N_{\alpha_2} \times \cdots \times N_{\alpha_m}$ of bijective maps $N_{\alpha_i} : V(\Gamma) \to V(\Gamma)$. Let us assume that the map $u \to N_\alpha(u)$ is a bijection. For given vertex $v \in V(\Gamma)$ the computation π corresponds to the chain in the graph:

$$v \to v_1 = N(\alpha_1, v) \to v_2 = N(\alpha_2, v_1) \to \cdots \to v_n = N(\alpha_m, v_{m-1}) = v'.$$

Let G_π be the group generated by permutations π as above.

Let us consider the following graph (triple graph defined in terms of $D(n,K)$ (or $D(K)$). Let F_1 be the totality of all walks of length 3 in $D(n,K)$ of kind $u = (p_1)I[l]I(p_2)$. We consider similar variety F_2 of triples $[l_1](p)[l_2]$ Now we define the relation between vertices of the new graph:

$$\langle (p^1), [l], (p^2) \rangle R \{[l'^1], (p'), [l'^2]\} \Leftrightarrow$$
$$\Leftrightarrow [l] = [l'^1] \ \& \ (p^2) = (p') \ \& \ l'^2_{0,1} - p^2{}_{1,0} \in RegK$$

$$\{[l^1], (p), [l^2]\} R \langle (p'^1), [l'], (p'^2) \rangle \Leftrightarrow$$
$$\Leftrightarrow (p) = (p'^1) \ \& \ [l^2] = [l'] \ \& \ p'^2_{1,0} - l^2_{0,1} \in RegK$$

The colour of the arrow between $u = (p^1)I[l]I(p^2)$ and $u' = [l]I(p^2)I[l']$ is $l'_{0,1} - {p^2}_{1,0}$. Similarly the colour of the arrow between $u' = [l]I(p)I[l']$ and $u = (p)I[l'](p')$ is $p'_{1,0} - l'_{0,1}$. We define rainbow like colouring π.

Let us consider the permutation group $TF'_n(K)$ ($TF'(K)$) acting on $F_1 = K^{n+2}$ (K^∞, respectively) corresponding to the triple graph with the colouring π. Let $TF_n(K)$ ($TF(K)$) be the subgroup of products of even number of generators.

Theorem 3. *Sequence of subgroups $TF_n(K)$ of Cremona group $C_n(K)$ form a family of subgroups of degree 4.*

Proof. To find a family of subgroups of degree 4 we give a construction of triple directed graph. To this eend we would like to connect three vertices of the graph defined in section 2 to get two sets of vertices of new graph:

$$F = \left\{\langle (p^1), [l], (p^2)\rangle \mid (p^1)I[l]I(p^2)\right\}$$

$$F^{'} = \left\{\{[l^1], (p), [l^2]\} \mid [l^1]I(p)I[l^2]\right\}.$$

Now we have the following relation between vertices of the new graph:

$$\langle (p^1), [l], (p^2)\rangle R\{[l'^1], (p'), [l'^2]\} \Leftrightarrow$$

$$\Leftrightarrow [l] = [l'^1] \ \&\ (p^2) = (p') \ \&\ {l'}^2_{0,1} - {p^2}_{1,0} \in RegK$$

$$\{[l^1], (p), [l^2]\} R\langle (p'^1), [l'], (p'^2)\rangle \Leftrightarrow$$

$$\Leftrightarrow (p) = (p'^1) \ \&\ [l^2] = [l'] \ \&\ {p'}^2_{1,0} - l^2_{0,1} \in RegK$$

Using induction we can see that in steps (2k) and (2k+1) we get vertices with corresponding degrees:

$$\langle (p^{2k-2}), [l^{2k-1}], (p^{2k})\rangle =$$

$$= (p_{1,0}+\alpha_1+\ldots+\alpha_{(2k-3)}, p_{1,1}, \ldots, p_{i,j}, l^2_{0,1}+\alpha_2+\ldots+\alpha_{(2k-2)}, p_{1,0}+\alpha_1+\ldots+\alpha_{(2k-1)}),$$

$$\{[l^{2k-1}], (p^{2k}), [l^{2k+1}]\} =$$

$$= (l^2_{0,1}+\alpha_2+\ldots+\alpha_{(2k-2)}, l_{1,1}, \ldots, l_{i,j}, p_{1,0}+\alpha_1+\ldots+\alpha_{(2k-1)}, l^2_{0,1}+\alpha_2+\ldots+\alpha_{(2k)})$$

where

$$\deg p^{(2k)}_{i,j}(l_1, l_2, \ldots, l_k, p_1, l_12) = \begin{cases} 3, & (i,j) = (i,i)^{'} \text{ or } (i,j) = (i,i+1), \\ 4, & (i,j) = (i,i) \text{ or } (i,j) = (i+1,i) \end{cases}$$

and

$$\deg l^{(2k+1)}_{i,j}(l_1, l_2, \ldots, l_k, p_1, l_12) = \begin{cases} 4, & (i,j) = (i,i)^{'} \text{ or } (i,j) = (i,i+1), \\ 3, & (i,j) = (i,i) \text{ or } (i,j) = (i+1,i) \end{cases}$$

Finally using the affine transformation in the same way as in [25], independently from the length of the password we get the polynomials of degree 4. □

Canonical graph homomorphisms $D(n,K) \to D(n-1,K)$ can be naturally expanded to group homomorphism $TF_{n+2}(K)$ onto $TF_{n+1}(K)$. It means that group $TF(K)$ is a projective limit of $TF_n(K)$. Let δ_n be a canonical homomorphism of $TF(K)$ onto $TF_n(K)$.

Proposition 4. *The order of a product g of generators $s_{\alpha,\beta}$ of $TF(K)$, such that α and β are elements of* Reg(K) *is infinity. Let $g \in CD(K)$ be an element of length $l(g) = k$, then the order of $g_n = \delta_n(g)$, where $[n+5]/2 \geq k$, is bounded below by $[n+5]/2k$. The sequence g_n forms a family of stable elements.*

That statement follows from the fact that the orbit of g containing triple (0)[0](0) is an infinite set.

So element $h = \tau^{-1}h^{-1}g_n h\tau$, where $\tau \in AGL_n(K)$, $h \in TF_n(k)$ is an element for which $h^{-1}g_n h$ is a cubical map, can be used as the base for Diffie-Hellman algorithm as above.

4. Remarks on the complexity of public rules

The combination T_1NT_2 of graph transformation N with two affine transformations T_1 and T_2 can be used as polynomial public rules. Public user getting a formula:

$$y = (F_1(x_1, \dots, x_n), \dots, F_n(x_1, \dots, x_n)),$$

where $F_i(x_1, \dots, x_n)$ are polynomials of n variables of degree 4.

Hence the process of straightforward encryption can be done in polynomial time $O(n^5)$. But the cryptanalyst Catherine, having a only a formula for y, has very hard task to solve the system of n equations in n variables of degree 4. We know that the variety of solution has the dimension 0. So general algorithm for finding the solution of system of polynomials cubic equations has exponential time $4^{O(n)}$.

References

[1] N.L. Biggs, *Graphs with large girth*, Ars Combinatoria, 25C (1988), 73–80.

[2] B. Bollobás, *Extremal Graph Theory*, Academic Press,

[3] Neal Coblitz, *A Course in Number Theory and Cryptography*, Second Edition, Springer, 1994, 237 p.

[4] Neal Coblitz, *Algebraic Aspects of Cryptography*, Springer, 1998, 198 p.

[5] , P. Guinand and J. Lodge, "Tanner Type Codes Arising from Large Girth Graphs", Proceedings of the 1997 Canadian Workshop on Information Theory (CWIT '97), Toronto, Ontario, Canada, pp. 5-7, June 3-6, 1997.

[6] P. Guinand and J. Lodge, *Graph Theoretic Construction of Generalized Product Codes*, Proceedings of the 1997 IEEE International Symposium on Information Theory (ISIT '97), Ulm, Germany, p. 111, June 29-July 4, 1997.

[7] Jon-Lark Kim, U. N. Peled, I. Perepelitsa, V. Pless, S. Friedland, *Explicit construction of families of LDPC codes with no 4-cycles* , Information Theory, IEEE Transactions, 2004, v. 50, Issue 10, 2378 - 2388.

[8] M. Klissowski, V. Ustimenko, *On the implementation of public keys algorithms based on algebraic graphs over finite commutative rings*, Proceedings of International CANA conference, Wisla, 2010.

[9] S. Kotorowicz, V. Ustimenko, *On the implementation of cryptoalgorithms based on algebraic graphs over some commutative rings*, Condensed Matter Physics, 2008, vol. 11, No. 2(54), (2008) 347–360.

[10] F. Lazebnik, V. A. Ustimenko, A. J. Woldar, *A Characterization of the Components of the graphs $D(k, q)$*, Discrete Mathematics, 157 (1996) 271–283.

[11] F. Lazebnik F. and V. Ustimenko, *Explicit construction of graphs with an arbitrary large girth and of large size*, Discrete Appl. Math. , 60, (1995), 275 - 284.

[12] F. Lazebnik, V. A. Ustimenko and A. J. Woldar, *A New Series of Dense Graphs of High Girth*, Bull (New Series) of AMS, v.32, N1, (1995), 73-79.

[13] A. Lubotsky, R. Philips, P. Sarnak, *Ramanujan graphs*, J. Comb. Theory., 115, N 2., (1989), 62-89.

[14] G. A. Margulis, *Explicit construction of graphs without short cycles and low density codes*, Combinatorica, 2, (1982), 71-78.

[15] E. H. Moore, *Tactical Memoranda*, Amer. J. Math., v.18, 1886, 264-303.

[16] B. Mortimer, *Permutation groups containing affine transformations of the same degree*, J. London Math. Soc., 1972, 15, N3, 445-455.

[17] V. Ustimenko, *Graphs with Special Arcs and Cryptography*, Acta Applicandae Mathematicae, 2002, vol. 74, N2, 117-153.

[18] V. A. Ustimenko, *Linguistic Dynamical Systems, Graphs of Large Girth and Cryptography*, Journal of Mathematical Sciences, Springer, vol.140, N3 (2007) pp. 412-434.

[19] V. Ustimenko, *On the graph based cryptography and symbolic computations*, Serdica Journal of Computing, Proceedings of International Conference on Application of Computer Algebra, ACA-2006, Varna, N1 (2007).

[20] V. A. Ustimenko, *Maximality of affine group, and hidden graph cryptosystems*, J. Algebra and Discrete Math., 10 (October 2004), 51-65.

[21] V. A. Ustimenko, *Coordinatisation of regular tree and its quotients*, in "Voronoi's impact on modern science, eds P. Engel and H. Syta, book 2, National Acad. of Sci, Institute of Matematics, 1998, 228p.

[22] V. Ustimenko, *CRYPTIM: Graphs as Tools for Symmetric Encryption*, in Lecture Notes in Computer Science, Springer,2001, v. 2227, 278-287.

[23] V. Ustimenko, *On the extremal graph theory for directed graphs and its cryptographical applications* In: T. Shaska, W.C. Huffman, D. Joener and V. Ustimenko, Advances in Coding Theory and Cryptography, Series on Coding and Cryptology, vol. 3, 181-200 (2007).

[24] V. A. Ustimenko, *On the cryptographical properties of extremal algebraic graphs*, in Algebraic Aspects of Digital Communications, NATO Science for Peace and Security Series - D: Information and Communication Security, Volume 24, July 2009, 296 pp.

[25] A. Wroblewska *On some properties of graph based public keys* , Albanian Journal of Mathematics, Volume 2, Number 3, 2008, 229-234 p.

Maria Curie-Sklodowska University in Lublin (Poland)
E-mail address: ustymenko_vasyl@yahoo.com, awroblewska@hektor.umcs.lublin.pl