ALBANIAN JOURNAL
OF MATHEMATICS
Volume 4, Number 4, Pages 203–211
ISSN 1930-1235: (2010)

ON THE KEY EXCHANGE WITH MATRICES OF LARGE ORDER AND GRAPH BASED NONLINEAR MAPS

URSZULA ROMAŃCZUK AND VASYL USTIMENKO

HUMAN CAPITAL
NATIONAL COHESION STRATEGY

EUROPEAN
SOCIAL FUND

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. In the paper we discuss the group theoretical algorithm of Diffie - Hellman key exchange in the cases of symmetrical group S_{p^n} and more general Cremona group of polynomial automorphisms of free module $\mathbb{K}^n$ over arbitrary commutative ring $\mathbb{K}$. We show that conjugation of affine map with nonlinear polynomial map f can be element of large order and small degree. Same properties hold for each element of cyclic group generated by such elements. We consider some algorithms for generation of subgroups of large order and small degree of their elements.

1. Introduction

It is a well-known fact that the 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 a reputation to be a difficult one. But even in the case of cyclic group $\mathbb{Z}_n^*$ there are many open questions. If $n = p$ or $n = pq$ 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 other cases complexity of discrete logarithm problem is not 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 ${\mathbb{F}_p}^n$ into itself. Obviously $|S_{p^n}| = p^n!$, each permutation π can be written in the form

Key words and phrases. Key exchange, Public Key Cryptography, Symbolic Computations .

$$\begin{aligned}
x_1 &\to f_1(x_1, x_2, \ldots, x_n),\\
x_2 &\to f_2(x_1, x_2, \ldots, x_n),\\
&\ldots\\
x_n &\to f_n(x_1, x_2, \ldots, x_n),
\end{aligned}$$

where f_i are multivariable polynomials from $\mathbb{F}_p[x_1, x_2, \ldots, x_n]$. 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.

The Diffie Hellman key exchange is another breakthrough in public-key cryptography of the 1970s, invented by Whitfield Diffie and Martin Hellman in their groundbreaking 1976 paper New Directions in Cryptography. Algorithm Diffie-Hellman allows two users (Alice and Bob) to establish a shared secret key used by encryption algorithms, such as DES or MD5, over an insecure communications channel.

Algorithm 1. ***Symbolic Diffie-Hellman algorithm***

1. The first step Alice and Bob take is to agree on a finite group G, $G < S_{p^n}$ and a polynomial map g in G of large order in a group G. This is usually done long before the rest of the protocol. The next step is for Alice to pick a secret integer n_A that she does not reveal to anyone, while at the same time Bob picks an integer n_B that he keeps secret.
3. Bob and Alice use their secret integers to compute $A = g^{n_A}$ and $B = g^{n_B}$ in S_{p^n}, respectively. They use composition of multivariable map g with itself.
4. They next exchange these computed values, Alice sends A to Bob and Bob sends B to Alice.
5. Finally, Bob and Alice again use their secret integers to compute

$$AB \equiv B^{n_A} \equiv (g^{n_B})^{n_A} = g^{n_A n_B} \qquad \text{and} \qquad AB \equiv A^{n_B} \equiv (g^{n_A})^{n_B} = g^{n_A n_B}$$

Eavesdropper only learns p, g, g^{n_A} and g^{n_B}, but cannot calculate $g^{n_A n_B}$ without the computationally difficult discrete logarithm problem of A or B for the group G.

The security of the protocol depends heavily on the choice of the base g. It has to be an element of large order $|g|$, prime decomposition of $|g|$ is very important.

This scheme of "symbolic Diffie-Hellman algorithm" can be secure, if the 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 degh_A and deg$g$.

To avoid such trouble one can look at the element (base) g of S_{p^n} such that all its nonidentical powers q^k are of small degree $f(n)$, which is independent of parameter k. We refer to such g as stable element. In the of prime field $\mathbb{F}_p$, affine transformations form an affine group $AGL_n(\mathbb{F}_p)$ of order $(p^n-1)(p^n-p)\ldots(p^n-p^{n-1})$ in the symmetric group S_{p^n} of order $(p^n)!$. In [6] the maximality of $AGL_n(\mathbb{F}_p)$ 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 $\tau_1, \tau_2 \in AGL_n(\mathbb{F}_p)$ and g is a fixed map of degree

≥ 2. One may choose quadratic map of Imai - Matsumoto algorithm in case $p = 2$ (see [4]0 for its description and cryptanalysis by J. Patarin) or graph based cubical maps for general p ([12], [14], [16], [17]).

One of the obvious source of stable elements is the group $AGL_n(\mathbb{F}_p)$ of affine transformations. We can take the group G in the form $\tau H \tau^{-1}$, where H is a subgroup of $AGL_n(\mathbb{F}_p)$ and τ is a fixed element of S_{p^n}. Degree of each representative of $AGL_n(\mathbb{F}_p)$ is 1, this group contains elements of large order, like famous Singer cycle of order $p^n - 1$ (see [5] and further references) . The choice of nonlinear τ is important, it eliminates the usage of standard tools of linear algebra for studies of H-invariant subspaces.

One can consider the product of a Singer cycle with the matrix whose order is mutually prime with $p^n - 1$ to make the order flexible.

We refer to an element g of kind $f\tau f^{-1}$, where $\tau \in AGL_n(\mathbb{F}_p)$, f and f^{-1} are polynomial maps of ${\mathbb{F}_p}^n$ into itself of the same degree such as $f\tau \neq \tau f$ as quasi linear map. We say that $g = f\tau f^{-1}$ is of *irreducible degree* if $\deg(g) = \deg(f)\deg(f^{-1})$. In case of stable pseudo linear element g of irreducible degree all its nonidentical powers are of irreducible degree.

We suggest the following scheme:

(1) Choose an affine transformation τ of large order S (for instance a product of Singer cycle with the matrix of order t such that $gcd(t, p^n - 1) = 1$).
(2) Construct invertible polynomial transformation f of large degree of rather general form.
(3) Compute $b = f\tau f^{-1}$ ("most" elements of that kind $f\tau^k f^{-1}$ will be of maximal degree $\deg(f)\deg(f^{-1})$).

Method of construction of sequences of stable elements in S_{p^n} of nonpseudolinear nature with large degree and order are consider in the papers of [16].

We believe that independently on our scheme problems of generation of matrices of large order and construction of invertible polynomials of large degree are of applied nature.

We generalize the above problem for the case of Cremona group of the free module $\mathbb{K}^n$, where $\mathbb{K}$ is arbitrary commutative ring. So we need change ${\mathbb{F}_p}^n$ for free module $\mathbb{K}^n$ (Carthesian power of $\mathbb{K}$) and the family and symmetric group S_{p^n} for Cremona group $C_n(\mathbb{K})$ of all polynomial automorphisms of $\mathbb{K}^n$.

2. Linguistic graphs and nonlinear elements of Cremona group

The missing definitions of graph-theoretical concepts which appear in this paper can be found in [1]. 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 , for instance [1]).

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 neighbors of each element is finite and depends only on its type (point or line), then the incidence structure is a tactical configuration in the sense of Moore (see [7]).

Definition 1. Let Γ be a bipartite graph with partition sets P_i, $i = 1, 2$. Suppose that M be a disjoint union of finite sets M_1 and M_2. We say that Γ is a *bipartite parallelotopic graph* over (M_1, M_2) if

(i) there exists a function $\pi : V(\Gamma) \to M$ such that if $p \in P_i$, then $\pi(p) \in M_i$,
(ii) for every pair (p, j), $p \in P_i$, $j \in M_i$, there is a unique neighbour u with given $\pi(u) = j$.

It is clear that the bipartite parallelotopic graph Γ is a $(|M_1|, |M_2|)$ - biregular graph.

We refer also to the function π in the definition of bipartite parallelotopic graph as a *labelling*. We will often omit the term "bipartite", because all our simple graphs are bipartite.

Let P and L be two copies of n-dimensional free module $\mathbb{K}^n$ over the finite commutative ring $\mathbb{K}$. 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 choose two fixed bases and write:

$$(p) = (p_1, \dots, p_n, c_1, c_2, \dots, c_r)$$

$$[l] = [l_1, \dots, l_n, t_1, t_2, \dots, t_s]$$

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:

$$\begin{aligned}
a_1 l_1 - b_1 p_1 &= f_1(c_1, \dots c_r, t_1, \dots, t_s)\\
&\dots\\
a_i l_i - b_i p_i &= f_i(c_1, \dots c_r, t_1, \dots, t_s, l_1, \dots, l_{i-1}, p_1, \dots, l_{i-1})\\
&\dots\\
a_n l_n - b_n p_n &= f_n(c_1, \dots c_r, t_1, \dots, t_s, l_1, \dots l_{n-1}, p_1, \dots, p_{n-1})
\end{aligned} \tag{1}$$

where f_i, $i = 2, \dots, n$ can be any polynomial expressions in variables c_1, $\dots$, c_r, t_1, $\dots$, t_s, l_1, $\dots$, l_{i-1}, p_1, $\dots$, p_{i-1} over $\mathbb{K}$, a_i, b_i can be any nonzero elements from $\mathbb{K}$.

It is easy to see that the above graph is a parallelotopic graph such that tuples $c_1, \dots c_r$ and $t_1, \dots, t_s$ be the "colours" of (p) and $[l]$, respectively. Let $C(P) = \mathbb{K}^r$ and $C(L) = \mathbb{K}^s$ are sets of colours for points and Lines

Let us refer to the graph $I = I(n, r, s)$ defined by above equations as *linguistic graphs of triangular type over* $\mathbb{K}$ of type (r, s, n). We assume that one of the expressions f_i, $i = 1, 2, \dots, n$ has degree ≥ 2.

The *colour function* π for such a graph is just a projection of tuples $(p) \in P$ and $[l] \in L$ onto r and s last components, respectively. We assume that $N_c(v)$ is the operator of taking the neighbour of v of colour c in our parallelotopic graph.

The linguistic graphs naturally appear as induced subgraphs of Incidence Geometries of Finite Simple Groups of Lie type. They play an important role in studies of Large Schubert cell related to the geometry ([10], [11]). The following examples are induced subgraphs of incidence geometries of rank 2. The theory of incidence geometries corresponding to finite simple groups of Lie type the reader can find in [2], [9]. Special dynamical systems related to linguistic graphs were introduced in [15].

Example 1. Let $P = \{(x_1, x_2)|x_i \in GF(q)\}$, $L = \{[y_1, y_2]|y_i \in GF(q)\}$. Let us define an incidence relation I_1 as: $(a, b)I_1[x, y]$ if and only if $y - b = xa$. Let us consider the function $\pi : P \cup L \to GF(q)$, such that $\pi((x_1, x_2)) = x_1$, $\pi([y_1, y_2]) = y_1$. It is easy to check that π is a labelling for the graph I_1. It is a linguistic graph of type $(1, 1, 1)$ over $GF(q)$. This is the induced subgraph of the incidence graph of the geometry for simple group $A_2(q)$ (classical Desargues projective plane).

Example 2. Let $P = \{(x_1, x_2, x_3)|x_i \in GF(q)\}$, $L = \{[y_1, y_2, y_3]|y_i \in GF(q)\}$. Let us define an incidence relation I_2 as: $(a, b, c)I_2[x, y, z]$ if and only if

$$y - b = xa \text{ and } z - c = xb.$$

Let us assume that $\pi((x_1, x_2, x_3)) = x_1$ and $\pi([y_1, y_2, y_3]) = y_1$. It is clear, that I_2 defines a family of linguistic graphs over $GF(q)$ with parameters (1, 1, 2). This is the induced subgraph of the incidence graph of the geometry for simple group $B_2(q)$ (classical regular generalised quadragon). So the girth of I_2 (length of minimal cycle) is at least 8.

Example 3. Let $P = \{(x_1, x_2, x_3, x_4, x_5)|x_i \in GF(q)\}$, $L = \{[y_1, y_2, y_3, y_4, y_5]|y_i \in GF(q)\}$. Let us define an incidence relation I_3 as: $(a, b, c, d, e)I_3[x, y, z, u, v]$ if and only if

$$\begin{aligned} y - b &= xa \\ z - 2c &= -2xb \\ u - 3d &= -3xc \\ 2v - 3e &= 3zb - 3yc - ua \end{aligned}$$

From the equations above, it follows that $\pi : \pi((x_1, x_2, x_3, x_4, x_5)) = x_1$ and $\pi([y_1, y_2, y_3, y_4, y_5]) = y_1$ is a labelling for I_3.

This is the induced subgraph of the geometry of group $G_2(q)$ (generalised gexagon).

If char$GF(q) > 3$ then the girth of this graph is at least 12. Directly from the equations above we can get that I_3 is the linguistic graph with parameters (1, 1, 4) over $GF(q)$.

Example 4. Let $GF(q^2)$ be the quadratic extension of $GF(q)$ and $x \to x^q$ be the Frobenius automorphism of $GF(q^2)$. Let $P = \{(x_1, x_2, x_3)|x_1 \in GF(q), x_2 \in GF(q^2), x_3 \in GF(q)\}$, $L = \{[y_1, y_2, y_3]|y_1 \in GF(q^2), y_2 \in GF(q^2), y_3 \in GF(q)\}$. Let us define the incidence relation I_4 as: $(a, b, c)I_4[x, y, z]$ if and only if

$$\begin{aligned} y - b &= xa \\ z - c &= ay + ay^q. \end{aligned}$$

It is clear that rules $\pi((x_1, x_2, x_3)) = x_1$ and $\pi([y_1, y_2, y_3]) = y_1$ define the parallelotopic graph over $GF(q^2)$, It is a linguistic graph over $\mathbb{F}_q$ of the type it's parameters are $(1, 2, 3)$.

Algorithm 2. Let us consider the sequence of linguistic graphs $I_1, I_2, \dots, I_d$ of the same type (n, r, s) over commutative ring $\mathbb{K}$.

Let $C_j(P)$ and $C_j(L)$ be sets of colours for points and lines in the graph I_j. Let η_j, $j = 2, 3, \dots, d$ and ${\eta_j}'$, $j = 1, 2, \dots, d-1$ be the affine maps from $C_1(P)$ to $C_j(P)$ and $C_j(L)$, respectively. Let us assume that η_d is an invertible affine map.

We need also an invertible affine transformations $\delta_1$and δ_2 of the point set P_1 and the point set P_d within the graphs I_1 and I_d, respectively.

We take general point $\mathrm{x} = (x_1, x_2, \dots x_{n+r})$ from P_1 and compute $v_1 = \delta_1(\mathrm{x})$ and the color $c_1 = \pi(v_1)$. After that we are compute consequently colours ${c_j}' = \eta'_j(c_1)$, $j = 1, 2, \dots, d-1$, $c_j = \eta_j(c_1)$, $j = 2, 3, \dots, d$. It allows us to compute the bijective composition of $\delta_1 N_{c'_1} N_{c_2} N_{c'_2} \dots N_{c_{d-1}} N_{c'_{d-1}} N_{c_d} \delta_2$. Let

$$u = \delta_1 N_{c'_1} N_{c_2} N_{c'_2} \dots N_{c_{d-1}} N_{c'_{d-1}} N_{c_d} \delta_2(\mathrm{x}).$$

The inverse of our map is the following one. We apply ${\delta_2}^{-1}$ to u and get the vertex u' of the graph of colour $c_d = \eta_d(\pi(v_1))$. The map η_d is invertible. So we compute c_1 and all colours c_j and ${c_j}'$. It allows us to compute x as $N_{c'_{d-1}} N_{c_{d-1}} \dots N_{c_2} N_{c'_1} N_{c_1} {\delta_1}^{-1}(u')$.

Remark 1. In case of regular linguistic graphs we can also add $c'_d = \eta'_d(c_1)$.

Example 5. Let us consider the following bipartite algebraic graph $A = A(n, \mathbb{K})$ (*a*lternating graph) defined over commutative ring $\mathbb{K}$ by the following rules.

Partition sets P and L are two copies of the free module $\mathbb{K}^n$. Brackets and paranthesis allow us to distinguish point $\mathrm{p} = (p_1, p_2, \dots, p_n)$ and line $\mathrm{l} = [l_1, l_2, \dots, l_n]$. In case of even $n = 2t$ point p is incident to line l if and only if the following equations hold:

(1) $l_{2s} - p_{2s} = l_1 p_{2s-1}$ for $s = 1, 2, \dots t$, $t = [n/2]$
(2) $l_{2s-1} - p_{2s-1} = p_1 l_{2s-2}$ for $s = 2, 3, \dots, d$,

where $d = t$ for even n and d=t+1 if n is odd.

The graph is a linguistic graphs of triangular type over $\mathbb{K}$ of type $(1, 1, n-1)$.

We announce here the following statement.

Proposition 1. If we set $I_1 = A(n, \mathbb{K}), I_2 = A(n, \mathbb{K}), \dots, I_d = A(n, \mathbb{K})$, $n \geq 2$, $d \leq n$ and nonidentical map η_d of $\mathbb{K}$ onto itself, then the algorithm 2 produces a cubical map of $\mathbb{K}^n$ onto itself.

Let $C_j(P)$ and $C_j(L)$ be sets of colours for points and lines in the graph I_j. Let η_j, $j = 2, 3 \dots, d$ and $j = 1, 2 \dots, d$ and ${\eta_j}'$, $j = 2, 3 \dots, d$ be the affine maps from $C_1(P)$ to $C_j(L)$ and $C_j(L)$, respectively. Let us assume that η_d is an invertible affine map. We implement the key exchange algorithm in the case $\mathbb{K} = \mathbb{F}_q$ with the base $b = f^{-1} A f$ where f is a cubical map as in Proposition 1 and A is a linear map corresponding to Singer cycle of order $q^n - 1$. Alternatively we can use different cubical map defined in [12], [14], [16], [7]. Obviously the order of b is $q^n - 1$ and degree of each b^k is bounded by 9.

2.1. **Symbolic computations on flags of linguistic graphs.** Let us consider a tactical configuration of order (s, t) for biregular bipartite simple graphs with bidegrees $s+1$ and $r+1$. It corresponds to incidence structure with the point set P, line set L and symmetric incidence relation I. Its size can be computed as $|P|(s+1)$ or $|L|(t+1)$. For the simplicity we choose $t=s$

Directed graph is an irreflexive binary relation $\phi \subset V \times V$, where V is the set of vertices (see [1]).

Let us introduce two sets

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

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

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 $F = \{(p,l) | p \in P,\ l \in L,\ pIl\}$ be the totality of flags for the regular tactical configuration T with partition sets P (point set) and L (line set) and incidence relation I. We define the following irreflexive binary relation ϕ on the set F: Let (P,L,I) be the incidence structure corresponding to regular tactical configuration of order t.

Let $F_1 = \{(l,p) | l \in L, p \in P, lIp\}$ and $F_2 = \{[l,p] | l \in L, p \in P, lIp\}$ be two copies of the totality of flags for (P,L,I). Brackets and parenthesis allow us to distinguish elements from F_1 and F_2. Let $DF(I)$ be the directed graph (double directed flag graph) on the disjoint union of F_1 with F_2 defined by the following rules:

(i) $(l_1,p_1) \to [l_2,p_2]$ if and only if $p_1 = p_2$ and $l_1 \neq l_2$,
(ii) $[l_2,p_2] \to (l_1,p_1)$ if and only if $l_1 = l_2$ and $p_1 \neq p_2$.

Let Γ be a directed graph as above on the set of vertices $F_1 \cup F_2$.

Let us assume that additionally we have a parallelotopic colouring π on T . Then we assume that $\pi[l,p] = \pi(l)$ and $\pi(l,p) = \pi(p)$.

Then for each vertex v of double directed graph and each colour c we have unique vertex u such that $\pi(u) = c$ and $v \to u$. We assume that $N_c(v) = u$.

Algorithm 3. Let us consider the sequence of regular linguistic graphs I_1, I_2, …, I_d of the same type (r,r,n) over commutative ring $\mathbb{K}$. Suppose that $N_c^i(v)$, $i = 2,,3\dots,d$ be the sequence of the operators taking the neighbour of v of colour c in graph I_i. Let $\eta_i,\ i = 2,3,\dots,d$ be the sequence of affine maps of $\mathbb{K}^r$ into $\mathbb{K}^r$. We take η^d as inveritable map.

We need also an invariable affine transformations δ_i, $i = 1,2$ of the free module $\mathbb{K}^{n+2r}$ into itself.

We take the general flag x $= (x_1,\ x_2,\dots,\ x_{n+2r})$ from F_1 and the colour $c_1 \in \mathbb{K}^r$ and compute $N_{c_2}^2(\mathrm{x}) = v \in F_2$. After we compute the consequently colours $c_i = \eta_2(c_1)$, $i = 2,3,\dots,d$.

It allow us to compute symbolically the map $f = \delta_1 N_{c_3}^3 N_{c_4}^4 \cdots N_{c_{d-1}}^{d-1} N_{c_d}^d \delta_2$ of the free module $\mathbb{K}^{n+2r}$ into itself. The output of our algorithm is the flag $w = f(v)$.

Constructing an inverse mapping to f, we assume that the vertices which belong to F_1 now belong to F_2 and vice versa, vertices belonging to F_2 now belong to F_1. The map η_d is inveritable, so we compute c_1 and c_j, $j = 2,3,\dots,d$. It allows as to compute v as $\delta_2^{-1} N_{c_{d-2}}^{d-1} N_{c_{d-3}}^{d-2} \cdots N_{c_2}^3 N_{c_1}^2 \delta_1^{-1}(w)$.

Remark 2. *The above algorithm can be easily generalised on the sequence of biregular linguistic graphs of the same type* (r,s,n).

Table 1. Time of public key generation

	$d = 10$	$d = 20$	$d = 30$	$p = 40$	$d = 50$	$d = 60$
$n = 10$	7	7	8	15	15	16
$n = 20$	54	125	195	265	343	421
$n = 30$	304	742	1234	1703	2234	2805
$n = 40$	1109	3696	6414	9109	12284	14812
$n = 50$	2750	8937	17039	24976	33374	41164
$n = 60$	6101	21312	43961	69453	96421	121267
$n = 70$	11371	40726	84625	143094	202750	268320
$n = 80$	23007	82937	175320	309960	455890	601187
$n = 90$	46062	166320	354429	631469	947328	1262682
$n = 100$	929625	293641	641305	1110305	1752766	244981

Proposition 2. If we set $I_1 = A(n, \mathbb{K}), I_2 = A(n, \mathbb{K}), \ldots,\ I_d = A(n, \mathbb{K}),\ n \geq 2$, $d \leq n$ and nonidentical map η_d of K onto itself, then the algorithm 2 also produces a cubical map of $\mathbb{K}^n$ onto itself.

3. Time evaluation of the generation of the map f

The parameter n is the dimension of point space ${\mathbb{F}_{2^k}}^n$ of our graph. Below you can find time evaluation tables for symbolic computations of f in cases of finite fields $\mathbb{K} = \mathbb{F}_{2^k}$, $k \in \{8, 16, 32\}$.

All the tests were run on a computer with parameters:

- AMD Athlon 1.46 GHz processor
- 1 GB RAM memory
- Windows XP operating system.

The table **??** presents the time (in milliseconds) of the generation of the symbolic base depending on the number of variables (n) and the size of parameter (d). In fact we ignore the restriction $d < n$. In all cases the base is a cubical map. We use sparse linear transformations $\delta_i, i = 1, 2$ of kind $x_1 \to a_1x_2 + a_2x_3 + \ldots, a_nx_n$, $x_j \to x_j$, $j = 2, 3, \ldots$ where a_i are fixed nonzero field elements.

4. Remarks on the b^k as a public rule

The transformation b or b^k can be used as a public rules. Hence the process of straightforward computation of b for chosen point p can be done in polynomial time $O(n^{10})$. But the adversary having only a standard formula for b, has a very hard task to solve the system of n equations in n variables of degree 9 . We know that the variety of solution has the dimension 0. Therefore, general algorithm for finding the solution of system of polynomials cubic equations has exponential time $9^{O(n)}$.

References

[1] B. Bollobás, *Extremal Graph Theory*, Academic Press, 1982

[2] R. W. Carter, *Simple Groups of Lie Type*, Wiley, New York, 1977. (1972).

[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] A. Cossidente, M. J. de Ressmine, *Remarks on Singer Cycle Groups and Their Normalizers*, Desighns, Codes and Cryptography, 32, 97-102, 2004.

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

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

[8] J. Tits, *Sur la trialite at certains groupes qui s'en deduicent*, Publ. Math. I.H.E.S. 2 (1959), 15-20.

[9] J. Tits, *Buildings of spherical type and Finite BN-pairs, Lecture Notes in Math*, Springer Verlag, 1074.

[10] V. A. Ustimenko, *On the Varieties of Parabolic Subgroups, their Generalizations and Combinatorial Applications*, Acta Applicandae Mathematicae 52 (1998): pp. 223–238.

[11] V. A. Ustimenko, *Graphs with Special Arcs and Cryptography*, Acta Applicandae Mathematicae, vol. 71, N2, November 2002, 117-153.

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

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

[14] 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).

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

[16] V. A. Ustimenko, A. Wróblewska, *On the key exchange with nonlinear polynomial maps of degree 4* (to appear)

[17] A. Wróblewska *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: urszula_romanczuk@yahoo.pl, and ustimenko_vasyl@yahoo.com