Annales UMCS Informatica AI XI, 4 (2011) 11–19
DOI: 10.2478/v10065-011-0038-z

Annales UMCS
Informatica
Lublin-Polonia
Sectio AI
http://www.annales.umcs.lublin.pl/

On the key exchange with new cubical maps based on graphs

Urszula Romańczuk[1*], Vasyl Ustimenko[1†]

[1] *Institute of Mathematics, Maria Curie-Sklodowska University, pl. M. Curie-Sklodowskiej 5, 20-031 Lublin, Poland*

Abstract – Families of edge transitive algebraic graphs $F_n(K)$, over the commutative ring K were used for the graph based cryptographic algorithms. We introduce a key exchange protocol defined in terms of bipartite graph $A_n(K)$, $n \geq 2$ with point set P_n and line set L_n isomorphic to n-dimensional free module K^n. Graphs $A(n, K)$ are not vertex and edge transitive. There is a well defined projective limit $\lim A(n, K) = A(K)$, $n \to \infty$ which is an infinite bipatrtite graph with point set $P = \lim P_n$ and line set $L = \lim L_n$. Let K be a commutative ring contain at least 3 regular elements (not zero divisors). For each pair of (n, d), $n \geq 2, n \geq 1$ and sequence of elements $\alpha_1, \alpha_2, \ldots, \alpha_{2d}$, such that α_1, $\alpha_i + \alpha_{i+1}$, $i = 1, 2, \ldots, 2d$, $i = 1, 2, \ldots 2d-1$ and $\alpha_{2d}+\alpha_1$ are regular elements of the ring K. We define polynomial automorphism $h_n = h_n(d, \alpha_1, \alpha_2, \ldots, \alpha_{2d})$ of variety L_n (or P_n). The existence of projective limit $\lim A_n(K)$ guarantees the existence of projective limit $h = h(d, \alpha_1, \alpha_2, \ldots, \alpha_{2d}) = \lim h_n$, $n \to \infty$ which is cubical automorphism of infinite dimensional varieties L (or P). We state that the order of h is an infinity. There is a constant n_0 such that h_n , $n \geq n_0$ is a cubical map. Obviously the order of h_n is growing with the growth of n and the degree of polynomial map $(h_n)^k$ from the Cremona group of all polynomial automorphisms of free module K^n with operation of composition is bounded by 3. Let τ be affine automorphism of K^n i.e. the element of Cremona group of degree 1. We suggest "symbolic" Diffie Hellman key exchange with the use of cyclic subgroup of Cremona group generated by $\tau^{-1} h_n \tau$. In the case of $K = \mathbb{F}_p$, p is prime, the order of h_n is the power of p. So the order is growing with the growth of p. We use computer simulation to evaluate the orders in some cases of $K = \mathbb{Z}_m$, where m is a composite integer.

*urszula_romanczuk@yahoo.pl
†ustymenko_vasyl@yahoo.com

1 Introduction

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

The Diffie-Hellman key exchange uses the discrete logarithm problem for a general finite group G. This issue is dependent on the form of presentation of the group. A know example is the fact that the discrete logarithm problem for the group $G = \mathbb{Z}_p^*$, p is prime, is difficult and comes down to finding a positive integer x such that the condition $g^x = b$ is satisfied, where $g, b \in G$ are known. But the $\mathbb{Z}_p^*$ is isomorphic to the abstract linear group $\mathbb{Z}_{p-1}$ where the problem comes down to finding a solution to the linear equation $gx = b$, which is easy to solve.

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 of $x_1 \to f_1(x_1, x_2, \ldots, x_n)$, $x_2 \to f_2(x_1, x_2, \ldots, x_n)$, $\ldots$, $x_n \to f_n(x_1, x_2, \ldots, x_n)$, 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. Another reason is its universality: as it follows from the classical Cayley results each finite group G can be embedded in S_{p^n} for appropriate p and n in various ways. However, there is the problem if $g \in S_{p^n}$ and the degree of g^k is a linear function of k. In this case, the discrete logarithm is easy to solve. 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 the stable element. In the simplest case of prime field $\mathbb{F}_p$ the source of stable elements is the group $AGL_n(F_p)$ of affine transformations. Of course, the degree of each representative of $AGL_n(F_p)$ is 1. Affine transformations form an affine group $AGL_n(\mathbb{F}_p)$ of the order $(p^n - 1)(p^n - p)\ldots(p^n - p^{n-1})$ which is a subgroup in the symmetric group S_{p^n} of the order $(p^n)!$. In [**1**] 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 the 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 graph based cubical maps for general prime p ([**2, 3, 4**]).

The method of construction of sequences of stable elements in S_{p^n} of nonpseudolinear nature with a large degree and order are considered in paper [**4**].

Algorithm 1. Symbolic Diffie-Hellman algorithm Suppose Alice and Bob want to agree about a key K_{AB}.

1. The first step is for Alice and Bob to agree about a finite group G, $G < S_{p^n}$ and a polynomial map g in G of large order in a group G. 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.

2. 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.
3. They next exchange these computed values, Alice sends A to Bob and Bob sends B to Alice.
4. Finally, Bob and Alice again use their secret integers to compute
$$K_{AB} \equiv B^{n_A} \equiv (g^{n_B})^{n_A} = g^{n_A n_B},$$
$$K_{AB} \equiv A^{n_B} \equiv (g^{n_A})^{n_B} = g^{n_A n_B},$$
respectively.

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. An obvious bad example is the following: g sends x_i into ${x_i}^t$ for each i. In this case n_A is simply a ratio of deg$A$ and deg$g$.

We generalize the above mentioned problem for the case of Cremona group of the free module K^n, where K is an arbitrary commutative ring. So we need to change $\mathbb{F}_p^n$ for a free module K^n (Carthesian power of K) and the family and symmetric group S_{p^n} for the Cremona group $C_n(K)$ of all polynomial automorphisms of K^n. The elements of $C_n(K)$ are polynomial maps $f(x_1, x_2, \ldots, x_n) \in K[x_1, x_2, \ldots, x_n]$ such that the inverse map f^{-1} is also an element of $K[x_1, x_2, \ldots, x_n]$.

We define new families of cubical polynomial h_n from $C_n(K)$ such that

$$h = \lim_{n \to \infty} h_n$$

is a well defined projective limit, the order h acting on K^∞ is infinity and the degree of h is 3. This means that the order of T_n grows with n. Hence the polynomial of the kind $g = \tau^{-1} T_n \tau$, where τ is the affine transformation, can be used as a base for the Diffie-Hellman key exchange.

2 Graph theoretical preliminaries

A *graph* $G = (V,\ \varphi)$ *of a binary relation* $\varphi \in V \times V$ is the set of all points (x, y) (called *edges*) in a coordinate plane such that x is related to y through the binary relation φ. 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. The sequence of distinct vertices $v_0, v_1, \ldots, v_t$, such that $v_i \varphi v_{i+1}$ 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* 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 $v_i \varphi v_{i+1}$, $i = 1, \ldots, m-1$ and $v_m \varphi v_1$.

If x is related to y through the binary relation φ, then we will say that y is the *neighbour* of the vertex x. The *degree of a graph vertex* x of a graph G is the number of graph vertices which are in the relationship with the vertex x.

A *simple graph* $G = (V,\ \varphi)$ is the graph G of the binary relation φ, where φ is symmetric and irreflexive. That means a simple graph is an undirected graph containing no graph loops or multiple edges.

The missing definitions of graph-theoretical concepts in the case of simple graphs which appears in this paper can be found in **[5]**.

A *regular graph* G is the simple graph where each vertex has the same number of neighbours; i.e. every vertex has the same degree, and we say, that G is *biregular* if all the vertices of G have only two distinct values of degree. A graph G is *bipartite* i.e. if its vertices can be partitioned into two separable sets is such a way that any two vertices belonging to the same partition set are not in a relationship. The length of the shortest cycle in a graph is called the *girth* $g(G)$ of the graph G. The edge transitive graphs of large girth and their directed analogue have been used for different cryptographical algorithms **[1, 2, 3, 4, 6, 7, 8, 9, 10, 11, 12, 13]**. The paper **[14]** uses linear maps of large order conjugated by the nonlinear map of small degree for the key exchange. In this paper we use a family of algebraic graphs $A(n, K)$ for the key exchange protocol. The graphs from this family are neither edge transitive nor vertex transitive. Recall that the algebraic graph over the commutative ring K is the graph with a vertex set and an edge set, which are algebraic varieties over K in a the sense of Zarisski topology (see **[5]** or **[6]**).

3 Maps based on incidence structure

The *incidence structure* is the set V with the partition sets P (points) and L (lines) and the 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 the number of neighbours 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 **[15]**).

We will often omit the term "bipartite", because all our simple graphs are bipartite.

Let P and L be two copies of infinite dimensional free module K^∞ over the finite commutative ring K. The elements of P will be called *points* and elements of L will be called *lines*. To distinguish points from lines we use parentheses and brackets. It will also be advantageous to choose two fixed bases and write the follow way $(p) = (p_1, \ldots, p_n, \ldots)$ for the point and $[l] = [l_1, \ldots, l_n, \ldots]$ for the line. 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:

$$a_1 l_2 - b_1 p_2 = f_1(p_1, l_1)$$
$$a_i l_{i+1} - b_i p_{i+1} = f_i(p_1, p_2, \ldots, p_i, l_1, l_2, \ldots, l_i)$$

where f_i, $i = 2, 3, \ldots$, can be any polynomial expressions in variables p_2, p_2, $\ldots$, p_{i-1}, l_1,l_2, $\ldots$, l_{i-1} over K, a_i, b_i can be any nonzero elements from K and $\pi((p))$,$\pi([l])$ is the colour point (p) and line $[l]$, respectively. We will say that it defined an *infinite triangular algebraic graph* $G(K) = (P, L, I)$ over the commutative ring K, who has the set of vertices $P \cup L$ and the set of edges containing all pairs $\{(p), [l]\}$ for which $(p)I[l]$.

For each positive integer $n \geq 2$ we obtain a *triangular algebraic graph* $G(n, K) = (P_n, L_n, I_n)$ over commutative ring K in the following way. The first P_n and L_n are obtained from the P and L, respectively, by a simple projection of all vectors on the initial n coordinates. Secondly, the relation of incidence I_n is defined by the initial $n-1$ and ignoring all the other equations of the relation of incidence I.

There is a homomorphism Δ_n of the graph $G(n, K)$ into $G(n-1, K)$ mapping point $(p_1, p_2, \ldots, p_n)$ (line $[l_1, l_2, \ldots, l_n]$) into $(p_1, p_2, \ldots, p_{n-1})$ (line $[l_1, l_2, \ldots, l_{n-1}]$), respectively. It means that the projective limit $\lim_{n\to\infty} G(n, K)$ is well defined. It is clear that

$$\lim_{n\to\infty} G(n, K) = G(K)$$

We define the *colour function* π for the graph just as a projection of tuples $(p) \in P$ and $[l] \in L$ onto the first coordinate (p) or $[l]$, respectively. We assume that $N_c(v)$ is the operator of taking the neighbour of v of colour $\pi(v) + c$ in our graph.

We can generate the mapping g over $C_n(K)$ using the following algorithms.

Algorithm 2. Let $G(n, K) = (P_n, L_n, I_n)$ be the finite triangular algebraic graph over the commutative ring K. Let $c_1, c_2, \ldots, c_r$, where r is even, be a sequence of colours of vertices in our graph. Let us assume that τ is an invertible affine map over K.

We a take general point $\mathrm{x} = (x_1, x_2, \ldots x_n)$ from P and compute the bijective composition of $h_n = \tau^{-1} N_{c_1} N_{c_2} \ldots N_{c_r} \tau$.

The inverse of our map h_n is the form $h_n^{-1} = \tau^{-1} N_{-c_r} N_{-c_{r-1}} \ldots N_{-c_1} \tau$

The vertex $h_n(\mathrm{x})$ will be a point if r is even. If r is odd then $h_n(\mathrm{x})$ is the line.

So we can consider $\mathrm{x} \to h_n(\mathrm{x})$ as an element of the Cremona group $C_n(K)$.

It is useful to consider a similar map $h = \tau^{-1} N_{c_1} N_{c_2} \ldots N_{c_r} \tau$ in the infinite graph $G(K) = (P, L, I)$.

4 Families maps of cubical degree based on alternating graph

Let K be the commutative ring with at least 3 regular elements. Let us consider the following bipartite finite triangular algebraic graph $A(n, K)$ (*alternating graph*) defined over the commutative ring K.

The partition sets P_n and L_n are two copies of the free module K^n. Brackets and parentheses allow us to distinguish point $\mathrm{p} = (p_1, p_2, \ldots, p_n)$ and line $\mathrm{l} = [l_1, l_2, \ldots, l_n]$. In the 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 $s = 1, 2, \ldots t$, $t = [n/2]$
2. $l_{2s-1} - p_{2s-1} = p_1 l_{2s-2}$ for $s = 2, 3, \ldots, r$,

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

The graph $A(n, K)$ is the triangular algebraic graph over the commutative ring K. This family was defined in [**2, 16, 17**].

There is a well defined projective limit $\lim A(n, K) = A(K)$, $n \to \infty$ which is an infinite bipatrtite graph with the point set $P = \lim P_n$ and the line set $L = \lim L_n$. The family $A(n, K)$ was defined in [**2**] as a sequence of homomorphic images for the graphs from the family $D(m, K)$, $m \geq 2$. We can prove that the graphs $A(n, K)$, $n \geq 4$ are neither vertex-transitive nor edge-transitive

Let K be a commutative ring containing at least 3 regular elements (not zero divisors).

We refer to sequence of ring elements $\alpha_1, \alpha_2, \ldots, \alpha_{2d}$, such that α_1, $\alpha_i + \alpha_{i+1}$, $i = 1, 2, \ldots, 2d$, $i = 1, 2, \ldots, 2d - 1$ and $\alpha_{2d} + \alpha_1$ are regular elements of the ring K (non zero divisors) as to the cyclic regular sequence. For such a sequence we consider a bijective polynomial automorphism $h_n = h_n(d, \alpha_1, \alpha_2, \ldots, \alpha_{2d}) = N_{\alpha_1} N_{\alpha_2} \ldots N_{\alpha_{2d}}$ of variety L_n (or P_n).

The existence of the projective limit $\lim A(n, K)$ guarantees the existence of the projective limit $h = h(d, \alpha_1, \alpha_2, \ldots, \alpha_{2d}) = \lim h_n$, $n \to \infty$, which is a cubical automorphisms of infinite dimensional variety P (or L).

We introduce here the following statement.

Proposition 1. If we take algorithm 2 for the alternating graph $A(n, K)$ $(A(K))$ we get the polynomial automorphism of K^n onto itself of degree ≤ 3.

The following statement was proven in [**2**].

Lemma 1. Let $[y_1] I_n(y_2) I_n \ldots I_n [y_m]$ be the path in the graph $A(n, K)$, $n \geq 4$, starting at the zero line $y_1 = [0, 0, \ldots, 0]$ and determined by the sequence colours $0, a_1, a_2, \ldots, a_{m-1}$. Then the last two components of the vertex $[y_m]$ are $\psi = a_1 a_2 (a_1 - a_3) \ldots (a_{m-3} - a_{m-1})$ and $\zeta = -a_{m-2}\psi$.

The following proposition follows instantly from the lemma 1.

Proposition 2. The map $h = h(d, \alpha_1, \alpha_2, \ldots, \alpha_{2d})$ corresponding to the regular cyclic sequence is a cubical polynomial automorphism of infinitedimensional free module P (or L). The order of h is infinity.

Corollary 1. The order of h_n is growing with the growth of n.

Really, the assumption that $|h_n|$ is bounded leads to contradiction with Proposition 2.

Corollary 2. There is a constant n_0 such that for $n \geq n_0$ the map h_n is a cubical one.

Corollary 3. The degree of polynomial map $(h_n)^k$ (composition of h_n with itself) from the Cremona group $C(K^n)$ of all polynomial automorphisms of free module K^n is bounded by 3.

Really, the concatenation of regular cyclic sequence $\alpha_1, \alpha_2, \ldots, \alpha_{2d}$ with itself is also a regular cyclic sequence.

Remark 1. If $K = \mathbb{F}_q$, $q = p^n$ then the order of h_n is the power of p. So the order of h_n is growing with the growth of p.

Let $H_n(K)$ be the totality of all polynomial automorphisms of kind $h_n(d, \alpha_1, \alpha_2, \ldots, \alpha_{2d})$ for the free module $P_n = K^n$ (L_n), where $\alpha_1, \alpha_2, \ldots, \alpha_{2d}$ going through all cyclic regular sequences of length $d \geq 1$. Then the projective limit $H(K) = \lim H_n(K)$, $n \to \infty$ is well defined.

Proposition 3. The dimension of variety H of cubical polynomial automorphism of P (L) is infinity.

Corollary 4. The dimension of $H_n(K)$ is growing with the growth of n.

5 On the choice of the base for key exchange protocol

Let τ be affine automorphism of K^n, i.e. the element of the Cremona group of degree 1. We suggest a "symbolic" Diffie-Hellman key exchange with the use of a cyclic subgroup of the Cremona group generated by $\tau^{-1} h_n \tau$. We can choose parameters n and ring K to make the order of cubic map h as large as we want. After that we can use cubic h as a base for the symbolic Diffie-Hellman key exchange.

Conjecture 1. If we have $K = \mathbb{Z}_m$, where $m = p_1^{n_1} p_2^{n_2} \ldots p_s^{n_s}$ then orders of transformation h_n are powers of $p_1, p_2, \ldots, p_s$, i.e. there exist $k_1, k_2, \ldots, k_s \in \{0, 1, 2, \ldots\}$, such that the order is of kind $p_1^{k_1} p_2^{k_2} \ldots p_s^{k_s}$.

Table 1 present the results of computer computations for the orders of transformation h_n corresponding to the regular cyclic sequence of length d for the prime field $\mathbb{F}_p$. The program is written in the Java language. The results are achieved after 100 random tests. Table 2 presents the analogous computations for the ring $\mathbb{Z}_m$, where m is positive integer .

Table 1

	$n = 10$	$n = 100$	$n = 500$	$n = 1500$	$n = 2500$
$p = 13 \quad d = 2$	13^1	13^2	13^3	13^3	13^4
$p = 13 \quad d = 22$	13^1	13^2	13^3	13^3	13^4
$p = 13 \quad d = 30$	13^1	13^2	13^3	13^3	13^3
$p = 41 \quad d = 2$	41^1	41^2	41^2	41^2	41^3
$p = 41 \quad d = 22$	41^1	41^2	41^2	41^2	41^3
$p = 41 \quad d = 30$	41^1	41^2	41^2	41^2	41^3
$p = 113 \quad d = 2$	113^1	113^1	113^2	113^2	113^2
$p = 113 \quad d = 22$	113^1	113^1	113^2	113^2	113^2
$p = 113 \quad d = 30$	113^1	113^1	113^2	113^2	113^2

Table 2

	$n = 10$	$n = 50$	$n = 100$
$m = 2^2 5^1 \quad d = 2$	$2^1 5^1$, 5^2, 2^5, $2^1 5^2$, $2^5 5^2$	2^7, 5^3, $2^1 5^3$ $2^7 5^3$	5^3, 2^8, $2^1 5^3$, $2^5 5^2$
$m = 2^2 5^1 \quad d = 22$	$2^1 5^1$, $2^1 5^2$, $2^5 5^1$, $2^3 5^2$, $2^4 5^2$, $2^5 5^2$	5^3, $2^1 5^2$, $2^5 5^2$ $2^5 5^3$, $2^6 5^3$, $2^7 5^2$	5^3, $2^1 5^2$, $2^6 5^3$ $2^7 5^3$, $2^8 5^3$
$m = 7^1 13^1 \quad d = 2$	13^1, 7^2, $7^2 13^1$	13^2, $7^3 13^2$	13^2, 7^3, $7^3 13^2$
$m = 7^1 13^1 \quad d = 22$	$13^1 7^1$, $7^2 13^1$,	$7^2 13^2$, $7^3 13^2$	$7^3 13^2$
$m = 3^1 5^1 7^1 \quad d = 2$	3^3, 7^2, $3^3 5^2$, $5^2 7^2$ $3^3 7^3$, $3^3 5^2 7^2$	5^3, 7^3, $3^4 5^3$, $3^4 7^3$, $5^3 7^3$, $3^4 5^3 7^3$	5^3, 3^5, 7^3, $3^5 5^3$, $5^3 7^3$, $3^5 7^3$, $3^5 5^3 7^3$
$m = 3^1 5^1 7^1 \quad d = 22$	$3^3 5^1 7^1$, $3^2 5^2 7^1$, $5^2 7^1 7^2$ $3^1 5^2 7^2$, $3^3 5^1 7^2$, $3^2 5^2 7^2$ $3^3 5^2 7^2$	$5^3 7^3$, $3^3 5^3 7^2$, $3^4 5^3 7^2$, $3^3 5^3 7^3$ $3^4 5^3 7^3$	$5^3 7^3$, $3^3 5^3 7^3$ $3^4 5^3 7^3$, $3^3 5^3 7^3$
$m = 5^1 11^2 \quad d = 2$	11^1, 11^2, $5^2 11^1$, $5^2 11^2$	11^1, 5^3, 11^3, $5^3 11^1$, $5^3 11^1$, $5^3 11^3$	11^3, $5^3 11^1$, $5^3 11^3$
$m = 5^1 11^2 \quad d = 22$	$5^1 11^2$, $5^2 11^2$	$5^2 11^3$, $5^3 11^3$	$5^3 11^3$

As follows from Proposition 2 all powers of h have degrees bounded by 3. It means that h is a stable element.

OPEN PROBLEM: Let the order $\mathrm{ord}(H_n(K))$ of $H_n(K)$ be the maximal order of its representative $h_n \in H_n(K)$. Compute $\mathrm{ord}(H_n(K))$.

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

References

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

[2] Ustimenko V. A., Linguistic Dynamical Systems, Graphs of Large Girth and Cryptography, Journal of Mathematical Sciences 140(N3) (2007): 412.

[3] Ustimenko V., Algebraic graphs and security of digital communications, University of Maria Curie Sklodowska (2011): 154.

[4] Wróblewska A., On some properties of graph based public keys, Albanian Journal of Mathematics 2(3) (2008): 229.

[5] Biggs N., Algebraic Graph Theory (2nd ed), Cambridge, University Press (1993).

[6] Shaska T., Ustimenko V., On the homogeneous algebraic graphs of large girth and their applications, Linear Algebra and its Applications Article 430(7) (2009), Special Issue in Honor of Thomas J. Laffey.

[7] Ustimenko V. A., Graphs with Special Arcs and Cryptography, Acta Applicandae Mathematicae 71(N2) (2002): 117.

[8] Ustimenko V. A., Maximality of affine group, and hidden graph cryptosystems, J. Algebra and Discrete Math. 10 (2004): 51.

[9] Ustimenko V., CRYPTIM: Graphs as Tools for Symmetric Encryption, in Lecture Notes in Computer Science 2227 (2001): 278.

[10] Ustimenko V., 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 3 (2007): 181.

[11] Ustimenko V. A., On the extremal regular directed graphs without commutative diagrams and their applications in coding theory and cryptography, Albanian. J. of Mathematics, Special Issue "Algebra and Computational Algebraic Geometry" 1(N4) (2007): 387.

[12] Ustimenko V. A., On the cryptographical properties of extremal algebraic graphs, in Algebraic Aspects of Digital Communications, IOS Press (Lectures of Advanced NATO Institute), NATO Science for Peace and Security Series - D: Information and Communication Security 24 (2009): 296.

[13] Ustimenko V. A., Wróblewska A., On the key exchange with nonlinear polynomial maps of degree 4, Albanian Journal of Mathematics, Special Issue, Applications of Computer Algebra 4(4) (2010).

[14] Romańczuk U., Ustimenko V., On the key exchange with matrices of large order and graph based nonlinear maps, Albanian. J. of Mathematics, Special Issue, Applications of Computer Algebra 4(4) (2010): 203.

[15] Moore E. H., Tactical Memoranda, Amer. J. Math. 18 (1886): 264.

[16] Klisowski M., Romańczuk U., Ustimenko V., On the implementation of cubic public keys based on new family of algebraic graphs, Annales UMCS Informatica AI XI(2) (2011): 127.

[17] J. S. Kotorowicz, U. Romańczuk, V. Ustimenko *„On the implementation of stream ciphers based on a new family of algebraic graphs"* IEEE Computer Society Press, Proceedings of the Conference CANA, FedSCIS, pp. 485-490

[18] Klisowski M., Ustimenko V., On the public keys based on the extremal graphs and digraphs, International Multiconference on Computer Science and Informational Technology, October 2010, Wisla, Poland, CANA Proceedings.

[19] Koblitz N., Algebraic Aspects of Cryptography, Springer (1998): 198.

[20] Mortimer B., Permutation groups containing affine transformations of the same degree, J. London Math. Soc. 15(N3) (1972): 445.