Annales UMCS Informatica AI XI, 2 (2011) 95–111
DOI: 10.2478/v10065-011-0014-7

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

On the key expansion of $D(n, K)$-based cryptographical algorithm

Vasyl Ustimenko[1*], Aneta Wróblewska[1,2†]

[1] *Institute of Mathematics, Maria Curie-Sklodowska University*
pl. M. Curie-Sklodowskiej 1, 20-031 Lublin, Poland
[2] *Institute of Fundamental Technological Research Polish Academy of Sciences*
ul. Pawinskiego 5B; 02-106 Warszawa, Poland

Abstract

The family of algebraic graphs $D(n, K)$ defined over finite commutative ring K have been used in different cryptographical algorithms (private and public keys, key exchange protocols). The encryption maps correspond to special walks on this graph. We expand the class of encryption maps via the use of edge transitive automorphism group $G(n, K)$ of $D(n, K)$. The graph $D(n, K)$ and related directed graphs are disconnected. So private keys corresponding to walks preserve each connected component. The group $G(n, K)$ of transformations generated by an expanded set of encryption maps acts transitively on the plainspace. Thus we have a great difference with block ciphers, any plaintexts can be transformed to an arbitrarily chosen ciphertex by an encryption map. The plainspace for the $D(n, K)$ graph based encryption is a free module P over the ring K. The group $G(n, K)$ is a subgroup of Cremona group of all polynomial automorphisms. The maximal degree for a polynomial from $G(n, K)$ is 3. We discuss the Diffie-Hellman algorithm based on the discrete logarithm problem for the

*E-mail address: ustymenko_vasyl@yahoo.com
†E-mail address: awroblewska@hektor.umcs.lublin.pl

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

group $\tau^{-1}G\tau$, where τ is invertible affine transformation of free module P i.e. polynomial automorphism of degree 1. We consider some relations for the discrete logarithm problem for $G(n,K)$ and public key algorithm based on the $D(n,K)$ graphs.

1. Introduction

The graph $D(n,K)$, where K is a commutative ring, was used for the development of cryptographical algorithms:

(1) Symmetric numerical algorithms

Alice and Bob have the same key corresponding to the path in the graph $D(n,K)$ (in the case where K is not a field, the directed graph $DD(n,K)$ defined in terms of $D(n,K)$ was used).

(2) Diffie-Hellman key exchange algorithm, given in the form of public rule:

$$\tau^{-1}N_{\alpha_1}N_{\alpha_2}\dots N_{\alpha_k}\tau,$$

where τ is the affine transformation and $N_{\alpha_1}N_{\alpha_2}\dots N_{\alpha_k}$ is the graphical transformation.

(3) Public key encryption scheme:

$$g = \tau_1(g')^s\tau_2,$$

where

$$g' = N_{t_1}N_{t_2}\dots N_{t_l}$$

That means the string $(t_1t_2\dots t_l)$ repeats periodically s-times. Such encryption is protected by a discrete logarithm problem. Of course some may get the option of breaking without solution of discrete logarithm problem investigation.

In the paper we propose the extension of the key space for the symmetric algorithm and the expansion of the cubical stable group used for the key exchange problem.

The graph $D(n,K)$ is not connected so we are able to find vertices c and c' such that in the old algorithm given in [**1**] there is no encryption map moving c to c'. In the new extended algorithm the problem is solved by using automorphisms, which enables to move between different, connected components of graph $D(n,K)$ (or related $DD(n,K)$).

The discrete logarithm problem is a critical problem in the number theory, and is similar in many ways to the integer factorization problem. Like the factoring problem, the discrete logarithm problem is believed to be difficult and hard direction of a one-way function. For this reason, it has been the basis of several public-key cryptosystems, including the ElGamal system and DSS.

Although the discrete logarithm problem exists in any group, when used for cryptographic purposes the group is usually Z_n^*

The discrete logarithm problem is the following one: given an element g in a finite group G and another element $h \in G$, find a positive integer x such that $g^x = h$. The problem can be also used in elliptic curve groups.

If $C = Z_p^*$ or $C = Z_{pq}^*$ where p and q are sufficiently large primes then the complexity of discrete logarithm problem justifies the classical Diffie-Hellman key exchange algorithm and RSA public key encryption. In majority of other cases complexity of discrete logarithm problem is not investigated properly. The problem depends on the choice of the base g and the way of presentation of the data on the group. The group can be defined via generators and relations, as the automorphism group of algebraic variety, matrix group, permutation group etc. In this paper we assume that G is a subgroup of S_{q^n} which is a group of polynomial bijective transformation of the vector space ${F_q}^n$ into itself. Obviously $|S_{q^n}| = (q^n)!$.

Let g be a pseudorandomly chosen element from S_{q^n}. Then the order of the cyclic group G generated by g is unknown, if g is sufficiently large. It is known that complexity of finding g^{-1} is $d^{O(n^2)}$, where d is degree of g. So if t is the order of g, then g^{t-1} is the inverse. Hence finding t takes also time $d^{O(n^2)}$ and we have the discrete logarithm problem for the cyclic group of unknown order. We can call them a hidden symbolic discrete logarithm problem because t is unknown (hidden) and g is a polynomial map (symbolic).

It is known that each permutation π can be written in the form of $x_1 \to f_1(x_1, x_2, \dots x_n), x_2 \to f_2(x_1, x_2, \dots x_n), \dots x_n \to f_n(x_1, x_2, \dots x_n)$, where f_i, $i = 1, 2, \dots, n$ are multivariable polynomials from $F_q[x_1, x_2, \dots, x_n]$. The presentation of G as a subgroup of S_{q^n} is chosen because the Diffie-Hellman algorithm here will be implemented by the tools of symbolic computations. Another reason is universality, as it follows from the classical Cayley results each finite group G can be embedded in S_{q^n} for appropriate q and n in various ways.

Let F_q, where q is prime, be a finite field. The affine group $AGL_n(F_q)$ acting on ${F_q}^n$ is formed by the affine transformations $\mathrm{x} \to A\mathrm{x} + b$, where A is an invertible matrix and $b \in (F_q)^n$.

The order of the affine group $AGL_n(F_q)$ is $q^n(q^n - 1)(q^n - q) \dots (q^n - q^{n-1})$. Each permutation π can be presented as a composition of several maps of the kind $\tau_1 g \tau_2$, where $\tau_1, \tau_2 \in AGL_n(F_q)$ and g is a fixed map of degree ≥ 2, because the group $AGL_n(F_q)$ is maximal in S_{q^n} [**2**].

After choosing the base of ${F_q}^n$ we write each permutation $\pi \in S_{q^n}$ as a "public rule":

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

The degree of permutation π written in the polynomial form is hard to control. It can be very high, there is no good upper bound on it.

2. Families of groups of stable degree

A family of the subgroup $G = G_n$, $G_n < S_{q^n}$ is a family of subgroups with a stable degree, if for all $h \in G - \{e\}$ $\deg h \leq c$, where c is an independent constant. Of course, cyclic groups are important for the Diffie-Hellman type protocols.

The example of a family of subgroups of stable degree is the affine group $AGL_n(F_q)$, $n \to \infty$, where $c = 1$. If g is a linear diagonalisable element of $AGL_n(F_q)$, then the discrete logarithm problem for base g is equivalent to the classical number theoretical problem. Obviously, in this case we lose the flavour of symbolic computations. One can take a subgroup H of $AGL_n(F_q)$ and consider its conjugation with the nonlinear bijective polynomial map f. The group $H' = f^{-1}Hf$ will be also a stable group, but for "most pairs" f and H group H' will be of degree $\deg f \times \deg f^{-1} \geq 4$ because of nonlinearity of f and f^{-1}. Even we conjugate nonlinear C with the invertible linear transformation $\tau \in AGL_n(F_q)$, some of important cryptographical parameters of C and $C' = \tau^{-1}C\tau$ can be different. Conjugated generators g and g' have the same number of fixed points, the same cyclic structure as permutations, but a number of equal coordinates for the pairs $(x, g(x))$ and $(x , g'(x))$ may be different. So two conjugate families of stable degree are not quite equivalent because corresponding cryptoanalitical problems may have different complexity.

In [**3**] we generalized the above mentioned problem for the case of Cremona group of the free module K^n, where K is an arbitrary commutative ring K. For the cryptography, the case of finite rings is the most important one. The finite field F_{q^n}, $n \geq 1$ and cyclic rings Z_m (especially $m = 2^7$ (ASCII codes), $m = 2^8$ (binary codes), $m = 2^{16}$ (arithmetic), $m = 2^{32}$ (double precision arithmetic)) are especially popular. the case of infinite rings K of characteristic zero (especially Z or C) is an interesting one because of Matijasevich multivariable prime approximation polynomials can be defined there (see, for instance [**4**] and further references). So it is natural to change a vector space ${F_q}^n$ for free module K^n (Cartesian power of K) and the family and symmetric group S_{q^n} for the Cremona group $C_n(K)$ of all polynomial bijections of K^n.

We repeat our definition of stable group 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 an independent constant c.

Recall that the cases of degrees 2 and 3 are especially important.

The first family of stable subgroups of $C_n(F_q)$, $K = F_q$ with degree 3 was practically established in [**5**], where the degrees of polynomial graph based public key maps were evaluated.

Those results are based on the construction of the family $D(n, q)$ of graphs with large girth and the description of their connected components $CD(n, q)$. The existence of infinite families of graphs of large girth was proved by Paul Erdös' (see [**6**]). Together with known Ramanujan graphs introduced by G. Margulis [**7**] and investigated in [**8**] the graphs $CD(n, q)$ are one of the first explicit constructions of such families with unbounded degree. The graphs $D(n, q)$ were used for the construction of LDPS codes and turbocodes which were used in real satellite communications (see [**9**], [**10**], [**11**]), for the development of private key encryption algorithms [**12**],[**1**],[**13**],[**14**], the option to use them for public key cryptography was considered in [**15**], [**2**] and in [**16**], where the related dynamic system was introduced (see also surveys [**17**],[**4**]).

The computer simulation ([**18**]) shows that stable subgroups related to $D(n, q)$ contain elements of a very large order but our theoretical linear bounds on the order are relatively weak. We hope to improve this gap in the future and justify the use of $D(n, q)$ for the key exchange.

In [**3**] we used graphs and related finite automata for the constructions of families of stable subgroups with degree 3 of Cremona group $C_n(K)$ over general ring K containing elements of large order (order is growing with the growth of n). The first family of stable groups was obtained in [**19**] via the studies of simple algebraic graphs defined over F_q. For general constructions of stable groups over the commutative ring K we used directed graphs with the special colouring.

The following statement together with construction was proved in [**3**].

Theorem 1. *For each commutative ring K with at least 3 regular elements there is the family Q_n of Cremona group $C(K^n)$ of degree 3 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 was obtained via explicit constructions. So we may use the finite ring K with at least 3 regular elements of the sequence equivalent to g_n for the key exchange. We showed that the growth of the order of g_n when n is growing can be bounded from below by a linear function $\alpha \times n + \beta$. In the case of such a sequence of groups $G_n = Q_n$ a sequence g_i of elements of stable degree

was modified by conjugation with $h_i \in G_i$. A new sequence $d_i = {h_i}^{-1} g_i h_i$ is also a sequence of elements of stable degree.

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

3.1. Graphs and incidence system

The missing definitions of graph-theoretical concepts which appear in this paper can be found in [**6**].

Let G be a simple graph, i.e. a graph 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 will 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 neighbours). The sequence of distinct vertices $v_1, \ldots, v_t$, such that $v_i G v_{i+1}$ for $i = 1, \ldots, t-1$ is the path in the graph. The length of a path is a number of its edges. The distance $\mathrm{dist}(u, v)$ between two vertices is the length of the shortest path 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 neighbours (see [**20**] or [**6**]).

The incidence structure is the set V with partition sets P (points) and L (lines)($|P| = |L|$) 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 a 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 [**21**]). The graph is q-regular if each of its vertices has degree q, where q is a constant. In this section we reformulate results of [**22**], [**23**] where the q-regular tree was described in terms of equations over the finite field F_q.

Let q be a prime power, and let P and L be two countably infinite dimensional vector spaces over F_q. Elements of P will be called *points* and those of L *lines*. To distinguish points from lines we use parentheses and brackets: If $x \in V = P \cup L$, then $(x) \in P$ and $[x] \in L$. It will also be advantageous to adopt the notation for the coordinates of points and lines introduced in [**23**]:

$$(p) = (p_1, p_{11}, p_{12}, p_{21}, p_{22}, p'_{22}, p_{23}, \ldots, p_{ii}, p'_{ii}, p_{i,i+1}, p_{i+1,i}, \ldots),$$

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

We now define an incidence structure (P, L, I) in the following way. We say that 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 $D(q)$.

To facilitate notation in future results, it will be convenient for us to define $p_{-1,0} = l_{0,-1} = p_{1,0} = l_{0,1} = 0$, $p_{0,0} = l_{0,0} = -1$, $p'_{0,0} = l'_{0,0} = 1$, $p_{0,1} = p_1$, $l_{1,0} = l_1$, $l'_{1,1} = l_{1,1}$, $p'_{1,1} = p_{1,1}$, 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 $n \geq 2$ we obtain an incidence structure (P_n, L_n, I_n) in the following way. First, P_n and L_n are obtained from P and L, respectively, by simply projecting each vector onto its n initial coordinates. The incidence I_n is then defined by imposing the first $n-1$ incidence relations and ignoring all others. For fixed q, the incidence graph corresponding to the structure (P_n, L_n, I_n) is denoted by $D(n, q)$. It is convenient to define $D(1, q)$ to be equal to $D(2, q)$. The properties of the graphs $D(n, q)$ that we are concerned with are described in the following theorem:

Theorem 2. *([**23**]) Let q be a prime power, and $n \geq 2$. Then*
(i) $D(n,q)$ is a q-regular edge-transitive bipartite graph of order $2q^n$;
(ii) for odd n, $g(D(n,q)) \geq n+5$, for even n, $g(D(n,q)) \geq n+4$

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 $[l] = [l_1, l_2, \ldots, l_n, \ldots]$ and $(p) = (p_1, p_2, \ldots, p_n, \ldots)$ (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 above given definitions:

Proposition 1. *([**23**]) 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 us assume that $n \geq 6$, $t = [(n+2)/4]$, and let
$u = (u_1, u_{11}, \cdots, u_{tt}, u'_{tt}, u_{t,t+1}, u_{t+1,t}, \cdots)$ be a vertex of $D(n,q)$. (It does not matter whether u is a point or a line). For every r, $2 \leq r \leq t$, let

$$a_r = a_r(u) = \sum_{i=0}^{t} (u_{ii} u'_{r-i,r-i} - u_{i,i+1} u_{r-i,r-i-1}),$$

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

In [**22**] the following statement was proved.

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

Let us consider the following equivalence relation τ : $u \tau v$ iff $a(u) = a(v)$ on the set $P \cup L$ of vertices of $D(n,q)$ $(D(q))$. 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 $EQ_{(x)}(n,q)$ $(EQ_{(x)}(q))$ of the graph $D(n,q)$ (respectively, $D(q)$). When $(x) = (0, \cdots, 0)$, we will omit the index v and write simply $EQ(n,q)$.

Let $CD(q)$ be the connected component of $D(q)$ which contains $(0,0,\ldots)$. Let τ' be an equivalence relation on $V(D(n,K))$ $(D(q))$ such that the equivalence classes are the totality of connected components of this graph. Obviously $u \tau v$

implies $u\tau' v$. If char F_q is an odd number, the converse of the last proposition is true (see [**17**] and further references).

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

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

Corollary 1. *(Description of elements of $CD(n,F_q)$)*
Let us consider a general vertex

$$x = (x_1, x_{1,1}, x_{2,1}, x_{1,2} \cdots, x_{i,i}, x'_{i,i}, x_{i+1,i}, x_{i,i+1}, \cdots),$$

$i = 2, 3, \cdots$ of the connected component $CD(n,F_q)$, 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_q and $x'_{i,i}$ could be computed successively as the unique solutions of the equations $a_i(x) = a_i(v)$, $i = 1, \ldots$.

3.2. Regular directed graph with special colouring

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

Let us 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 that the cardinality of these two sets (input or output degree) are the same for each vertex.

Let Γ be a 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 $\rho : E \to M$ onto the set of colours M such that for each vertex $v \in V$ and $\alpha \in M$ there exists a unique neighbour $u \in V$ with the property $\rho((v,u)) = \alpha$. But there might not exist such colouring for every regular graph, hence we need an operator $N_\alpha(v) := N(\alpha, v)$ of taking the neighbour u of a vertex v within the arrow $v \to u$ of colour α, which is 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 $N_{\alpha_m} N_{\alpha_{m-1}} \ldots N_{\alpha_1}$ of bijective maps $N_{\alpha_i} : V(\Gamma) \to V(\Gamma)$, $i = 1, 2, \ldots, m$. Let us assume that the map $u \to N_\alpha(u)$ is a bijection. For a 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_Γ be the group generated by permutations π as above.

Let $F_1 = \{\langle (p), [l] \rangle \mid [l] \in L, (p) \in P, \ (p)I[l]\}$ and $F_2 = \{\{[l], (p)\} \mid [l] \in L, (p) \in P, \ [l]I(p)\}$ be two copies of the totality of flags for (P, L, I). Let $DD(K)$, over commutative ring K, be the directed graph (double directed flag graph) on the disjoint union of F_1 with F_2 defined by the following rules

$\langle (p), [l] \rangle \to \{[l^{'}], (p^{'})\}$ if and only if $[l] = [l^{'}]$ and $p_1 \neq p_1^{'}$,

$\{[l^{'}], (p^{'})\} \to \langle (p), [l] \rangle$ if and only if $(p^{'}) = (p)$ and $l_1^{'} \neq l_1$.

3.3. Construction of new stable groups corresponding to rainbow like graphs

Let us consider the double directed graph $DD(n, K)$ for the bipartite graph $D(n, K)$ and the infinite double directed flag graph $DD(K)$ for $D(K)(DD(K))$ defined over the commutative ring K, Let $N = N_{\alpha,\beta}(v)$ be the operator of taking the neighbour alongside the output arrows of colours $\alpha, \beta \in \mathrm{Reg(K)}$ of vertex $v \in F_1 \cup F_2$ by the following rule. If $v =< (p), [l] >\in F_1$ then $N(v) = v' = [[l], (p')] \in F_2$, where the colour of v' is $\alpha = p'_{1,0} - p_{1,0}$, if $v = [[l], (p)] \in F_2$ then $N(v) = v' =< (p), [l'] >\in F_1$, where the colour of v' is $\beta = l'_{1,0} - l_{1,0}$.

Let us consider the elements $Z(\alpha, \beta) = N_{\alpha,0} N_{0,\beta}$. It moves $v \in F_1$ into $v' \in F_1$ at a distance two from v and fixes each $u \in F_2$. Notice that $Z(\alpha, \beta) Z(-\alpha, -\beta)$ is an identity map.

We consider the group $GF_{n+1}(K)$ ($GF(K)$, respectively) generated by all transformations $Z(\alpha, \beta)$ for nonzero $\alpha, \beta \in K$ acting on the variety K^{n+1} (K^∞).

Theorem 3. *The sequence of subgroups $GF_n(K)$ of the Cremona group $C_n(K)$ forms a family of subgroups of degree 3.*

Canonical graph homomorphisms $\omega_n : DD(n, K) \to DD(n-1, K)$ can be naturally expanded to the group homomorphism $GF_{n+1}(K)$ onto $GF_n(K)$. It means that the group $GF(K)$ is a projective limit of $GF_n(K)$. Let δ_n be a canonical homomorphism of $GF(K)$ onto $GF_n(K)$.

Let $\mathrm{Reg}(K)$ be the totality of regular elements of K, i. e. non zero divisors. We may consider the restriction $\widetilde{DD(n, K)}$ of the graph $DD(n, K)$ via the following additional condition:

$$\langle (p),[l]\rangle R\{[l^{'}],(p^{'})\} \;\Leftrightarrow\; [l]=[l^{'}]\ \&\ p_1-p_1^{'}\in \mathrm{Reg}(K)$$

$$\{[l^{'}],(p^{'})\}R\langle (p),[l]\rangle \;\Leftrightarrow\; (p^{'})=(p)\ \&\ l_1^{'}-l_1\in \mathrm{Reg}(K).$$

We restrict the operators $N_{\alpha,\beta}$ and $Z(\alpha,\beta)$ simply by adding the restrictions $\alpha,\beta\in \mathrm{Reg}(K)$. Let $Q_n=Q(n,K)$ be the restricted group and $Q=Q(K)$ is a projective limit of $Q(n,K)$, $n\to\infty$.

In [**16**],[**2**] was shown that the projective limit of graphs $\widetilde{DD(n,K)}$ is an acyclic graph and the length of minimal directed cycle in $\widetilde{DD(n,K)}$ is bounded below by $[n+5]/2$. It means that we get the following statement.

Proposition 4. *The order of each nonidentical element g acting on the infinite graph is infinity.*

4. Generalization of the algorithm using linear symmetries

Let us introduce a group of automorphisms of the infinite graph $D(K)$:

$$G=\langle t_{1,0}(\beta),t_{0,1}(\gamma),\ \beta,\gamma\in K\rangle$$

$$G'=\langle t_{m,m}(\beta),t'_{m,m}(\gamma),\ \beta,\gamma\in K\rangle$$

defined below:

Map $t_{1,0}(\beta)$ changes every coordinate of a line $[l]$ and a point (p) according to the rule:

$l_{i,i}\to l_{i,i}$
$l_{i,i+1}\to l_{i,i+1}$
$l_{i+1,i}\to l_{i+1,i}+l_{i,i}\beta$
$l'_{i,i}\to l'_{i,i}+l_{i-1,i}\beta$
$p_{i,i}\to p_{i,i}+p_{i-1,i}\beta$
$p_{i,i+1}\to p_{i,i+1}$
$p_{i+1,i}\to p_{i+1,i}+(p_{i,i}+p'_{i,i})\beta+p_{i-1,i}\beta^2$
$p'_{i,i}\to p'_{i,i}+p_{i-1,i}\beta$.

Map $t_{0,1}(\gamma)$ changes every coordinate of a line $[l]$ and a point (p) according to the rule:

$l_{i,i}\to l_{i,i}+l_{i,i-1}\gamma$
$l_{i,i+1}\to l_{i,i+1}+(l_{i,i}+l'_{i,i})\gamma+l_{i,i-1}\gamma^2$
$l_{i+1,i}\to l_{i+1,i}$
$l'_{i,i}\to l'_{i,i}+l_{i,i-1}\gamma$
$p_{i,i}\to p_{i,i}+p_{i,i-1}\gamma$
$p_{i,i+1}\to p_{i,i+1}+p'_{i,i}\gamma$

$p_{i+1,i} \to p_{i+1,i}$
$p'_{i,i} \to p'_{i,i}$.

Map $t_{m,m}(\beta)$ changes every coordinate of a line $[l]$ and a point (p) according to the rule:

$l_{i,i} \to l_{i,i} - l_{r,r}\beta,\ r = i - m \geq 0$
$l_{i,i+1} \to l_{i,i+1} - l_{r,r+1}\beta,\ r = i - m \geq 0$
$l_{i+1,i} \to l_{i+1,i}$
$l'_{i,i} \to l'_{i,i}$
$p_{i,i} \to p_{i,i} - p_{r,r}\beta,\ r = i - m \geq 0$
$p_{i,i+1} \to p_{i,i+1} - p_{r,r+1}\beta,\ r = i - m \geq 0$
$p_{i+1,i} \to p_{i+1,i}$
$p'_{i,i} \to p'_{i,i}$.

Map $t'_{m,m}(\gamma)$ changes every coordinate of a line $[l]$ and a point (p) according to the rule:

$l_{i,i} \to l_{i,i}$
$l_{i,i+1} \to l_{i,i+1}$
$l_{i+1,i} \to l_{i+1,i} + l_{r+1,r}\gamma,\ r = i - m \geq 0$
$l'_{i,i} \to l'_{i,i} + l'_{r,r}\gamma,\ r = i - m \geq 0$
$p_{i,i} \to p_{i,i}$
$p_{i,i+1} \to p_{i,i+1}$
$p_{i+1,i} \to p_{i+1,i} + p_{r+1,r}\gamma,\ r = i - m \geq 0$
$p'_{i,i} \to p'_{i,i} + p'_{r,r}\gamma,\ r = i - m \geq 0$.

Automorphism of infinite simple graph $D(K)$, listed above, can be naturally considered as automorphism of the double directed graph $DD(K)$ to get the groups:

$$\widetilde{G} = \langle \widetilde{t_{1,0}(\beta)}, \widetilde{t_{0,1}(\gamma)},\ \beta, \gamma \in K \rangle,$$

$$\widetilde{G'} = \langle \widetilde{t_{m,m}(\beta)}, \widetilde{t'_{m,m}(\gamma)},\ \beta, \gamma \in K \}$$

where:
$\langle (p), [l] \rangle^{\widetilde{t_\lambda(x)}} = \langle (p^{t_\lambda(x)}), [l^{t_\lambda(x)}] \rangle$,
$\{ [l], (p) \}^{\widetilde{t_\lambda(x)}} = \{ [l^{t_\lambda(x)}], (p^{t_\lambda(x)}) \}$,
where $\lambda \in \{(1,0), (0,1), (m,m), (m,m)'\}$ and $x = \beta, \gamma$.
Then we take a composition of these maps and get:
$T_s = \widetilde{t_{1,0}(\beta_1)} \widetilde{t_{0,1}(\gamma_1)} \widetilde{t_{1,0}(\beta_2)} \widetilde{t_{0,1}(\gamma_2)} \dots \widetilde{t_{1,0}(\beta_s)} \widetilde{t_{0,1}(\gamma_s)}$
$T_{f,h} = \{ \prod_{m \in J} \widetilde{t_{m,m}(\beta_m)} \prod_{l \in J'} \widetilde{t'_{l,l}(\gamma_l)}$, where
$J \subset \Omega = \{i | (ii)$ is a coordinate of the tuple $((x_{1,0}, x_{11}, x_{12}, x_{21}, x_{22}, x'_{22}, x_{23}, \dots)\}$,
$J' \subset \Omega' = \{i | (ii)'$ is a coordinate of the tuple $((x_{1,0}, x_{11}, x_{12}, x_{21}, x_{22}, x'_{22}, x_{23}, \dots)\}$
and
$f:\ J \to K$

$h: J' \to K$

Now we can combine it with transformation, given by the chain in the graph of length k, where k is even positive integer:

$N_k = N_{\alpha_1} N_{\alpha_2} \dots N_{\alpha_k}$

with the condition $\alpha_i + \alpha_{i+1} \in \mathrm{Reg}K$ and $\alpha_1 + \alpha_2 \in \mathrm{Reg}K$

Proposition 5. *$T_s T_{f,h} N_k = N_k T_s T_{f,h}$.*

Proposition 6. *For the infinite graph $D(K)$, the order of $N_k = N_{\alpha_1} N_{\alpha_2} \dots N_{\alpha_k}$, where k is even and $\alpha_i + \alpha_{i+1} \in RegK$, $\alpha_1 + \alpha_2 \in RegK$, is infinity.*

Proposition 7. *If K has at least 3 regular elements (non zero divisors), then the order of T_s, acting on vertices of infinite graph, is infinity.*

For implementation reasons we project N_k, T_s and $T_{f,h}$ into n initial coordinates to obtain finally the transformations N_k^n, T_s^n and $T_{f,h}^n$, respectively.

From Propositions 6 and 7 it follows that the orders of N_k^n and T_s^n are growing with the growth of n.

Proposition 8. *The order of $g = T_s^n T_{f,h}^n N_k^n$ is the minimal common multiple of $T_s T_{f,h}^n$ and N_k.*

5. Symbolic Diffie-Hellman algorithm

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

The order of g in the symbolic Diffie-Hellman algorithm must be "sufficiently large" and the number n_A (or n_B)can not be easily computable as functions from degrees for g and h_A. The map g which sends x_i into ${x_i}^t$ for each i obviously is bad choice of the base for the discrete logarithm problem. In this case n_A is just a ratio of $\deg h_A$ and $\deg g$.

To avoid such trouble we can look at the family of subgroups G_n of S_{q^n}, $n \to \infty$ such that the maximal degree of its elements equals c, where c is the small independent constant (groups of degree c or groups of stable degree).

Let us discuss the asymmetry of our modified Diffie-Hellman algorithms of the key exchange in detail. The correspondents Alice and Bob have different information for making computation. Alice chooses dimension n, element g_n

as in the theorem above, the element $h \in Q_n$ and the affine transformation $\tau \in AGL_n(K)$. So she obtains the base $b = \tau^{-1}h^{-1}g_nh\tau$ and sends it in the form of the standard polynomial map to Bob.

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

Notice that the position of adversary is similar to Bob's position. He (or she) needs 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 the family of groups Q_n.

The computer simulation shows that the number of monomial expressions of the kind $x^{i_1}x^{i_2}x^{i_3}$ with the nonzero coefficient is rather close to the 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.

Let us consider our symbolic Diffie -Hellman protocol for the infinite transformation group $\widetilde{DD(K)}$ combined with linear symmetries.

Let $AGL_n(F_q)$ be the group of affine transformation of the vector space F_q^n, i.e. maps $\tau_{A,b} : \widetilde{x} \to \widetilde{x}A + b$, where $\widetilde{x} = (x_1, x_2, \ldots, x_n)$, $b = (b_1, b_2, \ldots, b_n)$ and A is the invertible matrix with $\det A \neq 0$.

First Alice chooses the element $h = T_s^n N_k^n T_{f,h}^n$, using the linear symmetries T_s^n, $T_{f,h}^n$ given in the previous section and the graph transformation N_k^n.

Finally, we can take affine, bijective transformation $\tau_{A,b} :\in AGL_n(K)$ and use the composition $h' = \tau_{A,b}h\tau_{A,b}^{-1}$ as the base for the Diffie-Helman algorithm.

Like in the general Diffie-Hellman algorithm, the correspondents Alice and Bob establish $h' \in S_{p^n}$, $h' = \tau_{A,b}h\tau_{A,b}^{-1}$ via an open communication channel, choose the positive integers n_A and n_B, respectively, and exchange the public rules $h_A = (h')^{n_A}$ and $h_B = (h')^{n_B}$ via an open channel. Finally, they compute the common transformation ${h_B}^{n_A}$ and ${h_A}^{n_B}$, respectively, obtaining the collision vector $(h')^{n_An_B}$.

Because of linearity of symmetries the element $h' = \tau_{A,b}h\tau_{A,b}^{-1}$, where $\tau_{A,b} \in AGL_n(K)$, h' is a cubical map.

The group $\widetilde{G'} = \langle \widetilde{t_{m,m}(\beta)}, \widetilde{t'_{m,m}(\gamma)},\ \beta, \gamma \in K\}$ given in the previous section acts transitively on connected components of the graph $D(K)$ (or $D(n, K)$). It means that an arbitrary vertex can be shifted to any other vertex, even if they lie in different connected components.

6. Application of the algorithm in public key cryptography

The general idea of the graph based public key cryptography is to treat vertices of our graph as messages and use the iterative process of walking on such a graph as the encryption scheme. To improve our algorithm we use (given in the previous section) – linear symmetries, getting two advantages:

(1) the encryption scheme will be better protected
(2) each ciphertext can be obtained from each plaintext

To hide the graph and walking on it, we use two affine transformations - the only one aspect similar to the well known Imai-Matsumoto scheme. The cryptanalysis of Imai-Matsumoto can be found in [**?**]. Like in the traditional cryptography, Alice will be the holder of the key - she has knowledge about the password, graph, affine transformation and linear symmetries. Bob - the public user - has only an encryption map, given by the polynomial transformation, made by Alice using the following compostion:

$$g = \tau T_s^n (z')^s T_{f,h}^n \tau^{-1},$$

where

(1) $(z')^s$ is s iterations of $z' = N_{\alpha_1}^n N_{\alpha_3}^n \dots N_{\alpha_k}^n$.
(2) T_s^n and $T_{f,h}^n$ are the linear symmetries defined in Section 5
(3) τ – the affine transformation

Linearity of symmetries and affine transformation does not change the degree of graphical transformation which is equal to 3.

Hence, if plaintext is in the form $x_1, \dots, x_n$ then the ciphertext is given by polynomials in n variables written in the expanded form, i.e. as the sums of monomials of the kind ${x_1}^{i_1} \dots {x_n}^{i_n}$ with the coefficients from K. Finally, Alice makes polynomial equations public.

Again, like in the Imai-Matsumoto scheme, if Bob wants to send her a plaintext message x, he just substitutes x_i in the public equations and finds y_i. On the other hand, Catherine, who knows only the ciphertext and the public key must solve a nonlinear system for the unknowns x_i.

7. Geometrical interpretation of the generalised algorithm – truncated forests, jumps from one tree to another

The graph $D(K)$, where K is the integral domain, is a forest consisting of isomorphic edge-transitive trees (see [**15**] or [**13**]).

Notice that each tree is a bipartite graph. We may choose a vertex x and refer to all vertices on even distance from it as points. So all remaining vertices are lines.

We may identify all vertices from $P = K^{\infty}$ with the union of point-sets for all trees from $D(K)$. Another copy L of K^{∞} we will treat as totality of all lines in our forest.

For our Diffie-Hellman key exchange protocol Alice has to go to an infinite magic forest $D(K)$ and do the following lumberjack's business – truncate all trees there by deleting all components with the number $\geq n+1$ to get a finite dimensional graph $D(n, K)$, which is a union of isomorphic connected components $CD(n, K)$- truncated trees. Notice, if you plant a truncated tree $CD(n, K)$ and let $n \to \infty$ then it will grow to an infinite regular tree.

References

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

[2] Ustimenko V., 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).

[3] Ustimenko V., Wroblewska A., On the key exchange with nonlinear polynomial maps of stable degree, Fundamenta Informaticae, to appear

[4] Ustimenko V. A., 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, 24 (2009): 296.

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

[6] B. Bollobás, Extremal Graph Theory, Academic Press, London (1978).

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

[8] Lubotsky A., Philips R. and Sarnak P., Ramanujan graphs, J. Comb. Theory. 115(2) (1989): 62.

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

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

[11] Kim Jon-Lark, Peled U. N., Perepelitsa I., Pless V. and Friedland S., Explicit construction of families of LDPC codes with no 4-cycles , Information Theory, IEEE Transactions, 50(10) (2004): 2378.

[12] Ustimenko V. A., 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): 228.

[13] Ustimenko V., Graphs with Special Arcs and Cryptography, Acta Applicandae Mathematicae 74(2) (2002): 117.

[14] Kotorowicz S., Ustimenko V., On the implementation of cryptoalgorithms based on algebraic graphs over some commutative rings, Condensed Matter Physics 11(2(54)) (2008): 347.

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

[16] Ustimenko V. A., Linguistic Dynamical Systems, Graphs of Large Girth and Cryptography, Journal of Mathematical Sciences 140(3) (2007): 412.

[17] 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.

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

[19] Ustimenko V., Wroblewska 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).

[20] Biggs N.L., Graphs with large girth, Ars Combinatoria, 25C (1988): 73.

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

[22] Lazebnik F., Ustimenko V. A. and Woldar A. J., A Characterization of the Components of the graphs $D(k, q)$, Discrete Mathematics 157 (1996): 271.

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