Annales UMCS Informatica AI XIII, 1 (2013) 63–80
DOI: 10.2478/v10065-012-0047-6

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

On the key exchange and multivariate encryption with nonlinear polynomial maps of stable degree

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

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

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

In the paper we introduce the explicit constructions of sequences of elements of stable degree for the cases $c = 3$ and $c = \lfloor \frac{n+2}{4} \rfloor$ for each commutative ring K containing at least 3 regular elements and discuss the implementation of related key exchange and multivariate map algorithms.

1 Introduction

The discrete logarithm problem can be formulated for a general finite group G. Find a positive integer x satisfying condition $g^x = b$ where $g \in G$ and $b \in G$. The problem has reputation to be a difficult one. But even in the case of cyclic group C there are many open questions. If $C = Z^*_{p-1}$ or $C = Z^*_{pq}$ where p and q are

*ustymenko_vasyl@yahoo.com
†awroblewska@hektor.umcs.lublin.pl

"sufficiently large" primes then the complexity of discrete logarithm problem justifies the classical Diffie-Hellman key exchange algorithm and the RSA public key encryption, respectively. In most of other cases complexity of discrete logarithm problem is not properly investigated. The problem is very dependent on the choice of the base g and the way of presentation the data on the group. The group can be defined via generators and relations, as the automorphism group of algebraic variety, as the matrix group, as the 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 the vector space ${F_p}^n$ into itself. Obviously $|S_{p^n}| = (p^n)!$, it is known that each permutation π can be written in the form $x_1 \to f_1(x_1, x_2, \dots x_n), x_2 \to f_2(x_1, x_2, \dots x_n), \dots, x_n \to f_n(x_1, x_2, \dots x_n)$, where f_i are the multivariable polynomials from $F_p[x_1, x_2, \dots, x_n]$. The presentation of G as a subgroup of S_{p^n} is chosen because the Diffie-Hellman algorithm here will be implemented by the tools of symbolic computations. Another reason is 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.

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

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

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

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

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

In practice they can establish a common vector $v = (v_1, v_2, \dots, v_n)$, $v_i \in F_p$, $i = 1, \dots, n$ via open channel and use the collision vector $T(v)$ as a password for their private key encryption algorithm.

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

To avoid such trouble one can look at the family of subgroups G_n of S_{p^n}, $n \to \infty$ such that the maximal degree of its elements equals c, where c is a small independent

constant (groups of degree c or groups of stable degree). Our paper is devoted to explicit constructions of such families.

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

It is clear that the affine groups $AGL_n(F_p)$, $n \to \infty$ form a family of subgroups of stable degree for $c = 1$ and all nonidentical affine transformations are of stable degree. Notice that if g is a linear diagonalisable element of $AGL_n(F_p)$, then the discrete logarithm problem for base g is equivalent to the classical number theoretical problem. Obviously, in this case we miss the flavour of symbolic computations. One can take a subgroup H of $AGL_n(F_p)$ and consider its conjugation with the nonlinear bijective polynomial map f. Of course, 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 degf $\times$ deg$f^{-1} \geq 4$ because of nonlinearity f and f^{-1}.

So the problem of construction of infinite families of subgroups G_n in S_{p^n} of degrees 2 and 3 may attract some attention.

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

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

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

We generalize the above problem for the case of Cremona group of the free module K^n, where K is the arbitrary commutative ring K. For cryptography the case of finite rings is the most important. The finite field F_{p^n}, $n \geq 1$ and the 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 as well because of Matijasevich multivariable prime approximation polynomials can be defined there (see, for instance **[2]** and further references).

So it is natural to change a vector space ${F_p}^n$ for the free module K^n (Cartesian 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.

We repeat our definition for a 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 [**3**], where the degrees of polynomial graph based public key maps were evaluated. But the group theoretical language was not used there and the problem of the key exchange was not considered.

So we reformulate the results of [**3**] in terms of Cremona group over a general ring in Section 2 of this paper.

Additionally, we show the existence of cubic elements of large order in the case of finite field.

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 [**4**]). Together with famous Ramanujan graphs introduced by G. Margulis [**5**] and investigated in [**6**] 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 applied in real satellite communications (see [**7**], [**8**], [**9**], [**10**]), for the development of private key encryption algorithms [**11**],[**12**], [**13**],[**14**], the option to use them for public key cryptography was considered in [**15**], [**16**] and in [**17**] , where the related dynamic system was introduced (see also surveys [**18**], [**2**]).

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

In Section 4 we also will use graphs and related finite automata for the construction 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 via studies of simple algebraic graphs defined over F_q. For general construction of stable groups over commutative ring K we use directed graphs with the special colouring. The main result of the paper is the following statement.

Theorem 1. For each commutative ring K with at least 3 regular elements there is a 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 is obtained via explicit constructions. So we may use the sequence equivalent to g_n for the key exchange in the finite ring K with at least 3 regular elements. We show 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 $G_n = Q_n$ we can modify a sequence g_i of elements of stable degree by conjugation with $h_i \in G_i$. A new sequence $d_i = {h_i}^{-1} g_i h_i$ can be also a sequence of elements of stable degree.

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

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

Remark. Notice that the adversary is in the same shoes with the public user Bob. 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. We present its time evaluation (generation of b and b_A^n by Alice and computation of b_B^c by Bob) in the last section of paper. We continue the studies of orders of g_i theoretically and by computer simulation.

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.

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

2.1 Graphs and incidence system

The missing definitions of graph-theoretical concepts which appear in this paper can be found in [**4**]. All graphs considered are simple, i.e. undirected without loops and multiple edges. Let $V(G)$ and $E(G)$ denote the set of vertices and the set of edges of G, respectively. Then $|V(G)|$ is called the *order* of G, and $|E(G)|$ is called the *size* of G. A path in G is called *simple* if all its vertices are distinct. When it is convenient, we shall identify G with the corresponding anti-reflexive binary relation on $V(G)$, i.e. $E(G)$ is a subset of $V(G) \times V(G)$ and write vGu for the adjacent vertices u and v (or 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 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

$v_1, \ldots, v_m$ 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 **[19]** or **[4]**).

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 **[1]**). The graph is k-regular if each of its vertices has the degree k, where k is a constant. In this section we reformulate the results of **[20]**, **[21]** 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. The elements of P will be called *points* and those of L *lines*. To distinguish points from lines we use parentheses and brackets: If $x \in V$, then $(x) \in P$ and $[x] \in L$. It will also be advantageous to adopt the notation for the coordinates of points and lines introduced in **[5]**:

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

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

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

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

To facilitate notation in future results, it will be convenient for us to define $p_{-1,0} = l_{0,-1} = p_{1,0} = l_{0,1} = 0$, $p_{0,0} = l_{0,0} = -1$, $p'_{0,0} = l'_{0,0} = 1$, $p_{0,1} = p_1$, $l_{1,0} = l_1$, $l'_{1,1} = l_{1,1}$, $p'_{1,1} = p_{1,1}$, and to rewrite (1) in the form :

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

$$l_{i,i+1} - p_{i,i+1} = l_{ii}p_1$$

$$l_{i+1,i} - p_{i+1,i} = l_1 p'_{ii}$$

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

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

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

Theorem 2. [**21**] Let q be a prime power, and $k \geq 2$. Then
(i) $D(k, q)$ is a q-regular edge-transitive bipartite graph of the order $2q^k$;
(ii) for odd k, $g(D(k, q)) \geq k + 5$, for even k, $g(D(k, q)) \geq k + 4$

We have a natural one to one correspondence between the coordinates 2,3, ..., n, ... 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 the numbers $> i$" from $D(q)$ to $D(i, q)$, and $\eta_{i,j}$ be the map "deleting all coordinates with the numbers $> i$ " from $D(j, q)$, $j > i$ into $D(i, q)$.

The following statement follows directly from the definitions:

Proposition 1. (see, [**21**]) The projective limit of $D(i, q), \eta_{i,j}$, $i \to \infty$ is an infinite forest $D(q)$.

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

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

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

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

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

In [**20**] the following statement was proved.

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

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

Let $CD(q)$ be the connected component of $D(q)$ which contains $(0,0,\ldots)$. Let τ' be an equivalence relation on $V(D(k,q))$ $(V(D(q)))$ 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 **[2]** and further references).

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

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

Corollary 1. Let us consider a general vertex

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

$i = 2, 3, \cdots$ of the connected component $CD(k, F_q)$, which contains a chosen vertex v. Then the 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 solution of the equations $a_i(x) = a_i(v)$, $i = 1, \ldots$.

2.2 Geometrical interpretation of the algorithm

We can change F_q for the integral domain K and introduce the graph $D(K)$ as the graph given by equations (1) over K and repeat all results of the previous section. If we assume that K is the general commutative ring then we will lose just the bounds on the girth.

The graph $D(K)$, where K is the integral domain is a forest consisting of isomorphic edge-transitive trees (see **[11]** or **[17]**).

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 infinite magic forest $D(K)$ and do the following lumberjack's business

1) Truncate all trees there by deleting all components with the number $\geq n+1$. So Alice gets 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 a projective limit of $CD(n,K)$, which is an infinite regular tree.

2) We define a special colouring of graph $D(n,K)$ (or $D(K)$) in the following way. Let us identify our simple graph with the directed graph of corresponding symmetric binary relation. We introduce the colour of the directed arrow between two ordered vertices of our graph v_1 and v_2 as the difference of their first coordinates. It is $l_{0,1}-p_{0,1}$ if v_1 is a point (p) and $-(l_{0,1}-p_{0,1})$ if v_1 is a line $[l]$.

Let $X(\alpha,\beta)$ be the operator on the vertices of the graph $D(K)$ moving point (p) to its neighbor alongside the edge of colour α and moving line l to its neighbor alongside the edge of colour β. It is clear that $X(\alpha,\beta)X(-\beta,-\alpha)$ is an identity map e. So $X(\alpha,\beta)^{-1} = X(-\beta,-\alpha)$. We assume, that $N_{\alpha} = X(\alpha,\alpha)$.

Let us define the infinite group $GD(K)$ generated by the elements of the kind $g = N_{\alpha_1}N_{\alpha_2}\dots N_{\alpha_{2s-1}}N_{\alpha_{2s}}(\mathrm{x})$, $s = 1,2\dots$ corresponding to walks of even length within the tree starting in the general vertex x. It is a transformation group of variety $P \cup L$. It acts transitively on P (or L). $(GD(K),P)$ is a subgroup of Cremona group for the variety K^{∞}.

The computation of $g = N_{\alpha_1}N_{\alpha_2}\dots N_{\alpha_{2s-1}}N_{\alpha_{2s}}(\mathrm{x})$ in the transformation group $(GD(K),P)$ corresponds to walk in $D(K)$ of even length within the tree starting with the point x. So the group G is the totality of all point to point walks in our forest.

The composition of g_1 and g_2 from the variable x is the walk corresponding to g_1 with the starting point x combined with the walk corresponding to g_2 with the starting point $g_1(\mathrm{x})$ and the final point $g_2(g_1(\mathrm{x}))$,

Each pass of even length in the graph starting from a point (p) can be obtained as a sequence (p), $v_1 = N_{\alpha_1}(p), v_2 = N_{\alpha_2}(v_1),\dots,v_{2k} = N_{\alpha_{2k}}(v_{2k-1})$.

Each element of $GD(K)$ has an infinite order because our forest does not contain cycles.

Let us consider our symbolic Diffie -Hellman protocol for the infinite transformation group $GD(K),P$.

a) In the case of this group Alice hides a general point x by the "quasi random" affine transformation T and sends $g(T(\mathrm{x}))$ to Bob.

b) Further Bob chooses his key k_B and computes the transformation $h_b = g(T(x))^{k_B}$ of the point set for the tree. He makes this computation root in "darkness" because he has no information on the forest, he has to apply standard tools for symbolic computations.

c) Alice computes $h_A = g(T(x))^{k_A}$. She can make it fast because via the repetition of the walk g from the vertex $T(x)$ several times.

d) Alice and Bob get the collision vector as $h_B{}_A^k$ and $h_A{}_B^k$ respectively.

2.3 Truncated trees and corresponding stable group

Now we change the forest $D(K)$ into the bunch of truncated trees from $D(n, K)$. The computation $g = N_{\alpha_1} N_{\alpha_2} \dots N_{\alpha_{2s-1}} N_{\alpha_{2s}}(\mathrm{x})$ generates the group $(GD(n, K), P \cup L)$ corresponding all walks in $D(n, K)$ of even length starting in the vertex x.

Each pass of even length in the graph starting from a point (p) can be obtained as a sequence (p), $v_1 = N_{\alpha_1}(p), v_2 = N_{\alpha_2}(v_1), \dots, v_{2k} = N_{\alpha_{2k}}(v_{2k-1})$.

Now Alice and Bob can do the key exchange similarly to the case of $GD(K)$ but in the finite group $GD(n, K)$, where K is a finite ring

REMARK. The generalised graph $D(n, K)$ can be defined on the vertex set $K^n \cup K^n$ in the case of arbitrary ring K by equations (1). Notice that if K contains zero divisors then girth dropps, it is bounded by the constant.

The next result follows instantly from **[3]** .

Theorem 3. Let K be a commutative ring containing at least 3 regular elements. The sequence of subgroups $GD(n, K)$ of the Cremona group $C(n, K)$ forms a family of stable subgroups of degree 3.

We refer to the element $g = N_{\alpha_1} N_{\alpha_2} \dots N_{\alpha_{2s-1}} N_{\alpha_{2s}}$ for which $\alpha_i \neq \alpha_{i+1}$, $i = 1, 2 \dots, 2s-1$ as an irreducible element of length s.

Let ϕ_n be a canonical homomorphism of $GD(K)$ onto $GD(n, K)$.

The following proposition follows from the results on the girth of the previous section. Now it is very important that $K = F_q$

Proposition 4. The order of each nonidentical element of $GD(F_q)$ is an infinity. Let $g \in GD(F_q)$ be a regular element of length $l(g) = k$, then the order of $g_n = \phi_n(g)$, where $k \leq [n+5]/2$, is bounded below by $[n+5]/4k$ The sequence g_n is a family of stable elements.

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

3 On the regular directed graph with special colouring

The 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 the 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 the regular directed graph, $E(\Gamma)$ be the set of arrows of graph Γ. Let us assume that additionally, we have a colouring function i.e. the map $\pi : E \to M$ onto 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 $\pi((v, u)) = \alpha$ and the 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 and a bijection. In this case we refer to Γ as the *rainbow-like graph.*

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

E. Moore **[1]** used the term *tactical configuration* of order (s, t) for the biregular bipartite simple graphs with the bidegrees $s + 1$ and $r + 1$. It corresponds to the 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 $|L|(t + 1)$.

Let $F = \{(p, l) | p \in P, l \in L, pIl\}$ be the totality of flags for the tactical configuration with the partition sets P (point set) and L (line set) and the 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 the regular tactical configuration of the 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 parenthese 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

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

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

4 Construction of new stable groups corresponding to the rainbow like graphs

Let us consider a double directed graph $DD(n, K)$ for the bipartite graph $D(n, K)$ and an 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 the 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 the 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 $F_1 = K^{n+1}$ (K^∞).

Theorem 4. Sequence of the subgroups $GF(n,K)$ of the Cremona group $C(n,K)$ form a family of subgroups of degree 3.

Proof

In the first step we connect a point with a line to get two sets of vertices of the new graph:

$$F = \{\langle (p),[l]\rangle \mid (p)I[l]\} \cong K^{n+1}$$

$$F^{'} = \{\{[l],(p)\} \mid [l]I(p)\} \cong K^{n+1}.$$

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

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

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

Our key will be $\alpha_1,\alpha_2,\ldots,\alpha_n$, such that $\alpha_i \in RegK$.

As the first vertex we take

$$\{[l],(p)\} = (l_1, l_{1,1}, l_{1,2}, \ldots, l_{i,j}, p_1)$$

(our variables) . Using the above relation we get the next vertex:

$$\langle (p)^{(1)},[l]^{(2)}\rangle = (p_1, p_{1,1}^{(1)}, \ldots, p_{i,j}^{(1)}, l_1+\alpha_1)$$

with the coefficients of degree 2 or 3, where

$$\begin{aligned}
&p_{1,1}^{(1)} = l_{1,1} - l_1p_1,\ deg = 2\\
&p_{1,2}^{(1)} = l_{1,2} - l_{1,1}p_1\ deg = 2\\
&p_{2,1}^{(1)} = l_{2,1} - l_1(l_{1,1} - l_1p_1)\ deg = 3\\
&p_{i,i}^{'(1)} = l_{i,i}^{'} - p_1l_{i,i-1}\ deg = 2\\
&p_{i,i+1}^{(1)} = l_{i,i+1} - p_1l_{i,i}\ deg = 2\\
&p_{i,i}^{(1)} = l_{i,i} - l_1(l_{i-1,i} - p_1l_{i-1,i-1})\ deg = 3\\
&p_{i+1,i}^{(1)} = l_{i+1,i} - l_1(l_{i,i}^{'} - p_1l_{i,i-1})\ deg = 3
\end{aligned}$$

Similarly we get the third vertex:

$$\{[l]^{(2)},(p)^{(3)}\} = (l_1+\alpha_1, l_{1,1}, \ldots, l_{i,j}, p_1+\alpha_2)$$

also with the coefficients of degree 2 or 3, where

$$\begin{array}{l} l_{1,1}^{(2)} = l_{1,1} + l_1 p_1,\ deg = 2 \\ l_{1,2}^{(2)} = l_{1,2} + \alpha_1 p_1^2\ deg = 2 \\ l_{2,1}^{(2)} = l_{2,1} + \alpha_1 p_{1,1}^{(1)}\ deg = 2 \\ l_{i,i}^{(2)} = l_{i,i} + \alpha_1 p_{i-1,i}^{(1)}\ deg = 2 \\ l_{i+1,i}^{(2)} = l_{i+1,i} + \alpha_1 p_{i,i}^{'(1)}\ deg = 2 \\ l_{i,i}^{'(2)} = l_{i,i}^{'} + \alpha_1 p_1 p_{i-1,i-1}^{'(1)}\ deg = 3 \\ l_{i,i+1}^{(2)} = l_{i,i+1} + \alpha_1 p_1 p_{i-1,i}^{(1)}\ deg = 3 \end{array}$$

Let us represent:

$$p_1^{(2k-1)} = p_1 + \alpha_2 + \alpha_4 + \ldots + \alpha_{(2k-2)} = p_1^{(2k-3)} + \alpha_{(2k-2)}$$

$$l_1^{(2k)} = l_1 + \alpha_1 + \alpha_3 + \ldots + \alpha_{(2k-1)} = l_1^{(2k-2)} + \alpha_{(2k-1)}$$

Assume that the following vertices:

$$\langle (p)^{(2k-1)}, [l]^{(2k)} \rangle = (p_1^{(2k-1)}, p_{1,1}^{(2k-1)}, \ldots, p_{i,j}^{(2k-1)}, l_1^{(2k)})$$

$$\{ [l]^{(2k)}, (p)^{(2k+1)} \} = (l_1^{(2k)}, l_{1,1}^{(2k)}, \ldots, l_{i,j}^{(2k)}, p_1^{(2k+1)})$$

have the degrees:

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

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

Now we would like to find out degrees of polynomials of the vertices $\langle (p)^{(2k+1)}, [l]^{(2k+2)} \rangle$ and $\{ [l]^{(2k+2)}, (p)^{(2k+3)} \}$.

We have the components of the vertices with the corresponding degrees: :

$$\begin{array}{l} p_{i,i}^{'(2k+1)} = p_{i,i}^{'(2k-1)} - \alpha_{2k} l_{i,i-1}^{(2k)}\ deg = 2 \\ p_{i,i+1}^{(2k+1)} = p_{i,i+1}^{(2k-1)} - \alpha_{2k} l_{i,i}^{(2k)}\ deg = 2 \\ p_{i,i}^{(2k+1)} = p_{i,i}^{(2k-1)} + \alpha_{2k} l_1^{(2k)} l_{i-1,i-1})^{(2k)}\ deg = 3 \\ p_{i+1,i}^{(2k+1)} = p_{i+1,i}^{(2k-1)} + \alpha_{2k} l_1^{(2k)} l_{i,i-1}^{(2k)}\ deg = 3 \end{array}$$

and

$$\begin{array}{l} l_{i,i}^{(2k+2)} = l_{i,i}^{(2k)} + \alpha_{2k+1} p_{i-1,i}^{(2k+1)}\ deg = 2 \\ l_{i+1,i}^{(2+2)} = l_{i+1,i}^{(2k)} + \alpha_{2k+1} p_{i,i}^{'(2k+1)}\ deg = 2 \\ l_{i,i}^{'(2+2)} = l_{i,i}^{'(2k)} + \alpha_{2k+1} p_1^{(2k+1)} p_{i-1,i-1}^{'(2k+1)}\ deg = 3 \\ l_{i,i+1}^{(2+2)} = l_{i,i+1}^{(2k)} + \alpha_{2k+1} p_1^{(2k+1)} p_{i-1,i}^{(2k+1)}\ deg = 3 \end{array}$$

Hence using the induction we get:

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

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

Finally, using the affine transformation in the same way as in **[3]**, independently of the length of the password we get the polynomials of degree 3.

The 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 $Q = Q(K)$ a projective limit of $Q(n,K)$, $n \to \infty$.

In **[16]**, **[15]** it was shown that the projective limit of the graphs $\widetilde{DD(n,K)}$ is an acyclic graph and the length of the minimal directed cycle in $\widetilde{DD(n,K)}$ is bounded below by $[n+5]/2$. It means that we get the following statement.

Proposition 5. The order of each nonidentical element of $Q(K)$ is infinity. Let $g \in Q(K)$ be an element of length $l(g) = k$, then the order of its projection $g_n = \delta_n(g) \in Q_n$, where $k \leq [n+5]/2$, is bounded below by $[n+5]/2k$ The sequence g_n forms a family of stable elements of the increasing order.

Theorem 1 follows immediately from theorem 4 and proposition 5.

5 Operators L and P

Let L_{D,n,β_k} be the operator of taking the neighbour of point:

$$(p)^{2k-2} = (p_{0,1}, p_{1,1}, p_{1,2}, p_{2,1}, p_{2,2}, p_{2,2}^{\prime}, p_{2,3}, \ldots, p_{i,i}, p_{i,i}^{\prime}, p_{i,i+1}, p_{i+1,i}, \ldots),$$

of a kind

$$[l]^{2k-1} = [\beta_k, l_{1,1}, l_{1,2}, l_{2,1}, l_{2,2}, l_{2,2}^{\prime}, l_{2,3}, \ldots, l_{i,i}, l_{i,i}^{\prime}, l_{i,i+1}, l_{i+1,i}, \ldots],$$

where the parameters $l_{1,1}, l_{1,2}, l_{1,2}, l_{2,2}, \ldots, l_{i,i}, l_{i,i+1}, l_{i+1,i}, \ldots$ are computed consequently from the equations in the definition of $D(n,\mathbb{K})$ and all $l_{i,i}^{\prime}$ for $i = 2,3,\ldots$ are computed using the equation describing the connected component.

Similarly, P_{D,n,α_k} is the operator of taking the neighbour of line

$$[l]^{2k-1} = [l_{1,0}, l_{1,1}, l_{1,2}, l_{2,1}, l_{2,2}, \ldots, l_{i,i}, l_{i,i+1}, l'_{i,i}, l_{i+1,i}, \ldots],$$

of a kind

$$(p)^{2k} = (p_{0,1}^{2k-2} + \alpha_k, p_{1,1}, p_{1,2}, p_{2,1}, p_{2,2}, \ldots, p_{i,i}, p'_{i,i}, p_{i,i+1}, p_{i+1,i}, \ldots),$$

where the parameters $p_{1,1}$, $p_{1,2}$, $p_{2,1}$, $p_{2,2}$,..., $p_{i,i}$, $p_{i,i+1}$, $p_{i+1,i}$, ... are computed consequently from the equations in the definition of $D(n, \mathbb{K})$ and all $p'_{i,i}$ for $i = 2, 3, \ldots$ are computed using the equation describing the connected component.

Given the vector $(p)^0 = (p_{0,1}, p_{1,1}, p_{1,2}, p_{2,1}, p_{2,2}, p'_{2,2}, p_{2,3}, \ldots, p_{i,i}, p'_{i,i}, p_{i,i+1}, p_{i+1,i}, \ldots)$, (of length n) let us take the elements $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_k)$ and $\beta = (\beta_1, \beta_2, \ldots, \beta_k)$ from Q^k and the composition $F_{n,\alpha,\beta} = L_{D,n,\beta_1} P_{D,n,\alpha_1} L_{D,n,\beta_2} P_{D,n,\alpha_2} \ldots L_{D,n,\beta_k} P_{D,n,\alpha_k}$.

Theorem 5. (A. Wroblewska) Independently of the choice of $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_k) \in Q^k$ and $\beta = (\beta_1, \beta_2, \ldots, \beta_k) \in Q^k$, the map $F_{n,\alpha,\beta}$ of free module $\mathbb{K}^{n-\lfloor \frac{n+2}{4} \rfloor}$ is a bijective map with the degree $\lfloor \frac{n+2}{4} \rfloor$.

Theorem 6. (V. Ustimenko) The order $F_{n,\alpha,\beta}$ tends to ∞ when $n \to \infty$

6 Application

6.1 Multivariate Diffie-Hellman key exchange protocol

We consider the Diffie-Hellman algorithm for $C(K^n)$ for the key exchange in the case of a group. Let $AGL_n(F_q)$ be the group of affine transformation of the vector space F_q^n, i.e. the 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 sparse matrix with $\det A \neq 0$. Let h_n^k be the new public rule obtained via k iterations of $h_n = F_{n,\alpha,\beta} = L_{D,n,\beta_1} P_{D,n,\alpha_1} L_{D,n,\beta_2} P_{D,n,\alpha_2} \ldots L_{D,n,\beta_k} P_{D,n,\alpha_k}$. The correspondents Alice and Bob have different information for making computation. Alice chooses the dimension n, the element h_n as above, the affine transformation $\tau \in AGL_n(K)$. So she obtains the base $b = \tau h_n^k \tau^{-1}$ and sends it in the form of standard polynomial map to Bob.

So Alice chooses rather large number n_A computes $c_A = b^{n_A}$ and sends it to Bob. In his 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 $C(K^n)$.

6.2 Multivariate map cryptography

The composition of maps $P_{D,n,\alpha_1} P_{D,n,\alpha_2} \ldots P_{D,n,\alpha_k}$ and its usage in cryptography were investigated in detail in [**3**], where it was proved that polynomial maps have

degree 3 but unfortunately, finding an inverse map of this map takes the polynomial map $O(n^{10})$.

Good strengthening of the public rule is the usage of the following idea:

Let τ be the linear transformation $\tau : x \to Ax$, where A is the sparse matrix with thecondition $\det A \neq 0$ Map $\tau F_{n,\alpha,\beta}\tau^{-1}$ written as a multivariate public rule:

$$x_1 \to h_1(x_1, x_2, \ldots, x_n)$$

$$x_2 \to h_2(x_1, x_2, \ldots, x_n)$$

$$\ldots$$

$$x_n \to h_n(x_1, x_2, \ldots, x_n),$$

can be used in public key cryptography. Alice - the holder of the key - keeps linear transformation and $(\beta_1, \alpha_1, \beta_2, \alpha_2, \ldots, \beta_k, \alpha_k)$ secret. Bob (public user) has the above map.

Combining the transformation $F_{n,\alpha,\beta}$ with two linear transformations, Bob gets a formula:

$$y = (h_1(x_1, \ldots, x_n), \ldots, h_n(x_1, \ldots, x_n)),$$

where $h_i(x_1, \ldots, x_n)$ are the polynomials of n variables of the degree $\lfloor \frac{n+2}{4} \rfloor$.

Let us count the number of monomial expressions for $x_i \to h_i(x_1, \ldots, x_n)$. We know that before elimination of x'_{ii} for $i = 2, 3, \ldots, n$ the degree of $h_i(x_1, \ldots, x_n)$ is ≤ 2. We can write $h_i(x_1, \ldots, x_n)$ in the form $g_i(x_{i_1}, x_{i_2}, \ldots, x_{i_n}) + x'_{ii}l(x_{j_1}, x_{j_2}, \ldots, x_{j_n})$, where a list of variables $x_{i_1}, x_{i_2}, \ldots, x_{i_n}$ does not contain variables of the kind x'_{ii} and $\deg l(x_{j_1}, x_{j_2}, \ldots, x_{j_n}) \leq 1$. We have to conduct a specialization $x'_{ii} = x_{ii} + a_i$, where a_i, $\deg a_i = 2$ contain $\leq n$ quadratic monomial expressions. So the expression $(x_{ii} + a_i)l(x_{j_1}, x_{j_2}, \ldots, x_{j_n})$ contains $\leq n^2$ monomial expressions. It means that a new public rule $x_i \to h_i(x_1, \ldots, x_n)$ will contain $O(n^3)$ monomials. The degree of our multivariate map will be cn (c-constant) and the number of expressions h_i is n, so the computation of the map costs $O(n^4)$ operation. Notice that if $x \to Ax$ is a monomial linear transformation, then it can not change the total cost of computation because the number of monomial expression will be the same. The degree of inverse map is also cn, so linearisation attacks are not feasible for sufficiently large n. Therefore the algorithm can be used as a public key

6.3 Private key cryptography

Map $\tau F_{n,\alpha,\beta}\tau^{-1}$, where τ is the affine transformation, can be used as a private key for Alice. Alice and Bob share τ and the sequence $(\beta_1, \alpha_1, \beta_2, \alpha_2, \ldots, \beta_k, \alpha_k)$, where $\alpha_{i+1} - \alpha_i \in Q$ as well as $\beta_{i+1} - \beta_i \in Q$. For $k < \frac{n+5}{2}$ a different password produces a different ciphertext.

6.4 Multivariate private-key algorithm for multiusers' network.

Let us assume that Alice administers a large multiusers' information system (e-parllament, university quality support system, etc). The system is used by many pairs (J_k, B_k) , $k = 1, 2, \ldots$ of users (or groups of users, B and J stand for Brad and Jennifer). Alice has to develop symmetric tools for communication of each pair of the users (J_k, B_k) involved in the activities of the information system.

Alice makes a decision to work with the graph $T(n, K)_J$, $|J| = s$. She takes string $\alpha_1, \alpha_2, \ldots, \alpha_r$ in K^r. For simplicity we assume that r is even.

We assume that $\alpha_i + \alpha_{i+1} \in M(\mathbb{K})$ for $i = 1, 2, \ldots$.

Additionally, she takes the affine transformation τ_1, $\tau_2 = {\tau_1}^{-1}$ and forms the map $f_B = \tau_1 N_{\alpha_1} N_{\alpha_2} \ldots N_{\alpha_r} \tau_1^{-1}$ of degree $s + 3$ in a symbolic way (She can use "Maple", "Sage" or "Mathematica"). Here B stands for the pair b $= (\alpha_1, \alpha_2, \ldots, \alpha_r)$, τ_1.

She gets the encryption map as a nonlinear pseudopublic rule: $x_1 \to f_1(x_1, x_2, \ldots, x_n)$, $x_2 \to f_2(x_1, x_2, \ldots, x_n)$, $\ldots, x_n \to f_n(x_1, x_2, \ldots, x_n)$, where f_i are the multivariable polynomials from $\mathbb{K}[x_1, x_2, \ldots, x_n]$.

Let $S_k = (B_k, J_k)$, $k = 1, 2, \ldots, N$ be the pairs of users (B and J stand for Brad and Jennifer).

Alice provides each pair with the "seed" triple C_k, f_{B_k}, D_k, where C_k and D_k are the linear or affine transformations of the plainspace $\mathbb{K}^n$ of large order (like maps conjugated with the Singer cycles of the order $q^n - 1$ in the case of $\mathbb{K} = F_q$) and gives them also ${f_{B_k}}^{-1}$. So they can use the encryption map $C_k f_{B_k} D_k$ and decrypt with ${D_k}^{-1} f_{B_k}^{-1} {C_k}^{-1}$.

The pair (J_k, B_k) can take "quite close " primes p_1, p_2, p_3 (or pseudoprimes) numbers to $|C_k|$, $p_2 = |D_k|$ and $|f_{B_k}|$. They use the Diffie-Hellman key exchange protocol for ${\mathbb{Z}_{p_i}}^*$ and develop the collision triple $h_i \in {\mathbb{Z}_{p_i}}^*$, $i = 1, 2, 3$. During the session they use the encryption and decryption nonlinear maps ${C_k}^{h_1} {f_{B_k}}^{h_2} D_k^{h_3}$ and ${D_k}^{-h_3} {f_{B_k}}^{-h_2} D_k^{-h_1}$.

Notice that S_k is known to the trusted third party (Alice), but triple h_1, h_2, h_3 is the individual private password for Brad and Jennifer. There is no need to compute a new encryption map symbolically, users just apply $D_k^{h_3}$, $f_{B_k}^{h_2}$ and ${C_k}^{h_1}$ consequtively to the plainspace vector. In the next session of the key exchange, Brad and Jennifer can get a new triple $h'_j \in {\mathbb{Z}_{p_j}}^*$, $j = 1, 2, 3$ and use the numbers $h"_j = h'_j h_j \mathrm{mod} p_j$ for the modification of multivariate encryption map. This approach leads to dependence of the algorithm from the prehistory of communications.

The use of key exchange protocols as tools of protection against linearisation attacks is a standard one.

References

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

[2] 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.

[3] Wroblewska A., On some properties of graph based public keys, Albanian Journal of Mathematics 2(3) (2008): 229.
[4] Bollobás B., Extremal Graph Theory, Academic Press, London (1978).
[5] Margulis G. A., Explicit construction of graphs without short cycles and low density codes, Combinatorica 2 (1982): 71.
[6] Lubotsky A., Philips R., Sarnak P., Ramanujan graphs, J. Comb. Theory. 115(2) (1989): 62.
[7] Guinand P. S., 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.
[8] Guinand P. S., 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.
[9] Kim J.-L., Peled U. N., Perepelitsa I., Pless V., Friedland S., Explicit construction of families of LDPC codes with no 4-cycles, Information Theory, IEEE Transactions 50(10) (2004): 2378.
[10] 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).
[11] 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.
[12] Ustimenko V. A., CRYPTIM: Graphs as Tools for Symmetric Encryption, in Lecture Notes in Computer Science 2227 (2001): 278.
[13] Ustimenko V. A., 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., 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).
[17] Ustimenko V. A., Linguistic Dynamical Systems, Graphs of Large Girth and Cryptography, Journal of Mathematical Sciences, Springer 140(3) (2007): 412.
[18] Ustimenko V. A., 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.
[19] Biggs N. L., Graphs with large girth, Ars Combinatoria 25C (1988): 73.
[20] Lazebnik F., Ustimenko V. A., Woldar A. J., A Characterization of the Components of the graphs $D(k, q)$, Discrete Mathematics 157 (1996): 271.
[21] Lazebnik F., Ustimenko V., Explicit construction of graphs with an arbitrary large girth and of large size, Discrete Appl. Math. 60 (1995): 275.