Pobrane z czasopisma Annales AI- Informatica **http://ai.annales.umcs.pl**
Data: 10/09/2025 14:13:00

Annales UMCS Informatica AI XII, 3 (2012) 65–74
DOI: 10.2478/v10065-012-0030-2

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

Dynamical systems as the main instrument for the constructions of new quadratic families and their usage in cryptography

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 – Let K be a finite commutative ring and $f = f(n)$ a bijective polynomial map $f(n)$ of the Cartesian power K^n onto itself of a small degree c and of a large order. Let f^y be a multiple composition of f with itself in the group of all polynomial automorphisms, of free module K^n. The discrete logarithm problem with the "pseudorandom" base $f(n)$ (solve $f^y = b$ for y) is a hard task if n is "sufficiently large". We will use families of algebraic graphs defined over K and corresponding dynamical systems for the explicit constructions of such maps $f(n)$ of a large order with $c = 2$ such that all nonidentical powers f^y are quadratic polynomial maps. The above mentioned result is used in the cryptographical algorithms based on the maps $f(n)$ – in the symbolic key exchange protocols and public keys algorithms.

1 Introduction

The sequence of subgroups G_l of Cremona group $C(K^l)$, $l \to \infty$ is a *family of stable groups* if the degree of each g, $g \in G_l$, is bounded by the constant c independent of l. The construction of large stable subgroups G_l with $c \geq 2$ of the Cremona group is an interesting mathematical task. Obviously the subgroup $AGL_n(F_p)$ of all affine bijective maps $\mathrm{x}A + \mathrm{b}$, where x and b are the row vectors from V and A is a nonsingular square matrix, is of the order $p^n(p^n - 1)(p^n - p)\dots(p^n - p^{n-1})$. The affine transformations form a family of subgroups of stable degree with $c = 1$. There is an easy way to

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

Pobrane z czasopisma Annales AI- Informatica **http://ai.annales.umcs.pl**
Data: 10/09/2025 14:13:00

construct stable subgroups via conjugation of $AGL_l(K)$ with the nonlinear polynomial maps $f_l \in C(K^l)$. Let us refer to such families as the pseudolinear groups. Degrees of f_l and ${f_l}^{-1}$ are at least two. So, in the case of "pseudorandom" polynomials f_l, such that $\max(f_l, {f_l}^{-1})$ is bounded by constant, we obtain a stable family with $c \geq 4$. Algorithm for fast generation of nonlinear pairs $(f_l, {f_l}^{-1})$ is introduced in [**1**] and [**2**]. Let τ be a Singer cycle from $AGL_l(F_p)$ of the order $p^n - 1$, f_l and ${f_l}^{-1}$ are the nonlinear maps. Then $g = {f_l}^{-1}\tau f_l$ looks as the appropriate base for the hidden symbolic discrete logarithm problem.

Notice, that the degree of ${f_l}^{-1}\tau f_l$, where $\deg(\tau) = 1$ and f_l is the pseudorandom polynomial map of the degree ≥ 2, will be ≥ 4. So, the case of families of stable degree with $c \in \{2, 3\}$ is the most interesting. The family of large stable subgroups of $C(K^l)$ over the general commutative ring K containing at least 3 regular elements (non zero divisors), with $c = 3$ is constructed in [**3**] via the studies of encryption maps from [**4**] and the evaluation of their degrees [**5**]. In this paper we propose a similar result for the case of $c = 2$.

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 proven by Paul Erdös' (see [**6**]). Together with the common Ramanujan graphs, introduced by G. Margulis ([**7**], [**8**]), the graphs $CD(n, q)$ form one of the first explicit constructions of such families with the 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**],[**4**],[**13**],[**2**], the option to use them for public key cryptography was considered in [**14**], [**15**] and in [**16**], where the related dynamical system was introduced (see also surveys [**17**],[**18**]).

The computer simulation ([**1**]) shows that the 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 Section 2 we discuss the discrete logarithm problem for the symmetric group S_{p^n} considered as a totality of all polynomial bijective maps of n-dimensional vector space over F_p. We also consider a more general case of the Cremona group of the whole polynomial automorphism of the free module K^n over the general commutative ring K.

Section 3 is devoted to the explicit construction of the quadratic polynomial maps with the properties given above.

In Section 4 we present the cryptograpical application of the quadratic polynomial maps in the public key algorithm and the key exchange protocol.

Pobrane z czasopisma Annales AI- Informatica **http://ai.annales.umcs.pl**
Data: 10/09/2025 14:13:00

2 On the discrete logarithm problem for the Cremona groups

The discrete logarithm problem is a critical problem in the number theory. Like the factorization problem, the discrete logarithm problem is believed to be difficult and also to be the 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 group theoretical discrete logarithm problem is the following: an element g in a finite group G and another element $h \in G$ are given, find a positive integer x such that $g^x = h$.

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 the RSA public key encryption. In the majority of other cases complexity of discrete logarithm problem is not investigated properly. The problem consists in the choice of the base g and the way of the data representation on the group. A group can be defined via generators and relations, as an automorphism group of algebraic variety, as a matrix group, as a permutation group etc. The following example demonstrates the importance of the way of abstract group G representation.

The multiplicative groups ${Z_p}^*$ are isomorphic to the additive group of the ring Z_{p-1}, if p is "sufficiently large" then the discrete logarithm problem is known as a hard one, but for Z_{p-1} the problem is equivalent to solving of a linear equation.

Let us discuss the case of the symmetric group S_{p^n} of the order $p^n!$ presented as the Cremona group of all bijective polynomial automorphisms of n-dimensional vector space $V = {F_p}^n$ over the finite prime field F_p.

Let us choose the standard base of V. It is well known that each permutation π from the symmetric group S_{p^n} can be written in the form of "public rule" g:

$x_1 \to g_1(x_1, x_2, \ldots, x_n), x_2 \to g_2(x_1, x_2, \ldots, x_n), \ldots, x_n \to g_n(x_1, x_2, \ldots, x_n)$, where g_i are multivariable polynomials from $F_p[x_1, x_2, \ldots, x_n]$.

Notice that there is no good bound on the order of g. Usually the order of nonlinear polynomial map g^k (composition of g with itself, responding to the permutation π^k) increases with the increasing of k. The computation of the order t of "pseudorandom" g is a difficult task. Really, if t is known then the inverse map for g is g^{t-1}, but the best known algorithm of finding g^{-1} has complexity $d^{O(n)}$, where d is the degree of g (see [**?**]).The efficient general algorithm of finding g^{-1} is known only in the case the degree of g is one, i. e. g is the affine map $\mathrm{x}A + \mathrm{b}$, where x and b are the row vectors from V and A is the nonsingular square matrix. So, there is a serious complexity gap between linearity and nonlinearity.

The discrete logarithm problem for the cyclic group generated by the "pseudorandom" polynomial map $g \in S_{p^n}$, i. e. the problem of finding solution for the equation $g^x = b$, seems to be very hard. If x is known then $g^{t-x} = b^{-1}$, but the computation of $b{-}1$ takes $d^{O(n)}$. So, in the case of "pseudorandom" polynomial base g we can use the term *hidden symbolic* discrete logarithm problem, word *hidden* is taken because

Pobrane z czasopisma Annales AI- Informatica **http://ai.annales.umcs.pl**
Data: 10/09/2025 14:13:00

of the order t of the cyclic group is unknown, *symbolic* is taken because generation of the polynomial maps g and b can be done via tools of symbolic computations (popular "Maple" or "Mathematica" operating on the polyomial maps or special fast programs of Computer Algebra).

The above mentioned arguments on the complexity of discrete logarithm problem are valid for the Cremona groups $C(K^n)$ of all polynomial automorphisms of the free module K^n over the general commutative group. Recall that automorphism of K^n is a bijective polynomial map $f : K^n \to K^n$ such that f^{-1} is also a polynomial map.

Even in the case of fields, the importance of the requirement on polynomiality of f^{-1} is essential as demonstrated by the following example: for $n = 1$ and $K = R$ (real numbers) map $x \to x^3$ is a polynomial map but its inverse is $y \to y^{1/3}$ (rational map). As follows from the definition, $C(z_p{}^n)$ is isomorphic to S_{p^n}.

The group $C(K^n)$ is an important object of algebraic geometry. There are many open questions about this group. For instance, let $AGl_n(K)$ be the totality of all invertible affine maps of K^n onto itself. Describe proper subgroups X of $C(K^n)$ containing $AGL_n(K)$ as proper subgroups. If $K = F_p$ and $n \geq 3$ then $AGL_n(F_p)$ is a maximal subgroup of S_{p^n}, so X as above does not exist. For the majority of other rings the question is open.

3 Explicit construction of the quadratic polynomial maps

3.1 Graph theoretical base

The missing definitions of graph-theoretical concepts which appear in this paper can be found in [**6**]. All graphs under consideration 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_iGv_{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 the length m, i.e. the sequence of distinct vertices $v_1, \ldots, v_m$ such that v_iGv_{i+1}, $i = 1, \ldots, m-1$ and v_mGv_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 neighbuors (see [**19**] or [**6**]).

The incidence structure is the set V with partition sets P (points) and L (lines) and symmetric binary relation I such that the incidence of two elements implies that one of them is a point and another one 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

Pobrane z czasopisma Annales AI- Informatica **http://ai.annales.umcs.pl**
Data: 10/09/2025 14:13:00

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 **[20]**). The graph is k-regular if each of its vertices has degree k, where k is a constant. In this section we reformulate the results of **[21]**, **[3]** 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 **[7]**:

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

We now define an incidence structure (P, L, I) as follows. We say 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) is denoted $D(q)$. Now we refer to 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 the notation in the 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 $k \geq 2$ we obtain an incidence structure (P_k, L_k, I_k) as follows. P_k and L_k are obtained from P and L, respectively, by simply projecting each

Pobrane z czasopisma Annales AI- Informatica **http://ai.annales.umcs.pl**
Data: 10/09/2025 14:13:00

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 1. **[3]** 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, $g(D(k,q)) \geq k+4$.

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

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

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 **[21]** the following statement was proved.

Proposition 1. 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 the 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 **[18]** and further references).

Proposition 2. Let q be an odd number. The vertices u and v of $D(q)$ $(D(k,q))$ belong to the same connected component if and only if $a(u) = a(v)$, i.e., $\tau = \tau'$ and $EQ(q) = CD(q)$ $(EQ(k,q) = CD(k,q))$.

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

Pobrane z czasopisma Annales AI- Informatica **http://ai.annales.umcs.pl**
Data: 10/09/2025 14:13:00

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 the power of 2, $q>2$ is very important for the 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 $a_i(x)=a_i(v)$, $i=2,3,\ldots$.

Let $P_{D,t,n}=P_D(t,n,\mathbb{K})$ be the operator of taking the neighbour of point

$$(p)=(p_{0,1},p_{1,1},p_{1,2},p_{2,1},p_{2,2},p'_{2,2},p_{2,3},\ldots,p_{i,i},p'_{i,i},p_{i,i+1},p_{i+1,i},\ldots),$$

of the kind

$$[l]=[p_{0,1}+t,l_{1,1},l_{1,2},l_{2,1},l_{2,2},l'_{2,2},l_{2,3},\ldots,l_{i,i},l'_{i,i},l_{i,i+1},l_{i+1,i},\ldots],$$

where the parameters $l_{1,1},l_{1,2},l_{1,2},l_{2,2},\ldots,l_{i,i},l'_{i,i},l_{i,i+1},l_{i+1,i},\ldots$ are computed consequently from the equations in the definition of $D(n,\mathbb{K})$. Similarly, $L_{D,t,n}=L_D(t,n,\mathbb{K})$ is the operator of taking the neighbour of line

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

of the kind

$$(p)=(l_{1,0}+t,p_{1,1},p_{1,2},p_{2,1},p_{2,2},\ldots,p_{i,i},p'_{i,i},p_{i,i+1},p_{i+1,i},\ldots),$$

where the parameters $p_{1,1}$, $p_{1,2}$, $p_{2,1}$, $p_{2,2},\ldots$, $p_{i,i}$, $p'_{i,i}$, $p_{i,i+1}$, $p_{i+1,i}$, $\ldots$ are computed consequently from the equations written above.

Notice, that $P_n=L_n=\mathbb{K}^n$. So, we can think that $P_{D,t,n}$ and $L_{D,t,n}$ are the bijective operators on the free module $\mathbb{K}^n$.

Theorem 2. For each commutative ring $\mathbb{K}$ transformations $P_{D,t,n}$ and $L_{D,t,n}$ of $\mathbb{K}^n$ form the symmetric bipartite dynamical system $SB_D(\mathbb{K})$ of large girth with $c=1/2$, such that $t'=-t$, $t\in\mathbb{K}$ and nonidentical transformation of the kind $F_{D_P,t_1,t_2,\ldots,t_l,n}$ or $F_{D_L,t_1,t_2,\ldots,t_l,n}$, where $(t_1,t_2,\ldots,t_l)\in\mathbb{K}^l$ is a cubical map.

3.2 Explicit construction of families of quadratic polynomials

For the plaintext, let us take the point defined as above, but with the fixed first coordinate:

$(p)=(c_1,p_{1,1},p_{1,2},p_{2,1},p_{2,2},p'_{2,2},p_{2,3},\ldots,p_{s,s},p'_{s,s},p_{s,s+1},p_{s+1,s})$,

then consequently, for each element of the password $t_1,t_2,\ldots,t_l$ let us do the following steps:

(1) The coordinates $c_1,p_{1,1},p_{1,2},p_{2,1},p_{2,2},p'_{2,2},p_{2,3},\ldots,p_{s,s}$ are determined the operator $P_{D,t,n}$ or $L_{D,t,n}$, according to the following "rule":
$(p)^{(0)}\longrightarrow[l]^{(1)}=P_{D,t_1,n}((p)^{(0)})\longrightarrow(p)^{(2)}=L_{D,t_2,n}([l]^{(1)})\longrightarrow\ldots\longrightarrow[l]^{(l)}=P_{D,t_l,n}((p)^{(l-1)})\longrightarrow(p)^{(l+1)}=L_{D,t_{l+1},n}([l]^{(l)})$

Pobrane z czasopisma Annales AI- Informatica **http://ai.annales.umcs.pl**
Data: 10/09/2025 14:13:00

(2) The last coordinate with "primes", i.e., for $s = \lfloor n + 2/4 \rfloor$, using $a_r = a_r(u) = \sum_{i=0}^{r}(u_{ii}u'_{r-i,r-i} - u_{i,i+1}u_{r-i,r-i-1}) = 0$, we get:
$l'_{ss} = \sum_{i=0}^{s-2}(l_{ii}l'_{s-i,s-i} - l_{i,i+1}l_{s-i,s-i-1}) + l_{s-1,s-1}l_{11} - l_{s-1,s}l_1 + l_{ss}$ or
$p'_{ss} = \sum_{i=0}^{s-2}(p_{ii}p'_{s-i,s-i} - p_{i,i+1}p_{s-i,s-i-1}) + p_{s-1,s-1}p_{11} - p_{s,s-1}p_1 + p_{ss}$,
respectively.

(3) The last two coordinates $p_{s,s+1}, p_{s+1,s}$ are calculated using the operator $P_{D,t,n}$ or $L_{D,t,n}$.

Since we have fixed the first coordinate, the operators $P_{D,t,n}$ and $L_{D,t,n}$ of $\mathbb{K}^n$ make the coordinates $c_1, p_{1,1}, p_{1,2}, p_{2,1}, p_{2,2}, p'_{2,2}, p_{2,3}, \ldots, p_{s,s}$ linear maps. The coordinates l'_{ss} and p'_{ss}, which are quadratic maps, are made invisible. The last two coordinates $p_{s,s+1}$ and $p_{s+1,s}$ are also quadratic.

4 Public key cryptography and key exchange protocol

We may assume that g is a private key encryption map corresponding to the numerical string $(x_1, x_2, \ldots, x_s)$ (the key). It is clear that the inverse map corresponds to the reverse string $(x_s, x_{s-1}, \ldots, x_1)$.

We implement the public key encryption and the symbolic version of the Diffie-Hellman key exchange corresponding to the quadratic maps $f_1 g_n f_2$ and ${f_1}^{-1} g_n f_1$ with the fixed sparse affine transformations f_1 and f_2.

The typical choice of f_i is a linear transformation $x_1 \to x_1 + r_2 x_2 + \cdots + r_n x_n$, where the parameters r_j are taken consecutively from the infinite pseudorandom sequences of the regular elements $r_i, i = 2, 3, \ldots$.

Public key and key exchange algorithms are implemented on the level of symbolic computations while decryption ${f_2}^{-1} g_n {f_1}^{-1}$ will be done by numerical algorithm $A = A(f_1, f_2)$ with the key space $(x_1, x_2, \ldots, x_s)$ of variable dimension s. Obviously we can use A independently as the symmetric private key algorithm.

Notice, that in the case of $f_2 = {f_1}^{-1}$ and the periodic password obtained via repetition of the word $(a, b, \alpha_1, \alpha_2, \ldots, \alpha_{2s})$, where $-\alpha_{2s} + a$ and $-\alpha_{2s} + b$ are the regular elements of the ring K, the security of public rule and related stream cipher is connected with the studies of discrete logarithm problem in the Cremona group (the base is $f_1 g f_1 - 1$, where g is the encryption map corresponding to string $(a, b, \alpha_1, \alpha_2, \ldots, \alpha_{2s})$).

To use these results in the public key cryptography over $K = F_q$, let us combine the quadratic polynomial transformations N_l (given in 3.2) with two affine transformation T_1 and T_2. Alice can use $T_1 N_l T_2$ for the construction of the following public map of

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

$F_i(x_1, \ldots, x_n)$ are the polynomials of n variables written as the sums of monomials of the kind $x_{i_1}^{m_1} x_{i_2}^{m_2}$ with the coefficients from $K = F_q$, where $i_1, i_2 \in 1, 2, \ldots, n$ and m_1, m_2 are positive integers such that $m_1 + m_2 \leq 2$. As mentioned before, the polynomial equations $y_i = F_i(x_1, x_2, \ldots, x_n),\ i = 1, 2 \ldots n$, which are made public, are of

Pobrane z czasopisma Annales AI- Informatica **http://ai.annales.umcs.pl**
Data: 10/09/2025 14:13:00

degree 2. Hence the process of an encryption and a decryption can be done in the polynomial time $O(n^3)$. But the cryptoanalyst Cezar, having only a formula for y, has a very hard task to solve the system of n equations of n variables of degree 2. It can be solved in the exponential time $O(2^{n^2})$ by the general algorithm based on the Gröbner basis method. Anyway the studies of specific features of our polynomials could lead to effective cryptanalysis. This is an open problem for specialists.

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 the open communication channel, choose positive integers n_A and n_B, respectively, and exchange the public rules $h_A = g^{n_A}$ and $h_B = g^{n_B}$ via the open channel. Finally, they compute 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 a bad choice of the base for the discrete logarithm problem. In this case n_A is just a ratio of degh_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 a 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 above theorem, element $h \in Q_n$ and affine transformation $\tau \in AGL_n(K)$. So she obtains the base $b = \tau^{-1}h^{-1}g_n h\tau$ and sends it in the form of the standard polynomial map to Bob.

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

References

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

[2] 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.

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

Pobrane z czasopisma Annales AI- Informatica **http://ai.annales.umcs.pl**
Data: 10/09/2025 14:13:00

[4] Ustimenko V., CRYPTIM: Graphs as Tools for Symmetric Encryption, Lecture Notes in Computer Science 2227 (2001): 278.
[5] Wroblewska A., On some properties of graph based public keys, Albanian Journal of Mathematics 2 (3) (2008): 229.
[6] Bollobás B., Extremal Graph Theory, Academic Press,
[7] Margulis G. A., Explicit construction of graphs without short cycles and low density codes, Combirica 2 (1982): 71.
[8] Lubotsky A., Philips R., 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 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.
[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] Ustimenko V. A., Maximality of affine group, and hidden graph cryptosystems, J.Algebra and Discrete Math. 10 (2004): 51.
[15] 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).
[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] 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.
[19] Biggs N. L., Graphs with large girth, Ars Combinatoria 25C (1988): 73.
[20] Moore E. H., Tactical Memoranda, Amer. J. Math. 18 (1886): 264.
[21] Lazebnik F., Ustimenko V. A., Woldar A. J., A Characterization of the Components of the graphs $D(k, q)$, Discrete Mathematics 157 (1996): 271.