Pobrane z czasopisma Annales AI- Informatica **http://ai.annales.umcs.pl**
Data: 01/03/2026 17:37:22

Annales UMCS Informatica AI XIV, 1 (2014) 19–36
DOI: 10.2478/umcsinfo-2014-0004

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

On New Examples of Families of Multivariate Stable Maps and their Cryptographical Applications

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

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

Abstract – Let $\mathbb{K}$ be a general finite commutative ring. We refer to a family g_n, $n = 1, 2, \ldots$ of bijective polynomial multivariate maps of $\mathbb{K}^n$ as a family with invertible decomposition $g_n = g_n^1 g_n^2 \ldots g_n^k$, such that the knowledge of the composition of g_n^i allows computation of g_n^i for $O(n^s)$ $(s > 0)$ elementary steps. A polynomial map g is stable if all non-identical elements of kind g^t, $t > 0$ are of the same degree.

We construct a new family of stable elements with invertible decomposition. This is the first construction of the family of maps based on walks on the bipartite algebraic graphs defined over $\mathbb{K}$, which are not edge transitive. We describe the application of the above mentioned construction for the development of stream ciphers, public key algorithms and key exchange protocols. The absence of edge transitive group essentially complicates cryptanalysis.

1 Introduction

Post Quantum Cryptography could not use many security tools based on Number Theory, because of the factorization algorithm developed by Peter Shor. This fact and the fast development of Computer Algebra make multivariate cryptography (see [**2**] and [**5**]) an important fiels of research. The Quantum Computer is a special random computational machine. Recall that computation in the Turing machine can be formalised with the concept of finite automaton as a walk in the graph with th arrows labelled by special symbols. Żandom computationćan be defined as a random walk in the random graph. So, we are looking for the deterministic approximation of random

*awroblewska@hektor.umcs.lublin.pl
†vasyl@hektor.umcs.lublin.pl

Pobrane z czasopisma Annales AI- Informatica **http://ai.annales.umcs.pl**
Data: 01/03/2026 17:37:22

graphs by extremal algebraic graphs. It is known that the explicit solutions for optimization graphs have properties similar to random graphs. The probability of having rather short cycle in the walking process on a random graph is zero. So, the special direction of Extremal Graph Theory of the studies of graphs of the order v (the variable) without short cycles of maximal size (number of edges) can lead to the discovery of good approximations for random graphs. In the paper we introduce the explicit constructions of sequences of elements of the stable degree c for each commutative ring $\mathbb{K}$ containing at least 3 elements and each $c \geq 2$. Special cases of $c = 3$ and $c = 2$ were obtained in [**36**] and [**35**]. We discuss the implementation of related key exchange and public key algorithms. It is interesting that in the case of $c \geq 4$, the use of special affine bijections leads to sparse polynomial transformation with $O(n^3)$ monomial terms. These results are based on the construction of the family $D(n, q)$ of graphs with large girth (together with their generalisations $D(n, \mathbb{K})$ where $\mathbb{K}$ is a commutative ring) and the description of their connected components $CD(n, q)$ ($CD(n, \mathbb{K})$, respectively). The existence of infinite families of graphs of large girth was proved by Paul Erdös' (see [**1**]). Together with the famous Ramanujan graphs introduced by G. Margulis [**14**] and investigated in [**9**] the graphs $CD(n, q)$ are one of the first explicit constructions of such families with an unbounded degree. The graphs $D(n, q)$ were used for the construction of LDPS codes and turbocodes which were applied in real satellite communications ([**3**] and further references), for the development of private key encryption algorithms ([**22**], [**23**]), the option to use them for public key cryptography was considered in [**24**], [**29**] and in [**28**], where the related dynamic system was introduced. Notice, that many applications of graph stable polynomial maps are connected with the development of stream ciphers (see [**6**], [**7**], [**8**] for recent fast implementations and key exchange protocols (see [**16**], [**17**], [**35**], [**36**] and further references). The idea to use recurrencies in the construction of public key based on the family of multivariate maps is considered in [**19**].

Section 2 is devoted to the concept of multivariate family of stable map of the increasing order with polynomial density and invertible decomposition. The ideas of application of such families for the construction of key exchange protocols, private and public keys are given there. The method of protection of large network of users based on the special family of graph based maps was given in [**39**]. We describe its generalisation in the case of general family of stable maps with invertible decompositions considered in Section 3. Section 4 contains preliminaries on incidence structures and their polarities. Section 5 is devoted to the graphs of large girth $D(n, q)$, their generalisations $D(n, \mathbb{K})$ for the case of general commutative ring and special automorphisms of these graphs.

In Section 6 we introduce the algebraic technique of ćompressionóf graphs $D(n, \mathbb{K})$ which allows to eliminate some variables and decreases the number of connected components.

Notice that the first example of cubical family of stable multivariate maps was introduced in [**24**], but the degree of members of this family was computed in [**37**]. A similar family of degree 2 was introduced in [**36**]. Construction of the families of stable maps

Pobrane z czasopisma Annales AI- Informatica **http://ai.annales.umcs.pl**
Data: 01/03/2026 17:37:22

of the constant degree ≥ 4 is not a difficult problem itself. It becomes an interesting and practical task if we add the condition of existence of invertible decomposition. A higher degree of stable encryption transformation corresponds to a better resistance to linearisation attacks. In the case of the family of stable maps of unbounded degree, the linearisation attacks are not feasible, but for the creation of efficient public rule one needs polynomiality requirements on the density. The first example of such a family was given in [**38**] (see also [**39**]). Section 7 is devoted to the method of construction of new families of stable maps of polynomial density of bounded or unbounded degree with invertible decomposition obtained from the graphs $D(n, \mathbb{K})$ and corresponding to them polarity graphs by the ćompression"method.

2 On the Concept of Multivariate Families of Stable Maps and its Cryptographic Applications

Recall that Cremona group $C(\mathbb{K}^n)$, where $\mathbb{K}$ is a commutative ring, is a totality of all bijective polynomial transformations g of $\mathbb{K}^n$ such that g^{-1} is also a polynomial map. We say that the sequence g_n, $n \geq 3$, $n \to \infty$ of polynomial bijective maps of free module $\mathbb{K}^n$ over the commutative ring $\mathbb{K}$ is a sequence of stable degree if the degree of g_n is $c = O(n)$ and each map of the kind g_n^k (iteration of g with itself in the Cremona group) has a degree $\leq c$. We refer to the family $g_n \in C(\mathbb{K}^n)$ as the family with invertible decomposition if each g_n is a composition of several elementary polynomial maps g_n^i, $i = 1, 2, \ldots k_n$ of $\mathbb{K}^n$ such that their inverses can be computed for $O(n^s)$ elementary steps, where $s > 0$ is a constant. We say that the sequence $g_n \in C(\mathbb{K}^n)$ forms a family of maps of the increasing order if the order $|g_n|$ is $\geq cn$ for an independent positive constant c. We refer to g_n as a family of polynomial density if $d(g^n) = O(n^t)$ for an independent constant t.

The plainspace of the encryption algorithm (public or private) is $\mathbb{K}^n$, where $\mathbb{K}$ is the chosen finite commutative ring.

We assume that each map g_n from the stable family of polynomial density of the increasing order is a composition of several elementary polynomial automorphisms g_n^i, $i = 1, 2, \ldots k_n$ of $\mathbb{K}^n$ such that their inverses can be computed for $O(n^s)$ elementary steps, where $s > 0$ is a constant. We refer to a family g_n with such decomposition as a family of maps with invertible decomposition.

We create an encryption map h_n as a conjugation of g_n with the special invertible affine transformation $\tau = \tau_n$ (degree equals 1) of $\mathbb{K}^n$. In the case of private keys both correspondents Alice and Bob know the decompositions $g_n = g_n^1 g_n^2 \ldots g_n^{k_n}$, and the family τ_n of affine transformation.

For the creation of a public key encryption, Alice uses her knowledge on the decompositions $g_n = g_n^1 g_n^2 \ldots g_n^{k_n}$ and the family τ_n and computes symbolically the corresponding polynomial map $h = \tau^{-1} g_n \tau$ of $\mathbb{K}^n$ onto $\mathbb{K}^n$ in its standard form $h_1 \to h_1(x_1, x_2, \ldots x_n), h_2 \to h_2(x_1, x_2, \ldots x_n), \ldots, h_n \to h_n(x_1, x_2, \ldots x_n)$, where the

Pobrane z czasopisma Annales AI- Informatica **http://ai.annales.umcs.pl**
Data: 01/03/2026 17:37:22

monomial terms h_i $(i = 1, 2, \ldots, n)$ are listed in the lexicographical order. The public user, Bob has only the public rule h in the above written form.

Remark 1. Notice, that the family h_n is automatically the family of stable maps of increasing order, but in the case of creating the public rule Alice needs special choice of τ_n for making public rules of polynomial density. As it follows from the definitions of stable family, the inverse for h_n has a degree $\leq \deg(h_n)$. So, for resistance of public key against linearisation attacks we need the conditions $\deg(h_n) \geq cn$ and $\deg(\mathrm{h_n})^{-1} \geq \mathrm{cn}$, where c is a positive independent constant.

The family of stable transformations h_n of the polynomial density and the increasing order with the small constant degree k, can also be used as a base of the group theoretical Diffie-Hellman key exchange algorithm for the Cremona group $C(\mathbb{K}^n)$ of all regular automorphisms of $\mathbb{K}^n$. 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 the 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.

Remark 2. Notice, that for the practical use of Diffie - Hellman algorithms families of stable maps h_n such that $\deg(h_n) \leq c$, where c is a positive independent constant have a serious preference. The property to be a family with invertible decomposition is immaterial in the case of key exchange protocols.

Let $\tau = \tau_n$, $n = 1, 2, \ldots$ be a family of affine maps and h_n be a general family of nonlinear maps of polynomial density. We say that τ makes a left (right) polynomial shift for h_n if the sequence τh_n ($h_n\tau$, respectively) is also a family of polynomial density. We may convert the encryption map h_n of private or public key algorithms into the shifted map $\tau_n h_n$ ($h_n\tau_n$) if τ makes left (right, respectively) polynomial shift of nonlinear sequence. Notice, that the shifted stable family of maps is not usually stable. If $\deg(h_n)$ is bounded by the independent of n constant then each family of affine maps τ_n produces polynomial shift from the right and from the left.

2.1 Multivariate Private-Key Algorithm for Multiuser's Network

Let $S_k = (B_k, J_k)$, $k = 1, 2, \ldots, N$ be the pairs of users.

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

The pair (J_k, B_k) can take "quite close "primes p_1, p_2, p_3 (or pseudoprimes) numbers to $|C_k|$, $|D_k|$ and $|f_{B_k}|$. They use the Diffie-Hellman key exchange protocol for ${\mathbb{Z}_{p_i}}^*$

Pobrane z czasopisma Annales AI- Informatica **http://ai.annales.umcs.pl**
Data: 01/03/2026 17:37:22

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 $C_k^{h_1} f_{S_k}^{h_2} D_k^{h_3}$ and $D_k^{-h_3} f_{B_k}^{-h_2} D_k^{-h_1}$.

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

The use of key exchange protocols as tools of protection against linearisation attacks a standard one (see [**2**]).

2.2 Preliminaries on Graphs and Incidence Structures and their Polarities

The missing definitions of graph-theoretical concepts which appear in this paper can be found in [**1**]. All graphs we consider 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 a pass in a 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 a number of its neighbors (see [**1**]).

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 onr 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 [**15**]).

The graph is k-regular if each of its vertices has a degree k, where k is a constant.

In the next section we reformulate the results of [**10**], [**11**] where the q-regular tree was described in terms of equations over the finite field F_q.

Let us assume that Alice administers large a multi-user information system (e-parlament, 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 Bob and Jennifer). Alice has to develop symmetric tools for communications of each pair of users (J_k, B_k) involved in the activities of the information system.

Pobrane z czasopisma Annales AI- Informatica **http://ai.annales.umcs.pl**
Data: 01/03/2026 17:37:22

Alice makes a decision to work with a stable polynomial family $g(n,\mathbb{K})_J$, $|J| = s$ of the increasing order of polynomial density with the invertible decomposition $g(n,\mathbb{K}) = g^1(n,\mathbb{K})g^2(n,\mathbb{K})\dots g^{k_n}(n,\mathbb{K})$.

Additionally, she takes a family of bijective affine transformation τ_1 and $\tau_2 = {\tau_1}^{-1}$ and forms the left and right shifts of the family $g(n,\mathbb{K})$ by the map τ_1 and τ_2. Let $f(n,\mathbb{K}) = \tau_{1n}g(n,\mathbb{K})\tau_{2n}$. Alice has $f(n,\mathbb{K})^{-1}$ because of the existence of invertible decomposition.

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

2.3 Polarities of Incidence Structures and Related Polarity Graphs

Let P and L be disjoint sets, the elements of which we call *points* and *lines*, respectively. A subset I of $P \times L$ is called an *incidence relation* on the pair (P,L). The *incidence graph* Γ of geometry (P,L,I) is defined to be the bipartite graph with the vertex set $P \cup L$ and the edge set $\{\{p,l\}|p \in P, l \in L, (p,l) \in L\}$.

Let $\pi : P \cup L \to P \cup L$ be a bijection for which the following holds:

(i) $P^\pi = L$ and $L^\pi = P$,

(ii) for all $p \in P$, $l \in L$ $(l^\pi,\ p^\pi) \in I$ if and only if $(p,l) \in I$,

(iii) $\pi^2 = 1$.

We call such π a polarity of the incidence structure (P,L,I). Note that π induces an automorphism of the incidence graph Γ of order 2, which interchanges the partition sets P and L. We shall use the term "polarityąnd the notation "π"for the graph automorphism as well.

We now define the polarity graph Γ^π of the structure (P,L,I) with the respect to the polarity π. It is the graph with the vertex set $V(\Gamma^\pi) = P$ and the edge set $E(\Gamma^\pi) = \{\{p_1,p_2\}\}|p_1,p_2 \in P, p_1 \neq p_2, (p_1,{p_2}^\pi) \in I\}$.

Finally, we call point $p \in P$ an *absolute point* of the polarity π provided (p,p^π) in I.

Let N_π denote the number of absolute points of π.

Proposition 1. (see, for instance [**13**] and further references)

Let π be be a polarity of the finite incidence structure (P,L,I) and let Γ and Γ^π be the correspondent incidence and polarity graphs.

(a) $\deg_{\Gamma^\pi} = \deg_{\Gamma^\pi} - 1$ if p is an absolute point of π, and $\deg_{\Gamma_\pi} = \deg_\Gamma$ otherwise,

(b) $|V(\Gamma)^\pi| = 1/2|V(\Gamma)|$, $|E(\Gamma^\pi)| = |E(\Gamma)| - N_\pi$,

(c) If Γ^π contains a $(2k+1)$-cycle, then Γ contains a $(4k+2)$ cycle,

(d) If Γ^π contains a $2k$-cycle, then Γ contains two vertex disjoint $2k$ cycles C and C' such that $C^\pi = C'$. Consequently, if Γ is $2k$-cycle-free so is Γ^π,

(e) The girth of the two graphs is related by $g(\Gamma^\pi) \geq 1/2g(\Gamma)$.

Pobrane z czasopisma Annales AI- Informatica **http://ai.annales.umcs.pl**
Data: 01/03/2026 17:37:22

3 On Graphs $D(n,q)$, their Generalizations and Corresponding Polarities

Let $\mathbb{K}$ be a commutative ring, and let P and L be two countably infinite dimensional free modules over $\mathbb{K}$. 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 [**14**]:

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

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:

$$\begin{aligned} l_{11} - p_{11} &= l_1 p_1\\ l_{12} - p_{12} &= l_{11} p_1\\ l_{21} - p_{21} &= l_1 p_{11}\\ l_{ii} - p_{ii} &= l_1 p_{i-1,i}\\ l'_{ii} - p'_{ii} &= l_{i,i-1} p_1\\ l_{i,i+1} - p_{i,i+1} &= l_{ii} p_1\\ l_{i+1,i} - p_{i+1,i} &= l_1 p'_{ii} \end{aligned} \tag{2}$$

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

For the case $\mathbb{K} = F_q$, where q is a prime power, the graph $D(q) = D(F_q)$ was defined in [**10**], for the general $\mathbb{K}$ see [**21**]. It was shown that a graph in the graph $D(q)$ is a q-regular forest.

To facilitate 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 :

$$\begin{aligned} l_{ii} - p_{ii} &= l_1 p_{i-1,i}\\ l'_{ii} - p'_{ii} &= l_{i,i-1} p_1\\ l_{i,i+1} - p_{i,i+1} &= l_{ii} p_1\\ l_{i+1,i} - p_{i+1,i} &= l_1 p'_{ii} \end{aligned} \tag{3}$$

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 $l_{1,1} - p_{1,1} = l_1 p_1$.

Pobrane z czasopisma Annales AI- Informatica **http://ai.annales.umcs.pl**
Data: 01/03/2026 17:37:22

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 $D(k, q)$ we are concerned with are described in the following theorem.

Theorem 1. [**10**] 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 $2, 3, \ldots, n, \ldots$ 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 $D(\mathbb{K})$ to $D(i, \mathbb{K})$, and $\eta_{i,j}$ be map "deleting all coordinates with the numbers $> i$ "from $D(j, \mathbb{K})$, $j > i$ into $D(i, \mathbb{K})$.

The following statement follows directly from the definitions:

Proposition 2. (see, [**10**]) The projective limit of $D(i, \mathbb{K}), \eta_{i,j}, i \to \infty$ is an infinite graph $D(\mathbb{K})$.

3.1 Invariants of Connected Components

Let us investigate the connected components of the graphs.

Let $n \geq 6$, $t = \lfloor (n + 2)/4 \rfloor$, 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 $D(n, \mathbb{K})$. (It does not matter whether u is a point or a line). For every r, $2 \leq r \leq t$, let:

$$a_r = a_r(u) = \sum_{i=0}^{r} (u_{ii} u'_{r-i,r-i} - u_{i,i+1} u_{r-i,r-i-1}) \ , \tag{4}$$

and

$$a = a(u) = (a_2, a_3, \cdots, a_t) \ . \tag{5}$$

In [**11**] and [**12**] the following statement was stated and proved.

Proposition 3. 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:

Pobrane z czasopisma Annales AI- Informatica **http://ai.annales.umcs.pl**
Data: 01/03/2026 17:37:22

$$a(v) = (x_2, \ldots, x_t) = (x)\ . \tag{6}$$

Corollary 1. Let us consider a general vertex:

$$x = (x_1, x_{1,1}, x_{2,1}, x_{1,2} \cdots, x_{i,i}, x'_{i,i}, x_{i+1,i}, x_{i,i+1}, \cdots),\ i = 2, 3, \cdots \tag{7}$$

of the connected component $CD(n, \mathbb{K})$, 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 $\mathbb{K}$ and $x'_{i,i}$ could be computed successively as the unique solution of the equations $a_i(x) = a_i(v)$, $i = 2, 3, \ldots$. □

The following statement was given in [**13**] for $\mathbb{K} = F_q$ (see [**28**] for the case of general commutative ring)

Proposition 4. The map π given by the close formula:

$$\begin{aligned} \mathrm{p}^\pi =& [p_{10}, -p_{11}, p_{21}, p_{12}, -p'_{22}, -p_{22}, \ldots, -p'_{ii}, -p_{ii}, p_{i+1,i}, p_{i,i+1}, \ldots], \\ \mathrm{l}^\pi =& (l_{01}, -l_{11}, l_{21}, l_{12}, -l'_{22}, -l_{22}, \ldots, -l'_{ii}, -l_{ii}, l_{i+1,i}, l_{i,i+1}, \cdots) \end{aligned} \tag{8}$$

is a polarity of $D(2n, \mathbb{K})$. It preserves blocks of the equivalence relation τ.

Let $RD(2n, \mathbb{K})$ be a regular folding graph corresponding to the parallelotopic polarity π induced on the vertices of the graph $C(2n, \mathbb{K})$, i. e. a graph of binary relation I' such that $\mathrm{p}^1 I' \mathrm{p}^2$ for $\mathrm{p}^1, \mathrm{p}^2 \in P$ if and only if $p^1_{1,0} \neq p^2_{1,0}$ and $\mathrm{p}^1 I \pi(\mathrm{p}^2)$. If $\mathbb{K}$ is a finite ring, then $RD(2n, \mathbb{K})$ is a $|\mathbb{K}| - 1$ - regular subgraph of polarity graph of $D(2n, \mathbb{K})$ (see [**13**] for $\mathbb{K} = F_q$ and)

Notice, that polarity π preserves blocks of the equivalence relation τ. It means that, if points p_1 and p_2 are in the same connected components of the graph $RD(2n, \mathbb{K})$, then $a_i(\mathrm{p}_1) = a_i(\mathrm{p}_2)$ for $i = 2, 3, \ldots, t(2n)$.

4 On the Compressions of Graphs $D(n, \mathbb{K})$ and Related Polarity Graphs

Let us consider the following equivalence relation $\Leftrightarrow$ on the vertices of the graphs $D(n, \mathbb{K})$ and $RD(2n, \mathbb{K})$:

$$u \Leftrightarrow v \ \text{ if and only if } \ \mathrm{a}(u) = \mathrm{a}(v).$$

As it was proven in [**30**] in the case of char$\mathbb{K} \neq 2$ blocks of the above defined equivalence relation are connected components of the graph $D(n, \mathbb{K})$. In the case of $\mathbb{K} = F_2$ and $\mathbb{K} = F_4$ such blocks contain at least 2 connected component of the graphs (see [**21**]).

Pobrane z czasopisma Annales AI- Informatica **http://ai.annales.umcs.pl**
Data: 01/03/2026 17:37:22

Let $J = j_1, j_2, \ldots, j_s$, where $2 \leq j_1 \leq j_2, \ldots, j_s \leq [(n+2)/4]$. Let $T = T_n(\mathbb{K}, J, b_1, b_2, \ldots, b_s)$ be the subset of all vertices v of $D(n, \mathbb{K})$ satisfying the conditions $a_{j_1}(v) = b_i$, $i = 1, 2, \ldots, s$. This is a disjoint union of several connected components of the graph. Let $CD_J(n, \mathbb{K})$ be the graph of the restriction of incidence relation on the subset T.

We define the compressed graph $CD'_J(n, \mathbb{K})$ of $CD_J(n, \mathbb{K})$ with the points:

$$(p) = (p_1, p_{11}, p_{12}, p_{21}, p_{22}, p'_{22}, p_{23}, \ldots, p_{ii}, p'_{ii}, p_{i,i+1}, p_{i+1,i}, \ldots) \,, \tag{9}$$

and the lines:

$$[l] = [l_1, l_{11}, l_{12}, l_{21}, l_{22}, l'_{22}, l_{23}, \ldots, l_{ii}, l'_{ii}, l_{i,i+1}, l_{i+1,i}, \ldots) \,, \tag{10}$$

without the coordinates p'_{ii} and l'_{ii}, $i \in J$. The incidence I' is defined by the conditions (1) without the equations $l'_{ii} - p'_{ii} = l_{i,i-1}p_1$, $i \in J$.

The expressions for l'_{ii} (p'_{ii}), $i \in J$ in the remaining equations have to be substituted by $a'_i(\mathrm{l}) = b_i - (-1)^e l'_{ii}$ $(a'_i(\mathrm{p}) = \alpha_i - (-1)^e p'_{ii})$, where $e = 0$ if the parameters l_{ii} (p'_{ii}) appear as a sum of $a_i(\mathrm{l})$ $(a_i(\mathrm{p}))$, respectively) with the coefficient $+1$ and $e = 1$ in the opposite case (coefficient is -1). As it follows immediately from the definitions, the graph $CD_J(n, \mathbb{K})$ is an incidence structure (P', L', I'), where the varieties P' and L' are isomorphic to $\mathbb{K}^{n-|J|}$. The compression procedure Δ_J is an isomorphism of $CD_J(n, \mathbb{K})$ onto $CD'_J(n, \mathbb{K}) = \Delta_j(CD_J(n, \mathbb{K}))$. In the case of a maximal possible $J = \{2, 3, \ldots, t(n)\}$ we write simply $CD(n, \mathbb{K})$ and $CD'(n, \mathbb{K})$ and use Δ instead of Δ_J.

Let $\mathrm{p} = (p_{1,0}, p_{11}, \ldots)$ and $\mathrm{l} = [l_{0,1}, l_{1,1}, \ldots]$ be a point and a line of one of the graphs $D(\mathbb{K}), CD(\mathbb{K}), CD_J(n, \mathbb{K}), D(n, \mathbb{K}), CD(n, \mathbb{K})$. We refer to the first coordinates $\rho(\mathrm{p}) = p_{1,0}$ of p and $\rho(\mathrm{l}) = l_{0,1}$ of l as colours of point and line respectively. The colouring ρ as above satisfies the *parallelotopic* property (see **[21]** or **[23]**), i. e. for each vertex of the graph there is a unique neighbour of chosen colour. It is easy to see that Δ_J is a colour preserving graph homomorphism, i. e. $\rho(v) = \rho(\Delta_J(v))$.

Let Γ be one of the graphs $D(\mathbb{K})$, $CD(\mathbb{K})$, $CD'_J(n, \mathbb{K})$, $D(n, \mathbb{K})$, $CD'(n, \mathbb{K})$ with the colouring ρ. We consider the operator ${N^\Gamma}_\beta$ of taking the neighbour of vertex v (point or line) of the colour $\beta \in \mathbb{K}$. It is clear that $\Delta_J {N^{D_J(n,\mathbb{K})}}_\beta = {N^{D(n,\mathbb{K})}}_\beta \Delta_J$

Notice that the polarity π acts naturally on the vertices of $CD_J(2n, \mathbb{K})$. The induced permutation is a polarity of this graph. So, we can consider a polarity graph ${CD_J}^\pi(2n, \mathbb{K})$ and a regular folding graph $RD_J(2n, \mathbb{K})$.

Notice, that Δ_J maps $T \cap P$ $(T \cap L)$ onto itself. Let $M = M_\alpha$ be the operator of taking the neighbour of colour α in the graph $D^\pi(2n, \mathbb{K})$. We assume that $M^T_\alpha(v) = v$ if v is an absolute point in the polarity graph. We denote by M'_α the operator $\Delta_J^{-1} M_\alpha \Delta_J$ of taking the neighbour in ${CD'}^\pi_J(2n, \mathbb{K})$. In particular, we introduce the operator M'_α for the graph ${CD'}^\pi(2n, \mathbb{K})$.

Pobrane z czasopisma Annales AI- Informatica **http://ai.annales.umcs.pl**
Data: 01/03/2026 17:37:22

5 On Graph Based Families of Stable Maps of Increasing Order

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

$$(p)^{2k-2} = (p_{0,1}, p_{1,1}, p_{1,2}, p_{2,1}, p_{2,2}, p'_{2,2}, p_{2,3}, \ldots, p_{i,i}, p'_{i,i}, p_{i,i+1}, p_{i+1,i}, \ldots) , \quad (11)$$

of a kind

$$[l]^{2k-1} = [\beta_k, l_{1,1}, l_{1,2}, l_{2,1}, l_{2,2}, l'_{2,2}, l_{2,3}, \ldots, l_{i,i}, l'_{i,i}, l_{i,i+1}, l_{i+1,i}, \ldots] , \quad (12)$$

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 $l'_{i,i}$ for $i = 2, 3, \ldots$ are computed using the equation describing a connected component.

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

$$[l]^{2k-1} = [l_{1,0}, l_{1,1}, l_{1,2}, l_{2,1}, l_{2,2}, \ldots, l_{i,i}, l_{i,i+1}, l'_{i,i}, l_{i+1,i}, \ldots] , \quad (13)$$

of a kind

$$(p)^{2k} = (p_{0,1}^{2k-2} + \alpha_k, p_{1,1}, p_{1,2}, p_{2,1}, p_{2,2}, \ldots, p_{i,i}, p'_{i,i}, p_{i,i+1}, p_{i+1,i}, \ldots) , \quad (14)$$

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 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:

$$(p)^0 = (p_{0,1}, p_{1,1}, p_{1,2}, p_{2,1}, p_{2,2}, p'_{2,2}, p_{2,3}, \ldots, p_{i,i}, p'_{i,i}, p_{i,i+1}, p_{i+1,i}, \ldots) , \quad (15)$$

(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 $\mathbb{K}^k$ and the composition:

$$F_{n,\alpha,\beta} = L_{D,n,\beta_1} P_{D,n,\alpha_1} L_{D,n,\beta_2} P_{D,n,\alpha_2} \ldots L_{D,n,\beta_k} P_{D,n,\alpha_k} . \quad (16)$$

Let us consider the restriction F' of $F_{n,\alpha,\beta}$ onto the graph $CD(n, \mathbb{K})$ which contains all v, such that $a_2(v) = b_1, a_3(v) = b_2, \ldots$. It is clear that $F'' = \Delta^{-1} F' \Delta$ is an operator on the vertices of $CD'(n, \mathbb{K})$

Theorem 2. ([**38**], [**39**]) Independently of the choice of $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_k) \in \mathbb{K}^k$ and $\beta = (\beta_1, \beta_2, \ldots, \beta_k) \in \mathbb{K}^k$, the map $F'' = F''_{n,\alpha,\beta}$ of free module $\mathbb{K}^{n - \lfloor \frac{n+2}{4} \rfloor}$ of points for the graph $CD'(n, \mathbb{K})$ is bijective map with degree $\lfloor \frac{n+2}{4} \rfloor$. □

Corollary 2. The maps $F''_{n,\alpha,\beta}$, $n = 2, 3, \ldots$ form a family of stable maps of unbounded degree. □

Let us consider the restriction F'_J of F onto the graph $CD_J(n, \mathbb{K})$, $J = \{j_1, j_2, \ldots, j_s\}$, $2 \leq j_1 \leq j_2 \leq \ldots j_s \leq t(n)$. Let $F''_J = {\Delta_J}^{-1} F'_J \Delta_j$.

Corollary 3. The map $F''_{J\,n,\alpha,\beta}$ is a transformation of the point set $\mathbb{K}^{n-J}$ for $CD'_J(n, \mathbb{K})$ of the degree J. □

Pobrane z czasopisma Annales AI- Informatica **http://ai.annales.umcs.pl**
Data: 01/03/2026 17:37:22

Let $\mathbb{K}$ denote a commutative ring. The set Q of the ring $\mathbb{K}$ is **the multiplicative set** of ring $\mathbb{K}$, if it is closed under operation of multiplication ($x, y \in Q \Rightarrow x \cdot y \in Q$) and does not contain 0.

The following statement follows instantly from the results [**32**], [**33**].

Theorem 3. Let Q be a multiplicative subset of $\mathbb{K}$. If each $\alpha_i \in Q$, $i \in Q$ and $\beta_i - \beta_{i+1} \in Q$, $i = 1, 2, \ldots, k-1$ and $\beta_1 - \beta_k \in Q$. Then the order of $F''_{J\,n,\alpha,\beta}$ is going to ∞ when $n \to \infty$ and arbitrary J. □

The following statement is announced in [**38**] (it is proven in [**39**]).

Proposition 5. Let $F''_J(n, \mathbb{K})$ correspond to the strings $\alpha_1, \alpha_2, \ldots \alpha_k$ and $\beta_1, \beta_2, \ldots, \beta_k$, where k is an independent constant. Let us assume that this map is written in standard form $x_i \to F_i(x_1, x_2, \ldots, x_n)$, $i = 1, 2, \ldots, n$. Then density of each multivariate polynomial F_i is $O(n^3)$

From the statements of this section immediately follows

Corollary 4. The maps $F''_J(n, \mathbb{K})$ for $|J| \geq cn$, where c is an independent constant, satisfying conditions of previous statement form a family of stable maps of the unbounded degree and unbounded order with invertible decomposition and polynomial density. □

The following statement was proved in [**37**]

Proposition 6. Let $N_\alpha(v)$ ($N^J_\alpha(v)$) be an operator of taking a neighbour of vertex v of the graph $D(n, K)$ ($CD'^J(n, K)$, respectively) with the colour $\rho(v) + \alpha$. For each sequence $\alpha_1, \alpha_2, \ldots, \alpha_k$ such that $\alpha_i \neq \alpha_{i+1}$, $i = 1, 2, \ldots, k-1$ the transformation $N_{\alpha_1} N_{\alpha_2}, \ldots, N_{\alpha_k}$ is a cubical map.

The following statements can be deduced from theorem 2 and its corollaries.

Theorem 4. The transformation $G_J(n, k) = N^J_{\alpha_1} N^J_{\alpha_2}, \ldots, N^J_{\alpha_k}$ is a stable map of the degree $O(n)$ of polynomial density with invertible decomposition. If cardinality of J is an independent constant, then the degree of $G_J(n, \mathbb{K})$ is also bounded by the constant, which is independent of n. □

Remark 3. The inverse map for $G_J(n, \mathbb{K})$ is the transformation $G_J(n, k) = N^J_{-\alpha_k} N^J_{-\alpha_{k-1}} \ldots N^J_{-\alpha_k}$.

The following statement is formulated in [**32**], [**33**].

Theorem 5. Let Q be the multiplicative set of a ring $\mathbb{K}$. Let us assume that $\alpha_i + \alpha_{i+1} \in Q$ for $i = 1, 2, \ldots, k-1$ and $\alpha_1 + \alpha_k \in Q$. Then the order of transformation $G_J(n, k) = N^J_{\alpha_1} N^J_{\alpha_2} \ldots N^J_{\alpha_k}$ increases to infinity with the increase of integer n. □

Pobrane z czasopisma Annales AI- Informatica **http://ai.annales.umcs.pl**
Data: 01/03/2026 17:37:22

5.1 Description of Special Maps given by the Pass in the Non-bipartite Graph

Let us use the automorphism π of the graph $D(n,\mathbb{K})$ (n is even) given in the previous section to define the polarity graph

Let us define the operators $N_{D,n,\gamma}$ and $M_{D,n,y}$ in the following way:

$$\begin{aligned} N_{D,n,\gamma}((p_{0,1},p_{1,1},p_{1,2},p_{2,1},p_{2,2},p'_{2,2},p_{2,3},\ldots)) = n \\ = (p_{0,1}+\gamma, x_{1,1}, x_{1,2}, x_{2,1}, x_{2,2}, x'_{2,2}, x_{2,3},\ldots) \\ M_{D,n,y}((p_{0,1},p_{1,1},p_{1,2},p_{2,1},p_{2,2},p'_{2,2},p_{2,3},\ldots)) = \\ = (y, x_{1,1}, x_{1,2}, x_{2,1}, x_{2,2}, x'_{2,2}, x_{2,3},\ldots) \end{aligned} \tag{17}$$

where the parameters $x_{1,1}, x_{1,2}, x_{2,1}, x_{2,2}, x'_{2,2}, x_{2,3},\ldots$ are computed consequently from the equations in definition of a graph $D(n,\mathbb{K})$ and y is the function dependent on the first coordinate $p_{0,1}$.

Given the first vertex $(p)^{(0)} = (p_{0,1},p_{1,1},p_{1,2},p_{2,1},p_{2,2},p'_{2,2},p_{2,3},\ldots)$, we define the pass in the graph Γ^{π} with an odd length:

$$\begin{aligned} (p)^{(0)} \longrightarrow (p)^{(1)} = M_{D,n,y}((p)^{(0)}) \longrightarrow (p)^{(2)} = N_{D,n,\alpha_1}((p)^{(0)}) \longrightarrow \\ \longrightarrow (p)^{(3)} = N_{D,n,\beta_1}((p)^{(1)}) \longrightarrow (p)^{(4)} = N_{D,n,\alpha_2}((p)^{(0)}) \longrightarrow \\ \longrightarrow (p)^{(5)} = N_{D,n,\beta_2}((p)^{(1)}) \longrightarrow \ldots \\ \longrightarrow (p)^{(2k)} = N_{D,n,\alpha_k}((p)^{(0)}) \longrightarrow (p)^{(2k+1)} = N_{D,n,\beta_k}((p)^{(1)}). \end{aligned} \tag{18}$$

Let $H = H(n,\alpha_1,\alpha_2,\ldots\alpha_k,\beta_1,\beta_2,\ldots,\beta_k,\mathbb{K})$ be the transformation, which maps the starting point of the above written walk to its final point.

Let $T = T_n(\mathbb{K},J,\alpha_1,\alpha_2,\ldots,\alpha_s)$ be the subset of all points p of $D(n,\mathbb{K})$ satisfying the conditions $a_{j_1}(v) = a_i$, $a_i \in K$, $i = 1,2,\ldots,s$. Δ is the compression map of T onto the set of points for $CD'(n,\mathbb{K})$, which is the set of vertices of $CD''^{\pi}(n,\mathbb{K})$. Further we restrict H onto T and consider the transformation $H' = \Delta^{-1}H\Delta$ of the variety of vertices of $CD''^{\pi}(n,\mathbb{K})$.

Theorem 6. Independently of the choice of $\alpha = (\alpha_1,\alpha_2,\ldots,\alpha_k) \in \mathbb{K}^k$ and $\beta = (\beta_1,\beta_2,\ldots,\beta_k) \in \mathbb{K}^k$, the map $H'(n,\alpha,\beta)$ of free module $\mathbb{K}^{n-\lfloor\frac{n+2}{4}\rfloor}$ of points for the graph $CD'^{\pi}(n,\mathbb{K})$ is bijective map with a degree $\lfloor\frac{n+2}{4}\rfloor$. □

From the results of the previous section we got the following statements

Theorem 7. Let Q be a multiplicative subset of $\mathbb{K}$. If each $\alpha_i \in Q$, $i \in Q$ and $\beta_i - \beta_{i+1} \in Q$, $i = 1,2,\ldots,k-1$ and $\beta_1 - \beta_k \in Q$. Then the order of $H'_J(n,\alpha,\beta)$ goes to ∞ when $n \to \infty$ and arbitrary J. □

Proposition 7. Let $H'_J(n,\mathbb{K})$ correspond to the strings $\alpha_1,\alpha_2,\ldots\alpha_k$ and $\beta_1,\beta_2,\ldots,\beta_k$, where k is an independent constant. Let us assume that this map is

Pobrane z czasopisma Annales AI- Informatica **http://ai.annales.umcs.pl**
Data: 01/03/2026 17:37:22

written in the standard form $x_i \to F_i(x_1, x_2, \ldots, x_n)$, $i = 1, 2, \ldots, n$. Then density of each multivariate polynomial F_i is $O(n^3)$.

Notice, that the inverse map for $H'_J(n, \mathbb{K})$ corresponds to the reverse walk in the polarity graph.

Corollary 5. The maps $H'_J(n, \mathbb{K})$ for $|J| \geq cn$, where c is an independent constant, satisfying conditions of the previous statement from a family of stable maps of unbounded degree and unbounded order with invertible decomposition and polynomial density. □

Let $M_\alpha(v)$ $(M^J_\alpha(v))$, $\alpha \neq 0$ be an operator of taking neighbour of vertex v of the graph $RD(2n, \mathbb{K})$ $(RD'^J(2n, \mathbb{K})$, respectively) with the colour $\rho(v) + \alpha$. For each sequence $\alpha_1, \alpha_2, \ldots, \alpha_k$ such that $\alpha_i \neq \alpha_{i+1}$, $i = 1, 2, \ldots, k-1$, the transformation $M^J_{\alpha_1} M^J_{\alpha_2} \ldots M^J_{\alpha_k}$ is a cubical map.

Theorem 8. The transformation $S_J(n, k) = M^J_{\alpha_1} M^J_{\alpha_2}, \ldots, M^J_{\alpha_k}$ is a stable map of the degree $O(n)$ of polynomial density with invertible decomposition. If cardinality of J is an independent constant, then the degree of $S_J(n, \mathbb{K})$ is also bounded by the constant which is independent of n. □

Remark 4. The inverse map for $S_J(n, \mathbb{K})$ is the transformation $S_J(n, k) = M^J_{-\alpha_k} M^J_{-\alpha_{k-1}} \ldots M^J_{-\alpha_1}$.

Theorem 9. Let Q be a multiplicative subset of K. If each $\alpha_i \in Q$, $i \in Q$ and $\beta_i - \beta_{i+1} \in Q$, $i = 1, 2, \ldots, k-1$ and $\beta_1 - \beta_k \in Q$. Then the order of $S'_J(n, \alpha, \beta)$ is going to ∞ when $n \to \infty$ and arbitrary J. □

Corollary 6. The maps $S'_J(n, \mathbb{K})$ for $|J| \geq cn$, where c is an independent constant, satisfying the conditions of the previous statement from a family of stable maps of unbounded degree and unbounded order with invertible decomposition and polynomial density. □

6 An Example with Complexity Estimates

Let us consider the cryptosystem based on the family of stable maps of the increasing order based on the polarity graph $D^\pi(2n, \mathbb{K})$. The advantage of this example in comparison with $D(n, \mathbb{K})$ based encryption is the absence of vertex transitive or edge transitive automorphism group for the graph. Notice that the vertex set (the plainspace) is $\mathbb{K}^{2n}$. If x and y are a pair of vertices such that x is an absolute point and y is not, then there is no group automorphism which shifts x onto y. These facts do not allow the usage of the group theoretical technique for cryptanalysis of related cryptosystem.

Pobrane z czasopisma Annales AI- Informatica **http://ai.annales.umcs.pl**
Data: 01/03/2026 17:37:22

The key holder Alice choses the multiplicative subset Q of the ring $\mathbb{K}$ and the sequences $\alpha_1, \alpha_2, \ldots, \alpha_k$, $\alpha_i \in Q$ and $\beta_1, \beta_2, \ldots, \beta_k$, $\beta_i \in Q$, such that $\beta_i - \beta_{i+1} \in Q$ for $i = 1, 2, \ldots, k-1$, where k is an independent of n constant. She chooses the parameters $d_2, d_3, \ldots, d_{[(n+1)/2]+1}$ to work with the vertices v satisfying the equations $a_2(\mathrm{v}) = d_2, a_3(\mathrm{v}) = d_3, \ldots, a_{[(n+1)/2]+1}(\mathrm{v}) = d_{[(n+1)/2]+1}$ to make the compression of this block for the equivalence relation τ.

She generates the map H' on $\mathbb{K}^{2n-[(n+1)/2]}$ described in the previous section in the standard form:

$$\begin{aligned} x_1 &\to f_1(x_1, x_2, \ldots, x_d) \\ x_2 &\to f_2(x_1, x_2, \ldots, x_d) \\ &\ldots \\ x_d &\to f_d(x_1, x_2, \ldots, x_d) \end{aligned} \tag{19}$$

where $d = 2n - [(n+1)/2]$.

The time of generation of H' is comparable with that of stable map related to $D(2n, \mathbb{K})$ (see tables with the time estimates in [4]). Alice takes the monomial transformation τ_1 of the kind $x_i \to l_i x_i$, where l_i are regular elements of the ring for $i = 1, 2, \ldots, d$ and the invertible affine transformation $\mathrm{x} \to \mathrm{x}A + \mathrm{b}$, where A is the matrix of invertible affine transformation of $\mathbb{K}^d$ and b is a chosen vector.

She forms the composition $G = \tau_1 H' \tau_2$ in the standard form:

$$\begin{aligned} x_1 &\to g_1(x_1, x_2, \ldots, x_d) \\ x_2 &\to g_2(x_1, x_2, \ldots, x_d) \\ &\ldots \\ x_d &\to g_d(x_1, x_2, \ldots, x_d)\ . \end{aligned} \tag{20}$$

Notice that the total number of monomial expressions in f_i, $i = 1, 2, \ldots, d$ is $O(n^4)$. The linear transformation τ_1 does not change the number of monomials. The composition with the affine transformation τ_2 from the right can increase the total number of transformations in n times. So, the total number of monomials from all g_i can be estimated as $O(n^5)$. It means that the computation of value of G in a given point x can be done in the polynomial time. Thus, Alice may present the map G for the public user (Bob). Each monomial costs $O(n)$ elementary operations to compute.

So, Bob may compute the value of the public rule in time $O(n^6)$.

Notice, that Alice may use the decomposition of H' of the kind:

$$N_{\beta_1} N_{x_{1,0}+\alpha_1} N_{\beta_2} N_{x_{1,0}+\alpha_1+\alpha_2} \ldots N_{\beta_k} N_{x_{1,0}+\alpha_1+\alpha_2+\cdots+\alpha_k} \tag{21}$$

and compute the inverse walks corresponding to N^{-1} for the time $O(n)$.

Pobrane z czasopisma Annales AI- Informatica **http://ai.annales.umcs.pl**
Data: 01/03/2026 17:37:22

Literatura

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

[2] Ding J., Gower J. E., Schmidt D. S., Multivariate Public Key Cryptosystems, Springer, Advances in Information Security, 25 (2006).

[3] Kim Jon-Lark, 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): 2378–2388.

[4] Klisowski M., Ustimenko V. A., On the Comparison of Cryptographical Properties of Two Different Families of Graphs with Large Cycle Indicator, Mathematics in Computer Science, 6(2) (2012): 181–198.

[5] Koblitz N., Algebraic aspects of cryptography, Algorithms and Computation in Mathematics, 3, Springer (1998).

[6] Kotorowicz J. S., Ustimenko V., On the properties of stream ciphers based on extremal directed graphs, Cryptography Research Perspective (Roland E. Chen, ed.), Nova Science Publishers, April (2009): 125–141.

[7] Kotorowicz, S., Ustimenko V., On the implementation of cryptoalgorithms based on algebraic graphs over some commutative rings, Condens. Matter Phys. 11, 2(54) (2008): 347–360.

[8] Kotorowicz J. S., Ustimenko V., Romaúczk U., On the implementation of stream ciphers based on a new family of algebraic graphs, IEEE Computer Society Press, Proceedings of the Conference CANA, FedSCIS (2011): 485–490.

[9] Lubotsky A., Philips R., Sarnak P., Ramanujan graphs, J. Comb. Theory., 115(2) (1989): 62–89.

[10] Lazebnik F., Ustimenko V., Explicit construction of graphs with an arbitrary large girth and of large size, Discrete Appl. Math., 60 (1995): 275–284.

[11] Lazebnik F., Ustimenko V. A., Woldar A. J., New Series of Dense Graphs of High Girth, Bull (New Series) of AMS, 32(1) (1995): 73–79.

[12] Lazebnik F., Ustimenko V. A., Woldar A. J., A Characterization of the Components of the graphs $D(k, q)$, Discrete Mathematics, 157 (1996): 271–283.

[13] Lazebnik F., Ustimenko V. A., Woldar A. J., Polarities of 2k-cycle-free graphs, Discrete Mathematics, 197/198 (1999): 503–513.

[14] Margulis G. A., Explicit construction of graphs without short cycles and low density codes, Combinatorica, 2 (1982): 71–78.

[15] Moore E. H., Tactical Memoranda, Amer. J. Math., 18 (1886): 264–303.

[16] Romańczuk U., Ustimenko V.: On the key exchange with matrices of large order and graph based nonlinear maps, Proceedings of the conference Ąpplications of Computer Algebra", Vlora, Special Issue, 4(4) (2010): 203–211.

[17] Romańczuk U., Ustimenko V., On the family of cubical multivariate cryptosystems based on the algebraic graph over finite commutative rings of characteristic 2, Annales UMCS Informatica AI XII, 3 (2012): 89–106.

[18] Romańczuk U., Ustimenko V., On the key exchange with new cubical maps based on graphs, Annales UMCS Informatica, 4(11) (2011): 11–19.

[19] Romańczuk U., Ustimenko V., On regular forests given in terms of algebraic geometry, new families of expanding graphs with large girth and Multivariate cryptographical algorithms, Proceedings of International conference Ąpplications of Computer Algebra", Malaga (2013): 144–147.

[20] Romańczuk U., Ustimenko V., 0n the family of cubical multivariate cryptosystems based on exceptional extremal graphs, Third International Conference on Symbolic Computations and Cryptography, Castro Urdiales, Extended Abstracts, (2012): 169–175.

[21] Ustimenko V., Coordinatisation of Trees and their Quotients, In the "Voronoj's Impact on Modern Science", Kiev, Institute of Mathematics, 2 (1998): 125–152.

[22] Ustimenko V., CRYPTIM: Graphs as Tools for Symmetric Encryption, in Lecture Notes in Computer Science, Springer, 2227 (2001): 278–287.

Pobrane z czasopisma Annales AI- Informatica **http://ai.annales.umcs.pl**
Data: 01/03/2026 17:37:22

[23] Ustimenko V., Graphs with Special Arcs and Cryptography, Acta Applicandae Mathematicae, 74(2) (2001): 117–153.

[24] Ustimenko V., Maximality of affine group and hidden graph cryptosystems, J. Algebra Discrete Math., 1 (2005): 133–150.

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

[26] Ustimenko V., Schubert cells in Lie geometries and key exchange via symbolic computations, Proceedings of the International Conference Ąpplications of Computer Algebra", Vlora, Albanian Journal of Mathematics, Special Issue, 4(4) (2010): 135–145.

[27] 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): 181–200.

[28] Ustimenko V., Linguistic Dynamical Systems, Graphs of Large Girth and Cryptography, Journal of Mathematical Sciences, Springer, 140(3) (2007): 412–434.

[29] 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 (2007).

[30] Ustimenko V., Algebraic groups and small world graphs of high girth, Albanian J. Math. 3(1) (2009): 25–33.

[31] Ustimenko V., On extremal graph theory and symbolic computations Dopovidi National Academy of Sci of Ukraine, (in Russian), 2 (2013): 42–49.

[32] Ustimenko V., In the K - theory of graph based dynamical systems and its applications, Dopovidi National Academy of Sci of Ukraine, 8 (2013): 44–51.

[33] Ustimenko V., Romańczuk U., On Dynamical Systems of Large Girth or Cycle Indicator and their applications to Multivariate Cryptography, Artificial Intelligence, Evolutionary Computing and Metaheuristics, In the footsteps of Alan Turing Series: Studies in Computational Intelligence, Springer, 427 (2013): 257–285.

[34] Ustimenko V., Romańczuk U., On Extremal Graph Theory, Explicit Algebraic Constructions of Extremal Graphs and Corresponding Turing Encryption Machines, Artificial Intelligence, Evolutionary Computing and Metaheuristics, In the footsteps of Alan Turing Series: Studies in Computational Intelligence, Springer, 427 (2013): 231–256.

[35] Ustimenko V., Wróblewska A., On the key exchange with nonlinear polynomial maps of stable degree, Annalles UMCS Informatica AI XI, 2 (2011): 81–93.

[36] Ustimenko V., Wroblewska A., Dynamical systems as the main instrument for the constructions of new quadratic families and their usage in cryptography, Annales UMCS Informatica AI, ISSN 1732-1360.

[37] Wróblewska A., On some properties of graph based public keys, Albanian Journal of Mathematics, NATO Advanced Studies Institute: Ńew challenges in digital communications", 2(3) (2008): 229–234.

[38] Ustimenko V., Wróblewska A., On some algebraic aspects of data security in cloud computing, Proceedings of International conference Ąpplications of Computer Algebra", Malaga (2013): 144–147.

[39] Ustimenko V., Wróblewska A., On the key exchange and multivariate encryption with nonlinear polynomial maps of stable degree, Annales UMCS Informatica AI XIII, 1 (2013): 63–80.