Pobrane z czasopisma Annales AI- Informatica **http://ai.annales.umcs.pl**
Data: 30/06/2026 21:27:26

Annales UMCS Informatica AI XI, 2 (2011)
127–141; DOI: 10.2478/v10065-011-0007-6

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

The implementation of cubic public keys based on a new family of algebraic graphs

Michał Klisowski[1*], Urszula Romańczuk[1,2†], Vasyl Ustimenko[1,2‡]

[1] *Institute of Mathematics, Maria Curie-Sklodowska University, pl. M. Curie-Sklodowskiej 1, 20-031 Lublin, Poland*
[2] *Research supported by the project "Human - The Best Investment". The project is co-funded from the sources of the European Union within the European Social Fund*

Abstract

Families of edge transitive algebraic graphs defined over finite commutative rings were used for the development of stream ciphers, public key cryptosystems and key exchange protocols. We present the results of the first implementation of a public key algorithm based on the family of algebraic graphs, which are not edge transitive. The absence of an edge transitive group of symmetries means that the algorithm can not be described in group theoretical terms. We hope that it licates cryptanalysis of the algorithm. We discuss the connections between the security of algorithms and the discrete logarithm problem.

The plainspace of the algorithm is K^n, where K is the chosen commutative ring. The graph theoretical encryption corresponds to walk on the bipartite graph with the partition sets which are isomorphic to K^n. We conjugate the chosen graph based encryption map, which is a composition of several elementary cubical polynomial automorphisms of a free module K^n with special invertible affine transformation of K^n. Finally we compute symbolically the

[*] *E-mail address: mklisow@hektor.umcs.lublin.pl*
[†] *E-mail address: urszula_romanczuk@yahoo.pl*
[‡] *E-mail address: vasyl@hektor.umcs.lublin.pl*

Pobrane z czasopisma Annales AI- Informatica **http://ai.annales.umcs.pl**
Data: 30/06/2026 21:27:26

corresponding cubic public map g of K^n onto K^n. We evaluate time for the generation of g, and the number of monomial expression in the list of corresponding public rules.

1. Introduction

We implement the algorithm proposed in [**1**]. It is based on the family of graphs $A(n, K)$ which were introduced in [**2**]. The paper [**1**] discusses properties of the family of graphs related to the performance of the algorithm.

In publications [**3**], [**4**] some implementations of stream ciphers and public key algorithms based on an explicit construction of families of algebraic graphs $D(n, q)$ of large girth and their analogs $D(n, K)$ over the commutative ring K were discussed. It was shown that for each finite commutative ring K we can create a cubical polynomial map f of K^n onto K^n depending on a string of regular elements (non zero divisors $(\alpha_1\alpha_2, \ldots, \alpha_t)$ (password). If $t \leq (n+5)/2$ then different strings produce different ciphertexts. One can use such a map as a stream cipher. It is possible to combine f with two invertible sparse affine transformations τ_1 and τ_2 and use the composition $g = \tau_1 f \tau_2$ as a public rule. A public user is not able to decrypt τ_1, τ_2 without knowledge and the string $(\alpha_1\alpha_2, \ldots, \alpha_t)$.

One can set τ_2 as the inverse of τ_1 and use the "symbolic" generator g and the related cyclic group for the Diffie–Hellman key exchange protocol. The girth of graphs $D(n, q)$ grows with the growth of n It means that the order of g with $\tau_2 = {\tau_1}^{-1}$ grows as a function depending on n. Evaluation of the girth for $D(n, q)$ allows to prove that this is a family of graphs of large girth. Different properties of this family are investigated in [**5**], [**6**], [**7**], [**8**], [**9**], [**10**]. Families of graphs of large girth are an important instrument in Extremal Graph Theory dealing with classical problems of Turan type on the studies of the maximal size of simple graphs without prohibited cycles. Such problems are attractive for mathematicians because they are beautiful and difficult (see [**11**], [**12**]). Applications of these problems in Networking [**13**], Coding Theory and Cryptography (see [**7**] and further references) may attract the attention of Computer Scientists.

In this paper we use in a similar manner another family of graphs ($A(n, K)$, where K is one which is the collection of not edge transitive graphs). In the case $K = F_q$ a new family is a family of graphs of increasing girth (see [**1**]). Computer simulations support the conjectures that the graphs $A(n, q)$ form a family of large girth, but the absence of an edge transitive automorphism group complicates theoretical evaluation of the growth of girth with the growth of the parameter n. Computer simulations allow to conjecture that the graphs

Pobrane z czasopisma Annales AI- Informatica **http://ai.annales.umcs.pl**
Data: 30/06/2026 21:27:26

$A(n, K)$ have an advantage over $D(n, K)$ [**1**]. For instance, the graphs $A(n, Z_n)$ and $A(n, q)$ are connected contrary to $D(n, K)$.

Section 2 is devoted to the concept of the girth indicator and the family of large girth for digraphs.

In Section 3 we consider the definition of a family of affine algebraic digraphs of increasing girth over commutative rings with special colouring of arrows. Explicit constructions of such families of graphs can be used for the development of public key cryptosystems and key exchange protocols. We discuss the connection of these algorithms with the group theoretical discrete logarithm problem.

In section 4 we use the graphs $A(n, K)$ for the construction of a family of affine algebraic digraphs with the increasing girth indicator with the colouring as in section 3.

Section 5 is devoted to the latest implementation of the public key algorithm based on one of the families described in section 4.

In section 6 we discuss the execution of the decryption procedure for the key holder (Alice) and compare the cases of $A(n, K)$ and $D(n, K)$ based algorithms.

2. The families of directed graphs of large girth

The missing theoretical definitions of directed graphs can be found in [**14**]. Let ϕ be an irreflexive binary relation over the set V, i.e., $\phi \in V \times V$ and for each v the pair (v, v) is not the element of ϕ.

We say that u is the neighbour of v and write $v \to u$ if $(v, u) \in \phi$. We use the term *balanced binary relation graph* for the graph Γ of an irreflexive binary relation ϕ over a finite set V such that for each $v \in V$ the sets $\{x|(x, v) \in \phi\}$ and $\{x|(v, x) \in \phi\}$ have the same cardinality. It is a directed graph without loops and multiple edges. We say that a balanced graph Γ is k-regular if for each vertex $v \in \Gamma$ the cardinality of $\{x|(v, x) \in \phi\}$ is k.

Let Γ be the graph of binary relation. The *path* between the vertices a and b is the sequence $a = x_0 \to x_1 \to \cdots \to x_s = b$ of the length s, where x_i, $i = 0, 1, \ldots s$ are distinct vertices.

We say that the pair of paths $a = x_0 \to x_1 \to \cdots \to x_s = b$, $s \geq 1$ and $a = y_0 \to y_1 \to \cdots \to y_t = b$, $t \geq 1$ form an (s, t)- commutative diagram $O_{s,t}$ if $x_i \neq y_j$ for $0 < i < s$, $0 < j < t$. Without loss of generality we assume that $s \geq t$.

We refer to the number $\max(s, t)$ as the rank of $O_{s,t}$. It is ≥ 2, because the graph does not contain multiple edges.

Pobrane z czasopisma Annales AI- Informatica **http://ai.annales.umcs.pl**
Data: 30/06/2026 21:27:26

Notice that the graph of antireflexive binary relation may have a directed cycle $O_s = O_{s,0}$: $v_0 \to v_1 \to \cdots \to v_{s-1} \to v_0$, where v_i, $i = 0, 1, \ldots, s-1$, $s \geq 2$ are distinct vertices.

We will count directed cycles as commutative diagrams.

For the investigation of commutative diagrams we introduce *girth indicator* gi, which is the minimal value for $\max(s,t)$ for the parameters s, t of a commutative diagram $O_{s,t}$, $s+t \geq 3$. The minimum is taken over all pairs of vertices (a, b) in the digraph. Notice that two vertices v and u at the distance $<$ gi are connected by the unique path from u to v of the length $<$ gi.

We assume that the *girth* $g(\Gamma)$ of a directed graph Γ with the girth indicator $d+1$ is $2d+1$ if it contains a commutative diagram $O_{d+1,d}$. If there are no such diagrams we assume that $g(\Gamma)$ is $2d+2$.

In the case of a symmetric binary relation gi $= d$ implies that the girth of the graph is $2d$ or $2d-1$. It does not contain an even cycle $2d-2$. In a general case gi $= d$ implies that $g \geq d+1$. So in the case of the family of graphs with an unbounded girth indicator, the girth is also unbounded. We also have gi $\geq g/2$.

In the case of symmetric irreflexive relations the above mentioned general definition of the girth agrees with the standard definition of the girth of simple graph, i.e., the length of its minimal cycle.

We will use the term *the family of graphs of large girth* for the family of balanced directed regular graphs Γ_i of degree k_i and order v_i such that gi(Γ_i) is $\geq c\log_{k_i} v_i$, where c' is a constant independent of i.

As it follows from the definition $g(\Gamma_i) \geq c'\log_{k_i}(v_i)$ for an appropriate constant c'. So, it agrees with the well known definition for the case of simple graphs.

The diameter of the strongly connected digraph [**14**] is the minimal length d of the shortest directed path $a = x_0 \to x_1 \to x_2 \cdots \to x_d$ between two vertices a and b. Recall that a graph is k-regular, if each vertex of G has exactly k outputs. Let F be the infinite family of k_i regular graphs G_i of the order v_i and the diameter d_i. We say that F is a family of small world graphs if $d_i \leq C\log_{k_i}(v_i)$, $i = 1, 2, \ldots$ for some constant C independent of i. The definition of small world simple graphs and the related explicit constructions can be found in [**15**]. For the studies of small world simple graphs without small cycles see [**12**], [**8**].

3. The K-theory of affine graphs with the increasing girth indicator and its cryptographical motivations

We use here the concepts of [**16**], where reader can find additional examples of affine graphs over rings or fields.

Pobrane z czasopisma Annales AI- Informatica **http://ai.annales.umcs.pl**
Data: 30/06/2026 21:27:26

Let K be a commutative ring. A *directed algebraic graph* ϕ over K consists of two things, such as the *vertex set* Q being a quasiprojective variety over K of nonzero dimension and the *edge set* being a quasiprojective variety ϕ in $Q \times Q$. We assume that ($x\phi y$ means $(x, y) \in \phi$).

The graph ϕ is *balanced* if for each vertex $v \in Q$ the sets $\mathrm{Im}(v) = \{x \mid v\phi x\}$ and $\mathrm{Out}(v) = \{x \mid x\phi v\}$ are quasiprojective varieties over K of the same dimension.

The graph ϕ is *homogeneous* (or (r, s)-homogeneous) if for each vertex $v \in Q$ the sets $\mathrm{Im}(v) = \{x|v\phi x\}$ and $\mathrm{Out}(v) = \{x|x\phi v\}$ are quasiprojective varieties over F of fixed nonzero dimensions r and s, respectively.

In the case of *balanced homogeneous algebraic graphs* for which $r = s$ we will use the term r-homogeneous graph. Finally, *regular algebraic graph* is a balanced homogeneous algebraic graph over the ring K if each pair of vertices v_1 and v_2 is a pair of isomorphic algebraic varieties.

Let $\mathrm{Reg}(K)$ be the totality of regular elements (or nonzero divisors) of K, i.e., nonzero elements $x \in K$ such that for each nonzero $y \in K$ the product xy is different from 0. We assume that the $\mathrm{Reg}(K)$ contains at least 3 elements. We assume here that K is finite, thus the vertex set and the edge set are finite and we get a usual finite directed graph.

We apply the term *affine graph* for the regular algebraic graph such that its vertex set is an affine variety in the Zariski topology.

Let G be a r-regular affine graph with the vertex $V(G)$, such that Out v, $v \in V(G)$ is isomorphic to the variety $R(K)$. Let the variety $E(G)$ be its arrow set (a binary relation in $V(G) \times V(G)$). We use the standard term *perfect algebraic colouring of edges* for the polynomial map ρ from $E(G)$ onto the set $R(K)$ (the set of colours) if for each vertex v different output arrows $e_1 \in \mathrm{Out}(v)$ and $e_2 \in \mathrm{Out}(v)$ have distinct colours $\rho(e_1)$ and $\rho(e_2)$ and the operator $N_\alpha(v)$ of taking the neighbour u of vertex v ($v \to u$) is a polynomial map of the variety $V(G)$ into itself.

We will use the term *rainbow-like colouring* in the case when the perfect algebraic colouring is a bijection. Let $\mathrm{dirg}(G)$ be a directed girth of the graph G, i.e., the minimal length of a directed cycle in the graph. Obviously $\mathrm{gi}(G) \leq \mathrm{dirg}(G)$.

Studies of infinite families of directed affine algebraic digraphs over commutative rings K of large girth with the rainbow-like colouring is a nice and difficult mathematical problem. Good news is that such families do exist. In the next section we consider the example of such a family for each commutative ring with more than 2 regular elements.

Pobrane z czasopisma Annales AI- Informatica **http://ai.annales.umcs.pl**
Data: 30/06/2026 21:27:26

Here, at the end of section, we consider cryptographic motivations for studies of such families.

1) Let G be a finite group and $g \in G$. The discrete logarithm problem for group G is finding a solution for the equation $g^x = b$ where x is an unknown positive number. If the order $|g| = n$ is known we can replace G on a cyclic group C_n. So we may assume that the order of g is sufficiently large to make the computation of n unfeasible. For many finite groups the discrete logarithm problem is NP complete (see [**17**], [**18**]).

Let K be a finite commutative ring and M be an affine variety over K. Then the Cremona group $C(M)$ of whole polynomial automorphism of the variety M can be large. For example, if K is a finite prime field F_p and $M = {F_p}^n$ then $C(M)$ is a symmetric group S_{p^n}.

Let us consider the family of affine graphs $G_i(K)$, $i = 1, 2, \ldots$ with the rainbow-like algebraic colouring of edges such that $V(G_i(K)) = V_i(K)$, where K is a commutative ring, and the colour sets are algebraic varieties $R_i(K)$. Let us choose a constant k. The operator $N_\alpha(v)$ of taking the neighbour of a vertex v corresponding to the output arrow of colour α are the elements of $C_i = C(V_i(K))$. We can choose a relatively small number k to generate $h = h_i = N_{\alpha_1} N_{\alpha_2} \ldots N_{\alpha_k}$ in each group C_i, $i = 1, 2, \ldots$

Let us assume that the family of graphs $G_i(K)$ is the family of graphs of increasing girth. It means that the girth indicator $\mathrm{gi}_i = \mathrm{gi}(G_i(K))$ and the parameter $\mathrm{dirg}_i = \mathrm{dirg}(G_i(K))$ grow with the growth of i. Notice that $|h_i|$ is bounded below by dirg_i/k. So there is j such that for $i \geq j$ the computation of $|h_i|$ is impossible. In fact, the fastest growth of girth indicator will be in the case of family of large girth. Finally we can take the base $g = u^{-1} h_j u$ where u is a chosen element of C_j to hide the graph up to conjugation. We may use some package of symbolic computations to express the polynomial map g via the list of polynomials in many unknowns. For example, if $V_j(K)$ is a free module K^n then we can write g in a public mode fashion

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

The symbolic map g can be used for Diffie—Hellman *key exchange protocol* (see [**15**] for the details). Let Alice and Bob be correspondents. Alice computes the symbolic map g and sends it to Bob via an open channel. So the variety and the map are known for the adversary (Cezar).

Let Alice and Bob choose the natural numbers n_A and n_B, respectively.

Bob computes g^{n_B} and sends it to Alice, who computes $(g^{n_B})^{n_A}$, while Alice computes g^{n_A} and sends it to Bob, who is getting $(g^{n_A})^{n_B}$. The common secret information is $g^{n_A n_B}$ given in a "public mode fashion".

Pobrane z czasopisma Annales AI- Informatica **http://ai.annales.umcs.pl**
Data: 30/06/2026 21:27:26

Bob can be just a public user (no information about the way in which the map g was cooked), so he and Cezar are making computations much more slowly than Alice who has the decomposition $g = u^{-1}N_{\alpha_1}N_{\alpha_2}\dots N_{\alpha_k}u$.

We may modify slightly the Diffie - Hellman protocol using the action of the group on the variety. Alice chooses a rather short password $\alpha_1, \alpha_2, \dots, \alpha_k$, computes the public rules for the encryption map g and sends them to Bob via an open channel together with some vertex $v \in V_j(K)$.

Then Alice and Bob choose the natural numbers n_A and n_B, respectively.

Bob computes $v_B = g^{n_B}(v)$ and sends it openly to Alice, who computes $(g^{n_A})(v_B)$, while Alice computes $v_A = g^{n_A}(v)$ and sends it to Bob, who is getting $(g^{n_B})(v_A)$.

The common information is the vertex $g^{n_A \times n_B}(v)$.

In both cases Cezar has to solve one of the equations $E^{n_B}(u_A) = z$ or $E^{n_A}(u_B) = w$ for the unknowns n_B or n_A, where z and w are known points of the variety.

2) We can construct the *public key* map in the following manner:

The key holder (Alice) chooses the variety $V_j(K)$ and the sequence $\alpha_1, \alpha_2, \dots, \alpha_t$ of the length $t = t(j)$ to determine the encryption map g as above. Let $\dim(V_j(K)) = n = n(j)$ and each element of the variety be determined by independent parameters $x_1, x_2, \dots, x_n$. Alice presents the map in the form of public rules, such as

$x_1 \to f_1(x_1, x_2, \dots, x_n), x_2 \to f_2(x_1, x_2, \dots, x_n), \dots, x_n \to f_n(x_1, x_2, \dots, x_n)$.

We can assume (at least theoretically) that the public rule depending on the parameter j is applicable to the encryption of a potentially infinite text (parameter t is a linear function of j now).

For the computation she may use the Gröbner base technique or alternative methods, special packages for the symbolic computation (popular "Mathematica", "Maple" or special fast symbolic software). So Alice can use the decomposition of the encryption map into u^{-1}, maps of kind N_α and u to encrypt fast. For the decryption she can use the inverse graph $G_j(K)^{-1}$ for which $VG_j(K)^{-1} = VG_j(K)$ and the vertices w_1 and w_2 are connected by an arrow if and only if w_2 and w_1 are connected by an arrow in $G_j(K)$. Let us assume that the colours of $w_1 \to w_2$ in $G_j(K)^{-1}$ and $w_2 \to w_1$ in $G_j(K)$ are of the same colour. Let $N'_\alpha(x)$ be the operator of taking the neighbour of vertex x in $G_j(K)^{-1}$ of colour α. Then Alice can decrypt applying consequently $u^{-1}, N'_{\alpha_t}, N'_{\alpha_{t-1}}, \dots, N_{\alpha_1}$ and u to the ciphertext. So the decryption and the encryption for Alice takes the same time. She can use a numerical program to implement her symmetric algorithm.

Pobrane z czasopisma Annales AI- Informatica **http://ai.annales.umcs.pl**
Data: 30/06/2026 21:27:26

Bob can encrypt with the public rule but for a decryption he needs to invert the map. Let us consider the case $t_j = kl$, where k is a small number and the sequence $\alpha_1, \alpha_2, \ldots, \alpha_{t_j}$ has the period k and the transformation $h = u^{-1}N_{\alpha_1}N_{\alpha_2}\ldots N_{\alpha_k}u$ is known for Bob in the form of public key mode. In such a case a problem to find the inverse for g is equivalent to the discrete logarithm problem with the base h in the related Cremona group of all polynomial bijective transformations.

Of course for further cryptanalysis we need to study the information about possible divisors of order of the base of the related discrete logarithm problem, alternative methods to break the encryption. In the next section the family of digraphs $RE_n(K)$ will be described.

3) We may study the security of the private key algorithm used by Alice in the algorithm of the previous paragraph but with a parameter t bounded by the girth indicator of graph $G_j(K)$. In that case different keys produce distinct ciphertexts from the chosen plaintext. In that case we prove that if the adversary has no access to plaintexts then he can break the encryption via the brut-force search via all keys from the key space. The encryption map has no fixed points.

4. The family of affine digraph of increasing girth over commutative rings

E. Moore used the term *tactical configuration* of order (s, t) for biregular bipartite simple graphs with the bidegrees $s + 1$ and $r + 1$. It corresponds to the incidence structure with the point set P, the line set L and the 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 an 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 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 parentheses 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 $p_1 \neq p_2$.

Pobrane z czasopisma Annales AI- Informatica **http://ai.annales.umcs.pl**
Data: 30/06/2026 21:27:26

Below we consider the family of graphs $D(k, K)$, where $k > 5$ is a positive integer and K is a commutative ring. Such graphs are disconnected and their connected components were investigated in [**9**] (for the case when K is a finite field F_q see [**19**]).

Let P and L be two copies of Cartesian power K^N, where K is the commutative ring and N is the set of positive integer numbers. 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 co-ordinates of points and lines introduced in [**20**] for the case of general commutative ring K:

$$(p) = (p_{0,1}, p_{1,1}, p_{1,2}, p_{2,2}, p_{2,3}, \ldots, p_{i,i}, p_{i,i+1}, \ldots),$$
$$[l] = [l_{1,0}, l_{1,1}, l_{1,2}, l_{2,1}, l_{2,2}, l'_{2,2}, l_{2,3}, \ldots, l_{i,i}, l'_{i,i}, l_{i,i+1}, l_{i+1,i}, \ldots].$$

The elements of P and L can be thought as infinite ordered tuples of elements from K, such that only a finite number of components is different from zero.

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 co-ordinates hold:

$$l_{i,i} - p_{i,i} = l_{1,0}p_{i-1,i}$$
$$l_{i,i+1} - p_{i,i+1} = l_{i,i}p_{0,1}$$

We denote this incidence structure (P, L, I) as $A(K)$. We identify it with the bipartite *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 $(p)I[l]$.

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 with respect to the above order. The incidence I_k is then defined by imposing the first $k-1$ incidence equations and ignoring all others. The incidence graph corresponding to the structure (P_k, L_k, I_k) is denoted by $A(k, K)$.

For each positive integer $k \geq 2$ we consider the *standard* graph homomorphism ϕ_k of (P_k, L_k, I_k) onto $(P_{k-1}, L_{k-1}, I_{k-1})$ defined L_k by simply projection of each vector from P_k and L_k onto its $k-1$ initial coordinates with respect to the above order.

Let $DA_n(K)$ ($DA(K)$) be the double directed graph of the bipartite graph $A(n, K)$ ($A(K)$, respectively). Remember, that we have the arc e of kind $(l^1, p^1) \to [l^2, p^2]$ if and only if $p^1 = p^2$ and $l^1 \neq l^2$. Let us assume that the colour $\rho(e)$ of the arc e is $l^1_{1,0} - l^2_{1,0}$.

Pobrane z czasopisma Annales AI- Informatica **http://ai.annales.umcs.pl**
Data: 30/06/2026 21:27:26

Recall, that we have the arc e' of kind $[l^2, p^2] \to (l^1, p^1)$ if and only if $l^1 = l^2$ and $p^1 \neq p^2$. Let us assume that the colour $\rho(e')$ of arc e' is $p^1_{1,0} - p^2_{1,0}$. It is easy to see that ρ is perfect algebraic colouring.

If K is finite, then the cardinality of the colour set is $(|K| - 1)$. Let Reg$K$ be the totality of regular elements, i.e., not zero divisors. Let us delete all arrows with colour, which is a zero divisor. We will obtain a new graph $RA_n(K)$ $(RA(K))$ with the induced colouring into colours from the alphabet Reg(K). The vertex set for the graph $DA_n(K)$ consists of two copies F_1 and F_2 of the edge set for $A(n, K)$. It means that Group $U(n, K)$ acts regularly on each set F_i, $i = 1, 2$.

If K is finite, then the cardinality of the colour set is $(|K| - 1)$. Let Reg$K$ be the totality of regular elements, i.e., non-zero divisors. Let us delete all arrows with colour which is a zero divisor. We can show that a new infinite affine graph $A(K)$ does not contain cycles (see [**1**]). It means that the directed graph $RA(K)$ does not contain commutative diagrams and the digraphs $RA_n(K)$ form a family of digraphs with the increasing girth indicator. In fact computer simulations support the following assumption.

CONJECTURE: The graphs $RA_n(K)$ form a family of digraphs of large girth.

5. The implementation of the public key algorithm based on $RA_t(K)$

The set of vertices of the graph $RA_n(K)$ is a union of two copies of the free module K^{n+1}. So the Cremona group of the variety is the direct product of $C(K^{n+1})$ with itself, expanded by polarity π. In the simplest case of a finite field F_p, where p is a prime number $C(F_p)$ is a symmetric group $S_{p^{n+1}}$. The Cremona group $C(K^{n+1})$ contains the group of all affine invertible transformations, i.e., transformation of kind $\mathrm{x} \to \mathrm{x}A + \mathrm{b}$, where $\mathrm{x} = (x_1, x_2, \ldots, x_{n+1}) \in C(K^{n+1})$, $\mathrm{b} = (b_1, b_2, \ldots, b_{n+1})$ is a chosen vector from $C(K^{n+1})$ and A is a matrix of a linear invertible transformation of K^{n+1}.

The graph $RA_n(K)$ is a bipartite directed one. We assume that the plaintext K^{n+1} is a point $(p_1, p_2, \ldots, p_{n+1})$. We choose two affine transformations T_1 and T_2 and a linear transformation u will be of kind $p_1 \to p_1 + a_1 p_2 + a_3 p_3 + \cdots + a_{n+1}$. We will follow a general scheme, so Alice computes symbolically chosen T_1 and T_2, chooses a string $(\beta_1, \beta_2, \ldots, \beta_l)$ of colours for $RE_n(K)$, such that $\beta_i \neq -\beta_{i+1}$ for $i = 1, 2, \ldots, l - 1$. She computes $N_l = N_{\beta_1} \times N_{\beta_2} \cdots \times N_{\beta_l}$. Recall that N_α, $\alpha \in \mathrm{Reg}(K)$ is the operator of taking the neighbour of the vertex v alongside the arrow with the colour α in the graph $RA_n(K)$..

Alice keeps chosen parameters secret and computes the public rule g as the symbolic composition of T_1, N, and T_2.

Pobrane z czasopisma Annales AI- Informatica **http://ai.annales.umcs.pl**
Data: 30/06/2026 21:27:26

In the case $K = F_q$, $q = 2^n$ this public key rule has a certain similarity to the Imai-Matsomoto public rule, which is computed as a composition T_1ET_2 of two linear transformations T_1 and T_2 of the vector space $F_{2^nF_{2^s}}$, where F_{2^s} is a special subfield, and E is a special Frobenius automorphism of F_{2^n}. The public rule corresponding to T_1ET_2 is a quadratic polynomial map (see [**15**] and [**21**] for the detailed description of the algorithm, its cryptanalysis and generalizations by J. Patarin)

In the case of $RA_n(K)$ the degree of transformation N_l is 3, independently of the choice of length l [**16**]. So the public rule is a cubical polynomial map of the free module K^{n+1} onto itself.

5.1. The time evaluation for the public rule.

Recall that we combine a graph transformation N_l with two affine transformations T_1 and T_2. Alice can use $T_1N_lT_2$ 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 kind $x_{i+1} \ldots x_{i_3}$, where $i_1, i_2, i_3 \in 1, 2, \ldots, n_1$ with the coefficients from $K = F_q$. As mentioned before the polynomial equations $y_i = F_i(x_1, x_2, \ldots, x_n)$, which are made public, have the degree 3. Hence the process of an encryption and a decryption can be done in the polynomial time $O(n^4)$ (in one y_i, $i = 1, 2, \ldots, n$ there are $2(n^3 - 1)$ additions and multiplications). But the cryptanalyst Cezar, having only a formula for y, has a very hard task to solve the system of n equations of n variables of degree 3. It is solvable in the exponential time $O(3^{n^4})$ by the general algorithm based on the Gröbner basis method. Anyway studies of specific features of our polynomials could lead to effective cryptanalysis. This is an open problem for specialists.

We have written a program for generating a public key and for encrypting a text using the generated public key. The program is written in C++ and compiled with the gcc compiler.

We have implemented three cases:

- T_1 and T_2 are identities,
- T_1 and T_2 are of kind $x_1 \to x_1 + a_2x_2 + a_3x_3 + \cdots + a_{n+1}x_{n+1}$ (linear time of computing T_1 and T_2),
- $T_1 = A_1x + b_1$, $T_2 = A_2x + b_2$; matrices A_1, A_2 and vectors b_1, b_2 have mostly nonzero elements.

Table 1 applies to the second case. It presents the time (in milliseconds) of the generation of the public key depending on the number of variables (n) and the password length (p).

Pobrane z czasopisma Annales AI- Informatica **http://ai.annales.umcs.pl**
Data: 30/06/2026 21:27:26

TABLE 1. Time of public key generation ($K = F_{2^{32}}$)

	$p = 20$	$p = 40$	$p = 60$
	T_a	T_a	T_a
$n = 10$	16	16	31
$n = 20$	141	280	437 0
$n = 30$	562	1217	1888
$n = 40$	1513	3464	5678
$n = 50$	3261	8346	13089
$n = 60$	6271	16239	26426
$n = 70$	11139	29032	47440
$n = 80$	17301	47315	79279
$n = 90$	26582	72415	122866
$n = 100$	38173	104053	180790
$n = 110$	53149	144987	251380
$n = 120$	70169	189479	338258

The time of encryption process depends linearly on the number of monomials (the number of nonzero coefficients) in the cubic polynomials F_1, F_2, ... ,F_n in the public map $y = (F_1(x_1, \ldots, x_n), \ldots, F_n(x_1, \ldots, x_n))$. For $n = 120$ and $p = 60$ this number is about 390 in the first case, about 450000 in the second case and about 1800000 in the third case.

Tables 2, 3 and 4 apply to the aforementioned cases. They present the number of monomials in a public map depending on n and p.

TABLE 2. Number (percentage) of nonzero coefficients (1st case)

	$p = 20$	$p = 40$	$p = 60$
$n = 10$	31 (1.08%)	31 (1.08%)	31 (1.08%)
$n = 20$	65 (0.18%)	65 (0.18%)	65 (0.18%)
$n = 30$	96 (0.06%)	96 (0.06%)	96 (0.06%)
$n = 40$	130 (0.03%)	130 (0.03%)	130 (0.03%)
$n = 50$	161 (0.01%)	161 (0.01%)	161 (0.01%)
$n = 60$	195 (0.01%)	195 (0.01%)	195 (0.01%)
$n = 70$	226 (0.01%)	226 (0.01%)	226 (0.01%)
$n = 80$	260 (0.00%)	260 (0.00%)	260 (0.00%)
$n = 90$	291 (0.00%)	291 (0.00%)	291 (0.00%)
$n = 100$	325 (0.00%)	325 (0.00%)	325 (0.00%)
$n = 110$	356 (0.00%)	356 (0.00%)	356 (0.00%)
$n = 120$	390 (0.00%)	390 (0.00%)	390 (0.00%)

Pobrane z czasopisma Annales AI- Informatica **http://ai.annales.umcs.pl**
Data: 30/06/2026 21:27:26

TABLE 3. Number (percentage) of nonzero coefficients (2nd case)

	$p = 20$	$p = 40$	$p = 60$
$n = 10$	314 (10.98%)	314 (10.98%)	314 (10.98%)
$n = 20$	2449 (6.91%)	2449 (6.91%)	2449 (6.91%)
$n = 30$	7244 (4.43%)	7244 (4.43%)	7244 (4.43%)
$n = 40$	17699 (3.59%)	17699 (3.59%)	17699 (3.59%)
$n = 50$	32574 (2.78%)	32574 (2.78%)	32574 (2.78%)
$n = 60$	57749 (2.42%)	57749 (2.42%)	57749 (2.42%)
$n = 70$	88304 (2.03%)	88304 (2.03%)	88304 (2.03%)
$n = 80$	134599 (1.83%)	134599 (1.83%)	134599 (1.83%)
$n = 90$	186434 (1.60%)	186434 (1.60%)	186434 (1.60%)
$n = 100$	260249 (1.47%)	260249 (1.47%)	260249 (1.47%)
$n = 110$	338964 (1.32%)	338964 (1.32%)	338964 (1.32%)
$n = 120$	446699 (1.23%)	446699 (1.23%)	446699 (1.23%)

TABLE 4. Number (percentage) of nonzero coefficients (3rd case)

	$p = 20$	$p = 40$	$p = 60$
$n = 10$	1210 (42.31%)	1210 (42.31%)	1210 (42.31%)
$n = 20$	8820 (24.90%)	8820 (24.90%)	8820 (24.90%)
$n = 30$	28830 (17.61%)	28830 (17.61%)	28830 (17.61%)
$n = 40$	67240 (13.62%)	67240 (13.62%)	67240 (13.62%)
$n = 50$	130050 (11.10%)	130050 (11.10%)	130050 (11.10%)
$n = 60$	223260 (9.37%)	223260 (9.37%)	223260 (9.37%)
$n = 70$	352870 (8.11%)	352870 (8.11%)	352870 (8.11%)
$n = 80$	524880 (7.14%)	524880 (7.14%)	524880 (7.14%)
$n = 90$	745290 (6.38%)	745290 (6.38%)	745290 (6.38%)
$n = 100$	1020100 (5.77%)	1020100 (5.77%)	1020100 (5.77%)
$n = 110$	1355310 (5.26%)	1355310 (5.26%)	1355310 (5.26%)
$n = 120$	1756920 (4.84%)	1756920 (4.84%)	1756920 (4.84%)

6. Private keys based on $A(n, K)$ and $D(n, K)$

We can see that the graphs $A(n, K)$ and $D(n, K)$ are given by equations which use $n - 1$ additions (or subtractions) and multiplications. So the algorithms based on these graphs or corresponding digraphs have the same speed evaluations. In fact, for the decryption we can use numerical implementations. Readers can find speed evaluation for the cases of rings Z_2^8, Z_2^{16} and Z_2^{32} in [16].

Pobrane z czasopisma Annales AI- Informatica **http://ai.annales.umcs.pl**
Data: 30/06/2026 21:27:26

Recently, private keys based on $D(n, F_q)$, $q = 2^8$, $q = 2^{16}$ and $q = 2^{32}$ have been implemented (see [**22**]).

The mixing properties of $D(n, Z_2^m)$, $m = 8, 16, 32$ based encryption in combination with special affine transformations were investigated in [**20**]. At the conference similar studies for mixing properties of $A(m, Z_q)$ based stream cipher (see [**23**], [**24**], [**1**], [**25**]) are presented.

References

[1] Romańczuk U., Ustymenko V., On some cryptographical applications of new family of expanding graphs, Presentation in Conference CECC'2011, Debrecen, Hungary.

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

[3] 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.

[4] Klisowski M., Ustimenko V. A., On the public keys based on the extremal graphs and digraphs, International Multiconference on Computer Science and Informational Technology, October 2010, Wisla, Poland, CANA Proceedings, 12 pp.

[5] Shaska T., Ustimenko V., On some applications of graph theory to cryptography and turbocoding, Albanian J. Math. 2(3) (2008): 249–255, Proceedings of the NATO Advanced Studies Institute: "New challenges in digital communications".

[6] Shaska T., Ustimenko V., On the homogeneous algebraic graphs of large girth and their applications, Linear Algebra Appl. 430(7) (2009): 1826–1837, Special Issue in Honor of Thomas J. Laffey.

[7] Ustimenko V., On the extremal graph theory for directed graphs and its cryptographical applications, Advances in Coding Theory and Cryptography (T. Shaska, D. W. C. Huffman, Joener, and V. Ustimenko, eds.), Series on Coding Theory and Cryptology, World Scientific 3 (2007): 181–199.

[8] Ustimenko V., On the extremal regular directed graphs without commutative diagrams and their applications in coding theory and cryptography, Albanian J. Math. 1(4) (2007), Special issue on algebra and computational algebraic geometry.

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

[10] Ustimenko V., On the cryptographical properties of extremal algebraic graphs, Algebraic Aspects of Digital Communications (Tanush Shaska and Engjell Hasimaj, eds.), NATO Science for Peace and Security Series - D: Information and Communication Security, 24, IOS Press, (2009): 256–281.

[11] Bollobás B., Extremal graph theory, Academic Press, London, (1978).

[12] Simonovits M., Extremal graph theory, Selected Topics in Graph Theory 2(2) (1983): 161–200 (L. W. Beineke and R. J. Wilson, eds.), Academic Press, London.

[13] Bien F., Constructions of telephone networks by group representations, Notices Amer. Math. Soc. 3 (1989): 5–22.

[14] Ore R., Graph theory, Wiley, London (1971).

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

Pobrane z czasopisma Annales AI- Informatica **http://ai.annales.umcs.pl**
Data: 30/06/2026 21:27:26

[16] Ustimenko V., Algebraic graphs and security of digital communications, Institute of Computer Science, University of Maria Curie Sklodowska in Lublin (2011) (supported by European Social Foundation), available at the UMCS web.

[17] Crandall R., Pomerance C., Prime Numbers. A Computational Perspective, Springer, New York (2001).

[18] Menezes A. J., van Oorschot P. C. and Vanstone S. A., Handbook of Applied Cryptography, CRC Press, Inc. third edition (1997).

[19] Lazebnik F., Ustimenko V. A., and Woldar A. J., A new series of dense graphs of high girth, Bull. Amer. Math. Soc. (N.S.) 32(1) (1995): 73–79.

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

[21] Patarin J., Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt '88, Advances in Cryptology — Crypto '95, Springer (1995): 248-261.

[22] Touzene A., Ustimenko V., AlRaissi M. and Boudeliouua I., Performance of Algebraic Graphs Based Stream-Ciphers Using Large Finite Fields (to appear).

[23] Klisowski M., Ustimenko V., On the implementation of cubic public keys based on algebraic graphs over the finite commutative ring and their special symmetries, Presentation in Conference CECC'2011, Debrecen, Hungary.

[24] Kotorowicz S., Romańczuk U. and Ustimenko V., On the implementation of stream ciphers based on a new family of algebraic graphs, Presentation in Conference FedCSIS'2011, Szczecin, Poland.

[25] Wróblewska A., Ustymenko V., On the key expansion of $D(n, K)$-based cryptographical algorithm, Presentation in Conference CECC'2011, Debrecen, Hungary.