Math.Comput.Sci. (2012) 6:181–198
DOI 10.1007/s11786-012-0121-x

Mathematics in Computer Science

On the Comparison of Cryptographical Properties of Two Different Families of Graphs with Large Cycle Indicator

Michał Klisowski · Vasyl Ustimenko

Received: 17 February 2011 / Revised: 7 June 2012 / Accepted: 8 June 2012 / Published online: 22 July 2012

Abstract The paper is devoted to the implementations of the public key algorithms based on simple algebraic graphs $A(n, K)$ and $D(n, K)$ defined over the same finite commutative ring K. If K is a finite field both families are families of graphs with large cycle indicator. In fact, the family $D(n, F_q)$ is a family of graphs of large girth (f.g.l.g.) with $c = 1$, their connected components $CD(n, F_q)$ form the f.g.l.g. with the speed of growth $4/3$. Family $A(n, q)$, $\mathrm{char} F_q \neq 2$ is a family of connected graphs with large cycle indicator with the largest possible speed of growth. The computer simulation demonstrates the advantage (better density which is the number of monomial expressions) of public rules derived from $A(n, q)$ in comparison with symbolic algorithm based on graphs $D(n, q)$.

Keywords Algebraic multivariate cryptography · Graph algorithms · Density of polynomial multivariate maps of small degree

Mathematics Subject Classification 14G50 · 05C85 · 11T71

1 Introduction

Multivariate cryptography in the narrow sense (see Wikipedia) is the generic term for asymmetric cryptographic primitives based on multivariate polynomials over finite fields. In certain cases these polynomials could be defined over both a ground and an extension field. If the polynomials have the degree two, we talk about multivariate quadratics. Solving systems of multivariate polynomial equations is proven to be NP-Hard or NP-Complete. That is why these schemes are often considered to be good candidates for post-quantum cryptography, once quantum computers can break the current schemes. Today multivariate quadratics could be used only to build signatures. This definition rises several questions: Why a finite field but not a commutative ring is used? Why quadratics are so important?

We define multivariable cryptography as studies of cryptosystems based on special regular automorphism f of algebraic variety $M_n(K)$ of dimension n in a sense of Zarisski topology over finite commutative ring K. An example of algebraic variety is a free module K^n which is simply a Cartesian product of n copies of K^n into iself. Regular automorphism is a bijective polynomial map of $M_n(K)$ onto itself such that f^{-1} is also a polynomial map.

M. Klisowski · V. Ustimenko (✉)
Maria Curie-Sklodowska University, Institute of Mathematics, pl. M. Curie-Skłodowskiej 1, 20-031 Lublin, Poland
e-mail: vasyl@hektor.umcs.lublin.pl

M. Klisowski
e-mail: mklisow@hektor.umcs.lublin.pl

Elements of K^n can be identified with strings $(x_1, x_2, \ldots, x_n)$ in alphabet K, nonlinear map f of restricted degree d can be used as a public rule if the key holder (Alice) knows the secret decomposition of f into composition of special maps $f_1, f_2, \ldots, f_s$ with known inverse maps ${f_i}^{-1}$. So she can decrypt by consecutive application of ${f_s}^{-1}, f_{s-1}^{-1}, \ldots, {f_1}^{-1}$. Notice, that public user (Bob) has to use symbolic computations to work with f, but Alice may use numerical computations for the implementation of private key decryption process. Of course K^n can be changed for the family of varieties $M_n(K), n = 1, 2, \ldots$, the commutative ring can be treated as an alphabet, element $v \in M_n(k)$ as a "potentially infinite" plaintext, parameter n as a measurement of size of v.

The complexity of the best general algorithms for the solution of nonlinear system of equation of kind $f(x) = y, x, y \in K^n$ equals $d^0(n)$ (see recent paper [5]). One can use Gröbner basis, Gauss elimination method or alternative options for the investigation of the system. Of course, one can write simple nonlinear equations which are easy to solve. So the system of nonlinear equations has to be tested on "pseudorandomness" and the map f has to be of large order. Notice, that one of the first attempts to create workable multivariate cryptosystem was proposed by Imai and Matsumoto. They used finite field of characteristic 2 and its extension, f has a decomposition $f_1 f_2 f_3$, where f_1 and f_2 are affine maps (of degree 1) and f_2 is a Frobenius automorphism. Cryptanalysis for the scheme the reader can find in [14], the history of its various modifications goes on (see, for instance survey in [40]). We have to notice that the failure of this cryptosystem is not a surprise for specialists in algebra. Despite its formal quadratic appearance Frobenius automorphism is quite close to linear maps (in his famous book [4] Dieudonné uses term 3/2 linear map for such automorphism). One of the popular directions in multivariate cryptography is the use of tools outside commutative algebra such as dynamical systems or extremal algebraic graphs (see [40,41] and further references) for the creation of nonlinear maps of pseudorandom nature.

Algebraic graphs are graphs defined by systems of algebraic equations, their vertex sets and edge sets are algebraic varieties in corresponding Zarisski topology. The walks on such graphs can be used for the generation of public rules of multivariate cryptography, reverse walk will provide the private key algorithm for the decryption process (see [24,27–33,35,37,38]). A girth of a graph is the length of its minimal cycle. Generalised m-gon is a bipartite biregular graph of girth $2m$ and diameter m. According to modifications of Even Cycle Theorem by P. Erdős, the size (number of edges) of the graph on v vertices of girth $>2n$ is $O(v^{1+1/n})$ and the size of known q-regular generalised m-gons ($m = 3, 4, 6$) belongs to this upper bound for $n = m - 1$. In some sense generalised m-gons are similar to random graphs. The multivariate cryptosystems based on affine parts of known generalised polygons have been proposed in [30] (see also [32]). A bit earlier we started an investigation of cryptosystems connected with families of k-regular graphs G_i of large girth for which girth g_i is $\geq c\log_k(v_i))$, where v_i is the order of $G_i, i = 1, 2, \ldots$.

The existence of such families was proved by P. Erdős in late 50th. The first explicit constructions appeared in [17,20]. They are family of special Cayley graphs for the group $PSL_2(p)$ and algebraic graphs of nonlinear nature $D(n, q)$ defined over general finite field F_q (see [19] for descriptions of their connected components $CD(n, q)$).

In publications [15] classes of stream ciphers and public key algorithms based on explicit construction of families of algebraic graphs of large girth $D(n, q)$ and their generalisations $D(n, K)$, where K is general commutative ring ($D(n, F_q) = D(n, q)$) were proposed. It was shown later [42] that for each finite commutative ring K we can create a cubical polynomial map f of K^n onto K^n depending on string of regular elements (non-zero divisors $(\alpha_1\alpha_2, \ldots, \alpha_t)$ (password). If $t \leq (n+5)/2$ and $\alpha_i + \alpha_{i+1}$ are regular ring elements then different strings produce different ciphertexts. One can use such a map as a stream cipher. Recently [40,41] we show that conditions of regularity we can change for $\alpha_i + \alpha_{i+1} \in M$, where the multiplicative clousure of a subset M of K does not contain zero. 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. Public user is not able to decrypt a ciphertext without the knowledge of τ_1, τ_2 and 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 related cyclic group for the Diffie-Hellman key exchange protocol. We can prove that the order of g corresponding to string $(\alpha_1\alpha_2, \ldots, \alpha_t)$, $\alpha_k + \alpha_1 \in M$ is growing with the growth of the parameter n.

The paper [11] is devoted to the implementation of generalisation of the above mentioned algorithms. We consider linear transformations T_a depending on the string $a = (\beta_1, \beta_2, \ldots, \beta_d)$, where $d = [n/4]$ and use fT_a instead of f.

The construction of transformation f uses graphs $D(n, K)$ (graphs of large girth for $K = F_q$), which were very useful for creation of good LDPC codes in Coding Theory. The transformation T_a is a special automorphism

of graph $D(n, K)$. The properties of such modified public keys were presented at MACIS 2011 conference in Beijing (see [12]). It is very natural to compare multivariate cryptosystems based on $D(n, K)$ and $D(n, K')$ over different rings of the same size. The densities of public rules in case $K = F_{2^m}$ and K' is a boolean ring of size $2^m, m = 8, 16, 32$ are discussed in [13]. The comparison of private keys for $K = F_{2^m}$ and arithmetical rings $K = Z_n, n = 2^m, m = 8, 16, 32$ the reader can make looking at material of [11,39].

In current publication we compare the public rules based on graphs $D(n, q)$ and rather new extremal graphs $A(n, q)$ (see [10,22]). Graphs $A(n, q)$ are important example connected with another optimisation problem on graphs—problem of finding the maximal size of graph of order v with cycle indicator $\geq m$ (the definition of this parameter is written below).

Classical problems of Turan type on studies of the maximal size of simple graphs without prohibited cycles are attractive for mathematicians because they are beautiful and difficult (see [2,25]). The concept of a family of simple graphs of large girth appears as an important tool for investigation of such problems. Later the applications of these problems in Networking [1], Coding Theory and Cryptography were found (see [33] and further references).

One of the important directions in W. C. Tutte research (see [2]) was an investigation of cycle matroids. Recall, that every finite graph (or multigraph) Γ gives rise to a matroid as follows: take as $E(\Gamma)$ the set of all edges in Γ and consider a set of edges independent if and only if it does not contain a simple cycle. Such an edge set is called a forest in graph theory. This is called the cycle matroid or graphic matroid of Γ. It is usually written $M(\Gamma)$. Any matroid that is equivalent to the cycle matroid of a (multi)graph, even if it is not presented in terms of graphs, is called a graphic matroid or cycle matroid. The matroids that are graphic have been characterized by Tutte.

Recall, that the girth $g(\Gamma)$ of simple graph Γ is the length of its minimal cycle. Let $g(x)$ be the length of the minimal cycle through the vertex x from the set $V(\Gamma)$ of vertices in graph Γ. We refer to $\max g(x), x \in V(\Gamma)$ as cycle indicator $\mathrm{Cind}(\Gamma)$ of the a graph. We say that vertex x is incident to subset E of $E(\Gamma)$ and write $x\,I\,E$ if there is an edge from E which contains x. We refer to E as connected set if graph $E, \{x|x\,I\,E\}$ is a connected graph. It is clear that graph with finite Cind is not a forest. For each $r, r \leq \mathrm{Cind}$ there is a vertex x such that for each connected $E, E\,I\,x$ of cardinality r is an element of $M(\Gamma)$ ($(E, \{x|x\,I\,E\})$ is a tree). Obviously $\mathrm{Cind}(\Gamma) \geq g(\Gamma)$.

The problem of finding the maximal size $e(v)$ of the graph on v vertices with cycle indicator $>2m$ is formally not a problem of Turan type but it is typical optimisation problem on graph closely connected with studies of extremal graphs without prescribed cycles. As it was stated in [41] $e(v) \Leftrightarrow cv^{1+1/m}$, where c is a constant. So in difference with the bound of Even Circuit Theorem the new bound is always sharp.

If Γ_i is a family of connected k-regular graphs of increasing order with increasing cycle indicator for which projective (or inductive) limit $\Gamma = \Gamma_i, i \to \infty$ is well defined, then Γ is a tree.

Let us introduce the natural generalisation of a family of graphs of large girth.

We refer to a family of regular simple graphs Γ_i of degree k_i and order v_i as *family with large cycle matroid* if $\mathrm{Cird}(\Gamma_i) \geq c\log(v_i)$ for some independent constant $c, c > 0$. It is nice to have speed c of growth of cycle indicator as large as it possible for a family of graphs.

If all degrees k_i are equal to certain constant k we will use the term *family of graphs of large cycle indicator*.

Families of connected graphs with large cycle matroids are interesting for applications because of the existence of large rooted tree with the root $x \in \Gamma_i$. Recall, that family of regular graphs Γ_i of degree k_i and increasing order v_i is a family of graphs of large girth *f.g.l.g.* if $g(\Gamma_i) \geq c\log(v_i)$ for some independent constant $c, c > 0$. *F.g.l.g.* plays an important role in Extremal Graph Theory, Theory of LDPC codes and Cryptography [6–8]. *F.g.l.g.* of bounded degree are hard to construct. This fact is a serious motivation for the studies of infinite families of graphs with large cycle matroid, which are generalisations of *f.g.l.g.*.

In our paper we discuss applications of family of graphs $A(n, q)$ with large cycle matroid with constant $c = 2$ to cryptography in terms of symbolic computations. It is easy to see that the size of $A(n, q)$ of order $v = 2q^n$ belongs to upper bound for $e(v)$. There is a conjecture that for fixed q family $A(n, q)$ form a family of graphs with large girth with the constant $c', c' < 2$.

The idea (see [22]) is to create families of cycle groups $C_n = \langle f_n \rangle$ with generator f_n, which is a bijective polynomial transformation of vector space ${F_q}^n$, such that the order $|C_n|$ is large and all g_n are polynomial maps of small degree.

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

In Sect. 3 we consider the definition of a family of affine algebraic digraphs of large girth over commutative rings. Explicit constructions of such families of graphs can be used for the development of public keys and a key exchange protocol. We discuss the connection of these algorithms with the group theoretical discrete logarithm problem.

The known examples of families of simple algebraic graphs were constructed just in the case of finite fields (see [18,19]). In Sect. 4 we consider an explicit construction of a family of affine algebraic digraphs of large girth over each finite commutative ring containing at least 3 regular elements. Different properties of this family are investigated in [23,24,33,34,36,37].

In Sect. 5 we discuss the implementation of public key algorithms based on a new family $A(n,q)$ of graphs with large cycle matroids for the generations of cyclic groups C_n of cubical transformations of ${F_q}^n$ and discuss corresponding public key algorithms. Section 6 is devoted to the comparison of the density of public keys related to $A(n,q)$ and $D(n,q)$.

2 On the Families of Directed Graphs of Large Girth

The missing theoretical definitions on directed graphs the reader can find in [21]. 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 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 vertices a and b is the sequence $a = x_0 \to x_1 \to \ldots x_s = b$ of 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. Notice that the graph of antireflexive binary relation may have a directed cycle $O_s = O_{s,0} : v_0 \to v_1 \to \ldots v_{s-1} \to v_0$, 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 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 distance <gi are connected by the unique path from u to v of 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 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 general case gi $= d$ implies that $g \geq d+1$. So in the case of the family of graphs with 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 [21] 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 order v_i and diameter d_i. We say, that F is a family of small world graphs if $d_i \leq C \log_{k_i}(v_i), i = 1, \ldots$ for some constant C independent on i. The

definition of small world simple graphs and related explicit constructions the reader can find in [2]. For the studies of small world simple graphs without small cycles see [25,34].

3 On the K-Theory of Affine Graphs of High Girth and Its Cryptographical Motivations

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 Zarisski topology.

Let G be 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 a 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.

Here, at the end of section, we consider cryptographical 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 about finding a solution for the equation $g^x = b$ where x is 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 unfeasible the computation of n. For many finite groups the discrete logarithm problem is NP complete.
   Let K be a finite commutative ring and M be an affine variety over K. Then the Cremona group $C(M)$ of all 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 elements of $C_i = C(V_i(K))$. We can chose 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 large girth. It means that the girth indicator $\mathrm{gi}_i = \mathrm{gi}(G_i(K))$ and the parameter $\mathrm{dirg}_i = \mathrm{dirg}(G_i(K))$ are growing 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. 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 [14] for the details). Let Alice and Bob be correspondents. Alice computes the symbolic map g and send it to Bob via open channel. So the variety and the map are known for the adversary (Cezar). Let Alice and Bob choose 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 information is $g^{n_A n_B}$ given in "public mode fashion". Bob can be just a public user (no information on the way in which the map g were cooked) , so he and Cezar are making computations much slower than Alice who has the decomposition $g = u^{-1}N_{\alpha_1}N_{\alpha_2}\ldots N_{\alpha_k}u$.
We may modify slightly the Diffie-Hellman protocol using the action of the group on the variety. Alice chooses a rather short password $\alpha_1, \alpha_2, \ldots, \alpha_k$, 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 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 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 $\alpha_1, \alpha_2, \ldots, \alpha_t$ of 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 $x_1, x_2, \ldots, x_n$. Alice presents the map in the form of public rules, such as

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

We can assume (at least theoretically) that the public rule depending on parameter j is applicable to encryption of potentially infinite text (parameter t is a linear function on j now).
For the computation she may use the Gröbner base technique or alternative methods, special packages for the symbolic computation (popular "Mathematica" or "Maple", package "Galois" for "Java" as well 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 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 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'_{α_t}, $N'_{\alpha_{t-1}}$, $\ldots$, N_{α_1} and u to the ciphertext. So the decryption and the encryption for Alice take the same time. She can use a numerical program to implement her symmetric algorithm.
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 a discrete logarithm problem with the base h in related Cremona group of all polynomial bijective transformations.

Of course for further cryptanalysis we need to study the information on possible divisors of order of the base of 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 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 On the Family of Affine Digraph of Large Girth over Commutative Rings

E. Moore used term *tactical configuration* of order (s, t) for biregular bipartite simple graphs with 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 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 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 parenthesis 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 $p_1 \neq p_2$.

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 [36] (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 [17] for the case of general commutative ring K:

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

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 are 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:

$$l_{i,i} - p_{i,i} = l_{1,0}p_{i-1,i}$$
$$l'_{i,i} - p'_{i,i} = l_{i,i-1}p_{0,1}$$
$$l_{i,i+1} - p_{i,i+1} = l_{i,i}p_{0,1}$$
$$l_{i+1,i} - p_{i+1,i} = l_{1,0}p'_{i,i}$$

(These four relations are defined for $i \geq 1$, $p'_{1,1} = p_{1,1}, l'_{1,1} = l_{1,1}$). This incidence structure (P, L, I) we denote as $D(K)$. 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 $D(k, K)$.

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 $DE_n(K)$ $(DE(K))$ be the double directed graph of the bipartite graph $D(n, K)$ $(D(K)$, 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 $l^1_{1,0} - l^2_{1,0}$.

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 a 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 show that a new graph $RE_n(K)$ $(RE(K))$ with the induced colouring into colours from the alphabet Reg(K) is vertex transitive. Really, according to [25] graph $D(n, K)$ is an edge transitive. This fact had been established via the description of regular on the edge set subgroup $U(n, K)$ of the automorphisms group Aut(G). The vertex set for the graph $DE_n(K)$ consists of two copies F_1 and F_2 of the edge set for $D(n, K)$.

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 affine graph $RE_n(K)$ $(RE(K))$ with the induced colouring into colours from the alphabet Reg(K) is vertex transitive (see [37]).

Notice, that each T_a acts naturally on the flags, it is an automorphism of $RE_n(K)$.

5 On the Family of Graph of Large Cycle Indicator

Below we consider the family of graphs $A(k, \mathbb{K})$, where $k > 5$ is a positive integer and $\mathbb{K}$ is a commutative ring.

Let P and L be two copies of Cartesian power $\mathbb{K}^{\mathbb{N}}$, where $\mathbb{K}$ is the commutative ring and $\mathbb{N}$ 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 coordinates of points and lines introduced in [22] for the case of a general commutative ring $\mathbb{K}$:

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

The elements of P and L can be thought of as infinite ordered tuples of elements from $\mathbb{K}$, such that only a finite number of components are 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:

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

The incidence structure (P, L, I) we denote as $A(\mathbb{K})$. 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 into 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 $A(k, \mathbb{K})$.

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 as simple projection of each vector from P_k and L_k onto its $k-1$ initial coordinates with respect to the above order.

The following statement is announced in [38].

Theorem 1 *For each finite field F_q graphs $A(n, F_q)$ form a family of graphs of large cycle indicator with maximal possible speed of growth. If* $\mathrm{char} F_q \neq 2$ *then $A(n, F_q)$ is a connected graph.*

Let $DA_n(\mathbb{K})$ ($DA(\mathbb{K})$) be the double directed graph of the bipartite graph $A(n, \mathbb{K})$ ($A(\mathbb{K})$, 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 $l^1_{1,0} - l^2_{1,0}$.

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 $p^1_{1,0} - p^2_{1,0}$.

The vertex set for the graph $DA_n(\mathbb{K})$ consists of two copies $\mathcal{F}_1$ and $\mathcal{F}_2$ of the edge set for $A(n, \mathbb{K})$.

Similarly to the content of previous section we define graph $RA_n(K)$ by simple deleting of edges with colours from $K - \mathrm{Reg}(K)$. It can be shown that computation corresponding to the pass of this graph $RA_n(K)$ is a cubical map $N = N_l$, where l stands for the length of the pass. We will combine new N with two affine transformation T_1 and T_2 and evaluate multivariate cryptosystem based on the map $T_1 N T_2$.

6 On the Implementation of the Public Key Algorithm Based on $RE_n(K)$ and $RA_n(K)$

The graphs $CRE_n(K)$ have the best known speed of growth of the girth indicator evaluated in the previous section. It turns out that for the computer implementation of the public key algorithm described in the Sect. 4 the family $RE_n(K)$ of "enveloping" for $CRE_n(K)$ graphs were chosen first. It is also a family of digraphs of large girth but the speed of the growth of girth indicator for the family is less of those for $RE_n(K)$. Graphs $RE_n(K)$ were defined via the family of graphs $D(n, K)$ in the way described in the previous section. So, in some publications the description of the algorithm was done in terms of $D(n, K)$. We introduced here a speed evaluation of the algorithm for its latest implementation.

The set of vertices of the graph $RE_n(K)$ is a union of two copies 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}.

Graph $RE_n(K)$ is a bipartite directed graph. 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 slightly modify a general scheme, so Alice computes symbolically of 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 $N_\alpha, \alpha \in \mathrm{Reg}(K)$ is the operator of taking the neighbour of the vertex v alongside the arrow with the colour α in the graph $RE_n(K)$. Alice chooses additionally string a.

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

In case $K = F_{q^n}, q = 2^m$ this public key rule has a certain similarity to the Imai-Matsumoto public rule, which is computed as a composition $T_1 E T_2$ of two linear transformations T_1 and T_2 of the vector space of dimension n over F_{q^m}, and E is a special Frobenius automorphism. The public rule corresponding to $T_1 E T_2$ is a quadratic polynomial map (see [14] for the detailed description of the algorithm, its cryptanalysis and generalizations by J. Patarin)

In the case of $RE_n(K)$ the degree of transformation N_l is 3, independently on the choice of length l [42]. So the public rule is a cubical polynomial map of the free module K^{n+1} onto itself. In case of a finite field the algorithm

Table 1 Number of monomials in public map, graph $D(n, K)$, $K = F_{2^{32}}$, case I

n	Password length			
	16	32	64	128
16	145	145	145	145
32	544	545	545	545
64	1,584	2,112	2,113	2,113
128	3,664	6,240	8,320	8,321

Table 2 Number of monomials in public map, graph $D(n, K)$, $K = F_{2^{32}}$, case II

n	Password length			
	16	32	64	128
16	2,062	2,062	2,062	2,062
32	15,475	15,476	15,476	15,476
64	82,722	119,855	119,856	119,856
128	369,250	636,430	943,463	943,464

is equivalent to the public rule considered in [31]. We implemented also a similar algorithm based on new graph $RA_n(K)$ which generate public rules given by cubical polynomials.

More information about the implementation of graph based cryptographic algorithms the reader can find in [3,9,16,26].

6.1 On the Time Evaluation for the Public Rule

Recall, that we combine a graph transformation N_l corresponding to graph $RE_n(K)$ or $RA_n(K)$ with two affine transformation T_1 and T_2. Alice can use $T_1 N_l T_a T_2$ 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 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 we mention 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 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 exponential time $O(3^{n^4})$ by the general algorithm based on 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 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 has mostly nonzero elements.

The Tables 1, 2, 3, 4, 5, and 6 present the number of monomials depending on the number of variables (n) and the password length in all three cases and both families of graphs $D(n, K)$ and $A(n, K)$.

The Tables 7, 8, 9, 10, 11, and 12 present the time (in milliseconds) of the generation of public key monomials depending on the number of variables (n) and the password length in all three cases and both families of graphs $D(n, K)$ and $A(n, K)$.

Table 3 Number of monomials in public map, graph $D(n, K)$, $K = F_{2^{32}}$, case III

n	Password length			
	16	32	64	128
16	6,544	6,544	6,544	6,544
32	50,720	50,720	50,720	50,720
64	399,424	399,424	399,424	399,424
128	3,170,432	3,170,432	3,170,432	3,170,432

Table 4 Number of monomials in public map, graph $A(n, K)$, $K = F_{2^{32}}$, case I

n	Password length			
	16	32	64	128
16	250	250	250	250
32	770	1,010	1,010	1,010
64	1,810	3,074	4,066	4,066
128	3,890	7,202	12,290	16,322

Table 5 Number of monomials in public map, graph $A(n, K)$, $K = F_{2^{32}}$, case II

n	Password length			
	16	32	64	128
16	3,426	3,426	3,426	3,426
32	19,392	26,310	26,310	26,310
64	89,472	148,420	206,222	206,222
128	383,232	692,676	1,161,356	1,633,054

Table 6 Number of monomials in public map, graph $A(n, K)$, $K = F_{2^{32}}$, case III

n	Password length			
	16	32	64	128
16	6,544	6,544	,6544	,6544
32	50,720	50,720	50,720	50,720
64	399,424	399,424	399,424	399,424
128	3,170,432	3,170,432	3,170,432	3,170,432

Table 7 Public key generation time (ms), graph $D(n, K)$, $K = F_{2^{32}}$, case I

n	Password length			
	16	32	64	128
32	160	320	640	1,280
64	1,680	3,310	6,650	13,330
96	9,050	18,040	36,000	72,000
128	26,980	53,790	107,610	215,770
160	62,960	125,420	249,460	500,660

Table 8 Public key generation time (ms), graph $D(n, K)$, $K = F_{2^{32}}$, case II

n	Password length			
	16	32	64	128
32	290	620	1,260	2,540
64	3,420	8,570	19,340	40,740
96	15,060	37,730	92,040	201,440
128	40,700	102,300	260,740	590,390
160	90,990	226,020	584,480	1,378,700

Table 9 Public key generation time (ms), graph $D(n, K)$, $K = F_{2^{32}}$, case III

n	Password length			
	16	32	64	128
32	1,160	2,200	4,280	8,440
64	19,050	34,730	66,090	128,810
96	109,620	194,420	364,020	703,220
128	355,260	615,260	1,135,260	2,175,260
160	935,370	1,601,130	2,932,650	5,595,690

Table 10 Public key generation time (ms), graph $A(n, K)$, $K = F_{2^{32}}$, case I

n	Password length			
	16	32	64	128
32	0	100	280	640
64	1,440	2,900	6,010	12,170
96	8,160	16,260	32,890	66,160
128	24,780	49,270	98,610	197,840
160	58,730	116,870	234,340	469,860

Table 11 Public key generation time (ms), graph $A(n, K)$, $K = F_{2^{32}}$, case II

n	Password length			
	16	32	64	128
32	330	840	1,920	4,080
64	3,450	9,470	25,330	58,210
96	14,970	39,780	109,920	274,810
128	40,880	106,370	296,840	788,550
160	91,300	232,620	642,250	1,760,530

Table 12 Public key generation time (ms), graph $A(n, K)$, $K = F_{2^{32}}$, case III

n	Password length			
	16	32	64	128
32	1,110	2,070	3,990	7,830
64	20,120	36,920	70,520	137,720
96	111,020	197,260	369,740	714,700
128	369,980	646,940	1,200,860	2,308,700
160	942,340	1,626,340	2,994,340	5,730,340

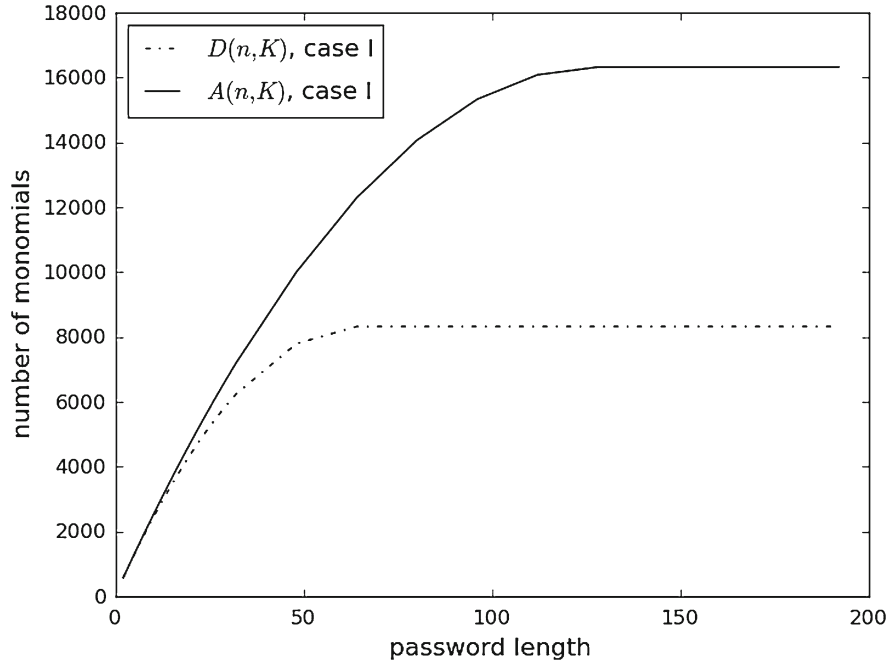

Fig. 1 The number of monomials in public map ($n = 128$, $K = F_{2^{32}}$), case I

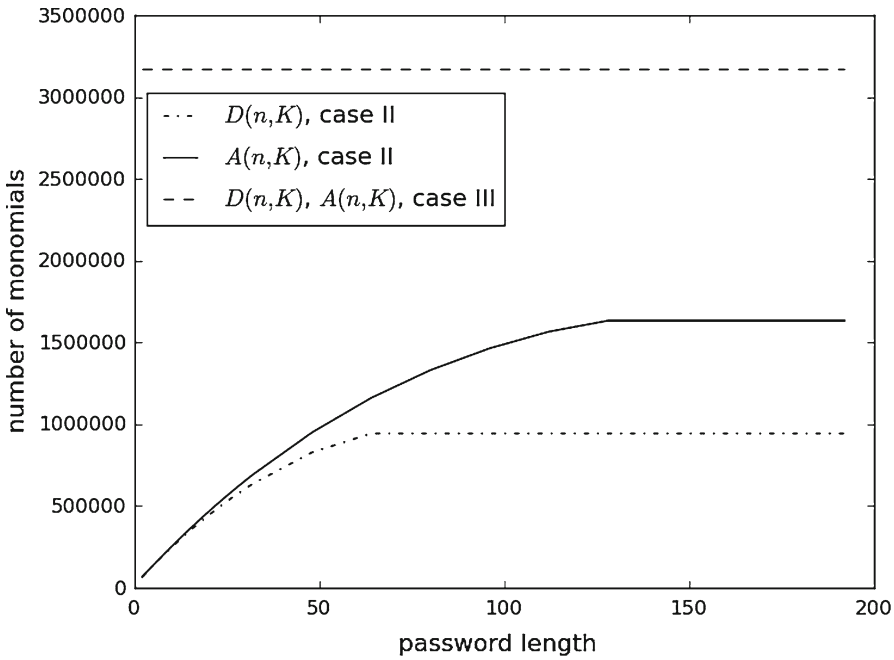

Fig. 2 The number of monomials in public map ($n = 128$, $K = F_{2^{32}}$), cases II and III

The time of encryption process depends linearly on the number of monomials (the number of nonzero coefficients) in cubic polynomials F_1, F_2 ...F_n in the public map $y = (F_1(x_1, \ldots, x_n), \ldots, F_n(x_1, \ldots, x_n))$.

Figures 1 and 2 compare the number of monomials in both families of graph and shows the dependence of this number on the length of the password.

Figures 3, 4, 5, 6, 7, and 8 show the time of the generation of public keys.

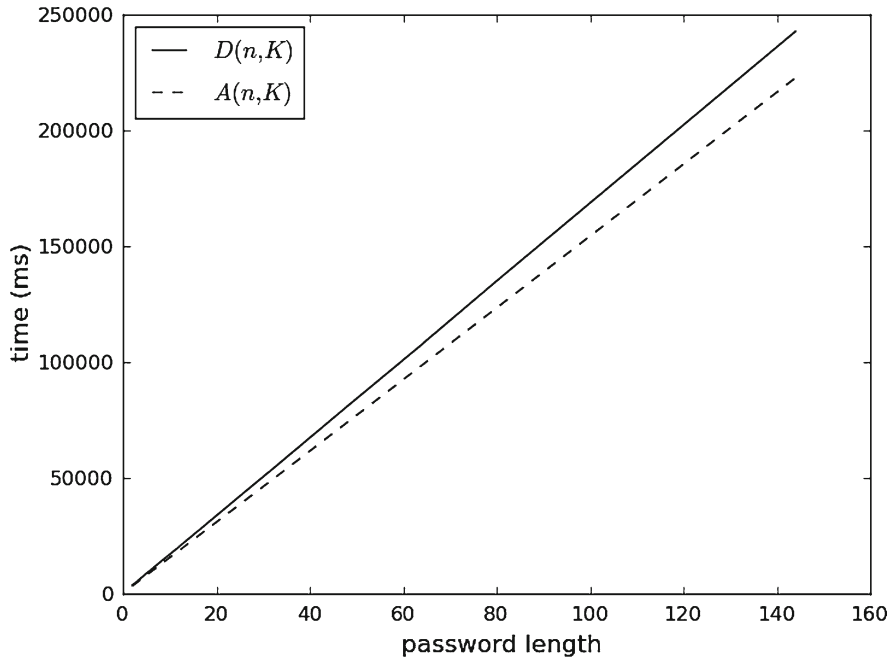

Fig. 3 Public key generation time for fixed graph ($n = 128$, $K = F_{2^{32}}$), case I

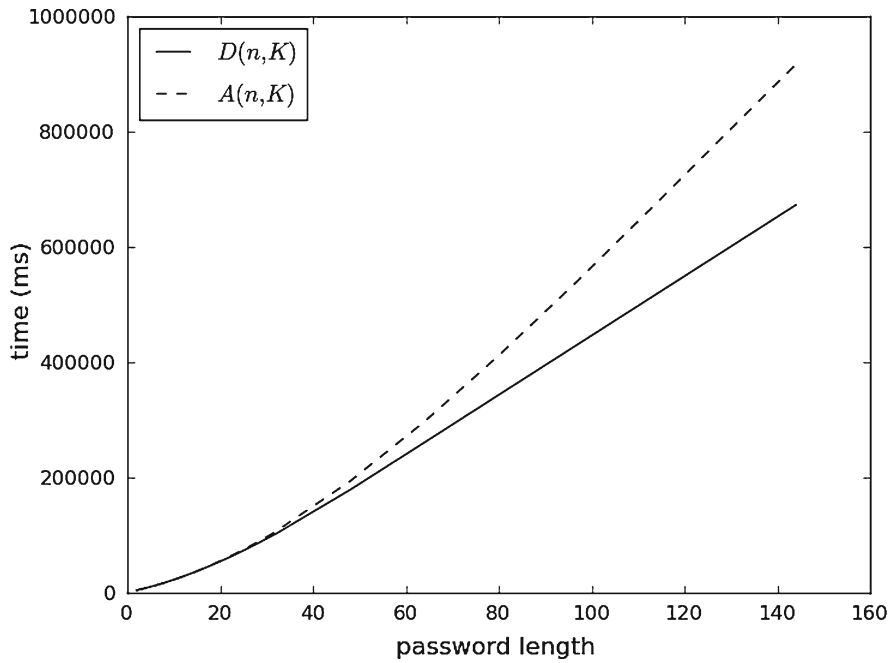

Fig. 4 Public key generation time for fixed graph ($n = 128$, $K = F_{2^{32}}$), case II

6.2 On the Case of Ring Extensions

Let us consider the case when a commutative ring $\mathbb{K}$ itself is a free module over the other ring R, i. e. $\mathbb{K} = R^m$. The reader may think over the following examples.

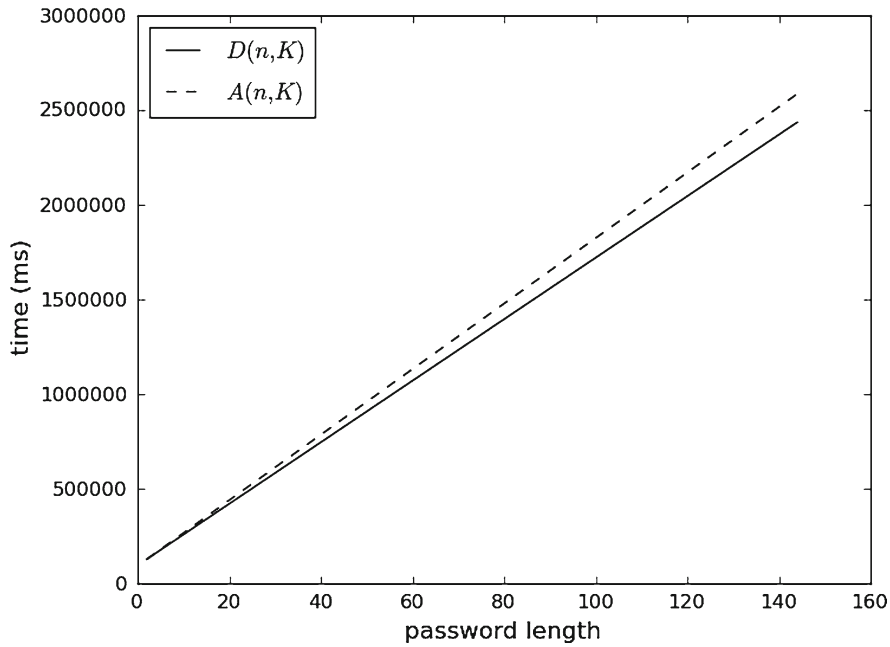

Fig. 5 Public key generation time for fixed graph ($n = 128$, $K = F_{2^{32}}$), case III

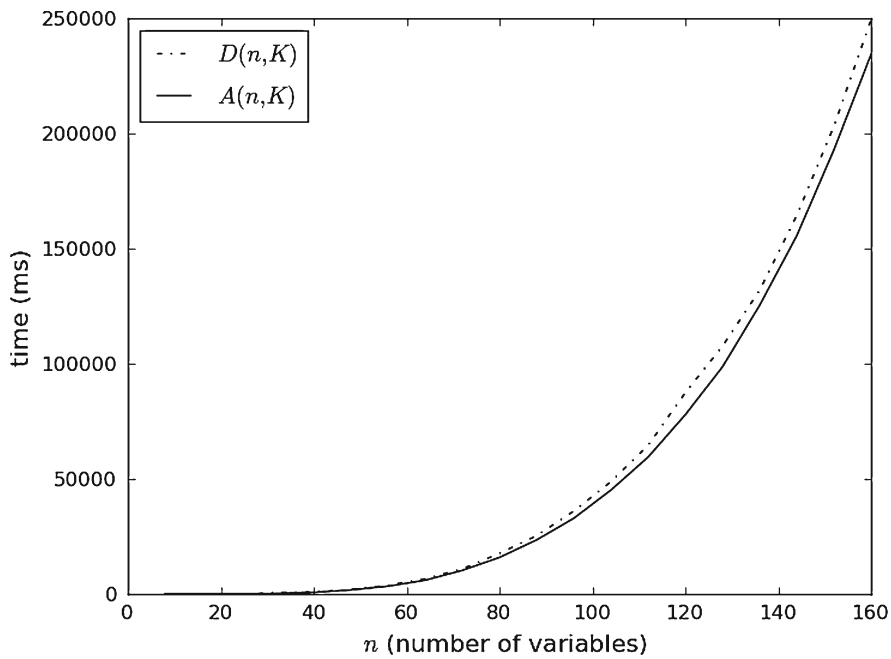

Fig. 6 Public key generation time for fixed password length (64), $K = F_{2^{32}}$, case I

(1) Commutative ring $\mathbb{K}$ is a Kronecker extension of R: there is a polynomial $p(x) \in R[x]$ of degree ≥ 2, such that $\mathbb{K} = R[x]/p(x)$. Commutative ring $R[x]/p(x)$ can be with large multiplicative sets. Obvious examples: if $p(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x$, then $Q = \{f(x) \in R[x]/p(x) | f(0) \neq 0\}$ is a multiplicative set, if $R = \mathbb{F}_p$, p is prime, and $p(x)$ is irreducible polynomial, then $\mathbb{K} = R[x]/p(x)$ is a finite field with multiplicative group $\mathbb{K} - \{0\}$.

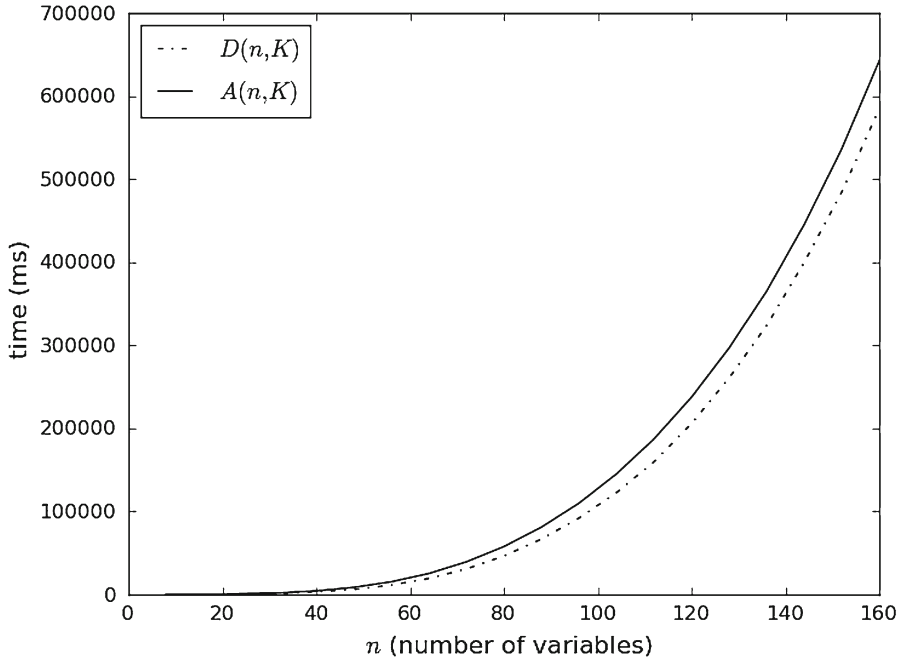

Fig. 7 Public key generation time for fixed password length (64), $K = F_{2^{32}}$, case II

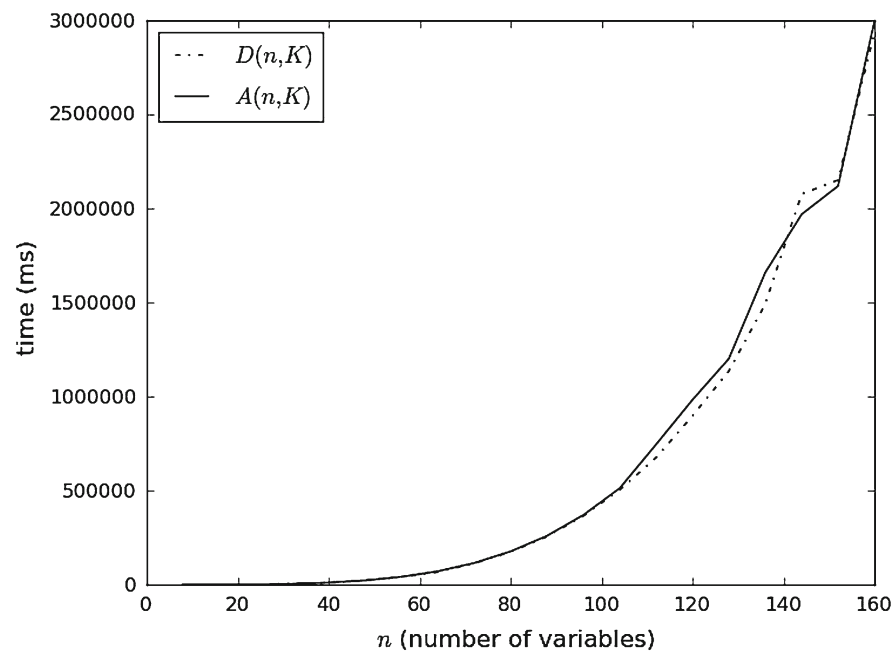

Fig. 8 Public key generation time for fixed password length (64), $K = F_{2^{32}}$, case III

(2) Recall, that a Boolean ring B_m is the Cartesian power $\mathbb{F}_2^m$ of the finite field $\mathbb{F}_2$, i.e a vector space over $\mathbb{F}_2$. We can generalize this example simply by consideration of mth Cartesian power R^m of general commutative ring R.

We can generalize the encryption map $T_n(D(\mathbb{K}), R, \tau_1, \tau_2)$ ($T_n(A(\mathbb{K}), R, \tau_1, \tau_2)$ associated with the family of graphs of large girth $D(n, K)$(or family $A(n, K)$ of graphs with large cycle indicator) via wider choice of linear transformations of the module $\mathbb{K}^n$. We assume, that maps are corresponding to the password $\alpha_1, \alpha_2, \ldots, \alpha_s$ where $\alpha_i + \alpha_{i+1} \in M$, $i = 1, 2, \ldots, s$ and M is a subset of K such that multiplicative closure of M does not contain zero.

The following statement the reader can find in [40].

Proposition 1 *Maps $T_n(D(\mathbb{K}), R, \tau_1, \tau_2)$ and $T_n(A(\mathbb{K}), R, \tau_1, \tau_2)$, where R is a finite commutative ring, $p(x) \in R[x]$, $\mathbb{K} = R[x]/p(x)$ and $\mathbb{K} = R^m$, are cubical maps of R^{mn} to itself.*

7 Conclusion

Results of computer simulation show that multivariate cryptosystem corresponding to family of graphs $A(n, F_q)$, $q = 2^i$, $i = 8, 16, 32, 64$ have a better density (number of monomial expressions with nonzero coefficients) in the comparison with algorithms based on $D(n, F_q)$, $q = 2^i$, $i = 8, 16, 32, 64$. Same is true for generalised encryptions of previous proposition in the case $R = F_2$, $K = F_q$, $q = 2^i$, $i = 8, 16, 32, 64$. Surprisingly the results of time evaluation of the process of public key generations are very similar in both cases ($A(n, F_q)$ and $D(n, F_q)$).

References

1. Bien, F.: Constructions of telephone networks by group representations. Notices Am. Math. Soc. **3**, 5–22 (1989)
2. Bollobás, B.: Extremal Graph Theory. Academic Press, London (1978)
3. Boudelioua, I., AlRaissi, M., Touzene, A., Ustimenko, V.: Performance of Algebraic graphs based streamciphers using large finite fields. Annalles UMCS Informatica AI X **1**(2), 8193 (2011)
4. Dieudonné, J.: La géométrie des groupes classiques, Ergebnisse der Mathematik und ihrer Grenzgebiete (N.F.), Heft 5. Springer, Berlin (1970)
5. Chistov, A.L.: An improvement of the complexity bound for solving systems of polynomial equations. Zapisky Nauchnych Seminarov POMI **390**, 299–306 (2011)
6. Guinand, P., Lodge, J.: Tanner Type codes arising from large girth graphs. In: Proceedings of the 1997 Canadian Workshop on Information Theory (CWIT 97), Toronto, pp. 57 (1997)
7. Guinand, P., Lodge, J.: Graph theoretic construction of generalized product codes, p. 111. In: Proceedings of the 1997 IEEE International Symposium on Information Theory (ISIT '97), Ulm, June 29–July 4 (1997)
8. Kim, J.L., Peled, U.N., Perepelitsa, I., Pless, V., Friedland, S.: Explicit construction of families of LDPC codes with no 4 cycles. IEEE Trans. Information Theory **50**(10), 2378–2388 (2004)
9. Klisowski, M., Romańczuk, M., Ustimenko, V.: On the implementation of cubic public keys based on new family of algebraic graphs. Annales UMCS Informatica AI XI **2**, 127–141 (2011)
10. Klisowski, M., Ustimenko, V.: On the implementation of public keys algorithms based on algebraic graphs over finite commutative rings. International Multiconference on Computer Science and Informational Technology, Wisla, Poland, CANA Proceedings, pp. 303–308 (2010)
11. Klisowski, M., Ustimenko, V.: On the implementation of cubic public keys based on algebraic graphs over the finite commutative rings and their symmetries. Albanian J. Math. **5**(3), 139–149 (2011)
12. Klisowski, M., Ustimenko, V.: On the implementation of cubic public keys based on algebraic graphs over the finite commutative ring and their symmetries. In: MACIS 2011: Fourth International Conference on Mathematical Aspects of Computer and Information Sciences, Beijing (2011)
13. Klisowski, M., Ustimenko, V.: On the implementation of multivariate cryptosystem over the boolean ring Annalles UMCS Informatica (to appear)
14. Koblitz, N.: Algebraic aspects of cryptography. In: Algorithms and Computation in Mathematics, vol. 3. Springer, Berlin (1998)
15. Kotorowicz, S., Ustimenko, V.: On the implementation of cryptoalgorithms based on algebraic graphs over some commutative rings, Condens. Matter Phys. **11**, no. 2(54), 347–360 (2008)
16. Kotorowicz, J.S., Ustimenko, V., Romańczuk, U.: On the implementation of stream ciphers based on a new family of algebraic graphs, pp. 485–490. In: Proceedings of the Conference CANA, FedSCIS, IEEE Computer Society Press (2012)
17. Lazebnik, F., Ustimenko, V.A.: New Examples of graphs without small cycles and of large size. Eur. J. Combin. **14**, 445–460 (1993)

18. Lazebnik, F., Ustimenko, V.: Explicit construction of graphs with an arbitrary large girth and of large size. Discrete Appl. Math. **60**, 275–284 (1995)
19. Lazebnik, F., Ustimenko, V.A., Woldar, A.J.: A new series of dense graphs of high girth. Bull. Am. Math. Soc. (N.S.) **32**(1), 73–79 (1995)
20. Margulis, G.: Explicit group-theoretical constructions of combinatorial schemes and their application to the design of expanders and concentrators. J. Probl. Inf. Transm. **24**(1), 3946 (1988)
21. Ore, R.: Graph Theory. Wiley, London (1971)
22. Romańczuk, U., Ustimenko, V.: On the key exchange with new cubical maps based on graphs. Annales UMCS Informatica AI XI **4**, 11–19 (2011)
23. Shaska, T., Ustimenko, V.: On some applications of graph theory to cryptography and turbocoding. Albanian J. Math., vol. 2, no. 3, pp. 249–255. In: Proceedings of the NATO Advanced Studies Institute: New challenges in digital communications' (2008)
24. Shaska, T., Ustimenko, V.: On the homogeneous algebraic graphs of large girth and their applications, Linear Algebra Appl. **430**, no. 7, 1826–1837, Special Issue in Honor of Thomas J. Laffey (2009)
25. Simonovits M.: Extremal graph theory. In: Beineke, L.W., Wilson, R.J. (eds.) Selected Topics in Graph Theory, vol. 2, pp. 161–200. Academic Press, London (1983)
26. Touzene, A., Ustimenko, V.: Graph Based Private Key Crypto System. Int. J. Comput. Res. Nova Science Publisher **13**(4) (2006)
27. Ustimenko, V.: Random Walks on Graphs and Cryptography, Extended abstracts, AMS Meeting, Loisville, March (1998)
28. Ustimenko, V.: Coordinatisation of Trees and their Quotients. In: Voronoi's Impact on Modern Science, vol. 2, pp. 125–152. Kiev, Institute of Mathematics (1998)
29. Ustimenko, V.: CRYPTIM: Graphs as Tools for Symmetric Encryption, vol. 2227, pp. 278–287. Lecture Notes in Computer Science. Springer, Berlin (2001)
30. Ustimenko, V.A.: Graphs with special arcs and cryptography. Acta Applicandae Mathematicae **71**(2), 117–153 (2002)
31. Ustimenko, V.: Maximality of affine group and hidden graph cryptosystems. J. Algebra Discrete Math. **10**, 51–65 (2004)
32. Ustimenko, V.: On the graph based cryptography and symbolic computations, Serdica J. Comput. In: Proceedings of International Conference on Application of Computer Algebra, ACA-2006, Varna, N1 (2007)
33. Ustimenko, V.: On the extremal graph theory for directed graphs and its cryptographical applications. In: Shaska, T., Huffman, W.C., Joener, D., Ustimenko, V. (eds.) Advances in Coding Theory and Cryptography. Series on Coding Theory and Cryptology, vol. 3, pp. 181–199. World Scientific, New Jersey (2007)
34. Ustimenko, V.: On the extremal regular directed graphs without commutative diagrams and their applications in coding theory and cryptography, Albanian J. Math. **1**(4) Special issue on algebra and computational algebraic geometry (2007)
35. Ustimenko, V.A.: Linguistic dynamical systems, graphs of large girth and cryptography. J. Math. Sci. Springer **140**(3), 412–434 (2007)
36. Ustimenko, V.: Algebraic groups and small world graphs of high girth. Albanian J. Math. **3**(1), 25–33 (2009)
37. Ustimenko, V.: On the cryptographical properties of extremal algebraic graphs, Algebraic Aspects of Digital Communications. In: Shaska, T., Hasimaj, E. (eds.) NATO Science for Peace and Security Series-D: Information and Communication Security, vol. 24, pp. 256–281. IOS Press, July (2009)
38. Ustimenko, V.: On extremal graph theory and symbolic computations. Dopovidi Ukr. Acad. Sci. (to appear)
39. Ustimenko, V., Kotorowicz, J.: On the properties of stream ciphers based on extremal directed graphs. In: Chen, R.E. (ed.) Cryptography Research Perspective, pp. 125–141. Nova Science Publishers, New York, April (2009)
40. Ustimenko, V., Romańczuk, U.: On dynamical systems of large girth or cycle indicator and their applications to multivariate cryptography. In: Artificial Intelligence, Evolutionary Computing and Metaheuristics, In the Footsteps of Alan Turing Series: Studies in Computational Intelligence, vol. 427. Springer, Berlin, June (2012)
41. Ustimenko, V., Romańczuk, U.: On extremal graph theory, explicit algebraic constructions of extremal graphs and corresponding Turing encryption machines. In: Artificial Intelligence, Evolutionary Computing and Metaheuristics, In the Footsteps of Alan Turing Series: Studies in Computational Intelligence, vol. 427. Springer, Berlin, June (2012)
42. Wróblewska, A.: On some applications of graph based public key, Albanian J. Math., vol. 2, no. 3, pp. 229–234. In: Proceedings of the NATO Advanced Studies Institute: New Challenges in Digital Communications (2008)