Annales UMCS Informatica AI XII, 3 (2012) 89–106
DOI: 10.2478/v10065-012-0029-8

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

On the family of cubical multivariate cryptosystems based on the algebraic graph over finite commutative rings of characteristic 2.

Urszula Romańczuk[1*], Vasyl Ustimenko[1,2†]

[1] *Institute of Mathematics, Maria Curie-Sklodowska University, pl. M. Curie-Skłodowskiej 1, 20-031 Lublin, Poland*
[2] *Institute of Telecommunications and Global Information Space, Kiev, National Academy of Science of Ukraine Chokolovsky Boulevard 13, Kiev, Ukraine*

Abstract – The family of algebraic graphs $A(n;\mathbb{K})$ defined over the finite commutative ring $\mathbb{K}$ were used for the design of different multivariate cryptographical algorithms (private and public keys, key exchange protocols). The encryption map corresponds to a special walk on this graph. We expand the class of encryption maps via the use of an automorphism group of $A(n,\mathbb{K})$. In the case of characteristic 2 the encryption transformation is a Boolean map. We change finite field for the commutative ring of characteristic 2 and consider some modifications of algorithm which allow to hide a ground commutative ring.

1 Introduction

Multivariate cryptography in the narrow sense (see[**1**]) is the generic term for asymmetric cryptographic primitives based on the 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. The algorithm of finding a solution of the multivariate polynomial equations system is proven to be NP-Hard or NP-Complete. That is why these schemes are often considered to be good candidates for the post-quantum cryptography, once quantum computers can break the current schemes. Today multivariate quadratics could be used only to

*urszula_romanczuk@yahoo.pl
†vasyl@hektor.umcs.lublin.pl

build signatures. This definition leads to several questions: Why is a finite field, not a commutative ring used? Why are quadratics so important?

We define multivariate cryptography as the studies of cryptosystems based on the special regular automorphism f of the algebraic variety $M_n(\mathbb{K})$ of dimension n in a sense of Zarisski topology over the finite commutative ring $\mathbb{K}$. An example of algebraic variety is a free module $\mathbb{K}^n$ which is simply a Cartesian product of n copies of $\mathbb{K}^n$ into itself. Regular automorphism is a bijective polynomial map of $M_n(\mathbb{K})$ onto itself such that f^{-1} is also a polynomial map. Elements of $\mathbb{K}^n$ can be identified with strings $(x_1, x_2, \ldots, x_n)$ in the alphabet $\mathbb{K}$, a nonlinear map f of the restricted degree d can be used as a public rule if the key holder (Alice) knows the secret decomposition of f into that of special maps $f_1, f_2, \ldots, f_s$ with known inverse maps ${f_i}^{-1}$. So, she can decrypt by the consecutive application of ${f_s}^{-1}, f_{s-1}^{-1}, \ldots, {f_1}^{-1}$. Notice, that the 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. Free module $\mathbb{K}^n$ can be changed for the family of varieties $M_n(\mathbb{K})$, $n = 1, 2, \ldots$, the commutative ring can be treated as an alphabet, the element $v \in M_n(\mathbb{K})$ as a "potentially infinite" plaintext, the parameter n as a measurement of variety size.

The complexity of the best general algorithms for the solution of nonlinear system of equations of the kind $f(x) = y$, $x, y \in \mathbb{K}^n$ equals $d^{0(n)}$ (see recent papers [**2**], [**3**]). One can use the Gröbner basis, the Gauss elimination method or alternative options for the investigation of the system. 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 a large order. Notice that one of the first attempts to create a workable multivariate cryptosystem was proposed by Imai and Matsumoto (see [**4**] and [**1**] for the historical survey in the area). They used the 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 the affine maps (of degree 1) and f_2 is a Frobenius automorphism. Cryptanalysis by J. Patarin for the scheme can be found in [**5**], [**6**], the history of its various modifications goes on (see, for instance survey in [**1**]). We have to notice that the failure of this cryptosystem is not a surprise for specialists in algebra. Despite its formal quadratic appearance the Frobenius automorphism is quite close to linear maps (in his known book [**7**] J.Diedonne uses the 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 [**8**], [**9**] and further references) for the creation of nonlinear maps of pseudorandom nature. We will study some properties of graph base public key, private key and key exchange algorithms, which were proposed in [**10**], [**11**], [**9**], [**12**]. Some results of implementation of this method can be found in [**10**], [**11**]. Some results about extremal properties of the corresponding graphs and relations with cryptographical algorithms based on the algebraic graphs over the finite commutative rings are included in [**13**]. In our paper we will use special commutative rings $\mathbb{K}$ of characteristic 2, which are algebraic extensions of finite field $\mathbb{F}_2$. We assume that the addition in the ring is usually the addition of m -

dimensional free module $\mathbb{K}^m$ over $\mathbb{F}_2$ and the multiplication of vectors $(x_1, x_2, \ldots, x_m)$ and $(y_1, y_2, \ldots, y_m)$ can be computed as $(f_1, f_2, \ldots, f_m)$, where f_i, $i = 1, 2, \ldots, m$ are the boolean functions in the variables x_j, y_j, $j = 1, 2, \ldots m$ in a special basis.

Some examples of the finite ring of characteristic 2:

(i) Boolean ring B_m: $B_m = F_{2^m}$ with the multiplication
$$(x_1, x_2, \ldots, x_m)(y_1, y_2, \ldots, y_m) = (x_1y_1, x_2y_2, \ldots, x_my_m),$$

(ii) commutative ring $\mathbb{K} = \mathbb{F}_2[x]/p(x)$, where $p(x)$ is a polynomial from $\mathbb{F}_2[x]$ of degree m. If $p(x)$ is irreducible, then $\mathbb{K}$ is a finite field $\mathbb{F}_q$ of characteristic 2 containing 2^m elements. In the case $p(x) = x^m$ and natural base 1, x, x^2, ... ,x^{m-1} the multiplication in $\mathbb{K}$ is a usual polynomial multiplication with the specialization $x^i = 0$ for $i = m$, $m + 1$, ..., $2m - 2$. We denote this ring by N_m.

It is clear that in the ring N_m or the case of Boolean ring B_m we have really "fast" multiplication.

In Section 2 we introduce some definitions needed to describe our algorithms. In Section 3 we recall and define some properties of the family of algebraic graphs $A(n, \mathbb{K})$ over a general commutative ring $\mathbb{K}$, in the case $\mathbb{K} = \mathbb{F}_q$ we have $A(n, \mathbb{K}) = A(n, q)$ and define the double directed graphs $DA(n, \mathbb{K})$ of the bipartite graphs $A(\mathbb{K})$. In section 4 we present the groups automorphism of these graphs. In Section 5, we show how to generate the bijective Boolean transformation based on the graphs $A(n, \mathbb{K})$ and $DA(n, \mathbb{K})$ over the finite commutative ring $\mathbb{K}$ with char$\mathbb{K} = 2$ from the above mentioned class of rings.

We formulate some properties of the generated boolean functions related to cryptographical applications.

In Section 6 we present the multivariate public key cryptosystem using the results from the previous sections.

Let us use traditional characters in Cryptography: Alice is the holder of the key, Bob - the public user (see **[5]**).

2 Graph theoretical preliminaries and some open problems

The missing definitions of graph-theoretical concepts in the case of simple graphs which appears in this paper can be found in **[14]**, **[15]**.

All graphs under consideration are *simple graphs*, i. e. undirected without loops and multiple edges. Let $V(\Gamma)$ and $E(\Gamma)$ denote the set of vertices and the set of edges of Γ, respectively. $|V(\Gamma)|$ is called the *order* of Γ, and $|E(\Gamma)|$ is called the *size* of G. A path in Γ is called *simple path* if all its vertices are distinct. When it is convenient, we shall identify Γ with the corresponding antireflexive binary relation on $V(\Gamma)$, i.e. $E(\Gamma)$ is a subset of $V(\Gamma) \times V(\Gamma)$. A graph Γ is *bipartite* if its vertices can be partitioned into two sets in such a way that no edge joins two vertices in the same set.

The *length of a path* is a number of its edges. The *girth* of a graph Γ, denoted by $g = g(\Gamma)$ is the length of the shortest cycle in Γ.

Let $g_x = g_x(\Gamma)$ be the length of the minimal cycle through the vertex x from the set $V(\Gamma)$ of vertices in graph Γ. We refer to

$$\mathrm{Cind}(\Gamma) = \max\{g_x,\ x \in V(\Gamma)\}$$

as *cycle indicator* of the graph Γ.

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

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

Recall, that a family of regular graphs Γ_i of degree k_i and increasing order v_i is the *family of graphs of large girth* if

$$g(\Gamma_i) \geq c\log_{\mathrm{k_i}}(v_i)$$

for an independent constant c, $c > 0$. This family plays an important role in Extremal Graph Theory, Theory of LDPC codes and Cryptography **[16]**,**[9]**, **[17]**. The family of graphs of a large girth of bounded degree is hard to be constructed. This fact is a serious motivation for the studies of infinite families of graphs of a large cycle indicator, which are generalisations of families of graphs of a large girth.

We refer to a family of regular simple graphs Γ_i of degree k_i and order v_i as a *family of graphs of a large cycle indicator*, if

$$\mathrm{Cind}(\Gamma_i) \geq c\log_{\mathrm{k_i}}(v_i)$$

for an independent constant c, $c > 0$. We refer to the maximal value of c satisfying the above mentioned inequality as a *speed of growth* of the girth indicator for the family of graphs Γ_i.

3 The algebraic graphs $A(n, \mathbb{K})$ over a finite commutative ring $\mathbb{K}$

In papers **[18]**, **[19]** were discussed the importance of finite automata related to the algebraic graph $B(S, \mathbb{K})$ over the commutative ring $\mathbb{K}$ defined by the system S of quadratic equations for the variety $P_n \cup L_n$, $P_n = \mathbb{K}^n$, $L_n = \mathbb{K}^n$ in the following manner.

The *point* $(x_1, x_2, \ldots, x_n)$ and *line* $[y_1, y_2, \ldots, y_n]$ are connected by an edge if and only if the following system S of relations holds.

$$\begin{aligned} &y_2 - x_2 = x_1 y_1, \\ &y_j - x_j = x_{k_j} y_{l_j},\ k_j < j, l_j < j, j = 3, 4, \ldots, n. \end{aligned}$$

Such graphs over fields play an important role in the theory of geometries associated with Simple Lie Algebras (see **[20]** and further references).

In this paper we will use the family of graphs $A(n, \mathbb{K})$. We can write the equations as follows;

$$\begin{aligned} y_2 - x_2 &= y_1 x_1, \\ y_3 - x_3 &= x_1 y_2, \\ y_4 - x_4 &= y_1 x_3, \\ y_5 - x_5 &= x_1 y_4, \\ &\dots \end{aligned} \tag{1}$$

with the last equation $y_n - x_n = y_1 x_{n-1}$, in the case of n even or the last equation $y_n - x_n = x_1 y_{n-1}$, in the case of n odd. So, $A(n, \mathbb{K})$ is a graph of the kind $B(S, \mathbb{K})$. We use the notation $A(n, q)$ for the graph $A(n, \mathbb{F}_q)$ over the finite field $\mathbb{F}_q$.

Another example is a family of Wenger graphs $W(n, \mathbb{K})$ defined by the system of equations

$$\begin{aligned} y_1 - x_1 &= x_1 y_1, \\ y_2 - x_2 &= x_1 y_2, \\ &\dots \\ y_n - x_n &= x_1 y_{n-1}. \end{aligned}$$

As it was proven in **[21]** for the fixed $\mathbb{K} = \mathbb{F}_q$ the family $W(n, \mathbb{K})$ is the family of small world graphs without small cycles. The stream cipher based on the Wenger graphs was proposed in **[21]**.

Historically, the graph $A(n, \mathbb{K})$ appears as homomorphic images of the graphs $D(n, K)$ or $CD(n, \mathbb{K})$, defined via the root system of Lie Algebra $\tilde{A}_1$ **[20]**. Positive roots of this system can be identified with the formal pairs (i, i), $(i+1, i)$, and $(i, i+1)$, where $i = 1, 2, \dots$ (see **[20]**, **[12]** and further references). So, we can use double indices in the definition of our graphs. First of all we define an infinite family of graphs $A(\mathbb{K})$.

Let P and L be two copies of a infinite-dimensional free module $\mathbb{K}^{\mathbb{N}}$, where $\mathbb{K}$ is the field commutative ring and $\mathbb{N}$ is the set of positive integer numbers.The elements of P will be called *points* and those of L *lines*. To distinguish points from lines we use parentheses and brackets. If $x \in V$, then $(x) \in P$ and $[x] \in L$. It will be also advantageous to adopt the notation for coordinates of points and lines. So, we take the following notation

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

The elements of P and L can be thought as infinite ordered tuples of elements from $\mathbb{K}$, 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 the point (p) is incident with the line $[l]$, and we write $(p)I[l]$, if the following relations between their coordinates hold:

$$\begin{aligned} l_{i,i} - p_{i,i} &= l_{1,0} p_{i-1,i} \\ l_{i,i+1} - p_{i,i+1} &= l_{i,i} p_{0,1} \qquad i = 1, 2, \dots. \end{aligned}$$

For each positive integer $n \geq 2$ we obtain an incidence structure (P_n, L_n, I_n) as follows. P_n and L_n are obtained from P and L, respectively, by simply projecting each vector into its n initial coordinates with respect to the above order. The incidence I_n is then defined by imposing the first $n-1$ incidence equations and ignoring all others. The incidence graph corresponding to the structure (P_n, L_n, I_n) is denoted by $A(n, \mathbb{K})$. It is clear, that $A(n, \mathbb{K})$ is a $|\mathbb{K}|$-regular bipartite graph of the order $2|\mathbb{K}|^n$, where $|\mathbb{K}|$ denotes the cardinality of ring $\mathbb{K}$.

For each positive integer $n \geq 2$ we consider the *standard graph homomorphism* ϕ_n of (P_n, L_n, I_n) onto $(P_{n-1}, L_{n-1}, I_{n-1})$ defined as simple projection of each vector from P_n and L_n onto its $n-1$ initial coordinates with respect to the above mentioned order.

To show how interesting are our graphs, we present them in small rings in Figs 1–4 and some of their properties in Table 1. For computer simulation in this paper there were used the Matlab and SAGE.

Table 1. Some properties of graphs $A(n, \mathbb{K})$ over finite rings $\mathbb{K}$ of characteristic 2, e.g. $\mathbb{F}_4$, $\mathbb{F}_8$, B_2 and N_2, respectively.

Properties	$A(2, \mathbb{F}_4)$	$A(2, \mathbb{F}_8)$	$A(2, B_2)$	$A(2, N_2)$
Order	2	128	32	32
Size	64	512	64	64
Density	$\frac{4}{31}$	$\frac{8}{127}$	$\frac{4}{31}$	$\frac{4}{31}$
Diameter	4	4	4	4
Girth	6	6	4	4
Degree	4	8	4	4
Regularity	4	8	4	4
The second largest eigenvalue	2	2.82842...	2.828427...	2.828427...
Is it connected?	true	true	true	true
Is it vertex transitive?	true	true	true	true
Is it hamiltonian?	true	true	true	true
Is it eulerian?	true	true	true	true
Vertex connectivity	4	8	4	4
Edge connectivity	4	8	4	4
Vertex cover	16	64	16	16

We define the *colour function* π for the graph $A(n, \mathbb{K})$ as a projection of tuples $(p) \in P_n$ and $[l] \in L_n$ onto the first coordinate (p) or $[l]$, respectively. So, the set of colours is $\mathbb{K}$.

Let $P_{t,n}$ be the operator of taking the neighbour of point of colour $p_{0,1} + t$

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

of a kind

$$[l] = [p_{0,1} + t, l_{1,1}, l_{1,2}, l_{2,2}, l_{2,3}, \ldots, l_{i,i}, l_{i,i+1}, \ldots],$$

where $n-1$ parameters $l_{1,1}$, $l_{1,2}$, $l_{2,2}$,$l_{2,3}$, …, $l_{i,i}$, $l_{i,i+1}$, … are computed consequently from the equations in the definition of $A(n, \mathbb{K})$. Similarly, $L_{t,n}$ is the operator of taking

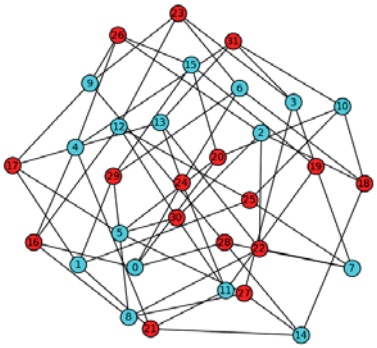

Fig. 1. Graph $A(2,4)$

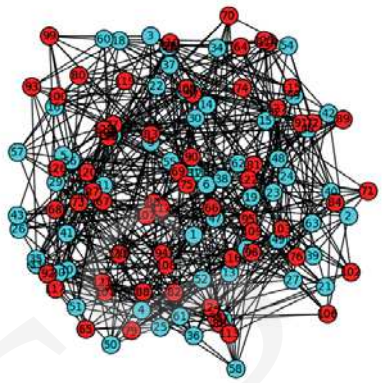

Fig. 2. Graph $A(2,8)$

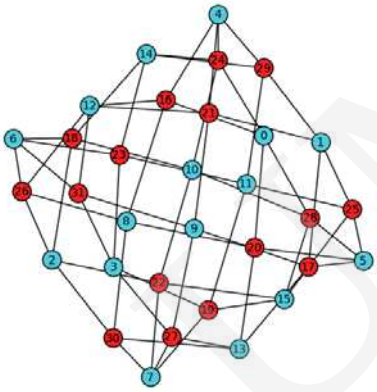

Fig. 3. Graph $A(2,\mathbb{B}_2)$

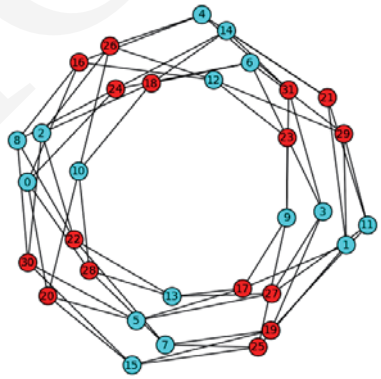

Fig. 4. Graph $A(2,\mathbb{N}_2)$

the neighbour of line of colour $l_{1,0}+t$

$$[l]=[l_{1,0},l_{1,1},l_{1,2},l_{2,2},l_{2,3},\ldots,l_{i,i},l_{i,i+1},\ldots]$$

of a kind

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

where $n-1$ parameters $p_{1,1}$, $p_{1,2}$, $p_{2,2}$, $p_{2,3}$,..., $p_{i,i}$, $p_{i,i+1}$, ... are computed consequently from the above written equations.

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

We use the term *multiplicative set* M for the subset M without zero of the ring $\mathbb{K}$, such that $x \in M, y \in M$ implies $xy \in M$. We say that $\{t_1,t_2,\ldots,t_s\}$ is a *set of multiplicative generators* if its closure under multiplication is a multiplicative set, i. e. it does not contain zero.

The following statement is presented in [**13**].

Theorem 1. Let $\mathbb{K}$ be a finite commutative ring $\mathbb{K}$ with $M \subset \mathbb{K}$, where M is a multiplicative set of cardinality larger than 2. Let us assume that $(t_1, t_2, \ldots, t_k) \in \mathbb{K}^k$. Then

(i) each nonidentical transformation $F_{P_n,t_1,t_2,\ldots,t_k,n}$, which is a composition of maps $P_{t_1,n}$, $L_{t_2,n}$, $\ldots$, $P_{t_{k-1},n}$, $L_{t_k,n}$ for an even number k or $P_{t_1,n}$, $L_{t_2,n}$, $\ldots$, $L_{t_{k-1},n}$, $P_{t_k,n}$ for an odd number k is a cubical map of P_n onto P_n and P_n onto L_n, respectively.

(ii) each nonidentical transformation $F_{L_n,t_1,t_2,\ldots,t_k,n}$, which is a composition of maps $L_{t_1,n}$, $P_{t_2,n}$, $\ldots$, $L_{t_{k-1},n}$, $P_{t_k,n}$ for the set $t_1, t_2, \ldots, t_k$, where k is an even number, or $L_{t_1,n}$, $P_{t_2,n}$, $\ldots$, $P_{t_{k-1},n}$, $L_{t_k,n}$, for an odd number k is a cubical map of L_n onto L_n and L_n onto P_n, respectively.

(iii) for nonidentical transformations $F_{P_n,t_1,t_2,\ldots,t_k,n}$ and $F_{L_n,t_1,t_2,\ldots,t_k,n}$, corresponding to the string $t_1, t_2, \ldots, t_k$ with $t_i + t_{i+1} \in M$,$i = 1, 2, \ldots, k-1$ and $t_1 + t_k \in M$ (k is even), the order goes to infinity with the growth of n.

We say, g is a *cubical map* if it has the form

$$g = (f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n)),$$

where $f_i(x_1, \ldots, x_n)$ are the polynomials of n variables written as the sums of monomials of the kind $x_{i_1}^{n_1} x_{i_2}^{n_2} x_{i_3}^{n_3}$, where $i_1, i_2, i_3 \in \{1, 2, \ldots, n\}$; $n_1,\ n_2,\ n_3 \in \{0, 1, 2, 3\}$, $n_1 + n_2 + n_3 \leq 3$, with the coefficients from $\mathbb{K}$. As we mentioned before the polynomial equations $y_i = f_i(x_1, x_2, \ldots, x_n)$, which are made public, are of degree 3.

From the computer simulation and from the fact, that the family of graphs $A(n, q)$ over the finite field $\mathbb{F}_q$ is neither edge nor vertex transitive, when $n > 5$ and $q \neq 2$, there raises the following problem:

Problem 1. Is the family of graphs $A(n, q)$ of a large girth?

Basically, just two explicit constructions of the families of graphs of a large girth for $k_i = k$, $i = 1, 2, \ldots$ (k is the independent constant) for the general case of arbitrary large k with the unbounded girth are known: the family of Ramanujan graphs with $c = 3/4$ introduced by G. Margulis approximately 40 years after the appearance of Erdős probabilistic construction (see **[22]**); the family of algebraic graphs $D(n, q)$ with $c = 1$ defined over the arbitrary finite field $\mathbb{F}_q$, their connected components $CD(n, q)$ with $c = 3/4$ and regular version of polarity graphs for $D(n, q)$ or $CD(n, q)$ introduced by F. Lazebnik, V. A. Ustimenko and A. J. Woldar (see **[23]**). In 1995 A. Lubotzky **[24]** presented the following known problem which is still open.

Problem 2. Does a family of graphs of large girth with $c > 4/3$ exist?

V. Ustimenko showed the following interesting result:

Theorem 2. **[25]** The family of $A(n, q)$ with $q \neq 2$ is the family of graphs of large cycle indicator with $c = 2$.

The family $A(n,q)$ is the family of graphs of large cycle indicator for which the maximal possible speed of growth $c = 2$. The family of algebraic graphs $A(n,q)$ is not edge transitive, then if Problem 1 had a positive solution, it would have to be $c < 2$ and therefore would be an example of the family of algebraic graphs such that $\mathrm{Cind}(A(n,q)) > g(A(n,q))$.

In the case of $\mathbb{K} = \mathbb{F}_q$ Theorem 3 is the corollary of Theorem 1.

Theorem 3. **[25]** The family of graphs $A(n,q)$, when $q \neq 2$, is the family of small world graphs.

Let $DA(n,\mathbb{K})$ be the double directed graphs of the bipartite graphs $A(\mathbb{K})$. 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 $A(n,\mathbb{K})$. We have the arc e of the 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 $p^1_{1,0} - p^2_{1,0}$.

We consider two families of bijective nonlinear polynomial transformations of the kind:

$$\hat{P}_{t,n+1} : \mathcal{F}_1 \to \mathcal{F}_2$$
$$\hat{L}_{t,n+1} : \mathcal{F}_2 \to \mathcal{F}_1,$$

$n = 3,4,\ldots$, $t \in \mathbb{K}$. It is easy to see that $\mathcal{F}_1 = \mathcal{F}_2 = \mathbb{K}^{n+1}$, so we may treat $\hat{P}_{t,n+1}$ and $\hat{L}_{t,n+1}$ as automorphisms of $\mathbb{K}_q^{n+1}$. Of course, $\hat{L}_{t,n+1}(v)$ is the operator of taking the neighbour of $v \in \mathcal{F}_2$ of colour t belonging to $\mathcal{F}_2$ and $\hat{P}_{t,n+1}(u)$ is the operator of taking the neighbour of $u \in \mathcal{F}_1$ of colour t belonging to $\mathcal{F}_2$.

The following statement is equivalent to the previous theorem.

Theorem 4. **[13]** Let $\mathbb{K}$ be a finite commutative ring $\mathbb{K}$ with $M \subset \mathbb{K}$, where M is a multiplicative set of cardinality larger than 2. Let us assume that $(t_1,t_2,\ldots,t_k) \in \mathbb{K}^k$. Then

(i) each nonidentical transformation $\hat{F}_{\mathcal{F}_1,t_1,t_2,\ldots,t_k,n}$, which is a composition of maps $\hat{P}_{t_1,n+1}$, $\hat{L}_{t_2,n+1}$, $\ldots$, $\hat{P}_{t_{k-1},n+1}$, $\hat{L}_{t_k,n+1}$ for an even number k or $\hat{P}_{t_1,n+1}$, $\hat{L}_{t_2,n+1}$, $\ldots$, $\hat{P}_{t_{k-1},n+1}$, $\hat{L}_{t_k,n+1}$ for an odd number k is a cubical map of $\mathcal{F}_1$ onto $\mathcal{F}_1$ and $\mathcal{F}_1$ onto $\mathcal{F}_2$, respectively.

(ii) each nonidentical transformation $\hat{F}_{\mathcal{F}_2,t_1,t_2,\ldots,t_k,n}$, which is a composition of maps $\hat{L}_{t_1,n+1}$, $\hat{P}_{t_2,n+1}$, $\ldots$, $\hat{L}_{t_{k-1},n+1}$, $\hat{P}_{t_k,n+1}$ for an even number k or composition of maps $\hat{L}_{t_1,n+1}$, $\hat{P}_{t_2,n+1}$, $\ldots$, $\hat{P}_{t_{k-1},n+1}$, $\hat{L}_{A,t_k,n+1}$ for an odd number k is a cubical map of $\mathcal{F}_2$ onto $\mathcal{F}_2$ and $\mathcal{F}_2$ onto $\mathcal{F}_1$, respectively.

(iii) for nonidentical transformations $\hat{F}_{\mathcal{F}_1,t_1,t_2,\ldots,t_k,n+1}$ and $\hat{F}_{\mathcal{F}_2,t_1,t_2,\ldots,t_k,n+1}$ corresponding to the string $t_1,t_2,\ldots,t_k$ with $t_i + t_{i+1} \in M$, $i = 1,2,\ldots,k-1$ and $t_1 + t_k \in M$ (k is even), the order goes to infinity with the growth of n.

4 A group of automorphisms of an infinite graph over the commutative ring $\mathbb{K}$

Let us introduce a group of automorphisms of infinite graph $A(\mathbb{K})$ over the commutative ring $\mathbb{K}$:

$$G =< \xi^a, \xi^b_{(1,0)},\ \ \xi^c_{(1,1)},\ \xi^d_{(j,j)},\ j = 2,3,\dots\ \ a,b,c,d \in \mathbb{K} >$$

generated by the maps ξ^a, $\xi^b_{(1,0)}$, $\xi^c_{(1,1)}$, $\xi^d_{(j,j)}$ defined below.

The map ξ^a changes every coordinate of a point (p) and a line $[l]$ as follows:
$p_{0,1} \to ap_{0,1},\ p_{i,i} \to a^{2i}p_{i,i}, p_{i,i+1} \to a^{2i+1}p_{i,i+1},\ \ i = 1,2,\dots$
$l_{1,0} \to al_{1,0},\ l_{i,i} \to a^{2i}l_{i,i},\ l_{i,i+1} \to a^{2i+1}l_{i,i+1},\ \ i = 1,2,\dots.$

The map $\xi^b_{(1,0)}$ changes every coordinate of a point (p) and a line $[l]$ as follows:
$p_{0,1} \to p_{0,1},\ \ p_{i,i} \to p_{i,i} - bp_{i-1,i},\ \ p_{i,i+1} \to p_{i,i+1},\ \ i = 1,2,\dots$
$l_{1,0} \to l_{1,0} + b,\ \ l_{i,i} \to l_{i,i},\ \ l_{i,i+1} \to l_{i,i+1},\ \ i = 1,2,\dots.$

The map $\xi^c_{(1,1)}$ changes every coordinate of a point (p) and a line $[l]$ as follows:
$p_{0,1} \to p_{0,1},\ \ p_{1,1} \to p_{1,1} + c,\ \ p_{1,2} \to p_{1,2} - cp_{0,1}$
$p_{i,i} \to p_{i,i} - cp_{i-1,i-1},\ \ p_{i,i+1} \to p_{i,i+1} - cp_{i-1,i},\ \ i = 2,3,\dots$
$l_{1,0} \to l_{1,0},\ \ l_{1,1} \to l_{1,1} + c,\ \ l_{1,2} \to l_{1,2},$
$l_{i,i} \to l_{i,i} - cl_{i-1,i-1},\ l_{i,i+1} \to l_{i,i+1} - cl_{i-1,i},\ \ i = 2,3,\dots$

The map $\xi^d_{(j,j)}$ changes every coordinate of a point (p) and a line $[l]$ as follows:
$p_{0,1} \to p_{0,1},\ \ p_{i,i} \to p_{i,i},\ p_{i,i+1} \to p_{i,i+1},\ \ \ i = 1,2,\dots,j-1,$
$p_{j,j} \to p_{j,j} + d,\ \ p_{j,j+1} \to p_{j,j+1} - dp_{0,1},$
$p_{k,k} \to p_{k,k} - dp_{k-j,k-j},\ \ p_{k,k+1} \to p_{k,k+1} - dp_{0,1},\ \ k = j+1, j+2,\dots$
$l_{1,0} \to l_{1,0},\ \ l_{i,i} \to l_{i,i}, l_{i,i+1} \to l_{i,i+1},\ \ \ i = 1,2,\dots,j-1,$
$l_{j,j} \to l_{j,j} + d,\ \ l_{j,j+1} \to l_{j,j+1},$
$l_{k,k} \to l_{k,k} - dl_{k-j,k-j},\ \ l,\ \ l_{k,k+1} \to l_{k,k+1},\ k = j+1, j+2,\dots.$

Automorphism of the infinite simple graph $A(\mathbb{K})$, listed above, can be naturally considered as an automorphism of double directed graph $DA(\mathbb{K})$. Such maps generate a group

$$\hat{G} =< \hat{\xi}^a, \hat{\xi}^b_{(1,0)},\ \hat{\xi}^c_{(1,1)},\ \hat{\xi}^d_{(j,j)},\ j = 2,3,\dots,\ a,b,c \in \mathbb{K} >$$

where $\hat{\xi}^a$, $\hat{\xi}^b_{(1,0)}$, $\hat{\xi}^c_{(1,1)}$, $\hat{\xi}^d_{(j,j)}$ are given by the rules

$$([l],(p))^{\hat{\xi}^a} = ([l]^{\xi^a},(p)^{\xi^a}), \qquad [[l],(p)]^{\hat{\xi}^a} = ([l]^{\xi^a},(p)^{\xi^a}),$$
$$([l],(p))^{\hat{\xi}^t_\alpha} = ([l]^{\xi^t_\alpha},(p)^{\xi^t_\alpha}), \qquad [[l],(p)]^{\hat{\xi}^t_\alpha} = ([l]^{\xi^t_\alpha},(p)^{\xi^t_\alpha)})$$

where $\alpha \in \{(0,1),(m,m), m = 1,2,\dots\}$, and t is equal to b, c and d, respectively.

5 Boolean transformation corresponding to the graph $A(n,\mathbb{K})$.

For simplicity we use the definition of the graph $A(n,\mathbb{K})$ given by the set of equations (1) over any commutative ring $\mathbb{K}$. Its clear that in the case $\mathbb{K}$ is a finite commutative ring of characteristic 2, the maps $F_{P_n,t_1,n}$ and $F_{L_n,t'_1,n}$ are the bijective Boolean transformations of the n-dimensional free module $\mathbb{K}^n$. We have

$$F_{P_n,t_1,n}((x_1,x_2,\dots,x_n)) = P_{t_1,n}((x_1,x_2,\dots,x_n)) = [f^{(1)}_{1,t_1}(x_1),\dots,f^{(1)}_{n,t_1}(x_1,\dots,x_n)]$$

where

$$\begin{aligned}
&f^{(1)}_{1,t_1}(x_1) = x_1 + t_1,\\
&f^{(1)}_{2,t_1}(x_1,x_2) = x_2 + x_1^2 + t_1x_1,\\
&f^{(1)}_{2s-1,t_1}(x_1,x_2,\dots,x_{2s-1}) = x_{2s-1} + x_1x_{2s-2} + x_1^2x_{2s-3} + t_1x_1x_{2s-3},\\
&f^{(1)}_{2s,t_1}(x_1,x_2,\dots,x_{2s}) = x_{2s} + x_1x_{2s-1} + t_1x_{2s-1}
\end{aligned}$$

for $s = 2,3,\dots,\lfloor \frac{n}{2} \rfloor$. If n is odd we need to add that

$$f^{(1)}_{n,,t_1}(x_1,\dots,x_n) = x_n + x_1x_{n-1} + x_1^2x_{n-2} + t_1x_1x_{n-2}.$$

And for the transformation $F_{L_n,t'_1,n}$ we obtain

$$F_{L_n,t'_1,n}([y_1,y_2,\dots,y_n]) = L_{t'_1,n}([y_1,y_2,\dots,y_n]) = (g^{(1)}_{1,t'_1}(y_1),\dots,g^{(1)}_{n,t'_1}(y_1,\dots,y_n)),$$

where

$$\begin{aligned}
&g^{(1)}_{1,t'_1}(y_1) = y_1 + t'_1,\\
&g^{(1)}_{2,t'_1}(y_1,y_2) = y_2 - y_1^2 - t'_1y_1,\\
&g^{(1)}_{2s-1,t'_1}(y_1,y_2,\dots,y_{2s-1}) = y_{2s-1} - y_1y_{2s-2} - t'_1y_{2s-2},\\
&g^{(1)}_{2s,t'_1}(y_1,y_2,\dots,y_{2s}) = y_{2s} - y_1y_{2s-1} + y_1^2y_{2s-2} + t'_1y_1y_{2s-2}
\end{aligned}$$

for $s = 2,3,\dots,\lfloor \frac{n}{2} \rfloor$. If n is odd we need to add that

$$g^1_{n,t'_1}(y_1,\dots,y_n,t_1) = y_n - y_1y_{n-1} - t'_1y_{n-1}.$$

Of course, $\lfloor x \rfloor = \text{floor}(x)$ is the largest integer, not larger than x. So, we have:

$$\deg f^{(1)}_{i,t_1} = \begin{cases} 1 & i=1\\ 2 & i=2\\ 3 & i=2s-1\\ 2 & i=2s, \end{cases} \quad \deg g^{(1)}_{i,t'_1} = \begin{cases} 1 & i=1\\ 2 & i=2\\ 2 & i=2s-1\\ 3 & i=2s, \end{cases}$$

where $s = 2,3,\dots,\lfloor \frac{n}{2} \rfloor$. If n is odd, then $\deg f^{(1)}_{n,t_1} = 3$ and $\deg g^{(1)}_{n,t'_1} = 2$.

The compositions $F_{P,t_1,t_2,n}$, $F_{L,t'_1,t'_2,n}$ of the maps $P_{t_1,n}$, $L_{t_2,n}$ and $L_{t'_1,n}$ $P_{t'_2,n}$, respectively, are the bijective transformation on the n-dimensional free module $\mathbb{K}^n$. We

have

$$F_{P,t_1,t_2,n}((x_1,x_2,\ldots,x_n)) = P_{t_1,n}L_{t_2,n}((x_1,x_2,\ldots,x_n)) = \\ = (f^{(2)}_{1,t_1,t_2}(x_1), f^{(2)}_{1,t_1,t_2}(x_1,x_2),\ldots,f^{(2)}_{n,t_1,t_2}(x_1,\ldots,x_n))$$

where

$$f^{(2)}_{1,t_1,t_2}(x_1) = x_1 + t_1 + t_2,$$
$$f^{(2)}_{2,t_1,t_2}(x_1,x_2) = x_2 - (t_1+t_2)(x_1+t_1),$$
$$f^{(2)}_{2s-1,t_1,t_2}(x_1,x_2,\ldots,x_{2s-1}) = x_{2s-1} - (t_1+t_2)[x_{2s-2} + x_1x_{2s-3} + t_1x_{2s-3}],$$
$$f^{(2)}_{2s,t_1,t_2}(x_1,x_2,\ldots,x_{2s}) = x_{2s} + (t_1+t_2)(x_1+t_1)[x_{2s-2} + x_1x_{2s-3} + t_1x_{2s-3}]$$

for $s = 2,3,\ldots,\lfloor \frac{n}{2} \rfloor$. If n is odd we need add that

$$f^{(2)}_{n,,t_1,t_2}(x_1,\ldots,x_n) = x_n - (t_1+t_2)[x_{n-1} + x_1x_{n-2} + t_1x_{n-2}].$$

And for the transformation $F_{L,t'_1,t'_2,n}$ of the composition of maps we obtain

$$F_{L,t_1,t_2,n}((x_1,x_2,\ldots,x_n)) = L_{t'_1,n}P_{t'_2,n}([x_1,x_2,\ldots,x_n]) = \\ = [(g^{(2)}_{1,t'_1,t'_2}(y_1), g^{(2)}_{2,t'_1}(y_1,y_2),\ldots,g^{(2)}_{n,t'_1,t'_2}(y_1,\ldots,y_n)),]$$

where

$$g^2_{1,t'_1,t'_2}(y_1) = y_1 + t'_1 + t'_2,$$
$$g^2_{2,t'_1,t'_2}(y_1,y_2) = y_2 + (t'_1+t'_2)(y_1+t'_1),$$
$$g^2_{3,t'_1,t'_2}(y_1,y_2,y_3) = y_3 + (t'_1+t'_2)(y_1+t'_1)^2,$$
$$g^2_{4,t'_1,t'_2}(y_1,y_2,y_3,y_4) = y_4 + (t'_1+t'_2)(y_3 - y_1y_2 - t'_1y_2),$$
$$g^2_{2s-1,t'_1,t'_2}(y_1,y_2,\ldots,y_{2s-1}) = y_{2s-1} + (t'_1+t'_2)(y_1+t'_1)[y_{2s-3} - y_1y_{2s-4} - t'_1y_{2s-4}],$$
$$g^2_{2s,t'_1,t'_2}(y_1,y_2,\ldots,y_{2s}) = y_{2s} + (t'_1+t'_2)[y_{2s-1} - y_1y_{2s-4} - t'_1y_{2s-2}]$$

for $s = 3,4,\ldots,\lfloor \frac{n}{2} \rfloor$. If n is odd we need add that

$$g^{(2)}_{n,t'_1,t'_2}(x_1,\ldots,x_n,t_1) = y_n + (t'_1+t'_2)(y_1+t'_1)[y_{n-2} - y_1y_{n-3} - t'_1y_{n-3}].$$

So, we have

$$\deg f^{(2)}_i = \begin{cases} 1 & i=1 \\ 1 & i=2 \\ 2 & i=2s-1, \\ 3 & i=2s, \end{cases} \quad \deg g^{(2)}_i = \begin{cases} 1 & i=1,2 \\ 2 & i=3,4 \\ 3 & i=2r-1 \\ 2 & i=2r, \end{cases}$$

where $s = 2,3,\ldots,\lfloor \frac{n}{2} \rfloor$ and $r = 3,4,\ldots,\lfloor \frac{n}{2} \rfloor$. If n is odd, then $\deg f^{(2)}_{n,t_1,t_2} = 2$ and $\deg g^{(2)}_{n,t'_1,t'_2} = 3$.

Mathematical induction can be used to prove the following statement.

Theorem 5. Let $\mathbb{K}$ be a finite commutative ring $\mathbb{K}$ of characteristic 2 with $M \subset \mathbb{K}$, where M is a multiplicative set of cardinality larger than 2. Let us assume that $t = (t_1, t_2, \ldots, t_k) \in \mathbb{K}^k$. Then

(i) each nonidentical Boolean transformation of the kind

$$F_{P_n,t,n} = (f_{1,t}^{(k)}(x_1), f_{1,t}^{(k)}(x_1, x_2), \ldots, f_{n,t}^{(k)}(x_1, \ldots, x_n))$$

has

$$\deg f_{i,t}^{(k)} = \begin{cases} 1 & i = 1, \\ 2 & i = 2, \\ 3 & i = 2s-1, \\ 2 & i = 2s, \qquad k \text{ is odd} \end{cases} \qquad \deg f_{i,t}^{(k)} = \begin{cases} 1 & i = 1, \\ 1 & i = 2, \\ 2 & i = 2s+1, \\ 3 & i = 2s, \qquad k \text{ is even} \end{cases}$$

where $s = 2, 3, \ldots, \lfloor \frac{n}{2} \rfloor$. If n is odd, then $\deg f_{n,t}^{(k)} = 3$ and $\deg f_{n,t}^{(k)} = 2$, respectively.

(ii) each nonidentical Boolean transformation of a kind

$$F_{L_n,t,n} = (g_{1,t}^{(k)}(x_1), g_{2,t}^{(k)}(x_1, x_2), \ldots, g_{n,t}^{(k)}(x_1, \ldots, x_n))$$

has

$$\deg g_i^{(l)} = \begin{cases} 1 & i = 1, \\ 2 & i = 2, \\ 2 & i = 2s-1, \\ 3 & i = 2s, \qquad k \text{ is odd} \end{cases} \qquad \deg g_i^{(l)} = \begin{cases} 1 & i = 1, 2 \\ 2 & i = 3, 4, \\ 3 & i = 2r-1, \\ 2 & i = 2r, \qquad k \text{ is even} \end{cases}$$

where $s = 2, 3, \ldots, \lfloor \frac{n}{2} \rfloor$ and $r = 3, 4, \ldots, \lfloor \frac{n}{2} \rfloor$. If n is odd, then $\deg g_{n,t}^{(k)} = 2$ and $\deg g_{n,t}^{(k)} = 3$, respectively.

(iii) for the nonidentical Boolean transformations $F_{P_n,t_1,t_2,\ldots,t_k,n}$, $F_{L_n,t_1,t_2,\ldots,t_k,n}$, with $t_i + t_{i+1} \in M$, $t_1 + t_k \in M$ (k is even), the order goes to infinity with the growth of n.

(iv) the inverse maps of nonidentical Boolean transformations $F_{P_n,t_1,t_2,\ldots,t_k,n}$ and $F_{L_n,t_1,t_2,\ldots,t_k,n}$ are $F_{P_n,-t_k,-t_{k-1},\ldots,-t_1,n}$ and $F_{L_n,-t_k,-t_{k-1},\ldots,-t_1,n}$ for k even and $F_{L_n,-t_k,-t_{k-1},\ldots,-t_1,n}$ and $F_{P_n,-t_k,-t_{k-1},\ldots,-t_1,n}$ for k odd, respectively.

(v) each nonidentical Boolean transformation $\hat{F}_{\mathcal{F}_1,t_1,t_2,\ldots,t_k,n}$, $\hat{F}_{\mathcal{F}_2,t_1,t_2,\ldots,t_k,n}$ is a cubical map, and if k is even and $t_i + t_{i+1} \in M$, $i = 1, 2, \ldots, k-1$, $t_1 + t_k \in M$, then the order of these maps goes to infinity with the growth of n,

(vi) the inverse maps of nonidentical Boolean transformations $\hat{F}_{\mathcal{F}_1,t_1,t_2,\ldots,t_k,n+1}$ and $\hat{F}_{\mathcal{F}_2,t_1,t_2,\ldots,t_k,n+1}$ are $\hat{F}_{\mathcal{F}_1,-t_k,-t_{k-1},\ldots,-t_1,n+1}$ and $\hat{F}_{\mathcal{F}_2,-t_k,-t_{k-1},\ldots,-t_1,n+1}$ for k even and $\hat{F}_{\mathcal{F}_2,-t_k,-t_{k-1},\ldots,-t_1,n+1}$ and $\hat{F}_{\mathcal{F}_1,-t_k,-t_{k-1},\ldots,-t_1,n+1}$ for k odd.

Proposition 1. Let be the commutative ring, $t = (t_1, t_2, \ldots, t_k) \in \mathbb{K}^k$. Then

(i) for the nonidentical Boolean transformations $F_{P,t_1,t_2,\ldots,t_k,n}$, $F_{L,t_1,t_2,\ldots,t_k,n}$ and any automorphism $\zeta \in G$ we have

$$\zeta F_{P_n,t_1,t_2,\ldots,t_k,n} = F_{P_n,t_1,t_2,\ldots,t_k,n}\zeta$$
$$\zeta F_{L_n,t_1,t_2,\ldots,t_k,n} = F_{L_n,t_1,t_2,\ldots,t_k,n}\zeta,$$

(ii) for the nonidentical Boolean transformations $\hat{F}_{\mathcal{F}_1,t_1,t_2,\ldots,t_k,n+1}$, $\hat{F}_{\mathcal{F}_2,t_1,t_2,\ldots,t_k,n+1}$ and any automorphism $\hat{\zeta} \in \hat{G}$ we have

$$\hat{\zeta}\hat{F}_{\mathcal{F}_1,t_1,t_2,\ldots,t_k,n+1} = \hat{F}_{\mathcal{F}_1,t_1,t_2,\ldots,t_k,n+1}\hat{\zeta}$$
$$\hat{\zeta}\hat{F}_{\mathcal{F}_2,t_1,t_2,\ldots,t_k,n+1} = \hat{F}_{\mathcal{F}_2,t_1,t_2,\ldots,t_k,n+1}\hat{\zeta}.$$

6 Application of algebraic graphs in Cryptography

In this section we present our multivariate public key cryptosystem using the results from the previous sections. Our cryptosystem will work over the general finite commutative ring $\mathbb{K}$. The plainspace of the algorithm is $\mathbb{K}^n$, the graph theoretical encryption corresponds to a path on the bipartite graph $A(n,\mathbb{K})$ with the partition sets, which are isomorphic to $\mathbb{K}^n$. We can identify the graph $A(n,\mathbb{K})$ with the corresponding symmetric binary relation on the vertex set $\mathbb{K}^n \cup \mathbb{K}^n$. Each neighbour of the point (line) v can be obtained as $u = F_{P_n,t,n}(v)$ ($u = F_{L_n,t,n}(v)$, respectively), $t \in \mathbb{K}$. So, we put the colour t on the arrow between v and u and the colour $-t$ on the reverse arrow between u and v.

For simplicity we assume that the encryption path has even length and the starting vertex is always a point. If the path corresponds to the sequence of colours $t_1, t_2, \ldots, t_k$ and the starting point is v belonging to P_n (L_n, respectively) , then the ending point can be computed as $F_{P_n,t_1,t_2,\ldots,t_k}(v)$ ($F_{L_n,t_1,t_2,\ldots,t_k}(v)$, respectively). We will treat v as a variable (potentially plaintext), using the term *password* for the sequence $(t_1, t_2, \ldots t_k)$ and refering to the map $v \to F_{P_n,t_1,t_2,\ldots,t_k}(v)$ ($v \to F_{L_n,t_1,t_2,\ldots,t_k}(v)$, respectively) as *the encryption map that is based on a simple graph.*

The slightly modified idea is to use the directed graph $DA(n,\mathbb{K})$. Recall that the vertex set of this graph is $\mathbb{K}^{n+1} \cup \mathbb{K}^{n+1}$. Let vertex v be an element of $\mathcal{F}_1$ ($\mathcal{F}_2$, respectively) then v and u are connected by arrow if and only if $u = \hat{P}_{\mathcal{F}_1,t,n+1}(v)$ ($u = \hat{L}_{\mathcal{F}_2,t,n+1}(v)$, respectively) for uniquely determined $t \in \mathbb{K}$. We put the colour t for the arrow from v to u. If the path of even length corresponds to the sequence of colours $t_1, t_2, \ldots, t_k$ and the starting vertex is v from $\mathcal{F}_1$ ($\mathcal{F}_2$, respectively), then the ending point can be computed as $\hat{F}_{\mathcal{F}_1,t_1,t_2,\ldots,t_k}(v)$ ($\hat{F}_{\mathcal{F}_2,t_1,t_2,\ldots,t_k}(v)$, respectively). We refer to the map $v \to \hat{F}_{\mathcal{F}_1,t_1,t_2,\ldots,t_k}(v)$ ($v \to \hat{F}_{\mathcal{F}_2,t_1,t_2,\ldots,t_k}(v)$, respectively) as the *encryption map that is based on the directed graph.*

Let $\mathbb{K}$ be a finite commutative ring $\mathbb{K}$ with $M \subset \mathbb{K}$, where M is a multiplicative set of cardinality larger than 2.

Private-key algorithms. We assume that the two users Alice and Bob share a common password for the simple graph based encryption which is the sequence of colour $t_1, t_2, \ldots, t_s$, where $t_{i+1} - t_i \in M$, $i = 1, \ldots, s-1$ and two affine transformations τ_1, τ_2 from the affine group $AGL(n,\mathbb{K})$ together with the linear automorphism ζ of the graph. Then, they encrypt the plaintext m and obtain the ciphertext c as follows:
$c = \tau_1\zeta F_{P_n,t_1,t_2,\ldots,t_s,n}\tau_2(m)$
The decryption process is as follows: $m = \tau_2^{-1}F^{-1}_{P_n,t_1,t_2,\ldots,t_k,n}\zeta^{-1}\tau_1^{-1}(c)$.

If $\mathbb{K} = \mathbb{F}_q$ and $k < \frac{g(A(n,q))}{2}$, then different keys produce distinct ciphertexts from the chosen plaintext. The same property holds in a more general case of $A(n, \mathbb{K})$, where $\mathbb{K}$ is a finite commutative ring and $t_i + t_{i+1}$, $i = 1, 2, \ldots$ form a set of multiplicative generators, and $k \leq \alpha n$, where the constant α depends on the ring $\mathbb{K}$. As follows from Theorem 1 in the case of $\tau_2 = \tau_1^{-1}$, the order of the encryption map grows to infinity with the growth of parameter n.

The graph $A(n, q)$, $q \neq 2$ is connected. It means that in the case $\mathbb{K} = \mathbb{F}_q$ for the arbitrary pair $v \in \mathbb{F}_q^n$ and $u \in \mathbb{F}_q^n$ and the fixed pair τ_1, τ_2 there is a password t_1, t_2, ..., t_k, such that the corresponding encryption map sends v to u. A small world property holds for $A(n, q)$, it means that we can transform v to u with a rather short password of length k of kind $\beta n + \alpha$, where β and α are the constants.

In the above described algorithm we can change the simple graph based encryption map for the directed graph based map $v \to \hat{F}_{\mathcal{F}_1, t_1, t_2, \ldots, t_k}(v)$ ($v \to \hat{F}_{\mathcal{F}_2, t_1, t_2, \ldots, t_k}(v)$, respectively). In the case of $\tau_2 = \tau_1^{-1}$ and the password $t_1, t_2, \ldots t_k$ of multiplicative generators the order of encryption map will grow with the growth of n.

Both algorithms (stream ciphers) have good mixing properties because the families of graphs $A(n, q)$ are good expanders. In fact, computer experiments demonstrate existence of a large spectral gap in the case of $A(n, \mathbb{K})$ where $\mathbb{K}$ is a small commutative ring. So, change of one character in the plaintext string or in the password leads to the change of 97 percents of symbols of the corresponding ciphertext (see Theorems 1 and 5).

Public-key algorithm. We assume that the password $t_1, t_2, \ldots, t_k$, $t_i + t_{i+1} \in M$ for $i = 1, 2, \ldots$. Alice takes τ_1, τ_2, the sequence $t_1, t_2, \ldots, t_k$ of elements from the commutative ring $\mathbb{K}$, authomorphism $\zeta \in G$ of graph $A(n, \mathbb{K})$. She stores this secret information in a secure way and computes the map

$$f_A = \tau_1 \zeta F_{P_n, t_1, t_2, \ldots, t_k, n} \tau_2$$

in a symbolic way (she can use the packages "Maple" , "Mathematica" or the tools of Computer Algebra for specialists). She gets a public rule, which is a cubical map:

$$\begin{aligned} x_1 &\to f_1(x_1, x_2, \ldots, x_n), \\ x_2 &\to f_2(x_1, x_2, \ldots, x_n), \\ &\ldots, \\ x_n &\to f_n(x_1, x_2, \ldots, x_n), \end{aligned}$$

where f_i are the multivariable polynomials from $\mathbb{K}[x_1, x_2, \ldots, x_n]$. If she uses the string $t_1, t_2, \ldots, t_k$ and the affine maps τ_1, τ_2, such that $t_i + t_{i+1}$, $i = 1, 2, \ldots, k-1$ are the multiplicative generators and $\tau_2 = \tau_1^{-1}$, then the order of cubical transformation is grows with the growth of n.

In the case when k is less than half of $n + 4$ different strings t_1, t_2, ..., t_k lead to distinct symbolic public rules.

Symbolic Diffie-Hellman algorithm. Suppose Alice and Bob want to agree with a key K_{AB}.

1. Alice uses the information on the graph $A(n, \mathbb{K})$. She picks up the string of ring

elements $t_1, t_2, \ldots, t_k$, such that $t_{i+1} - t_i$, $i = 1, \ldots, k-1$ and $t_k - t_1$ from the set of multiplicative generators. She chooses the linear automorphism ζ of the graph $A(n, \mathbb{K})$ and the invertible affine transformation τ of the free module $\mathbb{K}^n$.

The first step Alice computes symbolically $f = \tau\zeta F_{P_n,t_1,t_2,\ldots,t_k,n}\tau^{-1}$. She sends the cubical symbolic map f to Bob. The next step is for Alice to pick a secret integer n_A that she does not reveal to anyone, while at the same time Bob picks an integer n_B that he keeps secret.

2. Alice and Bob use their secret integers (n_A and n_B, respectively) to compute $A = f^{n_A}$ and $B = f^{n_B}$, respectively. Recall, that they use the composition of multivariable map f with itself. After that they exchange these computed cubical transformations.

3. Finally, Alice and Bob again use their secret integers to compute $K_{AB} = B^{n_A} = (f^{n_B})^{n_A} = f^{n_A n_B}$, and $K_{AB} = A^{n_B} = (f^{n_A})^{n_B} = f^{n_A n_B}$, respectively.

Security of the cryptographic algorithms usage is based on the complexity of hard discrete logarithm problem for the group generated by cubical transformations defined by graphs $A(n, \mathbb{K})$ (see Theorems 1 and 5).

Of course, in these algorithms (public key rule and key exchange protocol) we can change the simple graph based map for the directed graph based encryption transformation $v \to \hat{F}_{\mathcal{F}_1,t_1,t_2,\ldots,t_k}(v)$ ($v \to \hat{F}_{\mathcal{F}_2,t_1,t_2,\ldots,t_k}(v)$, respectively) acting on the module $\mathbb{K}^{n+1}$. In the case of $\tau_2 = \tau_1^{-1}$ and the password $t_1, t_2, \ldots t_k$ of multiplicative generators, the order of the encryption map will grow with the growth of n. If $k \leq (n+4)/2$, then different sequences of multiplicative generators produce distinct symbolic maps.

7 On the hidden ring multivariate cryptography

In the case of the ring $\mathbb{K} = \mathbb{F}_2^m$ from the class of commutative rings of characteristic 2 defined in Section 1, each map of $\mathbb{K}^n$ into itself can be treated as a cubical map of the vector space $\mathbb{F}_2^N$ to itself. So the graph based symbolic map F in the previous section ($F_{P_n,t_1,t_2,\ldots,t_k,n}$, $F_{L_n,t_1,t_2,\ldots,t_k,n}$, $\hat{F}_{\mathcal{F}_1,t_1,t_2,\ldots,t_k,n}$ or $\hat{F}_{\mathcal{F}_2,t_1,t_2,\ldots,t_k,n}$) can be written in the form

$$\begin{gathered} x_1 \to f_1(x_1, x_2, \ldots, x_N), \\ x_2 \to f_2(x_1, x_2, \ldots, x_N), \\ \ldots \\ x_N \to f_N(x_1, x_2, \ldots, x_N), \end{gathered}$$

where $N = mn$ in the case of the use of $A(n, \mathbb{K})$ based transformation and $N = m(n+1)$ in the case of the use of $DA(n, \mathbb{K})$.

So, we can consider analogy of algorithms from the previous section over $\mathbb{F}_2$. In the case of *private-key algorithms* and *public-key algorithms* we will combine the written above cubical bijective map F of $\mathbb{F}_2^N$ with two invertible affine transformations τ_1 and τ_2 of N-dimensional vector space over $\mathbb{F}_2$. Notice that the number of options to choose τ_1 is $2^N(2^{N-1})(2^N-2)(2^N-2^2)\ldots(2^N-2^{N-1})$. Recall, that the choice of $\tau_2 = {\tau_1}^{-1}$ will guarantee the growth of the order of encryption map with the growth of parameter N.

We can combine τ_1 with the linear automorphism ζ of the graph $A(n,\mathbb{K})$ or $DA(n,\mathbb{K})$. Notice that ζ will be a linear bijective map of the vector space $\mathbb{F}_2^N$ to itself.

Notice that all nonidentical powers of the encryption map $H = \tau_1\zeta F{\tau_1}^{-1}$ are the cubical Boolean maps. So this can be used for the *Symbolic Diffie-Hellman algorithm.* The correspondents, for example may "compress" the collision public rule $Z = H^{k_Ak_B}$ of the kind $x_1 \to z_1, x_2 \to z_2, \ldots, x_N \to z_N$ (composition of k_Ak_B copies of H) by the application of differential $D = d/d_{x_1} + d/d_{x_2} +, \ldots, +d/d_{x_N}$ three times to each component of the vector $(z_1, z_2, \ldots, z_N)$ to get a numerical string of the length nm or $(n+1)m$ over the field $\mathbb{F}_2$.

8 Conclusions

The modified method allows to hide a ring $\mathbb{K}$ in the definition of graph $A(n,\mathbb{K})$. After you apply, the traces of graph disappear. We have one of the first examples of multivariate cryptosystem over the ring with zero divisors. The case of the Boolean ring B_m is especially important because as the execution is very fast. It is possible to use logic gates and create a hardware device producing an encryption map.

References

[1] Ding J., Gower J. E., Schmidt D. S., Multivariate Public Key Cryptosystems, Springer, Advances in Information Security, 25 (XVIII) (2006): 260.

[2] Lazard D., Thirty years of Polynomial System Solving, and now?, J. Symb. Comput. 44 (3) (2009): 222.

[3] Chistov A. L., An improvement of the complexity bound for solving systems of polynomial equations, Zapisky nauchnych seminarov POMI 390 (2011): 299.

[4] Matsumoto T., Imai H., Public quadratic polynomial-tuples for efficient signatureverification and message-encryption, Eurocrypt '88, Springer-Verlag (1988): 419.

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

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

[7] Dieudonné J., La géométrie des groupes classiques, Ergebnisse der Mathematik und ihrer Grenzgebiete (N.F.) 5 (1970).

[8] Kotulski Z., J. Szczepański J., Discrete chaotic cryptography, Annalen der Physik 6 (1997): 381.

[9] Ustimenko V., On the cryptographical properties of extremal algebraic graphs, Algebraic Aspects of Digital Communications.- NATO Science for Peace and Security Series - D: Information and Communication Security 24 (2009): 256.

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

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

[12] Ustimenko V., Algebraic graphs and security of digital communications, Institute of Computer Science, University of Maria Curie Skłodowska in Lublin (2011): 151; (oppen access book supported by European Social Foundation): http://informatyka.umcs.lublin.pl/files/ustimenko.pdf.

[13] Romańczuk U., Ustimenko V., 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, Springer 427 (2012).

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

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

[16] Huffman W. C., Joener D., Ustimenko V., Shaska T., Advances in Coding Theory and Cryptography, Series on Coding and Cryptology, World Scientific (2007): 398.

[17] Guinand P.S., Lodge J., Tanner Type Codes Arising from Large Girth Graphs, Proceedings of the 1997 Canadian Workshop on Information Theory (CWIT '97), Toronto, Ontario, Canada, June 3-6 (1997): 5.

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

[19] Ustimenko V., Graphs with Special Arcs and Cryptography, Acta Applicandae Mathematicae 74 (2) (2002): 117.

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

[21] Futorny V., Ustimenko V., On Small World Semiplanes with Generalised Schubert Cells, Acta Applicandae Mathematicae 4 (2007).

[22] 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) (1988): 3946.

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

[24] Wróblewska, A., On some applications of graph based public key, Albanian J. Math. 2 (3) (2008): 229; Proceedings of the NATO Advanced Studies Institute: "New challenges in digital communications".

[25] Ustimenko V., On Extremal Graph Theory and Symbolic Computations, Dopovidi of the National Ukrainian Acad. Sci. (to appear).