On Extremal Algebraic Graphs and implementations of new cubic Multivariate Public Keys

Vasyl Ustimenko
0000-0002-2138-2357
Royal Holloway University of London
Institute of Telecommunication and Global
Information Space, Kyiv, Ukraine
Email: Vasyl.Ustymenko@rhul.ac.uk

Tymoteusz Chojecki, Michal Klisowski
0000-0002-3294-2794
0000-0002-2817-8404
Maria Curie-Sklodowska University,
Lublin, Poland.
Email: {tymoteusz.chojecki@umcs.pl, mklisow@hektor.umcs.lublin.pl}

***Abstract*—Algebraic Constructions of Extremal Graph Theory were efficiently used for the construction of Low Density Parity Check Codes for satellite communication, constructions of stream ciphers and Postquantum Protocols of Noncommutative cryptography and corresponding El Gamal type cryptosystems. We shortly observe some results in these applications and present idea of the usage of algebraic graphs for the development of Multivariate Public Keys (MPK). Some MPK schemes are presented at theoretical level, implementation of one of them is discussed.**

I. Introduction

EXTREMAL algebraic graphs were traditionally used for the construction of stream ciphers of multivariate nature (see [46] and further references). We introduce the first graph based multivariate public keys with bijective encryption maps. We hope that new recent results on algebraic constructions of Extremal Graph Theory [49] will lead to many applications in Algebraic Cryptography which includes Multivariate cryptography and Noncommutative Cryptography. Some graph based algebraic asymmetrical algorithms will be presented in this paper.

NIST 2017 tender starts the standardisation process of possible Post-Quantum Public keys aimed for purposes to be (i) encryption tools, (ii) tools for digital signatures (see [1]).

In July 2020 the Third Round of the competition started. In the category of Multivariate Cryptography (MC) remaining candidates are easy to observe. For the task (i) multivariate algorithm was not selected, single multivariate candidate is "The Rainbow Like Unbalanced Oil and Vinegar" (RUOV) digital signature method. As you see RUOV algorithm is investigated as appropriate instrument for the task (ii). During Third Round some cryptanalytic instruments to deal with ROUV were found (see [48]). That is why different algorithms were chosen at the final stage. In July 2022 first four winners of NIST standardisation competition were chosen. They all are lattice based algorithms. They all are not the algorithms of Multivariate Cryptography.

Noteworthy that all considered multivariate NIST candidates were presented by multivariate rule of degree bounded by constant (2 or 3) of kind
$x_1 \to f_1(x_1, x_2, \ldots, x_n)$,
$x_2 \to f_2(x_1, x_2, \ldots, x_n)$,
$\ldots$,
$x_n \to f_n(x_1, x_2, \ldots, x_n)$.

We think that NIST outcomes motivate investigations of alternative options in Multivariate Cryptography oriented on encryption tools for

(a) the work with the space of plaintexts ${F_q}^n$ and its transformation G of linear degree cn, $c > 0$ on the level of stream ciphers or public keys

(b) the usage of protocols of Noncommutative Cryptography with platforms of multivariate transformations for the secure elaboration of multivariate map G from $End(F_q[x_1, x_2, \ldots, x_n])$ of linear or superlinear degree and density bounded below by function of kind cn^r, where $c > 0$ and $r > 1$.

Some ideas in directions of (a) and (b) are presented in [43].

We hope that classical multivariate public key approach i. e. usage of multivariate rules of degree 2 or 3 is still able to bring reliable encryption algorithms. In this paper we suggest new cubic multivariate public rules.

Recall that the density is the number of all monomial terms in a standard form $x_i \to g_i(x_1, x_2, \ldots, x_n)$, $i = 1, 2, \ldots, n$ of multivariate map G, where polynomials g_i are given via the lists of monomial terms in the lexicographical order.

We use the known family of graphs $D(n, q)$ and $A(n.q)$ of increasing girth (see [2], [3] and further references) and their analogs $D(n, K)$ and $A(n, K)$ defined over finite commutative ring K with unity for the construction of our public keys. Noteworthy to mention that for each prime power q, $q > 2$ graphs $D(n, q)$, $n = 2, 3, \ldots$ form a family of large girth (see [3]), there is well defined projective limit of these graphs which is a q-regular forest. in fact if K is an integral domain both families $A(n, K)$ and $D(n, K)$ are approximations of infinitedimensional algebraic forests. The definitions of such approximations are given in Section 3 together with short survey of their applications.

In Section 2 we present the known mathematical definitions of algebraic geometry for further usage of them as instruments of Multivariate Cryptography. In particular definition of affine

This research is partially supported by British Academy Fellowship for Researchers at Risk 2022 and by UMCS program UMCS Mini-Grants.

Cremona semigroup of endomorphisms of multivariate ring $K[x_1, x_2, \ldots, x_n]$ defined over commutative ring K and affine Cremona group ${}^nCG(K)$ are presented there.

The concept of *trapdoor accelerator* of the transformation from affine Cremona semigroup ${}^nCS(K)$ is presented there as a piece of information which allows computation of reimage of the map in time $O(n^2)$.

This is a weaker version of the definition of trapdoor one way function. The definition of the trapdoor accelerator is independent from the conjecture $P \neq NP$ of the Complexity theory. Section 2 also contains some statements on the existence of the trapdoor accelerator with the restrictions on the degrees on maps and their inverses for families of elements of the affine Cremona group ${}^nCG(K)$.

Section 3 is dedicated to infinite forests approximations and their connections with Algebraic Geometry and Extremal Graph Theory.

The description of linguistic graphs $D(n, K)$ and $A(n, K)$ and some their properties are presented in Section 4, 5. These sections contain the descriptions of subgroups and subsemigroups of ${}^nCS(K)$ defined via walks in graphs $D(n, K)$ and their extensions $D(n, K[x_1, x_2, \ldots, x_n])$ and graphs $A(n, K)$ and $A(n, K[x_1, x_2, \ldots, x_n])$ respectively. Some statements about degrees of elements of these semigroups are given.

Section 6 contains examples of cryptographic applications of graph based trapdoor accelerators in the form of cubic multivariate public key.

Detailed description of multivariate public key related to one of presented families is presented in in the Section 7.

Remarks on security level connected with girth studies of tree approximations reader can find in section 8. Last Section 9 presents short conclusions.

II. On elements of Algebraic Geometry and trapdoor accelerators

Let K be a commutative ring with a unity. We consider the ring $K' = K[x_1,$
$x_2, \ldots, x_n]$ of multivariate polynomials over K. Endomorphisms δ of K' can be given via the values of $\delta(x_i) = f_i(x_1, x_2, \ldots, x_n)$, $f_i \in K'$. They form the semigroup $End(K[x_1, x_2, \ldots, x_n]) = {}^nCS(K)$ of K' known also as affine Cremona semigroup (see [3], [4]) after the famous Luigi Cremona (see [5]). The map $\tilde{\delta} : (x_1, x_2, \ldots, x_n) \to (f_1(x_1, x_2, \ldots, x_n), f_2(x_1, x_2, \ldots, x_n), \ldots, f_n(x_1, x_2, \ldots, x_n))$ is polynomial transformation of affine space K^n. These transformations generate transformation semigroup $CS(K^n)$. Note that the kernel of homomorphism of ${}^nCS(K)$ to $CS(K^n)$ sending δ to $\tilde{\delta}$ depends on the choice of commutative ring K.

Affine Cremona Group ${}^nCG(K) = Aut(K[x_1, x_2, \ldots, x_n])$ acts bijectively on K^n. Noteworthy that some elements of ${}^nCS(K)$ can act bijectively on K^n but do not belong to ${}^nCG(K)$. For instance endomorphism $x \to x^3$ of $R[x]$ acts bijectively on set R of real number but the inverse $x \to x^{1/3}$ of this map is birational element outside of ${}^1CG(R)$.

Recall that degree of δ is the maximal degree of polynomials $\delta(x_i)$, $i = 1, 2, \ldots, n$. The density of δ is a total number of monomial terms in all $\delta(x_i)$.

Assume that automorphism F from ${}^nCG(K)$ has constant degree d, $d \geq 2$. It is given in its standard form written as $x_1 \to f_1(x_1, x_2, \ldots, x_n)$, $x_2 \to f_2(x_1, x_2, \ldots, x_n)$, $\ldots$, $x_n \to f_n(x_1, x_2, \ldots, x_n)$ where f_i, $i = 1, 2, \ldots, n$ are elements of $K[x_1, x_2, \ldots, x_n]$ and used as public rule to encrypt plaintexts from K^n.

The following definition was motivated by the idea to have a weaker version of trapdoor one way function.

We say that family $F_n \in^n CG(K)$ of bijective nonlinear polynomial transformations of affine space K^n of degree ≤ 3 has *trapdoor accelerator* ${}^nT$ of level $\geq d$ if

(i) the knowledge of piece information ${}^nT$ ("trapdoor accelerator") allows to compute the reimage x for F_n in time $O(n^2)$

(ii) the degree of ${F_n}^{-1}$ is at least d, $d \geq 3$.

Notice that if F_n are given by their standard forms and degrees of ${F_n}^{-1}$ are equal to d then the inverse can be approximated in polynomial time $f(n, d) = O(n^{d^2+1})$ via linearisation technique. One can see that the approximation task becomes unfeasible if d is "sufficiently large" like $d = 100$. Examples of cubic families F_n with trapdoor accelerator of high level t are given in the case of special finite fields F_q in the section 3.

III. On algebraic forest approximations and their applications

We define thick forest as simple graph without cycles such that each of its vertex has degree at least 3. In probability theory branching process is a special stochastic process corresponding to a random walk on a thick forest. A genealogy of single vertex is a tree. One of the basic properties of finite tree is the existence of a leaf, i. e. vertex of degree 1. Thus each thick tree is an infinite simple graph.

Let K be a commutative ring and K^n be an affine space of dimension n over K (free module in other terminology). A subset M in K^n is an algebraic set over K if it is a solution set for the system of algebraic equations of kind $f = 0$ or inequalities of kind $g0$ where f and g are elements of $K[x_1, x_2, \ldots, x_n]$. There are several alternative approaches to define dimension of M. In the case when K is a field these approaches are equivalent and dimension of M can be computed with the usage of Groőbner basis technique (see [47], [48], [49]).

We say that graph Γ is algebraic over K if its vertex and edge sets are algebraic sets over K

We investigate a possibility to define thick forest F by system of equations over some commutative ring K, i.e. construct F as a projective limit of algebraic over K bipartite graphs Γ_i, $i = 1, 2, \ldots$. Noteworthy that the girth $g_i = g(\Gamma_i)$, which is the length of minimal cycle in Γ_i tends to infinity when i is growing. In this situation we refer to F as algebraic forest over K.

We say that the family Γ_i is an algebraic forest approximation over the ring K. In the case $g_i \geq cn_i$, where n_i are dimensions of the algebraic sets $V(\Gamma_i)$ of vertices of the graph Γ_i and c is some positive constant we use term *algebraic forest approximation of large girth*. Note that algebraic forest approximations of large girth over finite field F_q, $q > 2$ are *families of graphs of large girth* in sense of P. Erdős'(see [1], [2] and further references). The first algebraic forest approximation of a large girth was introduced by F. Lazebnik and V. Ustimenko (see [3], [4]) in the case of $K = F_q$.

The properties of trees of this algebraic forest and their approximations over Fq were investigated in the paper by [5].

In 1998 more general algebraic graphs $D(n, K)$ defined over arbitrary commutative ring K were introduced [6]. It was stated that a girth of $D(n, K)$ is $\geq n+5$ in the case of arbitrary integrity domain K. This inequality insures that $D(n, K)$, $n = 2, 3, \ldots$ is algebraic forest approximation of large girth. The prove of the inequality reader can find in [7], simpler prove of this fact the reader can find in [44].

Noteworthy that in the case of integrity domain K together with $D(n, K)$, $n = 2, 3, \ldots$ one can consider another thick forest approximation $D(n, K[x_1, x_2, \ldots, x_m])$ for each parameter m. Thus paper [6] opened a possibility to use extremal properties of these graphs in the Theory of Symbolic Computations and its various applications to Cryptography.

The paths of even length t on trees and their approximations can be used to induce multivariate transformations on varieties P_i and L_i of points and lines of $V(\Gamma_i)$. These transformations can serve as encryption maps acting on the potentially infinite space P_i of plaintexts (see [9]-[17]). They form a group $G_i = G(\Gamma_i)$ which can be a platform for the protocols of Noncommutative Cryptography (see [18]-[23]). Noteworthy that if t is at most half of the girth of Γ_i then different paths produce distinct transformations. So, forest approximations of large girth are preferable for cryptographic applications.

Other tree approximation over the integrity domain K is formed by graphs $A(n, K)$ defined in [8]. In fact these graphs were defined earlier [7] as homomorphic images $E(n, K)$ of graphs $D(n, K)$ or their connected components $CD(n, K)$. As it was stated recently in short paper [50] for each integrity domain K, $K \neq F_2$ graphs $A(n, K)$ form a tree approximation of large girth. For each vertex v of graph G we define its cycle indicator $Cind(v)$ as length of the shortest cycle through v. We define cycle indicator $Cind(G)$ of the graph as maximal value of $Cind(v)$ via all vertexes of the graph. Let family Γ_i be an algebraic forest approximation over the ring K. In the case $Cind(\Gamma_i) \geq\geq cn_i$, where n_i are dimensions of the algebraic manifolds $V(\Gamma_i)$ of vertices of the graph Γ_i and c is some positive constant we use term *algebraic forest approximation with the large cycle indicator*. We can assume that c is the largest possible constant for the property in the definition. As it was established in [44] for each integrity domain K algebraic graphs $A(n, K)$ form algebraic forest approximation with large cycle indicator for which $c = 2$.

We can compare properties $A(n, F_q)$ and widely known family $X(p, q)$ of Cayley Ramanujan graphs of large girth introduced by G. Margulis [28], [29] and investigated by A. Lubotzky, P. Sarnak and R. Phillips [30]. Both families are families of small world graphs in sense of [25]. Noteworthy that projective limit of $X(p, q)$ does not exist and this family is not a tree approximation. The speed of girth growth for $X(p, q)$ is $4/3$. A. Lubotzky conjectured that this is the highest possible speed of girth growth.

Noteworthy that speed of girth growth for $A(n, F_q)$ is not evaluated properly yet. Graphs $X(p, q)$, $D(n, F_q)$ and $A(n, F_q)$ were used for the construction of Low Density Parity Check Codes (LDPC) for satellite communications. The families $X(p, q)$, $CD(n, q)$ and $A(n, q)$ can be used for the constructions of LDPC codes for the noise protection in satellite communications. D. MacKay and M. Postol [40] proved that $CD(n, q)$ based LDPC codes have better properties than those from $X(p, q)$ for the constructions of LDPC codes. It was established that $A(n, q)$ based LDPC codes are even better than those from $CD(n, q)$ (see [39]). Some encryption algorithms (stream ciphers) based on $A(n, K)$ and $D(n, K)$ were already introduced (see [9], [10], [11], [12], [13], [14], [15], [16], [17], [42], [45] and further references).

Noteworthy that the study of homogeneous algebraic graphs of prescribed girth or diameter is classical area of Algebraic Geometry ([33]-[38]). Projective plane can be defined as a homogeneous algebraic graph of girth 6 and diameter 3 (see [33]). J. Tits defined generalized m-gon as homogeneous algebraic graph of diameter m and girth $2m$ (see [34]-[37]). Geometries of Chevalley groups $A_2(F)$, $B_2(F)$ and $G_2(F)$ are homogeneous algebraic graphs over the field F which are generalized m-gons for $m = 3, 4$ and 6 (see [37]).

IV. On linguistic graphs $A(n, K)$, related semigroups and groups and symmetric ciphers

Regular algebraic graph $A(n, q) = A(n, F_q)$ is an important object of Extremal Graph Theory. In fact we can consider more general graphs $A(n, K)$ defined over arbitrary commutative ring K.

This graph is a bipartite graph with the point set $P = K^n$ and line set $L = K^n$ (two copies of Cartesian power of K are used). It is convenient to use brackets and parenthesis to distinguish tuples from P and L.

So, (p) $= (p_1, p_2, \ldots, p_n) \in P_n)$ and [l] $= [l_1, l_2, \ldots, l_n] \in L_n$. The incidence relation $I = A(n, K)$ (or corresponding bipartite graph I) is given by the following condition.

pIl if and only if the equations

$p_2 - l_2 = l_1 p_1$, $p_3 - l_3 = p_1 l_2$, $p_4 - l_4 = l_1 p_3$, $p_5 - l_5 = p_1 l_4$, $\ldots$, $p_n - l_n = p_1 ln - 1$ hold for odd n and $p_n - l_n = l_1 p_{n-1}$ for even n.

In the case of $K = F_q$, $q > 2$ of odd characteristic graphs $A(n, F_q)$, $n > 1$ form a family of small world graphs because their diameter is bounded by linear function in variable n (see [8]).

Recall that the girth of the graph is the length of its minimal cycle. We can consider an infinite bipartite graph $A(K)$ with points $(p_1, p_2, \ldots, p_n, \ldots)$ and lines $[l_1, l_2, \ldots, l_n, \ldots]$ which is a projective limit of graphs $A(n,K)$ when n tends to infinity. If K, $|K|>2$ is an integrity domain then $A(K)$ is a tree and the girth g_n of $A(n,K)$, $n=2,3,\dots$ is bounded below by linear function cn for some positive constant c [50].

As a byproduct of this result we get that $A(n,q)$, $n=2,3,\dots$ for each fixed q, $q>2$ form a family of large girth in sense of Erdős'. In fact graphs $A(n,K)$ were obtained in [7] as homomorphism images of known graphs $CD(n,K)$ of large girth (see [3], [4], [5]).

Let K be a commutative ring with a unity. Graphs $A(n,K)$ belong to the class of linguitic graphs of type $(1,1,n-1)$ [40], i.e. bipartite graphs with partition sets $P=K^n$ (points of kind $(x_1,x_2,\dots,x_n)$, $x_i\in K$) and $L=K^n$ (lines $[l_1,l_2,\dots,l_n]$, $l_i\in K$) and incidence relation $I=I(n,K)$ such that $(x_1,x_2,\dots,x_n)I[y_1,y_2,\dots,y_n]$ if and only if $a_2x_2+b_2x_2=f_2(x_1,y_1)$, $a_3x_3+b_3x_3=f_3(x_1,x_2,y_1,y_2)$, $\dots$, $a_nx_n+b_nx_n=f_n(x_1,x_2,\dots,x_n)$, where a_i and b_i are elements of multiplicative group K^* of K and f_i are multivariate polynomials from $K[x_1,x_2,\dots,x_{i-1},y_1,y_2,\dots,y_{i-1}]$ for $i=2,3,\dots,n$.

The colour of $\rho(v)$ of vertex v of graph $I(K)$ is defined as x_1 for point $(x_1,x_2,\dots,x_n)$ and y_1 for line $[y_1,y_2,\dots,y_n]$.

The definition of linguistic graph insures that there is a unique neighbour with the chosen colour for each vertex of the graph. Thus we define operator $u=N_a(v)$ of taking neighbour u with colour a of the vertex v of the graph. Additionally we consider operator ${}^aC(v)$ of changing colour of vertex v, which moves point $(x_1,x_2,\dots,x_n)$ to point $(a,x_2,x_3,\dots,x_n)$ and line $[x_1,x_2,\dots,x_n]$ to line $[a,x_2,x_3,\dots,x_n]$.

Let us consider a walk $v,v_1,v_2,\dots,v_{2s}$ of even length $2s$ in the linguistic graph $I(K)$. The information on the walk is given by v and the sequence of colours $\rho(v_i)$, $i=1,2,\dots,2s$. The walk will not have edge repetitions if $\rho(v_2)\neq\rho(v)$, $\rho(v_i)\neq\rho(v_{i-2})$ for $i=3,4,\dots,n$. Notice that v and v_{2s} are elements of the same partition set (P or L). For each vertex v of $I(K)$ we consider a variety of *walks* with jumps, i. e. totality of sequences of kind v, $v_1=\ {}^{a_1}C(v)$, $v_2=N_{a_2}(v_1)$, $v_3=\ {}^{a_3}C(v_2)$, $v_4=N_{a_4}(v_3)$, $\dots$, $v_5=\ {}^{a_5}C(v_4)$, $\dots$, $v_{4s}=N_{a_{4s}}(v_{4s-1})$, $v_{4s+1}=\ {}^{a_{4s+1}}C(v_{4s})$. Note that for each s , $s\geq 0$ vertices v,v_1,v_{4s},v_{4s+1} are elements of the same partition. Let $u=(a_1,a_2,\dots,a_{4s},a_{4s+1})$ be the colours of the walk with jumps.

We introduce the following polynomial transformations of partition sets P and L. Firstly we consider the pair of linguistic graphs $I(K)$ and $I(K[x_1,$
$x_2,\dots,x_n])$. These graphs are defined by the same equations with coefficients from the commutative ring K. We look at sequences of walks with jumps of length $4s+1$ where $s\geq 0$ starting in the point $v=(x_1,x_2,\dots,x_n)$ (or line $[x_1,x_2,\dots,x_n]$) of the graph $K[x_1,x_2,\dots,x_n]$ which uses colors $a_1(x_1)$, $a_2(x_1)$, $\dots$, $a_{4s+1}(x_1)$ from $K[x_1]$. The final vertex of this walk is v_{4s+1} with coordinates $a_{4s+1}(x_1)$, $f_2(x_1,x_2)$, $f_3(x_1,x_2,x_3)$, $\dots$, $f_n(x_1,x_2,\dots,x_n)$). Let us consider the transformations ${}^uT_P$ and ${}^uT_L$ sending starting vertex to the destination point of the walk with jumps acting via the rule $x_1\to a_{4s+1}(x_1)$, $x_2\to f_2(x_1,x_2)$, $\dots$, $x_n\to f_n(x_1,x_2,\dots,x_n)$ on the partition sets P and L isomorphic to K^n. It is easy to see that transformations of kind ${}^uT_P$ (or ${}^uT_L$) form the semigroup $LS_P(I(K))$ $(LS_L(I(K))$ respectively). We refer to this transformation semigroup as *linguistic semigroup* of graph $I(K)$.

Let us consider an algebraic formalism for the introduction of linguistic semigroups. We take the totality of words $F(K[x])$ in the alphabet $K[x]$ and define the product of $u=(a_1(x),a_2(x),\dots,a_k(x))$ and $w=(b_1(x),b_2(x),\dots,b_s(x))$ as word $=(a_1(x)$, $a_2(x)$, $\dots$, $a_k(x))\times(b_1(x)$, $b_2(x)$, $\dots$, $b_t(x))=(a_1(x)$, $a_2(x)$, $\dots$, $a_{k-1}(x)$, $b_1(a_k(x))$, $b_2(a_k(x))$, $\dots$, $b_t(a(x)))$.

Obtained semigroup $F(K[x])$ is slightly modified free product of $End(K[x])$ with itself. Note that we can identify $a(x)$ from $K[x]$ with the map $x\to a(x)$ from $End(K[x])$.

Let F_K be a subsemigroup of words of length of kind $4s+1$, $s\geq 0$.

PROPOSITION. *Let $I(K)$ be a linguistic graph defined over commutative ring K with unity. The map ${}^{I(K)}\eta_P$: $F_K\to End(K[x_1,x_2,\dots,x_n])$ such that ${}^{I(K)}\eta(u)={}^u\ T_P$ (or $\eta(u)_L={}^u\ T_L$) is a semigroup homomorphism.*

It is easy to see that ${}^{I(K)}\eta_P(F_K)=LS_P(I(K)$ and ${}^{I(K)}\eta_L(F_K)=LS_L(I(K)$.

PROPOSITION. (see [45] and further references)

The image of $u=(a_1(x),a_2(x),\dots,a_k(x))$ from F_K under the map ${}^I(K)\eta_P$ (or ${}^I(K)\eta_P$ is invertible element of $LS_P(I(K)$ (or $LS_L(I(K)$ if and only if the map $x\to a_k(x)$ is an element of $\mathrm{Aut}(K[x])$.

REMARK. *The transformations $({}^{I(K)}\eta_P(u),P)$ and $({}^{I(K)}\eta_L(u),L)$ are bijective if and only if the map $x\to b(x)$ is bijective.*

ILLUSTRATIVE EXAMPLE.

Let $K=R$ (real numbers) or K be algebraically closed field of characteristic 0 and $b(x)=x^3$. The inverse map for $x\to x^3$ is birational automorphism $x\to x^{1/3}$ of $K[x]$. Thus $g_P={}^{I(K)}\ \eta_P(u)$ and $g_L^{I(K)}\eta_L(u)$ do not have inverses in $End(K[x])$. They have bijective birational inverses. Noteworthy that g_P and g_L are transformations of infinite order. Degree of polynomial transformations of ${g_P}^s$ and ${g_L}^s$ are at least 3^s.

So we have an algorithm of generation bijective polynomial maps of arbitrary large degree on variety K^n.

We refer to subgroups $G_P(I(K))$ and $G_L(I(K))$ of invertible elements of $LS_P(I(K))$ and $LS_L(I(K))$ as groups of linguistic graphs $I(K)$. They are different from automorphism group of $I(K)$.

Let us consider semigroup $\tilde{F}_K$ of words of kind $u=(x,f_1,f_1,f_2,\dots,f_s,f_s)$. It is easy to see that for each linguistic graph $I(K)$ the transformations $g_P(u)={}^I(K)\eta_P(u)$ and ${g_L}^I(K)\eta_L(u)$ are computed via consecutive usage of N_{f_i} in the linguistic graph. Thus we refer to $SW_P(I(K)=\{g_P(u)|u\in\tilde{F}_K\}$ and $SW_L(I(K)=\{g_L(u)|u\in\tilde{F}_K\}$ as semigroups of symbolic walks on partition sets of $I(K)$. We refer to $GW_P(I(K)=SW_P(I(K)\cup G_P(I(K))$ and $GW_L(I(K)=SW_L(I(K)\cap G_L(I(K))$ as groups of symbolic walks.

Finally we consider the semigroup $St(K)$ of words $u = (x+\alpha_1, x+\alpha_2, \ldots, x+\alpha_k)$ where α_i are elements of K. We consider $F_K = F_K \cap St_K$ $\tilde{F}_K = \tilde{F}_K \cap St_K = \Sigma_K$ and introduce groups ${}^{I(K)}\eta_P(F_K) = \tilde{H}_P(I(K))$, ${}^{I(K)|}\eta_P(F_K) = \tilde{H}_P(I(K))$, ${}^{I(K)|}\eta_P(\Sigma_K) = H_P(I(K))$, ${}^{I(K)|}\eta_P(\Sigma_K) = H_P(I(K))$.

We can change set P for the line set L and introduce ${}^{I(K)|}\eta_L(\Sigma_K) = H_L(I(K))$.

We refer to groups $H_P(I(K))$, $H_L(I(K))$ as groups of walks on partition sets of linguistic graph $I(K)$.

PROPOSITION.

If a linguistic graph $I(K)$ is connected then groups $H_P(I(K))$ and $H_L(I(K))$ are acting transitively on K^n.

The following statement was formulated in [15].

THEOREM. (see [45] or [15])

For each commutative ring K groups $H_P(A(n,K)) = GA(n,K)$ and $H_L(A(n,K)) = {}^*GA(n,K)$ are totalities of cubical automorphisms of $K[x_1, x_2, \ldots, x_n]$.

COROLLARY.

Let us consider element $u = (x, x+a_1, x+a_1, x+a_2, x+a_2, \ldots, x+a_{k-1}, x+a_{k-1}x+a_k, x^t$ of F_K for commutative ring K with unity with finite multiplicative group of order d, $d > 2$ where $t = 2$ or $t = 3$ and $(d,t) = 1$. Then transformation ${}^{A(n,K)}\eta(u)$ is a cubical one.

V. On linguistic graphs $D(n,K)$ and corresponding trapdoor accelerators

As we already mentioned graphs $A(n,K)$ appear as homomorphic quotients of linguistic graphs $D(n,K)$ or their connected components $CD(n,K)$. Isomorphic groups $H_P(D(n,K)$ and $H_L(D(n,K)$ were introduced in [12]. The fact that elements of $H_P(D(n,K))$ ($GD(n,K)$ in other notation) are transformations of degree ≤ 3 in other notations) was proved later (see [31] and further references). Theorem 4. 1 was deduced from this fact.

We already mentioned that graphs $A(m,K)$ were obtained as quotients of graphs $D(n,K)$). This incidence structure was defined in the following way.

Let K be an arbitrary commutative ring. We consider the totality P' of points of kind

$x = (x) = (x_{1,0}, x_{1,1}, x_{1,2}, x_{2,2}, \ldots, x_{i,i}, x_{i,i+1}, \ldots)$ with coordinates from K

and the totality L' of lines of kind

$y = [y] = [y_{0,1}, y_{1,1}, y_{1,2}, y_{2,2}, \ldots, y_{i,i}, y_{i,i+1}, \ldots]$. We assume that tuples (x) and $[y]$ has finite support and a point (x) is incident with a line $[y]$, i. e. xIy or $(x)I[y]$, if the following conditions are satisfied:

$x_{i,i} - y_{ii} = y_{i-1,i}x_{1,0}$,
$x_{i,i+1} - y_{i,i+1} = y_{0,1}x_{i,i}$ (2)
where $i = 1, 2, \ldots$.

We denote the graph of this incidence structure as $A(K)$. We consider the set $Root$ of indexes of points and lines of $A(K)$ as a subset of the totality of all elements $(i+1, i+1)$, $(i, i+1)$, $(i+1, i)$, $i \geq 0$ of root system $\tilde{A}_1$ of affine type. We see that $Root = \{(1,0), (0,1), (1,1), (1,2), (2,2), (2,3), \ldots\}$. So we introduce $R_{1,0} = Root - \{0,1\}$ and $R_{0,1} = Root - \{(1,0)\}$. It allows us to identify sets P' and L' with affine subspaces $\{f : R_{1,0} \to K\}$ and $\{f : R_{0,1} \to K\}$ of functions with finite supports.

For each positive integer $k \geq 2$, we obtain an incidence structure (P_k, L_k, I_k) as follows. Firstly, P_k and L_k are obtained from P' and L', respectively, by simply projecting each vector onto its k initial coordinates. The incidence I_k is then defined by imposing the first $k-1$ incidence relations and ignoring all the other ones. The incidence graph corresponding to the structure (P_k, L_k, I_k) is denoted by $A'(k,K)$. The comparison of equations of $A'(k,K)$ and $A(k,K)$ allows to justify the isomorphism of these graphs. It is convenient for us to identify graphs $A(k,K)$ with incidence structures I_k defined via relations (2).

The procedure to delete last coordinates of points and lines of graph $A(n,K)$ defines the homomorphism ${}^n\Delta$ of $A(n,K)$ onto $A(n-1,K)$, $n > 2$. The family of these homomorphisms defines natural projective limit of $A(n,K)$ which coincides with $A(K)$. We introduce the colour function ρ on vertexes of graph $A(K)$ or $A(n,K)$ as x_{10} for the point $(x_{10}, x_{11}, x_{12}, \ldots)$ and y_{01} for the line $[y_{01}, y_{11}, x_{12}, \ldots]$. We refer to $\rho(v)$ for the vertex v as *colour* of vertex v.

The family of graphs $D(n,K)$, $n = 2, 3, \ldots$ where K is arbitrary commutative ring defines the projective limit $D(K)$ with points $(p) = (p_{10}, p_{11}, p_{12}, p_{21}, p_{22}, p'_{22}, \ldots, p'_{ii}, p_{ii+1}, p_{i+1,i}, p_{i+1,i+1}, \ldots)$, and lines $[l] = [l_{01}, l_{11}, l_{12}, l_{21}, l_{22}, l'_{22}, \ldots, l'_{ii}, l_{ii+1}, l_{i+1,i}, l_{i+1,i+1}, \ldots]$, which can be thought as infinite sequences of elements in K such that only finitely many components are nonzero.

A point (p) of this incidence structure I is incident with a line $[l]$, i.e. $(p)I[l]$, if their coordinates obey the following relations:

$p_{i,i} - l_{i,i} = p_{1,0}l_{i-1,i}$,
$p'_{i,i} - l'_{i,i} = p_{i,i-1}l_{0,1}$,
$p_{i,i+1} - l_{i,i+1} = p_{i,i}l_{0,1}$, (3)
$p_{i+1,i} - l_{i+1,i} = p_{1,0}l'_{i,i}$.

(These four relations are well defined for $i > 1$, $p_{1,1} = p'_{1,1}$, $l_{1,1} = l'_{1,1}$.)

Let D be the list of indexes of the point of the graph $D(K)$ written in their natural order, i. e. sequence $(1,0)$, $(1,1)$, $(1,2)$, $(2,1)$, $(2,2)$, $(2,2)'$, ... Let ${}^kD$ be the list of k first elements of D. The procedure of deleting coordinates of points and lines of $D(k,K)$ indexed by elements of $D -{}^k D$ defines the homomorphism of $D(K)$ onto graph $D(k,K)$ with the partition sets isomorphic to the variety K^n and defined by the first $k-1$ equations from the list (3). We can see that the procedure of deleting of coordinates indexed by elements $D - (Root - \{(0,1)\})$ defines the homomorphism of graph $D(K)$ onto the graph isomorphic to $A(K)$.

Let us consider the set ${}^kA = {}^kD - {}^kD \cap Root$. The procedure of deleting coordinates of vertexes of $D(k,K)$ indexed by elements of ${}^kA$ defines the homomorphism η_k of $D(k,K)$ onto $A(m,k)$ where m is the cardinality of ${}^kD \cap Root$. Both families A(n, K) and D(n, K) are linguistic graphs of type $(1, 1, n-1)$.

THEOREM. (see [45]). *For each commutative ring K groups $H_P(D(n,K)) = GD(n,K)$ are totalities of cubical automorphisms of $K[x_1, x_2, \ldots, x_n]$.*

COROLLARY. *Let us consider element $u = (x, x+a_1, x+a_1, x+a_2, x+a_2, \ldots, x+a_{k-1}, x+a_{k-1}, x+a_k, x^t)$ of F_K for commutative ring K with unity with finite multiplicative group of order d, $d > 2$ where $t = 2$ or $t = 3$ and $(d,t) = 1$. Then transformation ${}^{D(n,K)}\eta(u)$ is a cubical one.*

VI. Explicit constructions of trapdoor accelerators and their applications

EXAMPLE 6.1

Let us consider general commutative ring K with unity and $F_n = T_1^{A(n,K)}\eta(u)T_2$, where T_1, T_2 are elements of $AGL_n(K)$ and the tuple $(x,\ x+\alpha_1,\ x+\alpha_1,\ x+\alpha_2,\ x+\alpha_2, \ldots, x+\alpha_2, \ldots, x+\alpha_s,\ x+\alpha_s)$ such that $cn < s < n$ for some constant $c > 0$. According to Theorem 3. 1 the transformations F_n and ${F_n}^{-1}$ are of degree 3. So $T = \{T_1, T_2, u\}$ is a trapdoor accelerator of F_n of degree 3 and level 3.

The following two constructions give families of cubic multivariate map with trapdoor accelerator of rather large level.

EXAMPLE 6. 2

Let us consider family of fields $K_n = F_{2^{n^a}}$ for some constant a and transformation $F_m = {}^{A(m,K_n)}\eta(x, x+a_1, x+a_1, x+a_2, x+a_2, \ldots, x+a_{s-1}, x+a_{s-1}, x+a_s, x^2)$. Then the map w: $x \to x^2$ is an automorphism of K_n. It is easy to see that w^{n^a} is identity map and $w^{n^a-1}$is an inverse map for w. Note that degree of w^k is 2^k. Thus the degree of inverse for w is 2^{n^a-1}. The degree t_n of ${F_n}^{-1}$ is proportional to degree of w. In fact it can be shown that $t_n = 3 \times 2^{n^a-1}$.

Let us assume that $\alpha m < s < m$ where α is a positive constant and two affine transformation T_1 and T_2 from the group $AGL_m(K_n)$. We consider the family of bijective transformation $G_m = T_1F_mT_2$. Standard forms of cubical maps G_m form family with trapdoor accelerators ${}^{m,n}T$ which are triples T_1, $(x,\ x+a_1,\ x+a_1,\ x+a_2,\ x+a_2, \ldots, x+a_{s-1},\ x+a_{s-1},\ x+a_s,\ x^2)$ and T_2 of level $t_n = 32^{n^a-1}$. Really, the knowledge on the triples gives us ${T_2}^{-1}$, $Rev((x, x+a_1, x+a_1, x+a_2, x+a_2, \ldots, x+a_{s-1}, x+a_{s-1}, x+a_s, x^2))$ and ${T_1}^{-1}$. It allows the computation of reimage of G_m in time $O(m^2)$. Alice can use cubic standard form G_m as public rule and trapdoor ${}^{m,n}T$ as her private key.

EXAMPLE 6.3.

We consider a modification of Example 6.1 in more general case of finite fields F_q where q is such that $(3, q-1) = 2$. We consider a triple which consists of T_1 and T_2 from $AGL_m(F_q)$ and tuple $u = (x,\ x+a_1,\ x+a_1,\ x+a_2,\ x+a_2, \ldots, x+a_{s-1},\ x+a_{s-1},\ x+a_s,\ x^3)$. We use the assumption that $\alpha \times m < s < m$ and s is even where α is a positive constant. Let G_m be the standard form of the composition of T_1, ${}^{A(m,q)}\eta(u)$ and T_2. The degree of ${G_m}^{-1}$ acting on ${F_q}^m$ is $\geq 3t$, where t is maximal power of 3 which $< q-1$ and transformations of kind $T_1F_mT_2$, $F_m = {}^{A(m,q)}\eta(u)$ can serve as public keys. This algorithm is implemented in the case of finite fields $F_{2^{63}}$.

We modify previous example to get explicit construction of family of cubic nonbijective trapdoor accelerators.

EXAMPLE 6.4.

We consider family $A(m,K)$, $m \geq 2$ defined over finite commutative ring K such that $d = |K^*| > 3$ and $(3,d) = 1$ to construct cubical map G_m of affine space K^m, $m \geq 2$ which acts injectively on $T_m(K) = {K^*}^m$ and has *eulerian* inverse E_n which is an endomorphism of $K[x_1, x_2, \ldots, x_m]$ such that the composition of G_m and E_m acts on ${}^{n,m}T(K)$ as identity map. The degree of $E_m(K)$ is at least $3{\times}t$ where t is maximal power of 3 which is $< d$. So we take affine transformation T_1 from $AGL_m(K)$ such that $T_1(x_1) = \alpha x_1$ where $\alpha \in K^*$ together with $T_2 \in AGL_m(K)$ and tuple, u =$(x,\ x+a_1,\ x+a_1,\ x+a_2,\ x+a_2, \ldots, x+a_{s-1},\ x+a_{s-1},\ x+a_s,\ x^3)$ where even s is selected as in the previous example. Standard form G_m of ${T_1}^{A(n,K)}\eta(u)T_2$ is a toric automorphism of $K[x_1, x_2, \ldots, x_m]$. The knowledge of trapdoor accelerator (T_1, u, T_2) allows to compute the reimage of $G({K^*}^m)$ in time $O(m^2)$. So we have cubic endomorphism with trapdoor accelerator of level t. It can be used for the construction of public keys with the space of plaintexts ${K^*}^m$ and the space of ciphertexts K^m.

We implement this algorithm in the case of $K = Z_{2^n}$, $n = 7, 8, 16.32, 64$. It uses cubical toric automorphism of level $3t$ where t is maximal power of 3 from interval $(0, 2^{n-1})$. In this case we can use more general form for T_1 defined by condition $T_1(x_1) = a_1x_1 + a_2x_2 + \ldots + a_m(x_m)$ where odd number of a_i are odd residues modulo 2^n (see [26], [28]). In the case of $K = F_q$ we get an example 6.3. In these examples we can change graph $A(n,K)$ for graph $D(n,K)$ and get Examples 6.5, 6.6 and 6.7 respectively.

Mentioned above examples were suggested in [43]. Let us consider the implementation of public key based on the trapdoor accelerator of Example 1.

VII. On the example of public key rule

As usually name Alice corresponds to owner of the public key and name Bob corresponds to public user of the cryptosystem. Alice has to select size of finite field and dimension of the space V of plaintexts. Assume that she takes field $F_{2^{3}2}$ and dimension $n = 256$. Additionally Alice has to identify vector space V with point set P or line set L. Assume that she select L. It means that her plaintext is the tuple $[x_{0,1}$, $x_{1,1}$, x_{12}, x_{22}, $\ldots, x_{127,128}$, $x_{128,128}]$. Additionally Alice has to select parameter s corresponding to length of the path in the graph $A(256, F_{2^{3}2})$. For proper selection of this parameter one can investigate cycle indicator $Cind(v)$ of the vertex v of the graph, i. e minimal length of the cycle through v and evaluate maximal value of $Cind(v)$ via all possible vertexes v (cycle indicator $A(256, F_{2^{32}})$ of the graph). Accordingly [Archive] cycle indicator of the graph $A(n, F_q)$ is at least $2n+2$. In fact $Cind(A(n, F_q)) = 2n+2$ for infinitely many special parameters q. There are $q^{[n/2]}$ lines $[l] \in L$ such that $Cind([l]) \geq 2n+2$. Let $[l] = [x_{01}, x_{11}, \ldots, x_{[n/2],[n/2]}]$ be one of the lines with written above property where parameter n is even integer. The trapdoor accelerator uses path $p(t_1, t_2, \ldots, t_s)$ of even length s starting in $[l]$ given by colours of vertexes x_{01}, $x_{01}+t_1$, $x_{0,1}+t_2$, $\ldots$, $x_{0,1}+t_s$ where

$t_2 \neq 0$, $t_i \neq t_{i-2}$, for $i = 3, 4, \ldots, s$. Let us assume that $s \leq n$ and u be the last vertex of the path. Lower bound for $Cind([l])$ insures that destination lines of $p(t_1, t_2, \ldots, t_s)$ and $p(t'_1, t'_2, \ldots, t'_s)$, $t_1 \neq t'_1$ are different. The accelerator uses destination line $[y]$ of path of $A(n, F_q[x_{01}, x_{11}, \ldots, x_{n,n}]$ with colours x_{01}, $x_{01} + t_1$, $x_{0,1} + t_2$, $\ldots$ $x_{0,1} + t_s$ starting in $[l]$. Assume that $[y] = [x_{01} + t_s$, g_{11}, $g_{1,2}$, $g_{2,2}$, …, $g_{n,n}]$, where g_{11} , $g_{1,2}$, …, $g_{n,n}$ are cubical or quadratic multivariate polynomials in variables x_{01}, x_{11}, …, $x_{n,n}$. The trapdoor accelerator uses cubical transformation $F(t_1, t_2, \ldots, t_s)$ of $L = F_q{}^n$ of kind $x_{01} \to x_{1,0} + t_s$,

$x_{1,1} \to g_{1,1}$,

…,

$x_{nn} \to g_{n,n}$.

It is important that the map $F(t_1, t_2, \ldots, t_s)$ differs from each of $(q-1)^s$ transformations $F(t'_1, t'_2, \ldots, t'_s)$, $t'_1 \neq t_1$ if $s \leq n$. So Alice can take $s = 256$ and select one of $q(q-1)^{255}$ sequence t_1, t_2, …, t_{256}.

To construct trapdoor accelerator Alice has to generate two bijective linear transformations ^1T and ^2T of L of kind

$x_{01} \to^i l_{01}(x_{01}, x_{11}, \ldots, x_{128,128})$

$x_{11} \to^i l_{11}(x_{01}, x_{11}, \ldots, x_{128,128})$

$x_{128,128} \to^i l_{11}(x_{01}, x_{11}, \ldots, x_{128,128})$ where $i = 1, 2$. In a spirit of LU factorisation Alice can generate each ^iT as a composition of lower triangular matrix ^iL, $i = 1, 2$ with nonzero entries on diagonal and upper triangular matrices ^iU with unity elements on diagonal. For selection of the tuple t_i, $i = 1, 2, \ldots, 256$, ^iL and ^iU, $i = 1, 2$ Alice can use pseudorandom generators of field elements or some methods of generating genuinely random sequences (usage of existing implementation the quantum computer, other Probabilistic modifications of Turing machine, quasi-stellar radio sources (quasars) and etc).

Alice takes tuple of variables $[x] = (x_{0,1}, x_{11}, \ldots, x_{128,128})$ and conducts the following steps.

Step 1.

She compute a product of $[x]$ and ^1T. The output is a string $[^1l_{01}(x_{0,1}, x_{11}, \ldots,$ $x_{128,128})$, $^1l_{11}(x_{0,1}, x_{11}, \ldots, x_{128,128})$, $\ldots$ $^1l_{128,128}(x_{0,1}, x_{11}, \ldots, x_{128,128})] = [^1u]$. Alice treats the output as the line of graph $A(256, F_{2^{32}}[x_{01}, x_{11}, \ldots, x_{128,128}])$

Step 2.

She computes the destination line $[^2u]$ of path with starting line $[^1u]$ and colours $^1u_{0,1}$, $^1u_{0,1} + t_1$, $^1u_{0,1} + t_2$, …, $^1u_{0,1} + t_{256}$.

Step 3.

Alice takes the tuple $[^2u] = [^1u_{0,1} + t_{256}, ^2u_{1,1}, ^2u_{1,2}, \ldots, ^2u_{128,128}]$ of elements $F_{2^{32}}[x_{01}, x_{11}, \ldots, x_{128,128}]$ and forms the line $^3u = [^1u_{0,1})^2$, $^2u_{1,1}$, $\ldots$ $^2u_{128,128}]$ of the vector space L.

Step 4.

She computes the composition of the tuple ^3u and the matrix of linear map ^2T. So Alice has the tuple of cubic multivariate polynomials $^4u = (f_{01}, f_{11}, \ldots,$ $f_{128,128})$. She presents coordinates of ^4u via their standard forms, i. e sums of monomial terms taken in the lexicographical order and writes the public rule F $x_{0,1} \to f_{0,1}(x_{01}, x_{11}, \ldots x_{128,128})$, $x_{1,1} \to f_{1,1}(x_{01}, x_{11}, \ldots x_{128,128})$, $x_{1,2} \to f_{1,2}(x_{01}, x_{11}, \ldots x_{128,128})$, $\ldots$ $x_{128,128} \to f_{128,128}(x_{01}, x_{11}, \ldots x_{128,128})$.

Finally Alice announces this multivariate rule for public users. Noteworthy that for the development of this private key Alice use only operations of addition and multiplication in the commutative ring $F_{2^{32}}[x_{01}, x_{11}, x_{1,2}, \ldots, x_{128,128}]$.

ENCRYPTION PROCESS.

Public user Bob creates her message p $=$ $(p_{0,1}$, from the space $(F_{2^{32}})^m$, $m = 256$. He computes tuple $(f_{0,1}(p_{01}, p_{11}, \ldots, p_{128,128})$, $f_{1,1}(p_{01}, p_{11}, \ldots, p_{128,128})$, $f_{1,2}(p_{01}, p_{11}, \ldots, p_{128,128})$, …, $f_{128,128}(x_{01}, x_{11}, \ldots x_{128,128}))$ of the ciphertext c. Theoretical estimation of the execution time is $O(m^4)$. Let $D(m)$ be the density of the public rule F, which is a total number of monomial terms in all multivariate polynomials f_{01}, f_{11}, f_{12}, …. Execution time is $cD(m)$ where constant c is time of the computation of single cubic monomial term. This constant depends on the choice of the computer. The following parameters can be useful. $D(16) = 5623$, $D(32) = 62252$, $D(64) = 781087$, $D(128) = 10826616$, $D(256) = 138266164$.

We can speed up the encryption process via reduction of parameter s. If we take twice shorter of the path of the graph, i.e. select $s = m/2$ then the values of $D(m)$ would be the following. $D(32) = 5623$, $D(64) = 62252$, $D(128) = 781087$, $D(256) = 10826616$.

This numbers disclose an interesting remarkable coincidences.

We can encode each character of $F_{2^{32}}$ by four symbols of F_{2^8}. Thus we can identify plaintext and the ciphertext with the tuple of binary symbols of length 1024. So we can encrypt files with extensions .doc, .jpg, .avi, .tif, .pdf and etc.

DECRYPTION PROCEDURE.

Alice has the private key which consists of the sequence t_1, t_2, …, t_{256} and matrices ^1T and ^2T. Assume that she got a ciphertext c from Bob. She computes $^2T^{-1} \times c =^1 c$ and treats this vector as line $[^1l] = [c_{01}$, c_{11}, c_{12}, …, $c_{128,128}]$. Alice computes parameter $d = c_{01}{}^{31}$. She changes the colour of $[^1l]$ for $d + t_256$ and gets the line $[l] = [d + t_{256}, c_{11}, c_{12}, \ldots, c_{128,128}]$. Alice has to form the path in the graph $A(256, F_{2^{32}})$ with the starting line $[l]$ and further elements defined by colours $d + t_{255}$, $d + t_{254}$, $d + t_{253}$, …, $d + t_1$ and d. So she computes the destination line $[^1l] = [d$, $d_{1,1}$, d_{12}, …, $d_{128,128}]$. Finally Alice computes the plaintext p as $[1^l] \times^2 T^{-1}$.

VIII. Heuristic arguments on security and cryptanalitic aspects

Recall that the piece of information T is a trapdoor accelerator for nonlinear σ if the knowledge of T allows us to compute the reimage of given value b in time $O(n^2)$.

Of course it is just instrument to search for practical trapdoor function. Without knowledge of T one has to solve nonlinear system of equations which generally is NP-hard problem. As you know that the existence of trapdoor functions is just a conjecture. In fact it is closely connected to Main Conjecture of Cryptography $P \neq NP$. Finding of inverse for σ is NP-hard problem if this map is in so called "general position". In case of the knowledge of specific additional information can lead to establishment of polynomial method for the construction of the inverse map. For instance if cubical σ has the inverse map of degree 3 then on can create $O(n^3)$ pairs of kind (plaintext, ciphertext) and reconstruct the inverse in time $O(n^{10})$. In the case of our nonlinear graph based the order of inverse is rather high. In fact we prove the following statement via presentation of explicit construction.

THEOREM.

Let F_{2^r} be a finite field and $r \geq 3$. Then for each n, $n \geq 3$ there exists an element $\sigma \in ({}^nCG(F_q))$ of degree 3 with trapdoor accelerator such that $deg(\sigma^{-1}$ is $\geq 2^{r-1}$.

We hope that presented lower bound on the degree is far from being sharp.

Specific multivariate candidates for being "practical trapdoor functions" often refers to some specific hard problems related to their cryptanalitic investigations. Recent example is MiniRank problem connected with the studies of properties Unbalanced rainbow Like Oil and Vinegar Cryptosystem. Last cryptanalitic results on this subject reader can find in [46]. So in the case of the cryptosystem we suggest in Example 6. 2 the following reference is relevant.

Cryptanalitic has to decompose G_m given in its standard form into $G_n = T_1F_nT_2$ where T_1 and T_2 are elements of affine group $AGL_n(F_q)$ and F_m is graph based transformation. This is difficult group theoretical problem of triple factorisation.

Let us assume that this problem is somehow solved. Then he/she has to solve the problem to find algorithm for the computation of reimages for F_m via investigation the pathes between selected vector $p = (p_1, p_2, \ldots, p_n)$ and vector of kind $(y,\ f_2(p_1, p_2, \ldots, p_n), f_3(p_1, p_2, \ldots, p_n), \ldots, f_n(p_1, p_2, \ldots, p_n))$. Let us assume that the length of the pass s is chosen by Alice as $\alpha n + \beta$, where α and β are constant, and even k is less than half of the girth of the graph $A(n, k)$ which is also given by some linear function from variable n (see [27]). Then specialisation of $y = b$ defines uniques path between $(p_1, p_2, \ldots, p_n)$ and ${}^bu$ $=(b,\ f_2(a_1, a_2, \ldots, a_n), f_3(x_1, x_2, \ldots, x_n), \ldots, f_n(p_1, p_2, \ldots, p_n))$. All specialisations of y are easy to observe. The path for some specialisation will give us remaining parameters a_1, a_2, …, a_s of the trapdoor. This natural way to break the system is not easy to implement. The path between p and ${}^bu$ can be computed with the usage of general Dijkstra algorithm for arbitrary graph of order v. The complexity of this algorith is just $vln(v)$ but v is $2q^n$ and we have exponential complexity in term of our parameter n. Alternatively one can use unknowns z_1, z_2, …, z_{s-1}, b corresponding to colours of the path with initial point p and final point ${}^bu$. He/ she can compute the coordinates h_i of the destination point of the path as polynomial expressionss from variables z_j, $j = 1, 2, \ldots, s-1$ and investigate the system of equations $h_j(z_1, z_2, \ldots, z_j) ={}^b u_j$, $j = 2, 3, \ldots, s-1$. This system of equations has linear degree as the expression from parameter n, secret length s is unknown. That is why this system is hard to solve. As we mentioned above the graph ${}''A(n, F_q)$ is an approximation of the infinite q-reqular tree for which the complexity of finding the path between vertices at length s is $q(q-1)^{s-1}$ ("breadth force search"). So the task of finding the shortest path in the tree approximation will lead to improvement of many applied algorithms in Computer Science.

if parameter s is greater than $(g-2)/2$ where g is the girth then the path between two points at the distance s is not uniquely determined. So the cryptanalisis becomes even more sophisticated task.

REMARK. We can use tree approximation $D(n, F_q)$ instead of $A(n, q)$. In the case the girth of the graph is at least $n + 5$.

IX. On the generalisations of the public keys and the implementations

We suggest modifications of cubic $D(n, K)$ transformations presented before which is based on the descriptions of the connected components of these graphs. Recall that the family of graphs $D(n, K)$, $n = 2, 3, \ldots$ where K is arbitrary commutative ring defines the projective limit $D(K)$ with points $(p) = (p_{10}, p_{11},$
$p_{12}, p_{21}, p_{22}, p'_{22}, \ldots, p'_{ii}, p_{ii+1}, p_{i+1,i}, p_{i+1,i+1}, \ldots)$, and lines $[l] = [l_{01}, l_{11}, l_{12}, l_{21},$
$l_{22}, l'_{22}, \ldots, l'_{ii}, l_{ii+1}, l_{i+1,i}, l_{i+1,i+1}, \ldots]$.

which can be thought as infinite sequences of elements in K such that only finitely many components are nonzero. The incidence of points and lines is given by the system of equations (3).

Let $k \geq 6$, $t = [(k+2)/4]$, and let $u = (u_i, u_{11}, \ldots, u_{tt}, u'_{tt}, u_{t,t+1}, u_{t+1,t}, ...)$ be a vertex of $D(k, K)$. We assume that $u_1 = u_{1,0}(u_{0,1})$ if u be a point (a line, respectively). It does not matter whether u is a point or a line. For every r, $2 \leq r \leq t$, let $a_r = a_r(u) = \Sigma_{i=0,r}(u_{ii}u'_{r-i,r-i}u_{i,i+1}u_{r-i,r-i-1})$

and $a = a(u) = (a_2, a_3, \ldots, a_t)$.

The following statement was proved in [58] for the case $K = F_q$. Its generalization on arbitrary commutative rings is straightforward, see [6], [7].

PROPOSITION 4.1.

Let K be a commutative ring with unity and u and v be vertices from the same connected component of $D(k, K)$. Then $a(u) = a(v)$. Moreover, for any $t1$ ring elements $x_i \in K$, $2 \leq i \leq [(k+2)/4] = t$, there exists a vertex v of $D(k, K)$ for which $a(v) = (x_2, x_3, \ldots, x_t) = (x)$.

So the classes of equivalence for the relation$\tau = \{(u, v) | a(u) = a(v)\}$ on the vertexes of the graph. $D(n, K)$ are unions of connected components.

THEOREM 4.1 [7]. *For each commutative ring with unity, the graph $D(k, K)$ is edge transitive.*

Equivalences classes of τ form an imprimitivity systems of automorphism group of $D(k, K)$. Graph $C(n, K)$ was introduced in [9] as the restriction of incidence relation of $D(k, K)$ on a solution set of system of homogeneous equations $a_2(x) = 0$, $a_3(x) = 0$, …, $a_t(x) = 0$. The dimension of this algebraic variety is $n - t = d$. Thus $d = [4/3n] + 1$ for $n = 0, 2, 3 \ mod \ 4$, $d = [4/3n] + 2$ for $n = 1 \ mod \ 4$. For convenience we assume that $C(n, K) = C_d(K)$ Symbol $CD(k, K)$ stands for the connected component of graph $D(k, K)$. The following statement holds.

THEOREM 4.2 (see [45] and further references).

The diameter of the graph $C_m(K)$, $m \geq 2$, K is a commutative ring with unity of odd characteristic, is bounded by parameter $f(m)$ which does not depend on K.

COROLLARY 4. 1.

If K is a commutative ring with unity of odd characteristics then $CD(n, K) = C(n, K)$.

Let us rename coordinates $y_{1,0}, y_{1,1}, y_{1,2}, y_{2,1}, \ldots$ of symbolic line $[y]$ of $D(n, K)$ accordingly to the natural order on them as y_1, $y_2, \ldots, y_n$ and write the equations of the graph in new coordinates. It allows as to write connectivity invariants of the line $y = [y_1, y_2, \ldots, y_n]$ as $a_i([y]) = a_i(y_1, y_2, \ldots, y_n)$ where $i = 2, 3, \ldots, t$. Similar notations we will use in the case of points.

We use graphs $D(n, K)$ and $D(n, K[y_1, y_2, \ldots, y_n])$ to define family of cubic multivariate maps F of kind $y_1 \rightarrow f_1(y_1, y_2, \ldots, y_n)$, $y_2 \rightarrow f_2(y_1, y_2, \ldots, y_n)$, …, $y_n \rightarrow f_n(y_1, y_2, \ldots, y_n)$ with trapdoor accelerator $F = T_1 G_A T_2, T_1, T_2 \in AGL_n(K)$.

We take the line $[y_1, y_2, \ldots, y_n]$ of the graph $D(n, K[y_1, y_2, \ldots, y_n]$ and compute

$a_r = a_r([y]) = a_r(y_1, y_2, \ldots, y_n)$, for $r = 2, 3, \ldots, t$. We form the nonlinear expression ${}^sB = (y_1^s + C(y_2, y_3, \ldots, y_n)$ where $C(y_2, y_3, \ldots, y_n) = \lambda_2 a_2 + \lambda_3 a_3 + \ldots + lambda_t a_t + \lambda_1$ with nonzero λ_i from K and parameter s is selected with the usage of following options. We can use $s = 2$ if the order d of K^* is odd or $s = 3$ if $(d, 3) = 1$ and

$s = 1$ can be selected in the case of arbitrary commutative ring. We form the walk in the graph $D(n, K[y_1, y_2, \ldots, y_n])$ starting from the line $[y]$ of colour y_1 and consecutive vertexes of colours $y_1 + \beta_1$, $y_1 + \alpha_1, y_1 + \beta_2$, $y_1 + \alpha_2$,. . ., $y_1 + \beta_l$, α_l such that $0 \neq \alpha_1, 0 \neq \beta_1$, $\alpha_i \neq \alpha_{i+1}$, $\beta_i \neq \beta_{i+1}$ for $i = 1, 2, \ldots, l - 1$.

We form the path with the starting line $v_0 = [y])$, $v_1 = N_{y_1+\beta_1}(v_0)$, $v_2 = N_{y_1+\alpha_1}(v_1)$, …, $v_{2l-1} = N_{y_1+\beta_t}(v_{2l-2}$, $v_{2l-1} = N_{y_1+\beta_l}, v_{2l} = N_{\alpha_l}(v_{2t-1}$ and consider $u = J_{{}^sB}(v_{2l})$. The vertex u allows us to define the following transformation ${}^sG =^s G_A$, $A = (\alpha_1, \alpha_2, \ldots, \alpha_l; \beta_1, \beta_2, \ldots, \beta_l, B(y_1, y_2, \ldots, y_n))$ of K^n to itself

$y_1 \rightarrow (y_1)^s + C(y_1), y_2, \ldots, y_n)$,

$y_2 \rightarrow u_2(y_1, y_2)$,

$\ldots$

$y_n \rightarrow u_n(y_1, y_2, \ldots, y_n)$.

We identify $A =^l A$ with the array $(\alpha_1, \alpha_2, \ldots, \alpha_l; \beta_1, \beta_2, \ldots, \beta_{l-1}, \lambda_1, \lambda_2, , \lambda_t)$.

PROPOSITION.

TABLE I
PUBLIC MAP GENERATION TIME (MS), $D(n; B(32))$, CASE II, LENGTH OF THE PATH $(2l)$

n	**32**	**64**	**128**	**256**
16	20	36	60	108
32	164	336	676	1352
64	2660	5480	11305	23502
128	82304	175455	362382	751748

Let T_1 and T_2 are bijective transformations from $AGL_n(K)$ and K is arbitrary commutative ring with unity. Then the standard form of cubic transformation $F = T_1^s G_{l^A} T_2$, $l = O(n)$ has a trapdoor accelerator given by coefficients of T_1 and T_2 together with the array A described above.

Proof.

We have to justify that the reimage x of $v = s_A^G(x)$ can be computed in time $O(n^2)$. The procedure of its computation is the following.

Step 1. Let the value v of ${}^sG_A$ is given. We have to form $z = [\alpha_l, v_2, v_3, \ldots, v_n]$ where x is a variable, compute $a_2(z)\lambda_2 + a_3(z)\lambda_3 + \ldots + a_t(z)\lambda_t + \lambda_1 = C(y_1), y_2, \ldots, y_n)$

Step 2. The computation of the solution $y_1 = c$ of the equation ${y_1}^s + b = v_1$.

Step 3. We form the parameters $d_1 = c + \beta_l$, $d_2 = c + \alpha_{l-1}$, $d_3 = c + \beta_{l-1}$, $d_4 = c + \alpha_{l-2}, \ldots, d_{2l-1} = c + \alpha_1$, $d_{2l} = c$ of reverse path with the starting line $[\alpha_l, v_2, v_3, \ldots, v_n] = [z]$.

Step 5. We conduct recurrent computations $N_{d_1}(z) =^1 u$, $N_{d_2}({}^1u) =^2 u$, …, $N_{d_{2l-1}(2l-2u)=^{2l-1}u, N_c({}^2l-1} =^2 lu = x$ (the reimage)

The complexity of the algorithm is $O(n^2)$. So the map has a trapdoor accelerator as it is stated.

The standard forms of transformations $F = T_1^s G_A T_2$ can be used as a public keys.

The idea of $D(n, K)$ based encryption with the usage of connectivity invariants was suggested in [59].

X. On the execution time of generation of $D(n, K)$ -based public keys

We use computer simulation to generate maps of kind $y = T_1 G_A T_2 h$ related to graphs $D(n, K)$ where K is one of the commutative rings: Boolean ring $B(32)$of order 2^{32}, modular ring $Z_{2^{32}}$ and finite field $F_{2^{32}}$.

We have implemented three cases of invertible affine transformations: 1) T_1 and T_2 are identities, its just evaluation of time execution of core quadratic transformation. 2) T_1 and T_2 are of kind $x_1x_1 + a_2x_2 + a_3x_3 + \ldots + a_nx_n$ (linear time of computing execution of T_1 and T_2), 3) $T_1 = A_1x + b_1 and T_2 = A_2x + b_2$, nonsingular matrices A_1, A_2 have nonzero entries and vectors b_1, b_2 with mostly all coordinates different from zero.

Execution time for the computation of standard forms of the maps in the cases 2 and 3 is presented in Tables 1-6. The program is written in C++ and compiled with the gcc compiler. We used an average PC with processor Pentium 3.00 GHz, 2GB memory RAM and system Windows 7.

TABLE II
PUBLIC MAP GENERATION TIME (MS), $D(n; Z2^{32})$, CASE II, LENGTH OF THE PATH $(2l)$

n	**32**	**64**	**128**	**256**
16	16	28	56	104
32	168	344	700	1428
64	2856	6112	12620	25652
128	80227	179877	398918	842802

TABLE III
PUBLIC MAP GENERATION TIME (MS), $D(n; F2^{32})$, CASE II, LENGTH OF THE PATH $(2l)$

n	**32**	**64**	**128**	**256**
16	48	100	212	420
32	648	1372	2816	5712
64	8397	19454	41568	85783
128	139366	357361	824166	1758059

XI. Conclusions

Multivariate Cryptography in wide sense is about constructions and investigations of Public Keys in a form of nonlinear Multivariate rule defined over some finite commutative ring K.

These rule F has to be written as transformation $x_i \to f_i$, $i = 1, 2, \ldots, n$, $f_i \in K[x_1, x_2, \ldots, x_n]$ over commutative ring K. It can be used for the encryption of tuples (plaintexts) from the affine space K^n. In the simplest case of bijective transformation decryption process can be thought as application of inverse rule G.

The rule F defines automorphism σ_n of multivariate ring $K[x_1, x_2, \ldots, x_n]$ into itself given by its values on variables x_i. Its degree can be defined as maximum of degrees of polynomials f_i. For the usage of F as efficient encryption tool degree of σ_n can be bounded by some constant c, cases of $c = 2$ or $c = 3$ are popular.

Multivariate public key scheme suggests that rule F is given publicly. Public users use it for encryption, they are unable to decrypt because the information on G is not given. Presumably G hast to be of high degree to be resistant against its approximation attempts. The key owner (Alice) suppose to have some additional piece T of private information about pair (F, G) to decrypt ciphertext obtained from public user (Bob). In [43] the following formalisation of T is given.

TABLE IV
PUBLIC MAP GENERATION TIME (MS), $D(n; B(32))$, CASE III, LENGTH OF THE PATH $(2l)$

n	**32**	**64**	**128**	**256**
16	16	32	56	108
32	240	416	764	1464
64	5357	8509	14802	27391
128	192324	310666	547293	1020502

TABLE V
PUBLIC MAP GENERATION TIME (MS),$D(n; Z2^{32})$, CASE III, LENGTH OF THE PATH $(2l)$

n	**32**	**64**	**128**	**256**
16	20	32	56	104
32	260	440	800	1520
64	5524	8780	15180	28381
128	180436	289475	507985	945409

TABLE VI
PUBLIC MAP GENERATION TIME (MS), $D(n; F2^{32})$, CASE III, LENGTH OF THE PATH $(2l)$

n	**32**	**64**	**128**	**256**
16	140	268	524	1036
32	2328	4541	8968	17828
64	40417	77480	151592	299844
128	812140	1526713	2946022	5792889

We say that family σ_n, $n = 2, 3, \ldots$ has trapdoor accelerator ${}^nT$ if the knowledge of the piece of information ${}^nT$ allows to compute reimage x of $y = \sigma_n(x)$ in time $O(n^2)$.

We use families of extremal algebraic graphs which approximate infinite forest (or tree) for the constructions of families of automorphisms σ_n with trapdoor accelerators and $(\sigma_n)^{-1}$ of large order. We use bipartite regular graphs ${}^nG(K)$ with partition sets K^n (set of points and set of lines), such that incidence relation between point and line is given by system of linear equations over K and projective limit of bipartite graphs ${}^nG(K)$ is well defined tends to infinite regular forest. Two families $D(n, K)$ and $A(n, K)$ defined over arbitrary integrity domain K, i. e. commutative ring without zero divisors, are known.

To define trapdoor accelerator for the family σ_n, $n = 2, 3, \ldots$ we use special walks on graphs ${}^nG(K)$ and ${}^nG(K[x_1, x_2, \ldots, x_n])$. This way in the case of $K = F_{2^m}$ we construct trapdoor accelerator ${}^nT$ for the special map σ_n with the inverse of order $> 3 \times 2^{m-1}$. So we can construct a family of public keys working with the space of plaintexts $F^n_{2^{64}}$ and multivariate rule F with the inverse of order $> 3 \times 2^{63}$. In this paper we discuss the implemention of not so ambitious case $m = 32$ which is also can give secure and efficient cryptosystem. A generalisation and obfuscation of this $D(n, F_q)$ based public key is given in a previous section on the case of general commutative ring K with unity. It uses connectivity invariants of these graphs. These algorithms are implemented in the cases of finite fields of characteristic 2, arithmetic rings Z_q where q is a power of 2 and Boolean rings.

We describe several other trapdoor accelerators defined with described above approach in selected cases of finite fields and arithmetical rings Z_m, where m is a prime power. They can be used for the constructions of multivariate public keys which is able to serve as tools for the encryption or construction of digital signatures.

References

[1] Erdős' P., R'enyi A., S'oc V. T. *On a problem of graph theory*, Studia. Sci. Math. Hungar.- 1.- 1966.- P. 215-235.

[2] Erdős' P., Simonovits M. *Compactness results in extremal graph theory* , Combinatorica.- 1982.-2 (3).- 1982.- P. 275-288.

[3] F. Lazebnik, V.Ustimenko, *Some Algebraic Constructions of Dense Graphs of Large Girth and of Large Size*, DIMACS series in Discrete Mathematics and Theoretical Computer Science , v.10, (1993) 75 93.

[4] F. Lazebnik, V.Ustimenko, *Some Algebraic Constractions of Dense Graphs of Large Girth and ofLarge Size*, DIMACS series in Discrete Mathematics and Theoretical Computer Science , v.10, (1993) 75 - 93.

[5] F.Lazebnik V. Ustimenko and A.J.Woldar, *A new series of dense graphs of high girth*, Bulletin of the AMS 32 (1) (1995), 73-79.

[6] V. Ustimenko, *Coordinatisation of Trees and their Quotients*, in the Voronoj's Impact on Modern Science, Kiev, Institute of Mathematics, 1998, vol. 2, 125-152.

[7] V. Ustimenko, *Linguistic Dynamical Systems, Graphs of Large Girth and Cryptography*, Journal of Mathematical Sciences.- Springer.- vol.140.- N3 .- 2007 .- P. 412-434.

[8] V. . Ustimenko *On the extremal graph theory and symbolic computations*, Dopovidi National Academy of Sci, Ukraine, 2013, No. 2, p. 42-49.

[9] V. Ustimenko, *CRYPTIM: Graphs as Tools for Symmetric Encryption*, Lecture Notes in Computer Science, Springer, LNCS 2227, Proceedings of AAECC-14 Symposium on Applied Algebra, Algebraic Algorithms and Error Correction Codes, November 2001, pp. 278-286.

[10] A. Tousene, V. Ustimenko, *CRYPTALL - a System to Encrypt All Types of Data*, Notices of Kiev - Mohyla Academy, vol. 23, 2004, pp. 12-15.

[11] A. Tousene, V. Ustimenko, *Graph based private key crypto-system*, International Journal on Computer Research, Nova Science Publisher, vol.13, issue 4, 2005, 12pp.

[12] V. Ustimenko, *On the graph based cryptography and symbolic computations*, Serdica Journal of Computing, Proceedings of International Conference on Applications of Computer Algebra 2006, Varna, N1 (2007).

[13] S. J. Kotorowicz, V. A. Ustimenko, *On the implementation of cryptoalgorithms based on algebraic graphs over some commutative rings*, Condenced Matters Physics, Special Issue: proceedings of the international conferences on finite particle systems, Complex systems theory and its application, Kazimerz Dolny, Poland, 2006, 11 no.2 (54), 2008, 347-360.

[14] J. Kotorowicz, U. Romaczuk, V. Ustimenko, *Implementation of stream ciphers based on a new family of algebraic graphs*, Proceedings of Federated Conference on Computer Science and Information Systems (FedCSIS), 2011, 13 pp.

[15] V. Ustimenko, U. Romaczuk, *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 TuringSeries: Studies in Computational Intelligence, Vol. 427, Springer, January , 2013, 257-285.

[16] M. Klisowski, V. Ustimenko, *On the comparison of cryptographical properties of two different families of graphs with large cycle indicator*, Mathematics in Computer Science, 2012, Volume 6, No. 2, pp. 181-198.

[17] V. Ustimenko, U. Romanczuk-Polubiec, A. Wroblewska, M. Polak, E. Zhupa, *On the constructions of new symmetric ciphers based on nonbijective multivariate maps of prescribed degree*, Security and Communication Networks, Volume 2019, Article ID 213756.

[18] Alexei G. Myasnikov, Vladimir Shpilrain, Alexander Ushakov. *Noncommutative Cryptography and Complexity of Group-theoretic Problems*. American Mathematical Society, 2011.

[19] A. G. Myasnikov, A. Roman'kov, *A linear decomposition attack*, Groups Complex. Cryptol. 7, No. 1 (2015), 81-94.

[20] V. A. Roman'kov, *A nonlinear decomposition attack*, Groups Complex. Cryptol. 8, No. 2 (2016), 197-207.

[21] V. Roman'kov, *An improved version of the AAG cryptographic protocol*, Groups, Complex., Cryptol, 11, No. 1 (2019), 35-42.

[22] A. Ben-Zvi, A. Kalka and B. Tsaban, *Cryptanalysis via algebraic span*, In: Shacham H. and Boldyreva A. (eds.) Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2018, Proceedings, Part I, Vol. 10991, 255-274, Springer, Cham (2018).

[23] B. Tsaban, *Polynomial-time solutions of computational problems in noncommutative-algebraic cryptography*, J. Cryptol. 28, No. 3 (2015), 601-622.

[24] B. Bollobas, *Extremal Graph Theory*, Academic Press 1978, Dover, 2004.

[25] B. Bollobas, *Random Graphs*, Academic Press 1985. Cambridge University Press, 2001.

[26] V. Ustimenko, *On infinite connected real networks without cycles and pseudorandom and random real sequences*, Isaac Newton Institute, workshop fractional kinetics, hydrodynamic limits and fractals, 21.03.2033-25.03.2022, Cambridge, UK.

[27] V. Ustimenko, *On new results on Extremal Graph Theory, Theory of Algebraic Graphs and their applications in Cryptography and Coding Theory*, IACR e-print archive, 2022/296.

[28] G. Margulis (1988), *Explicit group-theoretical constructions of combinatorial schemes and their application to desighn of expanders and concentrators*, Probl. Peredachi Informatsii, 24, No. 1, p.51-60.

[29] Margulis, Margulis G. A. *Explicit construction of graphs without short cycles and low density codes*, Combinatorica.- 2.- 1982, - P. 71-78.

[30] Lubotzky, Phillips, Sarnak, A. Lubotsky, R. Philips, P. Sarnak. *Ramanujan graphs*, J. Comb. Theory, 115, No. 2, 1989, p. 62-89.

[31] V. Ustimenko, M. Klisowski, *On Noncommutative Cryptography with cubical multivariate maps of predictable density*, In Intelligent Computing, Proceedings of the 2019 Computing Conference, Volume 2, Part of Advances in Intelligent Systems and Computing(AISC, volume 99, pp. 654-674.

[32] V. Ustimenko, *On semigroups of multivariate transformations constructed in terms of time dependent linguistic graphs and solutions of Post Quantum Multivariate Cryptography*. IACR e-print archive, 2021/1466.

[33] P. Dembovski, *Finite Geometries*, Springer, Berlin, 1968.

[34] J. Tits, *Sur la trialite at certains groups qui sendeduicent*, Publ. Math. I.H.E.S.(2), 1959, 15-20.

[35] J. Tits, Buildings of spherical type and Finite BN-pairs, Lecture Notes in Math, Springer Verlag,1974.

[36] J. A. Thas, Generalised polygons, Ch. 9 in. Buekenhout (ed) Handbook on Incidence Geometries, North Holland, Amsterdam,1995.

[37] A. Brouwer, A. Cohen, A. Niemaier, *Distance regular graph*, Springer, Berlin,1989.

[38] P.K. Wong, *Cages - a survey*, J. Graph Th.6(1982) 1-22.

[39] M. Polak, V. Ustimenko. *On LDPC codes corresponding to infinite family of graphs A(k,K)*, Proceedings of the Federated Conference on Computer science and information systems (FedCSIS) 2012, Wroclaw, pp. 11-23.

[40] MacKay, D. J. C. & Postol, M. S. (2003), *Weaknesses of Margulis and Ramanujan-Margulis low-dencity parity-check codes*. Electron. Notes Theor. Comput. Sci., 74, pp. 97-104.

[41] V. Ustimenko, *On new results on Extremal Algebraic Graph Theory and their connections with Algebraic Cryptography*, IACR e-print archive, 2022/1489.

[42] Tymoteusz Chojecki, Vasyl Ustimenko, *On fast computations of numerical parameters of homogeneous algebraic graphs of large girth and small diameter and encryption of large files*, IACR e-print archive, 2022/908.

[43] Vasyl Ustimenko, *On Extremal Algebraic Graphs and Multivariate Cryptosystems* IACR e-print archive, 2022/1537.

[44] Vasyl Ustimenko, *On the families of algebraic graphs with the fastest growth of cycle indicator and their applications*, IACR e-print archive, 022/1668(PDF)

[45] V. Ustimenko, *Graphs in terms of Algebraic Geometry, symbolic computations and secure communications in Post-Quantum world*, UMCS Editorial House, Lublin, 2022, 198 p.

[46] Anne Canteaut, Franois-Xavier Standaert (Eds.), *Eurocrypt 2021*, LNCS 12696, 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques Zagreb, Croatia, October 1721, 2021, Proceedings, Part I, Springer, 2021, 839p.

[47] O. Zariski, P. Samuel, *Commutative algebra*, 2, Springer (1975).

[48] I.R. Shafarevich, *Basic algebraic geometry*, Springer (1977) (Translated from Russian).

[49] R. Hartshorne, *Algebraic geometry*, Springer (1977).

[50] V. Ustimenko, *On new results on Extremal Graph Theory, Theory of Algebraic Graphs and their applications in Cryptography and Coding The ory*, Reports of Nath. Acad. of Sci. of Ukraine, 2022, No. 4, P. 42-49.

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

[52] N. Koblitz, *Algebraic aspects of cryptography*, Springer (1998), 206 P.

[53] L. Goubin, J.Patarin, Bo-Yin Yang, *Multivariate Cryptography, Encyclopedia of Cryptography and Security*, (2nd Ed.) 2011, 824-828.

[54] Post-Quantum Cryptography, *Call for Proposals:https://csrc.nist.gov/Project; Post-Quantum-Cryptography-Standardization / Call-for-Proposals, Post-Quantum Cryptography: Round 2 Submissions*.

[55] M. Noether, *Luigi Cremona*, Mathematische Annalen, 59 (1904), pp. 1-19.

[56] Yu. Bodnarchuk, *Every regular automorphism of the affine Cremona group is inner*, Journal of Pure and Applied Algebra 157 (2001) 115-119.

[57] I.R. Shafarevich, *On some infinite dimension groups II*, Izv. Akad. Sci. Ser. Math. 2 (1) (1981), 214-226.

[58] Lazebnik, F., Ustimenko, V.A. and A.J. Woldar, *A characterisation of the components of the graph $D(k, q)$*, Discrete Mathematics, 157 (1996), pp. 271-283.

[59] V. A. Ustimenko, *Graphs with special arcs and cryptography*, Acta Applicandae Mathematicae, vol. 71, N2, November 2002, pp. 117-153.