DOI: 10.15439/2023F7763
ISSN 2300-5963 ACSIS, Vol. 35

On the implementations of new graph based 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. Extended version of this article is available online at [31].**

I. Introduction

EXTREMAL algebraic graphs were traditionally used for the construction of stream ciphers of multivariate nature (see [19], [8] 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 [16] 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 [28]).

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 [20] and further references]). 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

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

Classical results of Multivariate Cryptography can find in [25], [26] and [27].

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 [17].

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 [1]-[6] 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 [1]), 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

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

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 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 named after the famous Luigi Cremona (see [29]). 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 $x_1 \to f_1(x_1, x_2, \ldots, x_n)$, $x_2 \to f_2(x_1, x_2, \ldots, x_n)$, …, $x_n \to f_n(x_1, x_2, \ldots, x_n)$ 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 $g \neq 0$ 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 [21], [22], [23]).

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 [15] and further references). The first algebraic forest approximation of a large girth was introduced by F. Lazebnik and V. Ustimenko (see [1], [2]) in the case of $K = F_q$.

The properties of trees of this algebraic forest and their approximations over F_q were investigated in the paper[30].

In 1998 more general algebraic graphs $D(n, K)$ defined over arbitrary commutative ring K were introduced [4]. 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 [5], simpler prove of this fact the reader can find in [18].

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 [5] 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 [7], [19], [8] and further references). They form a group $G_i = G(\Gamma_i)$ which can be a platform for the protocols of Noncommutative Cryptography (see [9]-[14]). 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 [6]. In fact these graphs were defined earlier [5] 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 [24] for each integrity domain K, $K \neq F_2$ graphs $A(n, K)$ form a tree approximation of large girth.

Some encryption algorithms (stream ciphers) based on $A(n, K)$ and $D(n, K)$ were already introduced (see [7], [19], [8], [16]).

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 [6]).

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 $A(n, K)$, $n = 2, 3, \ldots$ is bounded below by linear function cn for some positive constant c [24].

As a byproduct of this result we get that $A(n, q)$, $n = 2, 3, \ldots$ 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 [5] as homomorphism images of known graphs $CD(n, K)$ of large girth (see [1], [2], [3]).

Let K be a commutative ring with a unity. Graphs $A(n, K)$ belong to the class of linguitic graphs of type $(1, 1, n - 1)$ [19], i.e. bipartite graphs with partition sets $P = K^n$ (points of kind $(x_1, x_2, \ldots, x_n)$, $x_i \in K$) and $L = K^n$ (lines $[l_1, l_2, \ldots, l_n]$, $l_i \in K$) and incidence relation $I = I(n, K)$ such that $(x_1, x_2, \ldots, x_n) I [y_1, y_2, \ldots, y_n]$ if and only if $a_2 x_2 + b_2 x_2 = f_2(x_1, y_1)$, $a_3 x_3 + b_3 x_3 = f_3(x_1, x_2, y_1, y_2)$, $\ldots$, $a_n x_n + b_n x_n = f_n(x_1, x_2, \ldots, x_n)$, where a_i and b_i are elements of multiplicative group K^* of K and f_i are multivariate polynomials from $K[x_1, x_2, \ldots, x_{i-1}, y_1, y_2, \ldots, y_{i-1}]$ for $i = 2, 3, \ldots, n$.

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

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 $(x_1, x_2, \ldots, x_n)$ to point $(a, x_2, x_3, \ldots, x_n)$ and line $[x_1, x_2, \ldots, x_n]$ to line $[a, x_2, x_3, \ldots, x_n]$.

Let us consider a walk $v, v_1, v_2, \ldots, v_{2s}$ 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, $v_1 = {}^{a_1}C(v)$, $v_2 = N_{a_2}(v_1)$, $v_3 = {}^{a_3}C(v_2)$, $v_4 = N_{a_4}(v_3)$, …, $v_5 = {}^{a_5}C(v_4)$, …, $v_{4s} = N_{a_{4s}}(v_{4s-1})$, $v_{4s+1} = {}^{a_{4s+1}}C(v_{4s})$. 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 $a_1(x_1)$, $a_2(x_1)$, …, $a_{4s+1}(x_1)$ from $K[x_1]$. The final vertex of this walk is v_{4s+1} with coordinates $a_{4s+1}(x_1)$, $f_2(x_1, x_2)$, $f_3(x_1, x_2, x_3)$, …, $f_n(x_1, x_2, \dots, x_n)$). 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 $x_1 \to a_{4s+1}(x_1)$, $x_2 \to f_2(x_1, x_2)$, …, $x_n \to f_n(x_1, x_2, \dots, x_n)$ 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 $=$ $(a_1(x)$, $a_2(x)$, …, $a_k(x))$ × $(b_1(x)$, $b_2(x)$, …, $b_t(x)) = (a_1(x)$, $a_2(x)$, …, $a_{k-1}(x)$, $b_1(a_k(x))$, $b_2(a_k(x))$, …, $b_t(a(x)))$.

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 1.

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 2. (see [19] 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 1.

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 $u = (x + \alpha_1, x + \alpha_2, \dots, x + \alpha_k)$ 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 3.

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.

THEOREM 1. (see [19])

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 $K[x_1, x_2, \dots, x_n]$.

COROLLARY 1.

Let us consider element $u = (x, x + a_1, x + a_1, x + a_2, x + a_2, \dots, x + a_{k-1}, x + a_{k-1}x + a_k, x^t$ 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.

THEOREM 2. (see [19]). *For each commutative ring K groups $H_P(D(n, K)) = GD(n, K)$ are totalities of cubical automorphisms of $K[x_1, x_2, \dots, x_n]$.*

COROLLARY 2. *Let us consider element $u = (x, x + a_1, x + a_1, x + a_2, x + a_2, \dots, x + a_{k-1}, x + a_{k-1}, x + a_k, x^t)$ of F_K for commutative ring K with unity with finite multi-*

plicative 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.

V. Explicit constructions of trapdoor accelerators and their applications

EXAMPLE 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 $(x$, $x+\alpha_1$, $x+\alpha_1$, $x+\alpha_2$, $x+\alpha_2$, …, $x+\alpha_2$,…, $x+\alpha_s$, $x+\alpha_s)$ such that $cn < s < n$ for some constant $c > 0$. According to Theorem 2 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.

Let us consider the implementation of public key based on the trapdoor accelerator of Example 1.

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_{2^32} 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 $A(256, F_{2^32})$. 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}, $x_{01}+t_1$, $x_{0,1}+t_2$, …, $x_{0,1}+t_s$ 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}, $x_{01}+t_1$, $x_{0,1}+t_2$, … $x_{0,1}+t_s$ 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 $[{}^1l_{01}(x_{0,1}, x_{11}, \ldots,$ $x_{128,128})$, ${}^1l_{11}(x_{0,1}, x_{11}, \ldots, x_{128,128})$, … ${}^1l_{128,128}(x_{0,1}, x_{11}, \ldots, x_{128,128})] = [{}^1u]$. 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 ${}^3u = [{}^1u_{0,1})^2$, ${}^2u_{1,1}$, … ${}^2u_{128,128}]$ 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 $x_{0,1} \to f_{0,1}(x_{01}, x_{11}, \ldots, x_{128,128})$, $x_{1,1} \to f_{1,1}(x_{01}, x_{11}, \ldots, x_{128,128})$, $x_{1,2} \to f_{1,2}(x_{01}, x_{11}, \ldots, x_{128,128})$, … $x_{128,128} \to f_{128,128}(x_{01}, x_{11}, \ldots, x_{128,128})$.

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 $[{}^1l] = [c_{01}, c_{11}, c_{12}, \ldots, c_{128,128}]$. 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 $[{}^1l] = [d, d_{1,1}, d_{12}, \ldots, d_{128,128}]$. Finally Alice computes the plaintext p as $[1^l] \times^2 T^{-1}$.

VI. Conclusions

In [31] we describe several 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. In this paper we consider the important case of finite fields of characteristic 2. Computer simulations of several variants of implementation of this public keys are presented in [31] where time evaluation and numbers of monomial terms are given. In [31] the reader can find heuristic arguments on security of suggested public rules.

References

[1] 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.

[2] 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.

[3] 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.

[4] 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.

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

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

[7] 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.

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

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

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

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

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

[13] 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).

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

[15] B. Bolloba's', *Extremal Graph Theory*, Academic Press 1978, Dover, 2004.

[16] 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.

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

[18] 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)

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

[20] Anne Canteaut, François-Xavier Standaert (Eds.), *Eurocrypt 2021*, LNCS 12696, 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques Zagreb, Croatia, October 17–21, 2021, Proceedings, Part I, Springer, 2021, 839p.

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

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

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

[24] 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.

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

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

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

[28] $https : //csrc.nist.gov/pubs/pd/2021/08/04/migration - to - postquantum - cryptography/final$

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

[30] 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.

[31] V. A. Ustimenko, T. Chojecki, M. Klisowski, *On Extremal Algebraic Graphs and implementations of new cubic Multivariate Public Keys*, https://eprint.iacr.org/2023/744