On Extremal Algebraic Graphs and Multivariate Cryptosystems

Vasyl Ustimenko

Royal Holloway University of London,
Institute of Telecommunication and Global information Space, Kyiv, NAS of Ukraine
vasyl@hektor.umcs.lublin.pl
https://itgip.org/security_en/

Abstract. Multivariate rule $x_i \to f_i$, $i = 1, 2, \ldots, n$, $f_i \in K[x_1, x_2, \ldots, x_n]$ over commutative ring K defines endomorphism σ_n of $K[x_1, x_2, \ldots, x_n]$ into itself given by its values on variables x_i. Degree of σ_n can be defined as maximum of degrees of polynomials f_i. 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 extremal algebraic graphs for the constructions of families of automorphisms σ_n with trapdoor accelerators and $(\sigma_n)^{-1}$ of large order. We use these families for the constructions of new multivariate public keys and protocol based cryptosystems of El Gamal type of Postquantum Cryptography.

Some of these cryptosystems use as encryption tools families of endomorphisms σ_n of unbounded degree such that their restriction on the varieties $(K^*)^n$ are injective. As usual K^* stands for the multiplicative group of commutative ring K with the unity. Spaces of plaintexts and ciphertexts are $(K^*)^n$ and K^n. Security of such cryptosystem of El Gamal type rests on the complexity of word decomposition problem in the semigroup of Eulerian endomorphisms of $K[x_1, x_2, \ldots, x_n]$.

Keywords: Post Quantum Cryptography, extremal algebraic graphs, affine Cremona semigroup, Eulerian transformations, linguistic graphs over groups and commutative rings, public keys, protocols, protocol based cryptosystems

Funding: This research is supported by Fellowship of British Academy for Researchers at Risk, 2022

1 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 metho. As you see RUOV algorithm is investigated as appropriate instrument for the task (ii). During Third Round some cryptanalitic 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.

Noteworthy that all multivariate NIST candidates were presented by multivariate rule of degree bounded by constant (2 or 3) of kind $x_1 \to f_1(x_1, x_2, \ldots, x_n)$, $x_2 \to f_2(x_1, x_2, \ldots, x_n)$, $\ldots$, $x_n \to f_n(x_1, x_2, \ldots, x_n)$. In fact RUOV is given by quadratic system of polynomial equations. 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 $r > 1$.

We hope that classical multivariate public key approach is still able to bring reliable encryption algorithms.

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 small world graphs $A(n.q)$ (see [2], [3] and further references) and their analogs $A(n, K)$ defined over finite commutative ring K with unity for the construction of cubic multivariate public keys. Noteworthy to mention that for each prime power q, $q > 2$ graphs $A(n, q)$, $n = 2, 3, \ldots$ form a family of large girth (see [3]), there is well defined projective limit of these graphs which is a q-regular tree.

Further we obfuscate the encryption maps of these public keys via the combination of them with Eulerian transformation of K^n. We also use the new extraction technique to combine these public keys of degree 3 or linear degree αn, $\alpha > 0$ with postquantum protocols of Noncommutative Cryptography with the implementations on platform of Eulerian multivariate maps. We show that extraction technique can be used for the conversion of graph based symmetric ciphers to protocol based asymmetric algorithms of El Gamal type.

In Section 2 we present the known mathematical definitions of algebraic geometry for further usage of them as instruments of Multivariate Cryptography. In particular definitions of affine Cremona semigroup of endomorphisms of multivariate ring $K[x_1, x_2, \ldots, x_n]$ defined over commutative ring K, Eulerian transformations and affine Cremona group ${}^nCG(K)$ are presented there. This section contains the idea of Eulerisation of bijective map from affine Cremona semigroup, i.e. the usage of a composition of Eulerian transformation with the element of ${}^nCG(K)$.

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 ${}^nCG(K)$. This section also contains similar statements for toric transformations of ${}^nCS(K)$ which restrictions on $(K^*)^n$ are injective.

The description of linguistic graphs $A(n, K)$ and some their properties are presented in Section 3. It contains the description of subgroups and subsemigroups of ${}^nCS(K)$ defined via walks in graphs $A(n, K)$ and $A(n, K[x_1, x_2, \ldots, x_n])$. Some statements about degrees of elements of these semigroups are given.

Section 4 contains proofs of propositions of Section 2 via graph based explicite constructions. This section contain several examples of cryptographic applications of proven statements.

Implementation of twisted Diffie-Hellman protocol based on the platform semigroup ${}^nES(K)$ of Eulerian transformations is described in Section 5. Security of this protocol rests on the well known Conjugacy Power Search Problem (CPSP, see [14]) in the case of semigroup of Eulerian transformations. This unit also contains *tame homomorphism protocol* of [41] based on the canonical homomorphism of parabolic subgroup ${}^nP_m(K)$ onto ${}^nES(K)$ for $m > n$. Security of this protocol rests on the complexity of the Word Decomposition Search Problem for the case of group ${}^mES(K)$. The output of both protocols is the collision element from ${}^mES(K)$.

In Section 6 such output is used for the privatisation of earlier presented multivariate public keys with public rules from ${}^nCS(K)$. This process converts public rule to the protocol based El Gamal type cryptosystem. Its security rests on the security of the corresponding protocol. Two different methods are used for this purpose. The first one is safe delivery method which allows to transfer the public rule created by Alice to her partner Bob. The second method uses new idea of extraction the private password from the output of the protocol. So both correspondents use it for private key encryption of the public key.

In Section 7 extraction method is used for the conversion of symmetric stream ciphers of multivariate nature with encryption maps of nonpolynomial density to El Gamal type cryptosystems. In this case there are no options to use the encryption rule on the public key mode and linearisation attacks are not feasible.

More general idea to combine stream cipher of multivariate nature with the space of ciphertexts K^n with the output of the protocol based in computations in subgroups of affine Cremona semigroup ${}^mCS(K)$ is presented in Section 9. The combination is established via open logical scheme of key extraction given in terms of Predicates Calculus.

Section 8 is dedicated to the option of faster trapdoor accelerators with execution time $O(n^\alpha)$, $1 \leq \alpha < 2$ instead of $O(n^2)$. Some examples of this kind are given there.

Section 10 contains conclusions.

2 On elements of Algebraic Geometry, eulerisation of multivariate maps 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 $End(K[x_1, x_2, \ldots, x_n]) =^n CS(K)$ 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 kernal 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. Noteworty 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 $\delta(x_i)$. ${}^nES(K)$ stands for the semigroup of Eulerian endomorphisms, i. e. endomorfisms ω from ${}^nCS(K)$ such that $\omega(x_i) = a_i {x_1}^{a(i,1)} {x_2}^{a(i,2)} \ldots {x_{i_n}}^{a(i,n)}$, where a_i are elements of multiplicative group K^* of the ring.

We consider the group ${}^nEG(K)$ of all invertible elements of ${}^nES(K)$. We consider the totality $TA(n, K)$ of toric automorphisms, i. e. endomorphisms G from ${}^nCS(K)$ such that their restrictions on $(K^*)^n$ are injective maps. For G from $TA(n, K)$ we define its *toric inverter* as polynomial map G' from ${}^nCS(K)$ such that $G'G$ acts on $(K^*)^n$ as identity.

It is easy to see that if $G \in TA(n, K)$ and $H \in^n EG(K)$ then composition HG of H and G is a toric automorphism as well. a 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.

Then we can use *eulerisation* of this public rule given by standard form of $G_n = HF$ where H is an element of ${}^nEG(K)$. New public rule uses space of plaintexts $(K^*)^n$ and space of ciphertexts K^n. Noteworthy that the decryption is equivalent to consecutive application of ${F_n}^{-1)}$ and inverse H'_n in ${}^nEG(K)$ of H_n but the standard form of H'_nG^{-1} is impossible to compute.

More general class is the totality of *toric* multivariate rules G of kind $x_i \rightarrow G_i$ where G is a toric automorphism of $K[x_1, x_2, \dots, x_n]$ of constant degree d. We can take element H of ${}^nES(K)$ in "general position" and consider HG_n of linear degree and polynomial density with G_n. We say that HG_n is eulerisation of G_n. Recall that a transformation D is "in general position" if each $D(x_i)$ has monomial terms containing x_j for each $j = 1, 2, \dots, n$.

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 next section. We show there that the following statement holds.

PROPOSITION 2. 1.

For each commutative ring K with a unity there is a family of cubic maps $F_n \in^n CG(K)$ with trapdoor accelerator of level 3.

We say that family $F_n \in^n CG(K)$ has unbounded degree if degrees of F_n and ${F_n}^{-1}$ are bounded below by cn^α where c and α are positive constants.

The family F_n of unbounded degree has *symmetric trapdoor accelerator* T_n if the knowledge of piece of information ${}^nT$ allows to compute the value $y = F_n(x)$ for $x \in K^n$ and reimage x of given $y = F_n(x)$ in time $O(n^2)$.

THEOREM 2. 1.

For each commutative ring K with the unity there is the family $F_n \in^n CG(K)$ of unbounded degree with symmetric trapdoor accelerator ${}^nT$.

The explicit construction of the family as in the theorem is given in Section 3 and Section 4.

Notice that $\deg({F_n}^{-1})$ and $\deg(F_n)$ can be different. We say that F_n is unbalanced family of unbounded degree if $deg({F_n}^{-1})) - deg(f_n) \geq cn^\alpha$ for some $\alpha > 0$.

We present such families defined over special finite fields in the next sections.

REMARK 2.1.

Noteworthy that standard form (s. f.) of F_n of unbounded degree can be unknown.

REMARK 2.2.

The family as in Theorem 2. 1 can be used as stream cipher with the password ${}^nT$, the example is given in the next section.

REMARK 2.3.

Assume that the family of subsemigroups $S_n(K)$ of ${}^nCS(K)$ is used as platform of some protocol of Noncommutative Cryptography ([7]-[25]) with security based on complexity of Conjugacy Power Search Problem (CPSP).

The input consists of some elements of $S_n(K)$ and output is a collision element $C = C_n$ of the protocol. Asume that some *extraction function Ext* converts each element g of $S_n(k)$ to a trapdoor ${}^nT(K, g)$. Alice and Bob can conduct the protocol and use symmetric trapdoor accelerator ${}^nT(K, C_n$ to work with encryption function F_n and its inverse on the space K^n of plaintexts. The implementation of such scheme will be given in Section 5. Correspondents can also use other protocols of Noncommutative cryptography described in Section 4.

The family of toric automorphisms $F_n \in TA(n, K)$ has a *toric trapdoor accelerator* ${}^nT$ if the knowledge of ${}^nT$ allows for each $y \in F_n((K^*)^n)$ to find the solution x of $F_n(x) = y$ in time $O(n^2)$. The family of toric automorphisms $F_n \in TA(n, K)$ has *toric inverter* F_n if there is a family of $F'_n \in^n CS(K)$ such that $F_nF'_n$ acts on $(K^*)^n$ as the identity.

PROPOSITION 2.2.

For each finite commutative ring K with unity such that $|K| > 3$ and $|K|$ we construct a family of cubic toric automorphisms with toric trapdoor accelerator ${}^nT$ and inverter of degree $\geq 3t$ where t is maximal power of 3 in the interval $(0, |K|)$.

We say that family of toric automorphism has *unbounded degree* if $\deg(F_n)$ is $\geq cn^\alpha$ for some positive constants c and α.

PROPOSITION 2.3.

For each commutative ring K with $|K^*| > 1$ there is family $G_n \in^n EG(K)$ of unbounded degree with toric trapdoor accelerator.

PROPOSITION 2.4.

For each commutative ring K with $|K^*| > 1$ there is family of toric automorphisms F_n of unbounded degree and density $O(n^4)$ with toric trapdoor accelerator and inverter of non polynomial density.

Examples of families as in proposition above in the cases ($K = Z_m$ (see [26]) and $K = F_q$ (see [27]) were used for the construction of public keys with the space of plaintexts $(K^*)^n$ and ciphertexts K^n (implementation of one of such cryptosystems is described in [28]).

We show that the following statement holds.

PROPOSITION 2.5.

For each commutative ring K with $|K^*| \geq 3$ there is a family F_n of toric automorphisms of $K[x_1, x_2, \ldots, x_n]$ of unbounded degree and nonpolynomial density with toric trapdoor accelerator ${}^nT$ and inverter of unbounded degree.

Let F_n be a family of toric automorphisms with an invertor. We say that family G_n is its diagonaliser if for each n the composition of G_n and F_n is an element of ${}^nEG(K)$.

Examples in [26], [27] have cubic diagonaliser. Note that family $F_n \in^n CG(K)$ has identity transformation as diagonaliser. For each finite commutative ring we construct the family F_n satisfying the Proposition with the diagonaliser of unbounded degree.

PROPOSITION 2.6.

Let K be a finite commutative ring $d = |K^*| > 2$ and $(d, 3) = 1$. There is a family $F_n = H_nG_n$, where $H_n \in^n EG(K)$, $G_n \in^n CG(K)$ is unbalanced unbounded automorphism with toric trapdoor accelerator.

It is easy to see that diagonaliser of F_n is a family ${G_n}^{-1}$. Similar examples will be presented for each field F_{2^n}.

THEOREM 2. 2.

For each finite commutative ring K with large order d of K^* such that $(3, d) = 1$ there is a family F_n of toric automorphisms of $K[x_1, x_2, \ldots, x_n]$ with multivariate trapdoor and diagonaliser G_n of degree $\geq t$ where t is a maximal power of 3 from interval $(0, d)$.

Noteworthy that computations in the group ${}^nCS(K)$ are very difficult. The task of computation of the composition of n elements σ_1, σ_2, $\ldots$, σ_n in general position is not feasible because their degree are unbounded and degree of the composition of g_i and g_j in "majority cases" is the product of two degrees. Let S be a subsemigroup of ${}^nCS(K)$. Note that property of ability to compute the composition of arbitrary n polynomial maps from S in polynomial time implies the ability to compute the product of $O(n^t)$ elements from ${}^nCS(K)$. we say that S posesses the *property of multiple computation of composition*, shortly MCCP-property.

It is easy to see that General Affine Semigroup $AGS_n(K)$ of transformations of kind $(x_1, x_2, \ldots, x_n) \to (x_1, x_2, \ldots, x_n)A + (b_1, b_2, \ldots, b_n)$, where $A = (a(i, j))$ is a matrix with entries $a(i, j) \in K$, $i = 1, 2, \ldots, n$, $j = 1, 2, \ldots, n$ and $(b_1, b_2, \ldots, b_n) \in K^n$ and semigroup ${}^nES(K)$. Graph based constructions of other semigroups and groups with MCCP property will be considered in the next section.

3 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

$p_2 - l_2 = l_1p_1$, $p_3 - l_3 = p_1l_2$, $p_4 - l_4 = l_1p3$, $p_5 - l_5 = p_1l_4$, $\dots$, ,p$_n - l_n = p_1ln - 1$ hold for odd n and $p_n - l_n = l_1p_{n-1}$ 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 [2]).

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 $(p_1, p_2, \dots, p_n, \dots)$ and lines $[l_1, l_2, \dots, l_n, \dots]$ which is a projective limit of graphs $A(n, K)$ when n tends to infinity. If K, $|K| > 2$ is an integrity ring 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 [3].

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' (see [29]). In fact graphs $A(n, q)$ were obtained in [30] as homomorphis images of known graphs $CD(n, q)$ of large girth (see [31], [32], [33]).

Graphs $A(n, q)$ were intensively used for the constructions of LDPC codes for satellite communications (see [34]) and cryptographic algorithms (see [36], [35]) and further references). It was shown that $A(n, q)$ based LDPC codes have better properties in the comparison to those derived from $CD(n, q)$ or Cayley-Ramanujan graphs $X(p, q)$ [37] (see [38], [39]).

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 partitian 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 $u = (a_1, a_2, \ldots, a_{4s}, a_{4s+1})$ 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 $I(K[x_1, x_2, \ldots, x_n])$. 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 $v = (x_1, x_2, \ldots, x_n)$ (or line $[x_1, x_2, \ldots, x_n]$) of the graph $IK[x_1, x_2, \ldots, x_n]$ which uses colours $a_1(x_1)$, $a_2(x_1)$, ..., $a_{4s+1}(x_1)$ from $K[x_1]$. The final vertex of this walk is v_{4s+1} with coordinates $a_{4s+1}(x_1)$, $f_2(x_1, x_2)$, $f_3(x_1, x_2, x_3)$, ..., $f_n(x_1, x_2, \ldots, x_n)$). 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 $x_1 \to a_{4s+1}(x_1)$, $x_2 \to f_2(x_1, x_2)$, ..., $x_n \to f_n(x_1, x_2, \ldots, x_n)$ 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 $u = (a_1(x), a_2(x), \ldots, a_k(x))$ and $w = (b_1(x), b_2(x), \ldots, b_s(x))$ as word =(a$_1(x)$, $a_2(x)$, ..., $a_k(x)) \times (b_1(x)$, $b_2(x)$, ..., $b_t(x)$)=(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 3. 1.

Let $I(K)$ be a linguistic graph defined over commutative ring K with unity. The map ${}^{I(K)}\eta_P : F_K End(K[x_1, x_2, \ldots, x_n])$ 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 ${}^{I(K)\eta_L(F_K)=LS_L(I(K)}$.

POPOSITION 3. 2.

The image of $u = (a_1(x), a_2(x), \ldots, a_k(x))$ 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 $\mathrm{Aut}(K[x])$.

Proof. Let $u = (a_1(x), a_2(x), \ldots, a_k(x)$ be an element of F_K and $x \to a_k(x)$ has inverse $x \to b(x)$ in $End(K[x])$ in $SL_P(I(K))$. Then

$w = (a_{k-1}(b(x)), a_{k-2}(b(x), \ldots a_1(b(x)), b(x)) = Rev(u)$ is another element of F_K and ${}^{I(K)}\eta(u \times w)$ is the identity map. Thus ${}^{I(K)}\eta_P(w)$ is an inverse for ${}^{I(K)}\eta_P(u)$.

REMARK 3.1.

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 tranfrormations 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 $u = (x, f_1, f_1, f_2, \ldots, f_s, f_s)$. 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 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. 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.

REMARK 3.2.

Transitivity of $H_P(I(K)$ ($H_L(K)$) implies transitivity of group transformations of kind (G, K^n) where $G > H_P$ (or $G > H_L$ respectively.

PROPOSITION 3. 4. (see [30]).

Let K be an arbitrary commutative ring, $n \geq 2$ and $u = (x, f_1.f_1, f_2, f_2, \ldots, f_s, f_s)$, $s \leq n$ is an element of $\tilde{F}_K$. Then endomorphism $g = {}^A(n, K)\eta(u)$ has degree d, $d \geq 1 + deg(f_1) + (deg(f_2 - x) + (deg(f_3 - f_1)) + (deg(f_4 - deg f_2) \cdots + (deg(f_n - f_{n-2})$.

COROLLARY 3. 1.

If s is $\geq cn$ for $c > 0$ and $f_i - f_{i+2}$ are not constants than degree of g is $\geq cn)$ for some $c > 0$.

COROLLARY 3. 2.

Let $u = (x, f_1.f_1, f_2, f_2, \ldots, f_s, g_s)$ then $\deg(g) = {}^A(n, K)\eta(u)$ is at least maximum of d as above and $deg(g_s)$.

COROLLARY 3.3.

Assume that $x \to g_s$ is an automorphism of $K[x]$ and its inverse $x \to h(x)$ has degree t. Then reimage of g^{-1} is $Rev(u)$ for $u' = (x, f_1, f_2, \ldots, f_s, g_s)$. Note that $Rev(u) = (f_s(h),\ f_s(h),\ f_(s-1(h),\ f_{s-1}(h),\ f_1(h),\ f_1(h), h) of degree deg$ (h)(deg $(f_s) + deg(f_{s-1}) + deg(f_{s-3} - f_s) + deg(f_{s-4} - f_{s-2}) + \cdots + deg(h - f_1)$. So degree of inverse map is multiple of degree h.

The following statement was formulated in [42].

THEOREM 3. 1.

For each commutative ring K *group* $H_P(A(n,K)) = GA(n,K)$ *is a totality of cubical automorphisms of* $K[x_1, x_2, \ldots, x_n]$.

COROLLARY 3. 4.

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 with unity with finite multiplicatiove group of order* d, $d > 2$ *where* $t = 2$ *or* $t = 3$ *and* $(d,t) = 1$. *The transformation* ${}^{A(n,K)}\eta(u)$ *is a cubical one.*

As we already mentioned graphs $A(n,K)$ appear as homomorphic quotients of linguistic graphs $D(n,K)$ or their connected components $CD(n,K)$ (see [30]). Isomorphic groups $H_P(D(n,K)$ and $H_L(D(n,K)$ were introduced in [43]. The fact that elements of $H_P(D(n,K))$ $(GD(n,K)$ are transformations of degrre ≤ 3 in other notations) was proved in [44]. Theorem 1 was deduced from this fact. It is easy to see that the group $GA(n,K)$ possesses MCCP property.

4 Explicit constructions of trapdoor accelerators and their applications

PROOF OF PROPOSITION 2.1.

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.

PROOF OF THE THEOREM 2.1.

Let K be general commutative ring with unity. Let us consider the tuple of kind $u = (x,\ f_1(x),\ f_1(x),\ f_2(x),\ f_2(x),\ \ldots,\ f_s(x),\ f_s(x))$ from $K[x]^{2s+1}$ such that positive s is even and degrees d_i of each f_i satisfy condition $\alpha n < d_i < \beta n$ for some positive constants α and β and $d_i \neq d_{i+2}$, $i = 1, 2, \ldots, s-2$. Let us consider graph $A(n,K)$ and $F_n = T_1^{A(n,K)}\eta(u)T_2$ where T_1 and T_2 are elements of $AGL_n(K)$. Then according to Proposition 3.4 degrees of F_n and ${F_n}^1$ are of quadratic size cn^2 for $c > 0$. Let (p) = $(p_1,\ p_2,\ \ldots,\ p_n)$ from K^n be given. The knowledge of the triple $T = (T_1, T_2, u)$ allows to compute the colours $f_1(p_1)$, $f_2(p_1)$, $\ldots$, $f_s(p_1)$ of the walk with the starting point (p) in time $O(n^2)$. The computation of the destination of the walk also takes $O(n^2)$. The computation of colours of reverse walk and determination of its starting point take the same time. So T is a symmetric trapdoor accelerator of bijective multivariate map of unbounded degree. REMARK 4. 1.

In the case of finite commutative ring K with K^* of cardinality d, $d > 3$ such that $(d,3) = 1$ we can change the tuple u of the presented above construction for $u = (x,\ f_1(x),\ f_1(x),\ f_2(x),\ f_2(x),\ \ldots\ ,\ f_s(x),\ x^3)$. The family $F_n = T_1^{A(n,K)}\eta(u)T_2$ is formed by unbalanced multivariate maps of unbounded degree because degree of ${F_n}^{-1}$ coincides with degree ${}^{A(n,K)}\eta(Rev(u))$ which is

$> deg(F_n)$ and difference between $deg(F_n)$ and $deg{F_n}^{-1}$ is $\geq cn^2$ for some positive constant c. So we have example of unbalanced family of elements ${}^nEG(K)$ with symmetric trapdoor accelerator.

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

EXAMPLE 4. 1

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: $x \rightarrow x^2$ 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 $t_n = 32^{n^a-1}$.

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 accelerator ${}^{m,n}T$ 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 4.2.

We consider a modification of Example 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 toric automorphism with toric trapdoor accelerator.

EXAMPLE 4.3.

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 toric automorphism with trapdoor accelerator of level t. It can be used for the construction of public keys with the space of plaiexts $T_m(K)$ 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 $T_1(x_1) = a_1x_1 + a_2x_2 + \dots + a_m(x_m)$ 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 2.

The simplest example of family of toric transformations of unbounded degree can be defined as sequence of elements G_n from ${}^nEG(K)$.

EXAMPLE 4. 4.

Recall that ${}^nEG(K)$ stands for Eulerian group of invertible transformations from ${}^nES(K)$. It is easy to see that the group of monomial linear transformations M_n is a subgroup of ${}^nEG(K)$. So semigroup ${}^nES(K)$ is a highly noncommutative algebraic system. Each element from this semigroup can be considered as transformation of a free module K^n. Let π and σ be two permutations on the set $\{1, 2, \dots, n\}$. Let us consider a special transformation of $(K^*)^n$ where K is a commutative ring with the multiplicative group K^* of order d, $d > 2$. We define the transformation ${}^AJG(\pi, \sigma)$, where A is triangular matrix with positive integer entries $0 \leq a(i, j) < d$ from Z_d defined by the following closed formula (1).

$y_{\pi(1)=\mu_1 x^{a(1,1}_{\sigma(1)}}$,

$y_{\pi(2)=\mu_2 x^{a(2,1}_{\sigma(1)} x^{a(2,2}_{\sigma(2)}}$,

$\dots$

$y_{\pi(n)=\mu_n x^{a(n,1}_{\sigma(1)} x^{a(n,2}_{\sigma(2)} \dots x^{a(n,n}_{\sigma(n)}}$,

where $(a(1, 1), d) = 1$, $(a(2, 2), d) = 1$, $\dots$, $(a(n, n), d) = 1$.

We refer to ${}^AJG(\pi, \sigma)$ as Jordan - Gauss multiplicative transformation or simply JG element. It is an invertible element of ${}^nES(K)$ with the inverse of kind ${}^BJG(\sigma, \pi)$ such that $a(i, i)b(i, i) = 1$ $(mod\ d)$. Notice that in the case $K = Z_m$ straightforward process of computation the inverse of JG element is connected with the factorization problem of integer m. If $n = 1$ and m is a product of two large primes p and q the complexity of the problem is used in RSA public key algorithm. We say that τ is *tame Eulerian element* over K if it is a composition of several Jordan-Gauss multiplicative maps over commutative ring or field respectively. We take collection ^{n} of several Jordan Gauss transformations $J_1, J_2, \dots, J_k$, $k \geq 2$, $k = O(1)$ from ${}^nEG_n(K)$ and form $H_n = J_1J_2 \dots J_k$ written in its standard form. Assume that ${}^nT$ is expanded by adding ${J_i}^{-1}$ for $j = 1, 2, \dots, n$. It is clear that the knowledge of ${}^nT$ allows to compute the value $H_n(x)$ for $x \in (K^*)^n$ and ${H_n}^{-1}(y)$ for $y \in (K^*)^n$ in time $O(n^2)$. So H_n is a family of toric automorphisms with toric trapdoor accelerator ${}^nT$.

REMARK 4. 2. In the simplest case $k = 2$ users can work with J_1 and J_2 given by rules

$x_1 \to \mu_1 {x_1}^{a(1,1)}$

$x_2 \to \mu_1 {x_1}^{a(2,1)} {x_2}^{a(2,2)}$

...
$x_n \to \mu_1 {x_1}^{a(n,1)} {x_2}^{a(n,2)} \dots {x_n}^{a(n,n)}$
where $(a(1,1),d)=1$, $(a(2,2),d)=1$, ..., $(a(n,n),d)=1$.
and
$x_1 \to \beta_1 {x_1}^{b(1,1)} {x_2}^{b(1,2)} \dots {x_n}^{b(1,n)}$
$x_2 \to \beta_2 {x_2}^{b(2,2)} {x_2}^{b(2,3)} \dots {x_n}^{b(2,n)}$
...
$x_n \to \beta_n {x_n}^{b(n,n)}$
where $(b(1,1),d)=1$, $(b(2,2),d)=1$,..., $(b(n,n),d)=1$.

The inverter for H_n will be element ${J_2}^{-1}{J_1}^{-1}$ from ${}^nEG(K)$. Thus the diagonaliser of H_n can be taken as the unity of ${}^nEG(K)$.

The following examples are obtained via eulerisation of presented above families of multivariate maps with trapdoor accelerators.

EXAMPLE 4. 5.

Let K be arbitrary commutative ring with unity such that its multiplicative group contains at least 3 elements. We can use composition F_n of H_n described in Example 4 and G_n satisfying condition of Proposition 2.1 In the simplest case H_n is the composition of J_1 and J_2 which form the toric trapdoor. Recall that we constructed G_n as $T_1A(n,K)^{\eta}(u)T_2$ and its trapdoor accelerator (T_1,T_2,u) has level 3. The family of toric automorphisms F_n is the family of unbounded degree. Its density is $O(n^4)$. We have a factorization $F_n = J_1J_2T_1^{A(n,K)}\eta(u)T_2$. The knowledge on this factorization allows to compute $F_n(\mathrm{x})$, $\mathrm{x} \in {K^*}^n$ and solve equation of kind $F_n(\mathrm{x}) = \mathrm{y}$, $\mathrm{y} \in F_n({K^*}^n)$ in time $O(n^2)$. So (J_1,J_2,T_1,T_2,u) is a toric trapdoor accelerator of F_n. It is easy to see that the inverter $\mathrm{G}_n^{-1}{H_n}^{-1}$ has non polynomial density. So we prove the Proposition 2.4 It is easy to see that family F_n has cubic diagonaliser ${G_n}^{-1}$. The public key corresponding F_n satisfying Proposition 2.4 in the cases of finite fields and arithmetic rings Z_m were suggested in [26], [27], [47], their implementations are given in [28].

EXAMPLE 4. 6.

In the case of finite commutative ring K with multiplicative group K^* of order d, $d \geq 3$ such that $(d,3)=1$ we can change the string u from the Example 5 for the string $u = (x,\ x+a_1,\ x+a_1,\ x+a_2,\ x+a_2,\ \dots,\ x+a_{s-1},\ x+a_{s-1},\ x+a_s,\ x^3) and \mathrm{T}_1$ as in the Example 3. It is easy to see that the diagonaliser for modified family will have large degree. These explicit constructions give the proof of Theorem 2. 2.

EXAMPLE 4.7.

In the case of finite field F_{2^m} we modify example 5 via the change of u for $u = (x,\ x+a_1,\ x+a_1,\ x+a_2,\ x+a_2,\ \dots,\ x+a_{s-1},\ x+a_{s-1},\ x+a_s,\ x^2)$. So we get the toric automorphism of $K[x_1,x_2,\dots,x_n$ of linear degree of density $O(n^4)$ with the trapdoor accelerator (J_1,J_2,T_1,T_2,u). The diagonaliser for the member of the family will have degree $3 \times 2^{m-1}$. Noteworthy that in this case we have a free choice of elements T_1 and T_2 from $AGL_n(F_{2^m})$.

REMARK 4.3.

Note that in the example used for the prove of Proposition 2.1 as well in Examples 1, 2, 3, 5, 6, 7 the density of transformation F_n is $O(n^4)$. Computer simulation shows that if most of entries of T_1 and T_2 are non zero ring elements and the commutative ring K is chosen then the density $d(n,s)$ depends just on parameters n and s. The following list presents these densities in the case of Example 7 and $K = F_{2^{32}}$.

$d(16,16) = 76$, $d(16,32) = 148$, $d(16,64) = 288$, $d(16,128) = 576$, $d(16,256) = 1148$;

$d(32,16) = 1268$, $d(32,32) = 2420$, $d(32,64) = 4700$, $d(32,128) = 9268$, $d(32,256) = 18405$),

$d(64,16) = 22144$, $d(64,32) = 40948$,d(64, 64)=78551,d(64, 128)=153784,d(64, 256)=304240;

$d(128,16) = 460200$. $d(128,32) = 819498$, $d(128,64) = 153784$, $d(128,128) = 2970743$, $d(128,256) = 5836938$.

If we consider the case of $K = Z_{2^{32}}$ we obtain the following densities

$d(16,32) = 24$, $d(16,64) = 36$, $d(16,128) = 64$, $d(16,256) = 116$;

$$d(32,32) = 248$$

, $d(32,64) = 428$, $d(32,128) = 788$,d(32, 256)=1508,

$d(64,32) = 5317$, $d(64,64) = 5576$, $d(64,128) = 15216$, $d(64,256) = 28176$;

$d(128,32) = 180861$, $d(128,64) = 290432$, $d(128,128) = 509812$, $d(128,256) = 949652$.

The following examples give the polynomial maps of K^n for which the computation of its density is unfeasible. We will use Proposition 3.4 for these constructions.

EXAMPLE 4.8.

Let K be an arbitrary commutative ring,$n \geq 2$ and $u =(x,\ f_1,\ f_1,\ f_2,\ f_2,\ \ldots,\ f_s,\ f_s)$, $s \leq n$ is an element of $\tilde{F}_K$, such that $s \geq \alpha n$ for the constant $\alpha > 0$, $s \leq n$. Then endomorphism $G_{n,s} = {}^A(n,K)\eta(u)$ has degree d and $d \geq 1 + deg(f_1) + (deg(f_2 - x) + (deg(f_3 - f_1)) + (deg(f_4 - deg f_2) \cdots + (deg(f_n - f_{n-2})$. We select f_i of degree $> cn$ for $c > 0$ of size $O(n)$, $i = 1, 2, \ldots, s$ such that $\deg(f_i) \geq 1$, $deg(f_{i+2} \neq deg(f_i)$ for $i = 1, 2, \ldots, s-2$, $f_s = x + a$, $a \in K$ and density $O(1)$. We take two elements T_1 and T_2 in $AGL_n(K)$ and consider $F_n = T_1 G_{n,s} T_2$. The knowledge on the triple T $= (T_1, T_2, u)$ allows fast computation of $F_n(p_1, p_2, \ldots, p_n)$ and the reimage of transformation F_n. Note that elements of the tuple $(a_1 = f_1(p_1),\ a_2 = f_2(p_1),\ \ldots,\ a_s = f_s(p_1))$ can be computed in time $O(n)$ via Horner scheme with the usage of nested form of each f_i. So the tuple itself will be computed in time $O(n^2)$. The sequence of vertices $v_0 = (p_1, p_2, \ldots, p_n)$, $v_1 = N_{a_1}(v_0)$, $v_2 = N_{a_2}(v_1,\ \ldots,\ v_s = N_{a_s}(v_{s-1}$ also can be computed in time $O(n^2)$.

Assume that F_n(x) $= (c_1, c_2, \ldots, c_n)$ is given. We assume that standard forms of transformations ${T_1}^{-1}$ and ${T_2}^{-1}$ are known as well. So the computation of $y = {T_2}^{-1}(c_1, c_2, \ldots, c_n)$ of colour c_1 takes $O(n^2)$. The value of x_1 will be obtained from the equation $x_1 + a = y_1$.. Next step is the computation of $b_i = f_i(y_1 - a)$, its cost is also $O(n^2)$. Consecutive application of $N_{b_{s-1}}$, $N_{b_{s-2}}$, $\ldots$ N_{b_1} and N_{x_1} produces vector z in time $O(n^2)$. The reimage of $(c_1, c_2, \ldots, c_n)$ will be obtained as ${T_2}^{-1}(z)$ So we proved that T is a symmetric trapdoor accelerator for the bijective multivariate map F_n of unbounded degree.

EXAMPLE 4. 9.

Let $K = F_{2^m}$. We can take u as $(x,\ f_1,\ f_1,\ f_2,\ f_2,\ \ldots,\ f_s,\ x^2)$ where f_i are selected as in the previous example. Then the family of functions $F_n = {T_1}^{A(n,K)}\eta(u')T_2$ will be unbalanced bijective multivariate function of unbounded degreee with symmetric trapdoor accelerator (T_1, T_2, u').

EXAMPLE 4. 10.

Let us consider the case $K = F_q$ where $(q, 3) = 1$, $q \geq 4$. Then simple change of u' in the previous example for $\tilde{u} = (x,\ f_1,\ f_1,\ f_2,\ f_2,\ \ldots,\ f_{s-1},\ f_{s-1},\ f_s,\ x^3)$ leads to new example of unbalanced family of bijective maps with symmetric trapdoor accelerator.

EXAMPLE 4.11.

Let us consider the case of finite commutative ring K with zero divisors such that $(|K^*|, 3) = 1$ and work with $\tilde{u}$ as in the previous example. In this case we add additional requirements $T(x_1) = \beta x_1 where\beta$ is an element of K^*. In particular case Z_{2^m} we use condition $T(x_1) = x_1b_1 + x_2b_2 + \cdots + x_nb_n$ where number of odd residues b_i is odd. Then transformation $T_1^{A(n,K)}\eta(u)T_2$ is a toric automorphism of unbounded degree with symmetric trapdoor accelerator. The inverter of this map will be of unbounded degree.

REMARK 4.4.

In cases of Examples 4.9, 4.10, 4.11 let us consider "light trapdoor version" with transformations T_1 and T_2 of kind $x_1 \to x_1a_1 + x_2a_2 + \ldots x_na_n$ where a_i are elements of K^* and $x_j \to x_j$ for $j = 2, 3, \ldots$. We take $s = O(1)$, $s \geq 2$. Recall that degree of $f_1, f_2, \ldots f_{s-1}$ are $> cn$ for some positive constant c, their size is $O(n)$. It is easy to see that in this case F_n is still bijective function of unbounded degree but the knowledge of trapdoor allows to compute the value of multivariate function F_n and its reimage in time $O(n)$.

EXAMPLES 4.12, 4.13 and 4.14.

We can introduce further obfuscation of the previous Example 11 (toric automorphisms) and Examples 10 and 9 (bijective maps). After selection of commutative ring K elements of J_1 and J_2 from ${}^nES(K)$ as in Example 4 has to be constructed. In each of these cases we take transformation $W_n = J_1J_2T_1F_nT_2$ of nonpolynomial density. Its diagonaliser ${T_2}^{-1}{F_n}^{-1}{T_1}^{-1}$ has degree $\geq Cn^2$. The tuple (J_1, J_2, T_1, u, T_2) is a symmetric toric trapdoor accelerator of the toric automorphism of unbounded degree and nonpolynomial density.

The encryption via consecutive application of J_1, J_2, T_1, ${}^A(n, K)\eta(u)$, T_2 can be used in symmetric cipher working with the space of plaintexts $(K^*)^n$ and space of ciphertexts K^n.

5 On protocols of Noncommutative Cryptography with platforms of Eulerian transformations

5.1. TWISTED DIFFIE HELLMAN PROTOCOL.

Let S be an abstract semigroup which has some invertible elements.

Alice and Bob share element $g \in S$ and pair of mutually inverse elements h^{-1}, h from this semigroup. Alice takes positive integer $t = k_A$ and $d = r_A$ and forms $h^{-d}gh^d = g_A$. Bob takes $s = k_B$ and $p = r_B$ and forms $h^{-p}g^sh^p = g_B$. They exchange g_A and g_B and compute collision element X as ${}^Ag = h^{-d}{g_B}^th^d$ and ${}^Bg = h^{-p}{g_A}^sh^p$ respectively.

Adversary has g_A and g_B. He/she has to solve the equation $h^{-y}g^xh^y = g_A$ for x and y to break the protocol and get the collision element. This is well known Conjugacy Power Search Problem (CPSP) of Noncommutative Cryptography (see [8],[9], [14]). It is complexity depends on the choice of platform S. We use the case when S is a representative of family ${}^nES(K)$, $n = 2, 3, \ldots$ defined over finite commutative ring K with unity and order $d = |K^*|$ satisfying condition $d \geq 3$. With this platform CPSP is an intractable problem of Postquantum Cryptography.

One of the modifications of this algorithm is *group enveloped Diffie Hellman protocol* presented in [41]. It uses some generalization of CPSP property.

TAHOMA PROTOCOL 5. 2.

Let $S_1 <^1 S$ and $S_2 < 2^S$ be pairs of finite semigroups which contains invertible elements.

Assume that ϕ is homomorphism from S_1 to S_2. Then Alice and Bob can use the following *tame homomorphism (Tahoma) protocol.*.

1) Alice selects invertible element ${}^1h \in^1 S$ and ${}^2h \in^2 S$. Additionally she takes elements $g_1, g_2, \ldots, g_k$, $k \geq 2$ from ${}^1S$ and computes their homomorphic images $\phi(g_i)$, $i = 1, 2, \ldots, k$. Alice forms pairs $(a_i, b_i) = ({}^1hg_i{}^1h^{-1}, {}^2hg_i{}^2h^{-1})$

She sends these pairs (a_i, b_i), $i = 1, 2, \ldots, k$ to Bob.

He takes abstract alphabet $z_1, z_2, \ldots, z_k$ and forms the word of kind $w = w(z_1, z_2, \ldots, z_k) = z_{i_1}^{k(1)}z_{i_2}^{k(2)}\ldots z_{i_s}^{k(s}$, $s \geq 2$, $\{i_1, i_2, \ldots, i_s\}$ is a subset of cardinality s in $\{1, 2, \ldots, k\}$.

Bob forms specialisation $W(a_1, a_2, \ldots, a_k) = a_{i_1}^{k(1)}a_{i_2}^{k(2)}\ldots a_{i_s}^{k(s} = a$ and sends a to Alice. For himself he computes collision element

$W(b_1, b_2, \ldots, b_k) = b_{i_1}^{k(1)}b_{i_2}^{k(2)}\ldots b_{i_s}^{k(s} = b.$

Alice will compute the collision element via the sequence ${}^1a = {}^1h^{-1}a^1h$, ${}^2a = \phi({}^1a)$, ${}^3a =^2 h^2a^2h^{-1}$.

We consider the implementation of this algorithm in the case when S_1 and S_2 are Semigroups ${}^mES(K)$ and $ES_n(K)$, $m = m(n) > n$ and $|K^*| \geq 3$. Alice works with Parabolic subsemigroup $P(K) =^n P_m(K)$ of all endomorphisms g from S_1 such that $g(x_1)$, $g(x_2)$, …, $g(x_n)$ are monomials from $K[x_1, x_2, \ldots, x_n]$. She uses canonical homomorphism of ${}^nP_m$ to $End(K[x_1, x_2, \ldots, x_n])$ sending $g \in P(K)$ to $\phi(g) \in^n CS(K)$ given by the rule $x_i \to g(x_i)$, $i = 1, 2, \ldots, m$.

In the simplest case Alice takes ${}^1h$ as composition of ${}^1J_1$ moving x_i to $x_i^a(i,i)x_{i+1}^a(i,i+1)\ldots x_{i,m}^a(i,m)$, $(a(i,i),d) = 1$, $i = 1, 2, \ldots, m$ and ${}^1J_2$ moving x_i to $x_1^{b(1,i)x_2^{b(2,i)}x_2\ldots x_i^{b(i,i)}}$, $(b(i,i),d) = 1$, $i = 1, 2, \ldots, m$. where $a(i,j)$ and $b(i,j)$ for $i \neq j$ are presudorandom nonzero elements of Z_d. She forms ${}^1J_1 \times^1 J_2 =^1 h$.

Secondly Alice forms ${}^2h$ as composition of ${}^2J_1$ moving x_i to $x_i^c(i,i)x_{i+1}^c(i,i+1)\ldots x_{i,m}^c(i,m)$, $(c(i,i),d) = 1$, $i = 1, 2, \ldots, n$ and ${}^2J_2$ moving x_i to $x_1^{d(1,i)x_2^{d(2,i)}x_2\ldots x_i^{d(i,i)}}$

$(d(i,i),d)=1$, $i=1,2,\ldots,n$. where $c(i,j)$ and $d(i,j)$ for $i\neq j$ are presudorandom nonzero elements of Z_d. She forms ${}^2J_1 \times^2 J_2 =^2 h$. Alice selects elements g_1, g_2, …, g_k from $P(K)$ and starts the presented above protocol.

6 Privatisation of public keys

6. 1. PRIVATISATION OF CUBICAL PUBLIC RULES.

(i) *Save delivery method [41].*

Alice proposes to selected user Bob to start one of the protocol with output Y from ${}^nES(K)$ given by n monomial terms $q_i{x_1}^a(i,1){x_2}^{a(i,2)\ldots {x_n}^{a(i,n)}}$, $i=1,2,\ldots,n$. Alice and Bob form matrix A with entries $a(i,j)$ from Z_d and matrix B with entries $b(i,j)=(q_iq_j)^{a(i,j)}$. They form tuple f_i such that $f_1 = x+q_1$, $f_2 = x+q_2$, $f_3 = x+q_1+q_3$, $f_4 = x+q_2+q_4$, …. $x+q_1+q_3+\ldots q_{n-1}$, $x+q_2+q_4+\cdots+q_n$. She forms element of semigroup $u = (x,\ f_1,\ f_1,\ f_2,\ f_2,\ \ldots,\ f_n,\ f_n)$ and linear transformations R_1 moving x_i to $b(i,i)x_i+b(i,i+1)x_{i+1}+\cdots+b(i,n)x_{i,n}$, $i=1,2,\ldots,n$ R_2 moving x_i to b(1, i)x1 $+\, b(2,i)x_2x+\cdots+x_{i-1}^{b(i-1,i)}+x_i$, $i=1,2,\ldots,n$. Alice and Bob independently creates $H=R_1R_2^{A(n,K)}\eta(u)R_2R_1$ in its standard form. She creates one of cubical public rules G as above. She sends $H+G$ to Bob. He restores G and uses it for encryption.

(ii) *Extraction method in the case of a field.*

Let $K=F_q$. After the completion of the protocol each correspondent forms matrices A, B, transformations R_1 and R_2 as in (i). Instead of $u=(x,\ f_1,\ f_1,\ f_2,\ f_2,\ \ldots,\ f_n,\ f_n)$ they form $w=(x,\ f_1,\ f_1,\ f_2,\ f_2,\ \ldots,\ f_n,\ x^e)$, where $e=2$ in the case of even q, or $e=3$ on the case of $(3,q-1)=1$.

Each of them uses consecutive application of R_1, R_2, ${}^{A(n,K)}\eta(u)$, R_2, R_1 for the encryption and ${R_1}^{-1}$, ${R_2}^{-1}$, ${}^{A(n,K)}\eta(Rev(u))$, ${R_2}^{-1}$, ${R_1}^{-1}$ for the decryption. meth This is symmetric a cipher supported by postquantum secure key exchange protocol.

(iii) *Extraction method in the case of commutative rings.*

Each correspondent forms matrices R_1, R_2 as in the previous cases. They form R_1' moving x_i to $b(i,i)x_i+b(i,i+1)x_{i+1}+\cdots+b(i,n)x_{i,n}$, $i=2,3,\ldots,n$ such that $R_1'(x_1)=b(1,n)x_n$. Alice and Bob use consecutive application of R_2, R_1', ${}^{A(n,K)}\eta(u)$, R_1 and R_2 for the encryption.

REMARK 6.1.

In the case of $K=Z_{2^r}$, $r\geq 2$ correspondents can use more general expression for $R_1'(x_1)$ of kind $b(1,1)x_1+b(1,2)x_2+\cdots+b(1,n-1)+2b(1,n)$. Recall that we asumed that parameter n is even.

6.2. PRIVATISATION OF EULERISED PUBLIC RULES OF DENSITY $O(n^4)$.

(i) Alice constructs cubical public key G from ${}^nCG(K)$ via presented above method. She creates its Eulerisation via generation of J from ${}^nCG(K)$ via selected Jordan-Gauss automorphisms of $K[x_1,x_2,\ldots,x_n]$ and composition $JG=E$ of linear degree cn, $c>0$ and density $O(n^4)$. After the completion of protocol Alice and Bob elaborate matrices A and B. They create R_1, R_2 and sequence u and compute $H = R_1 R_2^A(n,K)\eta(u)R_2R_1$ (see (1) above). Additionally they use matrix A to create Jordan Gauss elements ${}^1J$ moving x_i to $x_i{}^{a'_{i,i}}x_{i+1}{}^{a(i,i+1)}x_{i+2}{}^{a(i,i+1)}\dots x_n{}^{a(i,n)}$, $i = 1,2,\dots,n$ and ${}^2J$ moving x_i to $x_i{}^{a'_{i,i}}x_1{}^{a(i,1)}x_2{}^{a(i,2)}\dots x_{i-1}{}^{a(i,i-1)}$, $i = 1,2,\dots,n$ where $a'(i,i) = a(i,i)$ if $(a(i,i),d) = 1$ and $a'(i,1) = 1$ in the oposite case. Each of correspondents forms H' as ${}^1J^2JH$.

Alice sends $E + H'$ to Bob. He restores the standard form of multivatiate map E of density $O(n^4)$ and linear degree.

(ii) Privatisation "by parts".

Alice creates the pair (J,G) as in (i). Correspondents execute protocol and get matrices A and B. They form ${}^1J$ and ${}^2J$ and their composition J' together with a cubical map H. Alice sends tuple of monomial terms $(J(x_1)J(x_1)$, $J(x_2)J'(x_2)$, $\dots$, $J(x_n)J'(x_n))$ together with the standard form $G+H$. Bob restores the pair (J,G).

So he encrypts via consecutive usage of J and G to a plaintext from K^{*n}. Alice decrypts via consecutive usage of $T_2{}^{-1}$, ${}^{A(n,K)}\eta(Rev(w))$, $T_1{}^{-1}$, J^{-1}. Complexity of encryption procedure by Bob is $O(n^4)$.

(iii) Extraction method.

Alice and Bob execute the protocol and get matrices A, B. In the case of $K = F_q$ correspondents construct linear transformations R_1 and R_2 and string $u = (x,\, f_1,\, f_1,\, f_2,\, f_2,\, \dots,\, f_n,\, f_n)$ as in (i).

In the case of characteristic 2 they have a choice to create $w = (x,\, f_1,\, f_1,\, f_2,\, f_2,\, \dots,\, f_n,\, x^2)$ or to use $w = (x,\, f_1,\, f_1,\, f_2,\, f_2,\, \dots,\, f_n,\, x^3)$ if $(3, q-1) = 1$. They form J_1 and J_2 accordingly to the method of (ii).

They use sequence J_1, J_2, R_1, R_2, ${}^{A(n,K)}\eta(w)$, R_2, R_1 to encrypt a plaintext from K^{*n} and use $R_1{}^{-1}$, $R_2{}^{-1}$, ${}^{A(n,K)}\eta(Rev(w))$, $R_2{}^{-1}$, $R_1{}^{-1}$, $J_2{}^{-1}, J_1{}^{-1}$ to decrypt a ciphertext from K^n.

The complexity of protected symmetric cipher is $O(n^2)$.

7 Asymmetric Cryptosystem with multivariate encryption of nonpolynomial density

Let K be a commutative ring with $d = |K^*| > 3$. We consider graphs $A(n,K)$ for even n, $n \geq 2$ and t the tuple $u = u(b_1, b_2, \dots, b_n)$ given as $f_1 = b_1x$, $f_2 = b_2x$, $f_3 = b_3x^2 + b_1$, $f_4 = b_4x^2 + b_1$, $f_5 = b_5x + b_1 + b_3$, $f_6 = b_6x + b_2 + b_4$, $\dots$, $b_{n-1}^x{}^alpha + b_1 + b_3 + \dots + b_{n-3}$, $b_nx^\alpha + b_1 + b_2 + \dots + b_{n-2}$ where $\alpha = 2$, $t = 1$ for $n = 0\ (mod\, 4)$ and $\alpha = 1$, $t = 2$ for $n = 2\ (mod\, 4)$, $b_1, b_2, \dots, b_n$ are elements from K^*.

Accordingly to the given above estimates degree of ${}^{A(n,K)}\eta(u')$ for $u' = u'(b_1, b_2, \dots, b_n) = (x,\, f_1,\, f_1,\, f_2,\, f_2,\, \dots,\, f_k,\, f_k)$ is at least $2n-2$. It is easy to see that degree of ${}^{A(n,K)}\eta((w))$ for $w(b_1, b_2, \dots, b_n) = (x,\, f_1,\, f_1,\, f_2,\, f_2,\, \dots,\, f_k,\, x^e)$ with $e < 2n-2$ coincides with ${}^{A(n,K)}\eta(u)$.

Assume that $(e,d) = 1$ and r is multiplicative inverse of e, i. e. $re = 1(modd)$. Then $x^{er} = x$, $(xx^e)^r$ is an identity map. Degree of the composition of xx^r and $x \to x^e$ is a product of these degrees. So they will be mutually inverse.

Let us assume that K is a field F_q, $q = 2^t$ and $e = 2$. In this case $r = 2^{t-1}$. Then the composition of $x \to x^{2^{t-1}}$ and xx^2 is an identity. The degree of inverse for $x \to x^2$ has degree 2^{t-1}. Notice that this degree is maximal power of 2 which is $< d$.

Let us consider the case of arbitrary e and a finite commutative ring K such that $(d, e) = 1$. The inverse δ^{-1} for the bijective map δ: $x \to x^e$ belongs to the cyclic group $C =< \delta >$. Noteworthy that $x \to x^{e^s}$ for $e^s < d$ can not be the inverse for δ if $e^{s+1} \neq d$. Thus $deg(\delta)^{-1}$ is $\geq$ than maximal power of e which is $< d$.

Notice that in the case of F_{p^t}, p is a prime and $e = p$ we have $d = p^t - 1$, $r = 3^{t-1}$. The inverse map of δ has degree which is equal to the maximal power of p in the interval $(0, p^t - 1)$.

Let us estimate degree $g =^{A(n,K)} \eta_n(Rev(w))$. Notice that $Rev(w) = (f_k(x^r)$, $f_k(x^r)$, $f_{k-1}(x^r)$, $f_{k-1}(x^r)$, $f_k - 1(x^r)$, $\ldots$, $f_1(x^r)$, $f_1(x^r)$, $x^r)$. It is easy to see that $deg(g) \geq 2(n-2)m$, where m is the maximal power of e from the interval $(0, d)$.

ALGORITHM 7.1. Alice and Bob execute on of the algorithm of section 5 with the output from the semigroup ${}^nES(K)$, where n is even parameter ≥ 2 and K is a finite commutative ring with multiplicative group K^* of order d, $d \geq 3$. They use the collision map to create matrices $A = (a(i, j)$ with $a(i, j) \in Z_d$ and $B = (b(i, j)$, $b(i, j) \in$K* as in previous section. Additionally they have a vecror $(q_1, q_2, \ldots, q_n)$ of coefficients from the standard form of the output. Correspondents agree on parameter e via open channel.

They form $w(b_1, b_2, \ldots, b_n)$, matrices R', R_1 and R_2 as in the previous section.

They work with the plaintexts $(x_1, x_2, \ldots, x_n)$ from $K{*}^n$ and ciphertexts from K^n.

The encryption algorithm contans the following steps.

Step 1. Sender takes the plaintext p $= (p_1, p_2, \ldots, p_n)$ and computes parameters $a_i = f_i(p_1)$, $i = 1, 2, \ldots, n$ together with $a = p_1$.

Step 2. Sender forms triangular matrices R', R_1, R_2 together with their inverses R'^{-1}, ${R_1}^{-1}$ and ${R_2}^{-1}$.

Step 3. Sender consecutively computes R'(p) $=^1$ p, $R_2({}^1rmp) =^2$ p, $N_{a_1}({}^2$p) $=^3$ p, $N_{a_2}({}^3$p) $=^4$ p, $\ldots$, N$_{a_n}({}^{n+1}$p) $=^{n+2}$ p, $J_a({}^{n+2}$p) $=^{n+3}$ rmp, $R_2R_1({}^{n+3}$p) = c.

This procedure can be executed in time $O(n)$.

For the decryption correspondent executes the following steps.

Step 1. Takes ciphertext c and nutes ${R_1}^{-1}{R_2}^{-1}$(c) $= (b, c_2, c_3, \ldots, c_n) =^1$ c.

Let $v = (v_1, v_2, \ldots, v_n) = R'R_2$(p). Notice that $v_1 \in K^*$.

Step 2. He/she computes $v_1 = b^r$ together with $a_n = f_n(v_1, a_{n-1} = f_{n-1}(v_1)$, $\ldots$, $a_1 = f_1(v_1)$

Step 3. Correspondent forms ^{2}c $= (p_1 + a_n, c_2, c_3, \ldots, c_n)$.

Step 4. He/she computes N$_{a_{n-1}}({}^2$c) $=^3$ c.

Step 5. Computation of $N_{a_{n-2}}({}^3$c) $=^4$ c.

...

Step $n + 3$. Computation of $N_{a_1}({}^{n+3}$c) $=^{n+4}$ c.

Step $n+4$. Computation of $N_{p_1}(^3\mathrm{c}) = \mathrm{v}$.

Final step is computation of $R_2{}^{-1}R'^{-1}(\mathrm{v}) = \mathrm{p}$.

In fact the encryption and decryption maps are multivariate transformations of K^n of degree $\geq (2n-2)$ and $\geq (2n-2)m$ where m is a maximal power of e which is $\leq d$.

REMARK 7.1. Noteworthy that decryption and encryption maps are transformations of nonpolynomial density, in practical cases their standard forms are impossible to compute. Symmetric cipher with such encryption was implemented (see [45]).

ALGORITHM 7. 2.

Let us consider the extraction method of privatization in the cases of Examples 12, 13, 14. Like in Algorithm 1 correspondents execute the protocol, takes its uutput G. They form matrices A and B together with vector $(q_1, q_2, \ldots, q_n)$ and construct T_1, T_2 and tuple u as in previous algorithm. Additionally they use matrix A to create transformation J_1 and J_2. So they use space of plaintexts $(K^*)^n$ and space of ciphertexts K^n.

8 On sparse trapdoor accelerators

Practical applications need "sparse trapdoor accelerators" which allows the computation of the value of toric automorphism from polynomial map and its toric reimage in time $O(n)$. In the case of map from ^nEG we can use walks in the following graph $^*A(n, H)$ defined over arbitrary commupative group H It is incidense structure with points set $^*P_n$ and line set $^*L$ isomorphic to H^n such that point $(p_1, p_2, \ldots, p_n)$ is incident to line $[l_1, l_2, \ldots, l_n]$ if and only if

$p_2/l_2 = l_1p_1$,

$p_3/l_3 = p_1l_2$,

$p_4/l_4 = l_1p_3$,

$\ldots$

$p_n/l_n = l_1p_{n-1}$ if n is even and $p_n/l_n = p_1l_{n-1}$ if n is odd.

Similarly to the case of graphs $A(n, K)$ we introduce colours p_1 and l_1 of point $(p_1, p_2, \ldots, p_n)$ and line $[l_1, l_2, \ldots, l_n]$ of the graph $^*A(n, H)$ and define operator $^\alpha N(v)$ of taking of neighbour of $v \in P_n \cup L_n$ of colour $\alpha \in H$.

We define $^*K[x_1, x_2, \ldots, x_n]$ as totality of monomials $\beta {x_1}^{\alpha_1} {x_2}^{\alpha_2} \ldots {x_n}^{\alpha_n}$ where $\beta \in K^*$ and α_i are elements of Z_d, $d = |K^*|$. This is an abelian group with natural operation of multiplication as in $K[x_1, x_2, \ldots, x_n]$ which contains K^*. We will use pair of graphs $^*A(n, K^*)$, $^*A(n, ^*K[x_1, x_2, \ldots, x_n])$ to define the transformation from $^nEG(K)$. We take point $(x_1, x_2, \ldots, x_n)$ of the graph $^*A(n, ^*K[x_1, x_2, \ldots, x_n])$ and the sequence u of elements ^1h, ^2h, $\ldots$, ^sh from $^*K[x_1]$ where parameter s is even. We assume that ^sh is element of kind $q{x_1}^{t(s)}$ where $(t(s), ^*|) = 1$.

We consider the walk in the graph $^*A(n, ^*K[x_1, x_2, \ldots, x_n])$ starting from point $(x_1, x_2, \ldots, x_n)$ and further vertices of colours ^1h. Let $\mu_n(u)$ be the transformtion from $^nEG(K)$ sending $(x_1, x_2, \ldots, x_n)$ to the destination point of the walk $(q{x_1}^{t(s)}, q_1{x_1}^{a(1,1}x_2^{a(1,2)}, q_2{x_1}^{a(2,1}x_2^{a(2,2)}, \ldots, q_n{x_1}^{a(n,1}x_2^{a(n,2)} \ldots {x_n}^{a(n,s)}$.

We can consider transformations ${}^1J$ and ${}^2J$ defined by the rules $x_1 \to c(i,1)x_1^{a(i,1)}{x_2}^{a(i,2)} \dots {x_n}^{a(i,n)}$, $x_2 \to c(i,2)x_2, \dots, x_n \to c(i,n)x_n$, $i = 1, 2$ where $c(i,j)$ are elements of K^*, $a(i,j)$ are elements of Z_d and $a(i,1)$, $i = 1, 2$ are mutually prime with d. The rule F_n is a composition of J_1, $\mu_n(u)$, J_2. It is clear that F_n has toric trapdoor accelerator (J_1, J_2, u). Noteworthy that if $s = O(1)$ and trapdoor is known that the value of F_n and the reimage of given tuple can be computed in time $O(n)$.

REMARK 8.1.

In all examples of families F_n from ${}^nCG(K)$ or toric automorphisms with trapdoor accelerator T there is an option to work with " sparce" trapdoor accelerator. In the case of elements from ${}^nEG(K)$ one can work with function $F_n =^1 J\mu_n(u)J_2$ as above in the case when length s of the walk of size $O(1)$.

In the cases of $F_n = T_1\eta_n(u)T_2$ one can use the space of linear transformations such that $T(x_1)$ and $T_2(x_1)$ are of kind $b_1x_1+b_2x_2+\cdots_n x_n$, $b_i \in K^*$. $T(x_j) = x_j$ for $j = 2, 3, \dots, n$ and use u of kind $(x,\ f_1,\ f_1,\ f_2,\ f_2,\ \dots,\ f_s,\ g(x))$ where the choice of f_i and $g(x)$ depens on the used algorithm.

In cases of Examples 9, 10, 11 degrees of $f_1,\ f_2,\ \dots,\ f_{s-1}$ are $> cn$ for some positive constant c, their size is $O(n)$. It is easy to see that in the case of s of size $O(1)$ the rule F_n is still bijective function of unbounded degree but the knowledge of trapdoor allows to compute the value of multivariate function F_n and its reimage in time $O(n)$.

In the cases 12, 13, 14 we create trapdoors of kind J_1, J_2, T_1, T_2, u as above and work with toric automorphism $F_n = J_1J_2T_1T_2u$ Special choice of trapdoor informalions allows us to compute the value and toric reimage in time $O(n)$.

REMARK 8. 2.

Alice and Bob can use one of protocols with platform ${}^nES(K)$. They take the collision element G and form the matrices A and B. Some "light extraction algoritm" can be used to select $(a(i,1),\ a(i,2),\ \dots,\ a(i,n))$, $i = 1, 2$ as some rows or columns of A and vectors from $(K^*)^n$ as rows or columns of matrix B.

9 On open schemes of collision maps extractions

.

Let K be a commutative ring with multiplicative group K^* of order ≥ 3. We consider an element ${}^TF_n = F_n$ from ${}^nCG(K)$ depending on piece of information T which is a trapdoor accelerator.

Note that we can take two affine transformations T_1 and T_2 from $AGL_n(K)$ and form a new element $G_n = T_1^TF_nT_2$. It is easy to see that automorphism G_n has trapdoor accelerator $T' = (T_1, T, T_2)$. We refer to T' as *deformation* of T. In many cases the information on T can be given via two vectors v_1 from K^t and v_2 from ${Z_m}^r$ for some parameters r, t and m. Note that part of information on T can be given publicly. In the case of G_n of polynomial density this map can be given via its standard form which can be used as a public rule and T' will be treated as a private key.

We can consider more general *toric trapdoor accelerator* of kind $G_n = T_1^T F_n T_2$ where G_n and F_n are toric automorphisms and solution for $F_n(x) = b$, $x \in (K^*)^n$ can be computed in time $O(n^2)$.

Other examples of toric trapdoor accelerators corresponds to Eulerian transformations from ${}^nEG(K)$. Let ${}^MJ$ element from ${}^nEG(K)$ such that the knowledge of M allows the computation of solution for ${}^MJ(x) = b$, $x, b \in K^*$ can be computed in time $O(n^2)$. Then $E_n = J_1{}^MJJ^2$ where J_1 and J_2 are products of $r = O(1)$ of Jordan-Gauss generators also has toric trapdoor accelerator (L_1, L_2, M) where L_1 and L_2 are lists of generators for J_i, $i = 1, 2$.

Noteworthy that we can combine trapdoor accelerators (L_1, L_2, M) and (T_1, T, T_2). Toric automorphism $Y_n = J_1{}^MJJ_2T_1{}^TF_nT_2$ has toric trapdoor accelerator (L_1, L_2, M, T_1, T, T_2). The first examples of realisations of these schemes are given in [26].

Alternatively Alice and Bob can use protocols of Noncommutative Cryptography based on semigroup platform S generated by several endomorphisms from ${}^sCS(K)$. The collision element g is given by the tuple of polynomials (f_1, f_2, ..., f_s). One can take vectors $v(i)$ of coefficients in front of monomials of g_i ordered in lexicographical order, amd the list $m(i)$ of normalised ordered monomials (with coefficient 1) ordered monomials of g_i.

We refer to the algorithm with input $v(i)$, $m(i)$, $i = 1, 2, \dots, s$ and output T' as trapdoor accelerator extraction procedure.

For the feasibility of protocol the seemigroup S of ${}^sC$ has satisfy tp Multiple Composition Computetion Property (MCCP) which insures the computation of s elements of S in plolynomial time.

One of the examples of semigroup with MCCP is the subgroup ${}^sES(K)$, other examples are *stable subsemigroups* of ${}^sCS(K)$ for which degree of elements are bounded by some constant. In the case of ${}^sES(K)$ the output g is the map $x_i \to q_i x_1{}^{a(i,1)} x_2{}^{a(i,2)} \dots x_s{}^{a(i,s)}$, $i = 1, 2, \dots, s$

So we form to matrices $B = (b(i, j))$, $b(i, j) = (q_i q_j)^{a(i,j)}$ and $A = (a(i, j)$. Assume that $v = (v_1, v_2, \dots, v_{s^2)})$ and $a = (a_1, a_2, \dots, a_{n^2})$ are lists of elements of B an A ordered lexicographically.

9. 1. EXTRACTION OF AFFINE TRANSFORMATIONS AND TUPLES OF POLYNOMIALS FROM THE PROTOCOL.

Take list of formal variables z_i, $i = 1, 2, \dots, n^2$ together with parameter m and form formal lower triangular matrix Z with rows $Z_j = (z_{i(1,j)}, z_{i(2,j)}, \dots, z_{i(j,j}, 0, 0, \dots, 0)$, $i(t, j \in \{1, 2, \dots, Sn^2\}$, $j = 1, 2, \dots, m$ and $R = (z_{l(1}, z_{l(2)}, \dots, z_{l(m)})$.

The list of variables y_i, $i = 1, 2, \dots, n^2$ will be used for a creation of formal upper triangular matrix Y of sise $m \times m$ with rows $Y_j = (0, 0, \dots, y_k(j, j), y_k(j, j + 1), \dots, y_{k(j,m)})$.

we consider polynomials of kind ${}^jQ(x) = z_{l(j,0)} + z_{l(j,1}x + \dots + z_{l(l(j,r(j))x^{r(j)}}$ where $l(j, i)$ are elements of $\{1, 2, \dots, n^2\}$, $j = 1, 2, \dots, s$, $i = 1, 2, \dots, r(j)$.

9. 2. PROTOCOL INTERPRETION.

Let us consider toric automorphism of kind $G_m = T_1^T F_m T_2$ from ${}^mCS(K)$ where F_m is graph based toric automorphism ${}^{A(m,K)}\eta(u)$ with trapdoor accelerator of kind (x, f_1, f_1, f_2, f_2, ..., f_s, g_s), $s = O(m)$. For the simplicity we assume that g_s is known bijective map on K. In particular we can take $g(x) = ax + b$, $a \in K^*$ or $K = F_q$ and $g(x) = ax^r + b$, $(r, q-1) = 1$, $a \neq 0$. Under this assumption F_n will be a bijective map.

One of correspondents selects parameter m and forms formal lower triangular matrices ${}^1Z$ ans ${}^2Z$ of sise $m \times m$ with rows ${}^1Z_j = (z_{{}^1i(1,j)}, z_{{}^1i(2,j)}, \dots, z_{{}^1i(j,j}, 0, 0, \dots, 0)$ and ${}^2Z_j = (z_{{}^2i(1,j)}, z_{{}^2i(2,j)}, \dots, z_{{}^2i(j,j}, 0, 0, \dots, 0)$. Words $({}^1i(1,j), z_{{}^1i(2,j)}, \dots, z_{{}^1i(j,j)})$ and $({}^2i(1,j), {}^2i(2,j), \dots, {}^2i(j,j)$ in the alphabet $\{1, 2, \dots, n^2\}$ can be generated by some pseudorandom algorithm.

Similarly he/she forms two formal upper triangular matrices ${}^lY$, $l = 1, 2$ with rows ${}^lY_j = (0, 0, \dots, y_{{}^lk(j,j)}, y_{{}^lk(j,j+1)}, \dots, y_{{}^lk(j,m)})$ and two vectors ${}^jR = (z_{{}^jl(1}, z_{{}^jl(2)}, \dots, z_{{}^jl(m)})$, $j = 1, 2$.

Secondly the correspondent forms polynomials of kind ${}^jQ(x) = z_{l(j,0)} + z_{l(j,1}x + \dots + z_{l(l(j,r(j))x^{r(j)}}$ where $l(j,i)$ are elements of $\{1, 2, \dots, n^2\}$, $j = 1, 2, \dots, s$, $i = 1, 2, \dots, r(j)$. We assume that $r(j) \geq 1$ of size $O(m)$

He/she sends these data to partner. So correspondents use it and create matrices ${}^rB$, $r = 1, 2$ via specialisation $z_{{}^ri(k,j)} = v_{{}^ri(k,j)}$ and ${}^rC$, $r = 1, 2$ via specialisation of matrices ${}^rY$ via specialisation ${}^rk(j,j) = v_(rk(j, j+1))$. They form two vectors ${}^jb$ of kind $(v_{{}^jl(1}, v_{{}^jl(2)}, \dots, v_{{}^jl(m)})$. They use specialisations ${}^jP(x)$ of ${}^jQ(x) = z_{l(j,0)} + z_{l(j,1}x + \dots + z_{l(l(j,r(j))x^{r(j)}}$ obrained via the rule $z_{l(j,t)} = v_{l(j,t)}$.

Each of correspondent uses affine transformations $T_r : \mathrm{x} : B_rC_r\mathrm{x} + b_r$, $r = 1, 2$ and tuple $u = (P_1, P_1, P_2, P_2, \dots, P_s, P_s)$ to encrypt with multivariate rule $\mathrm{x} \to T_1^{A(m,K)\eta(u)T_2}$. It is easy to see that encryption takes time $O(m^2)$. We assume that $\deg(P_i) \neq \deg P_{i+2}$, $i = 1, 2, \dots, m-2$, $\deg(P_i) \geq cm$, $s \geq cm$ for some constant c. Then degree of encryption map is $\geq cm^2$. The execytion time of encryption and decryption procedures is $O(m^2)$.

Let us assume that correspondents can use constants 0 and 1 together with coordinates of vector v. One can use sparce variant were $T_1 = C_1$, $T_2 = C_2$ obtained via specialisations of ${}^rY$, $r = 1, 2$ with first rows $(y_{{}^r(1,)}, y_{{}^rk(1,2)}, \dots, y_{{}^2k(1,m)})$ and other rows $(0, 1, 0, 0, \dots, 0)$, $(0, 0, 1, \dots, 0)$, $\dots$, $(0, 0, \dots, 0, 1)$. They select s of size $O(1)$. Then the encryption and decryption procedure will take time $O(m)$. We can slightly modify sparce version as above via the choice of s of size $O(m^t)$, $1 \leq t < 1$. Then execution of encryption and decryption will cost $O(m^{1+t})$.

REMARK 9. 1.

We can use arbitrary linguistic graph I defined over K instead of $A(m, K)$. The usage is defined via the change of ${}^{A(m,K)}\eta$ for ${}^I\eta$.

We can hide the graph taking some coefficients in equations of graph as variables v_i and degrees of monomials as some a_i. For instance we can use equations of kind $h_{i_2}x_2 + h_{j_2}y_2 = y_1{}^{c_{k(2)}}x_1{}^{c_{s(2)}}$, $h_{(i_3}x_3 + h_(j_3)y_3 = x_1{}^{c_k(3)}y_3{}^{c_s(3)}$, $\dots$ $h_{i_m}x_{i_m} + h_{j_m}y_{i_m} = y_1{}^c_{k(m)}x_{m-1}{}^c_{s(m)}$ if m is even and $h_{i_m}x_{i_m} + h_{j_m}y_{i_m} = x_1{}^c_{k(m)}y_{m-1}{}^{c_{s(m)}}$ if m is odd where i_l, j_l, $k(l)$, $s(l)$, $l \geq 2$ are elements of the alphabet $\{1, 2, \dots, n^2\}$ After the complition of the protocol correspondents specialise h_{i_s}, h_{j_s}, $s = 2, 3, \dots, m$ as v_{i_s} and v_{i_s}. They set $c_{k(s)} = a_{k(s)}$ if $a_{k(s)} \neq 0$ and $c_{k(s)} = 1$ for $a_{k(s)} = 0$. Similarly $c_{s(l)} = a_{s(l)}$ if $a_{s(l)} \neq 0$ and $c_{s(l)} = 1$ for $a_{s(l)} = 0$, $l = 2, 3, \dots, m$.

REMARK 9.2.

We can use more general formal polynomials ${}^{j}Q(x) = z_{l(j,0)} + z_{l(j,1}x^{d(t(j,1)} + z_{l(j,2}x^{(}2(d(t(j,2)) \cdots + z_{l(l(j,r(j))x^{r(j)^{j}d(t(j,i_r(j)))}}$, where $t(j,k)$ are elements of $\{1, 2, \ldots, n^2\}$.

For the specialisation we will use tuple $(c(1), c(2), \ldots, c(n^2))$ such that $c(i) = a_i$ if $a_i \neq 0$ and $c(i) = 1$ for $a_i = 0$ and set $d(t(j,k)) = c(t(j,k))$.

9. 3. EXTRACTION OF EULERIAN TRANSFORMATIONS ANd TUPlES Of ELEMENTS OF ${}^{1}ES(K)$.

Let m be a positive integer. We consider list of variables ${}^{t}z({}^{t}k(i,j))$, $1 \leq i \leq j \leq m$, $t = 1, 2$ where ${}^{t}k(i,j)$ is an element of alphabet $\{1, 2, \ldots, n^2\} = N$ Additionally we will work with list of variables ${}^{t}u({}^{t}r(i,j))$, $m \geq i \geq j \geq 1$, $t = 1, 2$ where ${}^{t}r(i,j) \in N$. We set lists of variables ${}^{t}x_{{}^{t}k(i)}$, $k(i) \in N$, $i = 1, 2, \ldots, m$, $t = 1, 2, 3, 4$ together with ${}^{t}y_{{}^{t}l(i)}$, $l^{t}(i) \in N$, $i = 1, 2, \ldots, s$, $s = O(m)$, $t = 1, 2$.

Assume that Alicia sends these lists to Bob. After the execution of protocol correspondents specialised variables ${}^{t}x_{{}^{t}k(i)}$ as $v_{{}^{t}k(i)}$ and get tuples $({}^{1}q_1, {}^{1}q_2, \ldots, {}^{1}q_m)$ and $({}^{2}q_1, {}^{2}q_2, \ldots, {}^{2}q_m)$. They form arrays ${}^{t}z({}^{t}k(i,j)) = c({}^{t}k(i,j))$ and ${}^{t}u({}^{t}k(i,j)) =^{c} ({}^{t}r(i,j))$. They form the following Jordan-Gauss transformations ${}^{1}J$ and ${}^{2}J$

${}^{t}J(x_1) =^{t} qx_1{}^{{}^{t}c'({}^{t}k(1,1))}$,

${}^{t}J(x_2) =^{t} qx_1{}^{{}^{t}c({}^{t}k(2,1))}x_2{}^{{}^{t}c'({}^{t}k(2,2))}$,

$\ldots$,

${}^{t}J(x_m) =^{t} qx_1{}^{{}^{t}c({}^{t}k(m,1))}x_2{}^{{}^{t}c({}^{t}k(m,2))} \ldots x_m{}^{{}^{t}c'({}^{t}k(m,m))}x_m{}^{{}^{t}c'({}^{t}k(m,m))}$

where $c'(i)$ is maximal number from the interval $[1, c(i)]$ which is mutualy prime with d and $t = 1, 2$

Additionally they generate ${}^{3}J$ and J^4 of kind

${}^{t}J(x_1) =^{k} qx_1{}^{{}^{k}c'({}^{t}r(1,1))}x_2{}^{{}^{t}c({}^{t}r(1,2))} \ldots x_m{}^{{}^{t}c({}^{t}k(1,m-1))}x_m{}^{{}^{t}c({}^{t}k(1,m))}$

${}^{t}J(x_2) =^{k} qx_2{}^{{}^{k}c'({}^{t}r(2,2))}x_2{}^{{}^{t}c({}^{t}r(2,3))} \ldots x_m{}^{{}^{t}c({}^{t}k(2,m-1))}x_m{}^{{}^{t}c({}^{t}k(2,m))}$

$\ldots$

${}^{t}J(x_m) =^{t} qx_1{}^{{}^{t}c'({}^{t}r(m,m))}$,

where $t = 3, 4$.

They use specialisations of variables ${}^{1}y_{{}^{1}l(i)} = v_{{}^{1}l(i)}$, $i = 1, 2, \ldots, s$, ${}^{2}y_{{}^{2}l(i)} = c_{{}^{2}l(i)}$, $i = 1, 2, \ldots, s$ where parameter s is even.

Correspondents form $u' = (v_{{}^{1}l(1)x^{{}^{2}l(1)}, v_{{}^{1}l(2)x^{{}^{2}l(2)}}, \ldots, v_{{}^{1}l(2)x^{{}^{2}l(2)}})}$.

They will encrypt plaintexts from K^{*m} with element $E_m =^{1} J^3 J^{A(n,K^*)}\mu(u)^2 J^4 J$. It is easy to check that E_m from ${}^{m}EG(K)$ has toric trapdoor accelerator (J_1, u', J_2) where $J_1 =^{1} J^3 J, J_2 =^{2} J^4 J$.

COMBINED EXTRACTION ALGORITHM.

One of correspondents selects parameters m and n. He/she executes extraction algorithm 1 and 2 above. Alice and Bob compllete the protocol based on platform ${}^{n}ES(K)$. Each of correspondents implement the protocol implementations to get toric maps $F_1 = T_1^{A(m,K)\eta(u)T_2}$ and Eulerian transformation $F = J_1\mu(u')J_2$.

After they work with the space of plaintexts $(K^*)^m$ and space of ciphertexts K^m. We can see that tuple $(J_1, J_2, u', T_1, T_2, u)$ is a toric trapdoor accelerator. So encryption and decryption requires $O(m^2)$ elementary operations.

REMARK 9.3.

Let us consider extraction algorithm to generate toric automorphism of kind $G_m = T_1^T F_m T_2$ from ${}^mCS(K)$ where $F_m = \eta(u)$, $u = (x,\ f_1(x),\ f_1(x),\ f_2,\ f_2,\ \ldots,\ f_{s-1},\ f_{s-1},\ f_s,\ g_s)$ in the case when the equations of kind $g_s(x) = b$, $x \in K^*$ has a unique solution but function g_s is not a bijection on K. We use described above scheme with special selection of ${}^lY_1$ as $(0, 0, \ldots, O, y_{{}^l k(1,j)}, 0, \ldots, 0)$ for some $1 \leq m$. Additionally we change the positions of B_r and C_r and define ${}^rT$ as transformations x: $C_r B_r \mathrm{x} + b_r$, $r = 1, 2$ during the process of protocol implementation. Then modified algorithm produces toric automorphism $G_m = T_1^T F_m T_2$ with toric trapdoor accelerator $(T_1,\ T_2,\ u)$ and toric automorphism G_m is not an element of ${}^mCG(K)$.

10 Conclusions

Extremal algebraic graphs were traditionally used for the construction of stream ciphers of multivariate nature. We introduce first graph based multivariate public keys with bijective encryption maps.

We use family of graphs $A(n, F_q)$ where q is large prime power such that $(q-1, 3) = 1$ or char$F_q = 2$ to define cubical bijective maps F_n of vector space $F_q)^n$ with inverse maps of large degree. In particular for each pair $(2^m, n)$, $m \geq 2$, $n \geq 2$ we have example of cubical bijective transformation G_n of $F_{2^m}^n$ with degree of the inverse map $3 \times 2^{m-1}$.

More general families $A(n, K)$, $n \geq 2$ are defined over finite commutative ring K such that $d = |K^*| > 3$ and $(3, d) = 1$ is used to construct cubical map G_n of affine space K^n, $n \geq 2$ which act injectively on $T_n(K) = K^{*m}$ and have *Eulerian* inverse E_n which is endomorphism of $K[x_1, x_2, \ldots, x_n]$ such that the composition of G_n and E_n acts on $T_n(K)$ as identity map. The degree of $E_n(K)$ is at leat $3{\times}t$ where t is maximal power of 3 which is $< d$. It can be used for the construction of public keys with the space of plaintexts $T_n(K)$ and the space of ciphertexts K^n.

In the case when K is a field G_n and E_n are bijective maps on K^n. So, in the case of q such that $(3, q-1) = 2$ degree of ${G_n}^{-1}$ acting on ${F_q}^n$ is $\geq 3t$, where t is maximal power of 3 which $< q-1$ and transformations of kind $T_1 F_n T_2$, $T_1, T_2 \in AGL_n(F_q)$ can serve as public keys. We consider obfuscations of G_n and F_n of kind $F'_n = H_n T_1(F_q) F_n T_2$, $T_1,\ T_2 \in AGL_n(F_q)$ and $G'_n = H_n(K) T_1 G_n T_2$, $T_2 \in AGL_n(K)$,T_1 is a special affine transformation, where $H_n(q)$ and $H_n(K)$ are Eulerian automorphisms of $F_q[x_1, x_2, \ldots, x_n]$ and $K[x_1, x_2, \ldots, x_n]$ respectively, i.e., transformations moving each x_i to a monomial term with coefficient from K^*. Maps F'_n and G'_n has linear degree and the same densities with F_n and G_n. In the case of usage of such obfuscations as public keys adversary has to approximate the "decryption map" of non polynomial density.

Finally we convert proposed public keys to protocol based cryptosystems of El Gamal type with the usage of algorithms of Noncommutative Cryptography with platforms of Eulerian endomorphisms of $K[x_1, x_2, \ldots, x_n]$. Security of these cryptosystems rests on the complexity of Power Conjugacy Problem or Word

Decomposition Problem for Eulerian endomorphisms given in their standard forms.

Additionally we introduced a cryptosystem with the encryption map on non polynomial density. This map is impossible to use on public key mode.

1. *Post-Quantum Cryptography: Call for Proposals:https://csrc.nist.gov/*, Project: Post-Quantum-Cryptography-Standardization/Call-for-Proposals, Post-Quantum Cryptography: Round 2 Submissions.
2. V. Ustimenko. *On the extremal graph theory and symbolic computations*, Reports of Nath Acad of Sci, of Ukraine, 2013, No. 2, p. 42-49.
3. V. Ustimenko, *On new results on Extremal Graph Theory, Theory of Algebraic Graphs and their applications in Cryptography and Coding Theory.* Reports of Nath Acad of Sci, of Ukraine, No. 4, p. 42-49.
4. Yu. Bodnarchuk, *Every regular automorphism of the affine Cremona group is inner*, Journal of Pure and Applied Algebra 157 (2001) 115-119.
5. I.R. Shafarevich, *On some infinite dimension groups II*, Izv. Akad. Sci. Ser. Math., 2 (1) (1981), 214-226.
6. Max Noether, *Luigi Cremona*, Mathematische Annalen 59, 1904, p. 119.
7. D. N. Moldovyan, N. A. Moldovyan, *A New Hard Problem over Non-commutative Finite Groups for Cryptographic Protocols*, International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security, MMM-ACNS 2010: Computer Network Security, pp. 183-194.
8. L. Sakalauskas., P. Tvarijonas , A. Raulynaitis, *Key Agreement Protocol (KAP) Using Conjugacy and Discrete Logarithm Problema in Group Representation Level*, INFORMATICA, 2007, vol. !8, No 1, 115-124.
9. V. Shpilrain, A. Ushakov, *The conjugacy search problem in public key cryptography: unnecessary and insufficient*,Applicable Algebra in Engineering, Communication and Computing, August 2006, Volume 17, Issue 34, pp 285289
10. Delaram Kahrobaei, Bilal Khan, *A non-commutative generalization of ElGamal key exchange using polycyclic groups*, In IEEE GLOBECOM 2006 - 2006 Global Telecommunications Conference [4150920] DOI: 10.1109/GLOCOM.2006.
11. Delaram Kahrobaei, Bilal Khan, *A non-commutative generalization of ElGamal key exchange using polycyclic groups*, In IEEE GLOBECOM 2006 - 2006 Global Telecommunications Conference [4150920] DOI: 10.1109/GLOCOM.2006.
12. Zhenfu Cao (2012). *New Directions of Modern Cryptography.* Boca Raton: CRC Press, Taylor Francis Group. ISBN978-1-4665-0140-9.
13. Benjamin Fine, et. al., *"Aspects of Non abelian Group Based Cryptography: A Survey and Open Problems*,. arXiv:1103.4093.
14. Alexei G. Myasnikov; Vladimir Shpilrain; Alexander Ushakov. *Non-commutative Cryptography and Complexity of Group-theoretic Problems.* Amer. Math Soc. 2011
15. Anshel, I., Anshel, M., Goldfeld, D., *An algebraic method for public-key cryptography.* Math. Res.Lett. 6(34), 287291 (1999).
16. Blackburn, S.R., Galbraith, S.D., *Cryptanalysis of two cryptosystems based on group actions*, In: Advances in CryptologyASIACRYPT 99. Lecture Notes in Computer Science, vol. 1716, pp. 5261. Springer, Berlin (1999).
17. C Ko, K.H., Lee, S.J., Cheon, J.H., Han, J.W., Kang, J.S., Park, C.: *New public-key cryptosystem using braid groups.* In: Advances in CryptologyCRYPTO 2000, Santa Barbara, CA. Lecture Notes in Computer Science, vol. 1880, pp. 166183. Springer, Berlin (2000).

18. Maze, G., Monico, C., Rosenthal, *J.: Public key cryptography based on semigroup actions*. Adv.Math. Commun. 1(4), 489507 (2007).
19. P.H. Kropholler, S.J. Pride , W.A.M. Othman K.B. Wong, P.C. Wong, *Properties of certain semigroups and their potential as platforms for cryptosystems*, Semigroup Forum (2010) 81: 172186.
20. J. A. Lopez Ramos,J. Rosenthal,D. Schipani,R. Schnyder,*Group key management based on semigroup actions*, Journal of Algebra and its applications, vol.16 , 2019.
21. Gautam Kumar and Hemraj Saini, *Novel Noncommutative Cryptography Scheme Using Extra Special Group*, Security and Communication Networks ,Volume 2017, Article ID 9036382, 21 pages, https://doi.org/10.1155/2017/9036382.
22. V. A. Roman'kov, *A nonlinear decomposition attack*, Groups Complex. Cryptol. 8, No. 2 (2016), 197-207.27.
23. V. Roman'kov, *An improved version of the AAG cryptographic protocol*, Groups, Complex., Cryptol, 11, No. 1 (2019), 35-42.
24. 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, 255274, Springer, Cham (2018).
25. B. Tsaban, Polynomial-time solutions of computational problems in noncommutative-algebraic cryptography, J. Cryptol. 28, No. 3 (2015), 601-622.
26. V. Ustimenko, *On new multivariate cryptosystems based on hidden Eulerian equations*, Reports Nath Acad of Sci, Ukraine (2017), no. 5, 17–24.
27. V. Ustimenko,*On new multivariate cryptosystems based on hidden Eulerian equations over finite fields*, Cryptology ePrint Archive, 2017/093.
28. V. Ustimenko, O. Pustovit. *On the implementations of new multivariate public keys based on transformations of linear degree*, Proceedings of the Conference on Mathematical Aspects of Informatics, MFOI 2021, January 13-15, 2021.
29. B. Bollobash, *Extremal graph theory*, Academic Press, London, 1978.
30. V. Ustimenko, *Linguistic Dynamical Systems, Graphs of Large Girth and Cryptography*, Journal of Mathematical Sciences, Springer, vol.140, N3 (2007) pp. 412-434.
31. F. Lazebnik, V.Ustimenko, *Some Algebraic Constractions of Dense Graphs of Large Girth and of Large Size*, DIMACS series in Discrete Mathematics and Theoretical Computer Science , v. 10, (1993) 75 - 93.
32. F. Lazebnik, V. Ustimenko, A. J.Woldar, *A new series of dense graphs of high girth*, Bull. Amer. Math. Soc. (N.S.) 32 (1995), no. 1, 7379.
33. F.Lazebnik, V. Ustimenko and A. J. Woldar, *A characterisation of the components of the graphs D(k,q)*, Discrete Mathematics,157 (1996), 271-283.
34. M. Polak, V. A. Ustimenko . *On LDPC Codes Corresponding to Infinite Family of Graphs* $A(k,K)$. Proceedings of the Federated Conference on Computer Science and Informat. ion Systems (FedCSIS), 2012, CANA , Wroclaw, p. 11-23.
35. T. Shaska, W C Huffman, D. Joyner, V Ustimenko (Editors), *Advances in Coding Theory and Crytography* (Series on Coding Theory and Cryptology) World Scientific Publishing Company, 2007.
36. 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 pre-scribed degree*, Security and Communication Networks , Volume (2019), Article ID 2137561, 15 pp., https://doi.org/10.1155/2019/2137561.
37. A. Lubotzky, R. Phillips and P. Sarnak, *Ramanujan graphs*, Combinatorica, September 1988, Volume 8, Issue 3, pp. 261-277, DOI: https://doi.org/10.1007/BF02126799

38. G. Margulis, *Explicit group-theoretical constructions of combinatorial schemes and their application to desighn of expanders and concentrators*, Probl. Peredachi Informatsii., 24, N1, 51-60. English translation publ. Journal of Problems of Information transmission (1988), 39-46.
39. D. MacKay and M. Postol, *Weakness of Margulis and Ramanujan - Margulis Low Dencity Parity Check Codes*, Electronic Notes in Theoretical Computer Science, 74 (2003), 8 pp.
40. V. Ustimenko, *Maximality of affine group, hidden graph cryptosystem and graph's stream ciphers* , Journal of Algebra and Discrete Mathematics, 2005, vol.1, -P. 51-65.
41. V. Ustimenko, *On new symbolic key exchange protocols and cryptosystems based on hidden tame homomorphism*, Reports of. Nath. Acad. Sci. of Ukraine, 2018, n 10, pp. 26-36.
42. V. A. Ustimenko, U. Romanczuk (2012), *On Dynamical Systems of Large Girth or Cycle Indicator and their applications to Multivariate Cryptography*, in "Artificial Intelligence, Evolutionary Computing and Metaheuristics ", In the footsteps of Alan Turing Series: Studies in Computational Intelligence, 427, p. 257-285. https:/doi.org/ 10.1007/978-3-642-29694-$9_1$0
43. V. Ustimenko. *On the graph based cryptography and symbolic computations*, Proceedings of International Conference on Application of Computer Algebra, ACA-2006,v1, Serdica Journal of Computing, 2007, pp 131-156.
44. A. Wroblewska, *On some properties of graph based public keys*, Albanian Journal of Mathematics, Volume 2, Number 3, 2008, 229-234.
45. T. Chojecki, V. Ustimenko, *On fast computations of numerical parameters of homogeneous algebraic graphs of large girth and small diameter and encryption of large files*, , Cryptology ePrint Archive, 2022/908.
46. M. Polak, U. Romanczuk, V. Ustimenko and A. Wrblewska , *On the applications of Extremal Graph Theory to Coding Theory and Cryptography*, Electronic Notes in Discrete Mathematics ,(2017) no. 43, 329–342.
47. V. Ustimenko, *On semigroups of multiplicative Cremona transformations and new solutions of Post Quantum Cryptography*, Cryptology ePrint Archive, 133, (2019).
48. Anne Canteaut, Franois-Xavier Standaert (Eds.), *Eurocrypt 2021, LNCS 12696, 40th An-nual International Conference on the Theoryand Applications of Cryptographic Techniques Zagreb, Croatia, October 1721, 2021, Proceedings, Part I*, Springer, 2021, 839p.
49. V. Ustimenko, *New results on algebraic graphs of large girth and their ipact on Extremal Graph Theory and Algebraic Cryptography*, IACR e-print archive, 2022/1489.