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 \(x_i \rightarrow f_i, i = 1, 2, \ldots, n, f_i \in K[x_1, x_2, \ldots, x_n]\) over commutative ring \(K\) defines endomorphism \(\sigma_n\) of \(K[x_1, x_2, \ldots, x_n]\) into itself given by its values on variables \(x_i\). Degree of \(\sigma_n\) can be defined as maximum of degrees of polynomials \(f_i\). We say that family \(\sigma_n, n = 2, 3, \ldots\) 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 \(\sigma_n\) 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 \(\sigma_n\) 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

\[ x_1 \to f_1(x_1, x_2, \ldots, x_n), \quad x_2 \to f_2(x_1, x_2, \ldots, x_n), \ldots, \quad x_n \to f_n(x_1, x_2, \ldots, x_n). \]

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 \( \text{End}(F_q[x_1, x_2, \ldots, x_n]) \) 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 \( \alpha n, \alpha > 0 \) 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 explicit constructions. This section contain several examples of cryptographic applications of proven statements.

Implementation of twisted Diffie-Hellman protocol based on the platform semigroup $^mES(K)$ 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 $^mP_m(K)$ onto $^mES(K)$ 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 Cremoana 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 \(\delta\) 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 \(\text{End}(K[x_1, x_2, \ldots, x_n]) = ^nCS(K)\) of \(K'\) known also as affine Cremoana semigroup (see [3], [4]) after the famous Luigi Cremona (see [5]). The map \(\tilde{\delta} : (x_1, x_2, \ldots, x_n) \rightarrow (f_1(x_1, x_2, \ldots, x_n), f_2(x_1, x_2, \ldots, x_n), \ldots, f_n(x_1, x_2, \ldots, x_n))\) is polynomial transformation of affine space \(K^n\). These transformations generate transformation semigroup \(CS(K^n)\). Note that the kernel of homomorphism of \(^nCS(K)\) to \(CS(K^n)\) sending \(\delta\) to \(\tilde{\delta}\) depends on the choice of commutative ring \(K\).

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

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

\(^nES(K)\) stands for the semigroup of Eulerian endomorphisms, i. e. endomorphisms \(\omega\) from \(^nCS(K)\) such that \(\omega(x_i) = a_{i,1}x_1^{a_{i,1}}a_{i,2}x_2^{a_{i,2}}\ldots x_n^{a_{i,n}}\), 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 \(\omega\) 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 \(\omega\) from \(^nCS(K)\) such that \(\omega G\) acts on \((K^*)^n\) as identity.

It is easy to see that if \(G \in TA(n, K)\) and \(H \in ^nEG(K)\) then composition \(HG\) of \(H\) and \(G\) is a toric automorphism as well. Assume that automorphism \(F\) from \(^nCG(K)\) has constant degree \(d\), \(d \geq 2\). It is given in its standard form written as \(x_1 \rightarrow f_1(x_1, x_2, \ldots, x_n), x_2 \rightarrow f_2(x_1, x_2, \ldots, x_n), \ldots, x_n \rightarrow f_n(x_1, x_2, \ldots, x_n)\) 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 $^{n}EG(K)$ of $H_{n}$ but the standard form of $H_{n}'G^{-1}$ is impossible to compute.

More general class is the totality of toric multivariate rules $G$ of kind $x_{1} \rightarrow G_{1}$ where $G$ is a toric automorphism of $K[x_{1}, x_{2}, \ldots, x_{n}]$ of constant degree $d$. We can take element $H$ of $^{n}ES(K)$ 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 $j = 1, 2, \ldots, n$.

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 $\leq 3$ has trapdoor accelerator $^{n}T$ of level $\geq d$ if

(i) the knowledge of piece information $^{n}T$ ("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 $cn^{\alpha}$ where $c$ and $\alpha$ are positive constants.

The family $F_{n}$ of unbounded degree has symmetric trapdoor accelerator $^{n}T_{n}$ if the knowledge of piece of information $^{n}T$ 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 $^{n}T$.

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. Assume that some extraction function $\text{Ext}$ 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 $F_n F'_n$ 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 $\alpha$.

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 $O(n^3)$ 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 inverter. 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 $n \ EG(K)$.
Examples in [26], [27] have cubic diagonaliser. Note that family $F_n \in^n \text{CG}(K)$ 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 $F_n = H_n G_n$, where $H_n \in^n \text{EG}(K)$, $G_n \in^n \text{CG}(K)$ is unbalanced 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 $^n\text{CS}(K)$ are very difficult. The task of computation of the composition of $n$ elements $\sigma_1, \sigma_2, \ldots, \sigma_n$ 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 $^n\text{CS}(K)$. 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 $^n\text{CS}(K)$. we say that $S$ possesses the property of multiple computation of composition, shortly MCCP-property.

It is easy to see that General Affine Semigroup $^n\text{AGS}(K)$ of transformations of kind $(x_1, x_2, \ldots, x_n) \rightarrow (x_1, x_2, \ldots, x_n)A + (b_1, b_2, \ldots, b_n)$, 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 $^n\text{ES}(K)$. 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.

$pI$ if and only if the equations
In the girth and lines some positive constant can consider an infinite bipartite graph $A(n, F_q)$, $n > 1$ 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 $(p_1, p_2, ..., p_n, ...)$ and lines $[l_1, l_2, ..., l_n, ...]$ 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 $A(n, K)$, $n = 2, 3, ...$ is bounded below by linear function $cn$ for some positive constant $c$ [3].

As a byproduct of this result we get that $A(n, q)$, $n = 2, 3, ...$ 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 homomorph 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 linguistic graphs of type $(1, 1, n - 1)$ [40], i.e. bipartite graphs with partition sets $P = K^n$ (points of kind $(x_1, x_2, ..., x_n)$, $x_i \in K$) and $L = K^n$ (lines $[l_1, l_2, ..., l_n]$, $l_i \in K$) and incidence relation $I = I(n, K)$ such that $(x_1, x_2, ..., x_n)I[y_1, y_2, ..., y_n]$ if and only if $a_2x_2 + b_2x_2 = f_2(x_1, y_1), a_3x_3 + b_3x_3 = f_3(x_1, x_2, y_1, y_2), ..., a_nx_n + b_nx_n = f_n(x_1, x_2, ..., x_n)$, where $a_i$ and $b_i$ are elements of multiplicative group $K^*$ of $K$ and $f_i$ are multivariate polynomials from $K[x_1, x_2, ..., x_{i-1}, y_1, y_2, ..., y_n, y_{i-1}]$ for $i = 2, 3, ..., n$.

The colour of $\rho(v)$ of vertex $v$ of graph $I(K)$ is defined as $x_1$ for point $(x_1, x_2, ..., x_n)$ and $y_1$ for line $[y_1, y_2, ..., y_n]$. 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 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 $(x_1, x_2, ..., x_n)$ to point $(a, x_2, x_3, ..., x_n)$ and line $[x_1, x_2, ..., x_n]$ to line $[a, x_2, x_3, ..., x_n]$.

Let us consider a walk $v, v_1, v_2, ..., v_{2s}$, of even length $2s$ in the linguistic graph $I(K)$. The information on the walk is given by $v$ and the sequence of colours $\rho(v_i), i = 1, 2, ..., 2s$. The walk will not have edge repetitions if $\rho(v_2) \neq \rho(v), \rho(v_1) \neq \rho(v_{i-2})$ for $i = 3, 4, ..., n$. Notice that $v$ and $v_{2s}$ are elements of the same partition set ($P$ or $L$).

For each vertex $v$ of $I(K)$ we consider a variety of walks with jumps, i.e. totality of sequences of kind $v, v_1 = ^{a_1}C(v), v_2 = N_{a_2}(v_1), v_3 = ^{a_3}C(v_2), v_4 = N_{a_4}(v_3), ..., v_5 = ^{a_5}C(v_4), ..., v_{4s} = N_{a_{4s}}(v_{4s-1}), v_{4s+1} = ^{a_{4s+1}}C(v_{4s}).$
Note that for each \( s \), \( s \geq 0 \) vertices \( v, v_1, v_2, v_{4s+1} \) 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 \( a_1(x_1), a_2(x_1), \ldots, a_{4s+1}(x_1) \) from \( K[x_1] \). The final vertex of this walk is \( v_{4s+1} \) with coordinates \( a_{4s+1}(x_1), f_2(x_1, x_2), f_3(x_1, x_2, x_3), \ldots, f_s(x_1, x_2, \ldots, x_n) \).

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 \( x_1 \rightarrow a_{4s+1}(x_1), x_2 \rightarrow f_2(x_1, x_2), \ldots, x_n \rightarrow f_s(x_1, x_2, \ldots, x_n) \) 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 \( LSP(I(K)) \) (or \( LSL(I(K)) \)) 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 \( =(a_1(x), a_2(x), \ldots, a_k(x)) \times (b_1(x), b_2(x), \ldots, b_s(x)) = (a_1(x), a_2(x), \ldots, a_{k-1}(x), b_1(a_k(x)), b_2(a_k(x)), \ldots, b_s(a_k(x))) \).

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 \( x \rightarrow a(x) \) 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 \( I(K) \eta : F_K End(K[x_1, x_2, \ldots, x_n]) \) such that \( I(K) \eta(u) = ^uT_P \) (or \( I(K) \eta_L = ^uT_L \)) is a semigroup homomorphism.

It is easy to see that \( I(K) \eta_P(F_K) = LSP(I(K)) \) and \( I(K) \eta_L(F_K) = LSL(I(K)) \).

**Proposition 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 \( I(K) \eta_L \)) is invertible element of \( LSP(I(K)) \) (or \( LSL(I(K)) \) if and only if the map \( x \rightarrow a_k(x) \) is an element of \( Aut(K[x]) \).

**Proof.** Let \( u = (a_1(x), a_2(x), \ldots, a_k(x) \) be an element of \( F_K \) and \( x \rightarrow a_k(x) \) has inverse \( x \rightarrow b(x) \) in \( End(K[x]) \) in \( SL_P(I(K)) \). Then \( w = (a_{k-1}(b(x), a_{k-2}(b(x), \ldots a_1(b(x)), b(x)) = Rec_u(x) \) 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 \( (I(K) \eta_P(u), P) \) (or \( (I(K) \eta_L(u), L) \)) are bijective if and only if the map \( x \rightarrow b(x) \) 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 \( x \rightarrow x^3 \) is birational automorphism
Let $x \rightarrow x^{1/3}$ of $K[x]$. Thus $g_P = I_K \eta_P(u)$ and $g_L^I_K \eta_L(u)$ do not have inverses in $\text{End}(K[x])$. They have bijective birational inverses. Noteworthy that $g_P$ and $g_L$ are transformations of infinite order. Degree of polynomial transformations of $g_P$ and $g_L$ are at least $3^\alpha$.

Thus 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 $u = (x, f_1, f_2, \ldots, f_n, f_s)$. 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 $N_{I}$ 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 $St(I)$ of words $u = (x + \alpha_1, x + \alpha_2, \ldots, x + \alpha_k)$ where $\alpha_i$ are elements of $K$. Let $\tilde{F}_K = F_K \cap St_K = F_K \cap St_K$ and introduce groups $I_K \eta_P(F_K) = \tilde{H}_P(I(K))$, $I_K \eta_L(F_K) = \tilde{H}_L(I(K))$, $I_K(\eta_P(\Sigma_k)) = \tilde{H}_P(I(K))$, $I_K(\eta_L(\Sigma_k)) = \tilde{H}_L(I(K))$.

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

**Proposition 3.3.**

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 $H_P(I(K))$ and $H_L(I(K))$ 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 $u = (x, f_1, f_2, f_3, \ldots, f_n, f_s)$, $s \leq n$ 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 an element of $\tilde{F}_K$ then $g = A(n, K) \eta(u)$ is an automorphism of $K[x]$ and its inverse $x \rightarrow h(x)$ has degree $t$. Then image of $g^{-1}$ is $\text{Rev}(u)$ for $u' = (x, f_1, f_2, \ldots, f_s, g_s)$. Note that $\text{Rev}(u) = (f_s(h), f_s(h), f_s - 1(h), f_{s-1}(h), f_1(h), f_1(h), h)$. Let $d = \deg f_s + \deg f_1 + \deg f_{s-1} + \deg f_{s-3} + \deg f_{s-4} + \cdots + \deg h - f_1$.

**Corollary 3.2.**

Let $u = (x, f_1, f_2, f_3, \ldots, f_s, g_s)$ 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 $x \rightarrow g_s$ is an automorphism of $K[x]$ and its inverse $x \rightarrow h(x)$ has degree $t$. Then image of $g^{-1}$ is $\text{Rev}(u)$ for $u' = (x, f_1, f_2, \ldots, f_s, g_s)$. Note that $\text{Rev}(u) = (f_s(h), f_s(h), f_s - 1(h), f_{s-1}(h), f_1(h), f_1(h), h)$. Let $d = \deg f_s + \deg f_1 + \deg f_{s-1} + \deg f_{s-3} + \deg f_{s-4} + \cdots + \deg h - f_1$. 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 $u = (x, x + a_1, x + a_1, x + a_2, x + a_2, \ldots, x + a_{k-1}, x + a_k, x^t)$ of $F_K$ for commutative ring with unity with finite multiplicative 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 $H_k(D(n, K)$ were introduced in [43]. The fact that elements of $H_P(D(n, K)$ $(GD(n, K)$ are transformations of degree $\leq 3$ 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 $F_n = T_1A(n, K)\eta(u)T_2$, 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 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 $cn/s < n$ for some positive constants $\alpha$ and $\beta$ and $d_i \neq d_{i+2}$, $i = 1, 2, \ldots, s - 2$. Let us consider graph $A(n, K)$ and $F_n = T_1A(n, K)\eta(u)T_2$ 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 $(p) = (p_1, p_2, \ldots, p_0)$ 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 $F_n = T_1A(n, K)\eta(u)T_2$ 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
proportional to degree of

affine transformation of \( w \) that

is 2

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

Let us assume that \( c m < s < m \) where \( \alpha \) 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 \( G_{m} = T_{1}F_{m}T_{2} \). Standard forms of cubical maps \( G_{m} \) form family with trapdoor accelerator \( m\cdot n T \) which are triples \( T_{1}, \) \( (x, x + a_{1}, x + a_{2}, x + a_{3}, \ldots, x + a_{s}, x, x^{2}) \) and \( T_{2} \) of level \( t_{n} = 32^{n-1} \). Really, the knowledge on the triples gives us \( T_{2}^{-1} \), \( \text{Rev}((x, x + a_{1}, x + a_{2}, x + a_{3}, \ldots, x + a_{s}, x, x^{2})) \) 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 \( m\cdot n T \) 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 \( u = (x, x + a_{1}, x + a_{2}, x + a_{3}, \ldots, x + a_{s}, x^{2}) \). We use the assumption that \( \alpha \times m < s < m \) and \( s \) is even where \( \alpha \) is a positive constant. Let \( G_{m} \) be the standard form of the composition of \( T_{1}, \) \( \mathbb{A}(m,q) \eta(u) \) and \( T_{2} \). The degree of \( G_{m}^{-1} \) acting on \( F_{q} \) is \( \geq 3t \), where \( t \) is maximal power of 3 which \( \leq q - 1 \) and transformations of kind \( T_{1}F_{m}T_{2}, \) \( F_{m} = \mathbb{A}(m,q) \eta(u) \) can serve as public keys. This algorithm is implemented in the case of finite fields \( F_{2^{m}} \).

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 \( E_{n} \) acts on \( n\cdot m T(K) \) as identity map. The degree of \( E_{n}(K) \) is at least \( 3 \times t \) where \( t \) is maximal power of 3 which \( < d \). 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, \( u = (x, x + a_{1}, x + a_{2}, x + a_{3}, \ldots, x + a_{s}, x^{2}) \) where even \( s \) is selected as in the previous example. Standard form \( G_{m} \) of \( T_{1}A(m,K) \eta(u)T_{2} \) 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 $O(n^2)$. 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 plaintexts $T_m(K)$ and the space of ciphertexts $K^n$.

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 $T_1(x_1) = a_1x_1 + a_2x_2 + \cdots + a_m(x_m)$ 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 $\pi$ and $\sigma$ be two permutations on the set $\{1, 2, \ldots, n\}$. 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 $^\lambda JG(\pi, \sigma)$, 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).

\[
y_\pi(1) = y_\pi(2) = \cdots = y_\pi(n) = \mu_n a_{\pi(1)} a_{\pi(2)} \cdots a_{\pi(n)},
\]

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

We refer to $^\lambda JG(\pi, \sigma)$ as Jordan - Gauss multiplicative transformation or simply $JG$ element. It is an invertible element of $^nES(K)$ with the inverse of kind $^\lambda JG(\pi, \sigma)$ such that $a(i, j)b(i, i) = 1$ (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 $\tau$ 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 $J_1, J_2, \ldots, J_k$, $k \geq 2$, $k = O(1)$ from $^nEG_n(K)$ and form $H_n = J_1J_2\cdots J_k$ written in its standard form. Assume that $^nT$ is expanded by adding $J_j^{-1}$ for $j = 1, 2, \ldots, n$. 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

\[
x_1 \rightarrow \mu_1 x_1 a_{(1,1)}
\]
\[
x_2 \rightarrow \mu_1 x_2 a_{(2,1)}x_2 a_{(2,2)}
\]
\[ x_n \rightarrow \mu_1 x_1^{a(n,1)} x_2^{a(n,2)} \ldots x_n^{a(n,n)} \]

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

and

\[ x_1 \rightarrow \beta_1 x_1^{b(1,1)} x_2^{b(1,2)} \ldots x_n^{b(1,n)} \]

\[ x_2 \rightarrow \beta_2 x_2^{b(2,2)} x_2^{b(2,3)} \ldots x_n^{b(2,n)} \]

\[ \ldots \]

\[ x_n \rightarrow \beta_n x_n^{b(n,n)} \]

where \((b(1,1), d) = 1, (b(2,2), d) = 1, \ldots, (b(n,n), d) = 1.\)

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

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 \(T_1 A(n, K)^\eta(u)T_2\) 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 \(F_n = J_1 J_2 T_1^{\eta(n,K)} T_2\).

The knowledge on this factorization allows to compute \(F_n(x) \in K^{*n}\) and solve equation of kind \(F_n(x) = y, y \in F_n(K^{*n})\) 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 \(G_n^{-1} H_n^{-1}\) 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 \(u = (x, x + a_1, x + a_1, x + a_2, x + a_2, \ldots, x + a_{s-1}, x + a_{s-1}, x + a_3, x^3)\) and \(T_1\) 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 \(u = (x, x + a_1, x + a_1, x + a_2, x + a_2, \ldots, x + a_{s-1}, x + a_{s-1}, x + a_3, x^3)\). So we get the toric automorphism of \(K[x_1, x_2, \ldots, x_n]\) 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 proof 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 $K = F_{2^{14}}$.

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

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

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

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

If we consider the case of $K = Z_{2^{16}}$ we obtain the following densities

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

$$d(32,32) = 248, d(32,64) = 428, d(32,128) = 788, d(32,256) = 1508;$$

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

$$d(128,32) = 180861, d(128,64) = 290432, d(128,128) = 509812, d(128,256) = 949652.$$
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 degree 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 $\tilde{u} = (x, f_1, f_1, f_2, f_2, \ldots, f_s-1, f_s, x^3)$ 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 $\mathbb{Z}_{2^m}$ we use condition $T(x_1) = x_1 b_1 + x_2 b_2 + \cdots + x_n b_n$ 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 $x_1 \rightarrow x_1 a_1 + x_2 a_2 + \cdots x_n a_n$ where $a_i$ are elements of $K^*$ and $x_j \rightarrow x_j$ 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 $O(n)$.

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 $^n ES(K)$ as in Example 4 has to be constructed. In each of these cases we take transformation $W_n = J_1 J_2 T_1 F_n T_2$ 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 $h^{-p} g^s h^p = g_B$. They exchange $g_A$ and $g_B$ and compute collision element $X$ as $A = g = h^{-d} g_B h^d$ and $B = h^{-p} g_A h^p$ respectively.

Adversary has $g_A$ and $g_B$. He/she has to solve the equation $h^{-y} g^x h^y = g_A$ 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 $^n ES(K)$, $n = 2, 3, \ldots$ 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 $S_1 < S$ and $S_2 < 2S$ be pairs of finite semigroups which contains invertible elements.

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

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 $w = w(z_1, z_2, \ldots, z_k) = z_1^{\phi(1)}, z_2^{\phi(2)}, \ldots, z_s^{\phi(s)}$, $s \geq 2$, $\{i_1, i_2, \ldots, i_s\}$ is a subset of cardinality $s$ in $\{1, 2, \ldots, k\}$.

Bob forms specialisation $W(a_1, a_2, \ldots, a_k) = a_{i_1}^{\phi(1)} a_{i_2}^{\phi(2)} \ldots a_{i_s}^{\phi(s)} = a$ and sends $a$ to Alice. For himself he computes collision element $W(b_1, b_2, \ldots, b_k) = b_{i_1}^{\phi(1)} b_{i_2}^{\phi(2)} \ldots b_{i_s}^{\phi(s)} = b$.

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

We consider the implementation of this algorithm in the case when $S_1$ and $S_2$ are Semigroups $^m ES(K)$ and $ES_m(K)$, $m = m(n) > n$ and $|K^*| \geq 3$. Alice works with Parabolic subsemigroup $P(K) = ^n P_m(K)$ of all endomorphisms $g$ from $S_1$ such that $g(x_1), g(x_2), \ldots, g(x_m)$ are monomials from $K[x_1, x_2, \ldots, x_n]$. She uses canonical homomorphism of $^n P_m$ 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 $x_i \rightarrow g(x_i)$, $i = 1, 2, \ldots, m$.

In the simplest case Alice takes $^1 h$ as composition of $^1 J_1$ moving $x_i$ to $x_{i+1}^0(i, i) x_i^0(i, i+1) \ldots x_{i,m}^0(i, i, m)$, $(a(i, i), d) = 1$, $i = 1, 2, \ldots, m$ and $^1 J_2$ moving $x_i$ to $x_{i+1}^1(i, i) x_i^1(i, i) x_{i,j}^1(i, i)$, $(b(i, j), d) = 1$, $i = 1, 2, \ldots, m$, where $a(i, j)$ and $b(i, j)$ for $i \neq j$ are pseudorandom nonzero elements of $Z_d$. She forms $^1 J_1 \times ^1 J_2 = ^1 h$.

Secondly Alice forms $^2 h$ as composition of $^2 J_1$ moving $x_i$ to $x_{i+1}^2(i, i) x_i^2(i, i+1) x_i^1(i, i)$ and $^2 J_2$ moving $x_i$ to $x_{i,m}^2(i, i, m)$, $(c(i, i), d) = 1$, $i = 1, 2, \ldots, n$ and $^2 J_2$ moving $x_i$ to $x_i^d(i, i) x_i^d(i, i) x_i^d(i, i)$.
(d(i, i), d) = 1, i = 1, 2, . . . , n, where c(i, j) and d(i, j) for i ≠ j are presudorandom nonzero elements of Zd. She forms 2J1 × 2J2 = h. Alice selects elements g1, g2, . . . , gk 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 $q_1x_1a(i, 1)x_2a(i, 2)\ldots x_na(i, n)$, $i = 1, 2, \ldots , n$. Alice and Bob form matrix A with entries a(i, j) from Zd and matrix B with entries $b(i, j) = (q_1q_j)^{a(i, j)}$. They form tuple $f_i$ such that $f_1 = x + q_1, f_2 = x + q_2, f_3 = x + q_1 + q_3, f_4 = x + q_2 + q_4, \ldots , x + q_1 + q_3 + \ldots + q_{n-1}, x + q_2 + q_4 + \cdots + q_n$. 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 $x_1$ to $b(i, i)x_1 + b(i, i + 1)x_{i+1} + \cdots + b(i, n)x_{i,n}, i = 1, 2, \ldots , n$ $R_2$ moving $x_i$ to $b(1, i)x_1 + b(2, i)x_2 + \cdots + x_{i-1}^{b(i-1,i)} + x_i, i = 1, 2, \ldots , n$. Alice and Bob independently creates $H = R_1R_2^{A(n,K)}\eta(u)R_2^{-1}R_1^{-1}$ 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 $u = (x, f_1, f_2, f_2, \ldots , f_n)$ they form $w = (x, f_1, f_1, f_2, f_2, \ldots , f_n, x^c)$, where $c = 2$ in the case of even $q$, or $c = 3$ 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. 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 $R'_i$ 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 $R'_i(x_1) = b(1, i)x_1$. 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 $K = Z_2r, r \geq 2$ correspondents can use more general expression for $R'_i(x_1)$ of kind $b(1, 1)x_1 + b(1, 2)x_2 + \cdots + b(1, n - 1) + 2b(1, n)$. Recall that we assumed 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 $H = R_1 R_2^A(n, K) \eta(u) R_2 R_1$ (see (1) above). Additionally they use matrix $A$ to create Jordan Gauss elements $1 J$ moving $x_i$ to $x_i^1 x_{i+1} a^{1(i+1)} x_{i+2} a^{2(i+1)} \cdots x_n a^{(i,n)}$, $i = 1, 2, \ldots, n$ and $2 J$ moving $x_i$ to $x_i^1 x_{i+1} a^{1(i,1)} x_{i+2} a^{2(i,2)} \cdots x_{i-1} a^{(i-1,1)}$, $i = 1, 2, \ldots, n$ where $d(i,i) = a(i,i)$ if $(a(i,i), d) = 1$ and $a(i, 1) = 1$ in the opposite case. Each of correspondents forms $H'$ as $1 J^2 J H$.

Alice sends $E + H'$ to Bob. He restores the standard form of multivariate 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 $1 J$ and $2 J$ and their composition $J'$ together with a cubical map $H$. Alice sends tuple of monomial terms $(J(x_1) J(x_2), J(x_2) J'(x_2), \ldots, J(x_n) J'(x_n))$ 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 $T_2^{-1}, A(n,K) \eta(Rev(u))$, $T_1^{-1}, J^{-1}$. 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 $u = (x, f_1, f_2, f_3, \ldots, f_n)$ as in (i).

In the case of characteristic $2$ they have a choice to create $w = (x, f_1, f_2, f_3, \ldots, f_n, x^2)$ or to use $w = (x, f_1, f_2, f_3, f_4, \ldots, f_n)$ 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 $R_1^{-1}, R_2^{-1}, A(n,K) \eta(Rev(u))$, $R_2^{-1}, R_1^{-1}, J_2^{-1}, J_1^{-1}$ 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 $u = (u(b_1, b_2, \ldots, b_n)$ given as $f_1 = b_1 x, f_2 = b_2 x, f_3 = b_3 x^2 + b_1, f_4 = b_4 x^2 + b_1, f_5 = b_5 x + b_1 + b_3, f_6 = b_6 x + b_2 + b_4, \ldots, b^{n-1}_n a^T x_a + b_1 + b_3 + \cdots + b_{n-3}, b_n x^2 + b_1 + b_2 + \cdots + b_{n-2}$ where $\alpha = 2, t = 1$ for $n = 0 \pmod{4}$ and $\alpha = 1, t = 2$ for $n = 2 \pmod{4}$, $b_1, b_2, \ldots, b_n$ are elements from $K^*$.

Accordingly to the given above estimate degree of $A(n,K) \eta(u')$ for $u' = u(b_1, b_2, \ldots, b_n) = (x, f_1, f_2, f_3, f_4, \ldots, f_k, f_k)$ is at least $2n - 2$. It is easy to see that degree of $A(n,K) \eta(w)$ for $w(b_1, b_2, \ldots, b_n) = (x, f_1, f_2, f_3, f_4, \ldots, f_k, x^e)$ 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. $r e = 1 \pmod{d}$. Then $x^e = x, (x x^e)^r$ is an identity map. Degree of the composition of $x x^e$ 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 \( F_q, q = 2^l \) and \( e = 2 \). In this case \( r = 2^{l-1} \). Then the composition of \( x \to x^{2^l-1} \) and \( xx^2 \) is an identity. The degree of inverse for \( x \to x^2 \) has degree \( 2^{l-1} \). 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 \( \delta^{-1} \) for the bijective map \( \delta : x \to x^e \) belongs to the cyclic group \( C = \langle \delta \rangle \). Noteworthy that \( x \to x^e \) for \( e^s < d \) can not be the inverse for \( \delta \) 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 \( F_{p^s}, p \) is a prime and \( e = p \) we have \( d = p^l - 1, r = 3^{l-1} \). The inverse map of \( \delta \) has degree which is equal to the maximal power of \( p \) in the interval \((0, p^l - 1)\).

Let us estimate degree \( g = A(n, K) \eta_n(Rev(w)) \). Notice that \( Rev(w) = (f_1(x^r), f_2(x^r), f_2(x^r), f_2(x^r), f_2(x^r), f_2(x^r), f_2(x^r), f_2(x^r), f_2(x^r), f_2(x^r)) \). 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 \( ^*ES(K) \), where \( n \) is even parameter \( \geq 2 \) 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 \( B = (b(i, j)) \in K^* \) as in previous section. Additionally they have a vector \((q_1, q_2, ..., q_n)\) of coefficients from the standard form of the output. Correspondents agree on parameter \( e \) via open channel.

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

They work with the plaintext \((x_1, x_2, ..., x_n)\) from \( K^n \) and ciphertext from \( K^n \).

The encryption algorithm contains the following steps.

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

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

Step 3. Sender consecutively computes \( R'(p) = v^1 p, R_2^{-1}(rpm) = v_3 p, N_{a_1}(p^3) = v^2 p, N_{a_2}(p^4) = v_3 p, ..., N_{a_{n-1}}(p^{n+1}) = v_3 p, J_{a_2}(p^{n+2}) = v_3 rpm, R_2R_1(n+3) = v_3 \).

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

For the decryption correspondent executes the following steps.

Step 1. Takes ciphertext \( c \) and notes \( R_1^{-1}R_2^{-1}(c) = (b_1, b_2, c_3, ..., c_n) = v_1 c \).

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

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

Step 3. Correspondent forms \( v^2 c = (p_1 + a_n, a_2, c_3, ..., c_n) \).

Step 4. He/she computes \( N_{a_{n-1}}(v^2 c) = v_3 c \).

Step 5. Computation of \( N_{a_{n-2}}(v^3 c) = v_4 c \).

...
Step \( n + 4 \). Computation of \( N_{p_1}(c) = v \).
Final step is computation of \( R^{-1}R^{-1}(v) = p \).

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 output \( G \). 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 automorphism.

It is impossible to compute. Symmetric cipher with such encryption was implemented.

On Extremal Algebraic Graphs and Multivariate Cryptosystems 21
We can consider transformations $^1 J$ and $^2 J$ defined by the rules $x_1 \rightarrow c(i, 1)x_1^{a(i, 1)}x_2^{a(i, 2)}\ldots x_n^{a(i, n)}$, $x_2 \rightarrow c(i, 2)x_2$, $\ldots$, $x_n \rightarrow c(i, n)x_n$, $i = 1, 2$ 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 "CG($K$)" or toric automorphisms with trapdoor accelerator $T$ there is an option to work with "sparce" trapdoor accelerator. In the case of elements from "EG($K$)" one can work with function $F_n = J_2 \mu_{n}(u) J_2$ as above in the case when length $s$ of the walk $O(1)$.

In the cases of $F_n = T_1 \mu_n(u) T_2$ one can use the space of linear transformations such that $T(x_1)$ and $T_2(x_1)$ are of kind $b_1 x_1 + b_2 x_2 + \ldots + x_n, b_i \in K^*$. $T(x_j) = x_j$ for $j = 2, 3, \ldots, n$ and use $u$ of kind $(x, f_1, f_1, f_2, f_2, \ldots, f_s, g(x))$ where the choice of $f_j$ and $g(x)$ depends on the used algorithm.

In cases of Examples 9, 10, 11 degrees 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 the case 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 $F_n = J_1 J_2 T_1 T_2 u$ Special choice of trapdoor informations 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 "ES($K$)". They take the collision element $G$ and form the matrices $A$ and $B$. Some "light extraction algorithm" can be used to select $(a(i, 1), a(i, 2), \ldots, a(i, n)), i = 1, 2$ as some rows or columns of $A$ and vectors from $(K^*)^n$ as rows or columns of matrix $B$.

## 9 Open schemes of collision maps extractions

Let $K$ be a commutative ring with multiplicative group $K^*$ of order $\geq 3$. We consider an element $^T F_n = F_n$ from "CG($K$)" 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 $G_n = T_1^T F_n T_2$. It is easy to see that automorphism $G_n$ has trapdoor accelerator $T' = (T_1, T_2)$. We refer to $T'$ as deformation of $T$. In many cases the information on $T$ can be given via two vectors $v_1$ from $K^r$ 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 $G_n = T^T F_n T_2$ where $G_n$ and $F_n$ are toric automorphisms and solution for $F_n(x) = b$, $x \in (K^n)^n$ can be computed in time $O(n^2)$.

Other examples of toric trapdoor accelerators corresponds to Eulerian transformations from $^sEG(K)$. Let $^M J$ element from $^sEG(K)$ such that the knowledge of $M$ allows the computation of solution for $^M J(x) = b$, $b \in K^n$ can be computed in time $O(n^2)$. Then $E_n = J_1^M J J^2$ 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 $Y_n = J_1^M J J T_1 T F_n T_2$ 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 ($f_1, f_2, \ldots, f_s$). One can take vectors $v(i)$ of coefficients in front of monomials of $g_i$ ordered in lexicographical order, and the list $m(i)$ of normalised ordered monomials (with coefficient $1$) ordered monomials of $g_i$.

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

For the feasibility of protocol the semigroup $S$ of $^sC$ has satisfy tp Multiple Composition Computation Property (MCCP) which insures the computation of $s$ elements of $S$ in polynomial 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 $x_i \rightarrow q_i x_1^{a(1)} x_2^{a(2)} \ldots x_s^{a(s)}, i = 1, 2, s$

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 $v = (v_1, v_2, \ldots, v_n)$ and $a = (a_1, a_2, \ldots, a_n)$ are lists of elements of $B$ and $A$ ordered lexicographically.

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

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

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

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

9. 2. PROTOCOL INTERPRETATION.

Let us consider toric automorphism of kind $G_m = T^T F_m T_2$ from $^mCS(K)$ where $F_m$ is graph based toric automorphism $^A(m, K)\eta(u)$ with trapdoor accelerator of kind $(x, f_1, f_1, f_2, f_2, \ldots, f_s, g_s)$, $s = O(m)$. For the simplicity we assume
that $g_1$ 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 $Z$ ans $Z'$ of size $m \times m$ with rows $Z_j = (z_{i(1,j)},z_{i(2,j)},\ldots,z_{i(j,j)},0,0,\ldots,0)$ and $Z'_j = (z_{i(1,j)},z_{i(2,j)},\ldots,z_{i(j,j)},0,0,\ldots,0)$. Words $(l(1,j),z_{i(1,j)},\ldots,z_{i(j,j)})$ and $(l(1,j),l(2,j),\ldots,l(j,j))$ in the alphabet $\{1,2,\ldots,n^2\}$ can be generated by some pseudorandom algorithm.

Similarly he/she forms two formal upper triangular matrices $Y$, $l = 1,2$ with rows $Y_j = (0,0,\ldots,y_{k(j,j)},y_{k(j,j+1)},\ldots,y_{k(j,m)})$ and two vectors $R = (z_{l(1)},z_{l(2)},\ldots,z_{l(m)}), j = 1,2$.

Secondly the correspondent forms polynomials of kind $Q(x) = z_{l(0,j)} + z_{l(2)}x + \ldots + z_{l((r(j)),j)}x^{r(j)}$ where $l(j,i)$ are elements of the alphabet $\{1,2,\ldots,n^2\}$, $j = 1,2,\ldots,s$, $i = 1,2,\ldots,r(j)$. 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 $B, r = 1,2$ via specialisation $z_{w(i,j)} = v_{w(i,j)}$ and $C, r = 1,2$ via specialisation of matrices $Y$ via specialisation $k(j,i) = v_{k(j,i)}$. They form two vectors $B$ of kind $(v_{1(1)},v_{1(2)},\ldots,v_{1(m)})$. They use specialisations $P(x) = z_{l(0,j)} + z_{l(2)}x + \ldots + z_{l((r(j)),j)}x^{r(j)}$ obtained via the rule $z_{l(j,t)} = v_{l(j,t)}$.

Each of correspondents uses affine transformations $T_r : x \to B_r c_r x + b_r$, $r = 1,2$ and tuple $u = (P_1,P_2,P_3,\ldots,P_s, P_s)$ to encrypt with multivariate rule $x \to T_{1}^{A(m,K)}(x)^2 T_2$. It is easy to see that encryption takes time $O(m^2)$. We assume that $\deg(P_i) \neq \deg(P_{i+1})$, $i = 1,2,\ldots,m-2$, $\deg(P_i) \geq cm$, $s \geq cm$ for some constant $c$. Then degree of encryption map is $\geq cm^2$. The execution 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 sparse variant were $T_1 = C_1, T_2 = C_2$ obtained via specialisations of $Y$, $r = 1,2$ with first rows $(y_{1(1)},y_{1(2)},\ldots,y_{1(m)})$ and other rows $(0,0,0,\ldots,0)$, $(0,0,1,0,\ldots,0)$, $(0,0,0,\ldots,0,1)$. They select $s$ of size $O(1)$. Then the encryption and decryption procedure will take time $O(m)$. We can slightly modify sparse 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

$h_{i(3)l_1} x_1 + h_{i(3)l_2} y_2 = y_{l_1(x_2z_{i(3)}x_{1})}, h_{i(3)l_3} x_3 + h_{i(3)l_4} y_4 = x_{l_3(x_3z_{i(3)}x_{1})}, \ldots h_{i(3)l_m} x_m + h_{i(3)l_m} y_m = y_{l_m(x_4z_{i(3)}x_{1}),...}$

and $m$ is odd where $i_1, j_1, k(l), s(l), l \geq 2$ are elements of the alphabet $\{1,2,\ldots,n^2\}$. After the complition of the protocol correspondents specialise $h_{i_1}, h_{j_1}, s = 2,3,\ldots,m$ as $v_i$ and $v_j$. They set $c_{k(l)} = a_{k(l)}$ if $a_{k(l)} \neq 0$ and $c_{k(l)} = 1$ for $a_{k(l)} = 0$. Similarly $c_{s(l)} = a_{s(l)}$ if $a_{s(l)} \neq 0$ and $c_{s(l)} = 1$ for $a_{s(l)} = 0$, $l = 2,3,\ldots,m$. 
So encryption and decryption requires $O(n^2)$ 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 $z(i,k(i,j))$, $1 \leq i \leq j \leq m$, $t = 1,2$ where $k(i,j)$ is an element of alphabet $\{1,2,\ldots, n^2\} = N$. Additionally we will work with list of variables $u(r(i,j))$, $m \geq i \geq j \geq 1$, $t = 1,2$ where $r(i,j) \in N$. We set lists of variables $x_{k(i)}$, $k(i) \in N$, $i = 1,2,\ldots, m$, $t = 1,2,3,4$ together with $y_{r(i)}$, $t(i) \in N$, $i = 1,2,\ldots, s$, $s = O(m)$, $t = 1,2$.

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

\[ J(x_1) = x_1' c'(k(1,1)), \]
\[ J(x_2) = x_2' c'(k(2,1)), \]
\[ \vdots \]
\[ J(x_m) = x_m' c'(k(m,m)) \]

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 $J$ and $J'$ of kind

\[ J(x_1) = x_1' c'(r(1,1)) x_2' c'(r(1,2)) \ldots x_m' c'(r(1,m-1)) x_m' c'(r(1,m)) \]
\[ J(x_2) = x_2' c'(r(2,1)) x_2' c'(r(2,2)) \ldots x_m' c'(r(2,m-1)) x_m' c'(r(2,m)) \]
\[ \vdots \]
\[ J(x_m) = x_m' c'(r(m,m)) \]

where $t = 3,4$.

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

Correspondents form $u' = (v_{r(i)})$, $i = 1,2,\ldots, s$, $y_{r(i)} = c_{2r(i)}$, $i = 1,2,\ldots, s$, where parameter $s$ is even.

They will encrypt plaintexts from $K^m$ with element $E_m = J^3 J A(n.K^*) \mu(\mu)^2 J^4 J$.

It is easy to check that $E_m$ from $^n EG(K)$ has toric trapdoor accelerator $(J_1, u', J_2)$ where $J_1 = 1, J_2 = 2, J^3 J$.

COMBINED EXTRACTION ALGORITHM.

One of correspondents selects parameters $m$ and $n$. He/she executes extraction algorithm 1 and 2 above. Alice and Bob complete the protocol based on platform $^n ES(K)$. Each of correspondents implement the protocol implementation to get toric maps $F_i = T_A(m.K^*) \eta(u) \eta T_2$ 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 $F_m = \eta(u)$, $u = (x, f_1(x), f_2, f_3, \ldots, f_s, x)$ in the case when the equations of kind $g_s(x) = b, x \in K^*$ has unique solution but function $g_s$ is not a bijection on $K$. We use described above scheme with special selection of $^rT$ as transformations $x: C_x B_x + b_x, r = 1, 2$ during the process of protocol implementation. Then modified algorithm produces toric automorphism $G_m = T_1^T F_m T_2$ with toric trapezoid 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 ${\text{char}}F_q = 2$ 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 $F_q^{2n}$ with degree of the inverse map $3 \times 2^{m-1}$

More general families $A(n, F_q)$, $n \geq 2$ are defined over finite commutative ring $K$ such that $d = |K^{*}| > 2$ and $|3, d| = 1$ is used to construct cubical map $G_n$ of affine space $K^m$, $n \geq 2$ 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 least $3 \times t$ 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 $G^{-1}$ acting on $F_q^n$ is $\geq 3t$, where $t$ is maximal power of 3 which $< q - 1$ and transformations of kind $T_1 F_1 T_2, T_1, T_2 \in AGL_n(F_q)$ can serve as public keys. We consider obfuscations of $G_n$ and $F_n$ of kind $F'_n = H_n T_1(F_n) F_n T_2, T_1, T_2 \in AGL_n(F_q)$ and $G'_n = H_n(K) T_1 G_n T_2, T_2 \in AGL_n(K)$ 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.


49. V. Ustimenko, *New results on algebraic graphs of large girth and their impact on Extremal Graph Theory and Algebraic Cryptography*, IACR e-print archive, 2022/1489.