Communication Papers of the of the 17th Conference on Computer Science and Intelligence Systems pp. 199–206
DOI: 10.15439/2022F54
ISSN 2300-5963 ACSIS, Vol. 32

# On $D(n,q)$ quotients of large girth and hidden homomorphism based cryptographic protocols

Vasyl Ustymenko
Institute of Mathematics
Marie Curie-Sklodowska University
Pl. M. Curie-Skłodowskiej 5
Lublin, 20-031, Poland
Email: vasyl@hektor.umcs.lublin.pl

Michał Klisowski
Institute of Computer Science
Marie Curie-Sklodowska University
Pl. M. Curie-Skłodowskiej 5
Lublin, 20-031, Poland
Email: michal.klisowski@umcs.lublin.pl

***Abstract*—Noncommutative cryptography is based on applications of algebraic structures like noncommutative groups, semigroups, and noncommutative rings. Its intersection with Multivariate cryptography contains studies of cryptographic applications of subsemigroups and subgroups of affine Cremona semigroups defined over finite commutative rings. Efficiently computed homomorphisms between stable subsemigroups of affine Cremona semigroups can be used in tame homomorphisms protocols schemes and their inverse versions. The implementation scheme with the sequence of subgroups of affine Cremona group that defines the projective limit was already suggested. We present the implementation of another scheme that uses two projective limits which define two different infinite groups and the homomorphism between them. The security of the corresponding algorithm is based on complexity of the decomposition problem for an element of affine Cremona semigroup into a product of given generators. These algorithms may be used in postquantum technologies.**

***Index Terms*—Multivariate Cryptography, stable transformation groups and semigroups, decomposition problem of nonlinear multivariate map into given generators, tame homomorphisms, key exchange protocols, cryptosystems, algebraic graphs**

Support. This research is partially supported by British Academy Fellowship for Researchers at Risk 2022.

## I. Introduction

LET $k$ be a natural number $\geq 3$. The problem of approximation of $k$-regular tree by the family of $k$-regular graphs of increasing order and increasing girth, i.e. minimal length of cycle in the graph, is very important. Solution of this broblem can be used in many applications, like computer implementations of branching process, construction of low density parity check codes, various application to Opimisation Graph Theory and Cryptography (see [30], [32] and further references). Families of $k$-regular graphs $\Gamma_i$ of increasing order $v_i$ of increasing girth satisfying to one of the following 3 properties are especially interesting:

1) to be a family of large girth, i.e. family such that $g_i \geq C \log_{k-1}(v_i)$ for certain constant $C$ and each $i$,
2) to have a tree well defined projective limit of $\Gamma_i$ when $i$ tends to infinity,
3) to be a *family of small world graphs*, i.e. family such that diameter $d_i$ of graphs $\Gamma_i$ is at most $c \log_k(v_i)$.

The known families satisfying properties (1) and (2) were the families of $q$-regular graphs $D(n,q)$, $n = 1, 2, \ldots$ and $q$ are prime powers and their connected components $CD(n,q)$.

In recent publication [33], [34], were announced that special homomorphic images quotients $A(n,q)$ of graphs $D(n,q)$ form a family satisfying (1), (2) and (3) for each value of parameter $q$.

Cryptographic applications of $A(n,q)$ were already known. In particular, in paper [30] postquantum secure protocols which uses standard homomorphisms between $D(n,q)$ and $D(m,q)$ $(n \geq m)$ (or $A(n,q)$ and $A(m,q)$) were used for the construction of protocols of Noncommutative Cryptography.

Current paper is dedicated to protocols of Postquantum Cryptography which use "hidden" remarkable homomorphisms between $D(n,q)$ and $A(n,q)$. In the generalisation of these protocols general finite commutative ring $K$ can be used instead of finite field. We hope that the usage of remarkable graph homomorphism leads a strong postquantum secure protocol.

## II. On ideas of Noncommutative Cryptography with platforms of transformations of Multivariate Cryptography

Post Quantum Cryptography serves for the research of asymmetrical cryptographic algorithms which can be potentially resistant against attacks with the usage of a quantum computer. The security of currently popular algorithms is based on the complexity of the following well known three hard problems: integer factorization, discrete logarithm problem, discrete logarithm for elliptic curves. Each of these problems can be solved in polynomial time by Peter Shor's algorithm for the theoretical quantum computer. In fact, some rather old cryptosystems which were suggested in the late '70s of the 20 century potentially may have some resistance to attacks on quantum computers (see for instance McEliece cryptosystem [18]).

Modern PQC is divided into several directions such as Multivariate Cryptography, Nonlinear Cryptography, Lattice-based Cryptography, Hash-based Cryptography, Code-based Cryptography, studies of isogenies for superelliptic curves, Noncommutative cryptography, and others.

The Multivariate Cryptography (see [4], [12], [6]) uses polynomial maps of affine space $K^n$ defined over a finite commutative ring into itself as encryption tools. It exploits the complexity of finding a solution of a system of nonlinear equations from many variables. Multivariate cryptography uses as encryption tools nonlinear polynomial transformations of kind $x_1 \to f_1(x_1, x_2, \ldots, x_n), x_2, \to f_2(x_1, x_2, \ldots, x_n), \ldots, x_n \to f_n(x_1, x_2, \ldots, x_n))$, transforming affine space $K^n$, where $f_i : K[x_1, x_2, \ldots, x_n]$, $i = 1, 2, \ldots, n$ are multivariate polynomials usually given in a standard form, i.e. via a list of monomials in a chosen order.

Noncommutative cryptography appeared with attempts to apply the Combinatorial group theory to Information Security. If $G$ is a noncommutative group then correspondents can use conjugations of elements involved in the protocol, some algorithms of this kind were suggested in [19], [22], [23], [7], where group $G$ is given with the usage of generators and relations. The security of such algorithms is connected to Conjugacy Search Problem (CSP) and Power Conjugacy Search Problem (PCSP), which combine CSP and Discrete Logarithm Problem and their generalizations. Currently, Noncommutative cryptography is essentially wider than group-based cryptography. It is an active area of cryptology, where the cryptographic primitives and systems are based on algebraic structures like groups, semigroups, and noncommutative rings (see [20], [3], [5], [21], [1], [2], [11], [17], [13]). This direction of security research has very rapid development (see [16], [14] and further references in these publications).

One of the earliest applications of noncommutative algebraic structures for cryptographic purposes was the usage of braid groups to develop cryptographic protocols. Later several other noncommutative structures like Tompson groups and Grigorchuk groups have been identified as potential candidates for cryptographic post-quantum applications. The standard way of presentations of groups and semigroups is the usage of generators and relations (Combinatorial Group Theory). Semigroup based cryptography consists of general cryptographic schemes defined in terms of wide classes of semigroups and their implementations for chosen semigroup families (so-called platform semigroups).

The paper is devoted to some research on the intersection of Noncommutative and Multivariate Cryptographies. We try to use some abstract schemes in terms of Combinatorial Semigroup Theory for the implementation with platforms which are semigroups and groups of polynomial transformations of free modules $K^n$ where $K$ is a commutative ring.

The most popular form of Multivariate cryptosystem is the usage of a single very special map f in a public key mode. The first examples were based on families of quadratic bijective transformation fn(see [4], [12], [6]), such choice implies a rather fast encryption process. The paper is devoted to other aspects of Multivariate cryptography when some subsemigroup of affine Cremona semigroup of all polynomial transformations is used instead of a single transformation. Let us discuss a case of subsemigroup with a single generator. Everybody knows that Diffie-Hellman key exchange protocol can be formally considered in general case of any finite group or semigroup $G$. In the case of group $G$, the corresponding ElGamal cryptosystem can be introduced. Notice that the security of this algorithm depends not only on abstract group $G$ but on the way of its generation in computer memory. For instance, if $G = Z_p^*$ is a multiplicative group of a large prime field then the discrete logarithm problem (DLP) is a difficult one and guarantees the security of the protocol. If the same abstract group is given as an additive group of $Z_{p-1}$ protocol is insecure because DLP will be given by linear equation.

Notice that the implementation of the idea to use a multivariate generator in its standard form has to overcome essential difficulties. At first glance, the Diffie-Hellman protocol in affine Cremona semigroup looks like an unrealistic one because the composition of two maps of degree $r$ and $s$ taken in "general position" will be a transformation of degree $rs$. So in majority of cases $deg(F) = d$, $d > 1$ implies very fast growth of function $d(r) = deg(F^r)$. Of course in the case of the generator in common position, not only a degree but also a density (total number of monomial terms of the map in its standard forms) grows exponentially.

So we have to find special conditions on a subsemigroup of affine Cremona group which guarantees the polynomial complexity of procedure to compute the composition of several elements from subsemigroup. Such conditions can define a basis of Noncommutative Multivariate Cryptography. Hopefully, at least two conditions of this kind are already known [26] (see further references) and [28]. We consider them in the following section.

## III. On stable subsemigroups of Affine Cremona Semigroup, Eulerian transformations and corresponding cryptographic scheme

Stability condition demands that the degree of each transformation of the subsemigroup of affine Cremona semigroup has to be bounded by independent constant $d$. We refer to such subsemigroup as a stable subsemigroup of degree $d$. Examples of known families of stable subgroups of degree $d = 3$ reader can find in [26] (see further references) or [30]. Applications of such families to Symmetric Cryptography could be found in [32]. Some examples of stable families of subgroups of degree 2 are given in [25].

The eulerian condition demands that all transformations of subsemigroup of affine Cremona subgroup are given in a standard form $(x_1, x_2, \ldots, x_n) \to (f_1(x_1, x_2, \ldots, x_n), f_2(x_1, x_2, \ldots, x_n), \ldots, f_n(x_1, x_2, \ldots, x_n))$ where each $f_i$ has density 1. All transformations of this kind form General Eulerian Semigroup ${}^nGES(K)$ of transformations of kind $x_1 \to \mu_1 x_1^{a(1,1)} x_2^{a(1,2)} \ldots x_n^{a(1,n)}, x_2 \to \mu_2 x_1^{a(2,1)} x_2^{a(2,2)} \ldots x_n^{a(2,n)}, \ldots, x_n \to \mu_n x_1^{a(n,1)} x_2^{a(n,2)} \ldots x_n^{a(n,n)}$ where $a(i, j)$ are positive integers and $\mu_i \in K$.

First cryptosystems of Nonlinear Multivariate Cryptography in terms of ${}^nGES(K)$ are suggested in [28].

The *discrete logarithm problem* is the special simplest case of the *word decomposition problem* for semigroups. Let $S'$ be a subsemigroup of $S$ generated by elements $g_1, g_2, \ldots, g_t$. The *word problem* (WP) of finding the decomposition of $g \in S$ into a product of generators $g_i$ is difficult, i.e. polynomial algorithms to solve it with Turing machine or Quantum Computer are unknown. The idea to apply this problem in Cryptography was considered in [39] where some general schemes to use WP for constructions of algorithms of Noncommutative Cryptography were suggested. Of course, the complexity of the problem depends heavily on the choice of $S$ and the way of a presentation of the semigroup. In the cases of families of affine Cremona semigroups or $S =^n GES(K)$, the problem WP is computationally infeasible with a Turing machine and with Quantum Computer.

We are working on implementations of the following formal schemes of usage of the complexity of WP. Tame map means computable in polynomial time from parameter $m$.

*a) TORIC TAHOMA CRYPTOSYSTEM:* Let $K$ be a commutative ring, subgroups ${}^nG$ of ${}^nGES(K)$ act naturally on $(K^*)^n$, ${}^mS(n,K)$ is a subsemigroup of ${}^mGES(K)$ such that there is a tame homomorphisn $\Delta = \Delta(m,n)$ of ${}^mS(n,K)$ onto ${}^nG$. We assume that $m = m(n)$ where $m > n$ and consider the following *toric tahoma cryptosystem*:

Alice takes $b_1, b_2, \ldots, b_s$, $s > 1$ from ${}^mS(n,K)$ and $a_1, a_2, \ldots$, as where $a_i = \Delta(b_i)^{-1}$. She takes $g \in^m EG(K)$ and $h \in^n EG(K)$ and forms pairs $(g_i, h_i) = (g^{-1}b_i g, h^{-1}a_i h)$, $i = 1, 2, \ldots, s$ and sends them to Bob.

He writes the word $w(z_1, z_2, \ldots, z_s)$ in the alphabet $z_1, z_2, \ldots, z_s$ together with the reverse word $w'(z_1, z_2, \ldots, z_s)$ formed by characters of $w$ written in the reverse order. He computes element $b = w(g_1, g_2, \ldots, g_s)$ via specialization $z_i = g_i$ and $a = w'(h_1, h_2, \ldots, h_s)$ via specialization $z_i = h_i$. Bob keeps $a$ for himself and sends $b$ to Alice. She computes $a^{-1}$ as $h^{-1}\Delta(gbg^{-1})h$.

Alice writes her message $(p_1, p_2, \ldots, p_n)$ and sends ciphertext $a^{-1}(p_1, p_2, \ldots, p_n)$ to Bob. He decrypts with his function $a$. Symmetrically Bob sends his ciphertext $a(p_1, p_2, \ldots, p_n)$ to Alice and she decrypts with $a^{-1}$.

The problems of constructions of large subgroups $G$ of ${}^nGES(K)$, pairs $(g, g^{-1})$, $g \in G$, and tame Eulerian homomorphisms $\mu : G \to H$, i.e. computable in polynomial time $t(n)$ homomorphisms of subgroup $G$ of ${}^nGES(K)$ onto $H <^m GES(K)$ are motivated by tasks of Nonlinear Cryptography.

The first platforms for this scheme and some other abstract schemes are suggested in [28].

*b) AFFINE TAHOMA CRYPTOSYSTEM:* If we change semigroup ${}^mGES(K)$ for affine Cremona semigroup $S(K^m)$ we obtain the following *Affine Tahoma Cryptosystem* on stable transformations.

Let $K$ be a commutative ring, stable subgroups $n^G$ of $S(K^n)$ act naturally on $K^n$ and ${}^mS(n,K)$ be a subgroup of $S(K^m)$ such that there is a tame homomorphisn $\Delta = \Delta(m,n)$ of ${}^mS(n,K)$ onto ${}^nG$. We assume that $m = m(n)$ where $m > n$.

Alice takes $b_1, b_2, \ldots, b_s, s > 1$ from ${}^mS(n,K)$ and $a_1, a_2, \ldots, a_s$ where $a_i = \Delta(b_i)^{-1}$. She takes $g \in C(Q^m)$ and $h \in C(R^n)$ where $R$ and $Q$ are extensions of the commutative ring $K$ and forms pairs $(g_i, h_i) = (g^{-1}b_i g, h^{-1}a_i h)$, $i = 1, 2, \ldots, s$ and sends them to Bob. We assume that $g = g'T$, $h = h'T'$ where semigroup $\langle g', {}^m S(n,K)\rangle$ generated by $g'$ and elements of ${}^mS(n,K)$ and group $\langle h', G\rangle$ are stable semigroups of degree $d$ and $T \in AGL_n(R)$, $T' \in AGL_m(Q)$.

As in the previous algorithm Bob writes the word $w(z_1, z_2, \ldots, z_s)$ in the alphabet $z_1, z_2, \ldots, z_s$ together with the reverse word $w'(z_1, z_2, \ldots, z_s)$ formed by characters of $w$ written in the reverse order. He computes element $b = w(g_1, g_2, \ldots, g_s)$ via specialization $z_i = g_i$ and $a = w'(h_1, h_2, \ldots, h_s)$ via specialization $z_i = h_i$. Bob keeps $a$ for himself and sends $b$ to Alice. She computes $a^{-1}$ as $h^{-1}\Delta(gbg^{-1})h$.

Alice writes her message $(p_1, p_2, \ldots, p_n)$ from $R^n$ and sends ciphertext $a^{-1}(p_1, p_2, \ldots, p_n)$ to Bob. He decrypts with his function $a$. Symmetrically Bob sends his ciphertext $a(p_1, p_2, \ldots, p_n)$ to Alice and she decrypts with $a^{-1}$ (see [27]). Let ${}^nTC(K, R, Q)$ stand for affine Tahoma cryptosystem as above.

In [25] quadratic stable subsemigroups with corresponding homomorphisms are suggested as platforms of this scheme. Some other schemes are also implemented there with these platforms. Some cubical platforms were suggested in [27].

Only one family of platforms was investigated via computer implementation. Paper [31] is devoted to implementations of Affine Tahoma scheme with platforms of cubical stable groups. They were defined via families of linguistic graphs that form projective limits and the standard homomorphisms between two members of these sequences. So we have pairs $(G_n, \Delta n)$ where $G_n < S(K^n)$, $\Delta n$ is a homomorphism of $G_n$ onto $G_m$, $m = m(n)$ such that projective limits $\lim(G_n)$, $n \to \infty$ and $\lim(\Delta(G_n))$, $n \to \infty$ coincide with the same infinite transformation group $G$.

This article is devoted to another computer experiment with the new platform which uses the same groups $G_n$ but different tame homomorphisms $\eta_n$ . In the new scheme $\lim(G_n)$, $n \to \infty$ equals to $G$, but $\lim(\eta_n(G_n))$, $n \to \infty$ coincides with the image of homomorphism of $G$ with an infinite kernel.

We believe that the option to vary tame homomorphisms in the chosen sequence of semigroup makes the task of cryptanalytic much more difficult.

We use projective limits $D(K)$ and $A(K)$ of the well known graphs $D(n,K)$ (see [15], [35]) and $A(n,K)$ (see [31] and further references) defined over arbitrary finite commutative rings. Walks on the graphs $D(K)$ and $A(K)$ allow to define groups $GD(K)$ and $GA(K)$ of cubic transformations of infinite dimensional affine space over $K$. Group $GA(K)$ is a homomorphic image of $GD(K)$, both groups can be obtained as projective limits of sequences $GA_n(K)$ and $GD_n(K)$,$n = 1, 2, \ldots$ of finite cubical stable groups. We suggest key exchange protocols based on homomorphisms of $GD_j(K)$ onto $GA_i(K)$ for some $i$ and $j$.

Computer simulations demonstrate an interesting effect of density stabilization of generated cubical maps. The time execution tables for algorithms of generation of maps and numbers of monomial terms are given. They demonstrate the feasibility of algorithms. The method of generation allows constructing for each bijective transformation of the free module over $K$ its inverse map. Multivariate nature of collision maps allows using these algorithms for the safe exchange of multivariate transformations. Various *deformation rules* can be used for this purpose (see formal schemes of [27], [26], [25]).

## IV. Some basic definitions

Let us consider basic algebraic objects of multivariate cryptography, which are important for the choice of appropriate pairs of maps $f$, $f^{-1}$ in both cases of public key approach or idea of asymmetric algorithms with protected encryption rules. Let us consider the totality $SF_n(K)$ of all rules of kind: $x_1 \to f_1(x_1, x_2, \dots, x_n)$, $x2 \to f_2(x_1, x_2, \dots, x_n)$, $\dots$, $x_n \to f_n(x_1, x_2, \dots, x_n)$ acting on the affine space $K^n$, where $f_i$, $i = 1, 2, \dots, n$ are elements of $K[x_1, x_2, \dots, x_n]$ with natural operation of composition. We refer to this semigroup as semigroup of formal transformation $SF_n(K)$ of free module $K^n$. In fact it is a totality of all endomorphisms of ring $K[x_1, x_2, \dots, x_k]$ with the operation of their superposition. Each rule $f$ from $SF_n(K)$ induces transformation $t(f)$ which sends tuple $(p_1, p_2, \dots, p_n)$ into $(f_1(p1, p2, \dots, p_n)$, $f_2(p_1, p_2, \dots, p_n)$, $\dots$,$f_n(p_1, p_2, \dots, p_n))$. Affine Cremona semigroup $S(K_n)$ is a totality of all transformations of kind $t(f)$. The canonical homomorphism $t \to t(f)$ maps infinite semigroup $SF_n(K)$ onto finite semigroup $S(K_n)$ in the case of finite commutative ring $K$.

We refer to pair $(f, f')$ of elements $SF_n(K)$ such that $ff'$ and $f'f$ are two copies of identical rule $x_i \to x_i$, $i = 1, 2, \dots, n$ as pair of invertible elements. If $(f, f')$ is such a pair, then product $t(f)t(f')$ is an identity map. Let us consider the subgroup $CF_n(K)$ of all invertible elements of $SF_n(K)$ (group of formal maps). It means $f$ is an element of $CF_n(K)$ if and only if there is $f'$ such that $ff'$ and $f'f$ are identity maps. It is clear that the image of a restriction of $t$ on $CF_n(K)$ is affine Cremona group $C_n(K)$ of all transformations of $K^n$ onto $K^n$ for which there exists a polynomial inverse.

We say that a family of subsemigroups $S_n$ of $SF_n(K)$ (or $S(K_n)$) is stable of degree $d$ if maximal degree of elements from $S_n$ is an independent constant $d$, $d > 1$. If $K$ is a finite commutative ring then stable semigroup has to be a finite set.

Condition $d > 1$ is natural because of elements from the group $AGL_n(K)$ of all affine bijective transformations, i.e. elements of affine Cremona group of degree 1.

## V. On linguistic graphs and related semigroups of affine transformations

Linguistic graph $I$ of type $(1, 1, n-1)$ over commutative ring $K$ is a bipartite graph with partition sets $P = K^n$ (set of points) anf $L = K^n$ (set of lines) such that point $\mathrm{p} = (p_1, p_2, \dots, p_n)$ is incident to line $\mathrm{l} = [l_1, l_2, \dots, l_n]$ if and only if $a_2p_2 + b_2l_2 = f_1(p_1, l_1)$, $a_3p_3 + b_3l_3 = f_2(p_1, p_2, l_1, l_2)$, $\dots$, $a_np_n + b_nl_n = f_{n-1}(p_1, p_2, \dots, p_{n-1}, l_1, l_2, \dots, l_{n-1})$ where $a_i$ and $b_i$ are elements of $K^*$ and $f_i$ are multivariate polynomials with coefficients from $K$. We define colours of points and lines as $\rho(\mathrm{p}) = p_1$ and $\rho(\mathrm{l}) = l_1$. In linguistic graph for each vertex there is a unique neighbour with chosen colour. Symplectic homomorphism of lingustic graph is the homomorphism induced by selecting coordinates $p_i$ of points and $l_i$ where $i$ is an element of selected proper subset of $\{2, 3, \dots, n\}$. Elements of theory of linguistic graphs and their applications to graph based encryption reader can find in [29]. Some applications of linguistic graphs of type $(1, 1, n-1)$ are described in [24], [36], [38].

Let us concentrate on linguistic graphs of type $1, 1, m$. Let $N(a, v)$ be the operator of taking neighbour of the vertex $v$ with colour $a \in K$. We refer to sequences $(f_1, f_2, \dots, f_s)$ with $f_1 \in K[x_1]$ of even length s as symbolic strings. On the totality S1,1 (K) of such sequences we consider the product $(f_1, f_2, \dots, f_s)(g_1, g_2, \dots, g_r) = (f_1, f_2, \dots, f_s, g_1(f_s(x_1)), g_2(f_s(x_1)), \dots, g_r(f_s(x_1)))$.

**Proposition 1.** *Elements of $S_{1,1}(K)$ with defined product form a semigroup.*

If $Q$ is an extension of the ground commutative ring $K$ then linguistic graph $I(Q)$ and can be defined via the same set of equations. Let us take $Q = K[x_1, x_2, \dots, x_n]$ and consider infinite linguistic graph $I' = I(K[x_1, x_2, \dots, x_n])$ with partition sets $P'$ and $L'$ isomorphic to variety $K[x_1, x_2, \dots, x_n]^n$. For each symbolic string $(f_1, f_2, \dots, f_s)$ from $S_{1,1}(K)$ and consider the symbolic computation $C(f_1, f_2, \dots, f_s)$ which is a walk in $I'$ with starting point $X = (x_1, x_2, \dots, x_n)$ are generic elements of the commutative ring $K[x_1, x_2, \dots, x_n]$, other elements of the walk are $X_1 = N(f_1, X)$, $X_2 = N(f_2, X_1)$, $\dots$, $X_s = N(f_s, X_{s-1})$. Notice that operators $N(f_i, X_{i-1})$ are computed in the graph $I'$.

It is easy to see that $X_s = (f_s(x_1), g_2(x_1, x_2), \dots, g_n(x_1, x_2, \dots, x_n))$, where $g_i \in K[x_1, x_2, \dots, x_i]$. The rule $(x_1 \to f_s(x_1)$, $x_2 \to g_2(x_1, x_2), \dots, x_n \to g_n(x_1, x_2, \dots, x_n))$ defines the map from $S(K^n)$ into itself. We denote this map as $\Delta I(K)(f_1, f_2, \dots, f_s)$ and refer to it as a map of symbolic computation.

**Proposition 2.** *A map $\Delta I(K)$ from $S_{1,1}(K)$ into $s(K^n)$ sending symbolic string $(f_1, f_2, \dots, f_s)$ to $\Delta I(K)(f_1, f_2, \dots, f_s)$ is a homomorphism of $S_{1,1}(K)$ into $s(K^n)$.*

We refer to the image $PS(I(K))$ of homomorphism of proposition 2 as semigroup of symbolic point to point computations and refer to $\Delta I(K)$ as linguistic compression ($lc$) homomorphism. We define a semigroup $LS(I(K))$ of line-to-line computations via simple change of points for lines in $I$ and $I'$.

**Proposition 3.** *A symplectic homomorphism $\delta$ of linguistic graphs ${}^1I(K)$ and ${}^2I(K)$ of type $(1, 1, n)$ induces canonical*

*homomorphism of $PS({}^1I(K))$ onto $PS({}^2I(K))$.*

Let us consider subsemigroup $\Sigma(K)$ of $S_{1,1}(K)$ generated by symbolic shifting strings of kind $(x_1+a_1, x_1+a_2, \dots, x_1+a_s)$, where $a_i$, $i = 1, 2, \dots, s$ are elements of $K$. We identify tuple $C = (x_1 + a_1, x_1 + a_2, \dots, x_1 + a_s)$ with its code $\langle a_1, a_2, \dots, a_s\rangle$.

**Proposition 4.** *For each linguistic graph $I(K)$ of type $(1, 1, n-1)$ the image $\Sigma(I(K))$ of $\Sigma(K)$ under the linguistic compression homomorphism onto $PS(I(K))$ is a subgroup of affine Cremona group.*

In fact for invertibility of $\delta(f_1, f_2, \dots, f_s) \in PS(I(K))$ the bijectivity of $f_s$ is a sufficient and necessary condition. We refer to $\Sigma(I(K))$ as group of walks on points of linguistic graph $I(K)$.

Let $C = (x_1 + a_1, x_1 + a_2, \dots, x_1 + a_s)$ be a shifting symbolic string from the semigroup $\Sigma(K)$. We refer to $Rev(C) = (x_1 - a_s + a_{s-1}, x_1 - a_s + a_{s-2}, \dots, x_1 - a_s + a_1, x_1 - a_s)$ as revering string for $x$.

**Lemma.** *Let $\Delta = \Delta I(K)$ be linguistic compression map from $S_{1,1}(K)$ onto $PS(I(K))$ and $x \in \Sigma(K)$. Then inverse map for $\Delta(x)$ coincides with $\Delta(Rev(x))$.*

## VI. Stable groups of cubical maps defined in terms of linguistic graphs and their homomorphisms

Let $K$ be a commutative ring. We define $A(n, K)$ as bipartite graph with the point set $P = K^n$ and line set $L = K^n$ (two copies of a Cartesian power of $K$ are used). We will use brackets and parenthesis to distinguish tuples from $P$ and $L$. So $(p) = (p_1, p_2, \dots, p_n) \in P_n$ and $[l] = [l_1, l_2, \dots, l_n] \in L_n$. The incidence relation $I = A(n, K)$ (or corresponding bipartite graph $I$) is given by condition $pIl$ if and only if the equations of the following kind hold

$$p_2 - l_2 = l_1p_1, \quad p_3 - l_3 = p_1l_2, \quad p_4 - l_4 = l_1p_3, \quad p_5 - l_3 = p_1l_4,$$
$$\dots \quad , p_n - l_n = p_1l_{n-1} \text{ for odd } n \text{ and } p_n - l_n = l_1p_{n-1} \text{ for even } n.$$

Let us consider the case of finite commutative ring $K$, $|K| = m$. As it instantly follows from the definition the order of our bipartite graph $A(n, K)$ is $2m^n$. The graph is $m$-regular. In fact the neighbour of given point $p$ is given by above equations, where parameters $p_1, p_2, \dots, p_n$ are fixed elements of the ring and symbols $l_1, l_2, \dots, l_n$ are variables. It is easy to see that the value for $l_1$ could be freely chosen. This choice uniformly establishes values for $l_2, l_3, \dots, l_n$ . So each point has precisely $m$ neighbours. In a similar way, we observe the neighbourhood of the line, which also contains $m$ neighbours. We introduce the colour $\rho(p)$ of the point $p$ and the colour $\rho(l)$ of line $l$ as parameter $p_1$ and $l_1$ respectively.

It means that graphs $A(n, K)$ with colouring $\rho$ belong to the class of $\Gamma$ linguistic graphs of type $(1, 1, n-1)$.

Let $GA(n, K) = \Sigma(A(n, K))$ stands for the group of walks on points of $A(n, K)$. We have a natural homomorphism $GA(n+1, K)$ onto $GA(n, K)$ induced by symplectic homomorphism $\Delta$ from $A(n+1, K)$ onto $A(n, K)$ sending point $(x_1, x_2, \dots, x_n, x_{n+1})$ to $(x_1, x_2, \dots, x_n)$ and line $[x_1, x_2, \dots, x_n, x_{n+1}]$ to $[x_1, x_2, \dots, x_n]$. It means that there is well defined projective limit $A(K)$ of graphs $A(n, K)$ and groups $GA(K)$ of groups $G(n, K)$ when $n$ is growing to infinity. As it stated in [37] case of $K = F_q$, $q > 2$ infinite graph $A(F_q)$ is a tree. Some properties of infinite groups $GA(K)$ of transformation of infinite dimensional affine space over commutative ring $K$ the reader can find in [31].

Other family $D(n, K)$ of linguistic graphs of type $(1, 1, n-1)$ defined over the commutative ring $K$ were defined in [35] but its definition in the case of $K = F_q$ was known earlier. In fact graphs $D(n, q) = D(n, F_q)$ are widely known due to their applications in Extremal Graph Theory, in Theory of LDPC codes and Cryptography. Graphs $D(n, K)$ are bipartite with set of vertices $V = P \cup L, |P \cap L| = 0$. A subset of the vertices $P$ is called the set of points and another subset $L$ is called the set of lines. Let $P$ and $L$ be two copies of Cartesian power $K^n$, where $n \geq 2$ is an integer. Two types of brackets are used in order to distinguish points from lines. It has a set of vertices (collection of points and lines), which are $n$-dimensional vectors over $K$ : $(p) = (p_1, p_2, p_3, p_4, \dots, p_i, p_{i+1}, p_{i+2}, p_{i+3}, \dots, p_n)$, $[l] = [l_1, l_2, l_3, l_4, \dots, l_i, l_{i+1}, l_{i+2}, l_{i+3}, \dots, l_n]$. The point $(p)$ is incident with the line $[l]$, if the following relations between their coordinates hold: $l_2 - p_2 = l_1p_1$, $l_3 - p_3 = l_2p_1$, $l_4 - p_4 = l_1p_2$, $l_i - p_i = l_1p_{i-2}$, $l_{i+1} - p_{i+1} = l_{i-1}p_1$, $l_{i+2} - p_{i+2} = l_ip_1$, $l_{i+3} - p_{i+3} = l_1p_{i+1}$ where $i \geq 5$. Connected component of edge-transitive graph $D(n, q)$ is denoted by $CD(n, q)$ [15]. Notice that all connected components of the natural projective limit $D(q)$ of graphs $D(n, q)$, $n \to \infty$ are $q$-regular trees. Let $D(K)$ stands for the projective limit of graphs $D(n, K)$.

Let us denote as $GD(n, K)$ and $GD(K)$ the groups $\Sigma(D(n, K))$ and $\Sigma(D(K))$ of walks on points of graphs $D(n, K)$ and $D(K)$ respectively. For the description of certain symplectic quotients we will use the alternative description of graphs $D(K)$. It is based on the connections of these graphs with Kac-Moody Lie algebra with extended diagram $A_1$.The vertices of $D(K)$ are infinite dimensional tuples over $K$. We write them in the following way $(p) = (p_{0,1}, p_{1,1}, p_{1,2}, p_{2,1}, p_{2,2}, p'_{2,2}, p_{2,3}, \dots, p_{i,i}, p'_{i,i}, p_{i,i+1}, p_{i+1,i}, \dots)$, $[l] = [l_{1,0}, l_{1,1}, l_{1,2}, l_{2,1}, l_{2,2}, l'_{2,2}, l_{2,3}, \dots, l_{i,i}, l'_{i,i}, l_{i,i+1}, l_{i+1,i}, \dots]$. We assume that almost all components of points and lines are zeros. The condition of incidence of point $(p)$ and line $[l]$ ($(p)I[l]$) can be written via the list of equations below.

$$l_{i,i} - p_{i,i} = l_{1,0}p_{i-1,i}, \quad l'_{i,i} - p'_{i,i} = l_{i,i-1}p_{0,1},$$
$$l_{i,i+1} - p_{i,i+1} = l_{i,i}p_{0,1}, \quad l_{i+1,i} - p_{i+1,i} = l_{1,0}p'_{i,i}.$$

This four relations are defined for $i \geq 1$, ($p'_{1,1} = p_{1,1}$, $l'_{1,1} = l_{1,1}$).

Similarly, we can define the projective limit $A(K)$ of graphs $A(n, K)$, $n > 1$.

We can describe the bipartite infinite graph $A(K)$ on the vertex set consisting on points and lines $(p) = (p_{0,1}, p_{1,1}, p_{1,2}, p_{2,1}, p_{2,2}, p_{2,3}, \dots, p_{i,i}, p_{i,i+1}, \dots)$.

$[l] = [l_{1,0}, l_{1,1}, l_{1,2}, l_{2,1}, l_{2,2}, l_{2,3}, \ldots, l_{i,i}, l_{i,i+1}, \ldots]$ such that point $(p)$ is incident with the line $[l]$ ($(p)I[l]$, if the following relations between their coordinates hold: $l_{i,i} - p_{i,i} = l_{1,0}p_{i-1,i}$, $l_{i,i+1} - p_{i,i+1} = l_{i,i}p_{0,1}$.

It is clear that the set of indices $A = \{(1,0), (0,1), (1,1), (1,2), (2,2), (2,3), \ldots, (i-1,i), (i,i)\}$ is a subset in $D = \{(1,0), (0,1), (1,1), (1,2), (2,2), (2,2)', \ldots, (i-1,i), (i,i-1), (i,i), (i,i)', \ldots\}$. So graph $A(K)$ is a symplectic quotient of linguistic incidence structure $D(K)$. Let us use symbol $\Psi$ for the corresponding symplectic homomorphism. For each positive integer $m \geq 2$ we consider subsets $M = A^m$ and $M = D^m$ containing of first $m-2$ elements of $A' = A - \{(1,0), (0,1)\}$ and $D' = D - \{(1,0), (0,1)\}$ with respect to the above orders and obtain symplectic quotients $I_M$ of $D(K)$ and $A(K)$. One can check that corresponding quotients are isomorphic to graphs $D(m,K)$ and $A(m,K)$. The investigation of pair $A^m, D^m$ leads to following statement [35].

**Proposition 5.** *For each $n \geq 4$ there are a symplectic homomorphisms of $D(2n,K)$ onto $A(m,k)$, $2 \geq m \geq n+1$ and $D(2n+1,K)$ onto $A(m,K)$, $2 \geq m \geq n+2$. Notice that $D(n,K) = A(n,K)$ for $n = 2,3$.*

**Proposition 6.** *Groups $GD(K)$ and $GA(K)$ are stable cubical transformations of infinite-dimensional affine space over a commutative ring $K$. Graph homomorphism of Proposition 5 induces group homomorphism $\Sigma$ of $GD(n,K)$ onto $GA(n,K)$.*

**Corollary.** *$GD(n,K)$ and $GA(n,K)$ are stable cubical subgroups of Cremona group $C(K^n)$.*

### A. Tahoma word cryptosystem

Alice selects commutative ring $K$ and parameters $n$ and $m$ as in Proposition 5. She will prepare data for Affine Tahoma Cryptosystem presented in Section II in the simplest case of $K = Q = R$. She selects strings $C_i = \langle {}^i\alpha_1, {}^i\alpha_2, \ldots, {}^i\alpha_{t(1)} \rangle$, $i = 1,2,\ldots,r$ from $\Sigma(Q)$ and elements $B = \langle \beta_1, \beta_2, \ldots, \beta_s \rangle$ from $\Sigma(K)$ and $D = \langle \gamma_1, \gamma_2, \ldots, \gamma_k \rangle$ from $\Sigma(K)$. Alice computes $Rev(B)$ and $Rev(D)$. She takes affine transformations $T_1 \in AGL_n(K)$ and $T_2$ from $AGL_m(K)$.

Alice forms strings $B_i = Rev(B)C_iB$ and $D_i = Rev(D)Rev(C_i)D$, $i = 1,2,\ldots,r$ in $\Sigma(K)$ and $\Sigma(R)$. She computes images $CB_i$ and $CD_i$ of linguistic compression homomorphism $\Delta^{D(n,K)}$ and $\Delta^{A(m,K)}$ on elements $B_i$ and $D_i$. Finally Alice computes elements $T_1^{-1}CB_iT_1 = G_i$ and $F_i = T_2^{-1}CD_iT_2$ which are elements of affine Cremona groups $C(K^n)$ and $C(R^m)$.

Alice keeps the pairs $(G_i, F_i)$ and computes additionally for herself $H = T_1^{-1}\Delta^{D(n,K)}(Rev(B))$, $H^{-1} = \Delta^{D(n,K)}(B)T_1$ and $Z = T_2^{-1}\Delta^{DA(m,K)}(Rev(D))$, $Z^{-1} = \Delta^{A(m,K)}(D)T_2$. Alice sends pairs $G_i$ and $F_i$ to Bob and correspondents execute steps of the cryptosystem with this data.

The homomorphism $\delta : GD(n,Q) \to GA(m,Q)$ of the diagram is tame, i.e. its image can be computed in polynomial time in variable $n$. The triple $(GD(n,Q), A(m,Q), \delta)$ can be considered as a platform of Tahoma protocol introduced in [27], word tahoma stands for an abbreviation of tame homomorphism.

## VII. Graphs $A(n,q)$ and $D(n,q)$, digital condenced matters physics effect

We can substitute graph $A(n,K)$ for other linguistic graph $L$ of type $(1,1,n-1)$ defined over the commutative ring $K$ and rewrite the content of section VI. We use graphs $A(n,K)$ and well known linguistic graph $D(n,K)$ of this type to implement all algorithm of previous section. Graphs $D(n,K)$ are bipartite with set of vertices $V = P \cup L$, $|P \cap L = 0|$. A subset of the vertices $P$ is called the set of points and another subset $L$ is called the set of lines. Let $P$ and $L$ be two copies of Cartesian power $K^n$, where $n \geq 2$ is an integer. Two types of brackets are used in order to distinguish points from lines. It has a set of vertices (collection of points and lines), which are $n$-dimensional vectors over $K$ : $(p) = (p_1, p_2, p_3, p_4, \ldots, p_i, p_{i+1}, p_{i+2}, p_{i+3}, \ldots, p_n)$, $[l] = [l_1, l_2, l_3, l_4, \ldots, l_i, l_{i+1}, l_{i+2}, l_{i+3}, \ldots, l_n]$. The point $(p)$ is incident with the line $[l]$, if the following relations between their coordinates hold: $l_2 - p_2 = l_1p_1$, $l_3 - p_3 = l_2p_1$, $l_4 - p_4 = l_1p_2$, $l_i - p_i = l_1p_{i-2}$, $l_{i+1} - p_{i+1} = l_{i-1}p_1$, $l_i + 2 - p_{i+2} = l_ip_1$, $l_{i+3} - p_{i+3} = l_1p_{i+1}$ where $i \geq 5$. Connected component of edge-transitive graph $D(n,q)$ is denoted by $CD(n,q)$ [15]. Notice that all connected components of the natural projective limit $D(q)$ of graphs $D(n,q)$, $n \to \infty$ infinite graph $D(q)$ are $q$-regular trees.

Let us denote as $G'(n,K)$ the group of elements of kind $g = \eta(C)$ of *irreducible computation* computation $C = (a_1, a_2, \ldots, a_t)$ in the case of graphs $D(n,K)$.

We present time of generation (in ms) of element $g$ from $G(n,K)$ and $G'(n,K)$ in the cases of graphs $A(n,K)$ and $D(n,K)$ and number $M(g)$ of monomial terms for $g$.

We refer to parameter $t$ as *length of word*. We can see the "condensed matters physics" digital effect. If $t$ is "sufficiently large", then $M(g)$ is independent from $t$ constant $c$. It means that the density of cubical collision map in all algorithm is simply $c$.

We have written a program for generating of elements and for encrypting text using the generated public key. The program is written in C++ and compiled with the gcc compiler. We used an average PC with processor Pentium 3.00 GHz, 2GB memory RAM and system Windows 7. We have implemented three cases:

1) $T$ and $T_1$ are identities,
2) $T$ and $T_1$ are maps of kind $x_1 \to x_1 + a_2x_2 + a_3x_3 + \ldots + a_tx_t, x_2 \to x_2, x_3 \to x_3, \ldots, x_t \to x_t, a_i \neq 0$, $i = 1,2,\ldots,t$ (linear time of computing for $T$ and $T_1$), where $t = n$ and $t = m$, respectively,
3) $T = Ax+b$, $T_1 = A_1x+b_1$; matrices $A$, $A_1$ and vectors $b$, $b_1$ have mostly nonzero elements.

The tables I–II present the number of monomials depending on the number of variables ($n$) and the password length in the second and third case and the family of graphs $A(n,K)$,

where $K$ is a finite field of characteristic 2. The tables III–IV present the time (in milliseconds) of the generation of public key monomials depending on the number of variables n and the length of the word in the second and third case and the family of graphs $A(n,K)$. In [8], [10], [9] the similar program for the case when $K$ is Boolean ring was used for investigation of classical Diffie-Hellman protocol for cyclic group $\langle g\rangle$ and corresponding ElGamal cryptosystem. Currently, we expand this computer package on the case of commutative rings $Z_m$, where $m$ is the power of 2.

TABLE I
NUMBER OF MONOMIAL TERMS OF THE CUBIC MAP INDUCED BY THE GRAPH $A(n,\mathbb{F}_{2^{32}})$, CASE II

| | length of the word | | | | |
|---|---|---|---|---|---|
| $n$ | 16 | 32 | 64 | 128 | 256 |
| 16 | 5623 | 5623 | 5623 | 5623 | 5623 |
| 32 | 53581 | 62252 | 62252 | 62252 | 62252 |
| 64 | 454375 | 680750 | 781087 | 781087 | 781087 |
| 128 | 3607741 | 6237144 | 9519921 | 10826616 | 10826616 |

TABLE II
NUMBER OF MONOMIAL TERMS OF THE CUBIC MAP INDUCED BY THE GRAPH $A(n,\mathbb{F}_{2^{32}})$, CASE III

| | length of the word | | | | |
|---|---|---|---|---|---|
| $n$ | 16 | 32 | 64 | 128 | 256 |
| 16 | 6544 | 6544 | 6544 | 6544 | 6544 |
| 32 | 50720 | 50720 | 50720 | 50720 | 50720 |
| 64 | 399424 | 399424 | 399424 | 399424 | 399424 |
| 128 | 3170432 | 3170432 | 3170432 | 3170432 | 3170432 |

TABLE III
PUBLIC MAP GENERATION TIME (MS), $A(n,\mathbb{F}_{2^{32}})$, CASE II

| | length of the word | | | | |
|---|---|---|---|---|---|
| $n$ | 16 | 32 | 64 | 128 | 256 |
| 16 | 20 | 60 | 128 | 260 | 540 |
| 32 | 308 | 788 | 1776 | 3760 | 7716 |
| 64 | 3193 | 8858 | 23231 | 53196 | 113148 |
| 128 | 54031 | 137201 | 368460 | 950849 | 2164037 |

TABLE IV
PUBLIC MAP GENERATION TIME (MS), $A(n,\mathbb{F}_{2^{32}})$, CASE III

| | length of the word | | | | |
|---|---|---|---|---|---|
| $n$ | 16 | 32 | 64 | 128 | 256 |
| 16 | 76 | 148 | 288 | 576 | 1148 |
| 32 | 1268 | 2420 | 4700 | 9268 | 18405 |
| 64 | 22144 | 40948 | 78551 | 153784 | 304240 |
| 128 | 460200 | 819498 | 1532277 | 2970743 | 5836938 |

## CONCLUSION

We propose Post Quantum Cryptography information security solutions based on the complexity of the following problem Cremona Semigroup Word Decomposition (CSWD).

Thus we hope that introduced algorithms can be considered as serious candidates to be postquantum cryptographical tools. We believe that future studies of cryptanalytics confirm that CSWD problem remains unsolvable on ordinary Turing Machine and Quantum Computer under the condition of stability of platform S. Hope that the idea of an alternative disclosure of hidden homomorphism will attract the attention of cryptanalytics.

Complexity estimates for both correspondents demonstrate the possibility of the current usage of algorithms. Computer simulations demonstrate an interesting phase-transition effect that allows predicting the density of the collision maps of key exchange protocols and their inverse forms. This effect also demonstrates the feasibility of proposed cryptographic schemes. Direct and inverse protocols to elaborate collision multivariate transformation of free module $K^n$ of predictable density can be used together with stream cipher working with data written in alphabet $K$ or passwords written in this alphabet.

Correspondents can use collision maps to add them to part of a password or part of a plaintext or part of a ciphertext. There is an option to deform part of passwords, plaintext and ciphertext by outcomes of inverse protocols.

Reader can find various examples of protocol usage in [29]. Applications of graphs $A(n,K)$ to the development of stream ciphers reader can find in [40], [41].

## REFERENCES


[1] M. Anshel, M. Anshel, and D. Goldfeld. An algebraic method for public-key cryptography. *Math. Res. Lett.*, 6:287–291, 1999.

[2] S. Blackburn and S. Galbraith. Cryptanalysis of two cryptosystems based on group actions. In K. Lam, C. Xing, and E. Okamoto, editors, *Advances in Cryptology – ASIACRYPT '99*, Lecture Notes in Computer Science, pages 52–61. Springer, 1999.

[3] Z. Cao. *New Directions of Modern Cryptography*. CRC Press, 2012.

[4] J. Ding, J. E. Gower, and D. S. Schmidt. *Multivariate Public Key Cryptosystems*. Advances in Information Security. Springer, 2006.

[5] B. Fine, M. Habeeb, D. Kahrobaei, and G. Rosenberger. Aspects of nonabelian group based cryptography: A survey and open problems. arXiv:1103.4093 [cs.CR], 2011. http://arxiv.org/.

[6] L. Goubin, J. Patarin, and B.-Y. Yang. Multivariate cryptography. In *Encyclopedia of Cryptography and Security*, pages 824–828. Springer US, Boston, MA, 2011.

[7] D. Kahrobaei and B. Khan. A non-commutative generalization of elgamal key exchange using polycyclic groups. In *IEEE GLOBECOM 2006 - 2006 Global Telecommunications Conference*, 12 2006.

[8] M. Klisowski. *Zwiększenie bezpieczeństwa kryptograficznych algorytmów wielu zmiennych bazujących na algebraicznej teorii grafów*. PhD thesis, Politechnika Częstochowska, 2015.

[9] M. Klisowski and V. Ustimenko. On the comparison of cryptographical properties of two different families of graphs with large cycle indicator. *Mathematics in Computer Science*, 6(2):181–198, 2012.

[10] M. Klisowski and V. Ustimenko. Graph based cubical multivariate maps and their cryptographical applications. In L. Beshaj, T. Shaska, and E. Zhupa, editors, *Advances on Superelliptic Curves and their Applications*, volume 41 of *NATO Science for Peace and Security Series - D: Information and Communication Security*, pages 305–327. IOS Press, 2015.

[11] K. H. Ko, S. J. Lee, J. H. Cheon, J. W. Han, J.-S. Kang, and C. Park. New public-key cryptosystem using braid groups. In M. Bellare, editor, *Advances in Cryptology — CRYPTO 2000*, pages 166–183, Berlin, Heidelberg, 2000. Springer Berlin Heidelberg.

[12] N. Koblitz. *Algebraic Aspects of Cryptography*. Springer-Verlag, Berlin, Heidelberg, 1998.

[13] P. H. Kropholler, S. J. Pride, W. A. M. Othman, K. B. Wong, and P. C. Wong. Properties of certain semigroups and their potential as platforms for cryptosystems. *Semigroup Forum*, 81(1):172–186, 2010.

[14] G. Kumar and H. Saini. Novel noncommutative cryptography scheme using extra special group. *Security and Communication Networks*, 2017:1–21, 01 2017.

[15] F. Lazebnik, V. A. Ustimenko, and A. J. Woldar. A new series of dense graphs of high girth. *Bull. Amer. Math. Soc.*, 32:73–79, 1995.

[16] J. A. Lopez-Ramos, J. Rosenthal, D. Schipani, and R. Schnyder. Group key management based on semigroup actions. *J. Algebra Appl.*, 16(8), 2017.

[17] G. Maze, C. Monico, and J. Rosenthal. Public key cryptography based on semigroup actions. *Adv. Math. Commun.*, 1(4):489–507, 2007.

[18] R. J. McEliece. A public-key cryptosystem based on algebraic coding theory. *DSN Progress Report*, 44:114–116, Jan 1978.

[19] D. N. Moldovyan and N. A. Moldovyan. A new hard problem over non-commutative finite groups for cryptographic protocols. In I. Kotenko and V. Skormin, editors, *Computer Network Security*, pages 183–194, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg.

[20] A. Myasnikov, V. Shpilrain, and A. Ushakov. *Group-based Cryptography*. Advanced Courses in Mathematics — CRM Barcelona. Springer Basel AG, 2008.

[21] A. Myasnikov, V. Shpilrain, and A. Ushakov. *Non-commutative Cryptography and Complexity of Group-theoretic Problems*. Mathematical surveys and monographs. American Mathematical Society, 2011.

[22] E. Sakalauskas, P. Tvarijonas, and A. Raulynaitis. Key agreement protocol (kap) using conjugacy and discrete logarithm problems in group representation level. *Informatica, Lith. Acad. Sci.*, 18:115–124, 01 2007.

[23] V. Shpilrain and A. Ushakov. The conjugacy search problem in public key cryptography: Unnecessary and insufficient. *Applicable Algebra in Engineering, Communication and Computing*, 17(3):285–289, 2006.

[24] V. Ustimenko. On linguistic dynamical systems, families of graphs of large girth, and cryptography. *J. Math. Sci.*, 140(3):461–471, 2007.

[25] V. Ustimenko. On desynchronised multivariate el gamal algorithm. Cryptology ePrint Archive, Report 2017/712, 2017. https://eprint.iacr.org/2017/712.

[26] V. Ustimenko. On the families of stable multivariate transformations of large order and their cryptographical applications. *Tatra Mt. Math Publ.*, 70:107–117, 2017.

[27] V. Ustimenko. On new symbolic key exchange protocols and cryptosystems based on a hidden tame homomorphism. *Reports of the National Academy of Sciences of Ukraine*, (10):26–36, 2018.

[28] V. Ustimenko. On semigroups of multiplicative cremona transformations and new solutions of post quantum cryptography. Cryptology ePrint Archive, Report 2019/133, 2019. https://eprint.iacr.org/2019/133.

[29] V. Ustimenko and M. Klisowski. On noncommutative cryptography and homomorphism of stable cubical multivariate transformation groups of infinite dimensional affine spaces. Cryptology ePrint Archive, Report 2019/593, 2019. https://eprint.iacr.org/2019/593.

[30] V. Ustimenko and M. Klisowski. On noncommutative cryptography with cubical multivariate maps of predictable density. In K. Arai, R. Bhatia, and S. Kapoor, editors, *Intelligent Computing: Proceedings of the 2019 Computing Conference, Volume 2*, number 998 in Advances in Intelligent Systems and Computing, pages 654–674. Springer, 2019.

[31] V. Ustimenko and U. Romańczuk. On extremal graph theory, explicit algebraic constructions of extremal graphs and corresponding turing encryption machines. In *Artificial Intelligence, Evolutionary Computing and Metaheuristics*, pages 257–285. Springer, 2013.

[32] V. Ustimenko, U. Romańczuk-Polubiec, A. Wróblewska, M. K. Polak, and E. Zhupa. On the constructions of new symmetric ciphers based on nonbijective multivariate maps of prescribed degree. *Secur. Commun. Netw.*, 2019, 2019.

[33] V. Ustimenko. On new results of Extremal Graph Theory and Postquantum Cryptography. International Algebraic Conference "At the End of the Year 2021", December 27-28, 2021 Kyiv, Ukraine ABSTRACTS, p. 29.

[34] V. Ustimenko. On new results on Extremal Graph Theory, Theory of Algebraic Graphs and their applications in Cryptography and Coding Theory. Cryptology ePrint Archive, Report 2022/296, 2022. https://eprint.iacr.org/2022/296.

[35] V. A. Ustimenko. Coordinatization of regular tree and its quotients. In P. Engel and H. Syta, editors, *Voronoĭ's Impact on Modern Science*, number 2 in Proceedings of the institute of mathematics of the national academy of sciences of Ukraine. Institute of Mathematics, National Academy of Sciences of Ukraine, 1998.

[36] V. A. Ustimenko. Graphs with special arcs and cryptography. *Acta Applicandae Mathematicae*, 74, 2002.

[37] V. A. Ustimenko. Maximality of affine group, and hidden graph cryptosystems. *Alg. Dis. Mthm.*, 2005(1):133–150, 2005.

[38] V. A. Ustimenko. On graph-based cryptography and symbolic computations. *Serdica Journal of Computing*, 1(2):131–156, 2007.

[39] N. R. Wagner and M. R. Magyarik. A public key cryptosystem based on the word problem. In *Proceedings of CRYPTO 84 on Advances in Cryptology*, pages 19–36, New York, NY, USA, 1985. Springer-Verlag New York, Inc.

[40] V. Ustimenko, S. Kotorowicz, and U. Romanczuk. On the implementation of stream ciphers based on a new family of algebraic graphs. In M. Ganzha, L. A. Maciaszek, and M. Paprzycki, editors, *Federated Conference on Computer Science and Information Systems, FedCSIS 2011, Szczecin, Poland, 18-21 September 2011, Proceedings*, pages 485–490, 2011.

[41] V. Ustimenko, U. Romanczuk-Polubiec, A. Wróblewska, M. Polak, and E. Zhupa. On the implementation of new symmetric ciphers based on non-bijective multivariate maps. In M. Ganzha, L. A. Maciaszek, and M. Paprzycki, editors, *Proceedings of the 2018 Federated Conference on Computer Science and Information Systems, FedCSIS 2018, Poznań, Poland, September 9-12, 2018*, volume 15 of *Annals of Computer Science and Information Systems*, pages 397–405, 2018.