Expanding graphs of the Extremal Graph Theory and expanded platforms of Post Quantum Cryptography

Vasyl Ustymenko
Maria Curie-Skłodowska University
pl. Marii Curie-Skłodowskiej 1
20-031 Lublin, Poland
Email: vasylustimenko@yahoo.pl

Urszula Romaniczuk-Polubiec
Independent Researcher, Poland
Email: urszula_romanczuk@yahoo.pl

Aneta Wróblewska
Maria Curie-Skłodowska University
pl. Marii Curie-Skłodowskiej 1
20-031 Lublin, Poland
Email: awroblewska@hektor.umcs.lublin.pl

Abstract — Explicit constructions in Extremal Graph Theory give appropriate lower bounds for Turan type problems. In the case of prohibited cycles, the explicit constructions can be used for various problems of Information Security. We observe recent applications of algebraic constructions of regular graphs of large girth and graphs with large cycle indicator to Coding Theory and Cryptography. In particular, we present a new multivariate platforms of postquantum Non-commutative Cryptography defined in graph theoretical terms.

Index Terms — Graphs of large girth, graphs of large cycle indicator, graph based stream ciphers, multivariate cryptography, non-commutative cryptography

I. SOME DEFINITIONS OF EXTREMAL GRAPH THEORY

The missing definitions of graph-theoretical concepts in the case of simple graphs which appears in this paper can be found in [1]. All graphs we consider are simple ones, i.e. undirected without loops and multiple edges. When it is convenient, we shall identify \( \Gamma \) with the corresponding antireflexive binary relation on \( V(\Gamma) \). The girth of a graph \( \Gamma \), denoted by \( g = g(\Gamma) \), is the length of the shortest cycle in \( \Gamma \). The diameter \( d = d(\Gamma) \) of the graph \( \Gamma \) is the maximal length of the shortest path between its two vertices.

Let \( g_x = g_x(\Gamma) \) be the length of the minimal cycle through the vertex \( x \) from the set \( V(\Gamma) \) of vertices in graph \( \Gamma \). We refer to \( \text{Cind}(\Gamma) = \max \{ g_x, x \in V(\Gamma) \} \) as cycle indicator of the graph \( \Gamma \). The family \( \Gamma \) of connected \( k \)-regular graphs of constant degree is a family of small world graphs, if \( d(\Gamma(x)) \leq c \log_k(v(x)) \), for some constant \( c \), \( c > 0 \). Recall that every family of regular graphs \( \Gamma \) of degree \( k \) and increasing order \( v \) is a family of graphs of large girth, if \( g(\Gamma) \geq c \log_k(v) \), for some independent constant \( c \), \( c > 0 \). We refer to the family of regular simple graphs \( \Gamma \) of degree \( k \) and order \( v \), as a family of graphs of large cycle indicator, if \( \text{Cind}(\Gamma) \geq c \log_k(v) \) for some independent constant \( c \), \( c > 0 \).

Notice that for vertex –transitive graph its girth and cycle indicator coincide. Defined above families plays an important role in Extremal Graph Theory, Theory of LDPC codes and Cryptography (see [2] and further references).

II. THE ALGEBRAIC GRAPHS \( A(n, \mathbb{K}) \) AND \( D(n, \mathbb{K}) \), SOME RESULTS AND OPEN QUESTIONS

Below we consider the family of graphs \( A(n, \mathbb{K}) \) and \( D(n, \mathbb{K}) \), respectively where \( n \geq 5 \) is a positive integer and \( \mathbb{K} \) is a commutative ring. In the case of \( \mathbb{K} = \mathbb{F}_q \), we denote \( A(n, q) \) and \( D(n, q) \), respectively. We define these graphs as homomorphic images of infinite bipartite graphs \( \mathbb{A}(\mathbb{K}) \) and \( \mathbb{D}(\mathbb{K}) \) for which partition sets \( P \) and \( L \) formed by two copies of Cartesian power \( \mathbb{K}^3 \), where \( \mathbb{K} \) is the commutative ring and \( \mathbb{N} \) is the set of positive integer numbers. Elements of \( P \) will be called points and those of \( L \) lines. To distinguish points from lines we use parentheses and brackets. If \( x \in V \), then \( (x) \in P \) and \( [x] \in L \). The description is based on the connections of these graphs with Kac-Moody Lie algebra with extended diagram \( A_1 \).

The vertices of \( D(\mathbb{K}) \) are infinite dimensional tuples over \( \mathbb{K} \). We write them in the following way \( p = (p_0, p_1, p_2, p_1, p_2, p'_3, p_2, p_3, \ldots, p_{i-1}, p_i, p_{i+1}, p_{i+1}, \ldots, p_{i+1}, p_{i+1}, p_{i+1}, \ldots) \), \( l = [l_1, l_2, l_3, \ldots, l_i, l_{i+1}, l_{i+1}, l_{i+1}, l_{i+1}, \ldots] \). We assume that almost all components of points and lines are zeros. The condition of incidence of point \( p \) and line \( [l] \), i.e. \( (p) I [l] \), can be written via the list of equations below.

\[
\begin{align*}
I_{i,i} = p_{i+1} - p_{i+1} & = p_{i+1} - p_{i+1} = 0, \\
I_{i,i} = p_{i+1} - p_{i+1} & = p_{i+1} = 0, \\
I_{i,i} = p_{i+1} - p_{i+1} & = p_{i+1}, \\
I_{i,i} = p_{i+1} - p_{i+1} & = p_{i+1}.
\end{align*}
\]

This four relations are defined for \( i \geq 1 \), with \( p_{i+1} = p_{i+1} \), \( l_{i+1} = l_{i+1} \), \( l_{i+1} = l_{i+1} \).

Similarly we define graphs \( A(\mathbb{K}) \) on the vertex set consisting of points and lines \( p = (p_0, p_1, p_1, p_2, p_2, p_3, \ldots, p_{i-1}, p_i, p_{i+1}, \ldots) \), \( l = [l_1, l_2, l_3, l_4, l_5, \ldots, l_i, l_{i+1}, l_{i+1}, l_{i+1}, \ldots] \) such that point \( p \) is incident with the line \( [l] \), i.e. \( (p) I [l] \), if the following relations between their coordinates hold:

\[
\begin{align*}
I_{i,i} = p_{i+1} - p_{i+1} & = p_{i+1}, \\
I_{i,i} = p_{i+1} - p_{i+1} & = p_{i+1}.
\end{align*}
\]
It is clear that the set of indices $A = \{(1, 0); (0, 1); (1, 1); (2, 2); \ldots; (i - 1, i); (i, i); \ldots; \}$ is a subset in $D = \{(1, 0); (0, 1); (1, 2); (2, 2); \ldots; (i - 1, i); (i, i); \ldots; \}$. Points and lines of $D(\mathbb{K})$ are functions from $\mathbb{K}^D(D^{(1, 0)})$ and $\mathbb{K}^{D^{(0, 1)}}$ and their restrictions on $A = \{(1, 0)\}$ and $A = \{(0, 1)\}$ define homomorphism $\Psi$ of graph $D(\mathbb{K})$ onto $A(\mathbb{K})$. For each positive integer $m \geq 2$ we consider subsets $A(m)$ and $D(m)$ containing first $m + 1$ elements of $A$ and $D$ with respect to the above orders. Restrictions of points and lines of $D(m)$ onto $D(m) - \{(1, 0)\}$ and $D(m) - \{(0, 1)\}$ define graph homomorphism $\Delta(m)$ with image denoted as $D(n, \mathbb{K})$. Similarly restrictions of points and lines of $A(m)$ onto $A(m) - \{(1, 0)\}$ and $A(m) - \{(0, 1)\}$ defines homomorphism $\Delta(m)$ of graph $A(\mathbb{K})$ onto graph denoted as $A(m, \mathbb{K})$.

We also consider the map $\Delta(m)$ on vertices of graph $D(m, \mathbb{K})$ sending its point $p \in \mathbb{K}^{D(m) - \{(1, 0)\}}$ to its restriction into $D(m) \cap A - \{(1, 0)\}$ and its line $l \in \mathbb{K}^{D(m) - \{(0, 1)\}}$ to its restriction onto $D(m) \cap A - \{(0, 1)\}$. This map is homomorphism of $D(m, \mathbb{K})$ onto $A(n, \mathbb{K})$, $n = |D(m) \cap A| - 1$. Graph $D(q) = D(F_q)$ is q-regular forest. Its quotients $D(n, \mathbb{Q})$ are edge transitive graphs. So their connected components are isomorphic. Symbol $CD(n, q)$ stands for the graph which is isomorphic to one of such connected components. Family $CD(n, q)$, $n = 2, 3, \ldots$ is a family of large girth for each parameter $q$, $q > 2$ see [3] and further references. The question “Whether or not $CD(n, q)$ is a family of small world graphs?” is still open. Graph $A(q)$, $q > 2$ is a q-regular tree. Graphs $A(n, q)$ are not vertex transitive. They form a family of graphs with large cycle indicator, which is q-regular family of small world graphs [4]. The question “Whether or not $A(n, q)$, $n = 2, 3, \ldots$ is a family of large girth?” is still open. Graphs $CD(n, q)$ and $A(n, q)$ are expanding graphs (see [10], [20], [45], [46]) with spectral gap $q - 2\sqrt{q}$.

Groups $GD(n, \mathbb{K})$ and $GA(n, \mathbb{K})$ of cubical transformations of affine space $\mathbb{K}^n$ associated with graphs $D(n, \mathbb{K})$ and $A(n, \mathbb{K})$ are interesting objects of algebraic transformation group theory because of composition of two maps of degree 3 for vast majority of pairs will have degree 9. Applications of these groups to Symmetric Cryptography are observed in [5], [6], they are used in Multivariate Cryptography (see [7]-[13]). Papers [14],[15], [16] devoted to applications of these groups as so called platforms of Non-commutative Cryptography (see [17]). Cryptographic applications of other graphs are observed in [18].

III. ON LINGUISTIC AND EXTREMAL GRAPHS AND STABLE NONLINEAR SUBGROUPS OF AFFINE CREMONA GROUP

All graphs defined in section 2 belong to class $L$ of linguistic graphs $\Gamma = \Gamma(\mathbb{K})$ of type $(1, 1, n - 1)$, $n \in \mathbb{N}$ or $n = \infty$ defined over commutative ring $\mathbb{K}$ which contains bipartite graphs with the point set $P_0 = \mathbb{K}^n$ and line set $L_0 = \mathbb{K}^n$ such that $(p) = (p_1, p_2, \ldots, p_n) \in P_0$ and $[l] = [l_1, l_2, \ldots, l_n] \in L_0$, form an edge of $\Gamma$ if the following conditions holds
\[
\begin{align*}
&b_1l_2 - 2ap_2 = 2f(p_1, l_1), \\
&b_3l_2 - 3ap_3 = 3f(p_1, p_2, l_1, l_2), \\
&\vdots \\
&\alpha bl_n - \alpha ap_n = \alpha f(p_1, p_2, \ldots, p_{n-1}, l_1, l_2, \ldots, l_n-1),
\end{align*}
\]
where $\alpha$ and $\beta$, $i \geq 2$ are elements of multiplicative group $\mathbb{K}^*$ (see [43] or [44]) and $f$ are multivariate polynomials. We define colours $\rho_i(p)$ and $\rho_i(l)$ of the point $(p)$ and the line $[l]$ as their first coordinates $p_1$ and $l_1$. We introduce well defined the neighbour operator $N(v, u)$ of computing the neighbour of vertex $v$ of colour $a \in \mathbb{K}$ and the colour jump operator $J(v, a)$ sending point or line $v = (v_1, v_2, \ldots, v_n)$ to $u = (a, v_2, v_3, \ldots, v_n)$.

Let $S(\mathbb{K}^n)$ stands for the Cremona semigroup of polynomial transformations of free module $\mathbb{K}^n$ and $C(\mathbb{K}^n)$ be affine Cremona group of invertible elements of $S(\mathbb{K}^n)$ with the polynomial inverse. These algebraic structures are important objects of algebraic geometry. One of the difficult problem is about constructions of families of stable subgroups $G_n$ of $C(\mathbb{K}^n)$ (or semigroup $S_n$ of $S(\mathbb{K}^n)$), i.e. groups of polynomial transformation with maximal degree equals to constant $c$.

Notice that for the majority of pair $f, g \in C(\mathbb{K}^n)$ of degrees $r$ and $s$ their composition has degree $rs$. So this problem is difficult, it has strong cryptographical motivations.

We consider totality $S_t(\mathbb{K})$ of strings of kind $(f_1, f_2, \ldots, f_k)$, where $f_i \in \mathbb{K}[x]$. We will identify polynomial $f$ and the map $x \rightarrow f(x)$ from $S(\mathbb{K})$. The product of two chains $(f_1, f_2, \ldots, f_k)$ and $(g_1, g_2, \ldots, g_l)$ is the chain $(f_1, f_2, \ldots, f_k, g_1 f_k, g_2 f_k, \ldots, g_l f_k)$. Empty string is the unity of semigroup $S(\mathbb{K})$. In fact $S(\mathbb{K})$ is a semidirect product of a free semigroup over the alphabet $\mathbb{K}[x]$ and Cremona semigroup $S(\mathbb{K})$. We refer to $S_t(\mathbb{K})$ as semigroup of polynomial strings. Let $S'_t(\mathbb{K})$ stands for the semigroup of strings of even length from $S(t)(\mathbb{K})$ and $S(\mathbb{K})$ be subsemigroups of strings of even length with coordinates of kind $x + c$, $c \in \mathbb{K}$.

In the case of linguistic graph $\Gamma = \Gamma(\mathbb{K})$ of type $(1, 1, n - 1)$ the path consisting of its vertices $v_0, v_1, v_2, \ldots, v_k$ is uniquely defined by initial vertex $v_0$ and colours $\rho_i(v_j)$, $i = 1, 2, \ldots, k$ of other vertices from the path. We can consider graph $\Gamma' = \Gamma(\mathbb{K}[x_1, x_2, \ldots, x_n])$ defined by the same with $\Gamma$ equations but over the commutative ring $\mathbb{K}[x_1, x_2, \ldots, x_n]$. So the following symbolic computation can be defined. Take the symbolic point $x = (x_1, x_2, \ldots, x_n)$, where $x_i$ are generic variables of $\mathbb{K}[x_1, x_2, \ldots, x_n]$ and polynomial string $C \in S(\mathbb{K})$ which is a tuple of polynomials $f_1, f_2, \ldots, f_k$ from $\mathbb{K}[x_1]$ with even parameter $k$ ($k = x_1$). Form the path of vertices $v_0 = x$ and $\rho_i(v_0) = x_1$, $v_1$ such that $v_1 I v_0$ and $\rho_1(v_1) = f_1(x_1)$, $v_2$ such that $v_2 I v_1$ and $\rho_2(v_2) = f_2(x_1)$, \ldots, $v_k$ such that $v_k I v_{k-1}$ and $\rho_k(v_k) = f_k(x_1)$. We choose parameter $k$ as even number. So $v_k$ is the point from the partition set $\mathbb{K}[x_1, x_2, \ldots, x_n]$ of the graph $\Gamma'$. We notice that the computation of each coordinate of $v_k$ depending on variables $x_1, x_2, \ldots, x_n$ and polynomials
fs, f2, ..., fn needs only arithmetical operations of addition and multiplication. As it follows from the definition of linguistic graph final vertex vk (point) has coordinates (h1(x1), h2(x1, x2), h3(x1, x2, x3), ..., hn(x1, x2, ..., xn)), where h1(x1) = fs1(x1). Let us consider the map \( Γ(H(C)) : x_i → h_i(x_1, x_2, ..., x_n), i = 1, 2, ..., n \), which corresponds to polynomial string C.

**Proposition 1:** The map \( Γ : C \rightarrow Γ(H(C)) \) is a homomorphism of \( St^{l}(K) \) into Cremona semigroup \( S(K^n) \).

More general form of this statement is proven in [20]. We refer to \( Γ \) as the linguistic compression map. If \( K \) is finite then the map converts totality of potentially infinite strings into finite semifinite.

**Theorem 2:** If \( Γ \) is one of graphs \( D(n, K) \) and \( A(n, K) \), then \( Γ^i, Γ(\sum K) \) is stable subgroup of \( C(K^n) \) of degree 3.

We denote \( Γ^i, Γ(\sum K) \) for \( Γ = D(n, K) \) and \( Γ = A(n, K) \) as \( GD(n, K) \) and \( GA(n, K) \). These groups were already used in all cryptographic applications of graphs \( D(n, K) \) and \( A(n, K) \).

**Proposition 3:** Homomorphisms \( δ \) of \( D(n, K) \) onto \( A(m, K) \), \( n \geq m \) described in section 2 induces homomorphism of \( GD(n, K) \) onto \( GA(m, K) \), \( n \geq m \).

**IV. ON LINGUISTIC GRAPHS AND EXPANSIONS OF STABLE NONLINEAR SUBGROUPS OF AFFINE CREMONA GROUP**

Let \( St^{l}(K) \) stands for the semifield of strings of even length from \( St(K) \) and \( \sum K \) be subsemigroups of strings of even length with coordinates of kind \( x + c, c \in K \).

In the case of linguistic graph \( Γ = Γ(K) \) of type \((1, 1, n-1)\) the sequence of even length \( k = 2n \) consisting of initial vertex \( v_0 \) and \( v_1 = J(v_0, a_1), v_2 = N(v_1, b_1), v_3 = J(v_2, a_2), v_4 = N(v_3, b_2), ..., v_{k-3} = J(v_{k-2}, a_{k-2}), v_{k-2} = N(v_{k-1}, b_{k-1}) \) is uniquely defined by initial vertex \( v_0 \), and colours parameter \((a_1, a_2, ..., a_{k-2})\) and \((b_1, b_2, ..., b_{k-1})\). We can consider graph \( Γ' = Γ[K[x_1, x_2, ..., x_n]] \) defined by the same with \( Γ \) equations but over the commutative ring \( K[x_1, x_2, ..., x_n] \).

So the following symbolic computation can be defined. Take the symbolic point \( x = (x_1, x_2, ..., x_n) \), where \( x_i \) are generic variables of \( K[x_1, x_2, ..., x_n] \) and polynomial string \( C \in St^{l}(K) \), which is a tuple of polynomials \( f_1, f_2, ..., f_n \) from \( K[x] \) with even parameter \( k (x = x_1) \). Form the path of vertices \( v_0 = x, v_1 \) such that \( v_1 = J(v_0, f_1(x_1)), v_2 = N(v_1, f_2(x_1)), v_3 = J(v_2, f_3(x_1)), ..., v_{k-1} = J(v_{k-2}, f_{k-1}(x_1)), v_k = N(v_{k-1}, f_k(x_1)) \) and \( ρ(v_k) = f_k(x) \). We choose parameter k as even number. So \( v_k \) is the point from the partition set \( K[x_1, x_2, ..., x_n] \) of the graph \( Γ' \). We notice that the computation of each coordinate of \( v_i \) depending on variables \( x_1, x_2, ..., x_n \) and polynomials \( f_1, f_2, ..., f_n \) needs only arithmetical operations of addition and multiplication. As it follows from the definition of linguistic graph final vertex \( v_k (point) \) has coordinates \((h_1(x_1), h_2(x_1, x_2), h_3(x_1, x_2, x_3), ..., h_n(x_1, x_2, ..., x_n)) \), where \( h_1(x_1) = f_s(x_1) \). Let us consider the map \( Γ(L(C)) : x_i → h_i(x_1, x_2, ..., x_n), i = 1, 2, ..., n \), which corresponds to polynomial string C.

**Proposition 4:** The map \( Γ : C \rightarrow Γ(L(C)) \) is a homomorphism of \( St^{l}(K) \) into Cremona semigroup \( S(K^n) \).

More general form of this statement is proven in [Us pust].

**Theorem 5:** If \( Γ \) is one of graphs \( D(n, K) \) and \( A(n, K) \) then \( Γ^i(\sum K) \) is stable subgroup of \( C(K^n) \) of degree 3.

We denote \( Γ^i(\sum K) \) for \( Γ = D(n, K) \) and \( Γ = A(n, K) \) as \( JD(n, K) \) and \( JA(n, K) \). As it follows from definitions \( JD(n, K) > GD(n, K) \) and \( JA(n, K) > GA(n, K) \).

**Proposition 6:** Homomorphisms \( δ \) of \( D(n, K) \) onto \( A(m, K) \), \( n > m \) described in section 2 induces homomorphism of \( JD(n, K) \) onto \( JA(m, K) \), \( n > m \).

**V. ON CRYPTOGRAPHY BASED ON NEW MULTIVARIATE PLATFORMS OF NON-COMMUTATIVE CRYPTOGRAPHY**

Non-commutative cryptography appeared with attempts to apply Combinatorial group theory to Information Security. If \( G \) is non-commutative group then correspondents can use conjugations of elements involved in protocol, some algorithms of this kind were suggested in [22], [23], [24], [25], where group \( G \) is given with the usage of generators and relations. 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 Non-commutative 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 [26]-[33]). This direction of security research has very rapid development (see [34], [35] and further references in these publications).

One of the earliest applications of a non-commutative algebraic structures for cryptographic purposes was the usage of braid groups to develop cryptographic protocols. Later several other non-commutative 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 Non Commutative and Multivariate Cryptographies. We try to use some abstract schemes in terms of Combinatorial Semi- group Theory for the implementation with platforms which are semigroups and groups of polynomial transformations of free modules \( K^n \) where \( K \) is commutative ring.

The most popular form of Multivariate cryptosystem is the usage of a single very special map \( f \) in a public key mode. First examples were based on families of quadratic bijective transformation \( f_0 \) (see [36], [37], [38]), such choice implies rather fast encryption process.

Some of recent applications of extremal graphs are connected with other aspects of Multivariate cryptography when
some subsemigroup of affine Cremona semigroups of all polynomial transformations is used instead of a single transformation. Notice that the implementation of the idea to use several multivariate generators in its standard form has to overcome essential difficulties. At first glance this idea looks unrealistic one because of com-position 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 $d(r) = \deg(F'')$. Of course in the case of generator in common position not only degree but a density (total number of monomial terms of the map in its standard form) grows exponentially.

So we have to search for special conditions on subsemigroup of affine Cremona group which guarantee the polynomial complexity of procedure to compute the composition of several elements from subsemigroup. Such conditions can define a basis of Noncommutative Multivariate Cryptography. The stability condition on subsemigroup which we discussed above is one of them. Recently we noticed that condition of minimal density is used in [40] and [41] for the construction idea to combine representative of stable group (for example $\eta$ is one of them). Recently we noticed that condition of minimal density (total number of monomial terms of the map in its standard form) grows exponentially.

Extensions of groups $GD(n, \mathbb{K})$ and $GA(n, \mathbb{K})$ to new essentially large groups $JD(n, \mathbb{K})$ and $JA(n, \mathbb{K})$ allows to use new groups and defined above homomorphisms between them for new more secure realisations of Tahoma schemes. Obviously WP problem is harder un the case of generators freely chosen from the larger group.

Other advantage of the implementation of Tahoma cryptosystems with groups $mS(n, \mathbb{K})$ and $mG = JA(n, \mathbb{K})$ and homomorphism $\delta$ of Proposition 6 between them is much faster computation of generator $b_i$ as images of words $w_i$ under $\mu$, $\Gamma = D(m, \mathbb{K})$ and $a_i = \delta(b_i)^{-1}$ in comparison with case of $GD(m, \mathbb{K})$ and $GA(n, \mathbb{K})$. To make comparison fair we have to assume that length of words from $St'(\mathbb{K})$ is fixed. Currenly we are working on detailed complexity estimates and investigation of statistical mixing properties on the base of computer simulation.

VI. CONCLUSION

We present a short survey of our recent algorithms on applications of Extremal Expander Graphs to Cryptography which appear after publication of [2] at memorial Erdos conference and announce the theorem about new explicitly constructed families of stable groups. The main added instruments are

1. usage of non-bijective transformations defined in terms of algebraic graphs for the constructions of new stream ciphers and public key cryptosystems,
2. usage of compositions of stable transformation of affine space $\mathbb{K}^n$ and transformation of minimal possible density $(n)$,
3. work on the bridge between Multivariate Cryptography and Non-commutative Cryptography, modification of schemes of protocols and El Gamal cryptosystems for platforms of elements of affine Cremona semigroup, search for feasibility conditions,
4. constructions of new graph based stable groups and semigroups.

REFERENCES


