Position Papers of the Federated Conference on Computer Science and Information Systems pp. 41–46
DOI: 10.15439/2019F343
ISSN 2300-5963 ACSIS, Vol. 19

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 Romańczuk-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 Γ with the corresponding antireflexive binary relation on $V(\Gamma)$, i.e. $E(\Gamma)$ is a subset of $V(\Gamma)\times V(\Gamma)$. The *girth* of a graph Γ, denoted by $g=g(\Gamma)$, is the length of the shortest cycle in Γ. The *diameter* $d=d(\Gamma)$ of the graph Γ is the maximal length of the shortest pass 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 Γ. We refer to $Cind(\Gamma)=max\{g_x,\ x\in V(\Gamma)\}$ as *cycle indicator* of the graph Γ. The family Γ_i of connected k-regular graphs of constant degree is a *family of small world graphs*, if $d(\Gamma_i)\leq c\log_k(v_i)$, for some constant c, $c>0$. Recall that family of regular graphs Γ_i of degree k and increasing order v_i is a *family of graphs of large girth*, if $g(\Gamma_i)\geq c\log_k(v_i)$, for some independent constant c, $c>0$. We refer to the family of regular simple graphs Γ_i of degree k and order v_i as a *family of graphs of large cycle indicator*, if $Cind(\Gamma_i)\geq c\log_k(v_i)$ 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 $n>5$ 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 $A(\mathbb{K})$ and $D(\mathbb{K})$ for which partition sets P and L formed by two copies of Cartesian power $\mathbb{K}^{\mathbb{N}}$, 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 $(p)=(p_{0,1},p_{1,1},p_{1,2},p_{2,1},p_{2,2},p'_{2,2},p_{2,3},\dots,p_{i,i},p'_{i,i},p_{i,i+1},p_{i+1,i},\dots)$, $[l]=[l_{1,0},l_{1,1},l_{1,2},l_{2,1},l_{2,2},l'_{2,2},l_{2,3},\dots,l_{i,i},l'_{i,i},l_{i,i+1},l_{i+1,i},\dots]$. We assume that almost all components of points and lines are zeros. The condition of incidence of point (p) and line $[l]$, i.e. $(p)\ I\ [l]$, can be written via the list of equations below.

$$\begin{cases} l_{i,i}-p_{i,i}=l_{1,0}p_{i-1,i},\\ l'_{i,i}-p'_{i,i}=p_{0,1}l_{i,i-1},\\ l_{i,i+1}-p_{i,i+1}=p_{0,1}l_{i,i},\\ l_{i+1,i}-p_{i+1,i}=l_{1,0}p'_{i,i}. \end{cases} \quad (1)$$

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

Similarly we define graphs $A(\mathbb{K})$ on the vertex set consisting of points and lines $(p)=(p_{0,1},p_{1,1},p_{1,2},p_{1,2},p_{2,2},p_{2,3},\dots,p_{i,i},p_{i,i+1},\dots)$, $[l]=[l_{1,0},l_{1,1},l_{1,2},l_{2,1},l_{2,2},l_{2,3},\dots,l_{i,i},l_{i,i+1},\dots]$ such that point (p) is incident with the line $[l]$, i.e. $(p)\ I\ [l]$, if the following relations between their coordinates hold:

$$\begin{cases} l_{i,i}-p_{i,i}=l_{1,0}p_{i-1,i},\\ l_{i,i+1}-p_{i,i+1}=p_{0,1}l_{i,i}. \end{cases} \quad (2)$$

It is clear that the set of indices $A = \{(1,0);\ (0,1);\ (1,1);\ (1,2);\ (2,2);\ (2,3);\ \dots,\ (i-1,i);\ (i,i);\ \dots\}$ is a subset in $D = \{(1,0);\ (0,1);\ (1,1);\ (1,2);\ (2,2);\ (2,2)';\ \dots;\ (i-1,i);\ (i,i-1);\ (i,i);\ (i,i)';\ \dots\}$. Points and lines of $D(\mathbb{K})$ are functions from $\mathbb{K}^{D-\{(1,0)\}}$ and $\mathbb{K}^{D-\{(0,1)\}}$ and their restrictions on $A-\{(1,0)\}$ and $A-\{(0,1)\}$ define homomorphism Ψ 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 $D(\mathbb{K})$ onto $D(m)-\{(1,0)\}$ and $D(m)-\{(0,1)\}$ define graph homomorphism ${}^{D}\Delta(m)$ with image denoted as $D(n,\mathbb{K})$. Similarly restrictions of points and lines of $A(\mathbb{K})$ onto $A(m)-\{(1,0)\}$ and $A(m)-\{(0,1)\}$ defines homomorphism ${}^{A}\Delta(m)$ 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 $[l] \in K^{|D(m)-\{(0,1)\}|}$ 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 $D(q) = D(\mathbb{F}_q)$ is q-regular forest. Its quotients $D(n,q)$ 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 $CD(n,q)$, $n = 2,3,\dots$ 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 $A(n,q)$, $n = 2,3,\dots$ 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 $P_n = \mathbb{K}^n$ and line set $L_n = \mathbb{K}^n$ such that $(p) = (p_1,p_2,\dots,p_n) \in P_n$ and $[l] = [l_1,l_2,\dots,l_n] \in L_n$ form an edge of Γ if the following conditions holds

$$\begin{cases} {}^{2}bl_2 - {}^{2}ap_2 = {}^{2}f(p_1,l_1), \\ {}^{3}bl_3 - {}^{3}ap_3 = {}^{3}f(p_1,p_2,l_1,l_2), \\ \vdots \\ {}^{n}bl_n - {}^{n}ap_n = {}^{n}f(p_1,p_2,\dots,p_{n-1},l_1,l_2,\dots,l_{n-1}), \end{cases} \tag{3}$$

where ${}^{i}a$ and ${}^{i}b$, $i \geq 2$ are elements of multiplicative group $\mathbb{K}^*$ (see [43] or [44]) and ${}^{i}f$ are multivariate polynomials. We define colours $\rho((p))$ and $\rho([l])$ of the point (p) and the line $[l]$ as their first coordinates p_1 and l_1. We introduce well defined the *neighbour operator* $N(v,a)$ 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 $v = (v_1,v_2,\dots,v_n)$ to $u = (a,v_2,v_3,\dots,v_n)$.

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 $St(\mathbb{K})$ of strings of kind $(f_1,f_2,\dots,f_k)$, where $f_i \in \mathbb{K}[x]$. We will identify polynomial f and the map $x \to f(x)$ from $S(\mathbb{K})$. The product of two chains $(f_1,f_2,\dots,f_k)$ and $(g_1,g_2,\dots,g_t)$ is the chain $(f_1,f_2,\dots,f_k,g_1(f_k),g_2(f_k),\dots,g_t(f_k))$. Empty string is the unity of semigroup $St(\mathbb{K})$. In fact $St(\mathbb{K})$ is a semidirect product of a free semigroup over the alphabet $\mathbb{K}[x]$ and Cremona semigroup $S(\mathbb{K})$. We refer to $St(\mathbb{K})$ as semigroup of polynomial strings. Let $St'(\mathbb{K})$ stands for the semigroup of strings of even length from $St(\mathbb{K})$ and $\sum(\mathbb{K})$ 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 $v_0,v_1,v_2,\dots,v_k$ is uniquely defined by initial vertex v_0, and colours $\rho(v_i)$, $i = 1,2,\dots,k$ of other vertices from the path. We can consider graph $\Gamma' = \Gamma(\mathbb{K}[x_1,x_2,\dots,x_n])$ defined by the same with Γ equations but over the commutative ring $\mathbb{K}[x_1,x_2,\dots,x_n]$. So the following symbolic computation can be defined. Take the symbolic point $x = (x_1,x_2,\dots x_n)$, where x_i are generic variables of $\mathbb{K}[x_1,x_2,\dots,x_n]$ and polynomial string $C \in St'(\mathbb{K})$ which is a tuple of polynomials $f_1,f_2,\dots,f_k$ from $\mathbb{K}[x_1]$ with even parameter k ($x = x_1$). Form the path of vertices $v_0 = x$ and $\rho(v_0) = x_1$, v_1 such that $v_1\, I\, v_0$ and $\rho(v_1) = f_1(x_1)$, v_2 such that $v_2\, I\, v_1$ and $\rho(v_2) = f_2(x_1)$, ..., v_k such that $v_k\, I\, v_{k-1}$ and $\rho(v_k) = f_k(x_1)$. We choose parameter k as even number. So v_k is the point from the partition set $\mathbb{K}[x_1,x_2,\dots,x_n]$ 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_k needs only arithmetical operations of addition and multiplication. As it follows from the definition of linguistic graph final vertex v_k (point) has coordinates $(h_1(x_1), h_2(x_1,x_2), h_3(x_1,x_2,x_3),\ldots, h_n(x_1,x_2,\ldots,x_n))$, where $h_1(x_1) = f_k(x_1)$. Let us consider the map ${}^{\Gamma}H(C) : x_i \to h_i(x_1,x_2,\ldots,x_n)$, $i = 1,2,\ldots,n$, which corresponds to polynomial string C.

Proposition 1: The map ${}^{\Gamma}\eta : C \to {}^{\Gamma}H(C)$ is a homomorphism of $St'(\mathbb{K})$ into Cremona semigroup $S(\mathbb{K}^n)$.

More general form of this statement is proven in [20]. We refer to ${}^{\Gamma}\eta$ as the *linguistic compression map*. If $\mathbb{K}$ is finite then the map converts totality of potentially infinite strings into finite semigroup.

Theorem 2: If Γ is one of graphs $D(n,\mathbb{K})$ and $A(n,\mathbb{K})$, then ${}^{\Gamma}\eta(\sum(\mathbb{K}))$ is stable subgroup of $C(\mathbb{K}^n)$ of degree 3.

We denote ${}^{\Gamma}\eta(\sum(\mathbb{K}))$ for $\Gamma = D(n,\mathbb{K})$ and $\Gamma = A(n,\mathbb{K})$ as $GD(n,\mathbb{K})$ and $GA(n,\mathbb{K})$. These groups were already used in all cryptographical applications of graphs $D(n,\mathbb{K})$ and $A(n,\mathbb{K})$.

Proposition 3: Homomorphisms δ of $D(n,\mathbb{K})$ onto $A(m,\mathbb{K})$, $n > m$ described in section 2 induces homomorphism of $GD(n,\mathbb{K})$ onto $GA(m,\mathbb{K})$, $n > m$.

IV. On linguistic graphs and expansions of stable nonlinear subgroups of affine Cremona group

Let $St'(\mathbb{K})$ stands for the semigroup of strings of even length from $St(\mathbb{K})$ and $\sum(\mathbb{K})$ 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 sequence of even length $k = 2r$ consisting of initial vertex v_0 and $v_1 = J(v_0,a_1)$, $v_2 = N(v_1,b_1)$, $v_3 = J(v_2,a_2)$, $v_4 = N(v_3,b_2)$, ..., $v_{k-1} = J(v_{k-2},a_r)$, $v_k = N(v_{k-1},b_r)$ is uniquely defined by initial vertex v_0, and colours parameter $(a_1,a_2,\ldots,a_r)$ and $(b_1,b_2,\ldots,b_r)$. We can consider graph $\Gamma' = \Gamma(\mathbb{K}[x_1,x_2,\ldots,x_n])$ defined by the same with Γ 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 $C \in St'(\mathbb{K})$, which is a tuple of polynomials f_1, f_2, ..., f_k from $\mathbb{K}[x_1]$ with even parameter k ($x = x_1$). Form the path of vertices $v_0 = x$, v_1 such that $v_1 = J(v_0,f_1(x_1))$, $v_2 = N(v_1,f_2(x_1))$, $v_3 = J(v_2,f_3(x_1))$, $v_4 = N(v_3,f_4(x_1))$, ..., $v_{k-1} = J(v_{k-2},f_{k-1}(x_1))$, $v_k = N(v_{k-1},f_k(x_1))$ and $\rho(v_2) = f_2(x_1)$. 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 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_k needs only arithmetical operations of addition and multiplication. As it follows from the definition of linguistic graph final vertex v_k (point) has coordinates $(h_1(x_1), h_2(x_1,x_2), h_3(x_1,x_2,x_3), \ldots, h_n(x_1,x_2,\ldots,x_n))$, where $h_1(x_1) = f_k(x_1)$. Let us consider the map ${}^{\Gamma}L(C) : x_i \to h_i(x_1,x_2,\ldots,x_n)$, $i = 1,2,\ldots,n$, which corresponds to polynomial string C.

Proposition 4: The map ${}^{\Gamma}\mu : C \to {}^{\Gamma}L(C)$ is a homomorphism of $St'(\mathbb{K})$ into Cremona semigroup $S(\mathbb{K}^n)$.

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

Theorem 5: If Γ is one of graphs $D(n,\mathbb{K})$ and $A(n,\mathbb{K})$ then ${}^{\Gamma}\mu(\sum(\mathbb{K}))$ is stable subgroup of $C(\mathbb{K}^n)$ of degree 3.

We denote ${}^{\Gamma}\mu(\sum(\mathbb{K}))$ for $\Gamma = D(n,\mathbb{K})$ and $\Gamma = A(n,\mathbb{K})$ as $JD(n,\mathbb{K})$ and $JA(n,\mathbb{K})$. As it follows from definitions $JD(n,\mathbb{K}) > GD(n,\mathbb{K})$ and $JA(n,\mathbb{K}) > GA(n,\mathbb{K})$.

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

V. On cryptosystems 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 noncom-mutative 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 Semigroup Theory for the implementation with platforms which are semigroups and groups of polynomial transformations of free modules $\mathbb{K}^n$ where $\mathbb{K}$ 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_n (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 semigroup 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 as 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 $d(r) = deg(F^r)$. 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 forms) 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 possible density (each f_i in standard form has density 1) also guarantee efficiency of computations (see [19]). The idea to combine representative of stable group (for example $GD(n, \mathbb{K})$ or $GA(n, \mathbb{K})$) and non-bijective transformation of minimal density is used in [40] and [41] for the construction of new postquantum cryptosystems.

The abstract schemes of Nonlinear Cryptography has to be modified to work with stable subsemigrouos or subsemigroups of minimal density. The following TAHOMA CRYPTOSYSTEM on stable transformations were suggested in [15].

Let $\mathbb{K}$ be a commutative ring, stable subgroups ${}^nG$ of $S(\mathbb{K}^n)$ act naturally on Kn and ${}^mS(n, \mathbb{K})$ be a subgroup of $S(\mathbb{K}^m)$ such that there is a tame homo-morphisn $\Delta = \Delta(m, n)$ of ${}^mS(n, \mathbb{K})$ onto ${}^nG$. We assume that $m = m(n)$ where $m > n$. Alice takes b_1, b_2, ..., b_s, $s > 1$ from ${}^mS(n, \mathbb{K})$ and a_1, a_2, ..., a_s, where $a_i = \Delta(b_i)^{-1}$. She takes $g \in C(\mathbb{Q}^m)$ and $h \in C(\mathbb{T}^n)$ where $\mathbb{Q}$ and $\mathbb{T}$ are extensions of the commutative ring $\mathbb{K}$ 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 $< g', {}^m S(n, \mathbb{K}) >$ generated by g' and elements of ${}^mS(n, \mathbb{K})$ and group $< h', G >$ are stable semigroups of degree d and $T \in AGL_n(\mathbb{T}), T' \in AGL_m(\mathbb{Q})$.

As in the previous algorithm Bob writes the word $w(z_1, z_2, \ldots, z_s)$ in the alphabet z_1, z_2, ..., 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 $\mathbb{T}^n$ 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 [21]). Let ${}^nTC(\mathbb{K}, \mathbb{T}, \mathbb{Q})$ stand for Tahoma cryptosystem as above.

Paper [16] is devoted to implementations of Affine Tahoma scheme with platforms of cubical stable groups $GD(n, q)$ and $GA(n, q)$. They were defined via families of linguistic graphs which form projective limits and the standard homomorphisms between two members of this sequences. So we have pairs (G_n, Δ_n), where $G_n < S(\mathbb{K}^n)$, Δ_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.

The article [42] is devoted to another computer experiment with the new platform which uses the same groups G_n but different tame homomorphisms η_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 option to vary tame homomorphisms in the chosen sequence of semigroup makes the task of cryptanalytic much more difficult.

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 homomorphism 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 implememtation of Tahoma cryptosystems with groups ${}^m S(m, \mathbb{K}) = JD(m, \mathbb{K})$ and ${}^n G = JA(n, \mathbb{K})$ and homomorphism δ of Proposition 6 between them is much faster computation of generator b_i as images of words w_i under ${}^\Gamma\mu$, $\Gamma = D(m, \mathbb{K})$ 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

[1] B. Bollobas, *Extremal graph theory*, Academic Press, London, 1978.

[2] M. Polak, U. Romańczuk, V. Ustimenko and A. Wróblewska, "On the applications of Extremal Graph Theory to Coding Theory and Cryptography", *Electronic Notes in Discrete Mathema Discrete Mathematics*, N 43, 2013, p. 329-342. DOI: https://doi.org/10.1016/j.endm.2013.07.051

[3] F. Lazebnik, V. Ustimenko and A. J.Woldar, "A new series of dense graphs of high girth", *Bulletin of the American Mathematical Society* (N.S.) 32, no. 1, 1995, pp. 73-79

[4] V. Ustimenko, "On extremal graph theory and symbolic computations", *Dopovidi National Academy of Sciences of Ukraine*, , N2, 2013, pp. 42-49.

[5] V. Ustimenko, U. Romańczuk-Polubiec, A. Wróblewska, M. Polak and E. Zhupa, "On the implementation of new symmetric ciphers based on non-bijective multivariate maps", *Proceedings of the 2018 Federated Conference on Computer Science and Information Systems*, M.Ganzha, L. Maciaszek, M. Paprzycki (eds). ACSIS, Vol. 15, 2018, pp. 397-405 DOI: http://dx.doi.org/10.15439/2018F204

[6] V. Ustimenko, U. Romańczuk-Polubiec, A. Wróblewska, M. Polak and E. Zhupa, "On the constructions of new symmetric ciphers based on non-bijective multivariate maps of prescribed degree", *Security and Communication Networks*, Volume 2019, Article ID 2137561, 15 pages. DOI: https://doi.org/10.1155/2019/2137561

[7] M. Klisowski and V. Ustimenko, "Graph based cubical multivariate maps and their crypto-graphical applications", *Advances on Superelliptic curves and their Applications, IOS Press, NATO Science for Peace and Security series -D: Information and Communication Security*, vol 41, 2014, pp. 305 -327.

[8] U. Romańczuk-Polubiec and V. Ustimenko, "On Multivariate Cryptosystems Based on Polynomially Compressed Maps with Invertible Decompositions", *Cryptography and Security Systems, Third International Conference, CSS 2014, Lublin, Poland, September 22-24, 2014. Proceedings, Communications in Computer and Information Science*, 448, 2014, pp. 23-37. DOI: https://doi.org/10.1007/978-3-662-44893-9_3

[9] U. Romańczuk-Polubiec and V. Ustimenko, "On two windows multivariate cryptosystem depending on random parameters", *Algebra and Discrete Mathematics*, Volume 19, Number 1, 2015, pp. 101-129.

[10] U. Romańczuk and V. Ustimenko, "On Families of Graphs of Large Cycle Indicator, Matrices of Large Order and Key Exchange Protocols With Nonlinear Polynomial Maps of Small Degree", *Mathematics in Computer Science*, June 2012, Volume 6, Issue 2, pp 167-180, DOI: https://doi.org/10.1007/s11786-012-0115-8

[11] U. Romańczuk-Polubiec and V. Ustimenko, "On new key exchange multivariate protocols based on pseudorandom walks on incidence structures", *Dopovidi National Academy of Sciences of Ukraine*, No. 1, 2015, pp 41-49. DOI: https://doi.org/10.15407/dopovidi2015.01.041

[12] V. Ustimenko, "On algebraic graph theory and non-bijective maps in cryptography", *Algebra and Discrete Mathematics*, Volume 20, Number 1, 2015, pp. 152-170.

[13] V. Ustimenko, "Explicit constructions of extremal graphs and new multivariate cryptosystems", *Studia Scientarium Mathematicarium Hungarica* (Proceedings of Central. European Conference on Cryptology 2014, Budapest), vol 52, issue 2, June 2015, pp 185-204. DOI: https://doi.org/10.1556/012.2015.52.2.1312

[14] V. Ustimenko, "On the families of stable transformations of large order and their crypto-graphical applications", *Tatra Mt. Math. Publ.*, 70, 2017, pp. 107-117. DOI: https://doi.org/10.1515/tmmp-2017-0021

[15] V. Ustimenko, "On new symbolic key exchange protocols and cryptosystems based on hidden tame homomorphism", *Dopovidi National Academy of Sciences of Ukraine*, N. 10, 2018, pp. 26-36. DOI: https://doi.org/10.15407/dopovidi2018.10.026

[16] V. Ustimenko and M. Klisowski, "On Noncommutative Cryptography with cubical multiva-riate maps of predictable density", *Proceedings of "Computing 2019" conference, London, 16-17, July*, In: Arai K., Bhatia R., Kapoor S. (eds) Intelligent Computing. CompCom 2019. Advances in Intelligent Systems and Computing, vol 998. Springer, Cham. pp. 654-674. DOI: https://doi.org/10.1007/978-3-030-22868-2_47

[17] A. G. Myasnikov, V. Shpilrain and Alexander Ushakov, *Noncommutative Cryptography and Complexity of Group-theoretic Problems*, Mathematical Surveys and Monographs, American Mathematical Society, Volume 177, 2011. DOI: http://dx.doi.org/10.1090/surv/177

[18] P.L.K. Priyadarsini, "A Survey on some Applications of Graph Theory in Cryptography", *Journal of Discrete Mathematical Sciences and Cryptography*, 18:3, 2015, pp. 209-217. DOI: https://doi.org/10.1080/09720529.2013.878819

[19] V. Ustimenko, "On semigroups of multiplicative Cremona transformations and new solutions of Post Quantum Cryptography", *Cryptology ePrint Archive*, 133, 2019.

[20] O.S. Pustovit and V.O Ustimenko, "A new stream algorithms generating sensetive digests of digital documents", *Mathematical modelling in economics* (to appear).

[21] V. Ustimenko, "On desynchronised multivariate algorithms of El Gamal type for stable semigroups of affine Cremona group", *Theoretical and Applied Cybersecurity*, section: theoretical and cryptographic problems of cybersecurity , NTTU KPI, Kyiv, Vol. 1, No. 1, 2019, pp. 22-30.

[22] D. N. Moldovyan and N. A. Moldovyan, "A New Hard Problem over Non-commutative Finite Groups for Cryptographic Protocols", *International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security*, MMM-ACNS 2010: Computer Network Security pp. 183-194. DOI: https://doi.org/10.1007/978-3-642-14706-7_14

[23] L. Sakalauskas and P. Tvarijonas, "A. Raulynaitis, Key Agreement Protocol (KAP) Using Conjugacy and Discrete Logarithm Problema in Group Representation Level", *INFORMATICA*, 2007, Vol. 18, No. 1, pp. 115-124

[24] V. Shpilrain and A. Ushakov, "The conjugacy search problem in public key cryptography: unnecessary and insufficient", *Applicable Algebra in Engineering, Communication and Computing*, August 2006, Volume 17, Issue 3-4, pp. 285-289. DOI: https://doi.org/10.1007/s00200-006-0009-6

[25] D. Kahrobaei and B. Khan, "A non-commutative generalization of ElGamal key exchange using polycyclic groups", *In IEEE GLOBECOM 2006 - 2006 Global Telecommunications Conference* [4150920]. DOI: https://doi.org/10.1109/GLOCOM.2006.290

[26] A. Myasnikov, V. Shpilrain and A. Ushakov, *Group-based Cryptography*, Advanced Courses in Mathematics - CRM Barcelona, Birkhäuser Basel, XV, p. 183, 2008. DOI: https://doi.org/10.1007/978-3-7643-8827-0

[27] Zhenfu Cao, "New Directions of Modern Cryptography", *Boca Raton: CRC Press, Taylor & Francis Group*, 2012, ISBN 978-1-4665-0140-9.

[28] B. Fine, et. al. "Aspects of Non abelian Group Based Cryptography: A Survey and Open Problems". *ArXiv*:1103.4093.

[29] I. Anshel, M. Anshel, D. Goldfeld, "An algebraic method for public-key cryptography", *Mathematical Research Letters*, 1999, 6(3-4), pp. 287-291.

[30] S. R. Blackburn and S. D. Galbraith, "Cryptanalysis of two cryptosystems based on group actions", In: Advances in Cryptology-ASIACRYPT '99. *Lecture Notes in Computer Science*, Springer, Berlin, 1999, vol. 1716, pp. 52-61.

[31] C. Ko, K.H., Lee, S.J., Cheon, J.H., Han, J.W., Kang, J.S. and Park, C., "New public-key cryptosystem using braid groups", In: Advances in Cryptology-CRYPTO 2000, Santa Barbara, CA. *Lecture Notes in Computer Science*, Springer, Berlin, 2000, vol. 1880, pp. 166-83. DOI: https://doi.org/10.1007/3-540-44598-6_10

[32] G. Maze, C. Monico, J. Rosenthal, "Public key cryptography based on semigroup actions", *Advances in Mathematics of Communications*, 2007, 1(4), pp. 489-507. DOI: https://doi.org/10.3934/amc.2007.1.489

[33] 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*, 2010, Vol. 81, pp. 172-186. DOI: https://doi.org/10.1007/s00233-010-9248-8

[34] J. A. Lopez Ramos, J. Rosenthal, D. Schipani and R. Schnyder, "Group key management based on semigroup actions", Journal of Algebra and its applications, vol.16, No. 8, 2017. DOI: https://doi.org/10.1142/S0219498817501481

[35] G. Kumar and H. Saini, "Novel Noncommutative Cryptography Scheme Using Extra Special Group", Security and Communication Networks ,Volume 2017, Article ID 9036382, 21 pages. DOI: https://doi.org/10.1155/2017/9036382

[36] J. Ding., J. E. Gower and D. S. Schmidt, *Multivariate Public Key Cryptosystems*, Advances in Information Security, Springer, p. 260 v. 25, 2006. DOI: https://doi.org/10.1007/978-0-387-36946-4

[37] N. Koblitz, *Algebraic aspects of cryptography*, Springer, Berlin, Heidelberg, 1998. DOI: https://doi.org/10.1007/978-3-662-03642-6

[38] L. Goubin, J.Patarin, Bo-Yin Yang, *Multivariate Cryptography*, In: van Tilborg H.C.A., Jajodia S. (eds) Encyclopedia of Cryptography and Security. Springer, Boston, MA, (2nd Ed.), 2011, pp. 824-828. DOI: https://doi.org/10.1007/978-1-4419-5906-5

[39] R. Wagner, M. R. Magyarik, "A Public-Key Cryptosystem Based on the Word N Problem", *Advances in Cryptology*, Proceedings of CRYPTO

'84, Santa Barbara, California, USA, August 19-22, 1984. DOI: https://doi.org/10.1007/3-540-39568-7_3

[40] V. Ustimenko, "On new multivariate cryptosystems based on hidden Eulerian equations", *Reports of Nath Acad of Sci, Ukraine*, 2017. No. 5, pp 17-24. DOI: https://doi.org/10.15407/dopovidi2017.05.017

[41] V. Ustimenko, "On new multivariate cryptosystems based on hidden Eulerian equations over finite fields", *Cryptology ePrint Archive*, 093, 2017. 111

[42] V. Ustimenko and M. Klisowski, "On Noncommutative Cryptography and homomorphism of stable cubical multivariate transformation groups of infinite dimensional affine spaces", *Cryptology ePrint Archive*, 593, 2019.

[43] V. Ustimenko, "Maximality of affine group, hidden graph cryptosystem and graph's stream ciphers", *Journal of Algebra and Discrete Mathematics*, 2004, v.10, pp. 51-65.

[44] V. Ustimenko, "Linguistic Dynamical Systems, Graphs of Large Girth and Cryptography", *Journal of Mathematical Sciences*, Springer, Vol.140, N3, 2007, pp. 412-434. DOI: https://doi.org/10.1007/s10958-007-0453-2

[45] V. Ustimenko, "Graphs with Special Arcs and Cryptography", *Acta Applicandae Mathematica*, November 2002, Volume 74, Issue 2, pp. 117-153 DOI: https://doi.org/10.1023/A:1020686216463

[46] A. Lubotzky, R. Phillips and P. Sarnak, "Ramanujan graphs", *Combinatorica*, September 1988, Volume 8, Issue 3, pp. 261-277, DOI: https://doi.org/10.1007/BF02126799