On fast computations of numerical parameters of homogeneous algebraic graphs of large girth and small diameter and encryption of large files.

Tymoteusz Chojecki
Institute of Mathematics,
University of Maria Curie-Sklodowska, Poland
Email: tymoteusz.chojecki@umcs.pl

Vasyl Ustimenko
Institute of Mathematics,
University of Maria Curie-Sklodowska, Poland
University of London (Royal Holloway), UK
Institute of Telecommunications and Global Information Space,
Kyiv, Ukraine
Email: vasylustimenko@yahoo.pl

***Abstract*—The paper is dedicated to computer evaluation of parameters of members of family $A(n, F_q)$, $n \geq 2$ of small world algebraic graphs of large girth with well defined projective limit. We present the applications of these computations to some optimisation problems for algebraic graphs over various field and Cryptography. We show the impact of high girth property of known family of graphs $A(n, F_q)$ on properties of fast stream ciphers based on these graphs. Finally we modify these symmrtric encryption algorithms to make them resistant to linearization attacks.**

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

I. Introduction

Let k be a natural number ≥ 2. The problem of approximation of a 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. Solutions of this problem can be used in various applications such as computer implementations of branching process, constructions of Low Dencity Parity Check codes, various applications to Opimisation Graph Theory and Cryptography (see [29]) and further references). Current paper is dedicated to new results about the girth of known graphs $A(n, F)$, where F is a field, obtained theoretically and via computer simulations and their impact on applications to cryptography and Optimisation on Graphs.

II. On the approximation of regular and homogeneous trees.

In the Theory of Probability a branching process is a special stochastic process corresponding to random walk on t -regular forest F_t, i. e. simple regular graph of finite or infinite degree $t, t > 2$ without cycles. The genealogy of a single vertex is an infinite t-regular tree.

Deterministic branching processes with finite parameters t and some set of connected components C are very important objects in Theoretical Computer Science. In this area the following problem of approximation of forest F_t by the family G_i, $i = 1, 2, \ldots$ of finite t-regular graph of increasing order v_i and increasing girth $g_i = g(G_i)$, which is the minimal length of a cycle in G_i, appears naturally.

P. Erdos defined a *family of graphs of large girth* as t-regular sequence G_i for which $g_i \geq c \log_{t-1}(v_i)$ [1],[2]. He proved the existence of such families (see [3], [4]). Nowadays several explicit constructions of families of large girth are known (see, for example, [5]-[7]). One can add requirement on G_i of diameter d_i to be a family of small world graphs for which the inequality $d_i \leq c' \log_{t-1}(v_i)$ for some positive constant c' holds [4]. Only one family of finite small world graphs of large girth was known.

This is family $X(p, q)$ of Ramanujan Cayley graphs of group $PSL_2(F_p)$ introduced by G. Margulis [8]-[10] and investigated by Phillips, Lubotzky and P, Sarnak [11], the degree q of these graphs is a special prime number.

It is natural to demand some hereditary properties for consequtive members of forest approximations. One of them is the requirement that the family G_i, $i = 1, 2, \ldots$ of graphs of increasing girth allows to consider well defined projective limit F_t, when $i \to \infty$. We refer to the forest approximation G_i as projective approximation if the projective limit of G_i is well defined.

In the case of t-regular graph of large girth we talk about families of projective graphs of large girth. Noteworthy that graphs $X(p, q)$ for various primes p is not a projective approximation of q-regular tree. The first projective approximation of q-regular forest were proposed [12]. It is formed by bipartite graphs $D(n, q)$ of degree q and partition sets of cardinality q. For each q graphs $D(n, q)$, $n = 2, 3, \ldots$ form a family of large girth. The connected components of these edge-transitive graphs form a family $CD(n, q)$ which is a projective approximation of q-regular tree (see [13], [14]). This is of course an other family of large girth. The conjecture that they are also small world graphs was formulated by F. Lazebnik in 1995. It is still open.

Another natural demand for projective forest approximation G_i, $i = 1, 2, \ldots$ is the usage of homogeneous algebraic graphs, i. e graphs which vertices and edges are algebraic varieties over a commutative ring K in Zarisski topology given by corresponding systems of polynomial equations with coefficients from K. Additionally we asume that all neighbourhoods of vertices of G_i, $i = 1, 2, \dots$ are isomorphic to the same manifold $N(K)$ (see [15]). In this case the forest coincides with projective limit given by infinite system of polynomial equations. So, we have algebraic description of branching process.

One can define families of homogeneous algebraic graphs of large girth and families of small world graphs as sequences of algebraic graphs G_i over K with vertex sets of dimensions n_i such that $g(G_i) \geq cn_i$ and $diam(G_i) \leq c'n_i$ for some constants c and c'.

The simple change of F_q for the general commutative ring K leads to generalization $D(n, q), n \geq 2$ to the family of homogeneous algebraic graphs $D(n, K)$ (see [16]) where it was stated that in the case of integrity ring K the girth of $D(n, K)$ is $\geq n + 5$. The proof of this statement was given in [17]. As it was proven in [17] the girth of $D(n, F)$ defined over the field of characteristic zero equals $n + 5$.

Noteworthy that studies of homogeneous algebraic graphs of prescribed graphs or diameter is a classical area of Geometry. Projective plane can be defined as homogeneous algebraic graph of girth 6 and diameter 3. J. Tits defined generalized m-gons as graphs of diameter m and girth $2m$. Geometries of Chevalley groups $A_2(F)$, $B_2(F)$,$G_2(F)$ are homogeneous algebraic graphs over the field F which are generalized m-gons for $m = 3, 4, 6$.

So classical results of geometry motivate search for representatives of variety $\Omega(g, d)$ of homogeneous algebraic graphs of selected girth $g, g \geq 4$ and diameter $d, d \geq 2$. In the case of finite field similar studies of cages, i.e. k-regular graphs , with fixed $k > 2$, prescribed girth g and minimal number of vertices are well known (see [20], [21],[22]).

III. On some parameters of graphs $A(n, K)$

Homogeneous algebraic graph $A(n, K)$ were introduced in [17] as as homomorphic images of $D(n, K)$.

This graph is a 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). It is convenient to use brackets and parenthesis to distinguish tuples from P and L. So $(p) = (p_1, p_2, \dots, p_n) \in P$ and $[l] = [l_1, l_2, \dots, l_n] \in L$. The incidence relation $I = A(n, K)$ (or corresponding bipartite graph I) can be given by condition pIl if and only if the equations of the following kind hold.

$p_2 - l_2 = l_1p_1$, $p_3 - l_3 = p_1l_2$, $p_4 - l_4 = l_1p_3$, $p_5 - l_3 = p_1l_4, \dots, p_n - l_n = p_1l_{n-1}$ for odd n and $p_n - l_n = l_1p_{n-1}$ for even n (see [19]). Graphs $A(n, K)$ form projective forest approximation. They were intensively used for the constructions of LDPC codes for satellite communications and cryptographic algorithms (see [20], [21], [22]). In the case of $K = F_q$ of odd characteristic graphs $A(n, F_q)$, $n \geq 2$ form a family of small world graphs [19]. Various applications of small world graphs are widely known. Recently discovered bound $g(A(n, K)) \geq [(n + 2)/2]$ when K is integrity ring [23], [24] shows that $A(n, K)$ and is a family of algebraic graphs of large girth.

To summarise, we see that for odd q the family $A(n, F_q)$ is a family of projective small world graphs of large girth. The known bounds for girth and diameter of these graphs are far from to be sharp, So we computed the girth $A(n, F_3)$ for $4 \leq n \leq 14$ and diameter of $A(n, F_3)$ for $4 \leq n \leq 10$. Results can be seen in Table I.

IV. On the impact of computations on evaluation of girth and diameter indicators of $\Omega(g, d)$

In [15] the following analog of Tutte inequality on minimal order of finite k-regular graph.

Proposition 4.1: Let Γ be homogeneous algebraic graph over a field F of girth g such that the dimension of neighborhood N for each vertex is $n, n \geq 1$. Then $[(g - 1)/2] \leq dim(V)/n$.

We introduce girth indicator $\mathrm{gind}(\Gamma)$ of Γ as $n[(g - 1/2]/dimV$. So, we have $gind(\Gamma) \leq 1$. We introduce $gind(g, d)$ as maximal girth indicator of representative from $\Omega(g, d)$. The following statement is analog of Moore inequality for k-regular graphs of diameter d.

Proposition 4.2: Let Γ be homogeneous algebraic graph over a field F of diameter d such that the dimension of neighborhood N for each vertex is $n, n \geq 1$. Then $(d - 1) \leq dim(V)/n$.

We introduce diameter indicator $\mathrm{dind}(\Gamma)$ of Γ as $n(d - 1)/dimV$. So, we have $dind(\Gamma) \geq 1$. We introduce $dind(g, d)$ as minimal diameter indicator of representative from $\Omega(g, d)$. The existence of geometries of simple algebraic groups $A_2(F)$, $B_2(F)$ and $G_2(F)$ over the field F (generalized m-gons for $m = 3, 4, 6$) gives us $gind(6, 3) = gind(8, 4) = gind(12, 6) = 1$ and $dind(6, 3) = dind(8, 4) = dind(12, 6) = 1$

The computations of girth and diameter of $A(n, F_3)$ allow to formulate the following statement.

Theorem 4.1:

1) The totality $\Omega(8, 8)$ is nonempty. Let (x, y) be the pair $(gind(8, 8), dind(8, 8))$ then $x \geq 3/4$, $y \leq 7/4$.
2) The totality $\Omega(12, 12)$ has at least two elements. Let (x, y) be the pair $(gind(12, 12), dind(12, 12))$. Then $x = 1$, $y \leq 11/6$. The graph $A(5, 3)$ is the graph with optimal $gind(12, 12)$.
3) The totality $\Omega(12, 16)$ contains at least two elements. Let (x, y) be the pair $(gind(12, 16), dind(12, 16))$. Then $x \geq 5/7$, $y \leq 15/8$.
4) The totality $\Omega(16, 20)$ is not empty. Let (x, y) be the pair $(gind\ \Omega(16, 20), dind\ \Omega(16, 20))$. Then $x \geq 7/9$, $y \leq 19/9$.
5) The totality $\Omega(18, 20)$ is not empty. Let (x, y) be the the pair $(gind\ (16, 20), dind\ (16, 20))$. Then $x \geq 4/5$, $y \leq 19/10$.

Computations of minimal cycles through given vertex of $A(n, F_3)$ allow us to formulate the following statement.

TABLE I
GIRTH AND DIAM FOR $A(n, F_3)$

n	4	5	6	7	8	9	10	11	12	13	14	15
Girth	8	12	12	12	12	16	18	20	22	24	26	28
Diam	8	12	12	16	16	20	20					

Theorem 4.2: Let F be a field of characteristic 3. Then graphs $A(4, F)$, and $A(n, F)$ for $6 \leq n \leq 14$ are not vertex transitive.

Finally, we formulate

Conjecture 4.1: Let (x_n, y_n) stands for the pair $(gind\ A(n, F_3),\ dind\ A(n, F_3))$ Then sequences x_n and y_n tends to 1 and 2 when $n \to \infty$.

Some application of the results of this section were partially presented at plenary talkof V. Ustimenko "On infinite connected real networks without cycles, their dynamical systems and pseudorandom and random real sequences,Ť Isaack Newton Institute, INI Workshop: "Fractional kinetics, hydrodynamic limits and fractals", FD2W02, March 2022.

V. ALGEBRAISATION OF THE BRANCHING PROCESS AND NONLINEAR OPERATORS

Let K be a general commutative ring. We present algebraic transformation groups of K^n.

Recall that $A(n, K)$ is already defined bipartite graph with the point set $P = K^n$ and line set $L = K^n$. We will use brackets and parenthesis to distinguish tuples from P and L. So, $(p) = (p_1, p_2, \dots, p_n) \in P$ and $[l] = [l_1, l_2, \dots, l_n] \in L$.The incidence relation $I = A(n, K)$ (or corresponding bipartite graph I) is given by condition pIl if and only if the given above equations hold. We can consider an infinite bipartite graph $A(K)$ with points $(p_1, p_2, \dots, p_n, \dots)$ and lines $[l_1, l_2, \dots, l_n, \dots]$. If $K, |K| > 2$ is a field then $A(K)$ is a tree and $A(n, K), n = 2, 3, \dots$ is its algebraic small world approximation of large girth.

We refer to the first coordinates $p_1 = p((p))$ and $l_1 = p([l])$ as colours of vertices of $A(K)$ (or $A(n, K)$). It is easy to check that each vertex v of the graph has a unique neighbour $Na(v)$ of selected colour. So the walk of length $2k$ from vertex $(0, 0, \dots)$ will be given by the sequence with colours of its elements $b_1, a_1, b_2, a_2, \dots, b_k, a_k$.

It will be the path if $0 \neq a_1$, $a_i \neq a_{i+1}$ and $b_i \neq b_{i+1}$ for $i = 1, 2, \dots, k-1$. So we can identify walks from 0 point of even length point with sequence of kind w. Let $w' = (b'_1, a'_1, b'_2, a'_2, \dots, b'_s, a'_s)$. We define the composition u of w and w' as the sequence $u = (b_1, a_1, b_2, a_2, \dots, b_k, a_k, b'_1 + a_k, a_k + a'_1, b'_2 + a_k, \dots, b'_s + a_k, a'_s + a_k)$. If w and w' are paths and $b'_1 + a_k \neq b_k$ then u is also a path. Let $B_P(K)$ be a semigroup of all walks with this operation. One can identify empty string with the unity of $B_P(K)$. We use term branching semigroup for $B_P(K)$.

We can change points and lines of the tree and introduce $B_L(K)$ consisting walks with the starting vertex $[0, 0, \dots]$. Noteworthy that sets of points and lines of the tree $A(K)$ are affine varieties of infinite dimensions over K. Let us take graph $A(n, K)$ together with $A(n, K[x_1, x_2, \dots, x_n])$. For each element w from $B_P(K)$ we consider a walk $\Delta(w)$ in $A(n, K[x_1, x_2, \dots, x_n])$ with starting point $(x_1, x_2, \dots, x_n)$ where x_i are generic elements of $K[x_1, x_2, \dots, x_n]$ and special colours of vertices $x_1+b_1, x_1+a_1, \dots, x_1+b_k, x_1+a_k$. Let $p' = dest(\Delta(w))$ be a destination, i. e. a final point of this walk. The destination has coordinates $(x_1 + a_k, f_1(x_1, x_2), f_2(x_1, x_2, x_3), \dots, f_{n-1}(x_1, x_2, \dots, x_n))$ where f_i are elements of $K[x_1, x_2, \dots, x_n]$. We consider the transformation ${}^n\eta'(w)$ of $P = K^n$ defined bythe rule $x_1 \to x_1 + a_k, x_2 \to f_1(x_1, x_2), x_3 \to f_2(x_1, x_2, x_3), \dots, x_n \to f_{n-1}(x_1 x_2, \dots, x_n)$. This transformation is bijective map of K^n to itself. It is an element of affine Cremona group $CG(K^n)$ of elements from $Aut(K[x_1, x_2, \dots, x_n])$ acting naturally on K^n. The inverse for this map is ${}^n\eta'(w)^{-1}$ which coincides with ${}^n\eta'(w')$ for $w' = Rev(w) = (b_t - a_t, a_{t-1} - a_t, b_{t-1} - a_t, \dots, b_1 - a_t, -a_t)$. We refer to $Rev(w)$ as reverse string for w from $B_P(K)$.

Proposition 5.1: (see [26] and further references). The map ${}^n\eta'$ from $B_P(K)$ to $CG(K^n)$ is a homomorphism of the semigroup into group. We refer to ${}^n\eta'$ as compression map and denote ${}^n\eta'(B_P(K))$ as $GA(n, K)$. Degree of element g of Cremona group $CG(K^n)$ of kind $x_i \to g_i(x_1, x_2, \dots, x_n)$ is the maximal degree of polynomials g_i.

Theorem 5.1: (see [26] and further references). The maximal degree of multivariate element g from $GA(n, K)$ equals 3.

It means that subgroup G of kind $TGA(n, K)T^{-1}$ where T is an element of $AGL_n(K)$ can be used efficiently as a platform for the implementation of protocols of Noncommutative Cryptography. Some implementations of such protocol reader can find in [31].

Let $K = F_q$. We refer to a walk $b_1, a_1, b_2, a_2, \dots, b_k, a_k$ from $B_P(K)$ as irreducible one if $a_i \neq a_{i+1}$, $b_i \neq b_{i+1}$ for $i = 1, 2, \dots, t-1$. As it follows from written above lower bound for the girth of $A(n, Q)$ the order of ${}^n\eta(w)$ tends to infinity in the case of irreducible word w with $a_1 \neq 0$, $b_n + a_n \neq b_{14}$. If k is less than the girth of $A(n, q)$ then transformations ${}^n\eta(w)$ has no fixed points on K^n In the case when common length t of irreducible words w and w' is less than the girth the values of ${}^n\eta(w)(x)$ and ${}^n\eta(w')(x)$ are different vectors for each x from K^n. As we see computer simulation strongly support the statement that graphs $A(n, q)$ form a family of small world graph for each parameter q. It means that group $GA(n, q)$ acts acts transitively on K^n and for each pair $x, y \in K^n \times K^n$ there exists element $g \in GA(n, q)$ such that $g(x) = y$.and the value of g on a given vector can be computed in time $O(n^2)$.

VI. On some applications to cryptography

The following stream cipher was implemented by M. Klisowski (see [27]) and further references). Correspondents Alice and Bob work with the space of plaintexts K^n, i.e. they exchange words written in the alphabet K. the "potentially infinite" parameter n can be established via the open channel.

Correspondents shares irreducible word w from $B_P(K)$ of even length m, $m < n$. We assume $n = m^\alpha, \alpha \geq 1$. Additionally they keep safely two strings of nonzero characters ${}^ic = ({}^ic_1, {}^ic_2, \ldots, {}^ic_m)$, $i = 1, 2$ and parameter β, $0 < \beta < 1$. Alice and Bob create linear transformations T_i on K^n of kind $x_1 \to {}^ic_1x_1 + {}^ic_2x_2 + \cdots + {}^ic_mx^m + {}^ic_{m+1} + \ldots$, $x_j \to x_j$, $j + 1, 2, \ldots, n$ with periodical usage of vectors ${}^ic$ They compute parameter $t = [m^{\beta\alpha} - 1]$ and word $u = w^t$ of length mt from $B_P(K)$. We assume here that $\alpha \geq 1/\beta$ Alice writes the plaintext $p = (p_1, p_2, \ldots, p_n)$ and forms ciphertext $(T_2)^n\eta(u)(T_1)(p) = c$ via consequtive Application of T_1, ${}^\eta(u)$ and T_2. Bob gets c from Alice and restores p via consequtive applications of $(T_2)^{-1}$, $ta(Rev(u))$ and ${T_1}^{-1}$. It is easy to see that subquadratic complexity of encryption is $O(n^{1+\beta})$. Correspondents can vary parameter β and encrypt large files.. Let us assume that correspondents use vectors ${}^1c$ and ${}^2c$ constantly and able to change the word w via some key exchange protocol. Then any change of w leads to the change of the ciphertexr. High girth of graph $A(n, q)$ insures this property. Adversary can conduct costly linearization attacks with interception of n^3 messages and corresponding ciphertexts .The total cost of approximation of cubic multivariate encryption map is $O(n^{10})$ (see [28] and further references).

VII. Modified algorithm with the resistance to linearization attacks

We implement the following modification of the presented above $A(n, F_q)$ based stream cipher. We assume that correspondents share the same information. They have "potentially infinite" parameter n, even positive integer m, parameter, β, $0 < \beta < 1$, irreducible element $w \in B_P(F_q)$ of length m and vectors ${}^1c$ and ${}^2c$ from $(F_q)^m$ with nonzero components. Additionally they keep safely the tuple z of kind $(xc_1, xd_1, xc_2, xd_2, \ldots, xc_k, xd_k)$ of length $k = m/2$ with c_i and d_i from $F_q[x]$ for each i, where $c_1 \neq 0$, $d_1 \neq 0$, $c_i \neq c_{i+1}$, $d_i \neq d_{i+1}$. for $i = 1, 2, \ldots, k-1$, $d_k \neq d_1$, $c_k \neq c_1$ and d_kx is a bijective map on F_q such that the list of solution $g(b)$ for $d_k(x)x = b$ is given.. We assume that number of monomial terms of c_i or d_i is bounded by some constant r Alice and Bob concatenate t copies of z and get tuple z^t of length mt. They form $v = z + u = (v_1(x), v_2(x), \ldots, v_{mt}(x)))$. Encryption Alice with plaintext $p = (p_1, p_2, \ldots, p_n)$. She computes $T_1(p) = {}^1p = (p'_1, p'_2, \ldots, p'_n)$.

ENCRYPTION. Alice computes $v^* = (v_1(p'_1), v_2((p'_1), \ldots v_{mt}(p'_1))$. She computes ${}^n\eta(v^*)({}^1p) = {}^2p$ and forms ciphertext $c = T_2({}^2p)$.

DECRYPTION. Bob uses the following procedure.

1)He computes ${T_2}^{-1}(c) = {}^2p$. Bob solves $d_k(x)x + u_{mt} = {}^2p_1$ and finds $x = p'_1$ as $g({}^2p_1 - u_{mt})$. After that he computes v^* and ${}^n\eta(rev(v^*)({}^2p) = {}^1p$. Finally Bob find p as ${T_1}^{-1}({}^1p)$.

PROPERTIES. The map E of kind $(x_1, x_2, \ldots, x_n) \to {}^n\eta(v(x_1)$ depends on vector $xz^t = (y_1(x), y_2(x), \ldots, y_{mt}(x))$. As it follows from [17] degree of E is at least $\deg(y_1) + \deg(y_2) + \max(\deg(y_3), \deg(y_1)) + \max(\deg(y_4), \deg(y_2)) + \cdots + \max(\deg(y_{mt-1}),\deg(y_{mt-3}) + \max(\deg y_{mt}, \deg(y_{mt} - 2)$. So our restrictions on c_i and d_i insure that the degree of multivariate encryption map T_1ET_2 is at least tm. So it is bounded from below via linear function of kind c_n for some positive constant c. It can be shown that the degree of inverse of encryption map is also bounded from below by c', n where $c' > 0$. Thus linearization attacks by adversary are impossible.

Remark 7.1: Noteworthy that presented modification does not change the estimation $O(n^{1+\beta})$ of execution time of algorithms.

Remark 7.2: Assume that vectors ${}^1c$, ${}^2c$ and z remain unchanged. Correspondents can use some secure protocol to change password w. Note that the length of parameter tm is less than $n/4$ and the girth of $A(n, q)$. It means that any change of single change of character of w lead to the change of corresponding ciphertext.

Remark 7.3: Other modification of the algorithm described in section 5 is presented in [29]. This algorithm is also based on graphs A(n,q) but encryption function is nonbijective on K^n. Its restriction on $(K^*)^n$ is a bijective map and this fact allows to decrypt.

Some symbiotic combinations of presented above stream ciphers with $A(n, q)$ based secure protocols and some other protocols of Noncommutative Cryptography (see [30]-[34]) will be presented in the plenary talk of one of the authors at the satellite conference "Mathematical Aspects of post Quantum Cryptography" of International Congress of Mathematicians ICM -2022 (on line event, see [25]).

VIII. Implementation of nonlinear part of modified algorithm.

In this section we present implementation of "nonlinear part E of a encryption." and its inverse in the case $K = F_p$ where p is prime number > 2. So $+$, $*$ and $**$ are operations of addition, multiplication and exponentiation of this field. They can be given by laded operations tables. So we assume that linear transformations T_1 and T_2 are already computed. It is done by function *matrixT1* and *matrixT2*. Recall that actual encryption is given by T_1ET_2. We assume that $(p_1, p_2, \ldots, p_n)$ forms the input of E. It is calculated by function *codeToE*. Computation depends on the tuple of positive numbers $exp = (t_1, t_2, \ldots, t_{mt})$ and vector $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_{mt})$ from ${F_p}^{mt}$. We have $t_{mt} = 1$ and $t_i \neq t_{i-1}$, $\lambda_i \neq \lambda_{i-1}$, $i = 1, \ldots, mt$. We denote this tuples in pseudocode by lists *exp* and *lamb*. Plain text $x = (x_1, \ldots, x_n)$ we denote in pseudocode by list *text*.

So firstly we present how to obtain E. It is done by function *codeToE* it uses functions *neibLine* and *neibPoint* which calculates neighboring line for given point which has color in i iteration $c = x_1^{t_i} + \lambda_i$ or point for given line.

Algorithm 1 Coding to E

```
def neibLine(point, lamb,x1,exp):
#point - list, lamb,x1,exp - int
#returns Line l which l | point
# with color x1**exp+lamb
 line=[]
 line.append(x1**exp+lamb)
 for i>0 in range(len(point)):
  if i\%2==1:
   y=point[i]-line[0]*point[i-1]
  else:
   y=point[i]-line[i-1]*point[0]
   line.append(y)
 return line

 def neibPoint(line,lamb,x1,exp):
#line - list, lamb,x1,exp - int
#returns Point p which p | line
# with color x1**exp+lamb
 point=[]
 point.append((x1**exp+lamb))
 for i>0 in range(len(line)):
  if i\%2==1:
   x=line[i]+line[0]*point[i-1]
  else:
   x=line[i]+line[i-1]*point[0]
   point.append(x)
 return point

def codeToE(text,lamb,exp):
#text,lamb,exp - lists
#Coding text using lamb and exp
#it returns E
 temp=text
 p1=temp[0]
 for i in range(len(lamb)):
  if (i \% 2==0):
    temp=neibLine(temp,lamb[i],p1,exp[i])
  else:
    temp=neibPoint(temp,lamb[i],p1,exp[i])
 E=temp
 return E
```

The computation of composition of T_1, E and T_2 is also given. The last part is to calculate $D = T_1ET_2$. It is done by function *Code*.

The decoding process is reversed. Firstly we use function *Decode* which calculates $T_1^{-1}DT_2^{-1}$ to obtain E. Then we use function *decodeFromE* to obtain plain text x.

We present the execution time of T_1ET_2 in the case p=127, mt=50, 100, 1000 and size of plaintext 10 Kb, 20Kb and 40Kb in Table II on the next page.

Algorithm 2 Coding T_1ET_2

```
def matrixT1():#creates matrix T1
def matrixT2(): #creates matrix T2

def Code(text,lamb,exp):
#text,lamb,exp- lists
 E=codeToE(text,lamb,exp)
 T1=matrixT1()
 T2=matrixT2()
 return T1*E*T2
```

Algorithm 3 Decoding

```
def decodeFromE(cipher,lamb,exp):
#cipher,lamb,exp - lists
#Decodes cipher E retuns original text
 temp=cipher
 x1=temp[0]-lamb[len(lamb)-1]
 for i in range(len(lamb)):
  if i>0:
    if(i\%2==1):
     temp=neibLine(temp,lamb[len(lamb)-1-i]
      ,p1,exp[len(lamb)-1-i])
    else:
     temp=neibPoint(temp,lamb[len(lamb)-1-i]
      ,p1,exp[len(lamb)-1-i])
 temp=neibPoint(temp,0,x1,1)
 return temp

def invertT1():#creates invert of matrix T1
def invertT2(): #creates invert of matrix T2

def Decode(cipher,lamb,exp):
#cipher, lamb,exp - lists
 IT1=invertT1()
 IT2=InvertT2()
 E=IT1*cipher*IT2
 return decodeFromE(E,lamb,exp)
```

References

[1] Paul Erdős, "Graph theory and probability", Canadian Journal of Mathematics, 11, 1959 34-38, doi:10.4153/CJM-1959-003-9.

[2] Paul Erdős and Horst Sachs. Regulare graphen gegebener Taillenweite mit minimaler Knotenzahl. Wiss. Z. MartinLuther-Univ. Halle-Wittenberg Math.-Natur. Reihe, 12:251-257, 1963

[3] B. Bollobash, Extremal graph theory, Academic Press, London, 1978.

[4] B. Bollobash, Random Graphs, Academic Press, London, 1985, 447 pp..

[5] N. Biggs, Algebraic graphs theory, Second Edition, Cambridge University Press, 1993.

[6] N. Biggs, A. G. Boshier, Note on the Girth of Ramanujan Graphs, Journal of Combinatorial Theory, Serie B 49, 1990, 191-194.

[7] Wilfried Imrich. Explicit construction of regular graphs without small cycles. Combinatorica, 4(1):53-59, March 1984.

[8] G.A. Margulis. Graphs without short cycles, Combinatorica 2, 1982, 71-78.

[9] Grigori Margulis. Explicit constructions of graphs without short cycles and low density codes. Combinatorica, 2(1):71-78, March 1982.

TABLE II
THE ALGORITHM'S RUNTIME

File size	10Kb	20Kb	40Kb
mt=50	1,75s	3,41s	6,72s
mt=100	3,31s	6,74s	12,8s
mt=1000	32,72s	65,21s	125,1s

[10] G. Margulis(1988). Explicit group-theoretical constructions of combinatorial schemes and their application to desighn of expanders and concentrators, Probl. Peredachi Informatsii, 24, No. 1, p.51-60.

[11] A. Lubotsky, R. Philips, P. Sarnak (1989). Ramanujan graphs, J. Comb. Theory, 115, No. 2, p. 62-89. https://doi.org/10.1007/BF02126799

[12] F. Lazebnik, V.Ustimenko (1993). Some Algebraic Constractions of Dense Graphs of Large Girth and of Large Size, DIMACS series in Discrete Mathematics and Theoretical Computer Science, 10, p.75-93. https:/doi.org/10.1090/dimacs/010/07

[13] Lazebnik F., Ustimenko V. A. and Woldar A. J (1995). New Series of Dense Graphs of High Girth //Bull (New Series) of AMS, 32, No. 1, p. 73-79. https:/doi.org/10.1090/S0273-0979-1995-00569-0

[14] F.Lazebnik, V. Ustimenko and A. J. Woldar (1996). A characterisation of the components of the graphs D(k,q), Discrete Mathematics,157, p. 271-283. https:/doi.org/10.1016/S0012-365X(96)83019-6

[15] T. Shaska, V. Ustimenko (2009). On the homogeneous algebraic graphs of large girth and their applications, Linear Algebra and its Applications, 430, No. 7, p. 1826-1837. https:/doi.org/10.1016/j.laa.2008.08.023

[16] V. Ustimenko (1998). Coordinatisation of Trees and their Quotients, in the Voronoj's Impact on Modern Science, Kiev, Institute of Mathematics, 2, p. 125-152.

[17] V.Ustimenko (2007). Linguistic Dynamical Systems, Graphs of Large Girth and Cryptography, Journal of Mathematical Sciences, Springer, 140, No. 3, p. 412-434. https:/doi.org/ 10.1007/s10958-007-0453-2

[18] P.K. Wong, Cages - a survey, J. Graph Th. 6 (1982) 1-22.

[19] V. A. Ustimenko (2013). On the extremal graph theory and symbolic computations, Dopovidi National Academy of Sci, Ukraine, No. 2, p. 42-49.

[20] V. A. Ustimenko, U. Romanczuk (2012). On Dynamical Systems of Large Girth or Cycle Indicator and their applications to Multivariate Cryptography, in "Artificial Intelligence, Evolutionary Computing and Metaheuristics ", In the footsteps of Alan Turing Series: Studies in Computational Intelligence, 427, p. 257-285. https:/doi.org/ 10.1007/978-3-642-29694-9_10

[21] M. Polak, V. A. Ustimenko (2012). On LDPC Codes Corresponding to Infinite Family of Graphs A(k,K). Proceedings of the Federated Conference on Computer Science and Information Systems (FedCSIS), CANA , Wroclaw, p. 11-23.

[22] D. MacKay and M. Postol (2003). Weakness of Margulis and Ramanujan - Margulis Low Dencity Parity Check Codes, Electronic Notes in Theoretical Computer Science, 74, p.97-104. https:/doi.org/ 10.1016/S1571-0661(04)80768-0

[23] 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.

[24] V. Ustimenko..On new results on Extremal Graph Theory, Theory of Algebraic Graphs and their applications in Cryptography and Coding Theory. Cryptology ePrint Archive , 2022/296.

[25] V. Ustimenko, On Extremal Expanding Graphs and postquantum secure delivery of passwords. encryption maps and tools for multivariate signatures, Cryptology ePrint Archive, 898, 2021.

[26] V. Ustimenko, M. Klisowski, On Noncommutative Cryptography with cubical multivariate maps of predictable density, In "Intelligent Computing" , Proceedings of the 2019 Computing Conference, London, Volume 2, Part of Advances in Intelligent Systems and Computing (AISC, volume 99)), pp, 654-674.

[27] M. Klisowski, V.A. Ustimenko, On the Comparison of Cryptographical Properties of Two Different Families of Graphs with Large Cycle Indicator, Mathematics in Computer Science, 2012, Volume 6, Number 2, Pages 181-198.

[28] Klisowski, V. Ustimenko, Graph based cubical multivariate maps and their cryptographical applications, in "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.

[29] V.Ustimenko, U. Romanczuk-Polubiec, A. Wroblewska, M. Polak, E. Zhupa, On the constructions of new symmetric ciphers based on nonbijective multivariate maps of prescribed degree, Security and Communication Networks, Wiley-Hindavi, 2019 . Volume 2019, Article ID 2137561, 15 pages.

[30] Alexei G. Myasnikov; Vladimir Shpilrain and Alexander Ushakov (2011). Non-commutative Cryptography and Complexity of Group-theoretic Problems. American Mathematical Society.

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

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

[33] 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 (to appear in 2019).

[34] Gautam Kumar and Hemraj Saini, Novel Noncommutative Cryptography Scheme Using Extra Special Group, Security and Communication Networks ,Volume 2017, Article ID 9036382, 21 pages, https://doi.org/10.1155/2017/9036382