On families of stream ciphers based on the approximations of regular forests

Vasyl Ustimenko[1,2], Oleksandr Pustovit[2]

1 *University of Royal Holloway in London, Egham Hill, Egham TW20 0EX, United Kingdom*
2 *Institute of Telecommunications and the Global Information Space of the National Academy of Sciences of Ukraine, Chokolivsky Boulevard 13, Kyiv, 02000, Ukraine*

Abstract

Discovery of q-regular forest description in terms of an infinite system of quadratic equations over finite field F_q had an impact on the development of Graph Based Cryptography and constructions of robust stream ciphers. We observe known encryption algorithms based on the forest approximations via families of q-regular graph, their modifications defined over the finite arithmetical rings and implementations of these ciphers. The main result is the construction of new family of stream ciphers based on forest approximation which has multivariate nature. The method allows selection of the polynomial degrees of multivariate encryption and decryption procedures.

Keywords: Post-Quantum Cryptography, Stream Ciphers, Graph Based Multivariate Cryptography, Regular Forest Approximations, Extremal Graph Theory.

1. Introduction

Graph Based Cryptography (GBC) area is moving with great speed into the main stream of computer design, Information sciences, Information and Computer programming, Artificial Intelligence and design, Artificial Intelligent and various field of research. Application of GBC is in diverse area such as Data structures, Communication networks and their security. A Graph-based approach centres on conserving the environment of security events by breaking down factors of observable data into a graph representation of all cyber vestiges, from all data aqueducts, counting for all once and present data. For secret communication, Ciphers can be converted into graphs. The Application of Graph Theory plays a vital role in various field of Engineering and Sciences. GBC is used for the key exchange, development of Multivariate Public Keys, key dependent message authentication codes and algorithms of Noncommutative Cryptography (see [24]-[38])

Especially Graph theory is commonly used as a tool of symmetric encryption. First cryptographical applications of Graph Theory appeared in the areas of Symmetric Cryptography and Network Security. This paper reflects some results in the area of applications of families of algebraic graphs of large girth of Extremal Graph Theory to the development of fast and secure encryption tools to process Big Data files. The vertices and edges of algebraic graphs form algebraic varieties defined over the field. The girth is the length of the minimal cycle in the graph. This parameter defines the size of the key space of corresponding cipher. The girth of several known families of algebraic graphs of large girth is not computed. It just evaluated via the lower bounds.

Proceedings ITTAP'2023: 3rd International Workshop on Information Technologies: Theoretical and Applied Problems, November 22–24, 2023, Ternopil, Ukraine, Opole, Poland
EMAIL: vasyl.ustymenko@rhul.ac.uk (A.1); sanyk_set@ukr.net(B.1);
ORCID: 0000-0002-2138-2357 (A.1); 0000-0002-3232-1787 (B.1);

Observed and presented new ciphers have a multivariate nature. The space of plaintexts is an affine variety K^n defined over finite commutative ring K. Bijective encryption map F can be given by nonlinear multivariate polynomials $f_1, f_2, \dots, f_n$ from the multivariate commutative ring $K[x_1, x_2, \dots, x_n]$. It acts on the affine space accordingly the rule $(x_1, x_2, \dots, x_n) \rightarrow (f_1(x_1, x_2, \dots, x_n), f_2(x_1, x_2, \dots, x_n), \dots, f_n(x_1, x_2, \dots, x_n))$, where f_i are given via corresponding list of monomial terms. Trapdoor accelerator (see [21]) is a piece of information A such that the knowledge of A allows to compute the reimage of F in time $O(n^2)$.

In presented ciphers correspondents Alice and Bob shares file A (the password) and encrypt according to the robust procedure in time $O(n)$ or $O(n^2)$. The adversary does not have a password he/she can intercept large amount of pairs plaintext/corresponding ciphertext and try to approximate maps F^{-1} and F. So degree of F is an important parameter for the cryptanalytical studies. The most important (active) part of password are is the information about the walk in the algebraic graph.

In fact the first description of selected graph based stream cipher based on approximations of q-regular tree where q is a prime power was presented in [7] or [45]. The first implementation of this algorithms appeared at the beginning of 2001 [1]. During last twenty years many new results on the construction of new encryption tools and there cryptanalysis were obtained. They lead to understanding of multivariate nature of these algorithms and necessity of usage of infinite algebraic graphs defined over infinite commutative rings of kind $F_q[x_1, x_2, \dots, x_n]$ or more general $K[x_1, x_2, \dots, x_n]$ where K is a finite commutative ring. Implemented in [1] encryption map is a polynomial map of degree 3 such that their inverse is also cubical transformation. So, adversary can use linearisation attacks and after the interception of $O(n^3)$ pairs of kind plaintexts/corresponding ciphertext he/she can approximate the encryption map in time $O(n^{10})$. So, Section 2 is dedicated to observation of ciphers based on algebraic graphs and resistant to such linearisation attacks.

The general scheme of flexible encryption algorithm based on special family of algebraic graphs defined over commutative ring is presented there.

The theory of approximations of regular trees is presented in Section 3 which contains description of q-regular forest approximation $D(n, q)$, $n \rightarrow \infty$ [2] and tree approximation $CD(n, q)$ [3]. Analogues of these families of graphs over an arbitrary commutative ring are presented there together with the known results on their properties and applications.

Precise description of observed graph based algorithm is given in the Section 4 together with evaluation of the degrees of encryption map and its inverse.

The special cases of $CD(n, 256)$ defined over the finite field F_{256} is selected for an implementation. Parameters of corresponding computer simulations are given at the end of Section 4.

Last Section 5 is the conclusion.

2. Short survey of ciphers based on the approximations of infinite regular trees

We have to report that the implemented case of $D(n, q)$ based encryption $E(n, q)$ is far from being optimal. As it was showed in [4, Serdica] the increase of parameter q leads to faster encryption of files of the same size. Noteworthy that the usage of loaded multiplication tables makes immaterial the difference between case of prime q and composed prime powers. Such tables allow to use $q=128$ corresponding to the alphabet ASCEE with the essential speed increase comparably to implemented in [1] $q=127$, where operator of taking modulo 127 is used cn times where constant c depends on the length of the password. The multivariate nature of $D(n, q)$ encryption was noticed in [4] (see also [22] for the case of arbitrary ring K), described their symbolic computations turned out to be cubic. This fact was mathematically proved in [5] for arbitrary parameters n and q.

The standard usage of multivariate transformation $E(n, q)$ with two affine transformation T_1 and T_2 in the form $T_1 E(n, q) T_2$ allow us to improve drastically the mixing properties of the cipher. Noteworthy that in the implemented case of $E(n, 127)$ encryption the change of single characters of the plaintext leads to the change of 48-52 percents of characters of corresponding ciphertexts. The experiment with special linear transformations T_1 and T_2 was described in [6]. To preserve linear time $O(n)$ of the encryption we have to select sparce transformations, i. e. those with $O(n)$ nonzero entries of corresponding matrices. Special sparce transformations allow us to improve drastically mixing

properties of $E(n, q)$ encryption. For selected in [6] cases the single change of a plaintext character leads to the change of more than *98* percents of characters of corresponding ciphertext. As it was shown in [8ust linguistic] transformation $E(n, q)$ with the password of length less than $[(n+5)]$ has no fixed points. This property holds for the case of ciphers of kind $T_1 E(n, q)(T_1)^{-1}$.

More general graphs $D(n, K)$ defined over arbitrary commutative ring K can be obtained via simple change of F_q for K (see [7]). Investigation of dynamical systems corresponding to these graphs showed the similarity of general graphs $D(n, K)$ of the graphs defined for the case of fields (see [8], [9] and [10]. If passwords corresponds to tuples of characters from the multiplicative group K^* of the ring K then different passwords of length $<[(n+5)/2]$ produce distinct ciphertext from the selected plaintext. It means that case of arithmetic rings Z_m of integers of modulo m is attractive for the implementations.

Noteworthy that the cases of fields F_q, $q=2^m$ of characteristic two and rings Z_q, $q=2^m$ are most convenient for implementations because of files in the computer are presented in the form *0, 1*-sequences.

Recall that the girth of a graph is the length of its minimal cycle. The connected components $CD(n, q)$, $n=2, 3,\ldots$ of algebraic graphs $D(n, q)$, $q>1$ form a family of tree approximations, i. e well defined projective limit of them is an infinite q-regular tree. Graphs $D(n, q)$ are edge transitive. So, their connected components are isomorphic. The system of quadratic equations which defines $CD(n,q)$ were presented in [11]. The union of these equations gives an algebraic description of q-regular tree. Existence of such description is very important for Computer Science because a q-regular tree is the deterministic part of branching process.

Noteworthy that the plaintext and the ciphertext of $E(n, q)$ encryption are located in the same connected component of $D(n, q)$. Graphs $CD(n, q)$ have a natural analogue $CD(n, K)$ defined over arbitrary commutative ring K with at least two elements, $CD(n, K)$ is an induced subgraph of $D(n, K)$ (see [7]). The description of $CD(n, K)$ in terms of the system of recurrent quadratic equations is given in [7] together with the description of $CD(n, K)$ based encryption $CE(n, K)$.

It works with the space of plaintexts K^m, $m=3/4n+c$ where c, $c<3$ is some nonnegative integer constant. It is important that group of transformations of $CE(n,K)$ corresponding to various passwords acts transitively on the space of plaintexts while the group generated by various transformations of kind $E(n, K)$ is intransitive. It leads to better mixing properties of $CE(n, K)$ in comparison with those of $E(n, K)$. In fact we have to use $T_1 CE(n, K)(T_1)^{-1}$ where T_1 is a special sparce transformation of $AGL_m(K)$.

Another q- regular tree approximation $A(n, q)$, $q=2,3,\ldots$were defined in [43]. It has some advantages in comparison with graphs $CD(n, q)$. For instance the graphs are defined by simple homogeneous equation with two linear and one quadratic monomial terms. Finite field F_q can be substituted by general commutative ring K and graphs $A(n, K)$ can be obtained this way (see [43] or [10]). The girth $g(A(n, q))$ of the graphs $A(n, q)=A(n, F_q)$ can be bounded from below via inequality $g(A(n, q))\geq[(n+2)/2]$ [44]. The computer simulation support the conjecture that $A(n, Z_m)$ based encryption with passwords from $((Z_m)^*)^t$, $m>2$, t is an even parameter $<[(n+2)/4$ is such that different passwords produce distinct ciphertext from the selected plaintext. We will use notation $AE(n, K)$ for the $A(n, K)$ based ciphers.

To summarise written above we discuss some properties of three graph based steam ciphers $E(n, K)$, $CE(n, K)$ and $AE(n, K)$ defined in the case $K=F_q$, $q>m$ and $K=Z_m$, $m>2$. All of them can be used for Information Systems protection. For practical implementation case of large finite fields and arithmetic rings Z_t, $t=2^m$ is preferable.

The families of graphs $D(n, K)$, $A(n, K)$ defined over arbitrary commutative ring K are bipartite graphs of type $(1, 1, n-1)$ with partition sets which are two copies of K^n (see [12]) , i.e. graphs with the incidence $I=I(K)={}^nI(K)$ between points $(x_1, x_2,\ldots, x_n)$ and lines $[y_1, y_2,\ldots, y_n]$ given by the system of equations $a_2x_2-b_2y_2= f_2(x_1, y_1)$, $a_3x_3-b_3y_3= f_2(x_1, x_2, y_1, y_2),\ldots, a_nx_n-b_ny_n= f_2(x_1, x_2, \ldots, x_{n-1}, y_1, y_2, \ldots, y_{n-1})$ where parameters $a_2, a_3, \ldots, a_{n-1}$ and $b_2, b_3, \ldots, b_{n-1}$ are taken from the multiplicative group K^* of the commutative ring K. Parameters $\rho((x_1, x_2,\ldots, x_n))=x_1$ and $\rho([y_1, y_2,\ldots, y_n])=y_1$ serve as colours of the point and the line. The following linguistic property holds. Each vertex of the graph has a unique neighbour of the chosen colour.

Graph $CD(n,K)$ after the elimination of computed recurrently parameters also can be written as linguistic graphs of type $(1, 1, m-1)$ where $m=[3/4n]+c$.

In fact the architecture require a partition of information into blocks of the same size. So, parameters n and m equals to some selected constant. the length of the password is another even constant which has an impact on the speed of encryption. Other option to increase speed of execution is the increase the cardinality of the ground field or ring. Let us consider the general scheme of creating the cipher based on the family of linguistic graphs ${}^nI(K)$, $n=2, 3, \ldots$

Noteworthy that we can expand defined above $I(K)$ to the infinite linguistic graph $I(K[x_1, x_2,\ldots, x_n])$ defined over the ring $K[x_1, x_2,\ldots, x_n]$ of all multivariate polynomials with coefficients from K and the variables x_i, $i=1,2,\ldots, n$. So points and lines of this graph are $X=(X_1(x_1, x_2,\ldots, x_n), X_2(x_1, x_2,\ldots, x_n),\ldots, X_n(x_1, x_2,\ldots, x_n)$ and $Y=[Y_1(x_1, x_2,\ldots, x_n), Y_2(x_1, x_2,\ldots, x_n),\ldots, Y_n(x_1, x_2,\ldots, x_n)]$. The incidence of this bipartite graph is given by equations $a_2X_2-b_2Y_2= f_2(X_1, Y_1)$, $a_3X_3-b_3Y_3= f_2(X_1, X_2, Y_1, Y_2),\ldots, a_nX_n-b_nY_n= f_2(X_1, X_2, \ldots, X_{n-1}, Y_1, Y_2, \ldots, Y_{n-1})$, where parameters $a_2, a_3, \ldots, a_{n-1}, b_2, b_3, \ldots, b_{n-1}$ and polynomials f_i, $i=2, 3,\ldots, n$ with coefficients from K are taken from the equations in the definition of the linguistic graph $I(K)$.

We define the polynomial map F from K^n *to* K^n via the following scheme (see [23]). Take the special point $X=(x_1, x_2,\ldots, x_n)$ of $I(K[x_1, x_2,\ldots x_n])$ and consider the list of colours $g_1(x_1), g_2(x_1), \ldots, g_t(x_1)$. We compute the path $v_0Iv_1Iv_2\ldots Iv_t$ where $v_0=X$ and v_{i+1} is the neighbour of v_i with the colour $g_i(x_1)$, $i=1,2, \ldots, t$ and $I=I(K[x_1, x_2,\ldots, x_n])$. Then the destination point v_t of this path can be written as $(g_t(x_1), F_2(x_1, x_2), \ldots, F_n(x_1, x_2,\ldots, x_n))$. The map F is given by the rule $x_1\rightarrow g_t(x_1)$, $x_2\rightarrow F(x_1, x_2),\ldots, x_n\rightarrow F(x_1, x_2,\ldots, x_n)$. It is easy to see that $F=F(g_1, g_2,\ldots, g_t)$ is a bijective map if and only if the equations of kind $g_t(x_1)=b$ have unique solutions for unknown x_1 for each b from K.

So family of linguistic graphs ${}^nI(K)$, $n=2, 3,\ldots$ together with family of affine transformations $T_n\epsilon AGL_n(K)$ can be used as a cipher with the space of plaintexts K^n and the password $g_1(x), g_2(x),\ldots, g_t(x)$ and the encryption map $T_n(F(g_1, g_2,\ldots, g_t)(T_n)^{-1}$

Correspondents Alice and Bob share the password given by $g_1, g_2,\ldots, g_t$ and the sequence of transformations T_n , $n=2, 3,\ldots$ We assume that inverse maps $(T_n)^{-1}$ are computed and presented explicitly. For the encryption of potentially infinite plaintext $(p)=(p_1, p_2,\ldots, p_n)$ they will use transformation $T_nF(g_1, g_2,\ldots, g_t)(T_n)^{-1}$. One of them creates the plaintext (p) and computes the ciphertext $T_n(F(g_1, g_2,\ldots, g_t)(T_n)^{-1}(p)=c$ recurrently. The procedure is the sequence of the following steps.

S_1. He/she computes $(T_n)^{-1}(p_1, p_2,\ldots, p_n) =(r(1), r(2),\ldots, r(n))=(r)$

S_2. He/she computes $a(1)=g_1(r_1), a(2)=g_2(r_1),\ldots, a(t)=g(r_1)$

S_3. Let $N_a(x_1, x_2,\ldots, x_n)$ be the operator of taking the neighbour of point $(x_1, x_2,\ldots, x_n)$ with the colour a in the linguistic graph ${}^nI(K)$ and ${}^aN(y_1, y_2,\ldots, y_n)$ be an operator of taking the neighbour of line $[y_1, y_2,\ldots, y_n]$ with the colour a. He/she executes the following operation. Computation of $v_1=N_{a(1)}(r), v_2={}^{a(2)}N(v_1), v_3=N_{a(3)}(v_2), v_4={}^{a(4)}N(v_3),\ldots, v_{t-1}= N_{a(t-1)}(v_{t-2}), v_t={}^{a(t)}N(v_{t-1})=u=(u_1, u_2,\ldots, u_n)$

S_4 He/she computes ciphertext as $T(u)=c$

DECRYPTION PROCEDURE.

Assume that one of correspondents received the ciphertext c. He/she decrypts via the following steps.

D_1. Computation of u as $(T_n)^{-1}(c)=u$ and getting the solution $x=r(1)$ of equation $g(x)=u_1$

D_2. Computation of parameters $a(1)=g_1(r(1)), a(2)=g_2(r(1)), \ldots,a(t-1)=g_{t-1}(r(1))$ and the completion of the recurrent procedure $v_{t-1}=N_{a(t-1)}(u), v_{t-2}= {}^{a(t-2)}N(v_{t-1}), v_{t-3}=N_{a(t-3)}(v_{t-2}), v_{t-4}={}^{a(4)}N(v_{t-3}),\ldots, v_1= N_{a(1)}(v_{t-2}), {}^{r(1)}N(v_{4t-1})=r$.

D_3. *Computation of the plaintext* (p) *as* $T(r)$.

OBFUSCATION OF THE ALGORITHM.

Let us consider the colour jump operator J_a which transforms point $(p_1, p_2,\ldots, p_n)$ *of* the graph $I(K)$ to the point $(a, p_2, p_3,\ldots, p_n)$.

We can change the encryption map $T_nF(g_1, g_2,\ldots, g_t)(T_n)^{-1}$ for the $T_nF(g_1, g_2,\ldots, g_t)J_g(T_n)^-$, where J_g is a colour jump operator acting on points of $I(K[x_1, x_2,\ldots x_n])$ with the colour $g(x_1)\epsilon K(x_1)$ such that the equation of kind $g(x_1)=b$ has a unique solution for each parameter b from K.

After this change assumption the bijection of g_t on K is immaterial. Encryption procedure requires computation of $(T_n)^{-1}(p_1, p_2,\ldots, p_n) =(r(1), r(2),\ldots, r(n))=(r)$, the computation of u accordingly step S_2. the computation of $J_g(u)=u'$ and application of affine transformation T_n to the tuple u'.

For the decryption of ciphertext c the user has to compute $u'=(u'_1, u'_2,\ldots, u'_n)$ as $(T_n)^{-1}(c)$, solve for x the equation $g(x)=u'_1$, use the solution $x=r(1)$ of this equation for the computation of

$a(1)=g_1(r(1))$, $a(2)=g_2(r(1)),\ldots$, $a(t)=g_t(r(1))$, compute $J_a(t)(u')=(u)=(u_1, u_2,\ldots, u_n)$ in the graph $I(K)$ and execute procedures D_3 and D_4 to get the original plaintext.

3. On families of algebraic graphs of large girth

3.1 General remarks

Girth and diameter of a graph are the minimal length of its cycle and the maximal distance of the graph. The constructions of finite or infinite graphs with prescribed girth and diameter is an important and difficult task of the Graph Theory.

Noteworthy that the incidence of classical projective geometry over various fields is a graph of girth 6 and diameter 3. J. Tits defined generalised m-gons as bipartite graphs of girth $2m$ and diameter m. Feit and Higman proved that finite generalised m-gons with bi-degrees >2 exist only in the cases of $m=3, 4, 6, 8$ and 12. Geometries of finite simple groups of rank 2 are natural examples of generalised m-gons for $m=3,4,6, 8$. Classification of flag transitive generalised m-gons of Moufang type were obtained by J. Tits and R.Weiss.

Infinite families of graphs of large girth of bounded degree are important objects of Extremal Graph Theory which were introduced by P. Erdős'. He proved the existence of such families via his well-known probabilistic method. Nowadays few explicit constructions of such families are known. The concept of infinite family of small world graphs of bounded degree turns out to be very important for various applications of graph theory.

Noteworthy that the only one family of small world graphs of large girth is known. This is the family $X(p, q)$ of Ramanujan graphs introduced by Gregory Margulis [13] and investigated via the computation of their girth, diameter and the second largest eigenvalue by A. Lubotsky, R.Phillips and P.Sarnak [14].

We have to admit that studies of families of graphs Γ_i with well defined projective limit Γ, which is isomorphic to infinite tree, is well motivated.

We refer to such family as tree approximation. There is only one approximation by finite graphs which is a family of large girth. This is the mentioned above family of $CD(n, q)$ defined by F. Lazebnik, V. Ustimenko and A.Woldar [3].

The question whether or not $CD(n, q)$ form a family of small world graphs has been still open since 1995.

In 2013 the tree approximation by finite graphs $A(n,q)$ which is a family of small world graphs was presented (see [43]).

One of the main statements of this paper is $A(n, q)$ where $n=2, 3,\ldots$ is a family of large girth.

We generalise these results in terms of the theory of algebraic graphs defined over arbitrary field and consider properties and applications of above mentioned graphs.

3.2. On graphs D(n, q), their properties and generalisations

All graphs we consider are simple, i. e. undirected without loops and multiple edges. Let $V(\Gamma)$ and $E(\Gamma)$ denote the set of vertices and the set of edges of Γ, respectively. The parameter $|V(\Gamma)|$ is called the order of Γ, and |E(G)| is called the size of Γ. A path in Γ is called simple if all its vertices are distinct. 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 length of a path is a number of its edges. The girth of a graph Γ, denoted by $g=g(\Gamma)$, is the length of the shortest cycle in Γ. Let $k\geq 3$ and $g\geq 3$ be integers. The distance between vertices v and u of the graph Γ is a minimal length of the path between them. The diameter of the graph is maximal distance between its vertices.

Graph is connected if its diameter is finite. Graph is k-regular if each vertex of the graph is incident exactly to k other vertexes. A tree is a connected graph which does not contain cycles

1. An infinite family of simple regular graphs Γ_i of constant degree k and order v_i such that $diam\ (\Gamma_i) \leq c\ log_{k-1}(v_i)$, where c is the independent of i constant and $diam\ (\Gamma_i)$ is diameter of Γ_i, is called a *family of small world graphs.*

2. Recall that infinite families of simple regular graphs Γ_i of constant degree k and order v_i such that $g(\Gamma_i) \geq c\ log_{k-1}(v_i)$,where $\boldsymbol{c}$ is the independent of i constant and $g(\Gamma_i)$ is a girth of Γ_i are called

families of graphs of large girth. Tree (q-regular simple graph without cycles) in terms of algebraic geometry over finite field F_q.

3. Projective limit of graphs Γ_i is well defined and coincides with q-regulat tree T_q.

We refer to family of graphs Γ_i satisfying condition (iii) as *tree approximation.* We known example of the family satisfying conditions 1, 2 and 3.

The family $X(p, q)$ formed Cayley graphs for $PSL_2(p)$, where p and q are primes, had been defined by G. Margulis [13] and investigated by A. Lubotzky, Sarnak and Phillips [14]. As it is easy to see the projective limit of $X(p, q)$ does not exist.

3. 3. On homogeneous algebraic graphs of large girth

Let F be a field. Recall that a projective space over F is a set of elements constructed from a vector space over F such that a distinct element of the projective space consists of all non-zero vectors which are equal up to a multiplication by a non-zero scalar. Its subset is called a quasiprojective variety if it is the set of all solutions of some system of homogeneous polynomial equations and inequalities.

An algebraic graph φ over F consists of two things: the vertex set Q being a quasiprojective variety over F of nonzero dimension and the edge set being a quasiprojective variety φ in Q × Q such that (x, x) is not element of φ for each $x \in Q$ and $x\varphi y$ implies $y\varphi x$ ($x\varphi y$ means $(x, y) \in \varphi$). The graph φ is homogeneous (or M-homogeneous) if for each vertex $v \in Q$ the set $\{x \mid v\varphi x\}$ is isomorphic to some quasiprojective variety M over F of nonzero dimension. We further assume that M contains at least 3 elements.

Theorem [15]. *Let Γ be homogeneous algebraic graph over a field F of girth g such that the dimension of neighborhood for each vertex is N, $N \geq 1$. Then $[(g - 1)/2] \leq dim(V)/N$.*

The following corollary is an analog of Even Circuit Theorem by Erdős' for finite simple graphs.

Corollary. *Let Γ be a homogeneous graph over a field F and $E(\Gamma)$ be a variety of its edges. Then $dim(E(\Gamma)) \leq dimV(\Gamma)(1 + [(g - 1)/2]^{-1}$.*

We refer to a family of homogeneous algebraic graphs φ_n for which the dimension of neighborhood for each vertex is independent constant N, $N \geq 1$ as a *family of large girth* if girth of each graph φ_n is bounded from below by linear function $\alpha n + \beta$ defined by constants α and β .

We refer to a homogeneous algebraic graph as algebraic forest if it does not contain cycles. Their term algebraic tree stands for the connected algebraic forest.

We say that family of homogeneous algebraic graphs φ_n is a forest (tree) approximation if projective limit of φ_n is an algebraic forest (tree).

3. 4. Graphs D(n,K).

Graphs $D(n,q)$ which defines projective limit $D(q)$ with points $(p)=(p_{01}, p_{11}, p_{12}, p_{21}, p_{22}, p'_{22}, \ldots, p'_{ii}, p_{i\,i+1}, p_{i+1,i}, p_{+i+1,i+1} \ldots)$, lines $[l]=[l_{10}, l_{11}, l_{12}, l_{21}, l_{22}, l'_{22}, \ldots, l'_{ii}, l_{i\,i+1}, l_{i+1,i}, l_{+i+1,i+1} \ldots]$ and incidence relation given by equations

$l_{ii}-p_{ii}=l_{10}\, p_{i-1,i}$;

$l'_{ii} - p'_{ii} = l_{i,i-1}\, p_{01}$;

$l_{i,i+1} - p_{i,i+1} = l_{ii}\, p_{01}$;

$l_{i+1i} - p_{i+1,i} = l_{10} p'_{ii}$.

This four relations are defined for $i \geq 1$, ($p'_{11} = p_{11}$, $l'_{11} = l_{11}$).

Remark. *You can see that indexes of vectors correspond to coordinates of positive roots of root system A_1 with a wave.*

Historically graph $D(q)$ is not the first example of description of q-regular forest in terms of Algebraic Geometry. Geometries of buildings (see [16] and further references) corresponding to extended Dynkin diagram A_1 as incidence structures are $q+1$-regular trees or $q+1$-regular forests. As a result we get a description of a tree in group theoretical terms.

In [17] it was noticed that the restriction of this incidence relation on orbits of Borel subgroup B^- acting on maximal parabolic subgroups are q-regular bipartite graphs. So we get a description of a q-regular tree in terms of positive roots of A_1 with a wave.

In [2] authors proved that $D(n,q)$ defined via first $n-1$equations of $D(q)$ form a family of graphs of large girth. The general point and line of these graphs are projections of (p) and $[l]$ onto the tuples of their first n coordinates.

Unexpectedly it was discovered that these graphs are disconnected if $n \geq 6$. So forest $D(q)$ contains infinitely many trees and the diameter is an infinity. F. Lazebnik conjectured that connected components of graphs $D(n, q)$, $n = 3,4, \ldots$ form a family of small world graphs. This conjecture is still open.

In 1994 it was found out how to describe connected components $CD(n, q)$ of graphs $D(n, q)$ in terms of equations (see [11], [3]). In the case of families of graphs of large girth we would like to have " speed of growth" c of the girth "as large as it is possible". P. Erdos' proved the existence of such a family with arbitrary large but bounded degree k with $c=1/4$ by his probabilistic method.

In the case of families $X(p,q)$ and $CD(n,q)$ the constant c is $4/3$. In the case of $A(n,q)$ we just get inequality $1 \leq c < 2$. So exact computation of the girth is the area of the future research. There are essential differences between family of graphs $X(p, q)$ and tree approximations. Recall that the projective limit of $X(p, q)$ does not exist.

Families $X(p,q)$, $CD(n,q)$ can be used for the constructions of LDPC codes for noise protection in satellite communications. D. MacKay and M. Postol [19] proved that $CD(n, q)$ based LDPC codes have better properties than those from $X(p,q)$ for the constructions of LDPC codes. In [18] it was proved that $A(n,q)$ based LDPC codes even better than those from $CD(n,q)$.

Cayley nature of $X(p,q)$ does not allow to use these graphs in multivariate cryptography. Various applications of graphs $D(n,q)$ and $CD(n,q)$ have been known since 1998.

3. 5. On the equations for graphs CD(n, K)

Let K stand for an arbitrary commutative ring. Noteworthy that graphs $D(n, K)$ are defined over arbitrary commutative ring K have been already presented.

To facilitate notation in the future results on "*connectivity invariants*" of $D(n, K)$, it will be convenient for us to define $p_{-1,0} = l_{0,-1} = p_{1,0} = l_{0,1} = 0$, $p_{0,0} = l_{00} = -1$, $p'_{0,0} = l'_{0,0} = -1$, $p_{1,1} = p'_{1,1}$, $l_{1,1} = l'_{1,1}$ and to assume that our equations are defined for $i \geq 0$.

Graphs $CD(k,K)$ with $k \geq 6$ were introduced in [10], [11] for as induced subgraphs of $D(k,K)$ with vertices u satisfying special equations $a_2(u)=0$, $a_3(u)=0, \ldots$, $a_t(u)=0$, $t=[(k+2)/4]$, where $u = (u_\alpha, u_{11}, u_{12}, u_{21}, \ldots, u_{r,r}, u'_{r,r}, u_{t\,t+1}\, u_{r,r+1}, u_{r+1,r}, \ldots)$, $2 \leq r \leq t$, $\alpha \in \{(1, 0), (0,1)\}$ is a vertex of $D(k, K)$ and $a_r = a_r(u) = \Sigma_{i=0,r}(u_{ii}\, u'_{r-i,\,r-i} - u_{i,i+1}\, u_{r-i,r-i-1})$ for every r from the interval $[2,t]$ for every r from the interval $[2,t]$.

We set $a = a(u) = (a_2, a_3, \ldots, a_t)$ and assume that $D(k, K) = CD(k,K)$ if $k = 2,3,4,5$. As it was proven in [11] graphs $D(n, K)$ are edge transitive. So their connected components are isomorphic graphs. Let ${}^{v}CD(k,K)$ be a solution set of system of equations $a(u) = (v_2, v_3, \ldots, v_t) = v$ for certain $v \in K^{t-1}$. It is proven that each ${}^{v}CD(k,K)$ is the disjoint union of some connected components of graph $D(n,K)$.

It is easy to see that sets of vertices of ${}^{v}CD(k,K)$, $v \in K^{t-1}$ form a partitions of the vertex set of $D(n,K)$. We consider more general graphs ${}^{v}CD\_J(k, K)$ defined via subset $J = \{i(1), i(2), \ldots, i(s)\}$, $1 \leq s \leq t-1$ of $\{2, 3, \ldots, t\}$ and tuple $(v_{i(1)}, v_{i(2)}, \ldots, v_{i(s)})$ formed by vertices $u \in K^n$ such that $a_{i(1)}(u) = v_{i(1)}$, $a_{i(2)}(u) = v_{i(2)}, \ldots, a_{i(s)}(u) = v_{i(s)}$.

We refer to ${}^{v}CD_J(k, K)$ as J-component of $D(n, K)$. We assume that equations $a_{i(1)} = v_{i(1)}$, $a_{i(2)} = v_{i(2)}, \ldots, a_{i(s)} = v_{i(s)}$ define *J-component* ${}^{v}CD_J(K)$ of $D(K)$. Noteworthy that in the case of finite commutative ring ${}^{v}CD_J(K)$ is a regular forest.

The concept of quasiprojective variety over commutative ring K can be introduced via simple substitution of K instead of field F. It leads to concepts of homogeneous algebraic graphs over K, forest and tree approximations and families of graphs of large girth over K. It was proven that for the case of commutative ring K with unity of odd characteristic graphs $CD(n,K)$ are connected (see [20]). So graph $CD(n,q) = CD(n, F_q)$ for odd q is a connected component of $D(n,q)$.

Theorem [11]. *For each commutative integrity ring K the families of graphs D(n, K), n=2,3,…,n=2,3,.. are forest approximations and families of graphs of large girth.*

4. On the description of selected algorithms based on algebraic graphs of large girth

To achieve linear speed $O(n)$ of the encryption described in Section 1 functions g_i, $i=1,2,..,$ t are selected in the form $x_1+c(i)$, $c(i)\epsilon K$ and the parameter t will be selected within the interval $[2, [(n+5)/2])$ when $I(K)=D(n, K)$ or $I(K)=CD(n, K)$.

Additionally we take parameters $b(1), b(2), ...,b(k)$, $a(1), a(2),...,a(k)$, $k=t/2$ from K^* *to* construct $c(i)$ recurrently via the following rules $c(1)=b(1)$, $c(2)=a(1)$, $c(i)=c(i-2)+b(i)$ if i, $i\geq 3$ is odd n and $c(i)=c(i-2)=a(i)$ if i, $i\geq 4$ is even.

We refer to the tuple $(b(1), b(2),..., b(k), a(1), a(2),...,a(k))$ as active password and affine transformation T as passive password.

Our choice insures that in the case of constant passive password the single change of a single character of active password leads to a change of the ciphertext produced from the selected plaintext. We choose an affine transformation T in the form of linear map given by the following rule

$T(x_1)=x_1+m(1)x_2+...+m(n-1)x_{n-1}$ where $m(i)$, $i=1,2,...,$ $n-1$ are elements of K^*. $T(x_i)=x_i$ for $i=2,3,..., n$. So $T^{-1}(x_1)=x_1-m(1)x_2-m(2)x_3-...-m(n-1)x_n$. $T^{-1}(x_i)=x_i$ for $i=2,3,..., n$.

Recall that explicit description of linguistic graphs $D(n, K)$ is given in the previous section and general encryption algorithm is described in section 2. So, ciphers $T\,E(n,K)\,T^{-1}$ and have full description. In the case of graph $CD(n, K)$ we will use in fact the induced subgraph ${}^hCD(n, K)$, $h=(h_2, h_3,..., h_t)$, $t=[(n+2)/4]$ *of* $D(n, K)$ of all points and lines $u=(u_\alpha, u_{11}, u_{12}, u_{21}, ..., u_{r,r}, u'_{r,r}, u_{t\,t+1}\,u_{r,r+1}, u_{r+1,r}, ...)$ satisfying conditions $a_i(u)=h_i$.

Linguistic graph ${}^hCD(n, K)$ can be thought as bipartite graph with points $(p)=(p_{01}, p_{11}, p_{12}, p_{21}, ..., p_{i\,i+1}, p_{i+1,i}, p_{+i+1,i+1} ...)$, $i=2,3,..., t-1$ and lines $[l]=[l_{10}, l_{11}, l_{12}, l_{21}, l_{22}, ..., l_{i\,i+1}, l_{i+1,i}, l_{+i+1,i+1} ...]$, $i=2,3,..., t-1$ of length $n-t$.

Their incidence is given by the following system of equations

$l_{ii}-p_{ii}=l_{10}\,p_{i-1,i}$;

$l_{i,i+1}-p_{i,i+1}=l_{ii}\,p_{01}$;

$l_{i+1i}-p_{i+1,i}=l_{10}p'_{ii}$.

where p'_{22} is defined by the equation $a_2(p_{01}, p_{11}, p_{12}, p_{21}, p_{22}, p'_{22})=h_2$ and can be written as $p'_{22}=a_2(p_{01}, p_{11}, p_{12}, p_{21}, p_{22}, p'_{22})-h_1+p'_{22}=b_2(p_{01}, p_{11}, p_{12}, p_{21}, p_{22})$, other parameters are $p'_{33}=a_3(p_{01}, p_{11}, p_{12}, p_{21}, p_{22}, p'_{22}, p_{2,3}, p_{3,2}, p_{3,3}\,p'_{3,3})-h_3+p'_{33}=b_3(p_{01}, p_{11}, p_{12}, p_{21}, p_{22}, p'_{22}, p_{2,3}, p_{3,2}, p_{,33})$, ..., $p'_{tt}=a\_t(p_{01}, p_{11}, p_{12}, p_{21}, p_{22}, p'_{22}, ..., p'_{t-1,t-1}, p_{t-1,\,t}, p_{t,\,t-1}, p_{t,\,t}, p'_{t,\,t})-h_t+p'_{t,t}=b_t(p_{01}, p_{11}, p_{12}, p_{21}, p_{22}, p'_{22}, ..., p'_{t-1,t-1}, p_{t-1,\,t}, p_{t,\,t-1}, p_{t,\,t})$.

The computation of symbolic expressions $p'_{i,i}$ recurrently *and their explicit* substitution in the system of equations give us the equations of the linguistic graph.

We assume that corresponding cipher has the space of *plaintexts* K^{n-t}. We use active passwords $(b(1), b(2),..., b(k), a(1), a(2),...,a(k))$ an linear transformations T *of* K^{n-t} constructed via described above rules. We assume that parameters $h_2, h_3,...,h_t$ *will be* considered as part of the active password and denote the cipher as $TCE(n, K)T^{-1}\,T_nF(g_1, g_2,..., g_t)J_g(T_n)^-$.

We will use presented in Section 2 obfuscation scheme for each cipher $TE(n, K)T^{-1}$ and $TCE(n, K)T^{-1}$ in the case $K=F_q$, $q>2$. We use special disturbance function g of I_g selected as $x\rightarrow x^e+b$ where $b\epsilon F_q$, $e\epsilon Z_d$, $d=q-1$ and $(e, d)=1$. So, the notations $DE(n, K)=TE(n, K)I_gT^{-1}$ and $DC(n,K)=TCE(n, K)I_gT^{-1}$ will be used for these encryption schemes with the disturbance.

Algorithms with the encryption maps $TE(n, K)T^{-1}$ independently on the choice of active and passive passwords have multivariate encryption and decryption functions of degree 3. In [39] the linearisations attacks on these ciphers with the interception of $O(n^3)$ pairs plaintext/cipheretext are presented. They can be executed in polynomial time $O(n^{10})$.

The ciphers $DE(n, K)$ use cubical encryption maps as well but the usage of disturbance map $D: x\rightarrow x^e$ lead to the increase of the degree r of inverse maps. Parameter r can be evaluated from below by the polynomial degree of transformation D^{-1} acting on the elements of multiplicative group K^*. So, if $K=F_q$, $q=2^{32}$ then the order of polynomial decryption map is at least 2^{31}. It justifies that direct linearisation attacks are not feasible.

Case $TCE(n, K)T^{-1}$ is principally different. As it follows from the results of [40] (ust wroblevskska) the encryption function corresponding to selected active password has degree $[(n+2)/4]+2$. So the generation of standard form for the encryption function can not be done in polynomial time.

So the directed linearisation attacks are theoretically impossible. Principle difference of $DC(n, K)$ and $TCE(n, K)T^{-1}$ is the fact that the usage of disturbance implies the fact that the degree of inverse function is essentially higher than those for encryption function.

We can use induced graphs ${}^{v}CD_J(k, K)$ of graphs $D(n, K)$ which are J-components of them where $J=J(n) =\{i(1), i(2), \dots, i(t(n))\}$ is the subset of $\{2, 3,\dots, [(n+2)/4]\}=M(n)$ and tuples $(v_{i(1)}, v_{i(2)},\dots, v_{j(t(n))})$ are elements of $K^{t(n)}$.

Similarly to the case of $CD(n, K)$ when $J(n)=M(n)$ we can find the equations for ${}^{v}CD_J(n, K)$ via the elimination of special symbolic coordinates of general vertex $<x>= <x_1, x_{1,1}, x_{12}, x_{2,1}, x_{2,2}, x_{2,2}, x_{2,3}, x_{32}, x_{3,3}, x'_{33},\dots, x_{i,i}, x_{i,i+1}, x_{i+1,i+1}, x'_{i+1,i+1}, \dots>$, $3 \le i \le[(n+2)/4-1]$ (point or line) *of* $D(n, K)$ given by the list $x'_{i(k),i(k)}$, $k=2,3,\dots, t(n)$. The variable $x'_{i(k), i(k)}$ can be found from the equation $a_{i(k)}(<x>)=v_i(k)$. The substitution of symbolic expressions *of* $x'_{i(k), i(k)}$ into the incidence conditions of $D(n, K)$ gives us the linguistic interpretation of ${}^{v}CD_J(n, K)$. This bipartite graph has the sets points and lines isomorphic to the affine space K^l where $l=n-t(n)$.

We associate with the family of graphs ${}^{v}CD_J(n, K)$ the sequence of encryption maps obtained by the following rules. We assume that symbolic vertex $<x>=(x)$ from $K^{n-t(n)}$ is a point and the graph is given in its linguistic interpretation. Let us rename the indexes of points and lines of ${}^{v}CD_J(k, K)$ by $1,2,\dots, n-k$. So $x=(x_1, , x_2,\dots, x_{n-t(n)})$.

The nonlinear graph N based transformation is the following one.

We select parameter k and form to tuples ${}^{k}a=(\alpha(1), a(2),\dots, a(k))$ *and* ${}^{k}b=(\beta(1), \beta(2),\dots, \beta(k))$ with the coordinates from the multiplicative group K^* of the commutative ring K.

Let ${}^{\alpha}N(u)$ be the operator of taking the neighbour of $u=(u_1, u_2,\dots, u_{n-t})$ from the graph ${}^{v}CD_J(k, K)$ with the colour of $u_1+\alpha$. We consider the sequence ${}^{1}u= {}^{\beta(1)}N(x)$, ${}^{2}u= {}^{\alpha(1)}N({}^{1}u)$, ${}^{3}u= {}^{\beta(2)}N({}^{2}u)$, ${}^{4}u= {}^{\alpha(2)}N({}^{3}u)$, …, ${}^{2k-1}u= {}^{\beta(k)}N({}^{2k-2}u)$, ${}^{2k}u= {}^{\alpha(k)}N({}^{2k-1}u)=(w_1, w_2,\dots,w_{n-t})$. We set $N(x_1, x_2,\dots, x_{n-t})=(w_1, w_2,\dots, w_{n-t})$.

We also will use the obfuscation ${}^{g}N((x_1, x_2,\dots, x_{n-t})=(g(x_1), w_2,\dots, w_{n-t})$, where $g(x)$ is selected bijective polynomial function on K of degree at most $t(n)+2$.

Let us investigate the multivariate nature of the map N. We may assume that coordinates of a general point (x) are variables $x_1, x_2,\dots, x_{n-t}$. We consider the multivariate ring $K[x_1, x_2,\dots, x_{n-t}]$ and the graph ${}^{v}CD_J(K[x_1, x_2,\dots, x_{n-t}])$ with points and lines of kind $<g_1, g_2,\dots, g_{n-t}>$, $g_i \in K[x_1, x_2,\dots, x_{n-t}]$.

We already select parameter k and form to tuples ${}^{k}a=(\alpha(1), a(2),\dots, a(k))$ *and* ${}^{k}b=(\beta(1), \beta(2),\dots, \beta(k))$ with the coordinates from the multiplicative group K^* of the commutative ring K.

We consider the walk in the graph with the starting point $u_0=(x), u_1, u_2,\dots., u_{2k}$ where colours of $u_1=x_1+ \beta(1), u_2=x_1+ \alpha(1), u_i=u_{i-2}+ \beta(i)$, $i=3, 5,\dots, 2k-1$, $u_i=u_{i-2}+ \alpha(i))$, $i=4, 6,\dots, 2k$.

Let $u_{2k}=(x_1+\alpha(1)+ \alpha(2)+\dots+ \alpha(k))$, $F_2(x_1, x_2,\dots, x_{n-t})$, $F_3(x_1, x_2,\dots, x_{n-t})$, …, $F_{n-t}(x_1, x_2,\dots, x_{n-t})$. So we may treat N as multivariate transformation of K^{n-t} to itself given by the rule $x_1 \to x_1+\alpha(1)+ \alpha(2)+\dots+ \alpha(k)$, $x_2 \to F_2(x_1, x_2,\dots, x_{n-t})$, $x_3 \to F_3(x_1, x_2,\dots, x_{n-t}),\dots, x_{n-t} \to F_{n-t}(x_1, x_2,\dots, x_{n-t})$.

As it follows from [40 Ust, Wrob] the maximal degree of F_i is $t(n)+2$. it is clear that the degree of obfuscated map ${}^{g}N$ is also $t(n)+2$. If g has degree d, $d>2$ and order r then g^{-1} has degree d^{r-1} and the degree of ${}^{g}N$ can be evaluated from below as $d^{r-1}(t(n)+2)$.

As in the cases of ciphers based on graphs $D(n, K)$ and $CD(n, K)$ the encryption map will be conjugated with the special linear transformation T given by the following rule. $T(x_1)=x_1+m(1)x_2+\dots+m(n-t-1)x_{n-t-1}$ where $m(i)$, $i=1,2,\dots, n-1$ are elements of K^*, $.T(x_i)=x_i$ for $i=2,3,\dots, n$.

We denoted described below cipher as ${}^{k}ED_1(n-t, K)$. The map $T^{g}NT^{-1}$ has active password $(\alpha(1), a(2),\dots, a(k), \beta(1), \beta(2),\dots, \beta(k))$, $v_{i(1)}, v_{i(2)},\dots, v_{j(t(n))})$.

Parameters $m(1), m(2)\dots, m(n-t-1)$ together with $J=\{i(1), i(2),\dots, i((t(n))$ form the passive password. We assume that constants k and $t(n)=t$ can be agreed by correspondents via an open channel. Under described above assumptions cipher has a linear speed $v(n)$ of size $O(n)$. The slope of the $v(n)$ is defined by the value of weight parameter $w=i(1)+i(2)+\dots+i(m)$.

The following important property holds. The change of the active password lead to the change of the ciphertext for the selected plaintext. It means that brut force attack on the cipher requires $p^{2k}q^t$ elementary operations where p is the order of K^* and q is the size of the commutative ring K.

The implemented case

For the first two implementation we select the cases of ciphers ${}^{k}ED_t(m, K), m=n-t$ with $K= F_{256}$, g of kind $g= x^2+b$ *and* $t=128$ with weights $w=2^{13}$ and 2^{16}. In both cases the degree of encryption map

will be at least 130 the degree of the encryption map will be bounded below by $130 \cdot 128$. So the linearisation attacks by adversary are unfeasible. The bruit forth attack require $(2^{15}) \cdot 255^k$, where $k=2l$ is the chosen length of the walk in the graph.

CRYPTALL 6 software is written in C++ programming language and therefore it is portable and runs in many platforms such as Unix/Window. The context diagram is depicted in Fig. 1. The interface is friendly. It allows users to enter active and passive password of selected length. The program is supported by key exchange protocol based on Eulerian transformations of F^*_{256} (see [21]). It allows the elaboration of the tuple of nonzero field elements of length k together with the tuple of arbitrary field elements of length 128 to form both passwords.

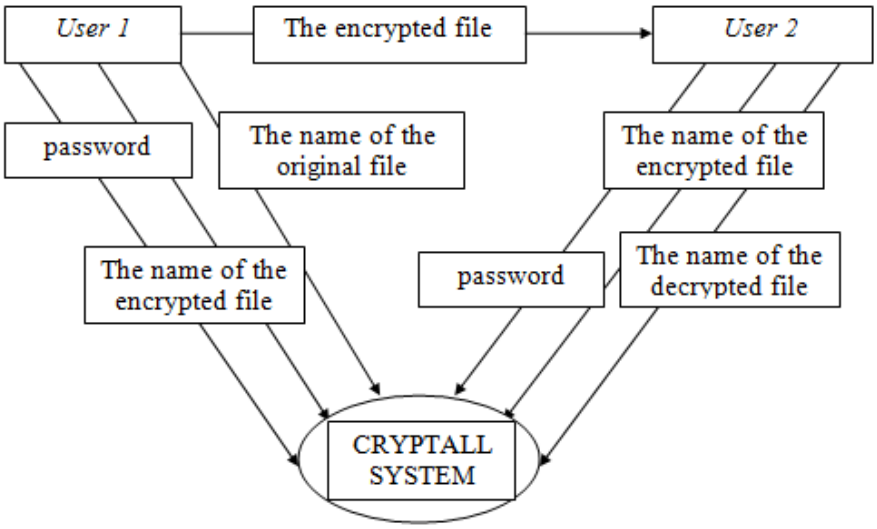

Figure. 1 Context Diagram of CRYPTALL 6

Experimental Measurements To evaluate the performance of our algorithm, we use with different size of files. We denote by $t\ (k, L)$ the time (in millisecond) that is needed to encrypt or decrypt (because of symmetry). The file size is in kilobytes for passwords of length L. Then the value of $t(k, L)$ can be represented by the following matrices (Fig. 2 and Fig 3).

L\k	**3000**	**4000**	**5000**	**6000**
4	1388	1864	2132.25	2575
8	2625.75	3641.5	4192.25	5039.25
12	3728.5	4988.25	6146	7350
16	4967	6592.5	8103.5	9648.25
20	6231.25	8231.5	10082.25	11989.75

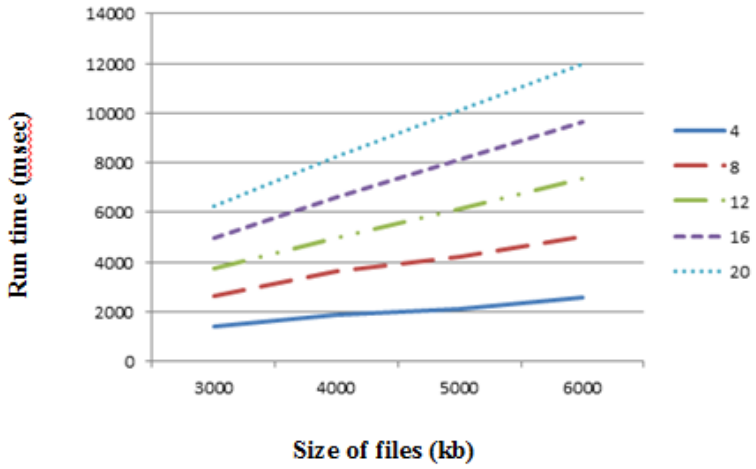

Figure 2 Run time for CRYPTALL 6 System

L\k	**3000**	**4000**	**5000**	**6000**
4	1796.25	2412.25	2759.25	3332.5
8	3398	4714	5425.25	6521.25
12	4825.25	6455.25	7953.5	9511.75
16	6427.75	8531.5	10486.75	12486
20	8064	10652.5	13047.75	15516

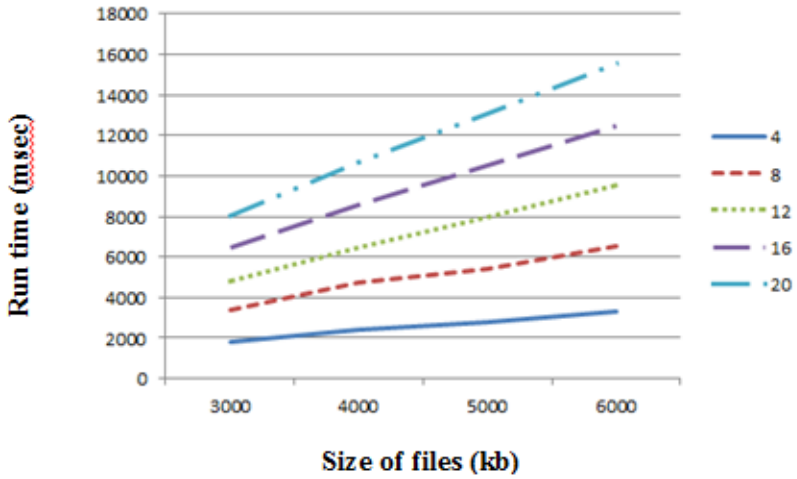

Figure 3 Run time for CRYPTALL 6 System

In both cases algorithms have nice mixing properties. change of single character lead to the change at leas 98 percents of the characters in the ciphertext.

5. Conclusion

The main theoretical result of the paper is explicit construction of the family of multivariate map of affine maps F_n based on the graphs $CD(n, K)$ with the trapdoor accelerator of linear degree cn , $c=3/4$ acting on affine space K^n defined over arbitrary commutative ring K with at least 3 elements. Corresponding cipher has execution speed of kind $¼ n^2+O(n)$ which is proportional to the length of active password of size $O(1)$. The decryption procedure takes the same time with the encryption process.

The disadvantage of F_n in the comparison with the $D(n, K)$ based cipher is essentially lower speed of encryption, $O(n^2)$ instead of $O(n)$. So the usage of F_n will drastically improve the security level of the encryption but the speed of processing is essentially slower than in the case of the usage of graphs $D(n, K)$.

Noteworthy that speed of processing is very important parameter. That is why we suggest usage of flexible ciphers ${}^kED_t(m, K),m=n-t$ where t is the selected constant. All of them have a linear speed of execution. Case $t=0$ corresponds to $D(n, K)$ based cipher. Increasing of parameter t leads to the increase of resistance of cipher against linearisation attacks.

So correspondents can govern the security level within the family of ${}^kED_t(m, K),m=n-t$ *ciphers.* The idea to use connectivity invariants of graphs $D(n, K)$ was formulated in [42].

The implemented stream ciphers based on algebraic graphs given by equations found practical usage in Fiji Islands and Australia (see [1], [42], [46], [55], [56], [57]), Ukraine ([41], [58], [65]), Poland ([6], [39], [50], [54],[55], [62]), Brasil ([47]Ustimenko Futorny), Sultanate of Oman ([48], [52],[62], [63],) and Canada [59], [60], [64]). In all cases the degree of the inverse map was bounded by 3. We suggest new class of ciphers based on algebraic graphs with option to unbounded increase of the inverse map by customers. We hope that new algorithms with the resistant to linearization attacks and linear speed of encryption will be successfully used for protection of Information systems and Big Data Processing.

6. Acknoledgements

This research is partially supported by the Fellowship of British Academy for RaR 2022.

7. References

[1] V. Ustimenko, “CRYPTIM: Graphs as tools for symmetric encryption,” in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 2227, 2001.

[2] 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.

[3] 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.

[4] V. Ustimenko, “On graph-based cryptography and symbolic computations,” Serdica Journal of Computing, vol. 1, no. 2, pp. 131–156, 2007.

[5] Aneta Wroblewska, "On some properties of graph based public keys’’, Albanian Journal of Mathematics, Albanian J. Math. 2(3), 229-234, (2008).

[6] J. S. Kotorowicz and V. A. Ustimenko, “On the implementation of cryptoalgorithms based on algebraic graphs over some commutative rings,” in Condensed Matter Physics, vol. 11, no. 2, 2008.

[7] 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.

[8] 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
[9] V. A. Ustimenko, U. Romanczuk, 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, 2012, p. 231-256, https:/doi.org/ 10.1007/978-3-642-29694-9_10
[10] V. A. Ustimenko, U. Romanczuk, On Extremal Graph Theory, Explicit Algebraic Constructions of Extremal Graphs and Corresponding Turing Encryption Machines, in "Artificial Intelligence, Evolutionary Computing and Metaheuristics ", In the footsteps of Alan Turing Series: Studies in Computational Intelligence, Vol. 427, Springer, January, 2013, 257-285.
[11] 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
[12] V. Ustimenko, Maximality of affine group, hidden graph cryptosystem and graph's stream ciphers, Journal of Algebra and Discrete Mathematics, 2005, v.1, pp 51-65.
[13] G. Margulis(1988). Explicit group-theoretical constructions of combinatorial schemes and their application to design of expanders and concentrators, Probl. Peredachi Informatsii, 24, No. 1, p.51-60.
[14] A. Lubotsky, R. Philips, P. Sarnak (1989). Ramanujan graphs, J. Comb. Theory, 115, No. 2, p. 62-89. https://doi.org/10.1007/BF02126799
[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] F. Buekenhout (editor), Handbook in Incidence Geometry, Ch. 9, North Holland, Amsterdam, 1995.
[17] V. Ustimenko (1989). Affine system of roots and Tits geometries, Voprosy teorii grupp i gomologicheskoy algebry, Yaroslavl, p.155-157.
[18] 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.
[19] 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
[20] V. Ustimenko (2009). Algebraic groups and small world graphs of high girth, Albanian Journal of Mathematics,3, No. 1, p. 25-33.
[21] V. Ustimenko, On Extremal Algebraic Graphs and Multivariate Cryptosystems, Cryptology ePrint Archive, reprint 2022/1537.
[22] V. Ustimenko, On the extremal graph theory for directed graphs and its cryptographical applications In: T. Shaska, W.C. Huffman, D. Joener and V. Ustimenko, Advances in Coding Theory and Cryptography, Series on Coding and Cryptology, vol. 3, 181-200 (2007).
[23] V. Ustimenko, Graphs in terms of Algebraic Geometry, symbolic computations and secure communications in Post-Quantum world, Editorial House of University of Maria Curie – Sklodowska, Lublin, November, 2022, 196 pages.
[24] Geetha N K, Ragavi V, Graph Theory Matrix Approach in Cryptography and Network Security, Proceedings of 2022 Algorithms, Computing and Mathematics Conference (ACM), 29-30 Aug. 2022, https://ieeexplore.ieee.org/document/10202460
[25] Costache, A., Feigon, B., Lauter, K., Massierer, M., Puskás, A. (2019). Ramanujan Graphs in Cryptography. In: Balakrishnan, J., Folsom, A., Lalín, M., Manes, M. (eds) Research Directions in Number Theory. Association for Women in Mathematics Series, vol 19. Springer, Cham. https://doi.org/10.1007/978-3-030-19478-9_1
[26] P.L. K. Priyadarsini, A Survey on some Applications of Graph Theory in Cryptography, Journal of Discrete Mathematical Sciences and Cryptography, https://www.tandfonline.com/doi/abs/10.1080/09720529.2013.878819

[27] W. M. Al Etaiwi, , Encryption Algorithm Using Graph Theory, ;Journal of Scientific Research & Reports3(19): 2519-2527, 2014; Article no. JSRR.2014.19.004.
[28] Samid Gideon, Denial Cryptography based on Graph Theory, US patent 6823068-2004 http://www.patentstorm.us/patents/6823068.html
[29] Lothrop Mittenthal, Sequencings and Directed Graphs with Applications to Cryptography, S.W. Golomb et al. (Eds.): Springer-Varlag LNCS 4893, pp 70–81, 2007.
[30] Moni Naor and Adi Shamir. Visual cryptography. In Advances in Cryptology - EURO-CRYPT'94, LNCS, vol 950, pp 1–12, 1994.
[31] Steve Lu, Daniel Manchala and Rafail Ostrovsky, Visual Cryptography on Graphs, COCOON 2008: pp. 225–234, 2008.
[32] William Stallings, Cryptography and Network Security Principles and Practices, Prentice Hall India, 2006.
[33] Dawn Song, David Zuckermany and J. D. Tygar, Expander Graphs for Digital Stream Authentication and Robust Overlay Networks, Proceedings of the 2002 IEEE Symposium on Security and Privacy (S&P.02), 2002.
[34] M Yamuna, Meenal Gogia, Ashish Sikka and Md. Jazib Hayat Khan, "Encryption using graph theory and linear algebra", International Journal of Computer Application, pp. 2250-1797, 2012.
[35] A Paszkiewicz et al., Proposals of graph based ciphers theory and implementations. Research Gate, 2001.
[36] Cusack, B.; Chapman, E. Using graphic methods to challenge cryptographic performance. In Proceedings of the 14th Australian Information Security Management Conference, Edith Cowan University, Perth, Australia, 5–6 December 2016; pp. 30–36. [Google Scholar]
[37] Chapman, E. Using Graphic Based Systems to Improve Cryptographic Algorithms. Ph.D. Thesis, Auckland University of Technology, Auckland, New Zealand, 2016. [Google Scholar]
[38] Kinani, E.H.E. Fast Mapping Method based on Matrix Approach For Elliptic Curve Cryptography. Int. J. Inf. Netw. Secur. (IJINS) 2012, 1, 54–59.
[39] M. Klisowski. Zwiększenie bezpieczeństwa kryptograficznych algorytmów wielu zmiennych bazujących na algebraicznej teorii grafów. Rozprawa doktorska, Politechnika Częstochowska, Częstochowa, 2014.
[40] Vasyl Ustimenko , Aneta Wroblewska, On the key exchange and multivariate encryption with nonlinear polynomial maps of stable degree, DOI: http://dx.doi.org/10.2478/v10065-012-0047-6, Annales of UMCS, Informatica, Vol 13, No 1 (2013) , pp. 63-80.
[41] Pustovit O.S. Application of the theory of extreme graphs to modern problems of information security. - Dissertation for obtaining the scientific degree of candidate of technical sciences in the specialty 05.13.06 - Information technologies. – Institute of Telecommunications and Global Information Space of the National Academy of Sciences of Ukraine, Kyiv, 2021.
[42] V. Ustimenko, Graphs with special arcs and cryptography, Acta Applicandae Mathematicae (Kluwer) 2002, 74, pp. 117-153.
[43] V. A. Ustimenko. On the extremal graph theory and symbolic computations, Dopovidi National Academy of Sci, Ukraine, 2013, No. 2, p. 42-49.
[44] V. Ustimenko, On new results on extremal graph theory, theory of algebraic graphs, and their applications, Reports of National Acad. of Sci. of Ukraine, 2022, N4, pp. 25-32.
[45] V. Ustimenko, Random Walks on graphs and Cryptography, Extended abstracts, AMS meeting, March, Louisville, 1998.
[46] V. Ustimenko, D. Sharma, Special Graphs in Cryptography, The Poster Papers Collection, Third International Workshop on Practice and Theory in Public Key Cryptography , PKC 2000.
[47] V. Futorny, V. Ustimenko, On small world semiplanes with generalised Schubert cells, Acta Applicandae Mathematicae, 98, N1 (2007) 47-61.
[48] V. Ustimenko, On the Cryptography with “Mathematica package”, Proceedings of the conference ”Leaning Mathematics and Technology Middle East Conference” , University of Arizona and Sultan Qaboos University, Oman, March, 2007, 11 p.
[49] A. Tousene, V. Ustimenko, Graph based private key cryptosystem, International Journal on Computer Research, Nova Science Publisher, 2005, vol.13, issue 4 (with A Touzene) 12p.

[50] V. Ustimenko, S. Kotorowicz, On the properties of Stream Ciphers Based on Extremal Directed graphs, In "Cryptography Research Perspectives", Nova Publishers, Ronald E. Chen (the editor), 2008.
[51] Y. Khmelevsky, Gaetan Hains, E. Ozan, V. Ustimenko, Chris Kluka and D. Syrotovsky) International Cooperation in SW Engineering Research Projects, Proceedings of Western Canadien Conference on Computing Education, University of Northen British Columbia, Prince George BC, May 6-7, 2011, 14p.
[52] A. Touzene, Marwa AlRaisi, Imene Boudelioua, Performance of Algebraic Graphs Based Stream-Ciphers Using Large Finite Fields, Annalles UMCS Informatica AI X1, 2 (2011), 81-93.
[53] J. Kotorowicz U. Romanczuk, V. Ustimenko, Implementation of stream ciphers based on a new family of algebraic graphs, Proceedings of Federated Conference on Computer Science and Information Systems (FedCSIS), 2011, 13 pp.
[54] V. Ustimenko, M. Klisowski, 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.
[55] V. Ustimenko, D. Sharma, CRYPTIM: system to encrypt text and image data, Proceedings of International ICSC Congress on Intelligent Systems 2000, Wollongong, 2001, 11pp.
[56] V. Ustimenko, Yu Khmelevsky, Walks on graphs as symmetric and asymmetric tools for encryption, 2002, South Pacific Journal of Natural Studies, 2002, vol. 20, 23-41. www.usp.ac.fj/spjns
[57] V. Ustimenko, Yu Khmelevsky, Practical aspects of the Informational Systems reengineering, The South Pacific Journal of Natural Science, volume 21, 2003, p.75-21. www.usp.ac.fj/spjns/volume21
[58] V. Ustimenko, A Tousene, CRYPTALL - a System to Encrypt All types of Data , Notices of Kiev - Mohyla Academy, v. 23, 2004,pp 12-15.
[59] Y. Khmelevsky, M. Govorov,S. Sharma, v. Ustimenko, Security Solutions for Spatial Data in Storage (Implementation Case within Oracle 9iAS), Proceeings the 8th World Multiconference on Systemics, Cybernetics and Informatics (SCI 2004) Orlando, USA, in July 18-21, 2004.
[60] Y. Khmelevsky, Gaetan Hains, E. Ozan, Chris Kluka , V.,Ustimenko and D. Syrotovsky) International Cooperation in SW Engineering Research Projects, Proceedings of Western Canadien Conference on Computing Education, University of Northen British Columbia, Prince George BC, May 6-7, 2011, 14pp.
[61] S. Kotorowicz, V. Ustimenko, On the properties of Stream Ciphers Based on Extremal Directed graphs, In "Cryptography Research Perspectives", Nova Publishers, Ronald E. Chen (the editor), 2008. (with S. Kotorowicz).
[62] V. Ustimenko, A. Touzene, Graph Based Private KeyCrypto System, International Journal on Computer Research, NovaScience Publisher, volume 13 (2006), issue 4, 12p.
[63] A. Touzene, V. Ustimenko, Private and Public Key Systems Using Graphs of High Girth,In "Cryptography Research Perspectives", Nova Publishers, Ronald E. Chen (the editor), 2008, pp. 205-216.
[64] M. Govorov, Y. Khmelevsky, V. Ustimenko, and A. Khorev, “Security for GIS N-tier architecture,” Developments in Spatial Data Handling, pp. 71–83, 2005.
[65] Pustovit O., Ustymenko V., Pro zastosuvannia alhebraichnoi kombinatoryky do problem koduvannia ta kryptohrafii [On the application of algebraic combinatorics to the problems of coding and cryptography] // Matematychne modeliuvannia v ekonomitsi, No 1-2. - Kyiv. - 2017. - s. 31-46.