Families of Stream Ciphers based on Non-Bijective Multivariate Encryption Maps of High Degree

Vasyl Ustimenko[1,2] and 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, 13 Chokolivsky Boulevard, Kyiv, 02000, Ukraine*

Abstract

The discovery of q-regular forest description in terms of an infinite system of quadratic equations over a finite field F_q had an impact on the development of Graph-Based Cryptography and constructions of robust stream ciphers. The family of algebraic graphs $D(n, K)$ defined over arbitrary commutative ring K with unity already was used for the description of some graph-based ciphers. We introduce new ciphers constructed in terms of $D(n, K)$. Let K be arithmetical ring Z_q, $q = 2^l$, $l \geq 3$. We will use natural bijection between elements of multiplicative group K^* and elements of Z_p, $p = 2^{l-1}$. The space of plaintexts is $(Z_p)^{n-s}$ the space of ciphertexts is $(Z_q)^{n-s}$ where s of size $O(1)$ can be arbitrary parameter $<[(n+2)/5]$. The password can be selected as an arbitrary pair of tuples of kind $(a_1, a_2, ..., a_k) \in (K^*)^k$, $(d_1, d_2, ..., d_s) \in (K^*)^s$ where even k, $k<[(n+5)/2]$ has size $O(1)$. We prove that different passwords produce distinct ciphertext from the selected plaintext. So the cost of a direct attack by an adversary is $q^s p^k$. The encryption map has a multivariate nature, it is induced by non-bijective polynomial transformation F_n of K^{n-s} to itself of prescribed degree d. Users can select d, $d \geq 3$ as an arbitrary parameter of the size $O(n)$. Appropriate selection of large d makes linearisation attacks on the cipher of multivariate nature unfeasible. The speed of encryption/ decryption is $O(n)$. Additionally, we introduce similar ciphers based on the bijective transformation of the space of plaintexts K^{n-s} where K is an arbitrary commutative ring with unity with nontrivial multiplicative group K^*.

Keywords

Post Quantum Cryptography, linguistic graphs over commutative rings. Stream Ciphers, Graph-Based Multivariate Cryptography, Extremal Graph Theory.

1. Introduction

Graph-Based Cryptography (GBC) area is moving with great speed into the mainstream of computer design, Information sciences, Information and Computer programming, Artificial Intelligence, and design. Applications of GBC are in diverse areas such as Data structures, Communication networks, and their security. A Graph-based approach centers 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, GBC is used for the key exchange, development of Multivariate Public Keys, key-dependent message authentication codes, and algorithms of Noncommutative Cryptography [16–30].

Graph theory is commonly used as a tool for symmetric encryption. The first cryptographical applications of Graph Theory appeared in the areas of Symmetric Cryptography and Network Security. This paper [35] and monograph [15] reflect various results in the area of applications of families of algebraic graphs of the large girth of Extremal Graph Theory to the development of fast and secure encryption tools to process Big Data files. The girth is the length of the minimal cycle in the graph. This parameter defines the

CPITS-2023-II: Cybersecurity Providing in Information and Telecommunication Systems, October 26, 2023, Kyiv, Ukraine
EMAIL: Vasyl.Ustymenko@rhul.ac.uk (V. Ustimenko); sanyk_set@ukr.net (O. Pustovit)
ORCID: 0000-0002-2138-2357 (V. Ustimenko); 0000-0002-3232-1787 (O. Pustovit)

size of the key space of the corresponding cipher.

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 $f_1, f_2,..., f_n$ from the multivariate commutative ring $K[x_1, x_2,..., x_n]$. It acts on the affine space according to the rule $(x_1, x_2,..., x_n) \rightarrow (f_1(x_1, x_2,..., x_n), f_2(x_1, x_2,..., x_n),..., f_n(x_1, x_2,..., x_n))$, where f_i are given via corresponding list of monomial terms. The trapdoor accelerator (see [14]) is a piece of information A such that the knowledge of A allows us to compute the reimage of F in time $O(n^2)$.

In presented ciphers based on bijective maps correspondents Alice and Bob share file A (the password) and encrypt according to the robust procedure in time $O(n)$ or $O(n^{1+\alpha})$ where α is from the interval $[0,1]$. The adversary does not have a password he/she can intercept a large amount of pairs of plaintext/corresponding ciphertext and try to approximate maps F^{-1} and F. So the degree of F is an important parameter for cryptanalytical studies. The most important (active) part of the password is the information about the walk in the algebraic graph.

The first description of selected graph-based stream cipher based on approximations of the q-regular tree where q is a prime power was presented in [4] or [15]. The first implementation of these algorithms appeared at the beginning of 2001 [1]. During the last twenty years, many new results on the construction of new encryption tools and their cryptanalysis were obtained. They lead to an understanding of the multivariate nature of these algorithms and the necessity of usage of infinite algebraic graphs defined over infinite commutative rings of kind $F_q[x_1, x_2, ..., x_n]$ or more general $K[x_1, x_2,..., x_n]$ 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 a cubical transformation. So, the 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 $O(n^{10})$.

In [35] first graph-based encryption scheme with a nonbijective encryption map was presented.

Section 2 is dedicated to the general schemes of flexible encryption algorithms based on a special family of algebraic graphs defined over a commutative ring. The used class of algebraic graphs is known as the class of linguistic graphs of type $(1,1, n-1)$. Some of these schemes do not use descriptions of connected components of graphs. other schemes are based on the knowledge of connectivity invariants of the graphs. Some of them allow us to define bijective maps of corresponding affine space, and others are used for the creation of an injective map of $(K^*)^n$ into K^n where K is a commutative ring with the unity and K^* is its multiplicative group.

The remarkable well-known family of linguistic graphs $D(n, K)$ defined over K is introduced in Section 3. The connected components of these graphs and their properties and applications are discussed. In particular, we consider the theory of approximations of regular trees and forests with the example q-regular forest approximation $D(n, F_q) = D(n, q)$, $n \rightarrow \infty$ [2] and tree approximation via linguistic graphs $CD(n, q)$ [3].

The precise description of some graph-based algorithms of Section 2 in the case of $D(n, K)$ is given in Section 4 together with an evaluation of the degrees of the encryption map and its inverse. We select algorithms constructed without the usage of connectivity invariants of graphs.

Section 5 is dedicated to the family of bijective and non-bijective ciphers described in terms of connectivity invariants. We discuss implementations of some of these ciphers in the case of arithmetical rings Z_q, $q=2^l$ there.

Section 6 contains conclusive remarks.

2. Linguistic Graphs of Type (1, 1, n-1) and Encryption Schemes

The families of graphs $D(n, K)$ defined over arbitrary commutative ring K are linguistic bipartite graphs of type $(1, 1, n-1)$ with partition sets which are two copies of K^n (see [7] or [15]), i.e. graphs with the incidence $I = I(K) = {}^nI(K)$ between points $(x_1, x_2,..., x_n)$ and lines $[y_1, y_2,..., y_n]$ given by the system of equations $a_2x_2-b_2y_2 = f_2(x_1, y_1)$, $a_3x_3-b_3y_3 = f_2(x_1, x_2, y_1, y_2),..., a_nx_n-b_ny_n = f_2(x_1, x_{2,...,} x_{n-1}, y_1, y_{2,...,} y_{n-1})$ where parameters $a_2, a_{3,...,} a_{n-1}$ and $b_2, b_{3,...,} b_{n-1}$

are taken from the multiplicative group K^* of the commutative ring K. Parameters $\rho((x_1, x_2,..., x_n)) = x_1$ and $\rho([y_1, y_2,..., y_n]) = y_1$ serve as colors of the point and the line. The following linguistic property holds. Each vertex of the graph has a unique neighbor of the chosen color.

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 $m=[3/4n]+c$.

Parameters n and m are equal to some selected constant. the length of the password is another even constant that has an impact on the speed of encryption. Another option to increase the 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 ${}^nI(K)$, $n=2, 3, ...$

Noteworthy that we can expand the defined above $I(K)$ to the infinite linguistic graph $I(K[x_1, x_2,..., x_n])$ defined over the ring $K[x_1, x_2,..., x_n]$ of all multivariate polynomials with coefficients from K and the variables x_i, $I = 1,2,..., n$. So points and lines of this graph are $X = (X_1(x_1, x_2,..., x_n), X_2(x_1, x_2,..., x_n),..., X_n(x_1, x_2,..., x_n)$ and $Y = [Y_1(x_1, x_2,..., x_n), Y_2(x_1, x_2,..., x_n),..., Y_n(x_1, x_2,..., x_n)]$. The incidence of this bipartite graph is given by equations $a_2X_2-b_2Y_2 = f_2(X_1, Y_1)$, $a_3X_3-b_3Y_3 = f_2(X_1, X_2, Y_1, Y_2),..., a_nX_n-b_nY_n = f_2(X_1, X_{2,...,} X_{n-1}, Y_1, Y_{2,...,} Y_{n-1})$, where parameters $a_2, a_{3,...,} a_{n-1}, b_2, b_{3,...,} b_{n-1}$ and polynomials f_i, $I = 2, 3,..., n$ 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 [15]). Take the special point $X = (x_1, x_2,..., x_n)$ of $I(K[x_1, x_2,...x_n])$ and consider the list of colours $g_1(x_1), g_2(x_1), ..., g_t(x_1)$. We compute the path $v_0Iv_1Iv_2...Iv_t$ where $v_0 = X$ and v_{i+1} is the neighbour of v_i with the colour $g_i(x_1)$, $I = 1,2, ..., t$ and $I = I(K[x_1, x_2,..., x_n])$. Then the destination point v_t of this path can be written as $(g_t(x_1), F_2(x_1, x_2), ..., F_n(x_1, x_2,..., x_n))$. The map F is given by the rule $x_1 \to g_t(x_1)$, $x_2 \to F(x_1, x_2),..., x_n \to F(x_1, x_2,..., x_n)$. It is easy to see that $F = F(g_1, g_2,..., g_t)$ 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 ${}^nI(K)$, $n = 2, 3,...$ together with family of affine transformations $T_n \in AGL_n(K)$ can be used as a cipher with the space of plaintexts K^n and the password $g_1(x)$, $g_2(x),..., g_t(x)$ and the encryption map $T_n(F(g_1, g_2,..., g_t)(T_n)^{-1}$.

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

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

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

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

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

DECRYPTION PROCEDURE.

Assume that one of the 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 $a(1) = g_1(r(1))$, $a(2) = g_2(r(1)),...$, $a(t-1) = g_{t-1}(r(1))$ and the completion of the recurrent procedure $v_{t-1} = N_{a(t-1)}(u)$, $v_{t-2} = {}^{a(t-2)}N(v_{t-1})$, $v_{t-3} = N_{a(t-3)}(v_{t-2})$, $v_{t-4} = {}^{a(4)}N(v_{t-3}),...$, $v_1 = N_{a(1)}(v_{t-2})$, ${}^{r(1)}N(v_{4t-1}) = r$.

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

OBFUSCATIONS OF THE ALGORITHM.

O_1. Let us consider the colour jump operator J_a which transforms point $(p_1, p_2,..., p_n)$ of the graph $I(K)$ to the point $(a, p_2, p_3,..., p_n)$.

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

After this change assumption of 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 procedure D_2 and D_3 to get the original plaintext.

O_2. We can use "multiplicative equations" of kind $g(x_1) = b$ where $g:K^*\to K^*$ which has a unique solution if $b\in K^*$. *In* this case, we can use the previous scheme O_1 with T_n such that $T_n^{-1} = (r(1), r(2),\ldots, r(n))$ and $r(1)$ is an element of multiplicative group K^*.

O_3. Let $I(K)$ be a linguistic graph of type $(1, 1, n-1)$. We say that multivariate function f, $f \in K[x_1, x_2,\ldots, x_n]$ is a connectivity invariant of $I(K)$ if $f(x_1, x_2,\ldots, x_n) = f(y_1,y_2,\ldots y_n)$ for each pair of points $(x_1, x_2,\ldots, x_n)$, $(y_1, y_2, \ldots, y_n)$ from the same connected component of the graph $I(K)$. Assume that $f_1, f_2,\ldots, f_t$ are connectivity invariants. We can use functions of kind $g_i(x_1)+f_i(x_1, x_2,\ldots, x_n)$, $I = 1.2,\ldots, t$ instead of g_i in the cases of encryption schemes of type O_2. This idea was proposed in [7] and [33]. We can change points for lines in the definition of connectivity invariant.

O_4. We can take T_1 and T_2 from the group $AGL_n(K)$ and use T_1GT_2 where G is a graph-based transformation.

O_5. Let us assume that $K = Z_q$, $q = 2^m$. We can use graph based transformation G introduced in O_2 given by polynomials $g_1(x_1)$, $g_2(x_1),\ldots, g_t(x_1)$ and function $g(x_1)$ of the "multiplicative equations". Assume the graph $I_n(K)$ has connectivity invariants $f_1, f_2,\ldots, f_{k+1}$ from $K[x_1, x_2,\ldots, x_n]$. We change the colors g_i and g for $h_i = g_i(x_1)+f_i(x_1, x_2,\ldots, x_n)$ and. Let H be the graph-based transformation in terms of $I_n(K)$ and colors h_i and g. Correspondents can work with the graph-based stream cipher defined in terms of the family of graphs $I_n(K)$ and colors $h_i(x)$ and $h(x)$ which has the space of plaintexts $(K^*)^n$, encryption function $E = T_1HT_2$ where T_1, T_2 are elements of $GL_n(K)$ and $T_1(x_1)\in K^*$. Noteworthy that the matrix of the linear transformation T_1 can be constructed as a composition of low triangular matrix $L = (l(i,j))$ $(l(i,j) = 0$ *for* $j>i)$ and an upper triangular matrix $u = (u(i,j))$ $(u(i,j = 0$ for $i > j)$ such that $u(1,1) \in K^*$.

The space of plaintexts can be identified with the $(Z_p)^n$, $p = 2^{m-1}$. The map $\mu: x\to 2x+1$ estabishes the bijection between elements Z_p and $(Z_q)^*$.

Let us assume that Bob creates the plaintext $(p_1, p_2,\ldots, p_n) = v$. He computes v^* as $(\mu(p_1), \mu(p_2),\ldots, \mu(p_n))$ and creates the ciphertext $E(v^*) = c$.

Alice computes $(T_2)^{-1}$ $(c\ ) = (b_1. b_2\ldots,b_m)$. Secondly, she solves for x the equation $g(x) = b_1$. Let $x = x^*$ be the solution.

Alice takes the path in the graph with the starting point $d = (x^*, b_2, b_3,\ldots, b_n) = d$ and consecutive colors $h_t(x^*)$, $h_{t-1}(x^*)$, $h_{t-2}(x^*),\ldots, h_1(x^*)$, x^*. Notice that for the computation of colors, Alice uses the identity $f_i(x_1, x_2,\ldots, x_n) = f_1(x^*, b_2, b_3,\ldots, b_n)$.

The last vertex of the path is $(\mu(p_1), \mu(p_2),\ldots, \mu(p_n))$. Alice applies μ^{-1}, and gets the plaintext.

3. On Families of Algebraic Graphs of Large Girth

3.1. General Remarks

The girth and diameter of a graph are the minimal length of its cycle and the maximal distance of the graph. The construction of finite or infinite graphs with prescribed girth and diameter is an important and difficult task of 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 generalized m-gons as bipartite graphs of girth $2m$ and diameter m. Feit and Higman proved that finite generalized 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 generalized m-gons for $m = 3, 4, 6, 8$. Classification of flag transitive generalized m-gons of Moufang type was 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 an infinite family of small world graphs of bounded degree turns out to be very important for various applications of graph theory.

Noteworthy that 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 [8] and investigated via the computation of their girth, diameter, and the second largest eigenvalue by A. Lubotsky, R.Phillips and P.Sarnak [9].

We have to admit that studies of families of graphs Γ_i with well-defined projective limit Γ, which is isomorphic to an infinite tree, are 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 of whether or not *CD(n, q)* forms a family of small world graphs has been still open since 1995.

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 anti-reflexive binary relation on $V(\Gamma)$, i.e. $E(\Gamma)$ is a subset of $V(\Gamma)\times V(\Gamma)$. The length of a path is the 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 the maximal distance between its vertices.

The graph is connected if its diameter is finite. The 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 $diam\ (\Gamma_i)\leq clog_{k-1}(v_i)$, where c is the independent of i constant and $diam\ (\Gamma_i)$ is the 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 $g(\Gamma_i)\geq clog_{k-1}(v_i)$, 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. The projective limit of graphs Γ_i is well defined and coincides with the q-regulate tree T_q.

We refer to a family of graphs Γ_i satisfying condition (iii) as *tree approximation.* We know examples 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 [8] and investigated by A. Lubotzky, Sarnak, and Phillips [9]. As it is easy to see the projective limit of *X(p, q)* does not exist.

3.3. Graphs *D(n, K)*

Graphs *D(n, q) introduced in* [2] defines projective limit *D(q)* which is an infinite bipartite graph with partition sets formed by two infinite vector spaces over the finite field F_q_formed by points $(p) = (p_{01}, p_{11}, p_{12}, p_{21}, p_{22}, p'_{22}, \ldots, p'_{ii}, p_{i\,i+1}, p_{i+1,i}, p_{+i+1,i+1} \ldots)$ and 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}-$p_{i+1,I} = l_{10} p'_{ii}$.

These 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.*

Graph *D(n, q)* are bipartite graphs with the partition sets $(F_q)^n$ formed by the projections of points and lines of *D(q)* onto their first n coordinates and incidence given by first $n-1$ equations in the definition of *D(q).*

Historically graph *D(q)* is not the first example of a description of q-regular forest in terms of Algebraic Geometry. Geometries of buildings (see [10] and further references) correspond

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 [11] 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 [6], [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 $4/3$. So exact computation of the girth is the area of future research. There are essential differences between the family of graphs $X(p, q)$ and tree approximations. Recall that the projective limit of $X(p, q)$ does not exist.

Families $X(p, q)$ *and* $CD(n, q)$ can be used for the construction of LDPC codes for noise protection in satellite communications. D. MacKay and M. Postol [12] proved that $CD(n, q)$ based LDPC codes have better properties than those from $X(p, q)$ for the constructions of LDPC codes.

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

3.4. On the Equations for Graphs *CD(n, K)*

We can see that graphs $D(n, q)$ are defined as bipartite graphs with the partition sets $(F_q)^n$ via the system of homogeneous polynomial equations with nonzero coefficients 1 and -1.

Let K stand for an arbitrary commutative ring. We can introduce graphs $D(n, K)$ via a simple change of vector space $(F_q)^n$ on free modules K^n and the use of the same equations (see [4]–[5]).

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 [4]–[5] 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 $[2, t]$.

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 [5] graphs $D(n, K)$ are edge transitive. So their connected components are isomorphic graphs. Let ${}^vCD(k, K)$ be a solution set of a 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 ${}^vCD(k, K)$ is the disjoint union of some connected components of graph $D(n, K)$.

It is easy to see that sets of vertices of ${}^vCD(k, K)$, $v \in K^{t-1}$ form partitions of the vertex set of $D(n, K)$. We consider more general graphs ${}^vCD\_J(k, K)$ 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 ${}^vCD_J(k, K)$ as the 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* ${}^vCD_J(K)$ of $D(K)$. Noteworthy that in the case of a finite commutative ring ${}^vCD_J(K)$ 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 [13]). So graph

$CD(n, q) = CD(n, F_q)$ for odd q is a connected component of $D(n, q)$.

Theorem [5]. *For each commutative integrity ring K with at least 3 elements the families of graphs D(n, K), n = 2,3, … are forest approximations and families of graphs of large girth.*

4. On the Description of Selected Bijective Multivariate Maps of Some Ciphers 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 ensures that in the case of a constant passive password, the single change of a single character of an active password leads to a change of the ciphertext produced from the selected plaintext. We choose an affine transformation T in the form of a 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 an explicit description of linguistic graphs $D(n, K)$ is given in the previous section and the general encryption algorithm is described in section 2. So, ciphers $T\,E(n, K)\,T^{-1}$ have a 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 $p'_{33} = a_3(p_{01}, p_{11}, p_{12}, p_{21}, p_{22}, p'_{22}, p_{2,3}, p_{3,2}, p_{3,3}\, p'_{3,3})-h_3+p'_{33} = b_3(p_{01}, p_{11}, p_{12}, p_{21}, p_{22}, p'_{22}, p_{2,3}, p_{3,2}, p_{,33}), ..., p'_{tt}=a\_t(p_{01}, p_{11}, p_{12}, p_{21}, p_{22}, p'_{22}, ..., p'_{t-1,t-1}, p_{t-1,\,t}, p_{t,\,t-1}, p'_{t,\,t})-h_t+p'_{t,t} = b_t(p_{01}, p_{11}, p_{12}, p_{21}, p_{22}, p'_{22}, ..., p'_{t-1,t-1}, p_{t-1,\,t}, p_{t,\,t-1}, p_{t,\,t})$.

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 the corresponding cipher has the space of plaintexts K^{n-t}. We use active passwords $(b(1), b(2),..., b(k), a(1), a(2), ..., a(k))$ and 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 $TCE(n, K)T^{-1} = T_nF(g_1, g_2,..., g_t)J_g(T_n)^{-1}$.

We will use the 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 map $TE(n, K)T^{-1}$ independently on the choice of active and passive passwords have multivariate encryption and decryption functions of degree 3. In [31] the linearisation attacks on these ciphers with the interception of $O(n^3)$ pairs plaintext/ciphertext 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 $D: x\rightarrow x^e$ leads 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 the 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 [32] (ust wroblevskska) the encryption function corresponding to the selected active password has a degree $[(n+2)/4]+2$. So the generation of a standard form for the encryption function can not be done in polynomial time.

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

We can use induced graphs ${}^{v}CD_{J}(k, K)$ of graphs $D(n, K)$ which are J-components of them where $J = J(n) = \{i(1), i(2), ..., i(t(n))\}$ is the subset of $\{2, 3,..., [(n+2)/4]\} = M(n)$ and tuples $(v_{i(1)}, v_{i(2)},..., v_{j(t(n))})$ 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 $<x> = <x_1, x_{1,1}, x_{12}, x_{2,1}, x_{2,2}, x_{2,2}, x_{2,3}, x_{32}, x_{3,3}, x'_{33},..., x_{i,i}, x_{i,i+1}, x_{i+1,i+1}, x'_{i+1,i+1}, ...>$, $3 \le i \le [(n+2)/4-1]$ (point or line) of $D(n, K)$ given by the list $x'_{i(k),i(k)}$, $k = 2, 3,..., t(n)$. 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 sets of points and lines isomorphic to the affine space K^{l} where $l = n\text{-}t(n)$.

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 $1, 2,..., n\text{-}k$. So $x = (x_1, x_2,..., x_{n-t(n)})$.

The nonlinear graph-based transformation N is the following one.

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

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

We also will use the obfuscation ${}^{g}N((x_1, x_2,..., x_{n-t}) = (g(x_1), w_2,..., w_{n-t})$, 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 the coordinates of a general point (x) are variables $x_1, x_2,..., x_{n-t}$. We consider the multivariate ring $K[x_1, x_2,..., x_{n-t}]$ and the graph ${}^{v}CD_{J}(K[x_1, x_2,..., x_{n-t}])$ with points and lines of kind $<g_1, g_2,..., g_{n-t}>$, $g_i \in K[x_1, x_2,..., x_{n-t}]$.

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

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

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

As it follows from [32] the maximal degree of F_i is $t(n)+2$.

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

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

Parameters $m(1), m(2)..., m(n\text{-}t\text{-}1)$ together with $J = \{i(1), i(2),..., i((t(n))$ form the passive password. We assume that constants k and $t(n) = t$ can be agreed by correspondents via an open channel. Under the 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 the weight parameter $w = i(1)+i(2)+...+i(m)$.

The following important property holds. The change of the active password leads to the

change of the ciphertext for the selected plaintext. It means that a brute 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.

5. The Implemented Case of Non-Bijective Multivariate Graph-Based Maps

In this section, we concentrate on the case of commutative ring $K = Z_q$, $q = 2^l$, $l \geq 8$.

We modify the ciphers ${}^kED_t(m, K)$, $m = n-t$ with the active password $(\alpha(1), a(2),..., a(k), \beta(1), \beta(2),..., \beta(k))$, $v_{i(1)}, v_{i(2)},..., v_{j(d(n))}$ and the passive password defined by nonzero parameters $m(1), m(2)..., m(n-d(n)-1)$ together with the set $J = \{i(1), i(2),..., i((d(n))\}$ accordingly the special case of the scheme O_5 given in the Section 2.

Recall that the description of the generic connectivity invariants of $D(n, K)$ is given via expressions $a_r = a_r(u) = \Sigma_{i=0,r}(u_{ii}\, u'_{r-i,\, r-i}u_{i,i+1}\, u_{r-i,r-i-1})$ considered for every r from the interval $[2, k]$ where $k = [(n+2)/4]$.

It means that we can take arbitrary element F from $K[y_2, y_3,..., y_k]$, consider a symbolic vertex $(x) = <x_1, x_{1,1}, x_{12}, x_{2,1}, x_{2,2}, x_{2,2}, x_{2,3}, x_{32}, x_{3,3}, x'_{33},..., x_{i,i}, x_{i,i+1}, x_{i+1,i+1}, x'_{i+1,i+1}, ...>$ and gets the connectivity invariant $F(a_2(x), a_3(x),..., a_k(x))$.

Recall that the induced graph ${}^vCD_J(n, K)$ was obtained via the restriction of the incidence relation of the bipartite graph $D(n, K)$ onto the solutions set of equations $a_{i(k)}(<x>) = v_i(k)$. We can get recursively the variables $x'_{i(s),i(s)}$, $s = 1, 2,..., d(n)$ from these equations as quadratic expressions b_i in variables of $\{x_1, x_{1,1}, x_{12}, x_{2,1}, x_{2,2}, x_{2,2}, x_{2,3}, x_{32}, x_{3,3}, x'_{33},..., x_{i,i}, x_{i,i+1}, x_{i+1,i+1}, x'_{i+1,i+1}, ...\}$-$\{x'_{(1),i(1)}, x_{i(2),i(2)},..., x_{d(n),d(n)}\}$.

It means that generic connectivity invariants of the graph ${}^vCD_J(n, K)$ can be obtained via consideration of $J^* = \{2, 3,..., m\}$-J as the specialization A_j of a_j, $j \in J^*$ via the substitutions $x'_{ii} = b_i$, $i \in J$.

Let $J^* = \{j(1), j(2),..., j(s)\}$, $s = m-d(n)$. The general connectivity invariant is $F(A_{j(1)}, A_{j(2)},..., A_{j(s)})$ where F is a polynomial function in s variables $z_1, z_2,..., z_s$. Notice that F can be an expression of any even degree in variables $x_1, x_{1,1}, x_{12}, x_{2,1}, x_{2,2}, x_{2,2}, x_{2,3}, x_{32}, x_{3,3}, x'_{33},..., x_{i,i}, x_{i,i+1}, x_{i+1,i+1}, x'_{i+1,i+1}, ...$

We use forms $F(z_1, z_2,..., z_s)$ of connectivity invariants with density $O(1)$ and degree $O(n)$. In this case, the connectivity invariant can be computed in time $O(n)$.

Algorithm 1

Assume that one of the correspondents (Alice) creates the map. She selects the parameters n, m, the commutative ring K with at least 2 regular elements, the set $J = \{i(1), i(2),..., i((d(n))\}$ and the tuple of parameters $(v_{i(1)}, v_{i(2)}, ..., v_{i(d(n))})$. These parameters allow us to write down the linguistic equations of graphs ${}^vCD_J(n, K)$.

Alice uses the scheme O_5 with the following changes of the symbolic path in the graph ${}^vCD_J(n, K[x_1, x_{1,1}, x_{1,2}, x_{2,1}, x_{22}, ...]$ to make a difference with the case of cipher ${}^kED_t(m, K)$, $m = n-t$.

She takes two expressions $F_1, F_2 = K[z_1, z_2, ..., z_s]$, $s = m-d(m)$ of density $O(1)$ and linear degree $O(n)$. Alice works with $J^* = \{j(1), j(2),..., j(s)\}$, she forms the connectivity invariants $F_1(A_{j(1)}, A_{j(2)},..., A_{j(s)}) = G_1(x)$ and $F_2(A_{j(1)}, A_{j(2)},..., A_{j(s)}) = G_2(x)$. Similarly to the case of the cipher ${}^kED_t(m, K)$, $m = n-t$. Alice takes tuples of odd residues $b(1), b(2), ...,b(k), a(1), a(2),...,a(k)$, $k = t/2$ 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 and $c(i) = c(i-2)=a(i)$ if i, $i \geq 4$ is even. She constructs g_i, $I = 1, 2,..., t$ of the scheme O_5 as $g_i = x_i+G_1(x)+c_i$ for odd i, $g_i = x_1+G_2(x)+c_i$ for even I and takes linear g(x) of kind ax+b, where a$\in$K*'.

Algorithm 2

Correspondents select the commutative ring $K = Z_q$, $q = 2^l$, $l \geq 8$. They modify the previous algorithm via a selection of g in terms of O_5 in the form x^3+b for some b from K.

Noteworthy that $x^3 = d$ has a unique solution if $d \in K^*$ because 3 is mutually prime with $\varphi(2^l)$ where φ is the Euler function.

For the encryption and decryption Alice uses the standard procedures of O_5.

Let N = N($b(1), b(2), ..., b(k), a(1), a(2), ..., a(k), J, v_{i(1)}, v_{i(2)}, ..., v_{i(d(n))}$. F_1, F_2) stands for the described above encryption function. We use linear transformation T_1 and T_2 of kind $T_i(x_1) = x_1+ {}^im(2)x_2+{}^im(3)x_3+...+{}^im(n)x_n$, $I = 1, 2$ such that ${}^im(2)+{}^im(3)+...+{}^im(n)$ is an even parameter to form the encryption map ${}^3E(n, Z_q) = T_1\, N\, T_2$.

We assume that tuples $(b(1), b(2), ..., b(k), a(1), a(2),..., a(k))$ and $v_{i(1)}, v_{i(2)}, ..., v_{i(d(n))}$ form active password of ${}^3E(n, Z_q)$.

Forms F_i, $I = 1, 2$ together with parameters $n, q, {}^{i}m(2), {}^{i}m(3),\ldots,{}^{i}m(n)$ form a passive part of the password.

Alice selects passive and active passwords and delivers them to his correspondent Bob via a secure channel.

Remark 1

One of the option to use connectivity invariants $Fi.$, $I = 1, 2$ is to use of the forms $F_i(z_1, z_2,\ldots, z_s)$ of kind $(z_{k(1)})^{t(1)}\ (z_{k(2)})^{t(2)}\ldots(z_{k(r)})^{t(r)}$ for which $t(1)+k(2)+\ldots+k(r)$, $r\geq 1$ has linear size αn, $\alpha>0$ and $r=0(1)$.

Remark 2

Selection of forms F_i of linear degree ensures that the multivariate standard form of the encryption map has a degree at least αn, $\alpha>0$. The use of cubical map g guarantees that the degree of decryption is higher than the degree of encryption transformation.

Similarly to the algorithm described in the previous section described above assumptions ensure that the 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 $w = i(1)+i(2)+\ldots+i(d(n))$ and selection of forms F_i, $I = 1, 2$.

As in the case of ${}^{k}ED_t(m, K)$ the change of the active password leads to the change of the ciphertext for the selected plaintext. It means that a brute force attack on the cipher requires $p^{2k}q^{d(n)}$ elementary operations where $p = 2^{l-1}$ and $q = 2^{l}$.

Implementation

We implement the cipher ${}^{3}E(n, Z_q)$ *with* $q = 256$. *So the space of plaintexts is an affine space over* Z_{128} *and* $d(n) = 128$ with weights $w = 2^{13}$ and 2^{16}. In both cases, the degree of encryption map will be at least 256. So the linearisation attacks by adversaries are unfeasible.

CRYPTALL 7 software is written in C++ programming language and therefore it is portable and runs on many platforms such as Unix/Windows. The context diagram is depicted in Fig. 1. The friendly interface allows users to enter active and passive passwords of selected length. The program is supported by a key exchange protocol based on Eulerian transformations of Z^*_{256} [36]. This is one of the protocols of Noncommutative cryptography ([37–51] for the description of the area and [52–57] for the cryptanalytical studies).

The protocol allows the elaboration of the tuple of nonzero field elements of Z_{128} of length $2k$ together with the tuple of elements from Z_{256} of length 128 to form both passwords.

Experimental Measurements

To evaluate the performance of our algorithm, we use different sizes of files. We denote by $t\ (k, L)$ the time (in milliseconds) 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. 1 and Fig. 2).

L\k	3000	4000	5000	6000
4	1388.00	1864.00	2132.25	2575.00
8	2625.75	3641.50	4192.25	5039.25
12	3728.50	4988.25	6146.00	7350.00
16	4967.00	6592.50	8103.50	9648.25
20	6231.25	8231.50	10082.25	11989.75

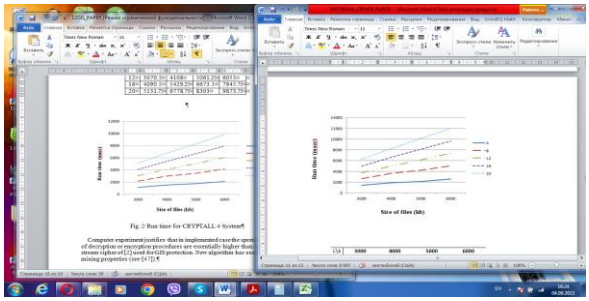

Figure 1: Run time for CRYPTALL 7 System

L\k	3000	4000	5000	6000
4	1796.25	2412.25	2759.25	3332.50
8	3398.00	4714.00	5425.25	6521.25
12	4825.25	6455.25	7953.50	9511.75
16	6427.75	8531.50	10486.75	12486.00
20	8064.00	10652.50	13047.75	15516.00

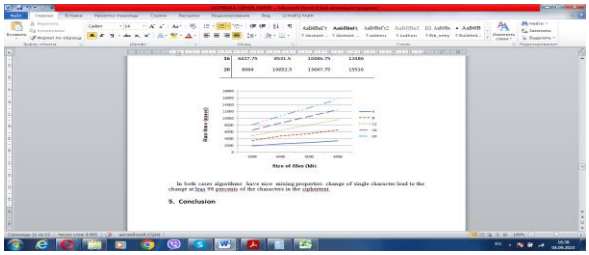

Figure 2: Run time for CRYPTALL 8 System

In both cases, algorithms have nice mixing properties. change of a single character leads to the change of at least 98% of the characters in the ciphertext.

6. Conclusion

The first result of the paper (Algorithm 1) is the explicit construction of the family of multivariate maps of affine maps F_n of linear degree $s(n) = cn$, $c>0$ based on the graphs $D(n, K)$ with the trapdoor accelerator. F_n acts on the affine space K^n defined over an arbitrary commutative ring K with at least 3 elements. The execution speed of the algorithm with encryption function is $O(n)$. It depends on active password A = ($a(1), a(2),..., a(k), b(1), b(2),..., b(k), v_1, v_2, ..., v_s$) from $(K^*)^{2k}K^s$ where parameters k and s can be selected by users. Let $p = |K^*|$, $q = |K|$.

Different active passwords produce distinct ciphertexts from the same plaintext. It means that the adversary's direct attack costs $p^{2k}q^s$ attempts. Correspondents can govern the security via a choice of parameters k and s.

The map F_n is multivariate. Its degree d depends from the choice of degrees $d(1)$ and $d(2)$ of F_1 and F_2 from $K[z_1, z_2, ..., z_l]$, $l = [(n+2)/4]-s$ and parameter s. We can justify that $d = 4d(1)+2d(2)+s$ is a degree of encryption and decryption maps. It means that users can select F_1 and F_2 of prescribed degrees and control the parameter d. Constructed trapdoor accelerator consists of active password A, maps $F_1, F_2, g(x)\epsilon K[x]$, $g(x) = ax+b$, $a\epsilon K^*$ and two affine transformations T_i, $I = 1, 2$.

If d is sufficiently large then the computation of the standard form of F_n is an unfeasible task. So this cipher is resistant to linearisation attacks by adversaries.

The important feature of this algorithm is the linear execution speed of size $O(n)$. So this method of encryption can be used for the processing of Big Data.

Another cipher described as Algorithm 2 is an obfuscation of Algorithm 1 obtained via the change of linear $g(x)$ of scheme O_5 for $g(x)$ of kind x^t+b such that $(t, p) = 1$, $t\le 4d(1)+2d(2)+s$. This modification can be implemented in the case of commutative ring K with at least 3 regular elements. The active password, transformations F_1, F_2, and T_2 are unchanged, but T_1 has to satisfy the condition $T(x_1)\epsilon K^*$. The space of plaintexts of the new algorithm is $(K^*)^{n-s}$ but the space of ciphertexts is K^{n-s} as in the case of Algorithm 1.

Algorithms 1 and 2 have the same degree of encryption map, but the nonlinear nature of $g(x)$ increases the degree of the decryption map.

We implement Algorithm 2 in the practically important case of $K = Z_q$, $q = 2^l$. In this case, the space of plaintexts is isomorphic to $(Z_p)^{n-s}$, $p = 2^{l-1}$.

We use loaded multiplication tables for K^*. These tables increase the speed of computations and make immaterial the computational difference between cases of fields F_q and arithmetical rings Z_q. Suggested ciphers have good mixing properties, the change of a single character of the active password leads to the change of 98% of characters of ciphertext produced from the selected plaintext.

We hope that new flexible algorithms with resistance to linearization attacks and linear speed of encryption will be successfully used for the protection of Information systems and Big Data Processing.

7. Acknowledgments

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

References

[1] V. Ustimenko, CRYPTIM: Graphs as tools for symmetric encryption, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (2001) 278-286. doi:10.1007/3-540-45624-4_29.

[2] F. Lazebnik, V. Ustimenko (1993). Some Algebraic Constractions of Dense Graphs of Large Girth and of Large Size, DIMACS Series Discrete Math. Theoretical Comput. Sci. 10 (1993) 75–93. doi:10.1090/dimacs/010/07.

[3] F. Lazebnik, V. Ustimenko, A. Woldar, A New Series of Dense Graphs of High Girth, Bull. Amer. Math. Soc. 32(1) (1995) 73–79. doi:10.1090/S0273-0979-1995-00569-0.

[4] V. Ustimenko, Coordinatisation of Trees and their Quotients, Voronoj's Impact on Modern Science 2 (1998) 125–152.

[5] V. Ustimenko, Linguistic Dynamical Systems, Graphs of Large Girth and Cryptography, J. Math. Sci. 140(3) (2007) 412–434. doi: 10.1007/s10958-007-0453-2.

[6] V. Ustimenko, A. Woldar, A Characterisation of the Components of the Graphs D(k,q), Discret. Math. 157(1-3) (1996) 271–283. doi: 10.1016/S0012-365X(96)83019-6.
[7] V. Ustimenko, Maximality of Affine Group, Hidden Graph Cryptosystem and Graph's Stream Ciphers, J. Algebra Discret. Math. 1 (2005) 51–65.
[8] G. Margulis, Explicit Group-Theoretical Constructions of Combinatorial Schemes and Their Application to Design of Expanders and Concentrators, Probl. Inf. Transm. 24(1) (1988) 51–60.
[9] A. Lubotsky, R. Philips, P. Sarnak, Ramanujan Graphs, J. Comb. Theory 115(2) (1989) 62–89. doi: 10.1007/BF02126799.
[10] F. Buekenhout, Handbook in Incidence Geometry, North Holland, Amsterdam (1995).
[11] V. Ustimenko, Affine system of roots and Tits geometries, Voprosy Teorii Grupp i Gomologicheskoy Algebry, Yaroslavl (1989) 155–157.
[12] D. MacKay, M. Postol, Weakness of Margulis and Ramanujan—Margulis Low Dencity Parity Check Codes, Electronic Notes Theor. Comput. Sci. 74 (2003) 97–104. doi:10.1016/S1571-0661(04)80768-0.
[13] V. Ustimenko, Algebraic Groups and Small World Graphs of High Girth, Albanian J. Math. 3(1) (2009) 25–33. doi: 10.51286/albjm/1236885681.
[14] V. Ustimenko, On Extremal Algebraic Graphs and Multivariate Cryptosystems, Cryptol. ePrint Arch. reprint (2022).
[15] V. Ustimenko, Graphs in Terms of Algebraic Geometry, Symbolic Computations and Secure Communications in Post-Quantum World, Editorial House of University of Maria Curie, Lublin (2022).
[16] N. Geetha, V. Ragavi, Graph Theory Matrix Approach in Cryptography and Network Security, Algorithms, Comput. Math. Conf. (ACM), (2022). doi: 10.1109/acm57404.2022.00025.
[17] A. Costache, et al., Ramanujan Graphs in Cryptography. Research Directions in Number Theory, Association for Women in Mathematics Series 19 (2019) 1–40. doi:10.1007/978-3-030-19478-9_1.
[18] P. Priyadarsini, A Survey on some Applications of Graph Theory in Cryptography, J. Discret. Math. Sci. Cryptogr. doi: 10.1080/09720529.2013.878819.
[19] W. Etaiwi, Encryption Algorithm Using Graph Theory, J. Sci. Res. Rep. 3(19) (2014) 2519–2527. doi: 10.9734/jsrr/2014/11804.
[20] S. Gideon, Denial Cryptography based on Graph Theory. URL: http://www.patentstorm.us/patents/6823068.html
[21] L. Mittenthal, Sequencings and Directed Graphs with Applications to Cryptography, Sequ. Subseq. Consequences (2007) 70–81. doi: 10.1007/978-3-540-77404-4_7.
[22] M. Naor, A. Shamir, Visual Cryptography. In Advances in Cryptology—EUROCRYPT'94 (1994) 1–12. doi: 10.1007/BFb0053419.
[23] S. Lu, D. Manchala, R. Ostrovsky, Visual Cryptography on Graphs, COCOON (2008) 225–234.
[24] W. Stallings, Cryptography and Network Security Principles and Practices, Prentice Hall India (2006).
[25] D. Song, D. Zuckerman, J. Tygar, Expander Graphs for Digital Stream Authentication and Robust Overlay Networks, IEEE Symposium on Security and Privacy (2002). doi: 10.1109/SECPRI.2002.1004376.
[26] M Yamuna, et al., Encryption Using Graph Theory and Linear Algebra, Int. J. Comput. Appl. 5(2) (2012) 102–107.
[27] A Paszkiewicz et al., Proposals of Graph Based Ciphers Theory and Implementations, Research Gate, (2001).
[28] B. Cusack, E. Chapman, Using Graphic Methods to Challenge Cryptographic Performance, 14th Australian Inf. Secur. Manag. Conf., (2016) 30–36. doi: 10.4225/75/58a6991e71023.
[29] E. Chapman, Using Graphic Based Systems to Improve Cryptographic Algorithms. Ph.D. Thesis, Auckland University of Technology (2016).
[30] E. Kinani, Fast Mapping Method Based on Matrix Approach For Elliptic Curve Cryptography. Int. J. Inf. Netw. Secur. 1 (2012) 54–59.
[31] M. Klisowski, Zwiększenie Bezpieczeństwa Kryptograficznych Algorytmów

Wielu Zmiennych Bazujących na Algebraicznej Teorii Grafów, Rozprawa Doktorska, Politechnika Częstochowska, Częstochowa (2014).
[32] V. Ustimenko, A. Wroblewska, On the Key Exchange and Multivariate Encryption with Nonlinear Polynomial Maps of Stable Degree, Ann. UMCS, Inf. 13(1) (2013) 63-80. doi: 10.2478/v10065-012-0047-6.
[33] V. Ustimenko, Graphs with Special Arcs and Cryptography, Acta Applicandae Math. 74 (2002) 117–153. doi: 10.1023/a:1020686216463.
[34] V. Ustimenko, Random Walks on graphs and Cryptography, Extended Abstracts, AMS Meeting (1998).
[35] V. Ustimenko, et al., On the Constructions of New Symmetric Ciphers Based on Non-Bijective Maps of Prescribed Degree, Secur. Commun. Netw. (2019). doi: 10.1155/2019/2137561.
[36] V. Ustimenko, On Eulerian Semigroups of Multivariate Transformations and Their Cryptographic Applications, European J. Math. (2023). doi: 10.1007/s40879-023-00685-2.
[37] D. Moldovyan, N. Moldovyan, A New Hard Problem over Non-commutative Finite Groups for Cryptographic Protocols, Int. Conf. Math. Method. Model. Archit. Comput. Netw. Secur. (2010) 183–194. doi: 10.1007/978-3-642-14706-7_14.
[38] L. Sakalauskas, P. Tvarijonas, A. Raulynaitis, Key Agreement Protocol (KAP) Using Conjugacy and Discrete Logarithm Problem in Group Representation Level, INFORMATICA 18(1) (2007) 115–124. doi: 10.15388/informatica.2007.167.
[39] V. Shpilrain, A. Ushakov, The Conjugacy Search Problem in Public Key Cryptography: Unnecessary and Insufficient, Appl. Algebra Eng. Commun. Comput. 17(3–4) (2006) 285–289. doi: 10.1007/s00200-006-0009-6.
[40] D. Kahrobaei, B. Khan, A Non-Commutative Generalization of ElGamal Key Exchange Using Polycyclic Groups, IEEE GLOBECOM 2006—2006 Global Telecommunications Conference. doi: 10.1109/GLOCOM.2006.
[41] A. Myasnikov, V. Shpilrain, A. Ushakov, Group-based Cryptography, Berlin: Birkhäuser Verlag (2008).
[42] Z. Cao, New Directions of Modern Cryptography, Boca Raton: CRC Press, Taylor & Francis Group (2012).
[43] B. Fine, et al. Aspects of Non Abelian Group Based Cryptography: A Survey and Open Problems, arXiv.
[44] A. Myasnikov; V. Shpilrain, A. Ushakov, Non-commutative Cryptography and Complexity of Group-theoretic Problems, Math. Surveys Monographs 177 (2011). doi: 10.1090/surv/177.
[45] I. Anshel, M. Anshel, D. Goldfeld, An Algebraic Method for Public-Key Cryptography, Math. Res. Lett. 6(3–4) (1999) 287–291. doi: 10.4310/mrl.1999.v6.n3.a3.
[46] S. Blackburn, S. Galbraith, Cryptanalysis of Two Cryptosystems Based on Group Actions. Cryptology—ASIACRYPT'99 (1999) 52–61.
[47] K. Ko, et al., New Public-Key Cryptosystem Using Braid Groups. Cryptology—CRYPTO (2000) 166–183.
[48] G. Maze, C. Monico, J. Rosenthal, Public Key Cryptography Based on Semigroup Actions, Adv. Math. Commun. 1(4) (2007) 489–507. doi: 10.3934/amc.2007.1.489.
[49] P. Kropholler, S. Pride, et al., Properties of Certain Semigroups and Their Potential as Platforms for Cryptosystems, Semigroup Forum 81 (2010) 172–186. doi: 10.1007/s00233-010-9248-8.
[50] J. Lopez-Ramos, et al., Group Key Management Based on Semigroup Actions, J. Algebra Appl. 16(08) (2017). doi: 10.1142/s0219498817501481.
[51] G. Kumar, H. Saini, Novel Noncommutative Cryptography Scheme Using Extra Special Group, Secur. Commun. Netw. (2017). doi: 10.1155/2017/9036382.
[52] A. Myasnikov, V. Roman'kov, A Linear Decomposition Attack, Groups Complex. Cryptol. 7 (2015) 81–94. doi: 10.1515/gcc-2015-0007.
[53] V. Roman'kov, A Nonlinear Decomposition Attack, Groups Complex. Cryptol. 8(2) (2017) 197–207. doi: 10.1515/gcc-2016-0017.

[54] V. Romankov, Two General Schemes of Algebraic Cryptography, Groups Complex. Cryptol. 10(2) (2018) 83–98. doi: 10.1515/gcc-2018-0009.
[55] V. Roman'kov, An Improved Version of the AAG Cryptographic Protocol, Groups Complex. Cryptol. 11(1) (2019). doi: 10.1515/gcc-2019-2003.
[56] B. Tsaban, Polynomial Time Solutions of Computational Problems in Noncommutative Algebraic Cryptography, J. Cryptol. 28(3) (2015) 601–622. doi: 10.1007/s00145-013-9170-9.
[57] A. Ben-Zvi, A. Kalka, B. Tsaban, Cryptanalysis via Algebraic Spans, Cryptology—CRYPTO (2018) 1–20.