Implementation of New Families of Graph-based Stream Ciphers with the Hidden Multivariate Nature

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

We present two families of new ciphers with the spaces of plaintexts of kind K^{n-r}, $K = F_q$ or $K = Z_q$, $q = 2^s$ and the variety of active passwords of kind A, $(\alpha_1, \alpha_2, \dots\alpha_r) \in K^r$, $(\beta_1, \beta_2,\dots,\beta_t) \in (K^*)^t$, where A is a subset of cardinality r of the set $\{1, 2, \dots, [(n+2)/4]-1\}$ car, $r<[(n+2)/4]$, even $t<[n+5]/2]$. It is proven that different active passwords produce distinct ciphertexts from the same plaintext. If freely selected parameters r and t have size $O(1)$ then the execution speed of the cipher is $O(n)$. These families of encryption maps are defined in terms of well-known algebraic graphs $D(n, K)$ which form a family of graphs of large girth in the case when K is a finite field. The encryption map is defined as a combination of the graph-based encryption and two polynomial transformations of $(Z_d)^{n-r}$ $d = 2^{s+1}$ preserving $(Z^*_d)^{n-r}$ and acting naturally on K^{n-r}. This trick does not allow to interpretation of the encryption map as a multivariate transformation over some commutative ring. It prevents linearization attacks by adversaries. We can change the defined above commutative rings F_q and $K = Z_q$ for Boolean ring B_s of size 2^s and obtain the third stream cipher with similar properties.

Keywords

Post-quantum cryptography, stream ciphers, graph-based cryptography, hidden algebraic maps, regular forest approximations, extremal graph theory.

1. Introduction

Everybody knows that each computation can be defined in terms of finite automaton, a roughly directed graph with labels on arrows, various applications of automata theory to cryptography are very hard to observe. So Graph Based Cryptography is a natural direction of research. It is used for the key exchange, development of Multivariate Public Keys, key-dependent message authentication codes, and algorithms of Noncommutative Cryptography [3–17].

Especially 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. The monograph [1] and papers [2, 40] reflect some 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 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 the corresponding cipher.

Several known ciphers based on algebraic graphs 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 according to the rule $(x_1, x_2, \dots, x_n) \to (f_1(x_1, x_2, \dots, x_n), f_2(x_1, x_2, \dots, x_n), \dots, f_n(x_1, x_2, \dots, x_n))$, where f_i are given via corresponding list of

CPITS-2024: Cybersecurity Providing in Information and Telecommunication Systems, February 28, 2024, 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)

monomial terms. Trapdoor accelerator [41] 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 ciphers based on algebraic graphs correspondents Alice and Bob share 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 has to intercept large amounts of pairs of plaintext/corresponding ciphertext and try to approximate multivariate maps F^{-1} and F. So degree of F is an important parameter for the cryptanalytical studies. The most important (active) part of the password is the information about the walk in the algebraic graph.

The first construction of graph-based stream cipher of multivariate nature based on algebraic approximations of q-regular tree or forest where q is a prime power was presented in [42] or [43]. The first implementation of these algorithms appeared at the beginning of 2001 [44].

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 various 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 development of some graph-based ciphers. The survey of known $D(n, K)$ based stream ciphers reader can be found in [1–2] or [40] where several encryption schemes of a multivariate nature were described.

In this paper we construct the modification of stream cipher suggested in [40] such that the encryption map is the conjugation of kind $F = YXY^{-1}$ of multivariate map X defined on the affine space $V = K^n$ where K is $F_{2^{s-1}}$, $Z_{2^{s-1}}$ or Boolean ring B_{s-1} of size 2^{s-1} and multivariate map Y acting on affine space $(Z_{2^s})^n$ of Eulerian type. The map Y preserves the variety$(Z^*_{2^s})^n$ which can be identified with K^n via the natural bijection between these sets.

The encryption map F cannot be interpreted as a multivariate map over a single commutative ring. Thus multivariate linearization attacks are not feasible.

The cipher has a large space of active passwords such the different passwords produce distinct ciphertexts from the chosen plaintext.

In Section 2 we discuss the general schemes of three stream ciphers in the different cases of commutative ring.

Section 3 is dedicated to tame Eulerian transformations which will be used as maps Y in the above scheme.

In Section 4 we consider trapdoor accelerators T of multivariate ciphers based on linguistic graphs of type $(1, 1, n-1)$ defined over the commutative ring K. The map $X = X_T$ can be used in the composition YXY^{-1}.

Ciphers constructed in terms of linguistic graphs $D(n, K)$ and their connected components are presented in section 5.

Section 6 is dedicated to combinations of Eulerian tame transformations with the ciphers defined in Section 5. We present the evaluation of the execution speed of chosen cases of implementations. Results of computer simulations are presented in Tables 1 and 2 and Figs. 1 and 2.

Section 7 contains conclusive remarks and suggestions of supporting protocols of Noncommutative Cryptography (NC) suggested in [45–46]. Of course, other postquantum secure protocols of NC can be used. This area is developing very fast [18–39].

2. General Schemes of Families of Stream Ciphers

The idea to combine general bijective multivariate map E of bounded degree with Eulerian transformation ψ sending each variable x_i into the monomial term for getting $x \rightarrow E(\psi(x))$ was considered in [47–48]. If the restriction of ψ onto $(K^*)^n$ acts bijectively on this set then the transformation E maps $(K^*)^n$ to K^n injectively. So E can be used as an encryption map with the space of plaintexts $(K^*)^n$ and the space of ciphertext K^n.

The case of $K = Z_{2^s}$ is an interesting one. It is easy to see that linear bijective maps H satisfying condition $H((K^*)^n) = (K^*)^n$ exist. The matrix M of H transfers $(x_1, x_2, \ldots, x_n) \in (K^*)^n$ to $(x_1, x_2, \ldots, x_n)M$ from $(K^*)^n$ if and only if each column of M contains an odd number of odd residues modulo 2^s. We can consider bijective map G on $(K^*)^n$ of kind $\psi_1 H \psi_2$. If the matrix of H has $O(n^2)$ nonzero entries and Eulerian transformations ψ_i, $i = 1, 2$ have linear degrees then G has linear degree and exponential density (number of monomial terms in all $G(x_i)$) [46].

It means that if correspondents share information on ψ_i and H and know Eulerian inverses $(\psi_i)^{-1}$ then they can use G as an encryption tool on the space $(K^*)^n$. The knowledge of the decomposition of G allows them to encrypt. The complexity of encryption and decryption is $O(n^2)$. We refer to this encryption scheme as Double Eulerian cipher.

The highly nonlinear nature of G makes the linearization attacks by adversaries impossible to conduct.

Of course, we have to consider the change of H on the nonlinear family of bijective multivariate maps ${}^nF$ such that computation of ${}^nF(p)$ and reimage of ${}^nF$ takes $O(n)$ if some trapdoor information is known. The problem is the hardness of the investigation of the condition ${}^nF((K^*)^n) = (K^*)^n$. To avoid this complication we use the following alternative approach.

We consider some computational relations between $Z_{2^{s-1}}$, $Z^*_{2^s}$, and $F_{2^{s-1}}$.

Recall that $Z^*_{2^s}$ is the totality of odd residues modulo 2^s.

We consider the map $б$ from $Z_{2^{s-1}}$ to $Z^*_{2^s}$ such that $б(t \bmod 2^{s-1})$ is $2t+1 \bmod 2^s$. It is a bijection. Let $б^{-1}$ be the inverse map from $Z^*_{2^s}$ to $Z_{2^{s-1}}$.

Notice that elements from $Z_{2^{s-1}}$ can be written as $b = e_0+e_12+e_22^2+\ldots+e_{s-2}2^{s-2} mod\ 2^{s-1}$, where $e_i \epsilon \{0,1\}$. Element of the finite field F_q, $q=2^{s-1}$ can be written as $g(x) = e_0+e_1x+e_2x^2+\ldots+e_{s-2}x^{s-2}$ $mod\ p(x)$ where $p(x)$ is the irreducible polynomial of degree s-1. Let π be the map such that $\pi(b) = g(x)$ and π^{-1} is the inverse map from F_q, $q = 2^{s-1}$ onto $Z_{2^{s-1}}$.

We consider the map Δ from F_q onto $(F_2)^{s-1}$ sending $g(x)$ to Boolean vector $(e_0, e_1, \ldots, e_{s-2})$ which we identify with the element of Boolean ring B_{s-1} of size 2^{s-1}.

Let us consider the map S of $(Z^*_{2^s})^n$ onto $(Z_{2^{s-1}})^n$ which sends $(x_1, x_2, \ldots, x_n)$ to $(б^{-1}(x_1), б^{-1}(x_2)), \ldots, б^{-1}(x_n))$. We define the map P of $(Z^*_{2^s})^n$ onto $(F_{2^{s-1}})^n$ which sends $(x_1, x_2, \ldots, x_n)$ to $(\pi(б^{-1}(x_1)), \pi(б^{-1}(x_2)), \ldots, \pi(б^{-1}(x_n))$. Let D be the map of $(Z^*_{2^s})^n$ onto $(B_s{}^-{}_1)^n$

Sending $(x_1, x_2, \ldots, x_n)$ to $(\Delta(\pi(б^{-1}(x_1))), \Delta(\pi(б^{-1}(x_2))), \ldots., \Delta(\pi(б^{-1}(x_n))))$. We assume that S^{-1}, P^{-1}, and D^{-1} are inverses of bijective maps S, P, and D.

Let us consider several modifications of the Double Eulerian cipher.

If K is a commutative ring and F is a map from K^n to K^n. Let T be a piece of information such that the knowledge of T allows us to compute the value of F on the given element of K^n and the reimage of F in time $O(n^2)$. We refer to T as a symmetric trapdoor accelerator. We say that pair (F, T) is a linear accelerator if it allows us to compute the reimage of F in time $O(n)$.

We suggest the following encryption schemes.

M1. Let $K = Z_{2^{s-1}}$ and ${}^nF$ be the family of polynomial maps of K^n onto K^n, i. e ${}^nF(x_i)$ is an element of $K[x_1, x_2, \ldots, x_n]$. Assume that ${}^nF$ has a trapdoor accelerator T.

Alice and Bob share $({}^nF, T)$ and Eulerian transformations ψ_i, $i = 1, 2$ defined on $(Z_{2^s})^n$ with their Eulerian inverses $(\psi_i)^{-1}$ for which $\psi_i(\psi_i)^{-1}(x) = x$ for $x \epsilon (Z^*_{2^s})^n$.

Then they can work with the family of ciphers with the space of plaintexts $(Z^*_{2^s})^n$ and use the encryption function $G = \psi_1S^nF\ (S^{-1})\ \psi_2$. The knowledge of T and the decomposition of G and G^{-1} into ψ_i, ${}^nF$, S, and their inverses allows to encrypt and decrypt in time $O(n^2)$.

M2. Let $K = F_{2^{s-1}}$ and ${}^nF$ be the family of polynomial maps of K^n onto K^n, i. e. ${}^nF(x_i)$ is an element of $K[x_1, x_2, \ldots, x_n]$. Assume that ${}^nF$ has a trapdoor accelerator T.

Alice and Bob share $({}^nF, T)$ and Eulerian transformations ψ_i, $i = 1, 2$ defined on $(Z_{2^s})^n$ with their Eulerian inverses $(\psi_i)^{-1}$ for which $\psi_i(\psi_i)^{-1}(x) = x$ for $x \epsilon (Z^*_{2^s})^n$.

Then they can work with the family of ciphers with the space of plaintexts $(Z^*_{2^s})^n$ and use the encryption function $G = \psi_1P^nF\ (P^{-1})\ \psi_2$. The knowledge of T and the decomposition of G and G^{-1} into ψ_i, ${}^nF$, P, and their inverses allows to encrypt and decrypt in time $O(n^2)$.

M3. Let $K = B_{s-1}$ and ${}^nF$ be the family of polynomial maps of K^n onto K^n, i. e ${}^nF(x_i)$ is an element of $K\ [x_1, x_2, \ldots, x_n]$. Assume that ${}^nF$ has a trapdoor accelerator T,

Alice and Bob share $({}^nF, T)$ and Eulerian transformations ψ_i, $i = 1, 2$ defined on $(Z_{2^s})^n$ with their Eulerian inverses $(\psi_i)^{-1}$ for which $\psi_i(\psi_i)^{-1}(x) = x$ for $x \epsilon (Z^*_{2^s})^n$.

Then they can work with the family of ciphers with the space of plaintexts $(Z^*_{2^s})^n$ and use the encryption function $G = \psi_1D^nF\ (D^{-1})\ \psi_2$. The knowledge of T and the decomposition of G and G^{-1} into ψ_i, ${}^nF$, P, and their inverses allows to encrypt and decrypt in time $O(n^2)$.

REMARK 1. *In each of the described above cases we can substitute ${}^nF$ with the trapdoor accelerator for its affine deformation, i. e. the map ${}^nF$ of kind $L_1{}^nFL_2$, $L_i \in AGL_n(K)$ which has a trapdoor accelerator L_1, L_2, T.*

REMARK 2. *We can identify $(Z^*_{2^s})^n$ with $(B_{s-1})^n$ and interpret the encryption function of Mi, i = 1, 2, 3 as the Boolean maps.*

Investigation of classes of these maps is an interesting theoretical task.

REMARK 3. *The Boolean functions defined above are given via the following three algebraic operations. They are the multiplication of Z_{2^s} and the multiplication and addition of one of the rings $Z_{2^{s-1}}$, $F_{2^{s-1}}$, and B_{s-1}. So the encryption is not defined as a multivariate map. This fact eliminates cryptanalytic studies in terms of multivariate Cryptography such as linearisation attacks.*

REMARK 4. *The schemes M_i, i = 1, 2, 3 are defined as the obfuscation of Double Eulerian cipher with the multivariate encryption map of linear degree and exponential density. We believe that this fact supports the conjecture that the cryptanalytic task is a hard problem.*

3. On Eulerian Semigroup and Hard Computational Problem

Let K be a finite commutative ring with the multiplicative group K^* of regular elements of the ring. We take Cartesian power ${}^nE(K) = (K^*)^n$ and consider an Eulerian semigroup ${}^nES(K)$ of transformations of the kind

$$\begin{aligned} &x_1 \rightarrow \mu_1 x_1^{a(1,1)} x_2^{a(1,2)} \ldots x_m^{a(1,n)}, \\ &x_2 \rightarrow \mu_2 x_1^{a(2,1)} x_2^{a(2,2)} \ldots x_m^{a(2,n)}, \\ &\ldots \\ &x_m \rightarrow \mu_n x_1^{a(n,1)} x_2^{a(n,2)} \ldots x_m^{a(n,n)}, \end{aligned} \qquad (1)$$

where $a(i, j)$ are elements of arithmetic ring Z_d, $d = |K^*|$, $\mu_i \in K^*$.

Let ${}^nEG(K)$ stand for the Eulerian group of invertible transformations from ${}^nES(K)$. A simple example of an element from ${}^nEG(K)$ is a written above transformation where $a(i,j) = 1$ for $i \neq j$ or $i = j = 1$, and $a(j,j) = 2$ for $j \geq 2$. It is easy to see that the group of monomial linear transformations M_n is a subgroup of ${}^nEG(K)$. So semigroup ${}^nES(K)$ is a highly noncommutative algebraic system. Each element from ${}^nES(K)$ can be considered as a transformation of a free module K^n.

Let π and δ be two permutations on the set *{1, 2, ..., n}*. Let K be a commutative ring with unity which has nontrivial multiplicative group K^* of order $d = |K^*| > 1$ and $n \geq 1$. We define transformation ${}^AJG(\pi, \delta)$ of the variety $(K^*)^n$, where A is a triangular matrix with positive integer entries $0 \leq a(i,j) \leq d$, $i \geq d$ defined by the following closed formula.

$$\begin{aligned} &y_{\pi(1)} = \mu_1 x_{\delta(1)}^{a(1,1)} \\ &y_{\pi(2)} = \mu_2 x_{\delta(1)}^{a(2,1)} x_{\delta(2)}^{a(2,2)} \\ &\ldots \\ &y_{\pi(n)} = \mu_n x_{\delta(1)}^{a(n,1)} x_{\delta(2)}^{a(n,2)} \ldots x_{\delta(n)}^{a(n,n)} \end{aligned}$$

where

$$(a(1,1),d) = 1, (a(2,2),d) = 1, \ldots, (a(n,n),d) = 1.$$

We refer to ${}^AJG(\pi, \delta)$ as Jordan transformations Gauss multiplicative transformation, or simply *JG* element. It is an invertible element of ${}^nES(K)$ with the inverse of kind ${}^BJG(\delta, \pi)$ such that $a(i,i)b(i,i) = 1 \pmod d$. Notice that in the case $K = Z_m$ straightforward process of computation the inverse of *JG* element is connected with the factorization problem of integer m. If $n = 1$ and m is a product of two large primes p and q the complexity of the problem is used in the RSA public key algorithm. The idea to use the composition of *JG* elements or their generalizations with injective maps *of* K^n into K^n was used in [47] ($K = Z_m$) and [48] ($K = F_q$.).

We say that τ is a *tame Eulerian element* over the commutative ring K if it is a composition of several Jordan Gauss multiplicative maps over a commutative ring or field respectively. It is clear that τ sends variable x_i to a certain monomial term. The decomposition τ into a product of Jordan Gauss transformation allows us to find the solution of equations $\tau(x) = b$ for x from $(Z_m^*)^n$ or $(F^*_q)^m$. So tame Eulerian transformations over Z_m or F_q. are special elements of ${}^nEG(Z_m)$ or ${}^nEG(F_q)$ respectively.

We refer to elements of ${}^nES(K)$ as multiplicative Cremona elements. Assume that the order of K is constant. As it follows from the definition the computation of the value of element from ${}^nES(K)$ on the given element of K^n is estimated by $O(n^2)$. The product of two multiplicative Cremona elements can be computed in time $O(n^3)$.

We are not discussing here the complexity of computing the inverse for general element $g \in {}^nEG(K)$ on the Turing machine or Quantum computer and the problem of finding the inverse for tame Eulerian elements.

If G is a tame Eulerian transformation of $(K^*)^n$, $K = Z_{2^s}$ which is defined as a composition of Jordan-Gauss transformations $J_1, J_2, \ldots, J_k$, $k > 1$, $k = O(1)$. Then $G_1 = SGS^{-1}$, $G_2 = PGP^{-1}$, and $G_3 = DGD^{-1}$ are transformations of affine spaces $(Z_{2^{s-1}})^n$, $(F_{2^{s-1}})^n$ and $(B_{m-1})^n$. The decomposition of G_i into S, P, D, and J_i is a symmetric trapdoor accelerator.

4. On Multivariate Transformations Based on Linguistic Graphs and Their Double Eulerisations

The families of graphs $D(n, K)$, defined over arbitrary commutative ring K are bipartite linguistic graphs of type $(1, 1, n-1)$ with partition sets which are two copies of K^n [42, 49–50], 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 $a_2x_2-b_2y_2 = f_2(x_1, y_1)$, $a_3x_3-b_3y_3 = f_2(x_1, x_2, y_1, y_2)$,..., $a_nx_n-b_ny_n = f_2(x_1, x_2, \ldots, x_{n-1}, y_1, y_2, \ldots, y_{n-1})$ 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 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 $CD(n, K)$ defined in [42] after the elimination of computed recurrently parameters also can be written as linguistic graphs of type $(1, 1, m-1)$ where $m = [3/4n] + c$.

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 the 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 $a_2X_2-b_2Y_2 = f_2(X_1, Y_1)$, $a_3X_3-b_3Y_3 = f_2(X_1, X_2, Y_1, Y_2)$, ..., $a_nX_n-b_nY_n = f_2(X_1, X_2, \ldots, X_{n-1}, Y_1, Y_2, \ldots, Y_{n-1})$, 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 [1]. 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 two families of affine transformations ${}^1L_n \epsilon AGL_n(K)$, ${}^2L_n \epsilon AGL_n(K)$, 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 ${}^1L_n(F(g_1, g_2, \ldots, g_t){}^2L_n$.

Correspondents Alice and Bob share the password given by $g_1, g_2, \ldots, g_t$, and the sequences of transformations ${}^1L_n, {}^2L_n$ $n = 2, 3, \ldots$ We assume that inverse maps $({}^iL_n)^{-1}$, $i = 1, 2$ are computed and presented explicitly. For the encryption of potentially infinite plaintext $(p) = (p_1, p_2, \ldots, p_n)$ they will use transformation $G = {}^1L_nF(g_1, g_2, \ldots, g_t){}^2L_n$. One of them creates the plaintext *(pp’77p)* and computes the ciphertext ${}^1L_nF(g_1, g_2, \ldots, g_t){}^2L_n(p) = c$ recurrently. The procedure is the sequence of the following steps.

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

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

S_4. He/she computes ciphertext as ${}^2L(u) = c$

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 $({}^2L_n)^{-1}(c) = u$ 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 $({}^1L)^{-1}\ (r))$.

Let us assume that transformation G is given in its standard form, i. e. via the list of monomial terms $G(x_i)$ ordered lexicographically. Assume that multivariate polynomials f_i in the definition of $I(K)$ and polynomials $g_i(x)$ have densities $O(1)$, and parameter t has size $O(n)$. Then equations in the definition of $I(K)$ and the sequence $(g_1, g_2,…, g_t)$ form the symmetric trapdoor accelerator of multivariate map G. We denote it as $T = [I(K), L_1, L_2, g_1, g_2, …, g_t]$.

Assume that ψ is some Eulerian transformations defined over the commutative ring K. It acts naturally on the sets $(K^*)^n$ and K^n. Assume that F is a multivariate map of K^n onto K^n of density $O(n^d)$ where d is the constant. Then Eulerisation $E = F(\psi(x))$ is well defined and has density $O(n^{d+1})$.

Some cryptographic applications of the Eulerisation procedure for special multivariate maps were considered in [47–48, 1].

In the special cases of $K = Z_{2^{s-1}}$, $K = F_{2^{s-1}}$, and $K = B_{s-1}$ we define procedures Mi, $i = 1, 2, 3$ to modify the multivariate map F on K^n with the trapdoor accelerator T via the composition with two tame Eulerian transformations ψ_1 and ψ_2 defined on the affine space $(Z_{2^s})^n$. In the case of $T = [I(K), L_1, L_2, g_1, g_2,…, g_t]$ as a result of double Eulerisation, we get a new transformation of K^n with the trapdoor accelerator ψ_i, $(\psi_i)^{-1}$, $i = 1, 2, I(K), L_1, L_2, g_1, g_2, …, g_t$.

Noteworthy that some parts of the trapdoor accelerator can be given to the public. In the case of graph-based ciphers graph $I(K)$ traditionally is known to the public.

In the next section, we apply double Eulerisation to stream cipher defined in terms of special induced subgraphs of the linguistic graph $D(n, K)$, $K \in \{ Z_{2^{s-1}}, F_{2^{s-1}}, B_{s-1}\}$.

5. On Some Ciphers Based 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 antireflective 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 $diam\ (\Gamma_i)\leq c\ log_{k-1}(v_i)$, 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 $g(\Gamma_i)\geq c\ log_{k-1}(v_i)$, 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. 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 [51] and investigated by A. Lubotzky, Sarnak, and Phillips [52]. As it is easy to see the projective limit of $X(p, q)$ does not exist.

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

$$l_{ii} - p_{ii} = l_{10}\, p_{i-1,i}$$
$$l'_{ii} - p'_{ii} = l_{i,i-1}\, p_{01}$$
$$l_{i,i+1} - p_{i,i+1} = l_{ii}\, p_{01}$$
$$l_{i+1i} - p_{i+1,i} = l_{10} p'_{ii}.$$

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

Historically graph $D(q)$ is the first example of a description of q-regular forest in terms of Algebraic Geometry.

In [53] authors proved that $D(n,q)$ defined via first n-1equations 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.

In 1994 it was found out how to describe connected components $CD(n, q)$ of graphs $D(n, q)$ in terms of equations [54–55. 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 $4/3$. 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.

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. Let us consider the system of equations that defines linguistic 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 [42, 49] 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 [49] graphs $D(n, K)$ are edge transitive. So their connected components are isomorphic graphs. Let ${}^vCD(k, K)$ 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 ${}^vCD(k, K)$ 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 a 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. So graph $CD(n, q) = CD(n, F_q)$ for odd q is a connected component of $D(n, q)$.

The following statement was proven in [49].

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

Let us describe selected multivariate algorithms based on algebraic graphs of large girth.

To achieve linear speed $O(n)$ of the encryption described in Section 1 functions g_i, $i = 1, 2, \ldots, t$ are selected in the form $x_1+c(i)$, $c(i) \in K$ 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 $b(1), b(2), \ldots, b(k), a(1), a(2), \ldots, a(k), k = t/2$ 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 $(b(1), b(2), \ldots, b(k), a(1), a(2), \ldots, a(k))$ 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 L in the form of a linear map given by the following rule

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

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 $L\,E(n, K)\,L^{-1}$ and have a full description. In fact, we take the case of $L_1 = L$ and $L_2 = L^{-1}$. In the case of graph $CD(n, K)$ we will use in fact the induced subgraph ${}^{h}CD(n, K)$, $h = (h_2, h_3, \ldots, h_t)$, $t = [(n+2)/4]$ *of* $D(n, K)$ of all points and lines $u = (u_\alpha, u_{11}, u_{12}, u_{21}, \ldots, u_{r,r}, u'_{r,r}, u_{t\,t+1}\, u_{r,r+1}, u_{r+1,r}, \ldots)$ satisfying conditions $a_i(u) = h_i$.

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

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 $p'_{33} = a_3(p_{01}, p_{11}, p_{12}, p_{21}, p_{22}, p'_{22}, p_{2,3}, p_{3,2}, p_{3,3}\ p'_{3,3})-h_3+p'_{33} = b_3(p_{01}, p_{11}, p_{12}, p_{21}, p_{22}, p'_{22}, p_{2,3}, p_{3,2}, p_{,\,33})$, …, $p'_{tt} = a_t(p_{01}, p_{11}, p_{12}, p_{21}, p_{22}, p'_{22}, \ldots, p'_{t-1,t-1}, p_{t-1,\,t}, p_{t,\,t-1}, p_{t,t}, p'_{t,\,t})-h_t+p'_{t,t} = b_t(p_{01}, p_{11}, p_{12}, p_{21}, p_{22}, p'_{22}, \ldots, p'_{t-1,t-1}, p_{t-1,\,t}, p_{t,\,t-1}, p_{t,\,t})$.

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 $K^{n\text{-}t}$. We use active passwords $(b(1), b(2), \ldots, b(k), a(1), a(2), \ldots, a(k))$ and linear transformations L of K^{n-t} constructed via described above rules. We assume that parameters $h_2, h_3, \ldots, h_t$ will be considered as part of the active password and denote the cipher as $LCE(n, K)L^{-1}$

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 [56] 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 case $LCE(n, K)L^{-1}$ is principally different. As it follows from the results of [57] the encryption function corresponding to the selected active password has 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.

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

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 $1, 2, ..., n–k$. 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 $N(x_1, x_2, ..., x_{n–t}) = (w_1, w_2, ..., w_{n–t})$.

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 $u_1 = x_1+\beta(1)$, $u_2 = x_1+\alpha(1)$, $u_i = u_{i-2}+\beta(i)$, $i = 3, 5, ..., 2k–1$, $u_i = u_{i–2}+\alpha(i))$, $i = 4, 6, ..., 2k$.

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 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 [57] 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 L given by the following rule. $L(x_1) = x_1+m(1)x_2+...+m(n–t–1)x_{n–t–1}$ where $m(i)$, $i = 1, 2, ..., n–1$ are elements of K^*, $L(x_i) = x_i$ for $i = 2, 3, ..., n–t$.

We denoted described below cipher as ${}^{k}ED_t(n, K)$. The map LNL^{-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 $m(1), m(2), ..., m(n–t–1)$ 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 $w = i(1)+i(2)+...+i(t)$.

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.

6. The Double Eulerisation of Multivariate Ciphers ${}^{\mathbf{k}}\mathbf{ED_t(n, K)}$

Let K be one of the commutative rings $F_{2^{s–1}}$, $Z_{2^{s–1}}$, and $B_{s–1}$. We consider the group ${}^{n}EG(Z_{2^s})$ *and select* Jordan-Gauss transformation J of kind

$x_1 \to x_1x_2^{d(1)}x_3^{d(2)}...x_{n–t–1}^{d(n–t–1)}$,

$x_i \to x_i$, $i = 2, 3,..., n–t–1$ where elements $d(i)$ are from $Z_{2^{s–1}}$.

The element J^{-1} is given by the rule $x_1 \to x_1x_2^{–d(1)}x_3^{–d(2)}...x_{n–t–1}^{–d(n–t–1)}$, $x_i \to x_i$, $i = 2, 3, ..., n–t–1$.

Let us consider double Eulerisation ${}^{k}F(s–1, n, t)$ of $E = {}^{k}ED_t(n, F_{2^{s–1}})$ given by transformation $P^{–1}JPEP^{–1}J^{–1}P$ and acting on the space of plaintexts $(F_{2^{s-1}})^{n-t}$.

Additionally, we consider double Eulerisation ${}^{k}E(s–1, n, t)$ of $E = {}^{k}ED_t(n, Z^{s–1})$ given by the transformation.

$S^{-1}JSES^{–1}J^{–1}S$ acting on the affine space $(Z_{2^{s–1}})^{n–t}$.

Finally, we take double Eulerisation ${}^{k}B(s–1, n, t)$ of $E = {}^{k}ED_t(n, B_{s–1})$, given by the transformation $D^{–1}JDED^{–1}J^{–1}D$ acting on the affine space $(B_{s–1})^{n–t}$.

Noteworthy that Double Eulerisations ${}^{k}F(s–1, n, t)$, ${}^{k}E(s–1, n, t)$ and ${}^{k}B(s–1, n, t)$ have the same active passwords with the corresponding multivariate ciphers ${}^{k}ED_t(n, K)$, $K = F_{2^{s–1}}$, $Z_{2^{s–1}}$ and $B_{s–1}$.

For the description of the passive password of new ciphers we need just simply add parameters $d(1), d(2), ..., d(n–t–1)$ of J to the passive password of the old cipher.

In the case of $K = F_{2^{s–1}}$ and $K = Z_{2^{s–1}}$ it is proven that different active passwords produce distinct ciphertexts. It means that in the case of fields brute force attack on the cipher requires $p^{2k}q^t$ elementary operations where $p = 2^{s-1}-1$ is the order of the multiplicative group of the field and $q = 2^{s-1}$.

In the case of arithmetical rings, we have to change the parameter $p = 2^{s-1}-1$ for $p = 2^{s-2}$.

In the case of Boolean ring B_{s-1}, its multiplicative group is trivial. We simply take tuples (*ą(1), ą(2), ..., ą(k)*) and *(β(1), β(2), ..., β(k))* from $(B_{s-1})^k$. We conjecture that in this case different active passwords also produce different ciphertexts. Computer simulations support this conjecture. In fact, we implement all 3 cases in the case of s = 9 and some restricted parameters *n, k,* and *t*.

For the first two implementations, we select the double Eulerisations of ciphers $^kED_t(m, K)$, $m = n\text{-}t$ with $K = F_{256}$, and $t = 128$ with weights $w = 2^{13}$ and 2^{16}.

Core encryption map has a highly nonlinear nature. Additionally, Eulerisation eliminates the multivariate nature of the encryption and decryption.

So the linearisation attacks by adversaries are unfeasible. The bruit fourth attack requires $(2^{15})\cdot 255^k$, where $k = 2l$ is the chosen length of the walk in the graph.

Our software is written in C++ programming language and therefore it is portable and runs on many platforms such as Unix/Windows. The 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 from $^nES(Z_{512})$ of Z_{512} [45–46]. It allows the elaboration of the tuple of nonzero elements from Z^*_{512} of length *n* together with the matrix of size n times n with entries from Z_{512}. This data can be used for the construction of passive and active 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 (Figs. 1 and 2).

L\k	3000	4000	5000	6000
4	1943.25	2609.5	2985.25	3605
8	3676	5098	5869.25	7055
12	5220	6983.5	8604.5	10290
16	6953.75	9229.5	11345	13507.5
20	8723.75	11524	14115.25	16785.5

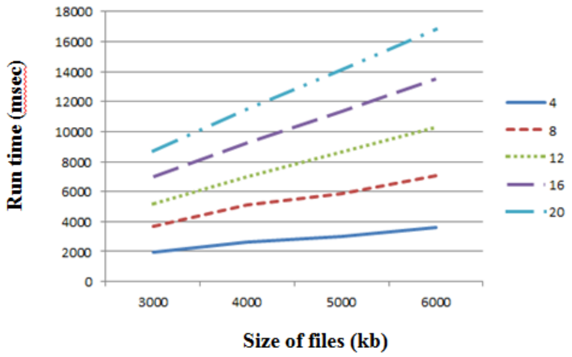

Figure 1: Run time for the System

L\k	3000	4000	5000	6000
4	2514.75	3377.25	3863	4665.5
8	4757.25	6599.5	7595.25	9129.75
12	6755.25	9037.25	11135	13316.5
16	8998.75	11944	14681.5	17480.5
20	11289.5	14913.5	18266.75	21722.5

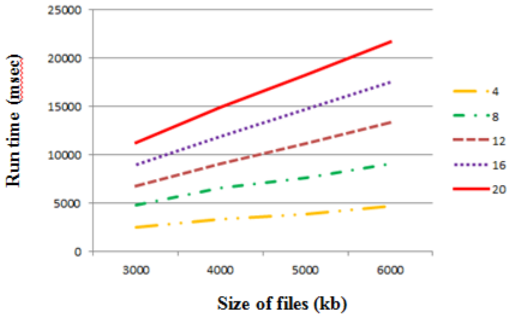

Figure 2 Run time for the System

In the implemented case the algorithm has nice mixing properties. change of a single character leads to the change of at least 98 percent of the characters in the ciphertext.

7. Conclusions

In [42] the first stream cipher based on algebraic graphs defined over the commutative ring *K* with unity was suggested. The corresponding bijective multivariate map acting on K^n was a cubical transformation as well as the inverse map. It means that the cost of linearisation attacks by an adversary is $O(n^{10})$ under the condition that the adversary intercepts $O(n^3)$ distinct pairs of kind plaintext. For the improvement of resistance of cipher against linearisation attack, many modifications and obfuscations of this algorithm were proposed.

Despite the various changes, all these modifications use the encryption map of a multivariate nature.

Our paper is the first attempt to construct a symmetric cipher of hidden multivariate nature of encryption and decryption procedures [46] where this general idea is used for the construction of asymmetrical cryptosystems.

In the case of $K = Z_{2^{s-1}}$, $K = F_{2^{s-1}}$, and Boolean rind B_{s-1} of order 2^{s-1} we use tame Eulerian transformations ψ_1 and ψ_2 from the group ${}^nEG (Z_{2^s})$ sending variable x_i to a monomial term. Assume that ${}^1T$ and ${}^2T$ are information about corresponding decompositions of ψ_i into Jordan-Gauss transformations. We use the bijection B_K between elements of the multiplicative group $Z^*_{2^s}$ of Z_{2^s} and elements of the ring K.

Effectively computable examples of such correspondences are presented above.

Let ${}^nB$ be the map sending tuple $(x_1, x_2, ..., x_n)$ to $(B_K(x_1), B_K(x_2),..., B_K(x_n))$ and ${}^nB^{-1}$ is the inverse map from K^n to $(Z^*_{2^s})$.

Assume that F is a multivariate map from K^n to K^n and T its trapdoor accelerator. We can consider map ${}^nE = {}^nB^{-1}\ \psi_1\ {}^nB\ F\ {}^nB^{-1}\ \psi_2\ {}^nB$ which maps K^n to K^n.

If correspondents Alice and Bob share the information on symmetric trapdoor accelerators T, ${}^1T$, and ${}^2T$ then the family of transformations ${}^nE$ can be used as stream cipher. The encryption and decryption procedures have complexity $O(n^2)$.

We use this scheme with sparse Eulerian transformations ψ_1, ψ_2 and graph-based pair (F, T) such that their reimages can be computed in time $O(n)$.

The $D(n, K)$ graph description which is part of information piece T can be given publicly.

In fact, the encryption procedure is given via the walk w in the induced subgraph $D_J(n, K)$ which is the union of several connected components of the $D(n, K)$.

The transformation F is an affine deformation of L_1GL_2 of the $D_J(K) = D_{J,a}(K)$ based transformation G induced via the special walk $w(J, a)$ on the graph. The set J of cardinality $r < t$, $t = [(n+2)/4]-1$ is some subset of $\{2, 3, ..., t\}$ and the tuple $a = (a_1, a_2, ..., a_r)$ *is formed* by elements from K. So we have $C^r_{n-r}q^r$, $q = 2^{s-1}$ nonintersecting induced subgraphs. The transformation G is induced by the path $w = w(b_1, b_2, ..., b_{2k})$ of selected length $2k$ depending on the parameters $b_i \in K^*$ if $K = Z_{2^{s-1}}$ or $K = F_{2^{s-1}}$ and $a_i \in B_{s-1}-\{0\}$ in the remaining case $K = B_{s-1}$.

Different pieces of information $(J, (a_1, a_2, ..., a_r), (b_1, b_2, ..., b_{2k}))$ form the active passwords of the cipher.

Selected sparse linear transformation $L_1 = L$ which depends on the selected tuple $(m_1, m_2, ..., m_{n-r-1})$ from $(K-\{0\})^{n-r-1}$ $n-r$ and $L_2 = L^{-1}$ hide the graph-based transformation.

Selected space Eulerian transformation G_1 of the variety $(Z_{2^s})^{n-r}$ depends on an element from $(Z_{2^s})^{n-r-1}$. G_2 is defined as the inverse of G_1. Eulerian transformations allow us to hide the multivariate nature of the encryption map.

The following fact is important.

Different active passwords produce distinct ciphertexts from the chosen plaintext.

If the length of tuples is $O(1)$ then we obtain three different secure stream ciphers with the speed of encryption $O(n)$. Correspondents can govern the level of protection via a selection of parameters r and k. We hope that the proposed robust and secure families of stream ciphers can serve various tasks of Big Data Protection.

We suggest supporting the stream cipher by the key exchange protocol of Noncommutative Cryptography implemented with the platform of Eulerian transformation ${}^nES(Z_{2^s})$ defined over the commutative ring Z_{2^s} [45–46]. Assume that secure protocol allows Alice and Bob to elaborate on the transformation of kind (1).

Then they share $\mu_1, \mu_2, ..., \mu_n$ from $Z^*_{2^s}$ and n^2 elements $a(i,j)$ from $Z_{2^{s-1}}$.

Correspondents can use the defined above bijections between $Z^*_{2^s}$, $Z_{2^{s-1}}$, $F_{2^{s-1}}$, and B_{s-1} to form the passive and active passwords of the stream cipher.

The main result of the paper is a complex cryptographical algorithm based on a highly noncommutative group of polynomial transformations $GA(n, K)$ of K^n, $n = 2, 3, ...$ defined over finite commutative ring K with a unity.

In the current postquantum reality the idea to change the cyclic group of Diffie Hellman protocol for a noncommutative group or semigroup with several generators can lead to safe protocols of Algebraic Postquantum Cryptography (APQ).

We suggest using $GA(m, K)$ for the safe elaboration of collision polynomial map G of degree 3 from K^n to K^m. G is written in its standard form of Computer Algebra. We can use $O(m^4)$ of its coefficients for the extraction of some "seed" S of size $s(m)$.

The protocol costs $O(m^{13})$ elementary operations. The security rests on the complexity of the known hard problem of APQ to find the decomposition of G into given generators from the affine Cremona group of polynomial transformations of K^m.

Correspondents can use a family of groups *GA(n, K)* for simultaneous construction of potentially infinite string R of characters from K^n of length *n* with the complexity *O(n).* Recovery of seed *S* is connected with the hard APQ problem of solving of system of nonlinear equations of unbounded degree.

Parts of *R* can be used as one-time pad keys, passwords of symmetric stream ciphers, or in key-dependent Message Authentication Codes. We also presented new APQ stable MACs and stream cipher to work with text of length *t* in time *O(t)* defined in terms of graphs from the family *A(n, K).*

Acknowledgments

This research is partially supported by the British Academy Fellowship for Researchers under Risk 2022 and partially supported by the British Academy award LTRSF\100333.

References

[1] V. Ustimenko, Graphs in Terms of Algebraic Geometry, Symbolic Computations and Secure Communications in Post-Quantum World, UMCS Editorial House (2022).

[2] V. Ustimenko, et al., On the Constructions of New Symmetric Ciphers Based on Nonbijective Maps of Prescribed Degree, Secur. Commun. Netw. (2019). doi: 10.1155/2019/2137561.

[3] N. Geetha, V. Ragavi, Graph Theory Matrix Approach in Cryptography and Network Security, Algorithms, Computing and Mathematics Conference (ACM) (2022). doi: 10.1109/ACM57404. 2022.00025.

[4] A. Costache, et al., Ramanujan Graphs in Cryptography, Research Directions in Number Theory, AWMS 19 (2019) 1–40. doi: 10.1007/978-3-030-19478-9_1.

[5] K. Priyadarsini, A Survey on some Applications of Graph Theory in Cryptography, J. Discrete Math. Sci. Cryptography 18(3) (2015) 209–217. doi: 10.1080/09720529.2013.878819.

[6] W. Etaiwi, Encryption Algorithm Using Graph Theory, J. Sci. Res. Reports 3(19) (2014) 2519–2527. DOI: 10.9734/JSRR/ 2014/11804.

[7] W. Etaiwi, Encryption Algorithm Using Graph Theory, J. Sci. Res. Reports 3(19) (2014) 2519–2527. DOI: 10.9734/JSRR/ 2014/11804.

[8] L. Mittenthal, Sequencings and Directed Graphs with Applications to Cryptography, Sequences, Subsequences, and Consequences, LNCS 4893 (2007) 70–81. doi: 10.1007/978-3-540-77404-4_7.

[9] M. Naor, A. Shamir, Visual cryptography, Advances in Cryptology—EURO CRYPT'94, LNCS 950 (1994)1–12. doi: 10.1007/BFb0053419.

[10] S. Lu, D. Manchala, R. Ostrovsky, Visual Cryptography on Graphs, COCOON (2008) 225–234.

[11] W. Stallings, Cryptography and Network Security Principles and Practices, Prentice Hall India (2006).

[12] D. Song, D. Zuckermany, J. Tygar, Expander Graphs for Digital Stream Authentication and Robust Overlay Networks, IEEE Symposium on Security and Privacy (S&P.02) (2002). doi: 10.1109/SECPRI.2002.1004376.

[13] M. Yamuna, et al., Encryption Using Graph Theory and Linear Algebra, Int. J. Comput. Appl. (2012) 2250–1797.

[14] A. Paszkiewicz, et al., Proposals of Graph Based Ciphers Theory and Implementations, Research Gate (2001).

[15] B. Cusack, E. Chapman, Using Graphic Methods to Challenge Cryptographic Performance, 14th Australian Information Security Management Conference, Edith Cowan University (2016) 30–36. doi: 10.4225/75/58a699 1e71023.

[16] E. Chapman, Using Graphic Based Systems to Improve Cryptographic Algorithms, Auckland University of Technology (2016).

[17] E. Kinani, Fast Mapping Method based on Matrix Approach For Elliptic Curve Cryptography, Int. J. Inf. Netw. Secur. (IJINS) 1 (2012) 54–59.

[18] D. Moldovyan, N. Moldovyan, A New Hard Problem over Non-commutative Finite Groups for Cryptographic Protocols, MMM-ACNS 2010: Computer Network Security, LNCCN 6258 (2010) 183–194. doi: 10.1007/978-3-642-14706-7_14.

[19] E. Sakalauskas, P. Tvarijonas, A. Raulynaitis, Key Agreement Protocol (KAP) Using Conjugacy and Discrete Logarithm Problema in Group Representation Level, INFORMATICA 8(1) (2007) 115–124. doi: 10.15388/INFORMATICA.2007.167.

[20] V. Shpilrain, A. Ushakov, The Conjugacy Search Problem in Public Key Cryptography: Unnecessary and Insufficient, Applicable Algebra in Engineering, Communication and Computing 17(3–4) (2006) 285–289. doi: 10.1007/s00200-006-0009-6.

[21] D. Kahrobaei, B. Khan, A Non-Commutative Generalization of ElGamal Key Exchange Using Polycyclic Groups, In IEEE GLOBECOM 2006 - 2006 Global Telecommunications Conference [4150920] DOI: 10.1109/GLOCOM.2006.

[22] A. Myasnikov; V. Shpilrain; A. Ushakov (2008). Group-based Cryptography. Berlin: BirkhäuserVerlag.

[23] A. Myasnikov; V. Shpilrain; A. Ushakov (2008). Group-based Cryptography. Berlin: BirkhäuserVerlag.

[24] Z. Cao (2012). New Directions of Modern Cryptography. Boca Raton: CRC Press, Taylor & Francis Group. ISBN 978-1-4665-0140-9.

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

[26] A. Myasnikov; V. Shpilrain; A. Ushakov, (2011). Non-commutative Cryptography and Complexity of Group-theoretic Problems. American Mathematical Society.

[27] I. Anshel, M. Anshel, D. Goldfeld, An algebraic method for public-key cryptography. Math. Res.Lett. 6(3–4), 287–291 (1999).

[28] S. Blackburn, S. Galbraith, Cryptanalysis of Two Cryptosystems Based on Group Actions, Advances in Cryptology—ASIACRYPT ’99, LNCS 1716 (1999) 52–61. doi: 10.1007/978-3-540-48000-6_6.

[29] K. Ko, et al., New Public-Key Cryptosystem Using Braid Groups, In: Advances in Cryptology—CRYPTO 2000, LNCS 1880 (2000) 166–183. doi: 10.1007/3-540-44598-6_10.

[30] 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.

[31] P. Kropholler, 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.

[32] J. Lopez-Ramos, et al., Group Key Management Based on Semigroup Actions, J. Algebra Appl. 16 (2019).

[33] G. Kumar, H. Saini, Novel Noncommutative Cryptography Scheme Using Extra Special Group, Security and Communication Networks 2017 (2017). doi: 10.1155/2017/9036382.

[34] A. Myasnikov, V. Roman’kov, A Linear Decomposition Attack, Gr. Complex. Cryptol. 7 (2015) 81–94. doi: 10.1515/gcc-2015-0007.

[35] V. Roman’kov, A Nonlinear Decomposition Attack. Gr. Complex. Cryptol. 8(2) (2017) 197–207. doi: 10.1515/gcc-2016-0017.

[36] V. Roman’kov, Two General Schemes of Algebraic Cryptography, Gr. Complex. Cryptol. 10(2) (2018) 83–98. doi: 10.1515/gcc-2018-0009.

[37] V. Roman’kov, An Improved Version of the AAG Cryptographic Protocol, Gr. Complex. Cryptol. 11(1) (2019). doi: 10.1515/gcc-2019-2003.

[38] 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.

[39] A. Ben-Zvi, A. Kalka, B. Tsaban, Cryptanalysis via Algebraic Spans, Advances in Cryptology—CRYPTO 2018, LNSC 109991 (2018) 1–20. doi: 10.1007/978-3-319-96884-1_9.

[40] V. Ustimenko, O. Pustovit, On Security of GIS Systems with N-Tier Architecture and Family of Graph Based Ciphers,

Environ. Saf. and Nat. Resour. 47(3) (2023) 113–132. doi: 10.32347/2411-4049.2023.3.113-132.

[41] V. Ustimenko, On Extremal Algebraic Graphs and Multivariate Cryptosystems, IACR e-Print Archive 1537 (2022).

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

[43] V. Ustimenko, Random Walks on Graphs and Cryptography, Extended Abstracts, AMS Meeting (1998).

[44] V. Ustimenko, CRYPTIM: Graphs as Tools for Symmetric Encryption, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, LNCS 2227 (2001) 278–286. doi: 10.1007/3-540-45624-4_29.

[45] V. Ustimenko, On Eulerian Semigroups of Multivariate Transformations and Their Cryptographic Applications, European J. Math. 9(93) (2023). doi: 10.1007/s40879-023-00685-2.

[46] V. Ustimenko, On Historical Multivariate Cryptosystems and Their Restorations as Instruments of Post-Quantum Cryptography, IACR e-Print Archive 91 (2024).

[47] V. Ustimenko, On New Multivariate Cryptosystems Based on Hidden Eulerian Equations, Dopovidi of National Academy of Science of Ukraine 5 (2017) 7–11. doi: 10.15407/DOPOVIDI2017.05.017.

[48] V. Ustimenko, On New Multivariate Cryptosystems Based on Hidden Eulerian Equations Over Finite Fields, IACR e-Print Archive 93 (2017).

[49] V. Ustimenko (2007). On Linguistic Dynamical Systems, Graphs of Large Girth and Cryptography, J. Math. Sci. 140(3) (2007) 412–434.

[50] V. Ustimenko, Maximality of Affine Group, Hidden Graph Cryptosystem and Graph's Stream Ciphers, J. Algebra Discret. Math. 4(1) (2005) 133–150.

[51] G. Margulis, Explicit Group-Theoretical Constructions of Combinatorial Schemes and Their Application to Design of Expanders and Concentrators, Probl. Peredachi Inf. 24(1) (1988) 51–60.

[52] A. Lubotsky, R. Philips, P. Sarnak, Ramanujan Graphs, J. Comb. Theor. 115(2) (1989) 62–89.

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

[54] F. Lazebnik, 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.

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

[56] M. Klisowski. Zwiększenie Bezpieczeństwa Kryptograficznych Algorytmów Wielu Zmiennych Bazujących na Algebraicznej Teorii Grafów, Rozprawa doktorska, Politechnika Częstochowska, Częstochowa (2014).

[57] V. Ustimenko, A. Wroblewska, On the Key Exchange and Multivariate Encryption with Nonlinear Polynomial Maps of Stable Degree, Ann. UMCS, Inform. 13(1) (2013) 63–80. doi: 10.2478/v10065-012-0047-6.