On the expanding graphs of large girth and algorithms of key establishment *

Vasyl Ustimenko[1,2,†], Tymoteusz Chojecki[2,*,†]

[1] Royal Holloway University of London, United Kingdom, Egham Hill, Egham TW20 0EX, United Kingdom

[2] Institute of Computer Science and Mathematics, UMCS pl. Marii Curie-Sklodowskiej 1, 20-031, Lublin, Poland,

Abstract

Let us assume that one of two trusted parties (administrator) manages the in-formation system (IS) and another one (user) is going to use the resources of this IS during the certain time interval. So they need establish secure user's access password to the IS resources of this system via selected authenticated key exchange protocol. So they need to communicate via insecure communication channel and secretly construct a cryptographically strong session key that can serve for the establishment of secure passwords in the form of tuples in certain alphabet during the certain time interval. Nowadays selected protocol has to be postquantum secure. We propose the implementation of this scheme in terms of Symbolic Computations. The key exchange protocol is one of the key exchange algorithms of Noncommutative Cryptography with the platform of multivariate transformation of the affine space over selected finite commutative ring. The session key is a multivariate map on the affine space. Platforms and multivariate maps are constructed with the use of algebraic constructions of expanding graphs of large girth.

Keywords

Expanding Graphs, Algebraic Graphs of Large Girth, Key establishment algorithms, Multivariate Cryptography, Noncommutative Cryptography, Multivariate public keys.

1. Introduction

Expander graphs, i. e. families of q-regular graphs with the second largest eigen-value bounded away from q are widely known because of their applications in Pure and Applied Mathematics [1]. As it was established recently known q-regular graphs of large girth *CD(n, q)* [2] turns out to be expanders. Computer experiments supports that the conjecture that their second largest eigenvalue is bounded from above by 2 square root of q [3]. Many applications of graphs *CD(n, q)* are known [4]. In this paper we present new applications of these graphs and their generalisations described in [3] to Multivariate Cryptography. We described some key establishment algorithms based on these graphs. Multivariate Cryptography (MC) is one of the fifth directions of Post-Quanum Cryptography designed for the constructions and investigations of asymmetric cryptographic algorithms with the resistance to attacks of the adversary who uses quantum computer. The security of algorithm of MC is based on the complexity of solving the system of nonlinear equations

*ITTAP'2025: 5th International Workshop on Information Technologies: Theoretical and Applied Problems, October 22–24, 2025, Ternopil, Ukraine, Opole, Poland *

Corresponding author.

† These authors contributed equally.

Vasyl.Ustymenko@rhul.ac.uk (V. Ustimenko); tymoteusz.chojecki@umcs.pl (T.Chojecki)

0000-0002-2138-2357 (V. Ustimenko); 0000-0002-3294-2794 (T.Chojecki)

over the finite commutative ring. Traditionally MC uses systems of equations of degree 2 or 3 defined over the finite field see [5]. Despite the fact that the last talk on Multivariate Cryptography on Eurocrypt conferences was in 2021 (see [6]) many new results in this area were obtained (see Proceedings of PQCrypts 2021-2024) and new cryptosystem [7] were submitted to NIST (USA).

Classical task of Multivariate Cryptography is the constructions of public keys in the form of multivariate maps of small degree over finite fields see ([22]-[38]). We consider more general task of construction of nonlinear multivariate map F on affine space K^n where K is a commutative ring with unity with the trapdoor accelerator T which is a piece of information such the knowledge of T allows us to compute the reimage of F in polynomial time (see [8] or [9] for some examples).

We assume that multivariate map F is given in its standard form of kind $x_i \longrightarrow fi(x_1, x_2, \dots , x_n)$, $i=1, 2, \dots , n$ where polynomials fi are given in the form of the some of monomial terms listed in the lexicographical order. We assume that monomial term M is written in the form $a(x_1)^{t(1)}(x_2)^{t(2)}\dots(x_n)^{t(n)}$, where $t(i)$ are elements of Z_m, m is the order of multiplicative group K^*.

The construction of such forms with the corresponding trapdoor accelerator is an interesting task of Algebraic Geometry for which cases of complex numbers or algebraically closed field K are especially important.

We assume that Multivariate Cryptography in wide sense is about applications of the theory of nonlinear trapdoor accelerators to Symmetric and Asymmetric Cryptography. In the case when K is a finite commutative ring the pair (F, T) can be used as instrument of symmetric encryption. The space K^n can serve as space of ciphertexts. Usually the knowledge of T allows efficient computation of the value of F on the given tuple. Both correspondents have the knowledge on T. So they do not need to compute the standard form. Adversary can use various attacks to investigate the multivariate nature of encryption procedure for the construction of the procedure to compute the reimages of the map. Standard forms of F with trapdoor accelerator can be considered as potential multivariate maps which can serve as instruments for encryption or conducting digital signatures.

Multivariate maps are elements of Cremona semigroup ${}^nCS(K)$ of endomorphisms of $K[x_1, x_2,\dots, x_n]$ (see [39]). Such endomorphism F can be given by its values $F(x_i)= fi(x_1, x_2, \dots, x_n)$, $i=1, 2, \dots, n$ on generic variables x_i. We assume that polynomials fi are given via their standard form and define degree and density of the map F.

Trapdoor accelerators can be used for the generation of subsemigroup H of ${}^nCS(K)$ with the property P of computation of the product of n elements from H in a polynomial time. Its alternative approach to combinatorial method of generators and relations. Note that ${}^nCS(K)$ itself does not posses P itself because the product of n its general representatives of degree k , $k\geq 2$ will be of degree k^n.

Subsemigroup H satisfying property P can be used as platforms of Noncommutative Cryptography [10] for the implementation of algebraic key exchange protocols of Postquantum Cryptography. Noncommutative Cryptography is an area of current intensive research (see [40]-[54]).

Some methods of construction of multivariate maps with the trapdoor accelerator in terms of Algebraic Graph Theory are presented in [8] (see also [9] and further references) together with some cryptographical applications.

The paper is dedicated to applications of graph based constructions of trapdoor accelerators to algorithm of the establishment of secure user's access password to the resources of Information System with further options of the password changes. We suggest the following general scheme.

Assume that Administrator A and his/her trusted user have safely protected password *t* for mutual authentication, This is the string from K^n. Administrator *A* of the Information System (IS) possesses the map *F* in *n*-variables and its trapdoor accelerator *T*. He/she is going to give secure access to the resources of IS to trusted user *U*. So *A* and *U* executes selected protocol of Noncommutative Cryptography in terms of special subsemigroup *S* of the affine Cremona semigroup of all multivariate maps of K^n into itself. The output of the protocol *X* can be used by *A* and *U* for the mutual identification. *U* sends *X(t)* to *A* who compares it with own computation of *X(t)*. Administrator creates the map *F* of the same degree *deg (X)* of the affine space of K^n

Administrator sends *F+X* to *U*. User restores *F*. Now *A* is able to create pseudorandom or genuinely random password $(p_1, p_2, ..., p_n) = p$ as the condition to enter the system. Administrator solves the equation $F(x)=b$ and sends the solution $x=(d_1, d_2,..., d_n)=d$ to the user together with the link for entering the password. User *U* gets the
password as $F(d_1, d_2,...., d_n)$.
Administrator has the option to change the password several times working with the same map *F* with the trapdoor accelerator. He/she is able to change *F* via a new session of the protocol and delivery scheme. Some modifications of this procedure are discussed in the conclusion of the paper.
The security of this scheme rests on the security of selected Postquantum Protocol on Noncommutative Cryptography. We describe Twisted Diffie-Helman protocol which use the complexity of Conjugation Power Problem of the subsemigroup of $^nCS(K)$ satisfying property *P*. The general idea of this scheme is given in [11], some other protocols and platforms can be found in [8] or [9]. Some of them use the semigroup $^nES(K)$ of Eulerian transformations (see [12]).

This paper is dedicated to the implementation of the scheme with constructions of graph based multivariate maps of prescribed degree and density with the trapdoor accelerators. We use the platforms generated by the transformations of densities *O(1)* or *O(n)*. Recall that the density of multivariate map *F* is a maximal value of densities of $fi= F(x_i)$, $i=1, 2, ...,n$ which are numbers of monomial terms of these multivariate polynomials. We define the global density *gden(F)* as $den(f_1)+den\ (f_2)+...+den(f_n)$.

The problem of safe key establishment and further key management is especially important currently when solution has to be secure in sense of Postquantum Cryptography. Research on this direction canbe found for instance in [13]-[15] where authors the postquantum technique different from Multivariate Cryptography. The description of one of the protocols of Noncommutative Cryptography and modifications of described above scheme of multivariate key establishment is given in the next section.

2. Twisted Diffie -Hellman protocol and multivariate key establishment.

Assume that Alice and Bob are going to work with multivariate maps of the affine space K^n where *K* is finite commutative ring and elaborate the collision multivariate map. Assume that

Alice decides to work with subsemigroup H of the Cremona semigroup ${}^nCS(K)$ of all multivariate maps of K^n to itself. Assume that all used elements are written in the form
$x_i \longrightarrow fi(x_1, x_2,..., x_n)$, $fi \in K[x_1, x_2,..., x_n]$ and each fi is written as the sum of monomial terms written lexicographically. Let noncommutative subsemigroup H contains invertible elements and satisfies to property P mentioned in previous section.
Assume that H consists of elements of density $O(1)$ and degree $O(n)$. Explicit constructions of such subsemigroups are given in [12] for each par (K, n). The complexity .of single multiplication in H in this case is $O(n^2)$. We can use subgroups H as above of prescribed degree d, $d=O(1)$ and density $O(n^{\alpha})$, $0<\alpha$. In this case the complexity of single multiplication is $O(n^{\alpha d+1})$ (see [8]).

Alice selects invertible element h and element g of H of densities $O(1)$. She sends g and h to her partner Bob via open channel. Next the correspondents conduct twisted Diffie Hellman protocol of Noncommutative Cryptography. Alice selects parameters $k(A)$ and $r(A)$. Alice sends $y(A)=h^{r(A)}g^{k(A)}h^{-r(A)}$ to Bob. He selects parameters $k(B)$ and $r(B)$ to compute $y(B)=h^{r(B)}g^{k(B)}h^{-r(B)}$ and send its standard form to Alice.
At the second stage of the algorithm Alice and Bob computes the collision map Y as $h^{r(A)}y(B)^{k(A)}h^{-r(A)}$ and $h^{r(B)}y(A)^{k(B)}h^{-r(B)}$ respectively.
Algorithm requires $O(1)$ multiplications in the semigroup H. So the complexity .of this algorithm is defined by the complexity of single multiplication.. Note that Bob and adversary has elements g and h but the subgroup H is unknown for them.
The solution of Conjugacy Power Problem in polynomial time in the case of affine Cremona semigroup ${}^nCS(K)$ is currently unknown. This argument is in the favour of the post quantum security of protocol.
Assume that elements g and h of H as above are prescribed degree d, $d=O(1)$ and density $O(n^{\alpha})$, $0<\alpha$.
The section 3-6 of this paper are dedicated to graph based explicit constructions of bijective multivariate map F on the affine space K^n of prescribed degree and density with the trapdoor accelerator. In the Appendix we describe the implementation of such algorithm in the selected cases.

We can use subsemigroups H and maps F with trapdoor accelerator to modify the key establishment scheme of previous section.
We assume that both parties has mutually known authentication passwords p_A (administrator) and p_B (trusted user). Tuples p_A and p_B are located in the safe data base of the system.
1 option. Authentication protocol with the multivariate platform satisfying the property P. So administrator Alice and IS user Bob have collision multivariate map G. Alice safely set the link to enter the system with the password of form $G(t)$ where t is the concatenation of p_B and p_A. Bob enters the initial password $G(t)$ and gets the access to the system. Alice can send a new access information r to Bob together with the link to access the system with the password $G(r)$. The tuple r can be of pseudorandom or genuinely random nature .
Note that Bob can make request to change the password and send r toAlice. She sets the access password as $G(r)$ and sends the link to Bob.
Alice or Bob can change the password several times. If they agree to make just single protocol adversary need to intercept quite many pairs $(r_i, G(r_i))$ and try to approximate map G. It is in fact difficult because Alice and Bob keep $H(r\ )$ safely. Only r_i are delivered via the open channel. In the case of quadratic map Alice can change the access password $O(n^{\alpha})$, $\alpha<2$.

The adversary can use specific features of the multivariate platform. Alice and Bob have to share some elements g_i, $i=1, 2,..., k$ from the platform. So adversary can try to investigate the platform generated by this elements. He/she can use specific features of the platform like a low degree and densities of elements. Sure that Alice and Bob can start new session of the protocol with other generators.

2 option. Alice can take arbitrary multivariate map F of degree at most d and sends $F+G$ to Bob. This steganographic one time pad like action is safe. So Bob Restores F. He sends $F(t)$ to Alice. She compares the received value with the her own computation of $F(t)$ with the registered in system t. Alice takes the tuple r as above sends it to Bob and set the link with the entering condition in the form of the password $F(r)$. The complexity to form the password for both parties after conducting single protocol is $O(n^{d+1})$. To change F Alice and Bob need to start a new protocol.

3 option. Let us assume that Alice creates the bijective multivariate map F of degree d with the trapdoor accelerator T which allows her to compute the reimage in time $O(n^{\alpha})$ where α is smaller than $d+1$. She sends $F+G$ to Bob. Bob sends $F(t)=c$. Alice compares $F^{-1}(c)$ with the registered t. Next Alice takes tuple r and computes $F^{-1}(r) =c$ and sends c to Bob. He restores r as $F(c)$. In this case the knowledge of T allows Alice to compute c for $O(n^{\alpha})$.

4 option. Bob has (F, T) and sends $F + G$ to Alice. Bob sends $F(t)$. Alice compares it with her own independent computation of $F(t)$. She sets r and forms the link with entering condition r, computes $c=F(r)$ and sends it to Bob via open channel. So the public user can complete r as $F^{-1}(c)$ the procedure for $O(n^{\alpha})$. In this case adversary has to intercept pairs (c, F^{-1}) but he has to approximate F^{-1} to get the procedure to enter the system. This is essentially harder task than the approximation of F.

3. Linguistic graphs of type (1, 1, n-1) and multivariate maps.

Missing definitions of Incidence Structures Theory or Graph Theory reader can find in [16], [17]. Let K be a commutative ring with unity. Recall that incidence structure is a triple (P, L, I) where P is the set of points, L is the set of lines and I is a bipartite graph with the partition sets P and L. We identify I with the corresponding binary relation on the disjoint union of P and L.

Let $P=K^n$ and $L=K^n$. We identify points with tuples of kind $(x)=(x_1, x_2,..., x_n)$ and lines with tuples $[y] =[y_1, y_2,..., y_n]$. Brackets and parenthesis are convenient to distinguished type of the vertex of the graph. If (x) and $[y]$ are incident $(x)I[y]$ if and only if the following relations hold.

$a_2x_2-b_2y_2=f_2(x_1, y_1)$,

$a_3x_3-b_3y_3=f_3(x_1, x_2, y_1, y_2)$,

$\dots$,

$a_nx_n-b_ny_n=f_n(x_1, x_2,..., x_{n-1}, y_1, y_2, ..., y_{n-1})$,

where a_j and b_j , $j = 2, 3, . . . , n-1$ are not zero divisors, and $f_j \in K[x_1. x_2\_, ... x_{j-1}, y_1, y_2,..., y_{n-1}]$, $j=2, 3,..., n$ are multivariate polynomials with coefficients from K (see [8], [9] and further references). The color $\rho(x) = \rho((x))$ (and $\rho(y) = \rho([y]))$ of point (x) (line $[y]$) is defined as the projection of an element (x) (respectively $[y]$) from a free module on its
initial coordinate. As it follows from the definition of linguistic
incidence structure, for each vertex of incidence graph there exists a unique neighbour of a chosen color.

We say that a linguistic graph is of Jordan-Gauss type if the map $[(x), [y]] \longrightarrow (f_2(x_1, y_1), f_3(x_1, x_2, y_1, y_2), \ldots,$
$f_n(x_1, x_2, \ldots, x_{n-1}, y_1, y_2, \ldots, y_{n-1}))$ is a bilinear map into K^{n-1}.
Thus, all f_i are special quadratic maps. In the case of Jordan-Gauss graphs, the neighbourhood of each vertex is given by the system of linear equations written in its row-echelon form.
Let $I_{n-1}=I_{n-1}(K)$ be a linguistic graph defined over the commutative ring K. Foreach $b \in K$ and $(p) = (p_1, p_2, \ldots, p_n)$, there is the unique neighbour $[l] = N_b(p)$ of the point with the color b. Similarly, for each $c \in K$ and line $l = [l_1, l_2, \ldots, l_n]$ there is the unique neighbour $(p) = N_c([l])$ of the line with the color c.
On the sets P and L of points and lines of the linguistic graph, we define jump operators $J = J_b(p) = (b, p_2, p_3, \ldots, p_n)$ and $J = J_b([l]) = [b, l_2, l_3, \ldots, l_n]$ where $b \in K$.
Let $i(1), i(2), \ldots, i(k)$ be an increasing sequence of elements from $\{2, 3, \ldots, n\}$ and polynomials $g_{i(s)}(x_1, x_2, \ldots, x_{i(s)}) \in K[x_1, x_2, \ldots, x_{i(s)}]$, $s=1, 2, \ldots, k$ such that for each pair of vertexes v and w with coordinates $v_1, v_2, \ldots, v_n$ and $w_1, w_2, \ldots, w_n$ from the same connected component of I the equalities $g_s(v_1, v_2, \ldots, v_{i(s)}) = g_s(w_1, w_2, \ldots, w_{i(s)})$ for $s=1, 2, \ldots, k$. In this case we refer to g_s, $s=1, 2, \ldots, k$ as family of triangular connectivity invariants of the linguistic graph $I_{n-1}(K)$ of type $i(1), i(2), \ldots, i(s)$.

Examples. Natural examples of Jordan -Gauss graphs of can be obtained as induced subgraphs of geometries of Kac-Moody group G. This group G contains Borel subgroups B^+ and B^- generated by root subgroups corresponding to positive roots. Standard parabolic subgroups P_i contains B^+. The geometry of G is defined as disjoint union of $(G:G_i)$ with the incidence relation $I: gG_i\, I gH_j$ if the intersection $gG_i \cap hG_i$ is not an empty set and type function t:
$t(gG_i)=i$. As it follows from [18] (see [8] and further references) the restriction of I onto the orbits of B^- containing P_i and P_j, $i \neq j$ is Jordan Gauss graph. If the rank n is 2 this is a linguistic graph of type $(1, 1, n-1)$. In the case of the finite field F_q, $q>2$ and finite Weyl groups (A_2, B_2, G_2) these graphs are bipartite graphs of orders $2q^2$, $2q^3$ and $2q^5$ correspondently.
In case when Weil group is infinite Dihedral group this graph is an infinite the corresponding q-regular graphs, but projections of partition sets on first n coordinates defines interesting Jordan-Gauss graphs $\Gamma_n(F_q)$ with well defined projective limit.
Special modifications $D(n, q)$ of $\Gamma_n(F_q)$ in the case of Kac-Moody algebras with the Cartan matrix

$$\begin{bmatrix} 2 & -2 \\ -2 & 2 \end{bmatrix}$$

provides explicit construction of graphs of large girth of Extremal Graph Theory, they are used for the constructions of LDPC codes in satellite communications (see [19] and further references).
If we simply consider general commutative ring K we obtain Jordan - Gauss graphs $I_n=D(n, K)$, $n \geq 2$ of type $(1, 1, n-1)$ which have triangular connectivity invariants a_s, $s=1, 2, \ldots, t$, $t= [(n+2)/4]-1$ of the type $i(1), i(2), \ldots, i(s)$ (see [3] and further references). These invariants define the partition of PUL into connected components if $char(K)$ is odd, i. e. two vertexes v and w are in the same connected component if and only if $a_1(v_1, v_2, \ldots, v_{i(s)}) = a_s(w_1, w_2, \ldots, w_{i(s)})$ for each $s=1, 2, \ldots, t$. In general case for arbitrary tuple $d=(d_1, d_2, \ldots, d_t)$ from K^t the totality ${}^dD(n, K)$ of tuples x with coordinates such that the conditions $a_s(x_1, x_2, \ldots, x_{i(s)}) = d_s$, $s=1,2,\ldots, t$ hold is nonempty set. Edge transitivity of $D(n, K)$ implies that set of vertexes of $D(n, K)$ is divided into classes ${}^dD(n, K)$, $d \in K^t$. The restriction of binary relation I on the set ${}^dD(n, K)$ is a bipartite graph ${}^dCD(n, K)$ with

partition sets isomorphic to K^{n-t}. All graphs ${}^{d}CD(n, K)$ are isomorphic. So we may omit index d and write simply $CD(n, K)$.
Graphs $CD(n, q)=CD(n, F_q)$, $q>2$ were introduced in [2]. Results on the triangular invariants for graphs $D(n, K)$ are observed in [3].
In fact graphs $CD(n, q)$ are connected if $q\neq 4$. In the case of the field F_4 this graph has exactly 4 connected components for each value of n, $n>2$.
We present the description of graphs $D(n, K)$ and their triangular connectivity invariants in the Section 3.

Algorithm 1.
Below we introduce the algorithm of generating multivariate maps on the selected partition set of linguistic graph $I_{n-1}(K)$ of type $(1, 1, n-1)$ with the triangular connectivity invariants g_s, $s=1, 2, \ldots, k$.
Assume that R is the extension of commutative ring K. Then we can associate graph ${}^{R}I_{n-1}(K)$ with the graph $I_{n-1}(K)$ such that partition sets of new graph are isomorphic to R^n but the incidence relation is given by the same system of equations with the coefficients from K. Assume that g_s, $s=1, 2, \ldots, k$ as family of triangular connectivity invariants of the linguistic graph $I_{n-1}(K)$ of type $i(1), i(2), \ldots, i(s)$.
In particular we can take list of variables $z_1, z_2, \ldots, z_n$ and take $R=K[z_1, z_2, \ldots, z_n]$.
We take the special point $v_0=(z_1, z_2, \ldots, z_n)$ parameter k and the sequence of colours $f_1(z_1, g_1(z_1, z_2,\ldots, z_{i(s)}, g_2(z_1, z_2,\ldots, z_{i(2)}),\ldots, g_s(z_1, z_2,\ldots, z_{i(s)}))=h_1(z_1, z_2,\ldots, z_{i(s)})$,
$f_2(z_1, g_1(z_1, z_2,\ldots, z_{i(s)}, g_2(z_1, z_2,\ldots, z_{i(2)}),\ldots, g_s(z_1, z_2,\ldots, z_{i(s)}))=h_2(z_1, z_2,\ldots, z_{i(s)})$,
$\ldots$, $f_k(z_1, g_1(z_1, z_2,\ldots, z_{i(s)}, g_2(z_1, z_2,\ldots, z_{i(2)}),\ldots, g_s(z_1, z_2,\ldots, z_{i(s)}))=h_k(z_1, z_2,\ldots, z_{i(s)})$, where $f_j \in K[y_1, y_2, \ldots, y_{i(j)+1}]$ and the equation $f_k(z_1, a_1, a_2, \ldots a_{i(s)})=b$ has unique solution for each tuple of parameters $a_1, a_2, \ldots, a_{i(s)}, b$ with coordinates from K.
Assume that we have some bijective polynomial map h on the commutative ring K.
We refer to this requirement on h_k as *reversibility condition*. We consider the walk on vertices of ${}^{R}I_{n-1}(K)$ with the starting point v_0 and consecutive elements $v_1, v_2, \ldots, v_k$ of colours $h_1, h_2,\ldots, h_k$ with the last vertex v_k with coordinates $h_k(z_1, z_2,\ldots, z_{i(s)})$, $u_2(z_1, z_2, \ldots, z_n)$, $u_3(z_1, z_2, \ldots, z_n)$, $\ldots$, $u_n(z_1, z_2,\ldots, z_n)$.
The vertex v_k is the point if k is even and v_k is the line if k is odd. Finally we apply operator $\mathcal{J}_g$, $g=h(h_k)$ to v_k and get the vertex v= $(h(h_k(z_1, z_2,\ldots, z_{i(s)}), u_2(z_1, z_2, \ldots, z_n), u_3(z_1, z_2, \ldots, z_n), \ldots, u_n(z_1, z_2,\ldots, z_n)$.

Proposition 3. 1. *The reversibility condition implies that polynomial map* $F:z_1\longrightarrow h(h_k(z_1, z_2,\ldots, z_{i(s)}))$, $z_2\longrightarrow u_2(z_1, z_2, \ldots, z_n)$, $z_3\longrightarrow u_3(z_1, z_2, \ldots, z_n),\ldots, z_n\longrightarrow u_n(z_1, z_2, \ldots, z_n)$ *is a bijective transformation. The information on the graph, its triangular invariants, the sequence of colours* $f_1, f_2,\ldots, f_k$ *is a trapdoor accelerator.*

The procedure of reimage computation is the following. Assume that the value of F on some unknown tuple $(z_1, z_2, \ldots, z_n)$ is $(c_1, c_2, \ldots, z_n)$. We compute $h^{-1}(c_1)=d$ and take the vertex $v_k=(d, c_2, c_3,\ldots, c_n)$ and the equation $f_k(z_1, g_1(z_1, z_2,\ldots, z_{i(1)}), g_2(z_1, z_2,\ldots, z_{i(2)}),\ldots, g_s(z_1, z_2,\ldots, z_{i(s)}))=d$. We compute the values $g_j(z_1, z_2,\ldots, z_{i(j)})$ as $g_j(d, c_2, c_3,\ldots, c_{i(j)})=d_j$, $j=1,2,\ldots, s$. The reversibility condition allows us to solve the equation $f_k(z_1, d_1, d_2,\ldots, d_s)=d$ for the variable z. Let $z=\alpha$. We compute the values of $f_j(\alpha, d_1, d_2, \ldots, d_s)=d_j$, $j=1, 2, \ldots, k-1$. We form the sequence of vertices with the starting point v_k and colours $d_{k-1}, d_{k-2}, ..., d_1, \alpha$. Last vertex of this sequence is the point $(\alpha,\alpha_1,...,\alpha_n)=(z_1, z_2, ..., z_n)=F^{-1}(c_1, c_2,..., c_n)$.

Algorithm 2.
We take the sequence of colours $h_1, h_2, ..., h_{k-1}$ and change h_k for the constant γ. So we take the walk as the sequence $v_0, v_1,...., v_{k-1}$ and compute $v'_k=N_\gamma(v_{k-1})$, $v_{k+1}=J_h(v'_k)$ where $h=h_k$. Recall that the first coordinate of the vertex v_{k+1} is $f_k(z_1, g_1(z_1, z_2,..., z_{i(s)}), g_2(z_1, z_2,..., z_{i(2)}),..., g_s(z_1, z_2,..., z_{i(s)}))=h_k(z_1, z_2,..., z_{i(s)})$, coordinates $(h_k(z_1, z_2,..., z_n), w_2(z_1, z_2, ..., z_n), w_3(z_1, z_2, ..., z_n),..., w_n(z_1, z_2, ..., z_n)$.

Proposition 3.2. *The reversibility condition implies that polynomial map* $H: z_1 \longrightarrow h_k(z_1, z_2,..., z_{i(s)})$, $z_2 \longrightarrow w_2(z_1, z_2, ..., z_n)$, $z_3 \longrightarrow w_3(z_1, z_2, ..., z_n)$,..., $z_n \longrightarrow w_n(z_1, z_2, ..., z_n)$ *is a bijective transformation. The information on the graph, its triangular invariants, sequence of colours* $f_1, f_2,..., f_k$ *and constant* γ *is a trapdoor accelerator.*

The procedure of reimage computation is the following. Assume that the value of H on some unknown tuple $(z_1, z_2, ..., z_n)$ is $(c)=(c_1, c_2, ..., c_n)$. We compute $J_\gamma(c)=(\gamma, c_2, c_3,..., c_n)=v_{k-1}$. Recall that the first coordinate of $\mathbf{v}_{k+1}$ is $f_k(z_1, g_1(z_1, z_2,..., z_{i(s)}), g_2(z_1, z_2,..., z_{i(2)}),..., g_s(z_1, z_2,..., z_{i(s)}))$ Noteworthy that $g_1(z_1, z_2,..., z_{i(s)})= g_1(\gamma, c_2, c_3, ..., c_{i(s)})=d_1$, $g_2(z_1, z_2,..., z_{i(2)}) = g_2(\gamma, c_2, c_3, ..., c_{i(s)})=d_2$,..., $g_s(z_1, z_2,..., z_{i(s)}) = g_s(\gamma, c_2, c_3, ..., c_{i(s)})=d_s$.
We take the equation is $f_k(z_1, d_1, d_2,..., d_s)$. The reversibility condition allows us to solve it for z_1. Let $z_1=\alpha$ be the solution.
We compute $fj(\alpha, d_1, d_2,..., d_s)=b_j$, $j=1, 2,..., k-2$ and take the path of vertexes of the graph with starting vertex v_{k-1} and consecutive colours $b_{k-2}, b_{k-3},..., b_1, \alpha$. The last vertex is $(z_1, z_2,..., z_n)=(\alpha,\alpha_2, \alpha_3\_...,\alpha_n)= H^{-1}(c_1, c_2,..., c_n)$.
Examples of h_k satisfying the reversibility condition:
$(pr_1(g_1, g_2, ..., g_s)+1)z_1 + r_2(g_1, g_2, ..., g_s)$ where $r_1, r_2 \epsilon Z_q[y_1, y_2, ..., y_s]$ in the case $K=Z_q$, $q=p^m$; $h(r_1(g_1, g_2, ..., g_s))(z_1)^t + r_2(g_1, g_2, ..., g_s)$, where $r_1, r_2 \epsilon F_q[y_1, y_2,..., y_s]$, $h(y)$ has no linear terms in its decomposition in $F_q[y]$ in the case of $K=F_q$, $q=p^m$, $(t, q)=1$; $\alpha z_1 + r(g_1, g_2, ..., g_s)$ where $\alpha \epsilon K^*$, $r \epsilon K[y_1,y_2, ..., y_s]$ in the case of general commutative ring with unity.
If linguistic graph coincides with $D(n, K)$ or their modifications presented in [3] then their connectivity invariants can be used for the constructions of multivariate maps with prescribed degree and density.

4. Jordan-Gauss graphs D(n, K) and their modifications.

J Jordan-Gauss graph $D(n, K)$ of type $1, 1, n-1$ is defined as incidence structure I_{n-1} with the partition sets isomorphic to K^n .The point $(p)=(x_1, x_2,..., x_n)$ of this graph is incident with the line $[y]=[y_1, y_2, ..., y_n]$, if the following relations between their coordinates hold: $x_2-y_2=y_1x_1$, $x_3-y_3=y_2x_1$, $x_4-y_4=y_1x_2$, $x_i-y_i=y_1x_{i-2}$, $x_{i+1}-y_{i+1}=y_{i-1}x_1$, $x_{i+2}-y_{i+2}=y_ix_1$, $x_{i+3}-y_{i+3}=y_1x_{i+1}$ where $i\geq 5$.
As it is easy to see the projective limit $D(K)$ is well defined. In fact if K is an integral domain the biregular graph $D(K)$ is the forest (see [3] and further references).
Recall that graphs $D(n, F_q)=D(n, q)$ are the modifications of $\Gamma_n(F_q)$ in the case of Kac-Moody algebras with the Dynkin diagram *Ext* A_1 (A_1 with wawe or extended Dynkin diagram of A_1). It is convinient to use positive roots of this root system as indexes of points and lines. The real roots are $k+1\alpha_1+k\alpha_2$, $k\alpha_1+(k+1)\alpha_2$ where $k\geq 0$ α_1, α_2 are simple roots and and the imaginary roots are

$k\alpha_1+k\alpha_2$ where $k\geq 1$. We identify roots with their coordinates in the lattice generated by simple roots $(k+1, k)$, $(k, k+1)$ and (k, k). The modification uses "twins'' of imaginary roots indexed as $(k, k)'$.

So graph $D(K)$ can be defined as the incidence with lines $[y]=[y_{01}, y_{11}, y_{12}, y_{21}, y_{22}, y'_{22}, \ldots, y'_{ii}, y_{i\,i+1}, y_{i+1,i}, y_{i+1,i+1} \ldots]$, points $(x)=(x_{10}, x_{11}, x_{12}, x_{21}, x_{22}, x'_{22}, \ldots, x'_{ii}, x_{i\,i+1}, x_{i+1,i}, x_{i+1,i+1} \ldots)$ and incidence relation given by equations

$x_{ii}-y_{ii}=x_{10}\, y_{i-1,i}$;

$x'_{ii} - y'_{ii} = x_{i,i-1}\, y_{01}$;

$x_{i,\,i+1} - y_{i,i+1} = x_{ii}\, y_{01}$; (1)

$x_{i+1i} - y_{i+1,i} = x_{10} y'_{ii}$.

This four relations are defined for $i\geq 1$, ($x'_{11}= x_{11}$, $y'_{11}= y_{11}$).

Note that tuples (x) and $[y]$ have finite support, i. e. only finite number of their coordinates differ from zero. Coordinates x'_{ii} and y'_{ii} correspond to the root $(i, i)'$.

Further we interpret $D(n, K)$ as homomorphic images of $D(K)$ obtained via the projection of points and lines into their first n coordinates. The incidence of points and lines of $D(n, K)$ is defined by the first $n-1$ equations of the system (1).

For the description of triangular connectivity invariants of $D(n, K)$, it will be convenient for us to define $x_{-1,0} = y_{0,-1} = x_{1,0} = y_{0,1}= 0$, $x_{0,0}= y_{00}= -1$, $x'_{0,0} = y'_{0,0} = -1$, $x_{1,1} = x'_{1,1}$, $y_{1,1} = y'_{1,1}$ and to assume that our equations (1) are defined for $i \geq 0$.

Let $u = (u_\alpha, u_{11}, u_{12}, u_{21}, \ldots, u_{r,r}, u'_{r,r}, u_{r\,r+1}\, u_{r,+1,r}, u_{r+1,r+1}, \ldots)$, $2 \leq r \leq t$, $\alpha \in \{(1, 0), (0,1)\}$ be 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 $[2,t]$, $t=[(n+2)/4]$.

Graph $D(k, K)$ has triangular connectivity invariants $g_s=a_{s+1}(u)$, $s=1, 2, \ldots, t-1$ of type $i(1), i(2),\ldots, i(s)$ where $i(1)=(2, 2)'$, $i(2)=(3, 3)'$, ..., $i(t-1)=(t, t)'$.

In introduced above set Δ of not simple roots (j, j), $(j+1, j)$, $(j, j+1)$, $(j+1, j+1)'$ where $j\geq 1$. We assume that each equation of (1) is identified by the root which appears as the index of the coordinates in the lefthand side of the equality. We consider subset Δ' of elements of $(j+1, j)$, $(j+1,j+1)'$, $j\geq 2$.

We assume that the elements of Δ are ordered accordingly to the list of coordinates of $D(K)$ in the presentation (1). Let $\Delta'(i+1, i)$ be the set of roots from A' which are higher than $(i+1, i)$ with respect to the defined order.

Assume that $\Delta'((i+1, i+1)')$ be the list of roots of Δ' with the order higher than $(i+1,i+1)'$. As it was proven in (i) deletion of coordinates with indexes from $\Delta'(i+1, i)$ and $\Delta'((i+1, i+1)')$ defines the homomorphism Ψ_i and Ψ'_i of graph $D(K)$. The incidence of elements of the images are defined by equations indexed by elements Δ- $\Delta'(i+1, i)$ and Δ- $\Delta'((i+1, i+1)')$ respectively.

The image of Ψ_1 is known as graph $A(K)$. The projection of points and lines $A(K)$ on its first n coordinates defines known graphs $A(n, K)$. Graphs $A(n, K)$, $n \geq 4$ differs from $D(n,K)$.

We introduce graphs ${}^iB(K)$ and ${}^iB'(K)$ as homomorphic images *of* Ψ_i and Ψ'_i .

We consider projections of points and lines of these graphs onto first n coordinates together with first $n-1$ equations. The images of these homomorphisms will be denoted as ${}^iB(n, K)$ and ${}^iB'(n, K)$ for $n \geq 4i$ and $n \geq 4i+2$ respectively.We use roots in their definitions for the description of some triangular connectivity invariants.

Proposition 4. 1. *Graphs* ${}^iB(n, K)$ *and* ${}^iB'(n, K)$ *has connectivity invariants* $g_s=a_{s+1}(u)$, $s=1, 2, \ldots, i-2$ of type $j(1), j(2),\ldots, j(i-2)$ *where* $j(1)=(2, 2)'$, $j(2)=(3, 3)'$, ..., $j(i-2)=(i, i)'$.

Let $T(i)=\{(2, 2)', (3, 3)', \ldots, (i, i)'\}$ and S its proper subset, $j(S)$ is minimal number k such that $(k, k)'\in \mathcal{J}(S)$.

We consider graphs ${}^iB_S(n, K)$ and ${}^iB'_S(n, K)$ obtained by deletion of coordinates $(r, r)'$, $(r, r)' \epsilon S$ from points and lines and replacement condition

$x_{r+1, r} - y_{r+1,r} = x_{10}y'_{r,r}$ by $x_{r+1, r} - y_{r+1,r} = x_{10}y_{r,r}$

These graphs were introduced in [3] in different notations.

Assume that $j(S)>2$ then ${}^iB_S(n, K)$ and ${}^iB'_S(n, K)$ have triangular connectivity invariant $g_s=a_{s+1}(u)$, $s=1, 2, \ldots, j(S)-2$. Note that partition sets of these graphs are isomorphic to K^{n-s} where s is the cardinality of S.

Let us consider the algorithms 1 and 2 in the cases of described graphs.

Assume that linguistic graph coincides with the Jordan-Gauss graphs presented in the Section 3 and multivariate maps F and H are defined via algorithms 1 and 2 respectively. Then the following propositions hold.

Proposition 4. 2. *Let L be element* of $AGL_n(K)$ of density $O(1)$, $k=O(1)$ and $h_1, h_2, \ldots, h_k$ *are functions of density O(1) and degree O(1).* Then transformations LF has density $O(n)$ and degree $O(1)$.

Proposition 4.3. *Let L be element of $AGL_n(K)$, $h_1, h_2, \ldots, h_{k-1}$ are functions of density O(1) and degree O(1). Assume that h_k has density O(n) and degree O(1). Then transformation LH has density O(n) and degree O(1).*

Corollary. Let L_1 be general element of $AGL_n(K)$. Then transformations LFL_1 and LHL_1 are pseudo quadratic. It means that for the standard forms of LFL_1 and LHL_1 the computation of their values on the given tuple costs $O(n^3)$.

In this section we propose the generalisation of implemented scheme of Algorithm 1.

Let $I_{n-1}(K)$ be the linguistic graph of type $(1, 1, n-1)$. Assume that g_s, $s=1, 2, \ldots, k$ is the family of its triangular connectivity invariants of type $i(1), i(2), \ldots, i(s)$. Let $(z_1, z_2, \ldots, z_n)$ be the element of pointset $(K[z_1, z_2, \ldots, z_n])^n$ of $I_{n-1}(K[z_1, z_2, \ldots, z_n])$.

We compute the symbolic expressions $g_s(z_1, z_2, \ldots, z_{i(s)})$ for $s=1, 2, \ldots, k$. We select element $z=z(y_1, y_2, \ldots, y_{k+1})$ from $K[y_1, y_2, \ldots, y_{k+1}]$ and compute the expression $b(z_1, z_2, \ldots, z_{i(k)})=z(z_1, g_1(z_1, z_2, \ldots, z_{i(1)}), g_2(z_1, z_2, \ldots, z_{i(2)}), \ldots, g_k(z_1, z_2, \ldots, z_{i(k)}))$. We take positive integer l and consider the sequence of colours

$h_1= b(z_1, z_2, \ldots, z_{i(k)})$, $h_2=z_1+\beta$, $\beta \epsilon K$, $h_i=h_{i-2}+\beta_i$, $\beta_i \epsilon K^*$.

Proposition 4. 4. *Let F be the map of Algorithm 1 with the described above data in the case of one of the graphs $D(n, K)$, ${}^iB_S(n, K)$ and ${}^iB'_S(n, K)$, ${}^iB(n, K)$, ${}^iB'(n, K)$ and bijective h from K[x] of degree s. Assume that degree of $b(z_1, z_2, \ldots, z_{i(k)})$ is t. Then degree of F is max (2t+1, st) if l is odd and max(t+2, st) if l is even. Then degree of F is max (2t+1, s) if **l** is even and max(t+2, st) if l is odd.*

In the cases of selected finite commutative rings of kind F_q or Z_q we take element L of $AGL_n(K)$ of the density $O(1)$, $L_1 \epsilon AGL_n(K)$ and generate the pseudo quadratic standard form of $G= LFL_1$ where F satisfies the conditions of Proposition 4.2 with the multivariate polynomial $b(z_1, z_2, \ldots, z_{i(k)})$ of density $O(1)$. So we get multivariate public key with the pseudo quadratic map of prescribed based on the trapdoor accelerator of Proposition 4.1.

5. Remarks on implemented cases of degree 2 and 3 and other options

The implementation of Algorithm 1 in the case of graphs $D(n, K)$ in the case of $K=F_q$, $q=2^s$ with $h_1=z_1+\beta_1$, $h_2= z_1+\beta_2$, $h_i=h_{1-2}+\beta_i$, $i \geq 2$ and $h(x) =\alpha x^2+\beta$, where $\beta_1 \in K$, $\beta_2 \in K$, $\beta \in K$, $\alpha \in K^*$, $\beta_i \in K^*$ for $i \geq 2$ was described in the paper [20].

The description of the implementation of Algorithm 2 in the case of $D(n, K)$, $K=F_q$, $q=2^s$, even parameter k special colours $h_1=\alpha_1$, $h_2=z_{1,0}+b_1$, $h_3=\alpha_3$, $h_4=z_{1,0}+b_2, \ldots$, $h_{k-2}=z_{1,0}+b_{k-2}$, $\alpha_{k-1}=\gamma$, $h_k=\alpha z_{1,0}+ \lambda_2 a_2(z_{1,0}, z_{1,1}, \ldots, z'_{2,2})+ \lambda_3 a_3(z_{1,0}, z_{1,1}, \ldots, z'_{3,3})+ \ldots +\lambda_t a_t(z_{1,0}, z_{1,1}, \ldots, z'_{t,t})$, $t=[(n+2)/4]$, where α_i, b_i and λ_i are constants, is given in [21].

If we change $K=F_q$ for $K=Z_q$ without the change of above written requirements on h_i, $i=1, 2, \ldots$ we get the new case for the implementation. The results of corresponding computer simulations are below.

We have written a program for generating elements and for encrypting a text using above algorithm. The program is written in SAGE. We used an MacBook with a Intel Core 1,2 GHz processor, 8GB RAM, and the macOS Monterey operating system. We have implemented three **cases:**

case 1. L_1 and L_2 are identities, **case 2**. L_1 and L_2 are maps of the kind $z_{1,0} \longrightarrow z_{1,0} + a_2 z_{1,1} + a_3 z_{1,2} + \cdots + a_t z_{t,t}$, $z_{1,1} \longrightarrow z_{1,1}$, $z_{1,2} \longrightarrow z_{1,2}, \ldots, z_{t,t} \longrightarrow z_{t,t}$, with a_i 0, $i = 1, 2, \ldots, n$ (linear time of computing for L_1 and L_2), **case 3**. $L_1 = Ax + b$, $L_2 = A_1 x + b_1$; matrices A, A_1 and vectors b, b_1 mostly have nonzero elements.

In Tables 1, 2 and 3, we describe the numbers of monomials in **case 1** for different sizes of the field. Tables 10,11,12 shows the generation time of the encryption.

In Tables 4, 5 and 6, we describe the numbers of monomials in **case 2** for different sizes of the field. Tables 13,14,15 shows the generation time of the encryption.

In Tables 7, 8 and 9, we describe the numbers of monomials in **case 3** for different sizes of the field. Tables 16,17,18 shows the generation time of the encryption.

Remark. After the change of the graph $D(n, K)$ on ${}^iB(n, K)$, ${}^iB_S(n, K)$, $i>1$, $n \geq 4i$ or ${}^iB'(n, K)$, ${}^iB'_S(n, K)$ with $i>1$, $n \geq 4n+2$ the map H is also quadratic transformation.

Table 1. Number of coefficients, ring of size 2^8, Case 1.

	Vector size			
Pass length	**16**	**32**	**64**	**128**
15	141	506	1474	3794
31	141	509	1914	5676
63	141	495	1852	7270
127	141	509	1916	7333

Table 2. Number of coefficients, ring of size 2^{12}, Case 1.

	Vector size			
Pass length	**16**	**32**	**64**	**128**
15	141	506	1474	3794
31	141	509	1914	5770
63	141	509	1917	7418
127	141	509	1917	7421

Table 3. Number of coefficients, ring of size 2^{16}, Case 1.

	Vector size			
Pass length	**16**	**32**	**64**	**128**
15	141	506	1474	3794
31	141	509	1914	5770
63	141	509	1917	7418
127	141	509	1917	7421

Table 4. Number of coefficients, ring of size 2^{8}, Case 2.

	Vector size			
Pass length	**16**	**32**	**64**	**128**
15	1021	6638	37090	175212
31	1034	6491	46899	270375
63	1075	6857	48063	367481
127	1018	6986	50212	367644

Table 5. Number of coefficients, ring of size 2^{12}, Case 2.

	Vector size			
Pass length	**16**	**32**	**64**	**128**
15	1076	7028	38664	172541
31	1077	7163	51443	290452
63	1078	7021	51403	391864
127	1065	7001	51073	391800

Table 6. Number of coefficients, ring of size 2^{16}, Case 2.

	Vector size			
Pass length	**16**	**32**	**64**	**128**
15	1078	7145	38665	178470
31	1078	7164	51758	292388
63	1078	7164	51386	391317
127	1078	7164	51764	391312

Table 7. Number of coefficients, ring of size 2^{8}, Case 3.

	Vector size			
Pass length	**16**	**32**	**64**	**128**
15	2416	17656	136665	1068347
31	2406	17862	136663	1064700
63	2419	17834	136468	1068305
127	2434	17858	136490	1068389

Table 8. Number of coefficients, ring of size 2^{12}, Case 3.

	Vector size			
Pass length	**16**	**32**	**64**	**128**

15	2448	17938	137206	1072917
31	2447	17942	137198	1072934
63	2447	17947	137183	1072803
127	2447	17946	137169	1072989

Table 9. Number of coefficients, ring of size 2^{16}, Case 3.

	Vector size			
Pass length	**16**	**32**	**64**	**128**
15	2448	17952	137275	1073226
31	2448	17952	137278	1073261
63	2447	17951	137274	1073226
127	2448	17912	137278	1073261

Table 10. Time (ms), ring of size 2^8, Case 1.

	Vector size			
Pass length	**16**	**32**	**64**	**128**
15	5	4	8	22
31	3	7	18	56
63	6	14	40	159
127	11	28	83	395

Table 11. Time (ms), ring of size 2^{12}, Case 1.

	Vector size			
Pass length	**16**	**32**	**64**	**128**
15	6	3	8	22
31	3	7	18	57
63	5	15	42	161
127	10	29	83	466

Table 12. Time (ms), ring of size 2^{16}, Case 1.

	Vector size			
Pass length	**16**	**32**	**64**	**128**
15	5	3	7	16
31	2	5	13	41
63	5	11	31	115
127	10	20	62	298

Table 13. Time (ms), ring of size 2^8, Case 2.

	Vector size			
Pass length	**16**	**32**	**64**	**128**
15	9	28	220	5602
31	7	58	688	13324
63	16	124	2008	46336
127	28	267	5034	171159

Table 14. Time (ms), ring of size 2^{12}, Case 2.

	Vector size			
Pass length	**16**	**32**	**64**	**128**
15	10	30	220	2981
31	8	56	661	9650
63	13	118	1890	33016

127	26	253	4608	129540

Table 15. Time (ms), ring of size 2^{16}, Case 2.

	Vector size			
Pass length	**16**	**32**	**64**	**128**
15	25	172	2014	78159
31	23	192	2862	90887
63	35	257	4628	143237
127	44	379	8583	257669

Table 16. Time (ms), ring of size 2^{8}, Case 3.

	Vector size			
Pass length	**16**	**32**	**64**	**128**
15	25	172	2014	78159
31	23	192	2862	90887
63	35	257	4628	143237
127	44	379	8583	257669

Table 17. Time (ms), ring of size 2^{12}, Case 3.

	Vector size			
Pass length	**16**	**32**	**64**	**128**
15	19	136	1917	76879
31	18	167	2665	97863
63	26	236	4172	138124
127	37	365	7796	215954

Table 18. Time (ms), ring of size 2^{16}, Case 3.

	Vector size			
Pass length	**16**	**32**	**64**	**128**
15	42	171	3065	118880
31	20	210	6001	170741
63	29	322	5208	703754
127	43	546	13970	886343

6. Conclusion

The expanding graphs of large girth *D(n, q)* and their generalisations *D(n, K)* defined over the commutative ring K turns out to be useful in the theory of LDPC codes, Message Authentication Codes, constructions of stream ciphers of symbolic nature, protocols of Noncommutative Cryptography , Multivariate Public Keys.

In this paper we present the applications of these graphs and their recent generalisations [3] to the design of the algorithms of key establishment.

Acknowledgements

This research is partially supported by British Academy Fellowship for Researchers under Risk 2022, British Academy/Cara/Leverhulme Research Support Grant LTRSF\100333 and UMCS Mini-Grant.

Declaration on Generative AI

The author(s) have not employed any Generative AI tools.

References

[1] A. Lubotzky, Expander Graphs in Pure and Applied Mathematics, Bulletin of the AMS,v.49, n.1, pp 113-14.

[2] Lazebnik, F., Ustimenko, V., Woldar, A.J., A new series of dense graphs of high girth. Bulletin of the AMS, vol. 32, no. 1, pp. 73--79 (1995).

[3] Chojecki, T., Erskine, G., Tuite, J. Ustimenko V. On affine forestry over integral domains and families of deep Jordan–Gauss graphs. European Journal of Mathematics 11, 10 (2025). https://doi.org/10.1007/s40879-024-00798-2.

[4] M. Polak, U. Romańczuk, V. Ustimenko, A. Wróblewska , On the applications of Extremal Graph Theory to Coding Theory and Cryptography, Electronic Notes in Discrete Mathematics, V. 43, N. 5 , 2013, pp 329-342.

[5] Ding, J., Petzoldt, A.: Current State of Multivariate Cryptography. IEEE Security \& Privacy, vol. 15, no. 4, pp. 28--36 (2017). \doi{10.1109/MSP.2017.3151328}.

[6] Buellens, W.: Improved cryptanalysis of UOV and Rainbow Improved cryptanal-ysis of UOV and Rainbow, In: Canteaut, A., Standaert, FX. (eds) Advances in Cryptology – EUROCRYPT 2021. EUROCRYPT 2021. Lecture Notes in Comput-er Science(), vol 12696. Springer, Cham.

[7] NIST PQC Digital Signature Project: TUOV Specification. \url{https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/TUOV-spec-web.pdf}, last accessed 2024/07/30.

[8] Ustimenko, V.: Graphs in terms of Algebraic Geometry, symbolic computations and secure communications in Post-Quantum world. UMCS Editorial House, Lublin (2022).

[9] V. Ustimenko, T. Chojecki, On graph based pseudo quadratic multivariate maps of prescribed degree as instruments of key establishment., Cryptology ePrint Archive (2025/ 743.

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

[11] V. Ustimenko, On new symbolic key exchange protocols and cryptosystems based on hidden tame hommorphism, Dopovidi. NAS of Ukraine, 2018, n 10, pp.26-36.

[12] V. Ustimenko, On Eulerian semigroups of multivariate transformations and their cryptographic applications. European Journal of Mathematics 9, 93 (2023), https://doi.org/10.1007/s40879-023-00685.

[13] Van Oorschot, P.C. (2020). Authentication Protocols and Key Establishment. In: Computer Security and the Internet. Information Security and Cryptography. Springer, Cham. https://doi.org/10.1007/978-3-030-33649-3_4

[14] Abdalla, M. (2014). Password-Based Authenticated Key Exchange: An Overview. In: Chow, S.S.M., Liu, J.K., Hui, L.C.K., Yiu, S.M. (eds) Provable Security. ProvSec 2014. Lecture Notes in Computer Science, vol 8782. Springer, Cham. https://doi.org/10.1007/978-3-319-12475-9_1.

[15] Tim Taubert, Christopher A. Wood: SPAKE2+, an Augmented Password-Authenticated Key Exchange (PAKE) Protocol. RFC 9383: 1-25 (2023)

[16] Bart De Bruyn, An Introduction to Incidence Geometry. Frontiers in Mathematics. Springer International Publishing Switzerland, 2016, 372 pages.

[17] R. Diestel, Graph Theory, Graduate Texts in Mathematics, Springer Berlin, Heidelberg, 2025, 455 pages.

[18] V.A. Ustimenko, U. Romanczuk. Finite geometries, LDPC codes and cryptography, Institute of Computer Science. University of Maria Curie Sklodowska University, 2012, 171 p.

[19] M. Polak, V. Ustimenko, LDPC Codes Based on Algebraic Graphs, Annales UMCS Informatica AI XII, 3 (2012) 107–119.
[20] Ward Beullens, Improved Cryptanalysis of UOV and Rainbow, In Eurocrypt 2021, Part 1, pp. 348-373. A. Lubotzky, Expander Graphs in Pure and Applied Mathematics, Bulletin of the AMS,v.49, n.1, pp 113-14.
[21] Lazebnik, F., Ustimenko, V., Woldar, A.J., A new series of dense graphs of high girth. Bulletin of the AMS, vol. 32, no. 1, pp. 73--79 (1995).
[22] Smith-Tone, D.: 2F - A New Method for Constructing Efficient Multivariate Encryption Schemes. In: PQCrypto 2022: The Thirteenth International Conference on Post-Quantum Cryptography, virtual, DC, US (2022).
[23] Smith-Tone, D.: New Practical Multivariate Signatures from a Nonlinear Modifier. IACR e-print archive, 2021/419.
[24] Smith-Tone, D., Tone, C.: A Nonlinear Multivariate Cryptosystem Based on a Random Linear Code. \url{https://eprint.iacr.org/2019/1355.pdf}, last accessed 2024/07/30.
[25] Jayashree, D., Dutta, R.: Progress in Multivariate Cryptography: Systematic Review, Challenges, and Research Directions. ACM Computing Survey, vol. 55, issue 12, No. 246, pp. 1--34 (2023). \doi{10.1145/3571071}
[26] Cabarcas, F., Cabarcas, D., Baena, J.: Efficient public-key operation in multivariate schemes. Advances in Mathematics of Communications, vol. 13, no. 2, pp. 343--343 (2019).
[27] Cartor, R., Smith-Tone, D.: EFLASH: A new multivariate encryption scheme. In: Proceedings of the International Conference on Selected Areas in Cryptography, pp. 281--299. Springer, Heidelberg (2018).
[28] Casanova, A., Faugère, J.-C., Macario-Rat, G., Patarin, J., Perret, L., Ryckeghem, J.: Gemss: A great multivariate short signature. Submission to NIST (2017).
[29] Chen, J., Ning, J., Ling, J., Lau, T. S. C., Wang, Y.: A new encryption scheme for multivariate quadratic systems. Theoretical Computer Science, vol. 809, pp. 372--383 (2020).
[30] Chen, M.-S., Hülsing, A., Rijneveld, J., Samardjiska, S., Schwabe, P.: SOFIA: MQ-based signatures in the QROM. In: Proceedings of the IACR International Workshop on Public Key Cryptography, pp. 3--33. Springer, Heidelberg (2018).
[31] Ding, J., Petzoldt, A., Schmidt, D.S.: Multivariate Public Key Cryptosystems. 2nd edn. Advances in Information Security. Springer, Heidelberg (2020).
[32] Duong, D.H., Tran, H.T.N., Susilo, W., Luyen, L.V.: An efficient multivariate threshold ring signature scheme. Computer Standards \& Interfaces, vol. 74 (2021).
[33] Faugère, J.-C., Macario-Rat, G., Patarin, J., Perret, L.: A new perturbation for multivariate public key schemes such as HFE and UOV. Cryptology ePrint Archive (2022).
[34] Canteaut, A., Standaert, F.-X. (eds.): Eurocrypt 2021, LNCS, vol. 12696, 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17–21, 2021, Proceedings, Part I. Springer, Heidelberg (2021).
[35] Saarinen, M.J., Smith, D.T. (eds.): Post Quantum Cryptography, 15th International Workshop, PQCrypto 2024, Oxford, UK, June 12-14, 2024, Proceedings, Part 2. Springer, Heidelberg (2024).
[36] Takagi, T., Wakayama, M., Tanaka, K., Kunihiro, N., Kimoto, K., Ikematsu, Y. (eds.): International Symposium on Mathematics, Quantum Theory, and Cryptography, Proceedings of MQC 2019. Open Access, Springer, Heidelberg (2021).
[37] Arai, K. (ed.): Advances in Information and Communication, Proceedings of the 2024 Future of Information and Communication Conference (FICC), Volumes 1-3. Lecture Notes in Networks and Systems, vols. 919-921, Springer, Heidelberg (2024).
[38] Ustimenko, V.: Schubert cells and quadratic public keys of Multivariate Cryptography. CEUR Workshop Proceedings ITTAP, \url{https://ceur-ws.org/Vol-3628/}, last accessed 2024/07/30.
[39] Liendo, A. Roots of the affine Cremona group. Transformation Groups 16, 1137–1142 (2011). https://doi.org/10.1007/s00031-011-9140-y.

[40] D. N. Moldovyan and N.A. Moldovyan, A New Hard Problem over Non-commutative Finite Groups for Cryptographic Protocols, International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security, MMM-ACNS 2010: Computer Network Security pp 183-194.
[41] E Sakalauskas, A Katvickis, G Dosinas Information Technology and Control 39 (1), 2010
[42] D Kahrobaei, M. Anshel, Applications of group theory in cryptography, Internal Journal of pure and applied mathematics, 2010, volume 58, N 1, 21-23.
[43] Zhenfu Cao (2012), New Directions of Modern Cryptography. Boca Raton: CRC Press, Taylor & Francis Group. ISBN 978-1-4665-0140-9.
[44] Benjamin Fine, et. al. "Aspects of Non abelian Group Based Cryptography: A Survey and Open Problems", arXiv:1103.4093, 2011.
[45] Alexei G. Myasnikov; Vladimir Shpilrain and Alexander Ushakov (2011), Non-commutative Cryptography and Complexity of Group-theoretic Problems, American Mathematical Society.
[46] P.H. Kropholler and S.J. Pride , W.A.M. Othman K.B. Wong, P.C. Wong, Properties of certain semigroups and their potential as platforms for cryptosystems, Semigroup Forum (2010) 81: 172–186.
[47] J.A. Lopez Ramos, J. Rosenthal, D. Schipani and R. Schnyder, Group key management based on semigroup actions, Journal of Algebra and its applications, 2017, vol.16,(08):1750148.
[48] Gautam Kumar and Hemraj Saini, Novel Noncommutative Cryptography Scheme Using Extra Special Group, Security and Communication Networks ,Volume 2017, Article ID 9036382, 21 pages, https://doi.org/10.1155/2017/9036382
[49] Myasnikov A., Roman'kov V. A linear decomposition attack // Groups, Complexity, Cryptology. 2015. Vol. 7. P. 81–94.
[50] Roman'kov V. A. A nonlinear decomposition attack. Groups, Complexity, Cryptology. 2017. Vol. 8, No. 2. P. 197–207.
[51] Romankov V. Two general schemes of algebraic cryptography. Groups, Complexity, Cryptology. 2018. Vol. 10, No. 2. P. 83–98.
[52] Roman'kov V. An improved version of the AAG cryptographic protocol. Groups, Complexity, Cryptology. 2019. Vol. 11, No. 1. 1 2.
[53] Tsaban B. Polynomial time solutions of computational problems in noncommutative algebraic cryptography. Journal of Cryptology. 2015. Vol. 28, No. 3. P. 601–622.
[54] Ben-Zvi A., Kalka A., Tsaban B. Cryptanalysis via algebraic spans. Advances in Cryptology – CRYPTO 2018 / eds.: H. Shachan, A. Boldyreva. Berlin: Springer, 2018. P. 1–20. (LNCS; vol. 109991).