Linear codes of Schubert type and quadratic public keys of Multivariate Cryptography

Vasyl Ustimenko

Royal Holloway University of London
Institute of Telecommunication and Global Information Space, Kyiv, Ukraine
Vasyl.Ustymenko@rhul.ac.uk

↪

Abstract. Studies of linear codes in terms of finite projective geometries form traditional direction in Coding Theory. Some applications of projective geometries are known. Noncommutative groups and semigroups defined in terms of projective geometries can serve as platforms of protocols of Post Quantum Cryptography. We introduce an idea of public keys of Multivariate Cryptography given by quadratic public rules generated via walks on incidence substructures of projective geometry with vertexes from two largest Schubert cells. It differs from the known algorithms of Code Based Cryptography and can be considered as the first attempt to combine ideas of this area with the approach of Multivariate Cryptography.

Keywords: Multivariate Cryptography, Code Base Cryptography, Projective Geometries, Largest Schubert Cells, Symbolic Computations

Funding: This research is supported by British Academy Fellowship for Researchers at Risk 2022.

1 Introduction

Finite projective geometries were traditionally used for the construction of algorithms of Coding Theory [1]. Their applications to other areas of Information Security have been published (see [2], [3] devoted to Network Coding). In particular, it was used in Cryptography (see [4], where projective geometry were used for authentication protocols). Nowadays finite geometries are widely used as tools for secret sharing.

Additionally they can be used for the design of some stream ciphers of multivariate nature and protocols of Noncommutative Cryptography (see [5] and further references). We introduce the first graph based multivariate public keys with bijective encryption maps generated via special walks on incidence graph of projective geometry.

The tender of US National Institute of Standartisation Technology (NIST, 2017) has started the standardisation process of possible Post-Quantum Public keys aimed for the purposes to be (i) encryption tools, (ii) tools for digital signatures (see [6], [7]).

In July 2020 the Third Round of the competition started. In the category of Multivariate Cryptography (MC) remaining candidates are easy to observe.

For the task (i) multivariate algorithm was not selected, single multivariate candidate is "The Rainbow Like Unbalanced Oil and Vinegar" (RUOV) digital signature method. As you see RUOV algorithm is investigated as appropriate instrument for the task (ii). During the Third Round some cryptanalytic instruments to deal with ROUV were found (see [8], [9]). That is why different algorithms were chosen at the final stage. In July 2022 first four winners of NIST standardisation competition were chosen. They all are lattice based algorithms.

Noteworthy that all multivariate NIST candidates were presented by multivariate rules of degree bounded by constant (2) of kind

$x_1 \to f_1(x_1, x_2, \ldots, x_n)$,
$x_2 \to f_2(x_1, x_2, \ldots, x_n)$,
$\ldots$,
$x_n \to f_n(x_1, x_2, \ldots, x_n)$.

We think that NIST outcomes motivate investigations of alternative options in Multivariate Cryptography oriented on encryption tools for

(a) the work with the space of plaintexts ${F_q}^n$ and its transformation G of linear degree cn, $c > 0$ on the level of stream ciphers or public keys

(b) the usage of protocols of Noncommutative Cryptography with platforms of multivariate transformations for the secure elaboration of multivariate map G from $End(F_q[x_1, x_2, \ldots, x_n])$ of linear or superlinear degree and density bounded below by function of kind cn^r, where $c > 0$ and $r > 1$.

Some ideas in directions of (a) and (b) are presented in [10].

Alternatively we hope that classical multivariate public key approach (see [11]), i. e. the usage of multivariate rules of degree 2 is still able to bring reliable encryption algorithms.

In this paper we suggest new quadratic multivariate public rules defined in terms of Projective Geometry. Recall that multivariate public rule G has to be given in its standard form $x_i \to g_i(x_1, x_2, \ldots, x_n)$, where polynomials g_i are given via the lists of monomial terms in the lexicographical order.

2 Linear codes and Schubert cellular graphs

The missing definitions of graph-theoretical concepts which appear in this paper can be found in [12]. All graphs we consider are simple graphs, i.e. undirected without loops and multiple edges. Let $V(G)$ and $E(G)$ denote the set of vertixes and the set of edges of G respectively. When it is convenient, we shall identify G with the corresponding anti-reflexive binary relation on $V(G)$, i.e. $E(G)$ is a subset of $V(G) \times V(G)$ and write vGu for the adjacent vertexes u and v (or neighbours). We refer to $|\{x \in V(G) | xGv\}|$ as degree of the vertex v.

The incidence structure is the set V with partition sets P (points) and L (lines) and symmetric binary relation I such that the incidence of two elements implies that one of them is a point and another one is a line. We shall identify I

with the simple graph of this incidence relation or bipartite graph. The pair x, y , $x \in P$, $y \in L$ such that xIy is called a *flag* of incidence structure I.

Projective geometry ${}^{n-1}PG(F_q)$ of dimension $n-1$ over the finite field F_q, where q is a prime power, is a totality of proper subspaces of the vector space $V = {F_q}^n$ of nonzero dimension. This is the incidence system with type function $t(W) = dim(W)$, $W \in {}^{n-1}PG(F_q)$ and incidence relation I defined by the condition $W_1 I W_2$ if and only if one of these subspaces is embedded in another one.

We can select standard base $e_1, e_2, \ldots, e_n$ of V and identify ${}^nPG(F_q)$ with the totality of linear codes in ${F_q}^n$. The geometry ${}^n\Gamma(q) = {}^{n-1}PG(F_q)$ is a partition of subsets ${}^n\Gamma_i(q)$ consisting of elements of selected type i, $i = 1, 2, \ldots, n-1$.

We assume that each element of V is presented in the chosen base as column vector $(x_1, x_2, \ldots, x_n)$. Let U stands for the unipotent subgroup of automorphism group $PGL_n(F_q)$ consisting of lower unitriangular matrices. Let us consider orbits of the natural action of U on the projective geometry ${}^nPG(F_q)$. They are known as large Schubert cells. Each of orbits on the set $\Gamma_m(F_q)$ contains exactly one symplectic element spanned by elements e_{i_1}, e_{i_2}, $\ldots$, e_{i_m}. So the number of orbits of $(U, \Gamma_m(F_q))$ equals to binomial coefficient $C(n, m)$. Noteworthy that the cardinality of ${}^n\Gamma_m(F_q)$ is expressed by Gaussian binomial coefficient. Unipotent subgroup U is generated by elementary transvections $x_{i,j}(t)$, $i < j$, $t \in F_q$. If we select i and j then elements of kind $x_{i,j}(t)$ form root subgroup $U_{i,j}$ corresponding to the positive root $e_i - e_j$ of root system A_n.

Let J be a proper subset of $\{1, 2, \ldots, n\} = N$, ${}^JS$ be Schubert cell containing symplectic subspace W_J spanned by $e_j \in J$, $\Delta(J) = \{(i, j) | i \in J, j \in N - J, i < j\}$. Then a subgroup $U(J)$ generated by root subgroups $U_{i,j}$, $(i, j) \in \Delta(J)$ of order q^k, $k = |\Delta(J)|$ acts regularly on ${}^JS$. It means that we can identify ${}^JS$ and $U(J)$. Noteworthy that each $\Gamma_m(F_q)$ has a unique largest Schubert cell of size $q^m(n-m)$, it is ${}^JS$ for $J = \{n, n-1, n-2, \ldots, n-m+1\}$. We denote this cell as ${}^mLS(q)$.

We consider the bipartite graph ${}^{m,k}I_n(F_q)$ of the restriction of I onto disjoint union ${}^mLS(F_q)$ and ${}^kLS(F_q)$. It is bipartite graph with bidegrees q^r and q^s where $r = —\Delta(\{n, n-1, n-2, \ldots, n-m+1\}) - \Delta(\{n, n-1, n-2, \ldots, n-m+1\}) \cap \Delta(\{n, n-1, n-2, \ldots, n-k+1\})|$ and $s = |\Delta(\{n, n-1, n-2, \ldots, n-k+1\}) - \Delta(\{n, n-1, n-2, \ldots, n-m+1\}) \cap \Delta(\{n, n-1, n-2, \ldots, n-k+1\})|$. We refer to ${}^{m,k}I_n(q)$ as Cellular Schubert graph and denote it as $CS_n^{m,k}(F_q)$ graph. In particular case $n = 2m+1$, $k = m$ these graphs are known as Double Schubert graphs [13].

3 Schubert cellular graphs over commutative ring

Let K be a commutative ring. We consider group $U = U_n(K)$ of lower unitriangular $n \times n$ matrices with entries from K. Let Δ be the totality of all entries of (i, j), $1 \leq i < j \leq n$, i. e. totality of positive roots from A_n. We identify element M from $U_n(K)$ with the function $f : \Delta \to K$ such that $f(i, j) = m_{i,j}$. The restriction $M|_D$ of M on subset D of Δ is simply $f|_D$.

For each proper nonempty subset J of $\{1, 2, \ldots, n\}$ we define $U(J)$ as totality of matrices $M = (m_{i,j})$ from U such that $(i, j) \in \Delta - \Delta(J)$ implies that $m_{i,j} = 0$.

We define incidence system ${}^{n-1}PG(K)$ as totality of pairs (J, M), $M \in U(J)$ with type function $t(J, M) = |J$ and incidence relation given by conditions $({}^1J, {}^1M)I({}^2J, {}^2M)$

if and only if one of subsets ${}^1J$ and ${}^2J$ is embedded in another one and $({}^1M - {}^2M)|_{\Delta({}^1J)\cap\Delta({}^2J)} = {}^1M \times {}^2M - {}^2M \times {}^1M$.

We refer to this incidence system as *projective geometry scheme* over commutative ring K. If $K = F$ is the field then ${}^{n-1}PG(F)$ coincides with $n-1$-dimensional projective geometry over F, i. e. totality of proper nonzero subspaces of the vector space F^n (see [14]).

The reader can find similar interpretations of Lie geometries and their Schubert cells in [15], [16], their generalisations via pairs of type (irreducible root system, commutative ring K) are presented in [17] and [5]. The concept of large and small Schubert cell in the classical case of field is presented in [18], [19].

We introduce $\Gamma_m(K)$, ${}^mLS(K)$ and graphs $CS_n^{m,k}(F_q)$ for $m = 1, 2, \ldots, n-1$ via simple substitution of K instead F_q. We refer to disjoint union of ${}^mLS(K)$, $m = 1, 2, \ldots, n-1$ with the restriction of incidence relation I and type function t on this set as Schubert geometry scheme of type A_n over commutative ring K. We refer to elements of this incidence system as linear codes of Schubert type. We can define Schubert schemes over other Dynkin-Coxeter diagrams.

4 Linguistic graphs of type (r, s, p) and symbolic computations

Let K be a commutative ring. We refer to an incidence structure with a point set $P = P_{s,m} = K^{s+m}$ and a line set $L = L_{r,m} = K^{r+m}$ as linguistic incidence structure $I_m(K)$ of type (r, s, m) if point $x = (x_1, x_2, \ldots, x_s, x_{s+1}, x_{s+2}, \ldots, x_{s+m})$ is incident to line $y = [y_1, y_2, \ldots, y_r, y_{r+1}, y_{r+2}, \ldots, y_{r+m}]$ if and only if the following relations hold

$a_1x_{s+1} + b_1y_{r+1} = f_1(x_1, x_2, \ldots, x_s, y_1, y_2, \ldots, y_r)$

$a_1x_{s+2} + b_2y_{r+2} = f_2(x_1, x_2, \ldots, x_s, x_{s+1}, y_1, y_2, \ldots, y_n, y_{r+1})$

$\ldots$

$a_mx_{s+m} + b_my_{r+m} = f_m(x_1, x_2, \ldots, x_s, x_{s+1}, \ldots, x_{s+m}, y_1, y_2, \ldots, y_r, y_{r+1}, \ldots, y_{r+m})$

where a_j and b_j, $j = 1, 2, \ldots, m$ are not zero divisors, and f_j are multivariate polynomials with coefficients from K. Brackets and parenthesis allow us to distinguish points from lines (see [20], [5]).

The colour $\rho(x) = \rho((x))$ ($\rho(y) = \rho([y])$) of point (x) (line $[y]$) is defined as projection of an element (x) (respectively $[y]$) from a free module on its initial s (relatively r) coordinates. As it follows from the definition of linguistic incidence structure for each vertex of incidence graph there exists the unique neighbour of a chosen colour.

We refer to $\rho((x)) = (x_1, x_2, \ldots, x_s)$ for $(x) = (x_1, x_2, \ldots, x_{s+m})$ and $\rho([y]) = (y_1, y_2, \ldots, y_r)$ for $[y] = [y_1, y_2, \ldots, y_{r+m}]$ as the colour of the point and the colour of the line respectively.

For each $b \in K^r$ and $p = (p_1, p_2, \ldots, p_{s+m})$ there is the unique neighbour of the point $[l] = N_b(p)$ with the colour b. Similarly, for each $c \in K^s$ and line $l = [l_1, l_2, \ldots, l_{r+m}]$ there is the unique neighbour of the line $(p) = N_c([l])$ with the colour c. We refer to operator of taking the neighbour of vertex accordingly chosen colour as *neighbourhood operator*.

On the sets P and L of points and lines of linguistic graph we define jump operators ${}^1J = {}^1 J_b(p) = (b_1, b_2, \ldots, b_s, p_1, p_2, \ldots, p_{s+m})$, where $(b_1, b_2, \ldots, b_s) \in K^s$ and ${}^2J = {}^2 J_b([l]) = [b_1, b_2, \ldots, b_r, l_1, l_2, \ldots, l_{r+m}]$, where $(b_1, b_2, \ldots, b_r) \in K^r$. We refer to tuple (s, r, m) as type of the linguistic graph I.

We say that linguistic graph has degree d, $d \geq 2$ if maximal degree of nonlinear multivariate polynomials f_i, $i = 1, 2, \ldots, m$ is d. Noteworthy, that the path $v_0, v_1, \ldots, v_k$ in the linguistic graph I_m is determined by starting vertex v_0 and colours of vertexes $v_1, v_2, \ldots, v_k$ such that $\rho(v_i) \neq \rho(v_{i+2})$ for $i = 0, 1, \ldots, k-2$.

We can consider graph $I_m(K)$ together with $\tilde{I}_m = I_m(K[y_1, y_2, \ldots, y_l])$ defined by the same polynomials f_i, $i = 1, 2, \ldots, m$ with coefficients from K.

Assume that $l = m + s$. We can consider the path of length $2k$ with starting point $(y_1, y_2, \ldots, y_s, y_{s+1}, y_{s+2}, \ldots, y_m)$ and colours $G_1 = ({}^1g_1(y_1, y_2, \ldots, y_s), {}^1g_2(y_1, y_2, \ldots, y_s), \ldots, {}^1g_r(y_1, y_2, \ldots, y_s))$, $H_1 = ({}^1h_1(y_1, y_2, \ldots, y_s), {}^1h_2(y_1, y_{2,\ldots,y_s}), \ldots, {}^1h_s(y_1, y_2, \ldots, y_s))$, $G_2 = ({}^2g_1(y_1, y_2, \ldots, y_s), {}^1g_2(y_1, y_2, \ldots, y_s), \ldots, {}^2g_r(y_1, y_2, \ldots, y_s))$, $\ldots$, $G_k = ({}^kg_1(y_1, y_2, \ldots, y_s), {}^kg_2(y_1, y_2, \ldots, y_s), \ldots, {}^kg_r(y_1, y_2, \ldots, y_s))$, $H_k = ({}^kh_1(y_1, y_2, \ldots, y_s), {}^kh_2(y_1, y_2, \ldots, y_s), \ldots, {}^kh_s(y_1, y_2, \ldots, y_s))$.

The last vertex of this path will be a point $(p) = ({}^kh_1(y_1, y_2, \ldots, y_s), {}^kh_2(y_1, y_2, \ldots, y_s), \ldots, {}^kh_s(y_1, y_2, \ldots, y_s), f_{m+1}(y_1, y_2, \ldots, y_s, y_{s+1}, y_{s+2}, \ldots, y_{s+m}),$

$f_{m+2}(y_1, y_2, \ldots, y_s, y_{s+1}, y_{s+2}, \ldots, y_{s+m}), \ldots, f_{m+s}(y_1, y_2, \ldots, y_s, y_{s+1}, y_{s+2}, \ldots, y_{s+m}))$.

We define the *passage* transformation $Pas(G_1, G_2, \ldots, G_k, H_1, H_2, \ldots, H_k)$ of K^{r+s} (space of points) with symbolic colours G_1, H_1 , $\ldots$, G_k, H_k via multivariate rule

$$
\begin{aligned}
&y_1 \to^k h_1(y_1, y_2, \ldots, y_s),\\
&y_2 \to^k h_2(y_1, y_2, \ldots, y_s),\\
&\ldots\\
&y_s \to^k h_s(y_1, y_2, \ldots, y_s),\\
&y_{m+1} \to f_{s+1}(y_1, y_2, \ldots, y_{m+s}), \quad (1)\\
&\ldots\\
&y_{m+2} \to f_{s+2}(y_1, y_2, \ldots, y_{m+s}),\\
&\ldots\\
&y_{m+s} \to f_{s+m}(y_1, y_2, \ldots, y_{m+s}).
\end{aligned}
$$

It is easy to see that this transformation is bijective if the map $y_i \to h_i(y_1, y_2, \ldots, y_s)$, $i = 1, 2, \ldots, s$ is bijective on K^s. Defined above transformations form a semigroup of multivariate transformation. Some basic properties of this semigroup are discussed in [5].

Of course we can use lines instead of points and define another semigroup formed by transformation of kind $Pas(H_1, H_2, \ldots, H_k, G_1, G_2, \ldots, G_k)$ acting on the variety K^{m+r}, where H_i are elements of $K[y_1, y_2, \ldots, y_r]^s$ and $G_i \in K[y_1, y_2, \ldots, y_r]^r$.

We define degree of tuple $(g_1, g_2, \ldots, g_d) \in K[x_1, x_2, , \ldots, x_l]^d$ as maximal degree of polynomials g_i, $i = 1, 2, \ldots, d$. The following two statements are proven in [5].

Theorem 1. *Let K be a commutative ring. Cellular Schubert graph $CS_n^{m,k}(K)$ is a linguistic graph of degree 2 of type (r, s, p) where $r = |\Delta(\{n, n-1, n-2, \ldots, n-m+1\}) - \Delta(\{n, n-1, n-2, \ldots, n-m+1\}) \cap \Delta(\{n, n-1, n-2, \ldots, n-k+1\})|$, $s = |\Delta(\{n, n-1, n-2, \ldots, n-k+1\}) - \Delta(\{n, n-1, n-2, \ldots, n-m+1\}) \cap \Delta(\{n, n-1, n-2, \ldots, n-k+1\})|$ and $p = |\Delta(\{n, n-1, n-2, \ldots, n-m+1\}) \cap \Delta(\{n, n-1, n-2, \ldots, n-k+1\})|$.*

Theorem 2. *Let $CS_n^{m,k}(K)$ be a Cellular Schubert as in the previous statement. Then transformations $Pas(G_1, G_2, \ldots, G_j, H_1.H_2, \ldots, H_j)$, $j \geq 1$ of the affine space K^{s+p} such that $deg(H_i) = 1$, $deg(G_i) = 1$, $i = 1, 2, \ldots, j$ are quadratic multivariate maps of this space into itself.*

5 Public key based on Cellular Schubert graph

5.1 Construction of the map

As usually we have to describe procedures for the owner of the key (Alice) and public user Bob. We start from the generating procedure for the multivariate map.

Alice selects parameter n, constants α and β from open interval $(0, 1)$ together with constants a and b from Z.

She sets parameters $m = [\alpha n + a]$ and $k = [\beta n + b]$, where parenthesis denote the flow function. Alice takes finite field $F = F_{2^t}$, $t \geq 32$.

Alice computes parameter s, r and p of the linguistic graph $CS_n^{m,k}(K)$. She selects the length of path j. Alice will use vector space F^{s+p} as space of plaintexts. Thus she selects square matrices A_1, A_2, ..., A_j of dimensions $s \times s$ and matrices B_1, B_2, ...,B_j of dimensions $r \times s$. Alice takes rows of $A_i(y_1, y_2, \ldots, y_s)^T$ as linear forms ${}^i h_l(y_1, y_2, \ldots, y_n)$ for $i = 1, 2, \ldots, j$, $l = 1, 2, \ldots, s$ and $B_i(y_1, y_2, \ldots, y_s)^T$ to get linear forms ${}^i g_l(y_1, y_2, \ldots, y_s)$, $i = 1.2, \ldots, j$, $l = 1, 2, \ldots, r$. Thus she constructed H_i and G_i for the computation of the path in the graph $CS_n^{m,k}(F[y_1, y_2, \ldots, y_s, y_{s+1}, \ldots, y_{s+p}])$ and transformation $Pas(G_1, G_2, \ldots, G_j, H_1, H_2, \ldots, H_j)$ of kind (1).

After creation of the point (p) = $({}^j h_1, {}^j h_2, \ldots, {}^j h_s, f_{s+1}, f_{s+2}, \ldots, f_{s+m})$ of the graph $CS_n^{m,k}(F[y_1, y_2, \ldots, y_s, y_{s+1}, \ldots, y_{s+p}])$. Alice uses jump operator to get ${}^1 J_{\mathrm{b}}(\mathrm{p})$ with b formed in the following way.

She divide variables into two groups y_1, y_2, ..., $y_{s(1)}$ and $y_{s(1)+1}$, $y_{s(1)+2}$, ..., y_s where positive integer $s(1)$ is a linear expression of kind $[\gamma \times s] + \sigma]$ with $0 \leq \gamma < 1$ and positive integer constant σ.

Alice takes map D of kind $y_1 \to {y_1}^2$, $y_2 \to {y_2}^2$, ..., $y_{s(1)} \to y_{s(1)}^2$ She takes element T from $AGL_{s(1)}(F_q)$ and forms a conjugation $Q = T^{-1}DT$ of degree 2. Let $Q_i = Q(y_i)$ for $i = 1, 2, \ldots, s(1)$. She forms the map E given by the following rule

$y_1 \to Q_1(y_1, y_2, \ldots, y_{s(1)})$,

$y_2 \to Q_2(y_1, y_2, \ldots, y_{s(1)})$,
$\ldots$,
$y_{s(1)} \to Q_{s(1)}(y_1, y_2, \ldots, y_{s(1)})$,
$y_{s(1)+1} \to a_{s(1)+1,1}y_1 + a_{s(1)+1,2}y_2 + \cdots + a_{s(1)+1,s(1)}y_{s(1)} + b_{1,1}y_{s(1)+1}, b_{1,2}y_{s(1)+2} + \cdots + b_{1,s-s(1)}y_s$,
$y_{s(1)+2} \to a_{s(1)+2,1}y_1 + a_{s(1)+2,2}y_2 + \cdots + a_{s(1)+2,s(1)}y_{s(1)} + b_{2,1}y_{s(1)+1}, b_{2,2}y_{s(1)+2} + \cdots + b_{2,s-s(1)}y_s$,
$\ldots$
$y_s \to a_{s,1}y_1 + a_{s,2}y_2 + \cdots + a_{s,s(1)}y_{s(1)} + b_{s-s(1),1}y_{s(1)+1}, b_{s-s(1),2}y_{s(1)+2} + \cdots + b_{s-s(1),s-s(1)}y_s$,
$y_{s+1} \to f_{s+1}(y_1, y_2, \ldots, y_{s+p}$,
$y_{s+2} \to f_{s+2}(y_1, y_2, \ldots, y_{s+p})$,
$\ldots$,
$y_{s+p} \to f_{s+p}(y_1, y_2, \ldots, y_{s+p})$.

where $a_{i,j}$ are chosen as some linear forms in variables y_1, y_2, $\ldots$, $y_{s(1)}$ and matrix $B = (b_{i,j})$ from $GL_{s-s(1)}(F_q)$ is selected as Singer cycle, i.e. element of $GL_{s-s(1)}(F_q)$ of order $q^{s-s(1)} - 1$.

Noteworthy that the restriction Q of E on variables $y_1, y_2, \ldots, y_{s(1)}$ has order m in the case of $q = 2^m$ and the degree of Q^{-1} is 2^{m-1}. We assume that parameter m is even.

The order of cyclic group generated by E' which is the restriction of E on variables $y_1, y_2, \ldots y_s$ is multiple of $m \times 2^{s-s(1)}$. Alice can use transformation of kind $C^{-1}E'C$, $C \in GL_s(F_q)$ instead of E'.

Alice selects two elements ${}^1T$ and ${}^2T$ of affine group $AGL_{s+p}(F)$. and computes the superposition $\tilde{E} = {}^1T E {}^2T$ in its standard form
$y_1 \to \tilde{f}_1(y_1, y_2, \ldots, y_{s+p})$,
$y_2 \to \tilde{f}_1(y_1, y_2, \ldots, y_{s+p})$,
$\ldots$
$y_{s+p} \to \tilde{f}_1(y_1, y_2, \ldots, y_{s+p})$.

She presents multivariate rule $\tilde{E}$ to public users.

The inverse of $\tilde{E}$ has polynomial degree $\geq 2^{m-1}$ Noteworthy that the choice ${}^2T =^1 T^{-1}$ insures that cyclic group generated by $\tilde{E}$ has order multiple to $m \times (2^m - 1)$.

Thus public user (Bob) works with the space of plaintexts ${F_q}^d$, $d = p + s$. He is able to encrypt his plaintext in time $O(d^3)$.

5.2 Description of decryption procedure

Let us consider the private key procedure for the decryption. Assume that Alice gets the ciphertext $\mathrm{c} = (c_1, c_2, \ldots, c_{s+p})$.

Step 1. She treats it as column vector and computes ${T_2}^{-1}(\mathrm{c}) = (q_1, q_2, \ldots, q_s, q_{s+1}, \ldots, q_{s+p})$.

Step 2. Alice uses affine transformation T and matrix B to solve the following equations.
$E'(z_1, z_2, \ldots, z_s) = c_1$,
$E'(z_1, z_2, \ldots, z_s) = c_2$,

$\ldots$,

$E'(z_1, z_2, \ldots, z_s) = c_s$,

Assume that $z_i = d_i$, $i = 1, 2, \ldots, s$ is the solution.

Step 3. She computes numerical colours $G_t(d_1, d_2, \ldots, d_s) = ({}^t a_1, {}^t a_2, {}^t a_r) = {}^t$ a and $H_t(d_1, d_2, \ldots, d_s) = {}^t$ b for $t = 1, 2, \ldots, j$.

Step 4.

Alice forms the point ^{1}p of the graph $CS_n^{m,k}(F)$ in the form

$({}^j b_1, {}^j b_2, \ldots, {}^j b_s, q_{s+1}, q_{s+2}, \ldots, q_{s+p})$.

Step 5. She computed the path in this graph with the starting point ^{1}p and consecutive colours ^{j}a, ${}^{j-1}$b, ${}^{j-1}$a, ${}^{j-2}$b, ${}^{j-2}$a, $\ldots$, ^{1}b, ^{1}a, ^{0}b $= (d_1, d_2, \ldots, d_s)$. Let ^{2}p be the final vertex of the computed path with the colour ^{0}b.

Step 6. Alice treats ^{2}p as column vector and computes the plaintexts as ${T_1}^{-1}({}^2\text{p})$.

6 Illustrative example, complexity estimates and implemented cases

We can define mentioned above Double Schubert Graph $DS(k, K)$ over commutative ring K simply as incidence structure defined as disjoint union of partition sets $PS = K^{k(k+1)}$ consisting of points which are tuples of kind $x = (x_1, x_2, \ldots, x_k, x_{1,1}, x_{1,2}, \ldots, x_{k,k})$ and $LS = K^{k(k+1)}$ consisting of lines which are tuples of kind $z = [z_1, z_2, \ldots, z_k, z_{11}, z_{12}, \ldots, z_{k,k}]$, where x is incident to z, if and only if $x_{i,j} - z_{i,j} = x_i z_j$ for $i = 1, 2, \ldots, k$ and $j = 1, 2, \ldots, k$. It is convenient to assume that the indexes of kind i, j are placed for tuples of $K^{k(k+1)}$ in the lexicographical order.

REMARK.

The term Double Schubert Graph is chosen, because points and lines of $DS(k, F_q)$ can be treated as subspaces of ${F_q}^{2k+1}$ of dimensions $k+1$ and k, which form two largest Schubert cells. Recall that the largest Schubert cell is the largest orbit of group of unitriangular matrices acting on the variety of subsets of given dimension.

We define the colour of point $x = (x_1, x_2, \ldots, x_k, x_{1,1}, x_{1,2}, \ldots, x_{kk})$ from PS as tuple $(x_1, x_2, \ldots, x_k)$ and the colour of a line $y = [z_1, z_2, \ldots, z_k, z_{11}, z_{12}, \ldots, z_{k,k}]$ as the tuple $(z_1, z_2, \ldots, z_k)$. For each vertex v of $DS(k, K)$, there is the unique neighbour $y = N_a(v)$ of a given colour $a = (a_1, a_2, \ldots, a_k)$.

Let us consider the list of variables corresponding to coordinates of the point. So we get y_1, y_2, $\ldots$, y_k , $y_{1,1}$, $y_{1,2}$, $\ldots$, $y_{k,k}$. We will use the ring $R = K[y_1, y_2, \ldots, y_k, y_{1,1}, y_{1,2}, \ldots, y_{k,k}]$.

Let $\tilde{DS}(k, K) = DS(k, R)$. To define $Pas = Pas(G_1, G_2, \ldots, G_j, H_1, H_2, \ldots, H_j)$ and construct the path with starting point $(y_1, y_2, \ldots, y_k, y_{11}, y_{12}, \ldots, y_{k,k})$ and the symbolic colours $G_i(y_1, y_2, \ldots, y_k) = {}^i b_1 y_1 + {}^i b_2 y_2 + \cdots + {}^i b_k y_k$, $H_i(y_1, y_2, \ldots, y_k) = {}^i a_1 y_1 + {}^i a_2 y_2 + \cdots + {}^i a_k y_k$, $a_i \in K$, $b_i \in K$ are used.

The complexity of computation of $T_1 Pas T_2$ is determined by the time of computation of the path u, ${}^1u$, ${}^2u$, $\ldots$, ${}^{2j}u$ in the graph $DS(k, R)$ with the starting

point $u = (T_1(y_1), T_1(y_2), \ldots, T_1(y_k), T_1(y_{11}), T_1(y_{1,2}), \ldots, T_1(y_{k,k}))$ and colours $G_1(u_1, u_2, \ldots u_k, u_{1,1}, u_{1,2}, \ldots, u_{k,k})$, $H_1(u_1, u_2, \ldots, u_k, u_{1,1}, u_{1,2}, \ldots, u_{k,k})$,

$G_2(u_1, u_2, \ldots, u_k, u_{1,1}, u_{1,2}, \ldots, u_{k,k})$, $H_2(u_1, u_2, \ldots, u_k, u_{1,1}, u_{1,2}, \ldots, u_{k,k}), \ldots,$ $G_j(u_1, u_2, \ldots, u_k, u_{1,1}, u_{1,2}, \ldots, u_{k,k})$, $H_j(u_1, u_2, \ldots, u_k, u_{1,1}, u_{1,2}, \ldots, u_{k,k})$.

The key parameter here is j. Let us assume that $j = O(k)$. The computation of selected coordinate of final point of the walk requires computation of $G_i H_i$ depending $k + k^2$ for each parameter i and adding obtained quadratic polynomials. Thus it takes ${2k^4}_j$ operations of addition and multiplication in K and the complexity is $O(k^5)$. We have to execute this procedure $k^2 + k$ times. So the complexity of public rule development is $O(k^7)$ or $O(d^{3+1/2})$, where $d = k^2 + k$ is the dimension of the space of plaintexts.

Public user encrypts in time $O(d^3)$.

Let us estimate the complexity of private encryption procedure of Alice.

She applies the inverse of T_2 to the obtained ciphertext c and gets ${}^1c = {T_2}^{-1}(c)$. It requires $O(d^2)$ elementary operations in the field K. Alice has to solve the system of k equations to find the reimage of ${}^1c$ of the map E' with the usage of known matrices T and B of size $\leq k \times k$. Getting the solution $z = (d_1, d_2, \ldots, d_k)$ of the system of equations requires less than $O(d^2)$ operations. It allows her to compute colours $g_i = G_i(d_1, d_2, \ldots, d_k)$, $h_i = H_i(d_1, d_2, \ldots, d_k)$, $i = 1, 2, \ldots, j$.

Alice changes the first coordinate of ${T_2}^{-1}(c)$ for h_j and gets the point ${}^{2j}u$. She computes the chain with the starting point ${}^{2j}u$ and further consecutive members with colours g_j, h_{j-1}, g_{j-1}, h_{j_2},..., g_1, h_1, z. Alice gets the final point u of the chain with the colur z in time less than $O(d^2)$. Finally she need $O(d^2)$ operation to compute the ciphertext as ${T_1}^{-1}$. So the complexity of entire private encryption procedure is $O(d^2)$

As we mentioned above graph $CS^{k,k}_{2k+1}(K)$ is isomorphic to Double Schubert graph $DS(k, K)$. It is easy to check that theoretical complexity of described above public key algorithm based on graph $CS^{k+\alpha,k+\beta}_{2k+\alpha+\beta+1}$, where α and β are nonnegative constants, is the same with the case of the $DS(k, K)$. The dimension of the space of plaintext is $d = (k + \alpha + \beta) \times (\alpha + 1)$. Cost of generation of public rule is $O(d^{3+1/2})$, complexity of private key decryption is $O(d^2)$, public encryption costs $O(d^3)$.

We select this class of algorithms and $K = F_{2^{32}}$ for the implementation.

7 Conclusions

Modern public key cryptography is based on the complexity of hard unsolved problems. Especially important is the fundamental assumption of cryptography that there are no polynomial-time algorithms for solving any NP-hard problem. A consequence of this assumption is that there are cryptographically interesting problems that are hard to solve in the quantum setting. Each of five core directions of Post Quantum Cryptography is based on the complexity of some NP-hard problem. The paper is connected with the following two directions.

Code-based cryptography.

Cryptographic primitives based on the hardness of decoding random linear codes are historically the first post-quantum systems. Since the late 1970s schemes like McEliece encryption have withstood a long series of cryptanalytic attacks. In order to embed a trapdoor that enables decryption one converts a structured code with good decryption capabilities like a Goppa code by linear transformations into a "random-looking" code C. An attacker now faces the problem to either distinguish C from a purely random code using the properties of the underlying structured code or to directly decode C. The last approach leads to the best known generic attacks. Recent significant progress on decoding binary linear codes C of dimension n leads to a new trend in code-based cryptography based on the usage of linear codes that are different than Goppa code initially proposed by McEliece (MDPC codes, Rank codes, quasi-cyclic codes, and others). New approach promises to decrease the size of the public key.

Multivariate cryptography.

Multivariate cryptography is usually defined as the set of cryptographic schemes using the computational hardness of the Polynomial System Solving problem over a finite field. Solving systems of multivariate polynomial equations is proven to be NP-hard or NP-complete. That is why these schemes are often considered to be good candidates for post-quantum cryptography. The first multivariate scheme based on multivariate equations was introduced by Matsumoto and Imai in 1988. Later J. Patarin found nice and efficient cryptanalytic solution to break this scheme (see [11]). Two following schemes suggest the most robust solutions. They are HFE (Hidden Field Equations) and UOV (Unbalanced Oil and Vinegar), both developed by J. Patarin in the late 1990s. Special variants of theses schemes have been submitted to the post-quantum standardization process organized by NIST. During this process new cryptanalytic methods to break these cryptosystems were found (see [7]). It motivates development of new public keys of Multivariate Cryptography.

We suggest the usage of the bridge between Coding Theory and Multivariate Cryptography based on the pairs of kind

$(PG_n(F_q), PG_n(F_q[x_1, x_2, \ldots, x_m])$ where $PG_n(F_q)$ is classical finite

n-dimensional projective geometry and $PG_n(F_q[x_1, x_2, \ldots, x_m])$ is its natural analog defined over multivariate ring $F_q[x_1, x_2, \ldots, x_m]$. For the construction of public key a hidden problem to find a path between two vertexes of the incidence graph of $PG_n(F_q[x_1, x_2, \ldots, x_m])$ is used. We take these vertexes in general position, i.e. they are of different type and belong to distinct largest Schubert cells. In the case of finite field F_{2^t} the multivariate rule is given by the system of quadratic equations. The choice of large t (like 32, 64) insures that the inverse map has a very large polynomial degree.

The bijective public rule can be used as instrument of encryption as well as for making digital signatures.

In case of digital signatures the usage of nonbijective modifications of $\tilde{E}$ as above is also possible.

References

1. 1. W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, 2003.
2. Anton Betten, Mihael Braun, Adalbert Kerber, Axel Kohnert, Alfred Wasserman *Error Correcting Linear Codes Isometry and Applications*, Springer, 2006.
3. Andreas Stephan Essenhans, Axel Kohnert, Alfed Wassermann, *Constructions of codes for Network Coding* , arXiv:1005, 2839[cs].
4. A. Beultespacher, *Enciphered Geometry, Some Applications of Geometry to Cryptography*, Annals of Discrete Mathematics, v. 37, 1988, 59-68.
5. V. Ustimenko, *Graphs in terms of Algebraic Geometry, symbolic computations and secure communications in Post-Quantum world*, UMCS Editorial House, Lublin, 2022, 198 p.
6. Post-Quantum Cryptography, *Call for Proposals:https://csrc.nist.gov/Project; Post-Quantum-Cryptography-Standardization / Call-for-Proposals, Post-Quantum Cryptography: Round 2 Submissions.*
7. Anne Canteaut, Franois-Xavier Standaert (Eds.), *Eurocrypt 2021*, LNCS 12696, 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 1721, 2021, Proceedings, Part I, Springer, 2021, 839p.
8. Jintai Ding, Joshua Deaton, Vishakha, and Bo-Yin Yang *The Nested Subset Differential Attack A Practical Direct Attack Against LUOV Which Forges a Signature Within 210 Minutes*, In Eurocrypt 2021, Part 1, pp. 329-347.
9. Ward Beullens, Improved Cryptanalysis of UOV and Rainbow, In Eurocrypt 2021, Part 1, pp. 348-373.
10. Vasyl Ustimenko, *On Extremal Algebraic Graphs and Multivariate Cryptosystems*, IACR e-print archive, 2022/1537.
11. L. Goubin, J.Patarin, Bo-Yin Yang, *Multivariate Cryptography*, Encyclopedia of Cryptography and Security, (2nd Ed.) 2011, 824-828.
12. A.Brouwer, A. Cohen, A. Niemaier, *Distance regular graph*, Springer, Berlin,1989.
13. Vasyl Ustimenko, *On computations with Double Schubert Automaton and stable maps of multivariate cryptography*, Position and Communication Papers of the 16th Conference on Computer Science and Intelligence Systems, M. Ganzha, L. Maciaszek, M. Paprzycki, D. lzak (eds). ACSIS, Vol. 26, pages 123130 (2021).
14. V. A. Ustimenko,*On some properties of Chevalley groups and their generalisations*, In: Investigations in Algebraic Theory of Combinatorial objects, Moskow, Institute of System Studies, 1985, in Investigations in Algebraic Theory of Combinatorial Objects, Kluwer, Dordrecht (1992) p. 112-119.
15. V. A. Ustimenko, *Linear interpretation of Chevalley group flag geometries*, Ukraine Math. J. 43, Nos. 7,8 (1991), pp. 10551061.
16. V. Ustimenko, *Small Schubert cells as subsets in Lie algebras*, Functional Analysis and Applications, v. 25, no. 4, 1991, pp. 8183.
17. V. Ustimenko, *On small world non Sunada twins and cellular Voronoi diagams*, 6th conference, Algebra and Discrete Mathematics, vol. 30, N1 (2020), pp. 118-142.
18. I. Gelfand, R. MacPherson,*Geometry in Grassmanians and generalisation of the dilogarithm*, Adv. in Math., 44 (1982), 279-312.
19. I. Gelfand, V. Serganova, *Combinatorial geometries and torus strata on homogeneous compact manifolds*, Soviet Math. Surv. 42 (1987), 133-168.
20. V. Ustimenko, *Maximality of affine group and hidden graph cryptsystems*, Journal of Algebra and Discrete Mathematics, October, 2004, v.10, pp. 51-65.