Schubert cells and quadratic public keys of Multivariate Cryptography

Vasyl Ustimenko[1,2]

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

Abstract

Studies of linear codes in terms of finite projective geometries form traditional direction in Coding Theory. Some applications of projective geometries are known. We introduce new 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

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 Standardisation 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 $x_1 \rightarrow f_1(x_1, x_2, \ldots, x_n), x_2 \rightarrow f_2(x_1, x_2, \ldots, x_n), \ldots, x_n \rightarrow f_n(x_1, x_2, \ldots, x_n)$. We think that NIST

Proceedings ITTAP'2023: 3rd International Workshop on Information Technologies: Theoretical and Applied Problems, November 22–24, 2023, Ternopil, Ukraine, Opole, Poland
EMAIL: Vasyl.Ustymenko@rhul.ac.ukl (A.1);
ORCID: 0000-0002-2138-2357 (A.1);

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 $End(F_q[x_1, x_2, \dots, x_n])$ 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 $x_i \to g_i(x_1, x_2, \dots, x_n)$, 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 vertexes 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 $V(G)\cdot V(G)$ and write $v\ G\ u$ 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 $x\ I\ y$ 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 $e_1, e_2, \dots, e_n$ of V and identify ${}^{n-1}PG(F_q)$ with the totality of linear codes in $(F_q)^n$.The geometry ${}^{n-1}\mathbb{\Gamma}(q)={}^{n-1}PG(F_q)$ is a partition of subsets ${}^{n-1}\mathbb{\Gamma}(q)_i$ consisting of elements of selected type $i,\ i=1,2, \dots, n-1$. We assume that each element of V is presented in the chosen base as column vector $(x_1, x_1, \dots, x_n)$. 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 ${}^{n-1}PG(F_q)$. They are known as large Schubert cells. Each of orbits on the set $\mathbb{\Gamma}_m(F_q)$ contains exactly one symplectic element spanned by elements $e_{i(1)}, e_{i(2)}, \dots, e_{i(m)}$. So the number of orbits of $(U, \mathbb{\Gamma}_m(F_q))$ equals to binomial coefficient $C(n,m)$. Noteworthy that the cardinality of ${}^{n-1}\mathbb{\Gamma}_m(F_q)$ 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-1}. Let J be a proper subset of $\{1, 2, \dots, n\}=N,\ {}^JS$ be Schubert cell containing symplectic subspace W_J spanned by $e_j \in J$, $\Delta(J)=\{ (i,j) \mid i\in J,\ j\in N-J,\ i<j \}$. 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 $\mathbb{\Gamma}_m(F_q)$ has a unique largest Schubert cell of size $q^{m(n-m)}$, it is ${}^JS$ for $J=\{n, n-1, n-2, \dots, n-m+1\}$. 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 $r=|\Delta(\{n, n-1, n-2, \backslash dots, n-m+1\})- \Delta(\{n, n-1, n-2, \dots, n-m+1\}) \cap \Delta(\{n, n-1, n-2, \dots, n-k+1\})|$ and $s=|\Delta(\{n, n-1, n-2, \dots, n-k+1\}) - \Delta(\{n, n-1, n-2, \dots, n-m+1\}) \cap \Delta(\{n, n-1, n-2, \dots, n-k+1\})|$. We refer to ${}^{m,k}I_n(F_q)$ as Cellular Schubert graph and denote it as ${}^{m,k}CS_n(F_q)$ graph. In particular case $n=2m+1,\ k=m$ these graphs are known as Double Schubert graphs [13].

2.1. 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 the entries from K. Let Δ be the totality of all entries of $(i, j),\ 1 \le i<j \le n$, i. e. totality of positive roots from A_{n-1}. 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 $\{1, 2, \dots, n\}$ 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 ${}^{n-1}\mathrm{PG(K)}$ as a 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 ${}^1M-{}^2M) \mid \Delta({}^1J)\cap\Delta({}^2J) = {}^1M \cdot {}^2M-{}^2M \cdot {}^1M$. 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, their generalisations via pairs of type (irreducible root system, commutative ring K) are presented in [5]. The concept of large and small Schubert cell in the classical case of field is presented in [15], [16].

We introduce $\Gamma_m(K)$, ${}^mLS(K)$ and graphs $CS^{m,k}{}_n(K)$ 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-1} over commutative ring K. We refer to elements of this incidence system aslinear codes of Schubert type. We can define Schubert schemes over other Dynkin-Coxeter diagrams.

2.2 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 $P=P_{s,m}=K^{m+s}$ and a line set $L=L_{r,m}=K^{m+r}$ 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

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

$$a_2x_{s+2}+b_2y_{r+2}=f_2(x_1, x_2, \ldots, x_s, x_{s+1}, y_1, y_2, \ldots, y_r, y_{r+1})$$

$$\ldots$$

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

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 [5] and further references).

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 $b\epsilon K^r$ 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 $c \epsilon K^s$ 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 ${}^1J={}^1J_b(p)=(b_1, b_2, \ldots, b_s, p_1, p_2, \ldots, p_{s+m})$, where $(b_1, b_2, \ldots, b_s)\epsilon K^s$ and ${}^2J={}^2J_b([l])=[b_1, b_2, \ldots, b_r, l_1, l_2, \ldots, l_{r+m}]$, where $(b_1, b_2, \ldots, b_r)\epsilon K^r$. We refer to tuple (s, r, m) as type of the linguistic graph I.

We say that point (p) is line $[l]$ are adjacent in the linguistic graph I if ${}^1J_b(p){}^2I\,{}^2J_c[l]$ for some colours $b \epsilon K^s$ and $c \epsilon K^r$. Let ψ stands for the adjacency relation of the linguistic graph. 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 $i=0, 1, \ldots, k-2$.

Let us consider the sequence of colours $c(1), c(2), c(3), c(4), c(5)$ where $c(1)$ *and* $c(4), c(5)$ are from K^s and $c(2), c(4)$ are elements of K^r.

Let $v_0=(x)$ be a general point of the graph I then for the vertices $v_1={}^1J_{c(1)}(v_0)$, $v_2=N_{c(2)}(v_1)$, $v_3={}^2J_{c(3)},(v_2)$, $v_4=N_{c(4)}(v_3)$, $v_5={}^1J_{c(5)}(v_4)$ the relations $v_0\psi v_3$, $v_2\ \psi v_5$ holds.

We consider the tuple of colours $c(1), c(2)\ldots., c(t)$, $t=1 \bmod 4$ such that $c(i)\epsilon K^s$ *for* $i=0,1 \bmod 4$ and $c(i) \epsilon K^r$ for $i=2,3 \bmod 4$.

We refer to the sequence of vertexes $v_1 ={}^1J(v_0)$, $v_2=N_{c(2)}(v_1)$, $v_3={}^2J_{c(3)}$, $v_4=N_{c(4)}(v_3)$, $v_5={}^1J(v_4)$, $v_6=N_{c(6)}(v_5)$, $v_7={}^2J_{c(7)}(v_6)$, $v_8=N_{c(8)}(v_7),\ldots., v_{t-1}=N_{c(t-1)}(v_{t-2})$, $v_t={}^1J(v_{t-1})$ as *walk on the adjacency graph* with the starting point (x) and the colour trace $c(1), c(2), \ldots, c(t)$.

For each positive integer l we can consider graph $I_m(K)$ together with ${}^lI_m= I_m(K[y_1, y_2, \ldots, y_l])$ 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 walk on the adjacency graph $\psi(K[y_1, y_2, \ldots, y_l])$ of length $4t+1$ with starting point $(y_1, y_2, \ldots, y_s, y_{s+1}, y_{s+2}, \ldots, y_{m+s})$ and colours $c(1), c(2), \ldots, c(t)$ such that $c(i)\epsilon K[y_1, y_2, \ldots, y_s]^s$ for $i=0,1 \bmod 4$ and $c(i)\epsilon K[y_1, y_2, \ldots, y_s]^r$ for $i=2,3 \bmod 4$.

Assume that $c(t)=(h_1(y_1, y_2,\ldots,y_s), h_2(y_1, y_2,\ldots, y_s), \ldots, h_s(y_1, y_2,\ldots, y_s))$.

Then $v_1=(h_1, h_2, \ldots, h_s, g_1, g_2,\ldots, g_m)$. Let us consider the polynomial map ${}^{I(K),c}Pass,\ c\epsilon K[x_1,x_2,\ldots, x_s]^{(2t+1)s+2rt}$ of K^{s+m} to itself which sends $(y_1, y_2,\ldots,y_s, y_{s+1},\ldots, y_{s+m})$ to v_t, i. e. the map

$y_1 \to h_1(y_1, y_2,\ldots,y_s)$, $y_2 \to h_2(y_1, y_2,\ldots,y_s),\ldots$, $y_s \to h_s(y_1, y_2,\ldots,y_s)$,

$y_{s+1} \to g_1(y_1, y_2,\ldots,y_s, y_{s+1}, y_{s+2},\ldots,y_{s+m})$, $y_{s+2} \to g_2(y_1, y_2,\ldots,y_s, y_{s+1}, y_{s+2},\ldots,y_{s+m}),\ldots$, $y_{s+m} \to g_m(y_1, y_2,\ldots,y_s, y_{s+1}, y_{s+2},\ldots,y_{s+m})$,

It is easy to see that this transformation is bijective if and only if the map $y_1 \to h_1(y_1, y_2,\ldots,y_s)$, $y_2 \to h_2(y_1, y_2,\ldots,y_s)$, …, $y_s \to h_s(y_1, y_2,\ldots,y_s)$, is bijective on K^s ([5]). Defined above transformations form a semigroup ${}^{I(K)}S_P$ 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 ${}^{I(K)}S_l$ formed by transformation of kind ${}^{I(K),c}Pass,\ c\epsilon K[x_1,x_2,\ldots, x_s]^{(2t+1)r+2\ ts}$ acting on the variety K^{m+r}.

We can treet the sequence c from $K[x_1,x_2,\ldots, x_s]^l$ as the tuple of its coordinates c_i from $K[x_1,x_2,\ldots, x_s]$ and define degree of c as of polynomials $c_i(x_1, x_2,\ldots, x_s)$. The following two statements are proven in [5].

Theorem 1.

Let K be a commutative ring. Cellular Schubert graph $CS^{m,k}{}_n(K)$ is a linguistic graph of degree 2 of type (s, r, p) where

$s=|\Delta(\{n, n-1, n-2, \ldots, n-m+1\})- \Delta(\{n, n-1, n-2, \ldots, n-m+1\}) \cap\Delta(\{n, n-1, n-2, \ldots, n-k+1\})|$,

$r=|\Delta(\{n, n-1, n-2, \ldots, n-k+1\}) - \Delta(\{n, n-1, n-2, \ldots, n-m+1\}) \cap\Delta(\{n, n-1, n-2,\ldots, n-k+1\})|$ 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 $CS^{m,k}{}_n(K)$be a Cellular Schubert as in the previous statement.Then transformations ${}^{I(K),c}Pass,\ c\epsilon K[x_1,x_2,\ldots, x_s]^{(2t+1)s+2rt}$, $t\geq 5$, $c\epsilon K[x_1,x_2,\ldots, x_s]^{(2t+1)s+2rt}$ of the affine space K^{s+p} such that $deg(c(i))+deg(c(i+1))\leq 2$ for $i=1 \bmod 2$, $i<t$ and $deg(c(t))\leq 2$, are elements of Cremona semigroup of degree ≤ 2. If the lefthand side of one of the written above inequalities is 2 then the degree of the transformation is 2.

3. Public key based on Cellular Schubert graph

3.1. 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. For the simplicity we assume that $0<\alpha < \beta$.

She sets parameters $m=[\alpha n+a]$ and $k=[\beta n+b]$, where parenthesis denote the flow function and a and b are selected constants. Alice takes finite field $F=F_q$, $q=2^d$, $d \geq 32$. Alice computes parameter s, r and p of the linguistic graph $CS^{m,k}{}_n(K)$. She selects the length of path j of kind $j=4t+1$.Alice will use vector space F^{s+p} as space of the plaintexts. Thus she selects parameters $d_1=deg\ c(1)$, $d_2=deg\ c(2),\ldots, d_t= deg\ c(t)$ which satisfy the condition of theorem 2. She selects them from $\{0,1, 2\}$ under the condition that $d_i\_+d_{i+1}\_=2$ for each odd parameter and $d_j =2$.

Alice forms maps $c(i),\ i=1, 2, \ldots. , j-1$ of kind $(f_1(y_1, y_2,\ldots, y_s), f_2(y_1, y_2,\ldots, y_s),\ldots, f_s(y_1, y_2,\ldots, y_s))$ or $(g_1(y_1, y_2,\ldots, y_s), g_2(y_1, y_2,\ldots, y_s),\ldots, g_r(y_1, y_2,\ldots, y_s))$ of degree d_i. She can form these tuples of polynomials via selection of their coefficients as pseudorandom or genuinely random parameters.

Alice selects linear transformation $(y_1, y_2,\ldots, y_{s-1})\to(y_1, y_2,\ldots, y_{s-1})C=(l_1(y_1, y_2,\ldots, y_s), l_2(y_1, y_2,\ldots, y_s),\ldots, l_{s-1}(y_1, y_2,\ldots, y_s), y_s\to(y_s)^2)$ where C is the matrix of the Singer cycle which is a linear transformation of order $q^{s-1}-1$, (see [17]) and forms c(j) as the tuple $(l_1(y_1, y_2,\ldots, y_s), l_2(y_1, y_2,\ldots, y_s),\ldots, l_{s-1}(y_1, y_2,\ldots, y_s), (y_s)^2)$. She constructs the transformation ${}^{I(K),c}Pass=F$ of Theorem 2 with selected as above $c=(c(1), c(2),\ldots, c(j))$.

Finally Alice selects bijective affine transformation T_1 and T_2 and computes the standard form of $T_1FT_2=G$.

She presents multivariate rule G to public users.

Remark. The choice of c_j insures that the inverse map of G has a polynomial degree $\geq 2^{d-1}$ (see [13]).

Noteworthy that the choice $T_2=(T_1)^{-1}$ insures that cyclic group generated by G has order multiple to $q^{s-1}-1$.

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

3.2. Description of decryption procedure.

Let us consider the private key procedure for the decryption. Assume that Alice gets the ciphertext $z=(z_1, z_2, \dots, z_{s+p})$.

Step 1.

She treats it as column vector and computes $(T_2)^{-1}(z)=(q_1, q_2, \dots, q_s, q_{s+1},\dots, q_{s+2}, \dots, q_{s+p})=(p)$.

Step 2.

Alice uses the matrix C of the Singer cycle to solve the following equations. $l_1(x_1, x_2, \dots, x_s)=q_1$, $l_2(x_1, x_2, \dots, x_s)=q_2,\dots, l_{s-1}(x_1, x_2, \dots, x_s)=q_{s-1}$, $(x_s)^2=q_s$

Assume that $x_i=d_i$, $i=1, 2, \dots, s$ is the solution.

Step 3.

She computes numerical colours

$c(i)(d_1, d_2, \dots, d_s)=({}^ia_1, {}^ia_2, \dots, {}^ia_s)=({}^ia)$ for $i=1, 0 \pmod 4$, $i\leq j$.

$c(i)(d_1, d_2, \dots, d_s)=({}^ib_1, {}^ib_2, \dots, {}^ib_r)=({}^ia)$ for $i=2, 3 \pmod 4$, $i<j$.

Step 4.

Alice forms the point ${}^1(p)$ of the graph $CS^{m,k}{}_n(F_q)$. in the form ${}^1J_{c(j-1)}(p)=({}^{j-1}a_1, {}^{j-1}a_2, \dots, {}^{j-1}a_s, q_{s+1}, q_{s+2}, \dots, q_{s+p})$.

Step 5. She computes the path in this Schubert adjacency graph with the starting point ${}^1(p)$ and other vertexes $N_{c(j-2)}({}^1(p))={}^2v$, ${}^2J_{c(j-3)}({}^2v)={}^3v$, $N_{c(j-4)}({}^3v)={}^4v, \dots, N_{c(1)}({}^{j-2}v)={}^{j-1}v$, ${}^1J_{c(0)}({}^{j-1}v)=v$ where $c(0)=(d_1, d_2, \dots, d_s)$.

Step 6.

Alice treats v as column vector and computes the plaintexts as $(T_1)^{-1}(v)=(r_1, r_2, \dots, r_{s+p})$.

3.3. Complexity estimates in the case of general position.

Let us assume the case of presented above public key in the case of finite field F_q of characteristic 2. So the space of plaintext will be a vector space $(F_q)^m$ where $m=s+p= =O(n^2)$, the colour spaces for points and lines will be the vector spaces $(F_q)^s$ and $(F_q)^r$ where $r=O(n^2)$ and $s = O(n^2)$. It will be convenient for us to use parameter n for the estimation of the complexity of decryption procedure for Alice

The complexity of computation of the image of $T_1{}^{I(K),c}$ *Pass* T_2 is determined by the time of computation of the path in the adjacence Schubert graph from the selected point from $(F_q)^m$ accordingly to the sequence of numerical colours ${}^i(a)$, $i=1, 2, \dots, j$ obtained via the specialisation of the tuples $c(j)$ of quadratic polynomials in s variables.

The key parameter for the computation of the complexity is j. The natural selection is $j=O(n)$. Each ${}^i(a)$ can be computed $O(n^6)$. So the sequence of numerical colours of length j can be computed in time $O(n^7)$. Computation of the values of operators ${}^1J$ and ${}^2J$ takes $O(n^2)$ elementary operation. The computation of neighbour $N(v)$ of v with colour c will take time $O(n^4)$.The repetition of this operation j times costs $O(n^5)$. Noteworthy that computation of affine transformation in $O(n^2)$ variables takes time $O(n^4)$. These arguments evaluate general complexity of the computation of the plaintexts as $O(n^7)$.

It means that the complexity of decryption is $O(m^{3.5})$ where m is the dimension of the space of plaintexts

4. 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 (see [20]).

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 (*see [18]).

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] or [19]). 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 these 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 $(PG_n(F_q), PG_n(F_q[x_1, x_2, \ldots, x_n]))$ where $PG_n(F_q)$ is classical finite n-dimensional projective geometry and $PG_n(F_q[x_1, x_2, \ldots, x_n])$ is its natural analogue defined over multivariate ring $F_q[x_1, x_2, \ldots, x_n]$.

For the construction of public key a hidden problem to find a path between two vertexes of the adjacency Schubert graph of $PG_n(F_q[x_1, x_2, \ldots, x_n])$ 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_q, $q=2^d$ the multivariate rule is given by the system of quadratic equations. The choice of large d (like d=*32, d=64*) insures that the inverse map has a very large polynomial degree.

The new bijective public rule can be used as instrument of encryption as well as for making digital signatures. The suggested new public key algorithm is an obfuscation of the multivariate cryptosystem of [13].

5. Acknoledgements

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

6. References

[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] PQC Standardization Process: Announcing Four Candidates to be Standardized, Plus Fourth Round Candidates, https://csrc.nist.gov/news/2022/pqc-candidates-to-be-standardized-and-round-4

[7] Anne Canteaut, François-Xavier Standaert (Eds.), Eurocrypt 2021, LNCS 12696, 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17–21, 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] V. 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] V. Ustimenko, Linear codes of Schubert type and quadratic public keys of Multivariate Cryptography, IACR e-print archive, 2023/175.
[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] I. Gelfand, R. MacPherson, Geometry in Grassmanians and generalisationof the dilogarithm, Adv. in Math., 44 (1982), 279-312.
[16] I. Gelfand, V. Serganova, Combinatorial geometries and torus strata on homogeneous compact manifolds, Soviet Math. Surv. 42 (1987), 133-168.
[17] A. Cossidente, M. J. De Resmini, Remarks on Singer Cyclic Groups and Their Normalizers, Designs, Codes and Cryptography, 32, 97–102, 2004.
[18] J. Ding and A. Petzoldt, "Current State of Multivariate Cryptography," in IEEE Security & Privacy, vol. 15, no. 4, pp. 28-36, 2017, doi: 10.1109/MSP.2017.3151328.
[19] N. Koblitz, Algebraic aspects of cryptography, Springer (1998), 206 p.
[20] N. Sendrier, "Code-Based Cryptography: State of the Art and Perspectives," in IEEE Security & Privacy, vol. 15, no. 4, pp. 44-50, 2017, doi: 10.1109/MSP.2017.3151345.