UDC 519.1, 514.128

Linear codes of Schubert cells and implementations of new quadratic public keys of Multivariate Cryptography

Vasyl Ustimenko[1], Oleksandr Pustovit[2]

[1] Professor, Doctor of Physical and Mathematical Sciences, University of Royal Holloway (London), Egham Hill, Egham TW20 0EX, United Kingdom and Institute of Telecommunications and Global Information Space of the National Academy of Sciences of Ukraine, Chokolivsky Boulevard 13, 03186, Kyiv, e-mail: vasylustimenko@yahoo.pl
[2] Candidate of Technical Sciences, Institute of Telecommunications and Global Information Space of the National Academy of Sciences of Ukraine, Chokolivsky Boulevard 13, 03186, Kyiv, e-mail: sanyk_set@ukr.net

Multivariate Cryptography and Code Base Cryptography together with three other directions form the list of core areas of Poat Quantum Cryptography. Secure quadratic multivariate cryptosystem from are able to establish the shortest digital signatures. An idea of multivariate cryptography algorithms with quadratic transformation induced by walks on Cellular Schubert Graphs was proposed recently. These graphs are defined via restriction of the incidence relations of finite projective geometry on two distinct Schubert cells. The method defines nonlinear transformation of the vector space of vertexes of one of this cells. In this paper the implementations of these multivariate cryptosystems are considered in the case of large finite fields of characteristic 2. Quadratic map of large order is combined with two affine transformations. The lower bound of polynomial degree of the inverse map and complexity estimates for private key decryption are introduced.

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

Introduction. It is well known that Coding based Cryptography, Multivariate Cryptography and Lattice based Cryptography are among five core areas of Post-Quantum Cryptography. Each of these areas is based on the complexity of certain NP hard problem. Noteworthy that fundamental assumption of cryptography that there are no polynomial-time algorithms for solving any NP-hard problem remains valid. So all five directions are well justified theoretically. The tender of US National Institute of Standardisation Technology (NIST, 2017) is dedicated to the standardisation process of possible real life Post-Quantum Public keys. Already selected in July of 2022 four cryptosystems are developed via methods of Lattice based Cryptography. This fact motivates researchers from other four core areas of Post Quantum Cryptography to continue design of new cryptographical primitives. Graph based multivariate public keys with bijective encryption maps generated via special walks on incidence graph of projective geometry were proposed in [1]. It can be count as attempt to combine methods of Coding based and Multivariate Cryptographies.

Classical multivariate public rule is a transformation of *n*-dimensional vector space over finite field F_q which move vector $(x_1, x_2,..., x_n)$ to the tuple $(g_1(x_1, x_2,..., x_n), g_2(x_1, x_2,..., x_n),..., g_n(x_1, x_2,..., x_n))$, where polynomials g_i are given in their standard form, i. e. lists of monomial terms in the lexicographical order. The degree of this transformation is the maximal value of $\deg(g_i)$. Traditionally public rule has degree *2* or *3*.

1. Projective geometries and Schubert cellular graphs

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

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 $e_1, e_2,..., e_n$ of *V* and identify ${}^{n-1}PG(F_q)$ with the totality of linear codes in $(F_q)^n$. The geometry ${}^{n}G(q)={}^{n-1}PG(F_q)$ is a partition of subsets ${}^{n}G_i(q)$ consisting of elements of selected type *i, i=1, 2,…, n-1*. Let *U* stands for the unipotent subgroup of automorphism group $PGL_n(F_q)$ consisting of lower unitriangular matrices.

Let us consider largest orbits ${}^{m}LS(q)$ of the natural action of *U* on ${}^{n}G_m(q)$ They are known as largest Schubert cells. We consider the bipartite graph ${}^{m,k}CS_n(F_q)$ of the restriction of *I* onto disjoint union ${}^{m}LS(F_q)$ and ${}^{k}LS(F_q)$. It is bipartite graph with bidegrees q^r and q^s. We refer to ${}^{m,k}CS_n(F_q)$ as Cellular Schubert graph.

In particular case *n=2m+1, k=m* these graphs are known as Double Schubert graphs (see [2] or [1] and further references). Fact that unipotent subgroup *U* can be defined in the case of affine spaces K^n allows to define cellular Schubert graphs ${}^{m,k}CS_n(K)$ over commutative ring *K* (see [2] or [1] and further references).

2. Linguistic graphs 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 *(s, r, m)* if point $x=(x_1,x_2,...,x_s,x_{s+1},x_{s+2},...,x_{s+m})$ is incident to line $y=[y_1,y_2,...,y_r,y_{r+1},y_{r+2},...,y_{r+m}]$ if and only if the following relations hold

$$a_1x_{s+1}+b_1y_{r+1}=f_1(x_1,x_2,...,x_s,y_1,y_2,...y_r),$$
$$a_2x_{s+2}+b_2y_{r+2}=f_2(x_1,x_2,...,x_s,x_{s+1},y_1,y_2,...,y_r,y_{r+1}),\ ...$$
$$a_mx_{s+m}+b_my_{r+m}=f_m(x_1,x_2,...,x_s,x_{s+1},...,x_{s+m},y_1,y_2,...,y_r,y_{r+1},...,y_{r+m}),$$

where a_j and b_j, *j=1,2, ...,m* are not zero divisors, and f_j are multivariate polynomials with coefficients from *K*.

The colour $\dot{\rho}(x)=\dot{\rho}((x))$ $(\dot{\rho}(y)=\dot{\rho}([y]))$ 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.

For each $b\in K^r$ and $p=(p_1,p_2,...,p_{s+m})$ 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 $l=[l_1,l_2,...,l_{r+m}]$ there is the unique neighbour of the line $(p)=N_c([l])$ with the colour *c*.On the sets *P* and *L* of points and lines of linguistic graph we define jump operators $J=J_b(p)=(b_1,b_2,...,b_s,p_{s+1},p_{s+2},...,p_{s+m})$, where $(b_1,b_2,...,b_s)\in K^s$ and $J=J_b([l])=[b_1,b_2,...,b_r,l_{r+1},l_{r+2},...,l_{r+m}]$, where $(b_1,b_2,...,b_r)\in K^r$ for the point $(p_1,p_2,...,p_{s+m})$ and the line $[l_1,l_2,...,l_{r+m}]$.

Noteworthy, that the path in $v_0,v_1,...,v_k$ the linguistic graph I_m is determined by starting vertex v_0 and colours of vertexes $v_1,v_2,...,v_k$. We can take commutative ring $R=K[y_1,y_2,...,y_l]$ and consider graph $I_m(K)$ together with infinite graph $I_m(R)=I_m(K[y_1,y_2,...,y_l])$ defined by the same polynomials $f_i, i=1,2,...,m$ with coefficients from *K* but with partition sets R^{s+m} and R^{r+m}.

Assume that *l=m+s*. We can consider the path in $I_m(R)$ of length *2k* in with starting point $(y_1,y_2,...,y_s,y_{s+1},y_{s+2},...,y_{s+m})$ and consecutive colours $G_1,H_1,G_2,H_2,...,G_k,H_k$ such that $G_i\in K[x_1,x_2,...x_s]^s$ and $H_i\in K[x_1,x_2,...,x_s]^r$. The last vertex of this path will be a point *(p)* with consecutive coordinates $h_1,h_2,h_s,f_{s+1},f_{s+2},...,f_{s+m}$ where $f_1,f_2,...,f_{s+m}$ are elements of $K[x_1,x_2,...,x_s,x_{s+1},x_{s+2},...,x_{s+m}]^s$.

Finally we consider $u=J_H(p)$ where $H=(g_1,g_2,...,g_s)$ is the element of $K[x_1,x_2,...,x_s]^s$. We define *passage transformation*

$Pas(G_1,G_2,...,G_k,H_1,H_2,...,H_k,H)$ of K^{r+s}

(space of points) with symbolic colours $G_1, H_2, ..., G_k, H_k$ and H via multivariate rule

$$y_1 \to g_1(y_1, y_2, ..., y_s), y_2 \to g_2(y_1, y_2, ..., y_s), ..., y_s \to g_s(y_1, y_2, ..., y_s),$$
$$y_{s+1} \to f_{s+1}(y_1, y_2, ..., y_{s+m}), y_{s+2} \to f_{s+2}(y_1, y_2, ..., y_{s+m}), ...,$$
$$y_{s+m} \to f_{s+m}(y_1, y_2, ..., y_{s+m}).$$

It is easy to see that this transformation is bijective if the map $y_i \to h_i(y_1, y_2, ..., y_s)$, *i=1, 2, … , s* is bijective on K^s.

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

Theorem 1. *Let K be a commutative ring. Cellular Schubert graph* ${}^{m,k}CS_m(K)$ *is a linguistic graph of degree 2 of type (s, r, p). Then transformations* $Pas(G_1, G_2, ..., G_j, H_1, H_2, ..., H_j, H), j \geq 1$ *of the affine space* K^{s+p} *such that* $\deg(H_i) = 1, \deg(G_i) = 1, i = 1, 2, ..., j$ *and H are quadratic multivariate tuples is a quadratic map on* K^{s+p}.

Conclusions. We are working on the algorithms for the generation of standard form of the map of kind ${}^1TG^2T$ where $G = Pas(G_1, G_2, ..., G_j, H_1, H_2, ..., H_j, H)$ *is a map of Theorem 1,* ${}^1T$ is bijective affine transformation of $V = (F_q)^d, d = p + s$ (element of $AGL_d(F_q)$) and ${}^2T$ is injective linear map from *V* to vector space *U* of dimension *l*, *l≥d*. This standard form $y_i \to f_i(y_1, y_2, ..., y_d), i = 1,2,..., l$ can be used as encryption tool or instrument for digital signatures.

We implement the generation in the case $K = F_q$, $q = 2^{32}$. Let us assume that *m, k, n, s, r, p, j* are parameters of Theorem 1 and 2 and *d=s+p*. For the generation of transformation *G* as above we select H_i and $G_i, i = 1,2,..., j$ of degree 1 with pseudorandom coefficients and take

$$H = (l_1, l_2, ..., l_{s-t}, (y_{s-t+1})^2, (y_{s-t+2})^2, ..., (y_s)^2),$$

where *t, 1 <t<s* is the constant, $l_i(y_1, y_2, ..., y_{s-t})$ are linear forms and rule $y_i \to l_i(y_1, y_2, ..., y_{s-t})$ is bijective transformation *D* of *V* of order $q^{s-t} - 1$, i. e. *D* is a Singer cycle. Accordingly [1] this choice insures that polynomial degree of G^{-1} is at least 2^{31} and its order is multiple of $q^{s-t} - 1$. We assume that *l=O(d)* and *m-k* is a constant and *m=an* for *0<a<1*. Under this condition public user can encrypt in time $O(d^3)$ and key owner can use his/her knowledge on H_i, G_i and *H* and decrypt in time $O(d^2)$.

Acknowledgements. This research is partially supported by British Academy Fellowship for Researchers under Risk 2022.

References

[1] *Vasyl Ustimenko*, Linear codes of Schubert type and quadratic public keys of Multivariate Cryptography, IACR e-print archive, 2023/175.
[2] *V. Ustimenko*, Graphs in terms of Algebraic Geometry, symbolic computations and secure communications in Post-Quantum world, UMCS Editorial House, Lublin, 2022, 198 p.

Лінійні коди клітин Шуберта та імплементації нових квадратичних публічних ключів криптографії від багатьох змінних

Василь Устименко, Олександр Пустовіт

Криптографія від багатьох змінних та Криптографія, що базується на кодах разом з трьома іншими напрямками, становлять список основних галузей Постквантової Криптографії. Безпечні квадратичні криптосистеми від багатьох змінних здатні реалізувати найкоротші цифрові підписи. Нещодавно була запропонована ідея алгоритмів криптографії від багатьох змінних з квадратичними перетвореннями, що індуковані блуканнями у клітинах графа Шуберта. Ці графи визначаються через обмеження відношення інцидентності скінченної проективної геометрії на дві різні найбільші клітини Шуберта. Метод визначає нелінійне пертворення на векторному просторі вершин однієї з клітин. У цій статті ми розглядаємо імплементацію цієї схеми для декількох сімейств графів, визначених над великими скінченними полями характеристики два. Квадратичне відображення великого порядку комбінується з двома афінними перетвореннями. Наводиться оцінка поліноміальної степені оберненого відображення та оцінка швидкодії приватного ключа.

Received 06.03.23