On Multivariate Algorithms of Digital Signatures of Linear Degree and Low Density.

Vasyl Ustimenko

University of Maria Curie Sklodowska, Lublin 20036, Poland

vasyl@hektor.umcs.lublin.pl

Abstract. Multivariate cryptography studies applications of endomorphisms of $K[x_1, x_2, \ldots, x_n]$ where K is a finite commutative ring. The importance of this direction for the construction of multivariate digital signature systems is well known. We suggest modification of the known digital signature systems for which some of cryptanalytic instruments were found . This modification prevents possibility to use recently developed attacks on classical schemes such as rainbow oil and vinegar system, and LUOV. Modification does not change the size of hashed messages and size of signatures. Basic idea is the usage of multivariate messages of unbounded degree and polynomial density for the construction of public rules. Modified algorithms are presented for standardization and certification studies.

Keywords: multivariate cryptography, multivariate digital signature systems, unbounded degree, standardisation.

1. On post quantum and multivariate cryptography.

Post Quantum Cryptography (PQC) is an answer to a threat coming from a full-scale quantum computer able to execute Shor's algorithm. With this algorithm implemented on a quantum computer, currently used public key schemes, such as RSA and elliptic curve cryptosystems, are no longer secure. The U.S. NIST made a step toward mitigating the risk of quantum attacks by announcing the PQC standardisation process [1] for new public key algorithms. In March 2019 NIST published a list of candidates qualified to the second round of the standardisation process. Few public key candidates are implemented, like candidate called Round 5 (see [2]) or classic Mc Eliece algorithm (see [3]).

Current candidates are developed within following directions of PQC: lattice based systems, code based cryptosystems, multivariate cryptography (see [4] and further references), hash based Cryptography, studies of isogenies for superelliptic curves.

Recall that Multivariate Cryptography (see [4]) uses polynomial maps of affine space K^n defined over a finite commutative ring K into itself as encryption tools. It exploits the complexity of finding a solution of a system of nonlinear equations from many variables. Multivariate cryptography uses as encryption tools nonlinear polynomial transformations of kind $x_1 \rightarrow f_1(x_1, x_2, \ldots, x_n)$, $x_2 \rightarrow f_2(x_1, x_2, \ldots, x_n)$, … , $x_n \rightarrow f_n(x_1, x_2, \ldots, x_n)$ transforming affine space K^n, where $f_i \in K[x_1, x_2, \ldots, x_n]$, $i=1,2,\ldots,n$ are multivariate polynomials usually given in a standard form, i. e. via a list of monomials in a chosen order (nonlinear endomorphisms of $K[x_1, x_2, \ldots, x_n]$.

2. On stable subsemigroups of formal Cremona group and their usage.

Let $K[x_1, x_2, \dots , x_n]$ be commutive ring of all polynomials in variables $x_1, x_2, \dots , x_n$ defined over a commutive ring K. Each endomorphism $F \in E_n(K)$ is uniquely determined by its values on formal generators x_1, $i=1,2,\dots, n$. Symbol $End(K[x_1, x_2, \dots , x_n])=E_n(K)$ stands for semigroup of all endomorphisms of $K[x_1, x_2, \dots , x_n]$. So we can identify F with the formal rule $x_1 \to f_1(x_1, x_2, \dots , x_n)$, $x_2 \to f_2(x_1, x_2, \dots , x_n)$, …, $x_n \to f_n (x_1, x_2, \dots , x_n)$ where $f_i \in K[x_1, x_2, \dots , x_n]$. Element F naturally induces the transformation $\Delta(F)$ of affine space K^n given by the following rule $\Delta(F):(\alpha_1, \alpha_2, \dots, \alpha_n) \to (f_1 (\alpha_1, \alpha_2, \dots, \alpha_n), f_2(\alpha_1, \alpha_2, \dots, \alpha_n), \dots, f_n(\alpha_1, \alpha_2, \dots, \alpha_n))$ for each $(\alpha_1, \alpha_2, \dots, \alpha_n) \in K^n$. Luigi Cremona [5] introduced $\Delta(E_n(K))= CS(K^n)$ which is currently called *affine Cremona semigroup*. A group of all invertible transformations of $CS(K^n)$ with an inverse from $CS(K^n)$ is known as *affine Cremona group* $CG(K^n)$ (shortly *Cremona group*, see for instance [6], [7]).

We refer to infinite $E_n(K)$ as *formal affine Cremona semigroup*. Density of the map F is the total number of monomial terms in all f_i.

3. On multivariate digital signatures algorithms and their privatisation scheme.

It is commonly admitted that Multivariate cryptography turned out to be more successful as an approach to build signature schemes primarily because multivariate schemes provide the shortest signature among post-quantum algorithms. Such signatures use system of nonlinear polynomial equations

$${}^1p(x_1,x_2 , \dots , x_n) = {}^1p_{i,j} \cdot x_ix_j+{}^1p_i \cdot x_i+ {}^1p_0$$

$${}^2p(x_1, x_2, \dots , x_n) = {}^2p_{i,j} \cdot x_ix_j +{}^2p_i \cdot x_i +{}^2p_0$$

$$\dots$$

$${}^mp(x_1,x_2 , \dots , x_n) = {}^mp_{i,j} \cdot x_ix_j+{}^m\mathrm{p}_\mathrm{i} \cdot x_i+ {}^mp_0$$

where ${}^kp_{i,j}$, ${}^kp_i$ are elements of selected commutative ring K.

The quadratic multivariare cryptography map consists of two bijective affine transformations, S and T of dimensions n and m, and a quadratic element P' of kind $x_i \to {}^ip$ of formal Cremona group, where ${}^ip$ are written above elements of $K[x_1, x_2, \dots,x_n]$.We denote via $\Delta(P')^{-1}(y)$ some reimage of $y=\Delta(P(x))$. The triple $\Delta(S)^{-1}$, $\Delta(P')^{-1}$, $\Delta(T)^{-1}$ is the private keyq also known as the trapdoor.

The public key is the composition S, P' and T which is by assumption hard to invert without the knowledge of the trapdoor. Signatures are generated using the private key and are verified using the public key as follows. The message is hashed to a vector y via a known hash function. The signature is $\Delta(T)^{-1}(\Delta(P')^{-1})(\Delta(S)^{-1})$. The receiver of the signed document must have the public key P in posession. He computes the hash y and checks that the signature x fulfils $\Delta(P)(y)=x$.

EXAMPLE. Assume that we have two groups of variables $z_1, z_2, \ldots, z_r$ and $z'_1, z'_2, \ldots, z_{n-r}$ such that the substitution $x_1=z_1, x_2=z_2, \ldots, x_r=z_r, x_{r+1}=z'_1, x_{r+2}=z'_2, \ldots, x_n=z'_{n-r}$ converts every single element ${}^ip$ to expression in the form $\Sigma\gamma_{ijk}z_jz'_k+\Sigma\lambda_{ijk}z'_jz'_k+\Sigma\varsigma_{ij}z_j+\Sigma\varsigma'_{ij}z'_j+\sigma_i$. In this situation we have to sign a given message y and the result is a valid signature x .The coefficients, $\gamma_{ijk}, \lambda_{ijk}, \varsigma_{ij}, \varsigma'_{ij}$and σ_i must be chosen secretly. The vinegar variables z'_i are chosen randomly (or pseudorandomly).The resulting linear equations system gets solved for the oil variables z_i.

Described above *unbalanced oil and vinegar (UOV) scheme* is a modified version of the oil and vinegar scheme designed by J. Patarin. Both are digital signature protocols. They are algorithms of multivariate cryptography. The security of this signature scheme is based on an *NP*-hard mathematical problem. To create and validate signatures a minimal quadratic equation system must be solved. Solving m equations with n variables is *NP*-hard. While the problem is easy if m is either essentially larger or essentially smaller than n, importantly, the problem is thought to be difficult in the average case when m and n are nearly equal, even when using a quantum computer. Multiple signature schemes have been devised based on multivariate equations with the goal of achieving quantum resistance.

4. Some semigroups of endomorphisms of $K[x_1, x_2, \ldots x_k]$ defined via linguistic graphs.

Let us consider graph based constructions of semigroups of formal Cremona semigroup $E_n(K)$.

Element $x_1 \rightarrow f_i(x_1, x_2, \ldots, f_n)$, $i=1,2,\ldots,n$ of this semigroup will be identified with the tuple of elements $(f_1, f_2, \ldots, f_n)$, $f_i \in K[x_1, x_2, \ldots, x_n]$ when it is convenient.

Let us consider a totality ${}^sBS(K)$ of sequences of kind $u=(H_0, G_1, G_2, H_3, H_4, G_5, G_6, \ldots, H_{t-1}, H_t)$, $t=4i$, where $H_k \in E_s(K)$, $G_j \in E_s((K)$. We refer to ${}^sBS(K)$ as a totality of free symbolic strings of rank s. We define a product of u with $u'=(H'_0, G'_1, G'_2, H'_3, H'_4, G'_5, G'_6, \ldots, H'_{l-1}, H_l)$ as $w=(H_0, G_1, G_2, H_3, H_4, G_5, G_6, \ldots, H_{t-1}, H'_0(H_t), G'_1(H_t), G'_2(H_t), H'_3(H_t), H'_4(H_t), G'_5(H_t), G'_6(H_t), \ldots, H'_{l-1}(H_t), H'_l(H_t))$. Notice that the compositions of maps is computed in $E_s(K)$.

It is easy to see that this operation transforms ${}^sBS(K)$ into the semigroup with the unity element (H_0), where E_0 is an identity transformation from

$S(K^s)$. Elements of kind $(H_0, G_1, G_2, H_3, H_4)$ are generators of the semigroup. This subsemigroup has some similarity with subsemigroup of special chains in the free product $E_s(K)$▪$E_s(K)$. We refer to ${}^sBS(K)$ as *semigroup of free regular strings of dimension s.*

Let us assume that H_t of written above $u \in {}^sBS(K)$ is a bijective map and its inverse is a polynomial map (in the case of infinite ring K). Then we can consider a reverse linguistic string $Rev(u)= (H_{t-1}(H_t^{-1}), G_{t-2}(H_t^{-1}), G_{t-3},(H_t^{-1}), H_{t-4}(H_t^{-1}),H_{t-5}^1(H_t), \ldots,G_2(H_t^{-1}), G_1(H_t^{-1}), H_0(H_t^{-1}), H_t^{-1})$ and refer to u as reversible string. Let ${}^sBR(K)$ stand for the semigroup of reversible strings.

Let K be a finite 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 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

$$a_1x_{s+1}+b_1\mathbf{y}_{r+1}=f_1 (x_1, x_2 ,\ldots , x_s, y_1,y_2, \ldots , y_r)$$
$$a_2x_{s+2}+b_2\mathbf{y}_{r+2}=f_2 (x_1, x_2 ,\ldots , x_s, x_{s+1}, y_1,y_2, \ldots , y_r, y_{r+1})$$
$$\ldots$$
$$a_mx_{s+m}+b_m\mathbf{y}_{r+m}=f_m (x_1, x_2 ,\ldots , x_s, x_{s+1},\ldots, x_{s+m}, y_1,y_2, \ldots , y_r, y_{r+1}, \ldots, y_{r+m})$$

where a_j, and b_j , $j=1,2,,,,m$ 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 [8]).

The colour $\rho(x)=\rho((x))$ $(\rho(y)=\rho([y]))$ of point $\mathbf{x}$ (line $[\mathbf{y}])$ 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 $[l]=N_b(p)=N((p),b)$ 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 $(p)= N_c([l])=N([l],b)$ with the colour c. We refer to operator of taking the neighbour of vertex accordingly chosen colour as sliding operator. On the sets P and L of points and lines of linguistic graph we define jump operators ${}^1J={}^1J_b(p)=J((p),b)=(b_1, b_2,\ldots,b_s, p_1, p_2 ,\ldots , p_{s+m})$, where $(b_1, b_2,\ldots,b_s)\in K^s$ and ${}^2J={}^2J_b ([l])=J([l],b) =[b_1, b_2,\ldots,b_r, l_1, l_2 ,\ldots , l_{r+m}]$, where $(b_1, b_2,\ldots,b_r)\in K^r$. We refer to tuple (s, r, m) as type of the linguistic graph $I=I(K)$.

Notice that we can consider the same set of above equations with coeficients from K for variables x_i and y_i from the extension K' of K and define graph ${}^{K'}I={}^{K}{}'I(K)$. Let $s=r$ and $K'=K[x_1, x_2 ,\ldots, x_n]$, $n=m+s$. We consider induced subgraph in I' of all vertices of ${}^{K'}I$ with colours from $K[x_1, x_2,\ldots, x_s]$ (tuples of $K[x_1, x_2,\ldots, x_s]^{s}$)

We form the sequence of vertices (walk with jumps) of graph *I'* with the usage of string *u* from free linguistic semigroupn ${}^{s}BS(K)$.

We take initial point (x)=$(x_1, x_2, \ldots, x_s, x_{s+1}, x_{s+2}, \ldots, x_{s+m})$ formed by the generic variables of K' and consider
a skating chain

$(x), J((x),H_0)=({}^{1}x), N(({}^{1}x),G_1)=[{}^{2}x], J([{}^{2}x],G_2)=[{}^{3}x], N([{}^{3}x],H_3)=({}^{4}x), J(({}^{4}x),H_4)=({}^{5}x), \ldots, J([{}^{t-2}x],G_{t-2})=[{}^{t-1}x], N([{}^{t-1}x],H_{t-1})=({}^{t}x), J(({}^{t}x),H_t)=({}^{t}x)$.

Let $({}^{t}x)$ be the tuple $(H_t, F_2, F_3, \ldots, F_n)$ where $F_i \in K[x_1, x_2, \ldots, x_n]$. We define ${}^{I}\Psi(u)$, $I=I(K)$ as the map $(x_1, x_2, \ldots, x_n) \rightarrow (H_t, F_2, F_3, \ldots, F_n)$ and refer to it *as chain transition of point variety.*

The statement written below follows from the definition of the map.

Lemma 1. *The map* $\psi={}^{I}\psi$**:** ${}^{s}BS(K) \rightarrow E_n(K)$ *is a homomorphism of semigroups,* $\psi({}^{s}BR(K))$ *is a group* ([9]),

We refer to ${}^{I}\psi({}^{s}BS(K))={}^{I}CT(K)$ as a *chain transitions semigroup* of linguistic graph *I(K)* and to map ψ as *linguistic compression map.* Notice that in the case of the finite commutative ring homomorphism composition $\Delta\psi$ *of homomorphism* Δ *and* ψ maps infinite semigroup into finite set of elements of $\Delta({}^{I}CT(K))$.

We define subsemigroup ${}^{s}GS(K)$ of *symbolic ground strings* as a totality of bipartite strings $u=(H_0, G_1, G_2, H_3, H_4, G_5, G_6, \ldots, H_{t-1}, H_t)$ in ${}^{s}BS(K)$ with $H_0=E_0$, $G_1=G_2$, $H_3=H_4$, $G_5=G_6, \ldots, H_{t-1}=H_t$ where E_0 is a unit of $E_n(K)$ and refer to ${}^{I}\psi({}^{s}GS(K))={}^{I}GCT(K)$ as *semigroup of ground chain transitions* on linguistic graph *I*.

5. Special homomorphisms of linguistic graphs and corresponding semigroups.

Let *I(K)* be linguistic graph over commutative ring *K* defined in section 3.1. and *M = {m1, m2,..., md}* be a subset of *{1, 2, ..., m}* (set of indexes for equations). Assume that equations indexed by elements from *M* of the following kind

$a_{m1}x_{m1} - b_{m1}y_{m1} = f_{m1}(x_1, x_2, \ldots, x_s, y_1, y_2, \ldots, y_r)$

$a_{m2}x_{m2} - b_{m2}y_{m2} = f_{m2}(x_1, x_2, \ldots, x_s, x_{m1}, y_1, y_2, \ldots, y_r, y_{m1})$

…

$a_{md}x_{md} - b_{md}y_{md} = f_{md}(x_1, x_2, \ldots, x_s, x_{m1}, x_{m2}, \ldots, x_{m\,d-1}, y_1, y_2, \ldots, y_r, y_{m1}, y_{m2}, \ldots, y_{m\,d-1,})$ define other linguistic incidence structure $I_{M.}$ Then the natural projections $\delta_{1,}: (x) \rightarrow (x_1, x_2, \ldots, x_s, x_{m1}, x_{m2}, \ldots, x_{md})$ and $\delta_2: [y] \rightarrow [y_1, y_2, \ldots, y_r, y_{m1}, y_{m2}, \ldots, y_{md}]$ of free modules define the natural homomorphism δ of incidence structure *I* onto $I_{M.}$. We will use the same symbol ρ for the colouring of linguistic graph $I_{M..}$

It is clear, that δ is colour preserving homomorphism of incidence structures (bipartite graphs). We refer to δ as symplectic homomorphism and graph I_M as symplectic quotient of linguistic graph *I.* In the case of linguistic graphs defined by infinite number of equations we may consider symplectic quotients defined by infinite subset M (see [9], where symplectic homomorphism was used for the cryptosystem construction).

Lemma 2. *A symplectic homomorphism $\acute{\eta}$ of linguistic graph I of type (r, s, m) onto I' defined over commutative ring K induces the semigroup homomorphism $\acute{\eta}^*$ of ${}^{I}CT(K)$ into ${}^{I'}CT(K)$ and the following diagram is commutative*

$$\begin{tikzcd}
{}^{s}BS_r(K) \arrow[r] \arrow[d] & {}^{I}CT(K) \arrow[dl, dash] \\
{}^{I'}CT(K) &
\end{tikzcd}$$

where horizontal and vertical arrows corresponds to linguistic compression homomorphisms ${}^{I}\psi$ and ${}^{I'}\psi$ and symbol / corresponds to η^*.

If S is a stable subsemigroup of ${}^{I}CT(K)$ (or $BCT_I(K)$) of degree d then $\acute{\eta}^*(S)$ is also a stable subsemigroup (or subgroup).The degree of $\acute{\eta}^*(S)$ is bounded above by d. We will search for subsemigroup X *of* ${}^{s}BS_r(K)$ and linguistic graphs $I(K)$ such that $\Psi(X)$ is a stable subsemigroups of ${}^{I}CT(K)$.

6. Example of stable subsemigroups of prescribed degree and density.

We define Double Schubert Graph $DS(k,K)$ over commutative ring K as incidence structure defined as disjoint union of partition sets $PS=K^{k(k+1)}$ consisting of points which are tuples of kind $x=(x_1, x_2, \dots, x_k, x_{11}, x_{12}, \dots, x_{kk})$ and $LS=K^{k(k+1)}$ consisting of lines which are tuples of kind $y=[y_1, y_2, \dots, y_k, y_{11}, y_{12}, \dots, y_{kk}]$, where x is incident to y, if and only if $x_{ij} - y_{ij}=x_i y_j$ for $i=1, 2,\dots, k$ and $j=1, 2,\dots, k$. It is convenient to assume that the indices of kind i,j are placed for tuples of $K^{k(k+1)}$ in the lexicographical order.

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 dimensions. We will consider these connection in details in the next section.

We define the colour of point $x=(x_1, x_2, \dots, x_k, x_{11}, x_{12}, \dots, x_{kk})$ from PS as tuple$(x_1, x_2, \dots, x_k)$ and the colour of a line $y=[y_1, y_2, \dots, y_k y_{11}, y_{12}, \dots, y_{kk}]$ as the tuple $(y_1, y_2, \dots, y_k)$. For each vertex v of $DS(k, K)$, there is the unique neighbour $y=N_a(v)$ of a given colour $a=(a_1, a_2, \dots, a_k)$. It means the graphs $DS(k, K)$ form a family of linguistic graphs.

Proposition 1. *Each subset J of M^2 defines symplectic homomorphism δ_J of $DS(k, K)$ onto linguistic graph $DS_J(k,K)$.*

It is easy to see that in the case of empty set J the image of the map is a complete bipartite graph with the vertex set K^kUK^k.

For a string $u=(H_0, G_1, G_2, H_3, H_4, G_5, G_{6,}..., H_{t-1}, H_t)$ we introduce function *dim(u)* which is the maximum of parameters $deg(H_0)+deg(G_1)$, $deg(G_2)+deg(H_3)$, $deg(H_4)+deg(G_5)$, $deg(G_6)+deg(H_7)$, $deg(G_{t-2})+deg(H_{t-1})$, $deg(H_t)$.

Proposition 2. *Let I(K) be an incidence relation of Double Schubert graph DS(k, K) or symplectic quotient of this graph and* $u=(H_0, G_1, G_2, H_3, H_4, G_5, G_{6,}..., H_{t-1}, H_t)$ *, t >0 be an element of* ${}^kBS(K)$. *Then transformation* ${}^I\psi(u)$ *has degree bounded by dim(u).*

Let us define a density *den(F)* of *F* of kind $x_i \rightarrow f_i(x_1, x_2, ...x_n)$ $\epsilon K[x_1,x_2, ..., x_n]$, $i=1,2,...n$ as maximum of densities $den(f_i)$.

For a string $u=(H_0, G_1, G_2, H_3, H_4, G_5, G_{6,}..., H_{t-1}, H_t)$ we introduce function *Den(u)* which is the maximum of $den(H_0)den(G_1)+den(G_2)den(H_3)+deg(H_4)deg(G_5)$, $deg(G_6)deg(H_7)+...+ den(G_{t-2})den(H_{t-1})$ and $den(H_t)$.

Proposition 3. *Let I(K) be an incidence relation of Double Schubert graph DS(k, K) or its linguistic quotient and* $u=(H_0, G_1, G_2, H_3, H_4, G_5, G_{6,}..., H_{t-1}, H_t)$ *,t>0 be an element of* ${}^kBS(K)$ *Then transformation* ${}^I\psi(u)$ *has density bounded from above by Den(u).*

Remark. *One can choose maps from* $E_k(K)$ *with equal densities of each coordinate. Then den(* ${}^I\psi(u)$*) =D(k). If all densities equals to parameter r. Then densty of* ${}^I\psi(u)=Den(u)=4r^2t$.

The proof is based on the fact that the chain transition ${}^I\psi$ *u* from moves $x_{i,j}$ into expression $x_{i,j}+T(u)$, where *T(u)* is a linear combination of products $f\epsilon K[x_1, x_2,..., x_k]$, $g\epsilon K[y_1, y_2,..., y_k]$.

Proposition 4. Let S_1 and S_2 are bijective linear monomial transformation from $E_m(K)$. The map $G=S_1F'S_2$ has degree and density bounded by *D(k)* and *d(k)*.

7. On families of multivariate digital signature schemes of unbounded degree.

Recall that the quadratic multivariare cryptography map consists of two bijective affine transformations *S* and *T* of dimensions *n* and *m*, and a quadratic element *P'* of kind $x_i \rightarrow {}^ip$ of formal Cremona group, where ${}^ip$ are written above elements of $K[x_1, x_2,...,x_n]$.

We suggest more general scheme where instead of *S* the combination *S' =DS* of nonlinear automorphism *G* of $K[x_1,x_2,...,x_n]$, $G\epsilon A_n(K)$ of density *O(1)* and unbounded degree of size *O(n)* with *S* is taken instead of *S*.

Construction of Multivariate Digital Signature scheme is given below. The public rule will be based on the family $G_n(K)$ constructed by the following scheme.

Let *[ ]'* be the ceiling operator, i. e. *[g(n)]'* be minimal integer $\geq g(n)$.

We select some constant *t* , *t>0* and consider function $[n^{1/2}]' +t =k$. Consider the linguistic graph $I=I(J,K)= DS_J (k, K)$ with the subset *J* of cardinality *n-k* in a set of cardinality k^2 and semigroup ${}^kB(K)$. We select element *u* with $dim (u)= \alpha n$, $\alpha=|K^*|$. According to the proposition 2 degree ${}^I\psi(u) =G'$ is bounded by αn. Notice that parameter α is selected because $x^k=e$ for $x \epsilon K^*$. As it follows from the construction of graph I we can easily select u such that $deg(G)=\alpha n$ and density c of G' is of size $O(1)$ (see proposition 3).

We considers $G_n = S_1 {}^{I(J,K)} \psi(u) S_2$ with pseudorandom monomial transformations of free module K^n. Now we create public rule $F=G_m SP'T$.

The density of F is $O(n^2)$ and linear degree is bounded by $2\alpha n$. It is clear that F can be used in obvious way as multivariate digital signature system with the same size of hashed message and format of signatures.

8. Conclusion.

Selected classical multivariate digital section based on quadratic public rules such as Rainbow like Unbalanced Oil and Vinegar algorithm and LUOV are presented for current NIST competition [1]. Cryptanalytics investigate efficiency of developed various attacks. So currently the search for modifications of algorithm to eliminate known attacks is already possible. Paper [14] suggests to transfer multivariate public rules onto secure El Gamal mode created via the usage of protocols of Noncommutative Cryptography.

This position paper suggests alternative approach based on the work with more sophisticated public rules. Suggested multivariate digital signature scheme is based on the composition of the map in n variables of linear degree αn, $\alpha>0$ and density $O(1)$ with the known nonbijective quadratic multivariate map. Recall that the density of endomorphism F of $K[x_1, x_2, \ldots, x_n]$ given by rule $x_i \to f_i(x_1, x_2, \ldots, x_n)$ is defined as maximum of numbers of monomial terms in f_i, $i=1,2,\ldots,n$.

Noteworthy that cryptosystems based on multivariate maps were proposed in [15] (the map is bijective) and [16], [17] (nonbijective transformations of K^n with injective restrictions on $(K^*)^n$)

The researchers of Institute of telecommunication and Global Information Space of National Academy of Sciences implemented the new digital signature algorithms on the level of prototype model. The combinations of described above
multivariate map of unbounded linear degree and density $O(1)$ is also taken with maps of Original Oil and Vinegar signature system, because the cryptanalytic instruments of [18] work only in the case of maps of bounded degree. Computer simulation is used for computation of densities and degrees on modernised public rules and for the comparison of time execution tables.

Noteworthy that in all cases K coincides with the ground finite fields selected for Rainbow like UOV, Lifted UOV and Original UOV. Selected multivariate digital signature schemes based on public rules of unbounded degree will be presented for the standardisation and certification processes conducted by the State Service of Special Communication and Information Protection of Ukraine (Kyiv).

References.

1. Post-Quantum Cryptography: Call for Proposals:https://csrc.nist.gov/Project; Post-Quantum-Cryptography-Standardization/Call-for-Proposals, Post-Quantum Cryptography: Round 2 Submissions.

2. M. Andrzejczak, The Low –Area FPGA Desighn for the Post – Quantum Cryptography Proposal Round 5, Proceedings of the Federated Conference on Computer Science and Information Systems (FedCSIS), Cryptography and Security Systems, Leipzig, 2019.
3. R. J. McEliece, A Public-Key Cryptosystem Based On Algebraic Coding Theory (1978), DSN Progress Report, 44: 114–116.
4. Jintai Ding and Albrecht Petzoldt. Current state of multivariate cryptography. *IEEE Security & Privacy*, 15(4):28–36, 2017.
5. Max Noether, Luigi Cremona , Mathematische Annalen 59, 1904, p. 1–19.
6. I.R. Shafarevich, On some in_nite dimension groups II, Izv. Akad. Nauk SSSR Ser. Mat., Volume 45, No. 1, pp. 214-226 (1981); Mathematics of the USSR-Izvestiya, Volume 18, No. 1, pp. 185-194 (1982).
7. Yu. Bodnarchuk, Every regular automorphism of the affine Cremona group is inner, Journal of Pure and Applied Algebra, Volume 157, Issue 1, pp. 115-119 (2001).
8. V. Ustimenko, Maximality of affine group, hidden graph cryptosystem and graph’s stream ciphers, Journal of Algebra and Discrete Mathematics, 1, 2004, v.10, pp. 51-65.
9. V.Ustimenko, On inverse protocols of Post Quantum Cryptography based on pairs of noncommutative multivariate platforms used in tandem, ePrint Archive, 897, 2019.
10. V. Ustimenko, On the usage of postquantum protocols defined in terms of transformation semigroups and their homomophisms, Theoretical and Applied Cybersecurity, National Technical University of Ukraine "Igor Sikorsky Kiev Polytechnic Institute", Volume 1, No. 2, pp. 32-44 (2020).
11. Jintai Ding and Joshua Deaton and Kurt Schmidt and Vishakha and Zheng Zhang, Cryptanalysis of The Lifted Unbalanced Oil Vinegar signature scheme, Cryptology ePrint Archive: Report 2019/1490.
12. Jintai Ding and Joshua Deaton and Vishakha and Bo-Yin Yang, The Nested Subset Differential Attack: A Practical Direct Attack Against LUOV which Forges a Signature within 210 Minutes, ePrint Archive: Report 2020/967.
13. Shuhei Nakamura and Yasuhiko Ikematsu and Yacheng Wang and Jintai Ding and Tsuyoshi Takagi. Shuhei Nakamura and Yasuhiko Ikematsu and Yacheng Wang and Jintai Ding and Tsuyoshi Takagi, New Complexity Estimation on the Rainbow-Band-Separation Attack, ePrint Archive: Report 2020/703
14. V. Utimenko, On Multivariate Algorithms of Digital Signatures on Secure El Gamal Type Mode, ePrint Archive: Report 2020/984.
15. V.Ustimenko, On multivariate public keys based on a pair of transformations with density gap, Reports of Nath . Acad of Sci, Ukraine, 2018. № 9, pp 21-27.
16. V. Ustimenko, On new multivariate cryptosystems based on hidden Eulerian equations, Reports of Nath. Acad of Sci, Ukraine, 2017. № 5, pp 17-24.
17. V. Ustimenko, On new multivariate cryptosystems based on hidden Eulerian equations over finite fields, ePrint Archive, 093, 2017.
18. A. Kipnis, A. Shamir, Cryptanalisis of the Oil and Vinegar Signature Scheme, Advances in Cryptology - Crypto 96, Lecture Notes in Computer Science, v. 1462, 257-266 (1996).