On historical Multivariate Cryptosystems and their restorations as instruments of Post-Quantum Cryptography

Vasyl Ustymenko[1,2]
[1] *Royal Holloway University of London, United Kingdom.*
[2] *Institute of telecommunications and global information space, Kyiv, Ukraine*
E - mail: Vasyl.Ustymenko@rhul.ac.uk

Abstract

The paper presents a short survey of the History of Multivariate Cryptography together with the usage of old broken multivariate digital signatures in the new protocol based cryptosystems constructed in terms of Noncommutative Cryptography. Cryptography is also presented. The general schemes of New cryptosystems is a combinations of Eulerian maps and quadratic maps with their trapdoor accelerators, which are pieces of information such than the knowledge of them allow to compute the reimages in a polynomial time. These schemes are illustrated by historical examples of Imai – Matsumoto multivariate digital signatures schemes and Unbalanced Oil and Vinegar Cryptosystems.

Keywords: Multivariate Cryptography, Digital signatures, Noncommutative Cryptography, Eulerian transformations , Protocol based cryptosystems, Public keys.

1 Introduction to Multivariate Cryptography

The interest to serious algebraic cryptological studies was stimulated recently by the research in Post Quantum Cryptography where among 5 core areas there are Multivariate Cryptography and Code - based Cryptography which need serious algebraic cryptography (linear codes, Goppa codes, Reed-Solomon codes used in Mc Elise cryptosystems and etc). The NIST project since 2017 is concentrated on Public Keys. aimed for the purposes to produce the encryption tools or instruments for the design of digital signatures (Canteaut et al., 2021). We has to admit that PQC secure quadratic multivariate rules can serve to create the shortest digital signature procedures. Recall that we have to add to mentioned above two directions of PQC the Hash based cryptography, Isogeny-based cryptography and Lattice based cryptography. We have to notice that all already NIST certified algorithms are not the public keys of Multivariate Cryptography. Quite long standing "The Rainbow Like Unbalanced Oil and Vinegar" (RUOV) digital signature method was rejected due to cryptanalytic studies published in the Proceedings of the Eurocrypt 2021 (Canteaut et al., 2021), (Buellens, 2021). The historical Multivariate Cryptography is a search for the pairs of kind *(F,T)* forming the quadratic or cubic trapdoor accelerator where *F* is a quadratic (or cubic) transformation of the vector space $(F_q)^n$ defined over the finite field and *T* is a polynomial invertor, i.e. the piece of information such that the knowledge of *T* allows to compute reimages of *F* in a polynomial time. Developers were hoped that the recovery of the reimage of *F* given in its standard form without a knowledge of *T* will stay as unsolved *NP*-hard problem. Recall that the standard form is the list of monomials of $F(x_i)$, $i=1,2,\ldots,n$ ordered lexicographically. The fact that quadratic transformations of public key *(F,T)* can provide the shortest known digital signatures is motivating a further search for appropriate trapdoor accelerators. This search was started by Imai and Matsumoto (Matsumoto et al, 1988) (see also (Ding et al, 2020)) who constructed a trapdoor accelerator in the case of finite fields of characteristic *2.* They use quadratic extensions F_2 of a finite field $F_1=F_q$, $q=2^m$ of characteristics *2* of degree *n*. They expressed a bijective transformation of F_r, $r=q^n$ of kind $x \rightarrow x^t$, $t=q^a+1$ where $(a+1, q^r-1)=1$ as quadratic transformation *F* of the vector space $(F_1)^n$. Authors suggested to use the standard form $G=L_1FL_2$ where L_1 and L_2 are elements of $\boldsymbol{AGL_n(F_1)}$ as the public rule corresponding to trapdoor accelerator (G, T), $T=(L_1, L_2, a)$.The cryptanalytic tools to break this potential cryptosystem were found by J. Patarin (see (Koblits, 1988) and further references). Long history of various modifications of Imai-Matsumoto cryptosystems is partially reflected in (Ding, 2004) or (Goubin et al, 2011). All of them were broken via corresponding cryptanalytic tools. We just mentioned some other cryptosystems inclusive Hidden Fields Equations suggested by J. Patarin and recent Unbalanced Oil and Vinegar cryptosystem for which corresponding cryptanalysis can be found in (Buellens, 2021). . The fact that quadratic transformations of public key *(F, T)* can provide the shortest known digital signatures is motivating a further search for appropriate polynomial invertors. The scheme is the following one. Let *(F, T)* be the pair such that the reimage of σ is not computable in polynomial time. Assume that Alice has *(F, T)* and public user Bob poses *F*. Let us assume that Alice and Bob use some symmetric cipher *H* and the hash function *f*. Bob receives encrypted by Alice document $H(p)=c$. Correspondents compute ''compressed'' message $f(c)=b$. Alice considers the equation $F(y)=b$. She uses her knowledge on *T* and reconstruct some reimage *r* of *b*. Finally Alice sends *r* to Bob. He is checking the relation $F(r\ )=b$. So Bob is sure that the decrypted by him document *p* was genuine and was sent by Alice. We believe in a future success of this direction of public key development. Incomplete list of publication with multivariate constructions, surveys and cryptanalytic studies is (Ding et al, 2021), (Ding at al., 2017), (Smith-Tone, 2022), (Smith-Tone, 2021), (Smith-Tone et al., 2019) , (Jayashree Dey et al., 2022), (Ikematsu et all, 2018), (Cartor et all, 2018), (Casanova et al., 2017), (Chen Jiahui et al..2020), (Chen Ming-Shing, et al., 2018), (Dung H. Duong et all, 2021).

In most examples of known pairs *(F, T)* the reimage of *F* can be computed in time $O(n^3)$. We refer to such *T* as a trapdoor accelerator.

2 On the bridge between Multivariate and Noncommutative Cryptographies

Another source of quadratic maps *F* with a trapdoor accelerators is Noncommutative Cryptography, which was created as attempt to generalise historical Diffie-Hellman protocol which uses cyclic group F^*_p for the elaboration of collision element. One can see that RSA cryptosystem uses cyclic subgroup of Z_{pq}, if we have some encryption public rule acting bijectively on the space of plaintext it is generating corresponding cyclic group. If the public rule is not bijective then it is generating of some monogenic semigroup of large order with some large index. We have to mention that usage of abelian groups or semigroups historically was started from Cesar's cipher which use'' belt'' cyclic group on the belly of the messenger. So Noncommutative Cryptography (NC) is an attempt to design of protocols via procedures described in terms of noncommutative groups, semigroups or other noncommutative algebraic objects. It has own history (see (Alexei G. Myasnikov et al. ,2011). It has very limited impact on NIST-2017 program because public keys are different from protocol based asymmetric algorithm. One of the direction of Noncommutative Cryptography has a close connection with Multivariate Cryptography. Multivariate rule on the affine space K^n where *K* is a finite commutative ring with unity is an endomorphism σ of $K[x_1, x_2, \ldots, x_n]$. It can be given by its values $\sigma(x_i)=f_i(x_1, x_2, \ldots, x_n)$, $i=1,2,\ldots,n$, polynomials f_i can be given by the lists of their monomial terms ordered lexicographically. This way of presentation of σ is known as its standard form. This form allows to define degree of σ as maximal degree of f_i , $i=1,2,\ldots,n$. All endomorphisms of $K[x_1, x_2, \ldots, x_n]$ form affine Cremona ${}^nCS(K)$.

It is an important object of Algebraic Geometry (see (Noether, 1904) about Mathematics of Luigi Cremona who was the prominent figure in Algebraic Geometry in the XIX century**,** **(**Yu. Bodnarchuk,. 2001) and further references on papers which use the term *affine Cremona group*). At first look $SC_n(K)$ is not convenient even for the implementation of Diffie-Hellman protocol with the nonlinear generator *g* in general position because $deg(g^n)= (deg (g))^n$.

Assumption that *g* is belong to some subsemigroup *S*, $S< {}^nSC(K)$ with the *Multiple Composition Property (MCP)*, i. e. the option to compute a composition of *n* elements in a polynomial time, brings the option to execute the protocol with *generator g.* Surprisingly in the case *of* $n>1$ variables such subsemigroups can be constructed.

One of the classes of subgroups is formed by *t*-stable subgroup, i.e subgroups such that maximal degree of its representative is the constant *t*, $t>1$ (see **(** Ustimenko et al., 2011), (Ustimenko, 2022)) **.** The first constructions of such subsemigroup with $\boldsymbol{t}=2$ were given in (Ustimenko, 2019, 2021**)***.* Assume that Alice and Bob use Diffie – Hellman protocol with generator of *2-stable monogenic* subsemigroup of ${}^nSC(K)$. Then the collision element *H* is the quadratic transformation**.** Alice can select the pair **(***F, T)* where $F \epsilon {}^nSC(K)$ and *T* is a trapdoor accelerator, and send the standard form of *F+H* to Bob. So he can use ***F*** as the encryption tool or the instrument for checking digital signatures. The security of this scheme is based on the protocol security**.** Diffie-Hellman ptotocol can be substitute for the protocol on Noncommutative Cryptography with the quadratic collision element from ${}^nSC(K)$ (see (Ustimenko , 2018). Additionally it can be used in the cases of other protocols for which can be constructed the deformation rule of the collision element *H* (or several collision elements) into quadratic transformation *d(H)* (see (Ustimenko, 2018) or the example in (Ustimenko,2023).

It is well known that Peter Shor suggested the use of quantum computer to solve Discrete logarithm problem in the case of F^*_p, where *p* is prime, in a polynomial time. Despite this fact the case of quadratic $g\epsilon {}^nCS(K)$ generating *t*-stable monogenic subsemigrop (or subsemigroup with MCP property) remains an interesting problem for cryptanalytics. The first implementation of this algorithms in the case when *g* generates 3-stable transformation of affine space K^n was considered in (Ustimenko et al., 2011), see (Ustimenko, 2022) for other examples.

3 Hidden tame homomorphism protocols on platforms of special multivariate transformations

3.1. Abstract scheme

The following abstract scheme can be used (see (Ustimenko, 2018). Assume that there are two families of subsemigroups $E_n(K)$ and $L_n(K)$ of ${}^nCS(K)$ $(E_n(K)>L_n(K))$ together with two families $E'_m(K)$ and $M_m(K)$ of subsemigroups ${}^mSC(K)$ $(E'_m(K)>M_m(K))$ such that $n>m$, $m=O(n)$ and there is a feasible homomorphism ψ from $L_n(K)$ into $M_m(K)$ (computable in time $O(n^k)$).

We assume that $E_n(K)$ and $E'_m(K)$ has rather large subgroups of invertible elements. Alice and Bob can execute the following protocol

Alice selects generators g_1 , g_2 ,…, g_d , $d\geq 2$ from $L_n(K)$ and the invertible elements *g* and *h* from $E_n(K)$ and $E'_m(K)$ respectively.

She computes images $h_1=\psi(g_1)$, $h_2=\psi(g_2)$,…, $h_d=\psi(g_d)$. After that Alice computes

$(a_i=gg_ig^{-1}, b_i=hh_ih^{-1}$), $i=1,2,\ldots,d$ and sends it to his partner Bob via open channel.

He take an alphabet $z_1, z_2,\ldots, z_d$ and writes the word $\mathbf{z_{i(1)}z_{i(2)}\ldots z_{i(l)}}$ of the length $l=O(1)$, $l>d$, $i(1), i(2),\ldots, i(l)$ are elements from $\{1,2,\ldots,d\}$**.** Bob computes the standard form $a=a_{i(1)}a_{i(2)}\ldots a_{i(l)}$ and sends it to Alice. He computes $b= b_{i(1)}b_{i(2)}\ldots b_{i(l)}$ and keeps it for himself.

Alice computes the collision element *b* accordingly to the following procedure.

1) She computes $g^{-1}ag ={}^1g$
2) she gets the standard form of $\psi({}^1g)={}^2g$
3) computes *b* as $h({}^2g)h^{-1}$.

The adversary has to decompose of *a* in its standard form into the word $w(a_1, a_2,\ldots, a_d)$ of given generators $a_1, a_2,\ldots, a_d$. If he/she solves this *NP*-hard problem then the adversary has the collision element as $w(b_1, b_2,\ldots, b_d)$.

3.2. The implementation with Eulerian transformation

Let *K* be a finite commutative ring with the multiplicative group K^* of regular elements of the ring. We take Cartesian power ${}^nE(K) =(K^*)^n$

and consider an Eulerian semigroup ${}^{n}ES(K)$ of transformations of kind

$$
\begin{aligned}
&x_1 \to \mu_1 x_1^{a(1,1)} x_2^{a(1,2)} \dots x_n^{a(1,n)},\\
&x_2 \to \mu_2 x_1^{a(2,1)} x_2^{a(2,2)} \dots x_n^{a(2,n)}, \quad (1)\\
&\dots\\
&x_m \to \mu_n x_1^{a(n,1)} x_2^{a(n,2)} \dots x_n^{a(n,n)}
\end{aligned}
$$

Let ${}^{n}EG(K)$ stand for Eulerian group of invertible transformations from ${}^{n}ES(K)$. They act as bijective maps on the variety $(K^*)^{n}$.

Let $J=\{1, 2,\dots,m\}$ we consider totality ${}^{m}P_n(K)$ of all transformation of kind

$$
\begin{aligned}
&x_1 \to \mu_1 x_1^{a(1,1)} x_2^{a(1,2)} \dots x_m^{a(1,m)}\\
&x_2 \to \mu_2 x_1^{a(2,1)} x_2^{a(2,2)} \dots x_m^{a(2,m)}\\
&\dots\\
&x_m \to \mu_m x_1^{a(m,1)} x_2^{a(m,2)} \dots x_m^{a(m,m)}\\
&x_{m+1} \to \mu_{m+1} x_1^{a(m+1,1)} x_2^{a(m+1,2)} \dots x_m^{a(m+1,m)} x_{m+1}^{a(m+1,m)} \dots x_n^{a(m+1,n)}\\
&x_{m+2} \to \mu_{m+2} x_1^{a(m+2,1)} x_2^{a(m+2,2)} \dots x_m^{a(m+2,m)} x_{m+1}^{a(m+2,m)} \dots x_n^{a(m+2,n)}\\
&\dots\dots\\
&x_n \to \mu_n x_1^{a(n,1)} x_2^{a(n,2)} \dots x_m^{a(n,m)} x_{m+1}^{a(n,m+1)} \dots x_n^{a(n,n)}
\end{aligned}
$$

Let ψ: ${}^{m}P_n(K)\to{}^{m}ES(K)$ be the homomorphism sending σ from ${}^{m}P_n(K)$ into its restriction onto $K[x_1, x_2,\dots, x_m]$.

We can use described above protocol in the case of $E_n(K)={}^{n}ES(K)$, $L_n(K)={}^{m}P_n(K)$ and $E'_m(K)=M_m(K)={}^{m}ES(K)$.

Alice and Bob conduct the protocol and elaborate the collision element $\boldsymbol{C}$ from the $\boldsymbol{{}^{m}ES(K)}$.

3.3. On protocol based cryptosystem formed by combination of Eulerian and linear transformations

Examples of cryptosystems based on this protocol are described in (Ustimenko, 2023). We add the following cryptosystems constructed in the case of $K=Z_q, q=2^s, s>1$.

Alice and Bob execute 2t, $t=O(1)$, $t\geq 2$ sessions of the protocol and elaborate elements ${}^{i}C$ of kind

$$
\begin{aligned}
&x_1 \to {}^{i}\mu_1 x_1^{a(1,1,i)} x_2^{a(1,2,i)} \dots x_m^{a(1,m,i)}\\
&x_2 \to {}^{i}\mu_2 x_1^{a(2,1,i)} x_2^{a(2,2,i)} \dots x_m^{a(2,m,i)}\\
&\dots\\
&x_m \to {}^{i}\mu_m x_1^{a(m,1,i)} x_2^{a(m,2,i)} \dots x_m^{a(m,m,i)}
\end{aligned}
$$

where $i=1,2,\dots, 2t$, $a(j,k, i)$ are elements from Z_d, $d=2^{s-1}$.

Noteworthy that regular elements of Z_q are odd residues modulo q.

Notice that matrix $B=(b(i,j))$ moves tuple $(x_1, x_2,\dots, x_m)\epsilon(Z^*_q)^m$ into $(y_1, y_2, \dots, y_m)= (x_1, x_2,\dots, x_m)B\epsilon(Z^*_q)^m$ if and only if each columns of B has odd regular components.

Let $D(m, q)$ be a totality of invertible matrices as above acting on $(Z^*_q)^m$.

Alice and Bob form matrices ${}^{k}B=({}^{k}b(i,j))$ with entries ${}^{k}b(i,j)=({}^{k}\mu_i{}^{k}\mu_j)^{a(i,j,k)}$, $k=1,2,\dots,t$.

Alice selects matrices ${}^{i}D$, $i=1,2,\dots, t$ from $D(m, q)$ with nonzero entries. Additionally she takes

Jordan-Gauss elements ${}^{i}J_1$, ${}^{i}J_2 ,\dots,{}^{i}J_{s(i)}$, $i=1, 2,\dots, t$, $s(i)\geq 2$, $t>1$ and forms their compositions

${}^{i}G\epsilon{}^{m}EG(Z_q)$. She sends ${}^{i}G(x_j)\,{}^{i+t}C(x_j)$, $i=1,2, \dots, t$, $j=1, 2,\dots,m$ to Bob together with matrices ${}^{k}B+{}^{k}D$, $k=1,2,\dots, t$. Bob restores linear transformations ${}^{i}L$ given by matrices ${}^{i}D$ and Eulerian transformations ${}^{i}G$.

Correspondents work with alphabets $z_1, z_2,\dots, z_t$ and $y_1, y_2, \dots, y_t$.

They agree via open channel on the word $z_{i(1)}y$ $z_{i(2)}z_{i(2)}y_{j(2)} \dots z_{i(k-1)2)}y_{j(k-1)}z_{j(k)}, k >t$

where $i(r)$ and $j(r)$ are elements of $\{1,2, \dots, t\}$.

Alice and Bob specialise z_i as ${}^{i}G$, $i=1,2,\dots,k$ and $\boldsymbol{y_i}$ as ${}^{i}L$, $i=1,2,\dots,k-1$.

To get digital signature of the document from his partner Bob computes the hash value $h\epsilon(Z^*_q)^m$ of the document. To check the signatures x obtained from Alice he will use the result of consecutive application of elements ${}^{1}G$, ${}^{1}L$, ${}^{2}G$, ${}^{2}L,\dots$, ${}^{k-1}G$, ${}^{k-1}L$, ${}^{k}G$ to x. He compares the resulting value $\boldsymbol{c(x)}$ with h.

Alice uses the knowledge on the decomposition of ${}^{i}G$ into Jordan-Gauss elements and transformations ${}^{i}D^{-1}$ for the computation of her signature x.

REMARK 1. *Let E be the composition of ${}^{1}G$, ${}^{1}L$, ${}^{2}G$, ${}^{2}L,\dots$, ${}^{k-1}G$, ${}^{k-1}L$, ${}^{k}G$ in the affine Cremona semigroup. It is clear that E has linear degree d(m) in variable m and an exponential density. So the computation of the standard form of E takes exponential time.*

It means that adversarial attacks on this cryptosystem via the interception of hashes of documents and corresponding signatures are unfeasible.

REMARK 2. *Bob checks the signature in time $O(m^2)$.*

We consider some computational relations between Z_2^{s-1} , $Z^*{}_2^s$ and $\mathbf{F_2^{s-1}}$.

Recall that $Z^*{}_2^s$ is the totality of odd residues modulo 2^s.

We consider the map σ from Z_2^{s-1} to $Z^*{}_2^s$ such that $\sigma(t \bmod 2^{s-1})$ is $2t+1 \bmod 2^s$. It is a bijection. Let σ^{-1} be the inverse map from $Z^*{}_2^s$ to Z_2^{s-1}.

Notice that elements from Z_2^{s-1}can be written as $b=e_0+e_1 2+e_2 2^2 +\dots+e_{s-2}2^{s-2} \bmod 2^{s-1}$, where $e_i \epsilon \{0,1\}$. Element of the finite field F_q, $q=2^{s-1}$ can be written as $g(x)=e_0+e_1x+e_2x^2+\dots+e_{s-2}x^{s-2} \bmod p(x)$ where $p(x)$ is the irreducible polynomial of degree s-1. Let π be the map such that $\pi(b)=g(x)$ and π^{-1} is the inverse map from F_q, $q=2^{s-1}$ onto Z_2^{s-1}.

Let us consider several modifications of the algorithm M1-M4.

We consider transformation S^{-1} sending $(x_1, x_2,\dots, x_m) \epsilon (Z^*{}_2^s)^m$ to $(\sigma^{-1}(x_1), \sigma^{-1}(x_2),\dots, \sigma^{-1} (x_m))$ from $(Z\__2^{s-1})^m$ and inverse bijection S. Let P be the map sending element $(x_1, x_2, \dots, x_n)$ from $(Z_2^{s-1})^m$ to $(x_1, x_2, \dots, x_m) \epsilon (F_2^{s-1})^m$.

M1.

We can simplify the algorithm computationally to define ${}^rA$ as matrix with entries $(\sigma(a(i,j, r))$.

So Alice sends ${}^rA+{}^rD$ to Bob instead ${}^rB+{}^rD$ in the modified algorithm.

M2. ${}^rD$, $r=1, 2, \dots, t$ can be taken from $GL_m(Z_2^{s-1})$. These transformations will be delivered from Alice via sending ${}^rA+{}^rD$. We identify ${}^rD$ with the corresponding linear transformations. Bob forms transformations $S^{-1}\, {}^rD\, {}^rS = {}^rL'$ which are bijective transformations of $(Z^*{}_2^s)^m$. He uses the composition E' of ${}^1G$, ${}^1L'$, ${}^2G$, ${}^2L',\dots$, ${}^{k-1}G$, ${}^{k-1}L'$, ${}^kG$ computed via consecutive computations of Eulerian maps and transformations ${}^iL'$.

M3. ${}^rD$, $r=1, 2, \dots, t$ can be taken from $GL_m(F_2^{s-1})$. Alice changes ${}^rD=({}^rd(i,j))$ *for* ${}^rD'=(\pi^{-1} ({}^rd(i,j)))$ and sends ${}^rD'+{}^rA$ to Bob. He restores ${}^rD$. Bob uses transformations ${}^rH= S^{-1} P ({}^rD) P^{-1} S$ of the variety $(Z^*{}_2^s)^m$. He uses the composition E' of ${}^1G$, ${}^1H$, ${}^2G$, ${}^2H,\dots$, ${}^{k-1}G$, ${}^{k-1}H$, ${}^kG$ computed via consecutive computations of Eulerian maps and transformations ${}^iH$.

M4. We can use cryptosystems M2 and M3 in combinations. Alice delivers ${}^rD$, $r=1, 2, \dots, t, t+1, t+2,\dots, t+t'$ selected in the group $GL_m(Z_2^{s-1})$. She forms $S^{-1}\, {}^rD^r\, S = {}^rL'$, $r=1, 2,\dots,$ t as in the cryptosystem M2 and forms ${}^rH= S^{-1} P ({}^{r+t}D) P^{-1} S$, $r=1, 2,\dots, t'$ as in M3.

Bob uses the composition E' of ${}^1G$, ${}^1Y$, ${}^2G$, ${}^2Y,\dots$, ${}^{k-1}G$, ${}^{k-1}Y$, ${}^kG$ where ${}^iY \epsilon \{ {}^rD, r=1, 2, \dots, t, {}^lH, l=1,2,\dots, t'\}$. He sends pairs $(j, i(j))$ such that ${}^jY={}^{i(j)}D$ and pairs $(j, k(j))$ such that ${}^jY={}^{k(j)}H$ *to* Alice. This information allows her to compute the signature.

3.4. On protocol On combinations of Eulerian transformations and the maps of symmetric encryption.

Let us consider the symmetric cipher working with the space of plaintexts $(F_q)^m$, $q=2^s$-1 or $(Z_q)^m$. Assume that E_P be the bijective encryption map depending on password Q (the information file).

So description of algorithm is available. We may assume that some part p' of Q can be available publicly.

Alice can deliver the remaining part p'' of P presented in the form of tuple $(p_1, p_2, \dots,p_d)$, $p_i \epsilon Z_q$ (or F_q) on the base of the presented above protocol.

So instead of several elements ${}^iY$ of the scheme **M4** the encryption procedure E_Q can be used with different passwords. Alice and Bob can use several $(O(1))$ symmetric ciphers for the modification of the selected protocol based algorithm.

EXAMPLE 1.

Let us consider described above private key of Imai-Matsumoto scheme. It consist of affine transformation L_1: $x \rightarrow xA+b$, $b=(b_1, b_2, \dots, b_m)$, L_2:$x \rightarrow xC+d$, $d=(d_1, d_2,\dots, d_m)$ and the map η: $x \rightarrow x^t$, $t=q^a+1$ where $x \epsilon F_q$ and $(q^a, q^m$-$1)=1$.

Let us present element a, $a<m$ as $a_1+a_2+\dots+a_m=a$ where $0 \le a_i<q$ and + is the addition in Z.

Alice and Bob can make two sessions of the protocol and elaborate vectors $({}^iM_1, {}^iM_2, \dots, {}^iM_1) = {}^im$, $i=1,2$ and matrices ${}^1A$ and ${}^2A$. Alice computes $S^{-1}({}^1m)$ and sends $(a_1, a_2,\dots, a_m)+(n_1, n_2,\dots, n_m)$ where + is the operation of Z_q to Bob. He restores parameter t.

Alice sends ${}^1A+(\pi^{-1}(a(i, j))$ and ${}^2A+(\pi^{-1}(c(i, j))$ to Bob. So he restores matrices A and C. Alice sends $(\pi^{-1}(b_1), \pi^{-1}(b_2),\dots, \pi^{-1}(b_m))+S^{-1}({}^2m)$ to Bob. So he gets vector (b). Alice and Bob construct d simply as $(a(1,1), a(2, 2),\dots, a(m,m))$. So finally they share the private key of Imai-Matsumoto encryption.

Correspondents make extra two sessions of the protocol for the delivery of ^1G and ^2G from Alice to Bob as in previous algorithms.

So Bob uses the composition E of $G_1\ S\ P\ L_1\eta L_2P^{-1}S^{-1}G_2$. Recall that the computation of η uses the identification of the vector space $(F_2{}^{s-1})^m$ with finite field $F_2{}^{(s-1)m}$.

Bob computes the hash value $h\epsilon(Z^*{}_q)^m$ of the document. To check the signatures x obtained from Alice he will use the result of consecutive application of elements ^1G, ^1L, G_1, S, P , L_1, η, L_2, P^{-1}, S^{-1}, G_2 to $\boldsymbol{x}$. He compares the resulting value $c(x)$ with h.

Alice uses the knowledge on the decomposition of ^iG, $i=1,2$ into Jordan-Gauss elements for the computation of her signature $\boldsymbol{x}$.

REMARK 1. *The complexity of conducting protocols for Bob is $O(m^3)$.Bob can check the signature intime $O(m^2)$.*

DIGITAL SIGNATURE SCHEME 1.

Let us consider the map F from $(F_q)^m$ onto $(F_q)^n$ given by the multivariate rule F: $(x_1, x_2, \ldots x_m)\rightarrow(y_1, y_2, \ldots, y_n)$ where $y_1=f_1(x_1, x_2, \ldots, x_m)$, $y_2=f_2(x_1, x_2, .., x_m), \ldots$, $y_n=f_n(x_1, x_2, \ldots, x_m)$. Let us assume that polynomials f_i are given in their standard forms, i. e. lists of monomial terms ordered lexicographically and $n=O(m)$. Let T be a trapdoor accelerator of F which is a piece of information such that the knowledge of T allows to compute the reimage of F in time $O(m^3)$.

Let L_1 be the affine transformation of $(F_q)^m$ given by the matrix A and vector b. L_2 stands for the affine transformation of $(F_q)^n$ given by the matrix C and vector d. We refer to $G= L_1FL_2$ as affine deformation of F. The map G has trapdoor accelerator (L_1, L_2, T).

If $q=2^{s-1}$ then Alice can use quadratic F (or G) for the following scheme of digital signature.

Correspondents conduct $\boldsymbol{n}$ sessions of the protocol with the collision map from $^mES(Z_q)$, $q=2^s$. So they get matrices ^rA, $r=1, 2, \ldots, n$ with the entries from $Z_{q'}$, $q'=2^{s-1}$ and vectors $^ru=(^r\mu_1, {}^r\mu_2, \ldots, , {}^r\mu_m)$. Additionally Alice and Bob conduct two protocols with the collision maps from $^mES(Z_q)$ and $^nES(Z_q)$ to get representatives of this semigroup ^1G and ^2G.

Alice creates a transformation H in the form $x_r\rightarrow\sum_{i\leq j} a(i,j, r)x_ix_j+ \sigma^{-1}(^r\mu_1)_{X1+} \sigma^{-1}(^r\mu_2)_{X2} + \ldots + \sigma^{-1}(^r\mu_m)^r{}_{Xm}+a(2, 1, r)=h_r(x_1, x_2, \ldots, x_m)$, $r=1, 2, \ldots n$. She writes F in the form $x_r\rightarrow\sum_{i\leq j} b(i, j, r)x_ix_j+ {}^rb_{1X1}+ {}^rb_{2X2} + \ldots + {}^rb_{mXm}+{}^rb_0 =f_r(x_1, x_2, \ldots, x_m)$, $r=1, 2, \ldots n$.

Alice considers
$F' = x_r\rightarrow\sum_{i\leq j} \pi^{-1}(b(i, j, r)x_ix_j + \pi^{-1}({}^rb_1)_{X1}+ \pi^{-1}({}^rb_2)_{X2} + \ldots + \pi^{-1}({}^rb_m)_{Xm}+ \pi^{-1}({}^rb_0) =f'_r(x_1, x_2, \ldots, x_m)$, $r=1, 2, \ldots, n$.

She computes $h_r(x_1, x_2, \ldots, x_m)+ f'_r(x_1, x_2, \ldots, x_m)$, $r=1, 2, \ldots, n$ and sends these polynomials to Bob. He restores the map F.

To check the signatures Bob uses the composition E of the maps ^1G, $(S_m)^{-1}$, P_m , F, $(P_n)^{-1}$, S_n, ^2G. He takes the hash value of the document in the form $(h_1, h_2, \ldots, h_n)=h$ written in the alphabet $Z^*{}_q$. Let u be a signature obtained from Alice. Bob checks the equality $E(u)=h$ via the consecutive application of transformations ^1G, $(S_m)^{-1}$, P_m , F, $(P_n)^{-1}$, S_n, ^2G. The knowledge of Alice on the trapdoor accelerator and the decompositions of Eulerian transformations into Jordan-Gauss maps allows her to construct the signature.

REMARK 2. *Practically hash function is convenient to compute in the form of vector* ***over*** *$F_{q'}$ and use $E' =(P_m)^{-1}(S_m)^{-1}E(S_n)^{-1}P_n$ instead of E. Noteworthy that E' is a Boolean map and h is a Boolean tuple.*

EXAMPLE 2.

Let us discussed the above scheme implementation in the case of the trapdoor accelerator of the quadratic map from the Oil and Vinegar algorithm.

It is commonly admitted that Multivariate cryptography turned out to be more successful historically 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

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

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

$$\ldots$$

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

where ${}^{k}p_{i,j}$, ${}^{k}p_{i}$ 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 $x_i \to {}^{i}p$ of formal Cremona group, where ${}^{i}p$ 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 $z_1, z_2, \dots, z_r$ and z'_1 , $z'_2, \dots, z_{n-r}$ such that the substitution $x_1=z_1$, $x_2=z_2,\dots$, $x_r=z_r$, $x_{r+1}=z'_1$, $x_{r+2}=z'_2,\dots$, $x_n=z'_{n-r}$ converts every single element ${}^{i}p$ 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, γ_{ijk}, λ_{ijk}, ς_{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 for cryptographic purposes, 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. We assume that parameter n can be selected in a free way and parameters n and m are connected via linear equation $\alpha n+\beta m+b$ where $\alpha\neq 0,\beta\neq 0$. So $m=0(n)$. We take integer k which ≥ $max(n, m)$, $k=O(n)$ and commutative ring $K[x_1,x_2,\dots,x_n, x_{n+1}, x_{n+2},\dots, x_k]$ where x_i, $i=1,2,\dots,n$ are variables of public equations ${}^{j}p(x_1,x_2 , . . . , x_n)$, $j=1,2, \dots,m$ and $x_{n+1}, x_{n+2},\dots,x_k$ are formal variables.

To summarise we say that in the case of the field $F_{q'}$ of characteristic 2 the map
with the corresponding trapdoor accelerator can be used as the pair (F, T) in the described above scheme of the protocol based cryptosystem.

DIGITAL SIGNATURE SCHEME 2.

We can substitute field $\boldsymbol{F_q}$, $q=2^{s-1}$ for arithmetical ring Z_q in the described above digital signatures scheme. So F will be the map from $(Z_q)^m$ onto $(Z_q)^n$ with the trapdoor accelerator. In that case we do not need to use π.Alice simply add H to F and Bob restores the standard form of F.

4. Conclusions.

We described the general schemes of digital signatures based on protocols on Noncommutative Cryptography implemented on the Platform of Eulerian transformations defined over arithmetical rings Z_q, $q=2^n$.

Let K be a finite commutative ring. Eulerian transformations are elements of semigroup of endomorphisms of $K[x_1, x_2,\dots,x_n]$ moving variable x_i to a monomial term. In (Ustimenko, 2024) these protocol is used for the secure delivery of quadratic transformation of affine space K^n from the protocol user to his/her partner. The security of protocol lays on the complexity of the word decomposition problem in the semigroup of Eulerian transformations. Its execution time is $O(n^3)$.

Users of the protocol share the standard form of quadratic transformation with a trapdoor accelerator which can be used as instrument of digital signatures on ‘’private mode’’. The cost of secure delivery is $O(n^4)$. The number of signed documents is restricted. So users have to conduct protocols periodically.

We discover that in the case of $K=Z_q$, $q=2^s$ there is an option to use one time delivery of quadratic transformation scheme for the establishment constant line for the digital signature procedure.

In this case there is an effective way to established one to one correspondence $\boldsymbol{\sigma}$ between set Z^*_q of elements of multiplicative group of Z_q and set $Z_{q'}$, $q'=2^{s-1}$. Additionally we can use effectively computable one to one correspondence $\boldsymbol{\pi}$ between $Z_{q'}$ and the finite field $F_{q'.}$ So we can identify sets $Z^*_{q,}$ $Z_{q'}$ with $F_{q'.}$

Noteworthy that the protocol allows secure delivery of element from Eulerian semigroup in time $O(n^3)$. If $K=Z_q$, $q=2^s$ we can modify this procedure for transportation of element from $AGL_n(F_{q'})$ or $AGL(Z_{q'})$ or corresponding semigroups of affine transformations.

So Alise can generate products ${}^1G$ and ${}^2G$ of several Jordan-Gauss transformations and deliver them to Bob together with transformation $H_1 \epsilon {}^nCS(F_{q'})$ and $H_2 \epsilon {}^nCS(F_{q'})$ of degree one.

So correspondents can use $E_1={}^1G\ H_1\ {}^2G$, $E_2={}^1G\ H_2\ {}^2G$ or even one of transformations $E_3=\ {}^1G\ H_1\ {}^2G\ H_2\ {}^1G$, $E_3=\ {}^1G\ H_2\ {}^2G\ H_1\ {}^1G$. The knowledge of decompositions of ${}^1G$ and ${}^2G$ allows Alice to compute the reimage $\boldsymbol{x}$ of one of the maps E_i in time $O(n^2)$.

Bob can verify the signature $\boldsymbol{x}$ from Alice in time $O(n^2)$ because of his knowledge on ${}^iG$ and H_i.

Recall that the protocol costs $O(n^3)$. So signing of $O(n^d)$, $d\geq 1$ documents costs $O(n^{d+2})$.

Noteworthy that degree of each E_i is a linear function in variable n and the density (number of monomial terms is exponential. So the adversary is not able to restore these standard forms and we get a protocol based cryptosystem with the reference on word decomposition problem
in the semigroup of Eulerian transformations.

Finally we suggest to use historical quadratic cryptosystems defined over the finite field F_i of characteristic 2 with their trapdoor accelerators instead of H_1 and historical quadratic polynomial stable maps of Noncommutative
Cryptography with trapdoor accelerator defined over arithmetical ring $Z_{q'}$ instead of H_2. In the case of such obfuscation the cost of the protocol based transportations of maps costs The cost of single signature is $O(n^3)$. So signing of $O(n^d)$, $d\geq 1$ documents costs $O(n^{d+3})$. This idea is illustrated via the case of Unbalanced Oil and Vinegar cryptosystem.

Alice can deliver F_i together with its trapdoor accelerator which allows to compute reimages in time $O(n^2)$. Then the complexity of digital signature procedure to sigh $O(n^d)$ documents $d\geq 2$ will be $O(n^{d+2})$.

This idea is illustrated via the case of historical Imai-Matsumoto cryptosystem.

Several cryptosystems have hidden multivariate nature. We use injective maps from Z_2^{s-1} to Z_2^s and F_2^{s-1} to Z_2^s which are not homomorphic embeddings. Their images coincide with the multiplicative group $Z^*{}_2^s$.

Boolean functions used in these cryptosystems are defined in the Calculus of Predicates via three binary operations operations. One of them is multiplication of Z_2^s and remaining two are addition and multiplication of Z_2^{s-1} or F_2^{s-1}. That is why cryptanalysis of defined Boolean maps can not be created in terms of Multivariate Cryptography. It requires new ideas.

Boolean functions in two examples are constructed as modification of classical Imai - Matsumoto and Unbalanced Oil and Vinegar cryptosystems.

References

Anne Canteaut, François-Xavier Standaert (Eds.). 1921. *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.

Ward Beullens. 2021. I*mproved Cryptanalysis of UOV and Rainbow*, In Eurocrypt 2021, Part 1: 348-373.

Matsumoto Tsutomu and Imai Hideki. 1988. *Public quadratic polynomial-tuples for efficient signature verification and message encryption.* In Proceedings of the Workshop on the Theory and Application of of Cryptographic Techniques. Springer, 419–453.

Ding, J., Petzoldt, A., Schmidt, D.S. 2020. *The Matsumoto-Imai Cryptosystem.* In: Multivariate Public Key Cryptosystems. Advances in Information Security, vol 80. Springer, New York, NY.

Jintai Ding. 2004. *New Variant of the Matsumoto-Imai Cryptosystem through Perturbation,* PKC 2004, Singapure.

Jintai Ding, Joshua Deaton, Vishakha, and Bo-Yin Yang. 2021. *The Nested Subset Differential Attack,A Practical Direct Attack Against LUOV Which Forges Signature Within 210 Minutes,* In Eurocrypt 2021, Part 1, pp. 329-347.

L. Goubin, J. Patarin, Bo-Yin Yang., 2011. *Multivariate Cryptography, Encyclopedia of Cryptog-raphy and Security, (2nd Ed.),* 824-828.

N. Koblitz. 1998. *Algebraic aspects of cryptography*, Springer ,206p.

Ikematsu, Y. , Perlner, R. , Smith-Tone, D. , Takagi, T. and Vates, J. 2018. HFERP -- A New Multivariate Encryption Scheme, PQCrypto 2018: The Ninth International Conference on Post-Quantum Cryptography, Fort Lauderdale, FL, US, [online].

Ding and A. Petzoldt,. 2017. *Current State of* Multivariate Cryptography, in IEEE Security & Privacy, vol. 15, no. 4, pp. 28-36.

Daniel Smith-Tone and Cristina Tone. 2019. A Nonlinear Multivariate Cryptosystem Based on a Random Linear Code, IACR e-print archive 2019/1355.

Jayashree, Dey, Ratna Dutta, 2022. *Progress in Multivariate Cryptography: Systematic Review, Challenges, and Research Directions*, ACM Computing Survey, volume 55, issue 12,No.246, pp 1-34.

Casanova Antoine, Faugère Jean-Charles, Macario-Rat Gilles, Patarin Jacques, Perret Ludovic, and Ryckeghem Jocelyn. 2017. Gemss: *A great multivariate short signature.* Submission to NIST (2017).y. Springer, Singapore, 209–229.

Chen Ming-Shing, Hülsing Andreas, Rijneveld Joost, Samardjiska Simona, and Schwabe Peter. 2018. *SOFIA: MQ-based signatures in the QROM*. In Proceedings of the IACR International Workshop on Public Key Cryptography. Springer, 3–33.

Chen Jiahui, Ning Jianting, Ling Jie, Lau Terry Shue Chien, and Wang Yacheng. 2020. *A new encryption scheme for multivariate quadratic systems. Theoretical Computer Sci-ence* 809, 372–383.

Cartor Ryann and Smith-Tone Daniel. 2018. EFLASH: *A new multivariate encryption scheme.* In Proceedings of the International Conference on Selected Areas in Cryptog-raphy. Springer, 281–299.

M. Noether, Luigi Cremona, Mathematische Annalen, 59 (1904), pp. 1-19.

Yu. Bodnarchuk. 2001 Every regular automorphism of the affine Cremona group is inner, Journal of Pure and Applied Algebra 157, 115-119.

V. Ustimenko, A. Wroblewska. 2011. *On the key exchange with nonlinear polynomial maps of stable degree,* Annalles UMCS Informatica AI XI, 2 (2011), 81-93.

V.Ustimenko. 2019. *On desynchronised multivariate algorithms of El Gamal type for stable semigroups of affine Cremona group*, Theoretical And Applied Cybersecurity, Vol. 1 No. 1.

V. Ustimenko, 2021. *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 pp. 123-130

V. Ustimenko. 2023. *On Eulerian semigroups of multivariate transformations and their cryptographic applications*. European Journal of Mathematics 9, 93.

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

V. Ustimenko 2024. *On short digital signatures with Eulerian transformations*. IACR e-print archive 2024/001.

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

Dung H. Duong, Ha T. N. Tran, Willy Susilo, and Le Van Luyen. 2021. *An efficient multi-ariate threshold ring signature scheme.* Computer Standards & Interfaces 74.

Smith-Tone, D. 2022. *2F - A New Method for Constructing Efficient Multivariate Encryption Schemes, Proceedings of PQCrypto 2022*:

The Thirteenth International Conference on Post-Quantum Cryptography, virtual, DC, US.

Daniel Smith Tone. 2021. New Practical Multivariate Signatures from a Nonlinear Modifier, IACR e-print archive,2021/419.

V. Ustimenko. 2022. Graphs in terms of Algebraic *Geometry, symbolic computations and secure communications in Post-Quantum world* UMCS Editorial House, Lublin, 2022, 198