On effective computations in special subsemigroups of polynomial transformations and protocol based multivariate cryptosystems.

Vasyl Ustimenko

University of Maria Curie-0klodowska (Lublin20036, Poland, pl Marii –Curie Sklodowskiej 1), Institute of Telecommunications and Global Information Space (Kyiv 02000, Ukraine, Chokolivs'kyi Blvd, 13)

Abstract. Large semigroups and groups of transformations of finite affine space of dimension *n* with the option of computability of the composition of *n* arbitrarily chosen elements in polynomial time are described in the paper. Constructions of such families are given together with effectively computed homomorphisms between members of the family. These algebraic platforms allow us to define protocols for several generators of subsemigroup of affine Cremona semigroups with several outputs. Security of these protocols rests on the complexity of the word decomposition problem, It allows to introduce algebraic protocols expanded to cryptosystems of El Gamal type which are not a public key system. In particular symbiotic combination of these protocol of Noncommutative cryptography with one time pad encryption is given. Some of these nonclassical multivariate cryptosystems are implemented with platforms of cubical transformations.

Key words: Post Quantum Crypography, Computer Algebra, multiple composition property, subgroups of affine Cremona group, computationally tame homomorphism, key exchange protocols.

1. Introduction.

Algebraic system on $K[x_1, x_2, \dots, x_n]$, where K is a commutative ring with operations of addition, multiplication and composition is the core part of Computer Algebra. Let $deg(f)$ be the degree of polynomial $f\epsilon\ K[x_1, x_2, \dots, x_n]$, then $deg\ (f)+deg(g)=max(deg(f), deg(g))$. The general formula for deg $(f(g))$ does not exist, only inequality $deg(f(g))\leq deg(f)deg(g)$ holds. The addition and multiplication of n polynomials from $K[x_1, x_2, \dots, x_n]$ of bounded degree can be computed in polynomial time but there is no polynomial algorithm for the execution of the computation of n elements from $K[x_1, x_2, \dots, x_n]$. It means that in Cremona semigroup $CS_n(K)$ (see [13]) of all endomorphisms of $K[x_1, x_2, \dots, x_n]$ the computation of the product of n representatives is unfeasible task. Noteworthy that each endomorphism $F\ \epsilon CS_n(K)$ is defined by its values f_i on x_i and can be identified with the rule $x_i \rightarrow f_i(x_1, x_2, \dots, x_n)$, $i=1,2,\dots,n,$ where f_i is given via the list of its monomial terms written in the lexicographical order.

Noteworthy that the semigroup $CS_n(K)$ and its subgroup $CG_n(K)$ of all automorphisms of $K[x_1, x_2, \ldots, x_n]$ are core objects of Multivariate Cryptography (MC). ,Classical Multivariate Cryptography considers only compositions of kind T_1FT_2 of single nonlinear element F of small degree (2 or 3) with linear bijective endomorphisms T_1 and T_2 of degree 1 because of the heavy complexity for the computation of compositions.

In 2017 the international tender of the National Institute of Standartisation Technology (NIST) of the USA for the selection of public key based on postquantum algorithms was announced. It has been considering algorithms for the encryption task and for the procedure of digital signature.

The last third round of this competition started in summer time of 2020. Only one candidate from the multivariare cryptography area remains. This is a special case of ‘’Rainbow like unbalanced oil and vinegar’’ digital scheme.The final list does not contain MC algorithms for encryption task.

This outcome stimulates alternative research on Mulivariate cryptography such as asymmetric algorithms which are not public keys, the usage of multivariate maps of unbounded degree and the usage of composition on nonlinear maps. Our paper is dedicated to some results on the mentioned above three directions.

2. Main results.

We are interested in constructions of special families of subsemigroups $S_n(K)<CS_n(K)$ over chosen commutative ring K such that computation of n general representatives of $S_n(K)$ takes $O(n^d)$ elementary ring operations for some positive parameter d. We refer to such sequence of $S_n(K)$ as family of semigroup with multiple polynomial computability (MPC-property). In the family $S_n(K)$ with the MPC property we can compute the composition of $O(n^t)$ general represantatives for each t,, $t>0$ in polynomial time.

Example of such family is subsemigroups $ES_n(F_q)$ all endomorphisms of $F_q[x_1, x_2, \ldots, x_n]$ defined over finite field F_q of kind $x_i \rightarrow (a_i)x_1^{a(i,1)} x_2^{a(i,2)}, \ldots x_n^{a(i,n)}$, $i=1,2,\ldots,n$. MPC property in this case follows from the fact that $(x)^q=x$ which implies $0 \leq a(i,j) \leq q-1$, a

THEOREM 1. *For each pair (n, d), $n \geq 2$, $d \geq 2$ and each commutative ring K* there is a subsemigroup ${}^dG(n,K)$ of affine Cremona semigroup $CS_n(K)$ such that maximal degree of its representatives is d.

THEOREM 2. *For each d, $d \geq 2$ there is a family of subsemigroups ${}^dG(n,K)$ satisfying to conditions of theorem 1 such that for each $n< a<2n$ there is a homomorphism ή of ${}^dG(n+a, K)$* onto ${}^dG(n,K)$ *for which the value ή(g) is computable in polynomial time in variable n.*

We refer to $\acute{\eta}$ from the theorem 2 as computationally tame homomorphism. Explicit constructions of semigroups ${}^{d}G(n,K)$ satisfying conditions of theorems 1 and 2 with large subgroups ${}^{d}G'(n,K)$ of all invertible elements are presented in [16], [17]. These families of subgroups allow to generate representative $g\epsilon\, {}^{d}G'(n,K)$ and inverse g^{-1} in polynomial time in variable n.

These results allow us to use modern technique of NONCOMMUTATIVE CRYPTOGRAPHY with platforms defined in terms of Multivariate Cryptography (see [1]-[12]).

The following abstract protocol of multivariate cryptography for the case t=1 was considered in [14].

PROTOCOL.

Let $G(n, d)$ be a family of subgroups satisfying condition of the theorem 2 for the chosen parameter d. Alice selects parameters a, $a\geq 2$ and k, together with two invertible linear transformations $T_1\epsilon AGL_{n+a}(K)$ and $T_2\epsilon AGL_{n+a}(K)$ of affine spaces K^{n+a} and K^n. She chooses element $g\epsilon G(n+a, K)$, $h\epsilon G(n, K)$ and selects elements $g_1, g_2, \ldots, g_k$ from $G(n+a, K)$ such that $g_i g_j \neq g_j g_i$. Alice uses homomorphism $\acute{\eta}$ of the heorem 2 and computes $h_i=\acute{\eta}(g_i)$, $i=1,2,\ldots, k$.

Finally Alice forms pairs (a_i, b_i), $i=1,2,\ldots,k$ *where* $a_i=T_1 g g_i g^{-1}(T_1)^{-1}$ and $b_i=T_2 h h_i g^{-1}(T_2)^{-1}$ and sends these pairs to Bob.

In his turn Bob selects t words in the alphabet $X=\{x(1), x(2),.., x(k)\}\}$ of kind $w_j=x(i_{1,j})^{r(j,1)}\, x(i_{2,j})^{r(j,2)} \ldots x(i_{k(j),j})^{r(j,k(j))}.\ j=1,2,\ldots,t$ where $i_{s,j}\neq i_{s+1,j.}$, $1\leq i_{s,j}\leq t.$

He substitutes $b(i_{s,j})$ from $\{b_1, b_2, \ldots, b_k\}$ instead of $x(i_{s,j})$ and keeps

$u_j=b(i_{1,j})^{r(j,1)}\, b(i_{2,j})^{r(j,2)} \ldots b(i_{k(j),j})^{r(j,k(j))}.\ j=1,2,\ldots,t$ in his private safe storage.

Bob substitutes $a(i_{s,j})$ from $\{a_1, a_2, \ldots, a_k\}$ instead of $x(i_{s,j})$ and keeps

$z_j=a(i_{1,j})^{r(j,1)}\, a(i_{2,j})^{r(j,2)} \ldots a(i_{k(j),j})^{r(j,k(j))}.\ j=1,2,\ldots,t$ and sends them to Alice.

She works with $z_{j,}.j=1,2,\ldots,t$ in their standard form and restores collision maps

$u_{j,}.j=1,2,\ldots,t$ because of her knowledge on the input data of algorithm.

SECURITY ASPECTS FOR THE PROTOCOL.

To get collision elements adversary has to decompose elements $u_{j,}$ into the composition of generators $b_1, b_2, \ldots, b_k$, i. e to solve WORD DECOMPOSITION

PROBLEM in a subsemegroup of affine Cremona semigroup. This is untractable problem for algorithm with the usage of ordinary and quantum computers.

PROTOCOL BASED CRYPTOSYSTEM.

Alice sets initial data for the above protocol. After its execution correspondents get collision elements $u_1, u_2, \ldots, u_t$ from $SC_n(K)$ of degree d.

Alice selects element $V_i \epsilon^d G'(n, K), i=1,2,\ldots t$ together with $T(i), P(i)$ from $CG_n(K)$ of degree 1. She generates V_i together with their inverses. Alice sets $E_i=T(i)V_iP(i)$ in their standard forms and triples $P^{-1}(i),\ V_{i,}{}^{-1}{}_{,} T^{-1}(i),$

She sends multivariate polynomials $Ei(x_j)+u_i(x_j)$ to Bob.

He restores elements $E_{i,}$ because of his knowledge of collision elements.

Encryption process. Correspondents use K^n *as* the plainspace and the cipherspace. Bob writes his message $p=(p_1, p_2, \ldots., p_n)$. Bob computes the sequence $p \rightarrow {}^1p=E_1(p),\ {}^1p \rightarrow E_2({}^1p),\ \ldots,\ {}^{t-1}p \rightarrow E_t({}^{t-1}p)={}^tp=c$ and sends ciphertext c to Alice. She decrypts via the consequtive usage of triples $P^{-1}(i),\ V_{i,}{}^{-1}{}_{,} T^{-1}(i),$

SECURITY ASPECTS FOR THE CRYPTOSYSTEM.

Adversary can break the cryptosystem via cryptanalysis of the protocol, but word decomposition problem currently is untractable. So he/she can use linearisation attacks via interceptions of plaintext with corresponding ciphertext.

Noteworthy that with quasirandom $P(i)$ and $T(i)$ degree of the composition E of $E_1, E_2, \ldots, E_t$ equals d^t. Thus condition $t \geq log_d(n)$ insures that degree of E will be of the size n. For this case appropriate linearization attacks are unknown.

REMARK. The combinations of multivariate protocol as above with known multivariate digital signature schemes can be defined in similar way (see [20],[24]).

3. Modification of the cryptosystems..

Alice can use abstract alphabet $Z=\{z(1), z(2), \ldots, z(t)\}$. She writes word of kind

$z_A=z(i_{1,})^{s(1)}z(i_{2,})^{s(2)} \ldots z(i_k)^{s(k)}$. where $i_s \neq i_{s+1.,}\ 1 \leq s \leq k\text{-}1,\ i_s \epsilon Z$ of length $s(1)+s(2)+\ldots+s(k)=O(log_d(n))$. Bob writes message $p=(p_1, p_2, \ldots., p_{n.})$. He applies Ei_1 to p exactly $s(1)$ times to get ${}^1c$, applies Ei_2 to ${}^1p$ exactly $s(2)$ times to get ${}^2p, \ldots$, applies Ei_k to ${}^{k-1}p$, exactly $s(k)$ times to get ${}^kp$ (the ciphertext c).

Alice decrypt with consequtive applications of $(Ei_k)^{-1}$ ($s(k)$ times) to c and gets ${}^1c$. $(Ei_{k-1})^{-1}$ to ${}^1c$ to get ${}^2c, \ldots, (Ei_1)^{-1}$ to ${}^{k-1}c$ to get plaintext p.

This flexible cryptosystem is obviously resistant to known cryptanalitical attacks.

4. Symbiotic combination of the protocol with one time pad encryption.

Correspondents can use one time pad encryption on the affine space K^n which transfer plaintext $(p_1, p_2, \ldots., p_n.)$ to the ciphrtext $(p_1+k_1, p_2+k_2, \ldots, p_n+k_n)$ created with the usage of the key $(k_1, k_2, \ldots., k_n.)$.

Currently they can not use classical Diffie-Hellman key exchange protocol because of discrete logarithm problem can be solved with the usage of quantum computer.

So we suggest the following modification of algorithm presented in the previous section,

The first two step are same. Correspondents executes protocol of the section 2. Secondly Alice (or Bob) uses abstract alphabet $Z=\{z(1), z(2), \ldots, z(t)\}$ and writes word of kind $z_A=z(i_1,)^{s(1)}z(i_2,)^{s(2)} \ldots z(i_k)^{s(k)}$. where $i_s \neq i_{s+1.}, 1 \leq s \leq k-1, i_s \epsilon Z$ of length $s(1)+s(2)+\ldots+s(k)=O(\log_d(n))$ and transfers it to partner. One of correspondents writes pseudorandom string $m=(m_1, m_2, \ldots., m_n.)$ and also sends it to his/her partner. Each of correspondents applies Ei_1 to m exactly $s(1)$ times to get ${}^1m$, applies Ei_2 to ${}^1m$ exactly $s(2)$ times to get ${}^2m, \ldots$, applies Ei_k to ${}^{k-1}m$, exactly $s(k)$ times to get ${}^km$ (the key $k=(k_1, k_2, \ldots., k_n.)$).

Finally Bob (or Alice) writes plaintext $p=(p_1, p_2, \ldots., p_n.)$ and sends $k+p$ to partner..

PRACTICAL ASPECTS.

After selection of parameter n in algoritm 4 correspondents can use single protocol of section 2.

After this Alice selects of E_1 as above, she selects rather large parameter d and some positive constant C. Alice suggest Cn^d as maximal number of messages for the exchange. For the increase of parameter n correspondents need to start a new session of the basic protocol.

REMARK. Modern quantum technologies allow to generate random sequences instead of pseudorandom sequences generated by deterministic Turing machines.

We think that usage of genuine random sequences makes above algorithms essentially stronger.

5. Example of a family of stable cubical groups.

The following family of stable groups $GA_n(K)$ is already used in some algorithms of symmetric cryptography and protocols of commutative and noncommutative cryptography (see [21], [22] and further references). Let K be a commutative ring. We define $A(n, K)$ as bipartite graph with the point set $P=K^n$and line set $L=K^n$ (two copies of a Cartesian power of K are used). We will use brackets and parenthesis to distinguish tuples from P and L. So $(p)=(p_1, p_2, \dots , p_n)\epsilon P_n$ and $[l]=[l_1, l_2, \dots , l_n]\epsilon L_n$. The incidence relation $I=A(n,K)$ (or corresponding bipartite graph I) is given by condition $pI\, l$ if and only if the equations of the following kind hold.

$p_2 - l_2=l_1p_1$, $p_3 - l_3= p_1 l_2$, $p_4 - l_4 = l_1p_3$, $p_5 - l_3 = p_1 l_4$, $\dots$, $p_n - l_n= p_1 l_{n-1}$ for odd n and $p_n - l_n = l_1 p_{n-1}$ for even n.

Let us consider the case of finite commutative ring K, $|K|=m$. As it instantly follows from the definition the order of our bipartite graph $A(n, K)$ is $2m^n$. The graph is m-regular. In fact the neighbour of given point p is given by above equations, where parameters $p_1, p_2,\dots, p_n$ are fixed elements of the ring and symbols $l_1, l_2,\dots, l_n$ are variables. It is easy to see that the value for l_1 could be freely chosen. This choice uniformly establishes values for $l_2, l_3, \dots , l_n$. So each point has precisely m neighbours. In a similar way we observe the neighbourhood of the line, which also contains m neighbours. We introduce the colour $\rho(p)$ of the point p and the colour $\rho(l)$ of line l as parameter p_1 and l_1 respectively.

Graphs $A(n, K)$ with colouring ρ belong to class of Γ *linguistic graphs* of type $(1. 1,n-1)$ considered in [23]. Linguistic graph $\Gamma= \Gamma(K)$ is defined over commutative ring K as a bipartite graph with partition sets L=K^n and P=K^k and colour sets K^s and K^r respectively. Projection ρ of point $x=(x_1, x_2, \dots, x_n)$, or line $y=[y_1, y_2, \dots,y_t]$, on the tuple of their first s and r coordinates respectively defines colours of vertices. Each vertex has a unique neighbour of selected colour. So $n+r=t+s$. The incidence of linguistic graphs is given by a system of polynomial equation over the ring K.

In the case of linguistic graph $\Gamma(K)$ with $s=r=1$ the path consisting of its vertices $v_0, v_1, v_2, ..., v_k$ is uniquely defined by initial vertex v_0, and colours $\rho(v_{i,})$, $i=1, 2,..., k$ of other vertices from the path. We can consider graph $\Gamma=\Gamma'(K[x_1, x_2, ..., x_n])$ defined by the same with Γ equations but over

the commutative ring $K[x_1, x_2, ..., x_n])$.

So the following symbolic computation can be defined. Take the *symbolic point* $x=(x_1, x_2, ..., x_n)$, where x_i are generic variables of $K[x_1, x_2, ..., x_n]$ and *symbolic string C* which is a tuple of polynomials $f_1,, f_2,, ... , f_k$, from $K[x_1]$ with even parameter k.. Form the path of vertices $v_0,=x$, v_1 such that v_1Iv_o and $\rho(v_1)=f_1(x_1)$, v_2 such that v_2Iv_1 and $\rho(v_2)=f_2(x_1)$, ..., v_k such that v_kIv_{k-1} and $\rho(v_k)=f_k(x_1)$. We choose parameter k as even number. So v_k is the point from the partition set $K[x_1, x_2,..., x_n]^n$ of the graph Γ'.

We notice that the computation of each coordinate of v_i depending on variables $x_1, x_2, ..., x_n$ and polynomials $f_1,, f_2,, ... , f_k$ needs only arithmetical operations of addition and multiplication. As it follows from the definition of linguistic graph final vertex v_k (point) has coordinates $(h_1(x_1), h_2(x_1,x_2), h_3(x_1,x_2,x_3),...,h_n(x_1,x_2,..., x_n))$, where $h_1(x_1)=f_k(x_1)$. Let us consider the map $H= \Gamma^\wedge\eta(C)$: $x_i\longrightarrow h_i(x_1, x_2,..., x_n)$, $i=1, 2,..., n$ which corresponds to symbolic string C. Assume that the equation $b=f_k(x_1)$ has exactly one solution. Then the map H:$x_i\longrightarrow h_i(x_1, x_2, ..., x_n)$, $i=1, 2,..., n$ is a bijective transformation. In the case of finite parameter k and finite densities of $f_i(x_1)$, $i=1, 2,..., n$ the map H also has finite density. If all parameters $\deg(f_i(x_1))$ are finite then the map H has a linear degree in variable n. The idea of symbolic computation (see [44] and further references) is the following one.

Let us consider the totality $St=St(K)$ of all symbolic strings with the product $(f_1, f_2,..., f_r) \cdot (g_1, g_2,..., g_s) = (f_1, f_2,..., f_s, g_1(f_r), g_2(f_r),...g_s(f_r))$. It is easy to see that $St(K)$ is a semigroup for which empty string serves as a unity.

One can check that the map $^{\Gamma}\eta=\eta$ *is a* homomorphism of semigroup $St(K)$ into Cremona semigroup $S(K^n)$ for each linguistic graph Γ with $r=s=1$ and point set K^n. We consider a subsemigroup $\sum=\sum(K)$ *of symbolic strings C* of kind $(x_1+a_i, x_2+ a_2 ..., x_t+a_t)$ where parameter t is even. In the case of a linguistic graphs with $r=s=1$ we identify a symbolic stringn C with the corresponding tuple $(a_1, a_2, ... , a_t)$. Natural product of two strings given by tuples $C_1=(a_1, a_2, ... , a_t)$ and $C_2=(b_1, b_2, ... , b_m)$ is a string $C=C_1\circ C_2=(a_1, a_2, ... , a_t , b_1+ a_t , b_2+ a_t, ... , b_m+a_t)$. This product transforms $\sum$ to a semigroup. The map η' sending C to $\eta(C)$ is a homomorphism of $\sum$ into affine Cremona group $C(K^n)$. It is a restriction of $^{\Gamma}\eta$ onto $\sum(K)$. Let $C=(x_1\ a_1, x_1 +a_2, ..., x_1+a_s)$ be a symbolic string from semigroup $\Sigma(K)$. We refer to Rev(C)=(x_1-a_s +a_{s-1}, x_1-a_s+a_{s-2}, … , x_1-a_s+a_1 , x_1-a_s) as a reversing string for C. It is easy to see that $\eta'(CRev(C))$ *is a unity* of Cremona semigroup.

In the case of linguistic graphs $\Gamma=A(n, K)$ the totality $GA(n, K) = \eta'(\sum(K))$ is a stable subgroup of degree 3 (see [21] and further references). We use notation ${}^n\eta'$ for the restriction of ${}^{\Gamma}\eta$, $\Gamma=A(n,K)$ onto $\sum$. We assume that $a_0=0$ and say that transformation $\eta'(C)$ is irreducible if $a_i\neq a_{i+2}$, $i=1, 2,..., t-2$. If $a_1\neq a_{t-1}$, and $a_2\neq a_t$ we say that irreducible symbolic string C and corresponding transformation $\eta'(C)$ are standard elements. We have a natural homomorphism $GA(n+1, K)$ onto $GA(n, K)$ induced by the homomorphism Δ from $A(n+1, K)$ onto $A(n, K)$ sending point $(x_1, x_2, ..., x_n, x_{n+1})$ to $(x_1, x_2, ..., x_n)$ and line $[x_1, x_2, ..., x_n, x_{n+1}]$ to $[x_1, x_2, ..., x_n]$. It means that there is well defined projective limit $A(K)$ of graphs $A(n, K)$ and groups $GA(K)$ of groups $GA(n, K)$ when n is growing to infinity. In fact in the case of $K=F_q$, $q>2$ infinite graph $A(F_q)$ is a tree.

It means that group $GA(F_q)$ is a group of walks of even length on q-regular tree starting in zero point with natural addition of them. A standard symbolic string C defines transformation ${}^n\eta'(C)$ in each group $GA(n, K)$, $n\geq 2$ and $GA(K)$. An irreducible transformation $\eta'(C)$ from $GA(K)$ has an infinite order.

We are going to use the family of maps introduced below.

Let $\Delta=\Delta n,k$, $n>k$ be a canonical homomorphism of $A(n,K)$ onto $A(k,K)$ corresponding to procedure of deleting of coordinates with indexes $k+1, k+2, ..., n$. This map defines the canonical homomorphism $M=\mu(n, k)$ of group $GA(n, K)$ onto $GA(k, K)$. Let us consider the diagram

$$\begin{tikzcd}
 & \sum(K) \arrow[dl, dash] \arrow[d] \\
GA(k, K) & GA(n, K) \arrow[l]
\end{tikzcd}$$

where vertical arrow corresponds to homomorphism ${}^n\eta'$ from $\sum(K)$, skew line corresponds to ${}^k\eta'$ and horizontal arrow stands for $M(n,k)$, $n>k$. It is easy to see that this diagram is a commutative one.

As it was noticed in [23] subgroups $G(n, K)$ of $E_n(K)$ form a family of stable cubical maps. So correspondents can take pair $GA(n, K)$ and $GA(k, K)$ with $n(k)=k+\gamma$ where parameter γ is a positive constant or a positive linear function in variable k.

Alice can use defined above computationally tame homomorphism $M=M(n,k)$, $n>k$ of groups $G(n,K)$ and $G(k,K)$.

She considers family of subgroups G_k=$G(n,K)$, n=$n(k)$, k-2,3 and famil G'_k=$G(k,K)$,k=2,3,...,n

She selects different strings w_1, w_2, ...w_s of even length of semigroup $\sum(K)$ such that $w_i\ w_j \neq w_j w_i$ for different i and from $\{1,2,...,s\}$. This condition implies that ${}^s\eta(w_i w_j) \neq {}^s\eta(w_j w_i)$ for $s \geq 2$. After the check of noncommutativity of generators Alice takes generators ${}^i g_j$=${}^{n(i)}\eta\ (w_j)$, j=1, 2, ..., s, $s \geq 2$ as in the described above protocol in the case of s generators. Correspondents have to use this protocol with t outputs and dimension of affine space k.

Similar description of similar groups $GD(n,K)$ connected with other linguistic graphs $D(n,K)$ is given in [15]. Desctpton of explicite constructionsof semigroups and groups of kind ${}^dG(n,, K)$ from theorem1 and 2 and tame homomorphisms between them is given in [24].

6. Some implementations.

Two implementations of the above protocol for the case ${}^3G(n, K)$ with t=1 is presented in **[13].** Two distinct graph based explicit constructions $GD(n,K)$ and $AD(n,K)$ were chosen as platforms of ${}^3G(n, K)$. We add the possibility of arbitrary t and implement described above protocol based cryptosystem.

The complexity estimates are the following.

1. The execution of the protocol requires $O(n^{12})$ elementary operations.
2. The encryption requires time $O(n^4)log_3(n)$ for Bob.
3. Graph based nature allows Alice to decrypt with $O(n^2 log_3\ n)$ elementary operations in general case when majority of entries of each matrix $T(i)$ and $P(i)$ are nonzero ring elements.

3'. In the case of special sparse matrices $P(i)$, $Q(i)$ with $O(n)$ nonzero entries decryption process has complexity $O(n)log_3\, n$.

Three following different cases for commutative ring K were selected

1. Finite fields of characteristic 2.
2. Arithmetic rings Z_m for which modulo m is a power of 2.
3. Boolean rings of size 2^m.

Maximal number of monomial terms m for encryption maps E_i, i=1,2,...,t is presented in the tables below. Let $den(f)$ be the density of multivariate polynomial f , i. e. the number of its monomial terms. So in each case we take $m(i)$=$den\ (E_i\ (x_1\ ))$+$den(E_i(x_2))$+...+$den\ (E_i(x_n\ ))$ and present m=$max\ m(j)$,j=1,2,..., t.

We implement above presented protocol and corresponding cryptosystem in the case of ${}^2G(n, K)$ with the usage of modified platforms presented in [14] and corresponding homomorphisms [15]. In this case the protocol costs $O(n^6)$ elementary operations, complexity of encryption is $O(n^3)\log_2(n)$ and decryption takes $O(n^2)\log_2(n)$ in the general case. Decryption in the case of sparse matrices takes $O(n)\log_2(n)$.

REMARK.

In the case of finite fields and $d=2, 3$ instead of endomorphisms $E_i(x), i=1,2,..t$ as above one can take standard forms of known encryption maps of public keys of Classical Multivariate Cryptography regardless of their crypt analytical status because they are not given publicaly in the presented above cryptosystem (see [17]). We are working on the implementation of the variant with bijective Imai-Matsumoto encryption in the case of finite fields of characteristic 2 (see [16]).

Implemented cryptosystems with bijective encryption maps can be used for tasks of ecryption as well as for the task of digital signature.

We note that psesented above methods can be also used in the case of nonbijective maps to create new digital signature (see [18]) with modified versions of Rainbow-like Unbalanced Oil and Vinegar algorithms.

Table 1. Number m of monomial terms of the cubic encryption map from the group $\boldsymbol{G_D}(n, \mathbb{F}_{2^{32}})$ (case of general matrices $P(i)$ and $Q(i)$)).

	length of the private password				
n	**16**	**32**	**64**	**128**	**256**
16	6544	6544	6544	6544	6544
32	50720	50720	50720	50720	50720
64	399424	399424	399424	399424	399424
128	3170432	3170432	3170432	3170432	3170432

Table 2. Number of monomial terms of the cubic encryption map from the group **G**$A(n, \mathbb{F}_{2^{32}})$,

	length of the private password				
n	**16**	**32**	**64**	**128**	**256**
16	6544	6544	6544	6544	6544
32	50720	50720	50720	50720	50720
64	399424	399424	399424	399424	399424
128	3170432	3170432	3170432	3170432	3170432

Table 3. Generation time for the map (ms) **G**$D(n, \mathbb{F}_{2^{32}})$,

	length of the private password				
n	**16**	**32**	**64**	**128**	**256**
16	76	140	268	524	1036
32	1224	2328	4541	8968	17828
64	21889	40417	77480	151592	299844
128	453798	812140	1526713	2946022	5792889

Table 4. Generation time for the map (ms) **G**$A(n,\mathbb{F}_{2^{32}})$.

	length of the password				
n	**16**	**32**	**64**	**128**	**256**
16	76	148	288	576	1148
32	1268	2420	4700	9268	18405
64	22144	40948	78551	153784	304240
128	460200	819498	1532277	2970743	5836938

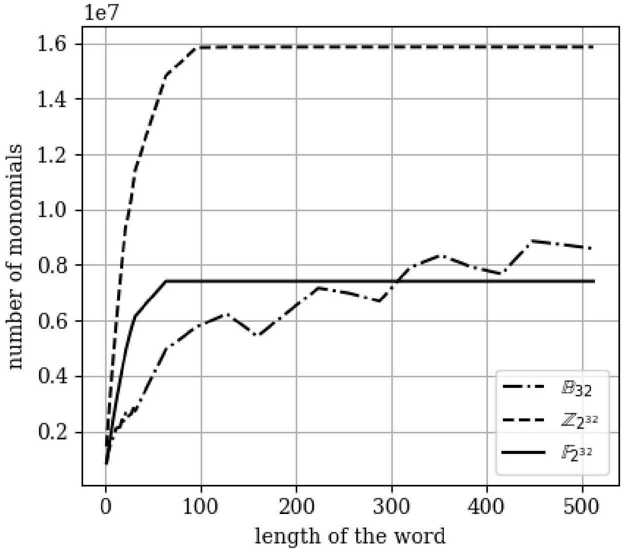
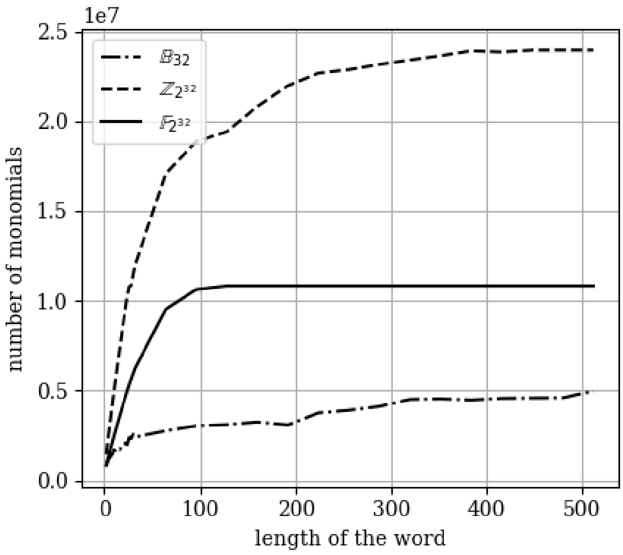


Fig. 1. Number of monomial terms of the cubic map, case of sparse matrices ($n = 128$) (group **G**$D(n,K)$, $K = B(32), Z_{2^{32}}, F_{2^{32}}$), (1.0 means 10000 terms).



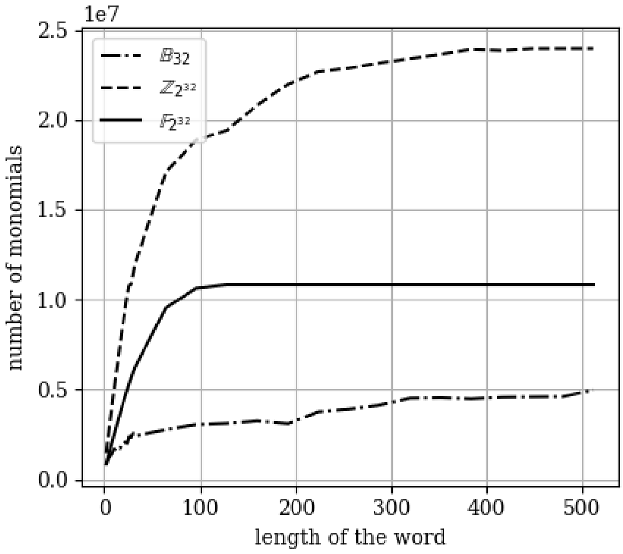


Fig.2. Number of monomial terms of the cubic map , case of the sparse matrices ($\boldsymbol{n = 128}$) (graph **G**$\boldsymbol{A(n,K)}$, $\boldsymbol{K = B(32), Z_{2^{32}}, F_{2^{32}}}$).

7. Conclusions

Multivariate cryptography (MC) together with Latice Based, Hash based , Code based and Superelliptic curves based Cryptographies form list of the main directions of Post Quantum Cryptography.

Investigations in the framework of tender of National Institute of Standardisation Technology (the USA) indicates that the potential of classical MC working with nonlinear maps of bounded degree and without the usage of compositions of nonlinear transformation is very restricted. Only special case of Rainbow like Unbalanced Oil and Vinegar digital signatures is remaining for further consideration. The remaining public keys for encryption procedure are not of multivariate. nature.

The paper presents large semigroups and groups of transformations of finite affine space of dimension *n* with the multiple composition property. In these semigroups the composition of *n* transformations is computable in polynomial time. Constructions of such families are given together with effectively computed homomorphisms between members of the family.

These algebraic platforms allow us to define protocols for several generators of subsemigroup of affine Cremona semigroups with several outputs. Security of these protocols rests on the complexity of the word decomposition problem,

Finally presented algebraic protocols expanded to cryptosystems of El Gamal type which is not a public key system. New nonclassical multivariate cryptosystems are implemented with platforms of cubical transformations for which theoretical complexity estimates and results of computer simulations are given in the cubical case.

References

[1]. Sakalauskas., P. Tvarijonas , A. Raulynaitis, Key Agreement Protocol (KAP) Using Con-jugacy and Discrete Logarithm Problema in Group Representation Level}, INFORMATICA, 2007, vol. !8, No 1, 115-124.

[2] D. N. Moldovyan, N. A. Moldovyan, A New Hard Problem over Non-commutative Finite Groups for Cryptographic Protocols, International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security, MMM-ACNS 2010: Computer Network Security, pp. 183-194.

[3] V. Shpilrain, A. Ushakov, The conjugacy search problem in public key cryptography: unnecessary and insufficient,Applicable Algebra in Engineering, Communication and Computing, August 2006, Volume 17, Issue 3–4, pp 285–289

[4]Delaram Kahrobaei, Bilal Khan, A non-commutative generalization of ElGamal key exchange using polycyclic groups, In IEEE GLOBECOM 2006 - 2006 Global Telecommunications Conference [4150920] DOI: 10.1109/GLOCOM.2006.

[5] Delaram Kahrobaei, Bilal Khan, A non-commutative generalization of ElGamal key exchange using polycyclic groups, In IEEE GLOBECOM 2006 -

2006 Global Telecommunications Conference [4150920] DOI: 10.1109/GLOCOM.2006.

[7] Zhenfu Cao (2012). New Directions of Modern Cryptography. Boca Raton: CRC Press, Taylor & Francis Group. ISBN 978-1-4665-0140-9.

[8] Alexei G. Myasnikov; Vladimir Shpilrain; Alexander Ushakov. Non-commutative Cryptography and Complexity of Group-theoretic Problems. Amer. Math Soc. 2011

[9] J. A. Lopez Ramos, J. Rosenthal, D. Schipani, R. Schnyder, Group key management based on semigroup actions, Journal of Algebra and its applications, vol.16 , 2019.

[10] Gautam Kumar and Hemraj Saini, Novel Noncommutative Cryptography Scheme Using Extra Special Group, Security and Communication Networks ,Volume 2017, Article ID 9036382, 21 pages, https://doi.org/10.1155/2017/9036382.

[11] V. A. Roman'kov, A nonlinear decomposition attack, Groups Complex. Cryptol. 8, No. 2 (2016), 197-207.**27**.

[12] V. Roman'kov, An improved version of the AAG cryptographic protocol, Groups, Complex., Cryptol, 11, No. 1 (2019), 35-42.

[13] A. Ben-Zvi, A. Kalka and B. Tsaban, Cryptanalysis via algebraic span, In: Shacham H. and Boldyreva A. (eds.) Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2018, Proceedings, Part I, Vol. 10991, 255{274, Springer, Cham (2018).

[14] B. Tsaban, Polynomial-time solutions of computational problems in noncommutative-algebraic cryptography, J. Cryptol. 28, No. 3 (2015), 601-622.

[15] Max Noether, Luigi Cremona , Mathematische Annalen 59, 1904, p. 1–19.

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

[17] V. Ustimenko, M. Klisowski, On Noncommutative Cryptography with cubical multivariate maps of predictable density, In “Intelligent Computing’’ , Proceedings of the 2019 Computing Conference, Volume 2, Part of Advances in Intelligent Systems and Computing (AISC, volume 99, pp, 654-674.

[18] V. Ustimenko, On desynchronised multivariate algorithms of El Gamal type for stable semigroups of affine Cremona group, Theoretical and Applied Cybersecurity, National Technical University of Ukraine "Igor Sikorsky Kiev Polytechnic Institute", vol 1, 2019, pp. 22-30.

[19]V.Ustimenko, On the usage of postquantum protocols defined in terms of transformation semi-groups and their homomorphisma, Theoretical and Applied Cybersecurity, National Technical University of Ukraine "Igor Sikorsky Kiev Polytechnic Institute", vol 2, 2020, pp. 32-44.

[20] N. Koblits, Algebraic Cryptography, Springer, 2000.

[21] V.Ustimenko, On affine Cremona semigroups, corresponding protocols of Non-commutative Cryptography and encryption with several nonlinear multivariate transformations on secure Eulerian mode. Cryptology ePrint Archive, 2019/1130.

[20] V, Ustimenko, On Multivariate Algorithms of Digital Signatures Based on Maps of Unbounded Degree Acting on Secure El Gamal Type Mode. Cryptology ePrint Archive, 2020/1116.

[21] V. A. Ustimenko, V. A. (2013). On the extremal graph theory and symbolic computations. Dopov. Nac. Akad. Nauk Ukr., 2013, No. 2, pp. 42-49.

[22] V. Ustimenko, On semigroups of multiplicative Cremona transformations and new solutions of Post Quantum Cryptography, Cryptology ePrint Archive, 133, 2019.

[23.] 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.

[24] V. Ustimenko.On Multivariate Algorithms of Digital Signatures on Secure El Gamal Type Mode. Cryptology ePrint Archive, 2020/984.