UDC 519.1, 514.128

On Inverse Protocols of Post Quantum Cryptography Based on Pairs of Noncommutative Multivariate Platforms Used in Tandem

Vasyl Ustymenko[1,2]

[1] *Royal Holloway University of London, United Kingdom.*
[2] *Institute of telecommunications and global information space, Kyiv, Ukraine*

Abstract
Non-commutative cryptography studies cryptographic primitives and systems which are based on algebraic structures like groups, semigroups and noncommutative rings. We continue to investigate inverse protocols of Non-commutative cryptography defined in terms of subsemigroups of Affine Cremona Semigroups over finite fields or arithmetic rings Z_m and homomorphic images of these semigroups as possible instruments of Post Quantum Cryptography. This approach allows to construct cryptosystem which are not public keys, when protocol finish correspondents have mutually inverse transformations on affine space K^n or variety $(K^*)^n$ where K is the field or arithmetic ring.
The security of such inverse protocol rests on the complexity of word problem to decompose element of Affine Cremona Semigroup given in its standard form into composition of given generators. We discuss the idea of usage combinations of two cryptosystems with cipherspaces$(K^*)^n$ and K^n to form a new cryptosystem with the plainspace$(K^*)^n$, ciphertextK^n and nonbijective highly nonlinear encryption map.

Keywords: Multivariate Cryptography, Noncommutative Cryptography, stable transformation groups and semigroups, semigroups of monomial transformations, word problem for nonlinear multivariate maps, hidden tame homomorphisms, key exchange protocols, cryptosystems, linguistic graphs

This research is supported by British Academy Fellowship for Researchers at Risk 2022

1. Introduction

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]. In June 20320 NIST published a list of candidates qualified to the third round of the PQC process. Some public key candidates are implemented like PQC Round 2 candidate called Round 5 (see [2]) or code based classic Mc Eliece algorithm (see [3]). The unique third round candidate defined via Multivariate Cryptography was selected in the category of digital signatures schemes. Noteworthy that during the following NIST project steps an interesting results on cryptanalysis of this candidate known as Unbalanced Rainbow Oil and Vinegar digital signatures schemes were found (see [34], [35], [36]). This scheme is defined via quadratic multivariate public rule, which refers to MiniRank problem Already selected in July of 2022 four cryptosystems are developed not in the area of Applide Algebra. This fact motivates algebraist to continue design of new cryptographical primitives in areas of Noncommutative Cryptography and Multivariate Cryptography.

In March 2021 it was announced that prestigious Abel prize will be shared by A. Wigderson and L.Lovasz. They contribute valuable applications of theory of Expanding graphs to Theoretical Computer Science (see [1], [2] and further references). We have been working on applications of these graphs to Cryptography. This paper is dedicated to the usage of geometrical expanders in sense of N. Alon [3] as encryption tools.

In this paper we discuss the development of new cryptosystems within alternative approach ([4], [5], [6]) to construct cryptosystems without usage of public rules. The idea is based on modifications of Diffie Hellman protocols on the case of multiple generators to construct procedures which output is a pair of mutually inverse multivariate transformations of affine space K^n defined over finite commutative ring K. Security of these algorithms rests on the complexity of word problem to decompose given multivariate map into generators of affine Cremona [7] semigroup. The first usage of the complexity of word problem for groups was considered in [8].

In the algorithms of this paper the encryption rule is not given publicly. We introduce new cryptosystems defined in terms of stable semigroups of transformations of affine K^n which consist on transformations of degree bounded by small constant. Main instruments are following. Let K be a commutative ring, $K[x_1, x_2,\dots,x_n]$ be a ring of polynomials in n variable. *Semigroup of endomorphisms* $End(K[x_1, x_2,\dots,x_n])=S(K^n)$ of $K[x_1, x_2,\dots,x_n]$ is known as Affine Cremona Semigroup, element f of $S(K^n)$ acts naturally on affine space K^n and can be given its standard form $x_1\to f_1(x_1,x_2,\dots,x_n), x_2\to f_2(x_1,x_2,\dots,x_n), \dots x_n\to f_n(x_1,x_2,\dots,x_n)$, where $f_1 \epsilon K[x_1, x_2,\dots,x_n]$.

We assume that K is a finite commutative ring. Symbol $C(K^n)$ stands for Affine Cremona Group of all invertible elements from $S(K^n)$.

Density of the map f is total number of monomial term in all f_i.

The computations in subgroups and subsemigroups of $S(K^n)$ are computationally coustly because for transformations g and h in ''general position '' degree of $g(h(x)$ coincides with degree of $h(g(x))$ and equals $deg(g)\cdot deg(h)$. The density of g^x is growing fast when x grows. So special conditions on subsemigroup S $<S(K^n)$ needed to make computations feasible.

We know two such conditions

(1) *stability condition,* group G such for $g \epsilon G$ maximal degree $deg(g)$ is d (the cases $d=2$ or $d=3$ are probably the most important).

(2) *minimality of density condition* (transformation $g \epsilon G$ has to be toric, i.e. its standard form is written as $x_i\to t_i(x_1,x_2,\dots,x_n)$, where t_i are monomial expressions. We refer to g as Eulerian map if coefficients are regular coefficients and the map g is bijective one on the variety $(K^*)^n$. Correspondents use this variety as the plainspace. Let ${}^nEG(K)$ be Eulerian group of all such transformations.

PLATFORMS. We discover classes of subgroups of kind (1) or (2) and fast algorithm to generate pairs g and g^{-1}. Look at cryptology e-print archive papers [9] and [6] and further references.

Notice that security of Diffie-Hellman algorithm for groups depends not only on abstract group G but on the way of its generation in computer memory. For instance if $G=Z^*_p$ is multiplicative group of large prime field then discrete logarithm problem (DLP) is difficult one and guarantees the security of the protocol, if the same abstract group is given as additive group of Z_{p-1} protocol is insecure because DLP will be given by linear equation.

If G is noncommutative group correspondents can use conjugations of elements involved in protocol, some algorithms of this kind were suggested in [10], [11], [12], [13], where group G is given with the usage of generators and relations. Security of such algorithms is connected with Conjugacy Search Problem (CSP) and Power Conjugacy Search Problem (PCSP), which combine CSP and Discrete Logarithm Problem and their generalisations.

This direction belongs to **Non-commutative cryptography** which is active area of cryptology, where the.cryptographic primitives and systems are based on algebraic structures like groups, semigroups and noncommutative rings (see [14], [15], [16], [17], [18], [19], [20], [23], [24]). Semigroup based cryptography consist of general cryptographical schemes defined in terms of wide classes of semigroups and their implementations for chosen semigroup families (so called platform semigroups).

Since 2015 several important cryptanalytic results have been obtained in this area ([37]-[42]).

As we already mentioned we work with subsemigroups of affine Cremona semigroup $S(K^n)$ on generalisations and modifications of

Diffie – Hellman protocols for the case of several generators. Elements of the subsemigroup are presented in their standard form of multivariate cryptography.

2. Some schemes of noncommitative cryptography with multivariate platforms

LetS'<$S(K^n)$ be a subsemigroup of affine Cremona semigroup andφ be a homomorphism fromS' onto $G< S(K^n)$, $n>m$.

2.1. Additionally we consider a *stable subsemigroup*S, $S'<S<S(K^n)$ and assume thatH is stable group$H$, $G<H<C(K^m)$. Alice selects elementss_1, s_2, … ,s_r , $r>1$ of subsemigroups$S'$and computes $\varphi(s_i)=u_i$. She takes invertible elements $h\epsilon S(K^n)$of kind av, $deg(a)=1$, $v\epsilon$ $S$and $f\epsilon C(K^n)$, $f=bg$,$deg(b)=1$, $g\epsilon H$and forms pairs ($a_i=hs_ih^{-1}$, $b_i=f\ u_if^{-1}$) and sends them to Bob.

He forms word $w=(a_{i(1)})^{\alpha(1)}(a_{i(2)})^{\alpha(2)}\dots(a_{i(t)})^{\alpha(t)}$, $t>r-1$, $i(j)\epsilon\{1,2,\dots,r\}$,$\alpha(j)>0$,$j=1,2,\dots,t$ and sends it to Alice. Bob changes alphabet via the substitution of $b_i$instead ofa_i and keeps the word$u=(b_{i(t)})^{\alpha(t)}(b_{i(t-1)})^{\alpha(t-1)}\dots(b_{i(t)})^{\alpha(t)}$..

Alice computes u^{-1} as $f\varphi(h^{-1}wh)f^{-1}$.

So Alice and Bob when the protocol ends have mutually inverse encryption/decryption tools $u^{-1}$and$u$ for the plainspaceK^m.

Examples of the implemetation of this algorithm can be found in [6].

2.2. Let us consider above algorithms in the case when semigroup$S$ consists on *toric elements* and $H<{}^mEG(K)$ and $S=S'$.

Alice forms h and h^{-1} from ${}^nEG(K)$together with pair f,f^{-1} from${}^mEG(K)$ and proceed with the modification of previous algorithm.

Alice selects elementss_1, s_2, … ,s_r , $r>1$ of semigroups $S$and computes $\varphi(s_i)^{-1} = u_i$. She takes invertible elements h and f toform pairs ($a_i=hs_ih^{-1}$, $b_i=f\,u_if^{-1}$) and sends them to Bob. The rest of the algorithm is identical to case of procedure 2.1.

After the completion of inverse protocol Alice and Bob have bijective maps $u^{-1}$and u on the plainspace$(K^*)^m$.

Security base: The adversary has to solve the ***word problem***for the subsemigroupS', i. e., find the decomposition of w from S'into generators a_i, $i= 1, 2,...,t$. The general algorithm to solve this problem in polynomial time for the variable $n$is unknown, as well as a procedure to get its solution in terms of quantum computations. The problem depends heavily on the choice of group.

Remark. Of course in each case alternative ways of computation of the value $\sigma(w)$ of antiisomorphismσ between semigroup $<a_1, a_2, \dots, a_r>$ and group $<b_1, b_2, \dots, b_r>$ given by the rule$\sigma(a_i)= b_i$have to be investigated.

2.3. On platforms acting in tandem.

2.3.1. Alice and Bob use algorithm 2.1 with output $u^{-1}$and$u$ on K^mas leading procedure. Supporting procedure is algorithm of kind 2.2 with the same commutative ring K and parameter m. Alice (or Bob) deforms the input of 2.2 for her/his correspondent via the change a_i,b_i fora_i,b_iv, $i=1,2,\dots, r'$ where $v$is u^{-1} or u. Notice that the maps b_iv are well defined injective mapsof$(K^*)^m$ intoK^m,they have*polynomial density.*

Bob (or Alice) computes pairs (a_i,b_i)because of his/her possession ofv^{-1}. After the completion of supporting procedure Alice and Bob get mutually inverse elements z^{-1}andzof ${}^mEG(K)$.They use $(K^*)^m$ *as* plainspace andK^mas cipherspace.

To encrypt Alice maps her message p to $z^{-1}(p)=m$ and then she computes theciphertext $c= u^{-1}(m)$.

Bob decrypts via application of u *to* c and computation $z(u(c))$.

Similarly Bob encrypts$p$ *via* consecutive computation *of*$z(p)$ and $u(z(p))$.

Alice applies $u^{-1}$to ciphertext c and computes the plaintext as $z^{-1}(u^{-1}(c))$.

Remark. Encryption and decryption functions of the above algorithm can be treated as polynomial maps of K^m toK^m because elements of ${}^mEG(K)$act naturally on K^m. Between encryption and decryption functions there is a density gap because decryption map is not a transformation of polynomial density. Such pairs can be used as non-bijective stream ciphers in a spirit of [25]. In the tandem procedure interception of plaintexts with corresponding ciphertext attacks are unfeasible without the computation of $\sigma(w)$.

2.3.2 Alice and Bob can use algorithm 2.2 with output u^{-1} and$u$ on $(K^*)^m$ as leading procedure. Supporting procedure is algorithm of kind2.1 with the same commutative ring $K$and parameter m.

Algorithms of generation of pairs (z, z^{-1}) from ${}^{m}EG(K)$ are described in [6].

3. On groups and semigroups defined in terms of linguistic graphs

3.1. On linguistic graphs over commutative rings and skating on them.

The missing definitions of graph-theoretical concepts which appear in this paper can be found in [28]. All graphs we consider are *simple* graphs, i.e. undirected without loops and multiple edges. Let $V(G)$ and $E(G)$ denote the set of vertices and the set of edges of G respectively.

When it is convenient we shall identify G with the corresponding anti-reflexive binary relation on $V(G)$, i.e. $E(G)$ is a subset of $V(G)\circ V(G)$ and write $v\ G\ u$ for the adjacent vertices u and v (or neighbours).

We refer to $|\{ x \in V(G)|\ xGv \}|$ as *degree of the vertex v*.

The *incidence structure* is the set V with partition sets P*(points)* and L *(lines)* and symmetric binary relation I such that the incidence of two elements implies that one of them is a point and another one is a line. We shall identify $I$with the simple graph of this incidence relation or *bipartite graph*. The pair x, y , $x \in P$, $y\in L$ such that $x\ I\ y$ is called a *flag* of incidence structure I.

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

a_1x_{s+1}-$b_1\mathbf{y}_{r+1}=f_1 (x_1,x_2 ,\dots ,x_s, y_1,y_2, \dots , y_r)$

a_2x_{s+2}-$b_2\mathbf{y}_{r+2}=f_2 (x_1,x_2 ,\dots ,x_s, x_{s+1}, y_1, y_2, \dots , y_r, y_{r+1})$

…

a_mx_{s+m}-$b_m\mathbf{y}_{r+m}=f_m (x_1,x_2 ,\dots ,x_s, x_{s+1},\dots, x_{s+m}, y_1,y_2, \dots , y_r, y_{r+1, \dots} y_{r+m})$

where a_j, and b_j, $j=1,2,,,,m$ are not zero divisors, and f_j are multivariate polynomials with coefficients from K [29]. Brackets and parenthesis allow us to distinguish points from lines.

The colour$\rho(x)$=$\rho((x))$ ($\rho(y)$=$\rho([y])$) of point x (line [y]) is defined as projection of an element (x) (respectively [y]) from a free module on its initial s (relatively r) coordinates. As it follows from the definition of linguistic incidence structure for each vertex of incidence graph there exists unique neighbour of a chosen colour.

We refer to $\rho((x))=(x_1, x_2 ,\dots , x_s)$ for $(x)=(x_1, x_2 ,\dots , x_{s+m})$ and $\rho([y])=(y_1, y_2, \dots , y_r)$ for $[y]=[y_1, y_2, \dots , y_{r+m}]$ as the colour of the point and the colour of the line respectively. For each b $\in K^r$ and p=$(p_1, p_2 ,\dots ,p_{s+m})$ there is a unique neighbour of the point $[l]=N_b(p)$ with the colour$b$. Similarly for each c$\in K^s$ and line $l=[l_1, l_2 ,\dots , l_{r+m}]$ there is a unique neighbour of the line $(p)= N_c([l])$ with the colour c. The triples of parameters s,r,m defines *type of linguistic graph.*

We consider also linguistic incidence structures defined by infinite number of equations.

Linguistic graphs are defined up to isomorphism. We refer to written above equations asb canonical equations of linguistic graph.

In the case of linguistic graph defined over commutative ring the walk consisting of its vertices $v_0, v_1, v_2, \dots,v_k$ is uniquely defined by initial vertex v_0, and colours$\rho(v_i,)$, $i=1, 2,\dots, k$ of other vertices from the path. We consider the equivalence relations on partition sets such that $(p)\approx(p')([l] \approx [l'])$*if* $p_{i+s}=p'_{i+s}$ $(l_{i+r}=l'_{i+r})$ for$i\in\{1,2,..m\}$.

We define *jump operator* $J(p, a)$, $a\in K^s$ on partitions set P ($J(l,a)$, $a\in K^r$ on partion set L) by conditions $J(p,a)\approx(p)$ and $\rho(J(p,a))=a$ ($J([l],a)\approx[l]$ and $\rho(J([l],a))=a$).

Already defined*neighbour computation operator* (or *ground moving operator)* $N(v, a)$ acts on *PUL* by rules $N(p, a)=[l]$ where $(p)I[l],\rho([l])=a$ and $N([l],a)=(p)$ where $(p)I[l],\rho((p))=a$.

Let us consider *skating chain* of the linguistic graph with starting point p which is a sequence$(p, p_0, l_1, l_2, p_3, p_4, \dots, l_{t-3}, l_{t-2}, p_{t-1},p_t)$, $t=4k$, $k\geq0$ such that $p\approx p_0,l_{2i+1}\approx l_{2i+2}$, $i\geq0$, $p_{2i+1}\approx p_{2i+2}$ and $p_{2i}Il_{2i+1}$for$i \geq0$.

Colours of elements from the skating chain and the starting point determine the sequence. Obviously sequence of alternating jump operators J_a and ground moving operators form the skating chain from starting point (p). In fact term skating chain is selected because of the similarity of computation the sequence with competitions on skating boards, roller skates, figure skating (various jumps and skate surface moves).

3.2. Semigroups of infinite symbolic strings and linguistic compression maps.

Let us consider semigroup $S(K^s)$ and the totality$S^{s,r}(K)$ of maps of kind $G:(y_1, y_2,\dots, y_r)\rightarrow(f_1(x_1, x_2,\dots ,x_s), f_2(x_1, x_2,\dots , x_s),\dots, f_r(x_1, x_2,\dots , x_s))$. If $H\epsilon S(K^s)$ then $G(H)$ for$G\epsilon S^{s,r}(K)$ is the map $(y_1, y_2,\dots, y_r)\rightarrow(f_1(H(x_1),H(x_2),\dots, H(x_s)), f_2(H(x_1),H(x_2),\dots, H(x_s)),\dots,f_r(H(x_1),H(x_2),\dots, H(x_s)))$.

When it is convenient we will identify elements of $S(K^s)$ with tuples from $K[x_1, x_2,\dots, x_s]^s$ and elements of$S^{s,r}(K)$ with tuples of $K[x_1,x_2,\dots,x_s]^r$.

Let us consider a to totality ${}^sBS_r(K)$ of sequences of kind

$u=(H_0, G_1, G_2, H_3,H_4,G_5, G_6,\dots, H_{t-1}, H_t)$, $t=4i$, where$H_k\epsilon S(K^s)$,

$G_j \epsilon S^{s,r}(K)$. We refer to ${}^sBS_r(K)$ as a totality of bigraded symbolic strings.

We define a product of u with $u'=(H'_0, G'_1, G'_2, H'_3, H'_4, G'_5, G'_6,\dots, H'_{l-1}, H_l)$ as $w=(H_0, G_1, G_2, H_3, H_4, G_5, G_6,\dots, H_{t-1}, H'_0(H_t), G'_1(H_t), G'_2(H_t), H'_3(H_t), H'_4(H_t), G'_5(H_t), G'_6(H_t), \dots, H'_{l-1}(H_t), H'_l(H_t))$.

It is easy to see that this operation transforms ${}^sBS_r(K)$ into the semigroup

with the unity element (H_0), where E_0 is an identity transformation from $S(K^s)$.

Elements of kind are $(H_0, G_1, G_2, H_3, H_4)$ are generators of the semigroup.

The refer to generator with $H_4=E_0$ as loop element. Let $L={}^sL_r(K)$ be the totality of loop elements. The semigroup generated by loop elements is isomorphic to free semigroup $F(L)={}^sF_r(K)$ of words in the alphabet L. We refer to $F(L)$ as semigroup of loop strings.

It is easy to see that ${}^sBS_r(K)$ is isomorphic to semidirect product of $F(L)$ and affine Cremona semigroup $S(K^s)$.

Let us consider the homomorphism of the group ${}^sBS_r(K)$ into Cremona

Semigroup $S(K^{s+m})$ defined in terms of linguistic graph $I=I^m(K)$. Notice that one can consider graph $I^m(K')$ over the extension K' of K with the usage of the same equations.Let us take $K'=K[x_1, x_2,\dots, x_{m+s}]$ where x_i are formal variables and consider an infinite graph $I^m(K[x_1,x_2,\dots,x_n])$, $n=m+s$

with partition sets $P'=K[x_1,x_2,\dots, x_{m+s}]^{m+s}$and $L'=K[x_1, x_2,\dots, x_{m+s}]^{m+r}$. After that we take a bipartite string $u=(H_0, G_1, G_2, H_3, H_4, G_5, G_6,\dots, H_{t-1}, H_t)$ formed by a totality of multivariate polynomials from the subring $K[x_1, x_2,\dots,x_s]$ of $K[x_1, x_2,\dots,x_n]$ and the point $(x)=(x_1, x_2,\dots, x_n)$ formed by generic elements of K'. This data defines uniquely a skating chain

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

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

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

Lemma 1 [44]. *The map* $\psi={}^I\psi$: ${}^sBS_r(K)\rightarrow S(K^n)$ *is a homomorphism of semigroups.*

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

3.3. Some subsemigroups of symbolic strings and their homomorphic linguistic graphs over commutative rings and skating on them.

We define subsemigroup${}^sGS_r(K)$ of *symbolic ground strings* as a totalityof bipartite strings$u=(H_0, G_1, G_2, H_3, H_4, G_5, G_6,\dots, H_{t-1}, H_t)$ in${}^sBS_r(K)$ with

$H_0=E_0$, $G_1=G_2$, $H_3=H_4$,$G_5=G_6,\dots, H_{t-1}=H_t$and refer to ${}^I\psi({}^sGS_r(K)={}^IGCT(K)$ as *semigroup of ground chain transitions* on linguistic graph I.

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

Lemma 2 [44]. *The homomorphic image* ${}^I\psi({}^sBR_r(K))=BCT_I(K)$ *is a subgroup of affine Cremona group* $C(K^n)$.

Really ${}^I\psi(u\cdot Rev(u))$, $u\epsilon {}^sBR_r(K)$ is an identity map.

We refer to $BCT_I(K)$ as subgroup of bijective chain transitions of linguistic graph I.

4. On semigroups and groups related to Double Schubert graphs and corresponding inverse protocols

4.1. Construction of graphs, related semigroups and their homomorphisms.

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 tuples of $K^{k(k+1)}$ in the lexicographical order.

Remark.

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.

Let us consider the subsemigroup ${}^kY(d, K)$ of ${}^kBS_k(K)$ consisting of strings $u=(H_0, G_1, G_2, H_3, H_4, G_5, G_6, \dots, H_{t-1}, H_t)$ such that maximum of parameters $deg(H_0)+deg(G_1)$, $deg(G_2)+deg(H_3)$, $deg(H_4)+deg(G_5)$,

$deg(G_6)+deg(H_7)$, $deg(G_{t-2})+deg(H_{t-1})$, $deg(H_t)=1$

equals to d, $d>1$.

Theorem 1. *Let $I(K)$ be an incidence relation of Double Schubert graph $DS(k, K)$. Then ${}^I\psi({}^kY(d, K))={}^kU(d,K)$ form a family of stable semigroups of degree d.*

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

New semigroup ${}^kU(d, K)$ consists of transformations of the free module K^t, $t=(k+1)k$. If $d=2$ then ${}^kU(d, K)$ contains semigroups of quadratic transformation defined in [9], which consists of ground chain transitions.

Let J be subset of the Cartesian square of $M=\{1,2,\dots,k\}$. We can identify its element (i,j) with the index ij of Double Schubert Graph $DS(k,K)$.

Proposition 1 [44]. *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 corresponds to complete bipartite graph with the vertex set $K^k U K^k$.

Corollary 1. *Let $I(J, K))$ be an incidence relation of linguistic graph $DS_J(k, K)$. Then ${}^{I(J,K)}\psi({}^kY(d, K))={}^kU_J(d,K)$ form a family of stable semigroups of degree d.*

4.2. Implementation of inverse protocols and their extensions with double Schubert graphs and their symplectic homomorphisms.

Let us consider the implementation of algorithm 2.1 in the case of $S=S'$ and $G=H$. We consider the family of graphs $DS(k, K)$ and form the family $DS_{J(k)}(k, K)$. We assume that $j(k)=|J(k)|$ and $c'(k^2)<j(k)<c(k^2)$ for some constants $0<c'<c<1$. We set $S={}^kS={}^I\psi({}^kY(d, K))={}^kU(d,K)$ which is a subgroup of affine Cremona group $C(K^n)$, $n=k+k^2$ and $G={}^kG={}^kU_J(d,K)<C(K^m)$, $m=k+j(k)^2$. Alice selects elements $u_i=({}^iH_0, {}^iG_1, {}^iG_2, {}^iH_3, {}^iH_4, {}^iG_5, {}^iG_6, \dots, {}^iH_{t-1}, {}^iH_{t(i)})$, $i=1,2, \dots, r$, $r>1$ of subsemigroup ${}^kY(d, K)$ and computes $Rev(u_i)$.

She takes $h\epsilon{}^kY(d, K)$ together with $Rev(h)$. Alice forms elements u_i and $Rev(u_i)=v_i$ and computes $\varphi(hu_iRev(h))=a'_i$ for $\varphi={}^I\psi$.

She takes f from ${}^kY(d, K)$ and forms strings $fRev(u_i)Rev(f)$. Alice computes ${}^{I(J,K)}\psi(f\,Rev(u_i)Rev(f))=b'_i$. She takes invertible affine $j=1,2,\dots,t$ transformations T and L of free modules K^n and K^m of kind and forms pairs $(a_i=Ta'_iT^{-1}, b_i=L\,b_i\,L^{-1})$ and sends them to Bob.

He forms word $w=(a_{i(1)})^{\alpha(1)}(a_{i(2)})^{\alpha(2)}\dots(a_{i(t)})^{\alpha(t)}$, $t>r-1$, $i(j)\epsilon\{1,2,\dots,r\}$, $\alpha(j)>0$, and sends it to Alice. Bob changes alphabet via the substitution of b_i instead of a_i and keeps the reverse word $u=(a_{i(t)})^{\alpha(t)}(a_{i(t-1)})^{\alpha(t-1)}\dots(a_{i(t)})^{\alpha(t)}$.

Alice computes u^{-1} as $L\psi(f)f\sigma(\varphi(h)^{-1}(T^{-1}wT)^{-1}\varphi(h))\psi(f)^{-1}) \cdot L^{-1}$ where $\psi={}^{I(J,K)}\psi$ and σ homomorphism of ${}^kU(d,K)$ onto ${}^kU_J(d,K)$ induced by graph homomorphism δ_J. So Alice and Bob when the protocol ends have mutually inverse encryption/decryption tools u^{-1} and u for the plainspace K^m.

The algorithm is implemented in the cases of $K=Z_p$, $p=2^t$ and $K=F_p$, $p=2^t t=7, 8,\ldots, 32$ for $d=2$.

4. 3. Remarks on complexity.

Let us estimate the complexity of computations for Bob. He need to create two words of finite lengths in corresponding affine Cremona semigroup via several compositions of quadratic polynomials in $n=k^2+2k$ variables**.** It takes him $O(n^7)$ elementary ring operations. Computation of quadratic map in given point of K^n, $n=k^2+2k$ takes time $O(k^6)$. Thus the total complexity of computations for Bob is $O(n^7)$**.**

Let us estimate the complexity of decryption process for Alice. She need computation of product of linear and quadratic maps, product oftwoquadratic maps of densities $O(k^2)$ and $O(k^4)$**,** product of two quadratic maps of densities $O(k^4)$ and $O(k^2)$**.** It requires $O(k^{10})$ operations.

5. On Eulerian semigroups and corresponding inverse protocols

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 ${}^nES(K)$ of transformations of kind $x_1 \to \mu_1 x_1^{a(1,1)} x_2^{a(1,2)} \ldots x_n^{a(1,n)}$, $x_2 \to \mu_2 x_1^{a(2,1)} x_2^{a(2,2)} \ldots x_n^{a(2,n)}$,…,$x_n \to \mu_n x_1^{a(n,1)} x_2^{a(n,2)} \ldots x_n^{a(n,n)}$,where $a(i,j)$ are elements of arithmetic ring Z_d, $d=|K^*|$, $\mu_i \in K^*$.

Let ${}^nEG(K)$ stand for Eulerian group of invertible transformations from ${}^nES(K)$. It is easy to see that the group of monomial linear transformations M_n is a subgroup of ${}^nEG(K)$. So semigroup ${}^nES(K)$ is a highly noncommutative algebraic system. Each element from ${}^nES(K)$ can be considered as transformation of a free module K^n.

The problems of constructions of large subgroups G of ${}^nEG(K)$, pairs (g, g^{-1}), $g\in G$, and tame Eulerianhomomorphisms $\mu: G \to H$, i. e. computable in polynomial time $t(n)$homomorphisms of subgroup G of ${}^nEG(K)$ onto $H<{}^mEG(K)$ are motivated by tasks of Nonlinear Cryptography.

Each element of the semigroup ${}^nES(K)$ is written in the chosen basis $e_1, e_2,\ldots, e_n$.

Let $J=\{i(1), i(2),\ldots, i(k)\}$ be a subset of $\{1,2,..,n\}$and $W_J=<e_{i(1)}, e_{i(2)},\ldots, e_{i(k)}>$ be a corresponding symplectic subspace . We refer to totality ${}^nP_J(K)$ of maps $F \in {}^nES(K)$ preserving W_J as parabolic semigroup of ${}^nES(K)$. The map F from ${}^nP_J(K)$ transforms tuple $(x_{i(1)}, x_{i(2)},\ldots, x_{i(n)})$ according to the rule $x_{i(1)} \to \mu_{i(1)} x_{i(1)}^{a(1,1)} x_{i(2)}^{a(1,2)} \ldots x_{i(k)}^{a(1,k)}$, $x_{i(2)} \to \mu_{i(2)} x_{i(1)}^{a(2,1)} x_{i(2)}^{a(2,2)} \ldots x_{i(k)}^{a(2,k)}$,…, $x_{i(k)} \to \mu_{i(k)} x_{i(1)}^{a(k,1)} x_{i(2)}^{a(k,2)} \ldots x_{i(k)}^{a(2,k)}$.

Let π_J be the restriction of element F from ${}^nP_J(K)$ onto W_J . The map π_J defines canonical homomorphism of ${}^nP_J(K)$ onto ${}^kES(K)$.

6.Conclusion

The usage of stable inverse platforms was discussed in [4]. For instance correpondents can use cubical collision rules keeping in mind attacks by adversary with the interception of plaintext – ciphertext pairs. In the case of plainspace K^n adversary has to intercept $O(n^3)$ pairs to conduct successful linearization attack in time $O(n^{10})$. Thus correspondents can follow natural recommendation to start a new session of the inverse protocol after the exchange of $O(n^2)$ messages. Instead of a new protocol Alice can use idea of deformation rule. She can use same platform to generate its element g together with its inverse g^{-1}, combine g with two affine bijective maps T_1 and T_2, use her encryption map e_A already elaborated during the session of inverse protocol and send $e_A(T_1 gT_2)$ (or $T_1 gT_2(e_A)$) to Bob. He can restore $T_1 gT_2$ and use it as the new encryption rule. Alice can decrypt because of her knowledge of the inverse map.

We believe that the case of single toric inverse algorithm has similarity with the case of stable protocol. Adversary has to intercept set of pairs plaintext /ciphertext of polynomial cardinality to interpolate encryption function.

Research on finding of exact upper bounds is an in interesting task. Other interesting question is about the existence of polynomial algorithm to find the inverse of element g from ${}^nEG(K)$ (or ${}^nEG'(K)$). Similarly to the problem of finding the inverse of bijective multivariable map a polynomial algorithm to invert g is currently unavailable.

Despite the difference in interpolation of encryption functions security of both toric and stable inverse protocols rests on the same difficult word decomposition problem for the large semigroup, which is intractable with ordinary Turing machine and Quantum Computer.

The usage of tandem which consists of toric and stable inverse protocol allows to create ‘’eternal’’ encryption rule similar to public key but not given publicly. Let us assume that toric and stable protocols of tandem algorithm elaborate pairs of maps (${}^{t}e_{A}$, ${}^{s}e_{A}$) and (${}^{t}e_{B}$, ${}^{s}e_{B}$) for Alice and Bob. The problem to interpolate composition ${}^{s}e_{A}({}^{t}e_{A}$), which is non-bijective map of $(K^*)^n$ to K^n of unbounded degree and polynomial density is unfeasible task and decryption function has non polynomial density.

Example of inverse protocols based on toric and stable platforms with outputs acting on $(K^*)^n$ and K^n gives algorithms 5.3 with arbitrary parameter k and l+|J|=n together with algorithm 4.4 with usage graphs $DS(k', K)$ and $DS_{J'}(l',K)$ where $l'+|J'|=n$ and K is a finite field or arithmeticring. Implementation of different from 4.4 stable algorithms is given in [31], [32], [33], alternative to procedure of 5.3 is given in [6].

Notice that in all mentioned above platforms group enveloped inverse Diffie – Hellman protocol [4] can be used instead of inverse protocols 2.1 and 2.2. Recently some new platforms which are formed by families of stable subsemigroups of affine Cremona semigroups have been constructed (see [43], [45], [46]). They can be also used in the combinations with the subsemigroups of Eulerian transformations.

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, September, 2019.

[3] R. J. McEliece, A Public-Key Cryptosystem Based On Algebraic Coding Theory (1978), DSN Progress Report, 44: 114–116.

[4] 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.

[5] V. Ustimenko, On the families of stable transformations of large order and their cryptographical applications, Tatra Mt. Math. Publ., 70 (2017), 107-117.

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

[7] Max Noether, Luigi Cremona , MathematischeAnnalen 59, 1904, p. 1–19.

[8] R. Wagner, M. R. Magyarik, ``A Public-Key Cryptosystem Based on the Word Problem", Advances in Cryptology, Proceedings of CRYPTO '84, Santa Barbara, California, USA, August 19-22, 1984.

[9] V. Ustimenko, On desynchronised multivariate El Gamal algorithm, Cryptology ePrint Archive, 712, 2017.

[10] D. N. Moldovyan and 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.

[11] L. Sakalauskas, P. Tvarijonas and A. Raulynaitis, Key Agreement Protocol (KAP) Using Conjugacy and Discrete Logarithm Problem in Group Representation Level, INFORMATICA, 2007, vol. 18, No 1, 115-124.

[12] 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.

[13] Delaram Kahrobaei and 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.

[14] Alexei Myasnikov; Vladimir Shpilrain and Alexander Ushakov (2008), Group-based Cryptography, Berlin: BirkhäuserVerlag.

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

[16] Benjamin Fine, et. al. "Aspects of Non abelian Group Based Cryptography: A Survey and Open Problems", arXiv:1103.4093.

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

[18] I. Anshel, M. Anshel and D. Goldfeld, An algebraic method for public-key cryptography. Math. Res.Lett. 6(3–4), 287–291 (1999).

[19] S.R. Blackburn and S.D. Galbraith, Cryptanalysis of two cryptosystems based on group actions. In: Advances in Cryptology—ASIACRYPT ’99. Lecture Notes in Computer Science, vol. 1716, pp. 52–61. Springer, Berlin (1999).

[20] K.H. Ko, S.J. Lee, J.H. Cheon, J.W. Han, J.S. Kang and C. Park, New public-key cryptosystem using braid groups. In: Advances in Cryptology—CRYPTO 2000, Santa Barbara, CA. Lecture Notes in Computer Science, vol. 1880, pp. 166–183. Springer, Berlin (2000)

[21] G. Maze, C. Monico and J. Rosenthal, Public key cryptography based on semigroup actions, Adv.Math. Commun. **1**(4), 489–507 (2007).

[22] P.H. Kropholler and S.J. Pride , W.A.M. Othman K.B. Wong, P.C. Wong, Properties of certain semigroups and their potential as platforms for cryptosystems, Semigroup Forum (2010) 81: 172–186.

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

[24] 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.

[25] V. Ustimenko, U. Romanczuk-Polubiec, A. Wroblewska, M. Polak, E. Zhupa, On the constructions of new symmetric ciphers based on non-bijective multivariate maps of prescribed degree,Security and Communication Networks, Volume 2019, Article ID 2137561, 15pages https://doi.org/10.1155/2019/2137561.

[26] V. A. Ustimenko, “On Schubert cells in Grassmanians and new algorithms of multivariate cryptography”, *Tr. Inst. Mat.*, **23**:2 (2015), 137–148.

[27] Vasyl Ustimenko, “On algebraic graph theory and non-bijective multivariate maps in cryptography”, *Algebra Discrete Math.*, **20**:1 (2015), 152–170.

[28] N. Biggs, Algebraic graphs theory, Second Edition, Cambridge University Press, 1993.

[29] V. Ustimenko, Maximality of affine group, hidden graph cryptosystem and graph's stream ciphers, Journal of Algebra and Discrecadete Mathematics, 2005, v.1, pp 51-65.

[30] U. Romańczuk-Polubiec, V. Ustimenko, (2015). On two windows multivariate cryptosystem depending on random parameters// Algebra and Discrete Math., 2015, 19, No. 1, pp. 101-129.

[31] 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 ofAdvances in

Intelligent Systems and Computing (AISC, volume 998), pp, 654-674.

[32] V. Ustimenko, M. Klisowski, On Noncommutative Cryptography and homomorphism of stable cubical multivariate transformation groups of infinite dimensional affine spaces,Cryptology ePrint Archive, 593, 2019.

[33] 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.

[34] Anne Canteaut, François-Xavier Standaert (Eds.), Eurocrypt 2021}, LNCS 12696, 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques Zagreb, Croatia, October 17–21, 2021, Proceedings, Part I, Springer, 2021, 839p.

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

[36] Ward Beullens, Improved Cryptanalysis of UOV and Rainbow, In Eurocrypt 2021, Part 1, pp. 348-373.

[37] Roman'kov V. A. A nonlinear decomposition attack. Groups, Complexity, Cryptology. 2017. Vol. 8, No. 2. P. 197–207.

[38] Romankov V. Two general schemes of algebraic cryptography. Groups, Complexity, Cryptology. 2018. Vol. 10, No. 2. P. 83–98.

[39] Roman'kov V. An improved version of the AAG cryptographic protocol. Groups, Complexity, Cryptology. 2019. Vol. 11, No. 1. 1 2.

[40] Tsaban B. Polynomial time solutions of computational problems in noncommutative algebraic cryptography. Journal of Cryptology. 2015. Vol. 28, No. 3. P. 601–622.

[41] Ben-Zvi A., Kalka A., Tsaban B. Cryptanalysis via algebraic spans. Advances in Cryptology – CRYPTO 2018 / eds.: H. Shachan, A. Boldyreva. Berlin: Springer, 2018. P. 1–20. (LNCS; vol. 109991).

[42] Myasnikov A., Roman'kov V. A linear decomposition attack // Groups, Complexity, Cryptology. 2015. Vol. 7. P. 81–94.

[43] V. Ustimenko, Linear codes of Schubert type and quadratic public keys of Multivariate Cryptography, IACR e-print archive, 2023/175

[44] [V. Ustimenko, Graphs in terms of Algebraic Geometry, symbolic computations and secure communications in Post-Quantum world, University of Maria Curie Sklodowska Editorial House, Lublin, 2022, 198 p.

[45] V. Ustimenko, On Extremal Algebraic Graphs and Multivariate Cryptosystems, IACR e-print archive, 2022/1537

[46] V. Ustimenko, A. Wroblewska, Extremal algebraic graphs, quadratic multivariate public keys and temporal rules, IACR e-print 2023/738.