# On-Time Dependent Linguistic Graphs and Solutions of Postquantum Multivariate Cryptography

Vasyl Ustimenko[1,2] and Oleksandr Pustovit[2]

[1] *University of Royal Holloway in London, Egham Hill, Egham TW20 0EX, United Kingdom*
[2] *Institute of Telecommunications and the Global Information Space of the National Academy of Sciences of Ukraine, 13 Chokolivsky boul., Kyiv, 02000, Ukraine*

**Abstract**

Time dependent linguistic graphs over abelian group $H$ are introduced. Subsemigroups of such endomorphisms together with their special homomorphic images are used as platforms of cryptographic protocols of noncommutative cryptography. The security of these protocol is evaluated via complexity of hard problem of decomposition of Eulerian transformation into the product of known generators of the semigroup. Nowadays the problem is intractable one in the Postquantum setting. The symbiotic combination of such protocols with special graph based stream ciphers working with plaintext space of kind $K^m$ where $m = n^t$ for arbitrarily chosen positive parameter $t$ is proposed. This way we obtained a cryptosystem with encryption/decryption procedure of complexity $O(m^{1+2/t})$.

**Keywords**

Post quantum cryptography, computer algebra, affine Cremona semigroup, Eulerian transformations, linguistic graphs, commutative rings.

## 1. Introduction

Theoretical danger of quantum computers to Information Security has been known since 1994. In the case of asymmetrical cryptography it affects both protocol based cryptosystems for which encryption tools are not given to public and public key cryptosystems.

For instance, a symbiotic combination of Diffie -Hellman protocol (DH) with one time pad encryption or El Gamal cryptosystem in terms of DH algorithm will not be safe in Postquantum era because discrete logarithm problem is not quantum resistant. Popular RSA public key cryptosystem is not quantum secure because factorisation problem can be solved in polynomial time with the usage of quantum computer. Nowadays this vulnerability is not only theoretical because large corporations like IBM, Google, governmental scientific centers in Europe, China, UK, Jappan and USA began to build working quantum computers.

That is why NSA has advised researchers to work on new security products, NIST and ETSI are currently investigating relevant standards and evaluating proposed public key algorithms. Asymmetrical Cryptography is largely based on theoretical complexity assumptions. Fundamental question whether or not $P = NP$ have been open for decades. This assumption is connected with fundamental conjecture of cryptography that there are no polynomial-time algorithms for solving any NP-hard problem.

Such theoretical danger to Cryptography increase interest to problems that are hard to solve in the quantum setting. Noteworthy that many of the fundamental problems about polynomial time problems have analogs at the level of computability. Many NP-hard problems have analogs over various algebraic and combinatorial structures. Techniques from computational or statistical algebra afford insights into the distribution of hard instances.

Post Quantum Cryptography is divided into the following major areas: Code-based cryptography, Lattice-based cryptography, Multivariate cryptography. Hash functions base cryptography, Supersingular elliptic curve isogeny cryptography, Noncommutative Cryptography. This paper is dedicated to a new

CPITS-2022: Cybersecurity Providing in Information and Telecommunication Systems, October 13, 2022, Kyiv, Ukraine
EMAIL: vasulustimenko@yahoo.pl (V. Ustimenko); sanyk_set@ukr.net (O. Pustovit)
ORCID: 0000-0002-2138-2357 (V. Ustimenko); 0000-0002-3232-1787 (O. Pustovit)

branch of Multivariate Cryptography (MC) dealing with polynomial transformations of affine spaces over various commutative rings of unbounded degree and large semigroups or groups of such transformations.

Multivariate cryptography is usually defined as the set of cryptographic schemes using the computational hardness of the Polynomial System Solving problem over a finite field. Solving systems of multivariate polynomial equations is proven to be NP-hard or NP-complete. That is why those schemes are often considered to be good candidates for post-quantum cryptography. Classical Multivariate Cryptography uses systems of quadratic (rarely cubic) equations. The idea to use degree 2 is motivated by possibility to transform system of equations of any constant degree to equivalent quadratic system of large size. Some weakness of this argument is caused by the fact that such transformation can seriously affect the complexity of system.

The first quadratic multivariate scheme based on multivariate equations was introduced by Matsumoto and Imai in 1988. These authors not only introduced a multivariate scheme but in fact a general principle to design public-key cryptosystems using multivariate equations. There are now plenty of proposals based on this principle that are attractive because they offer the possibility to have very short asymmetric signatures that require only a small amount of resources on embedded devices [1–3]. After an intense period of cryptanalysis, few schemes emerged as the most robust solutions: HFE (Hidden Field Equations) and UOV (Unbalanced Oil and Vinegar), both developed by J. Patarin in the late 1990's. Variants of these schemes have been submitted to the post-quantum standardization process for public key algorithms as encryption tools or digital signature instruments organized by NIST. For the third round of this competition in July 2020 NIST does not select multivariate algorithm in the category of encryption instruments. Remaining Unbalanced Oil and Vinegar Rainbow system is investigated as possible digital signature tool.

We believe in the capacity of Multivariate Cryptography (MC) in wide sense as a source of encryption cryptosystems. Recent constructions of families of semigroups and groups of transformation of affine spaces $K^n$ with possibility of computation of n elements from the semigroup in polynomial time gives opportunity to use methods of Semigroup based cryptography in multivariate settings. So instead of one nonlinear transformation of Classical Multivariate Cryptography we can work with several polynomial maps. It allows to construct protocols which security rests on difficult problem to decompose multivariate map into composition of several given generators. If the map and generators are given in a standard form of Multivariate Cryptography then the decomposition task is intractable problem of Post Quantum Cryptography. In fact we work in the area of intersection of MC with the Noncommutative Cryptography which uses complexity of problems from Noncommutative algebra on groups, semigroups, algebras and other algebraic systems [4–21], recently interesting cryptanalytic results have been obtained in this area [22, 23].

The output of the protocol can be used for safe creation of multivariate encryption map or safe delivery of such map from one correspondent to another [6, 24]. This approach can be also used for the construction of digital signatures [6]. Note that protocol based multivariate algorithms essentially differs from traditional for MC public keys. The speed of execution of protocols eseentially differs in the cases of different platforms. In this paper, we continue to use algebraic graphs for the construction of multivariate transformations. We select the case of most efficient *($O(n^3)$)* case of Eulerian transformations [25, 26], and suggest faster algorithm of generation initial data constructed in terms of algebraic graphs theory. We convert the protocol based on Eulerian transformations of affine space $K^n$ to the cryptosystem of El Gamal type which work with potentially infinite tuples of characters of elements from commutative ring K. In fact, the dimension of plaintext space is $m = O(n^t)$ where parameter $t$ is more 1. The symmetric encryption algorithm has complexity $O(m^{1+2/t})$. So, it is possible to work with the large files. We hope that this postquantum cryptosystem can be used instead of symbiotic combination of classical Diffie-Hellman algorithm and one time pad.

In Section 2 we define affine Cremona group and affine Cremona semigroup over general commutative ring $K$ which are central objects of Multivariate Cryptography and Theory of Symbolic Computations. Additionally, we introduce Eulerian semigroup $ES_n(K)$ and group $EG_n(K)$ via endomorphism of $K[x_1, x_2, ..., x_n]$ moving generic variable $x_i$ into monomial term. We define invertable Jordan-Gauss transformations of $EG_n(K)$ as triangular transformation of $(K^*)^n$ with obvious procedure of reimage computation. Semigroup $EG_n(K)$ satisfies to multiple composition property (MCP), which means ability to compute the composition of $n$ elements in polynomial time. Other subgroups of affine Cremona group with MCP can be constructed as stable subgroups formed by elements with maximal degree $d$, where $d$ is constant [27, 28]. Other classes of subsemigroups of $ES_n(K)$ can be defined via the concept of linguistic graph over abelian group $G$ in the case $G = K^*$ and more general concept of a time dependent linguistic graph of type $(s, r,m)$ which is simply a tuple of linguistic graphs of this type. We introduce semigroups ${}^{s}ST_r(K^*)$ of tuples of multivariate maps (elements of Cartesian powers $ES_1(K)$ in the case of $G = K^*$ and $l = r = s$) named as semigroups of symbolic strings. These semigroups are used for the constriction of semigroup ${}^{s,r}SW_m(K^*)$ of symbolic walks on time dependent linguistic graphs. Effectively computable homomorphism ${}^{s,r}SW_m(K^*) \rightarrow ES_n(K)$, $n = m + s$ is presented there. Its image is a special subsemigroup of $ES_n(K)$. This homomorphism and the concept of Jordan- Gauss transformation allows to define Eulerian transformations with inverting accelerator. It can be used as instrument for the development of public keys algorithms. Section 3 presents the concept of homomorphisms of time dependent linguistic graphs over $K^*$. Such graph homomorphism induces homomorphism of corresponding subsemigroups of Eulerian transformations. The description of Tahoma protocol in terms of time dependent graph over $K^*$ and its quotients is also presented there. This section also contains examples of sparse families of time dependent graphs. They can be used for the faster generation of data for the protocol by Alice (creator of protocols data). Finally we present a brief description of symbiotic combination of the protocol and graph based stream cipher working with potentially infinite plaintext space [31].

## 2. On Affine Cremona Semigroups and Semigroups of Special Eulerian Transformations

Let $K[x_1, x_2,\dots, x_n]$ be commutative ring of all polynomials in variables $x_1, x_2,\dots x_n$ defined over a commutative ring $K$. Each endomorphism $F$ of $K[x_1, x_2,\dots, x_n]$ is uniquely determined by its values on formal generators $x_i$, $i = 1, 2,\dots, n$. Symbol $End(K[x_1, x_2,\dots, x_n]) = E_n(K)$ stands for semigroup of all endomorphisms of $K[x_1, x_2,\dots, x_n]$. So we can identify $F$ and the formal rule $x_1 \rightarrow f_1(x_1, x_2,\dots, x_n)$, $x_2 \rightarrow f_2(x_1, x_2,\dots, x_n),\dots, x_n \rightarrow f_n(x_1, x_2,\dots, x_n)$ where $f_i \in K[x_1, x_2,\dots, x_n]$. Element $F$ naturally induces the transformation $\Delta(F)$ of affine space $K^n$ given by the following rule $\Delta(F){:}(\alpha_1, \alpha_2,\dots, \alpha_n) \rightarrow (f_1(\alpha\ 1, \alpha_2,\dots, \alpha_n), f_2(\alpha\ 1, \alpha_2,\dots, \alpha_n),\dots, f_1(\alpha\ 1, \alpha_2,\dots, \alpha_n))$ for each $(\alpha_1, \alpha_2,\dots, \alpha_n) \in K^n$. Luigi Cremona [29] introduced $\Delta(E_n(K)) = CS(K^n)$ which is currently called affine Cremona semigroup. A group of all invertible transformations from $CS(K^n)$ with an inverse from $CS(K^n)$ is known as affine Cremona group $CG(K^n)$ (shortly Cremona group, see, for instance [30]). We refer to infinite $E_n(K)$ as formal affine Cremona semigroup. Density of the map $F_i$ is the maximal number of monomial terms in $f_i$, $i = 1, 2,\dots, n$.

Let $K$ be a finite commutative ring with the unity such that multiplicative group $K^*$ of regular elements of this ring contains at least 2 elements. We take Cartesian power $(K^*)^n$ and consider an Eulerian semigroup $ES_n(K)$ of transformations of kind

$$x_1 \rightarrow \mu_1 x_1^{a(1,1)} x_2^{a(1,2)} \dots x_n^{a(1,n)},$$
$$x_2 \rightarrow \mu_2 x_1^{a(2,1)} x_2^{a(2,2)} \dots x_n^{a(2,n)},$$
$$\dots$$
$$x_n \rightarrow \mu_n x_1^{a(n,1)} x_2^{a(n,2)} \dots x_n^{a(n,n)},$$

where $a(i, j)$ are elements of arithmetic ring $Z_d$, $d = |K^*|$, $\mu_i \in K^*$.

Let $EG_n(K)$ stand for Eulerian group of invertible transformations from $ES_n(K)$.It is easy to see that the group $M_n$ of monomial linear transformations of kind $x_i \rightarrow \mu_i x_{\pi(i)}$, $i = 1, 2,\dots, n$, where $\mu_i \in K^*$and $\pi$ is a permutation on {1,2,…,n}, is a subgroup of $EG_n(K)$. So, semigroup $ES_n(K)$ is a highly noncommutative algebraic system. Each element from $ES_n(K)$ can be considered as transformation of a free module $K^n$.

Let $\pi$ and $\sigma$ be two permutations on the set {1,2,…,n}.

We define transformation $JG_{A,m}(\pi, \sigma)$ which sends $(x_1, x_2,\dots, x_n)$ into $(y_1, y_2,\dots, y_n)$ defined by triangular matrix $A = (a(i; j))$ with integer entries $a(i,j)<d$ and $m=(\mu_1, \mu_2,\dots, \mu_n) \in (K^*)^n$ via the following closed formula.

$$y_{\pi(1)}=\mu_1 x_{\sigma(1)}^{a(1,1)},$$
$$y_{\pi(2)}=\mu_2\, x_{\sigma(1)}^{a(2,1)} x_{\sigma(2)}^{a(2,2)},$$
$$\dots$$
$$y_{\pi(n)}=\mu_n x_{\sigma(1)}^{a(n,1)} x_{\sigma(2)}^{a(n,2)} \dots\ x_{\sigma(n)}^{a(n,1)},$$

where $(a(1; 1); d) = 1, (a(2; 2); d) = 1,\dots, (a(n; n); d) = 1$.

We refer to $JG_{A,m}(\pi, \sigma)$ as Jordan - Gauss multiplicative transformation or simply JG element. It is an invertible element of $ES_n(K)$ with the inverse which is also JG element. The idea to use composition of JG elements or their generalisations with injective maps of $K^n$ into $K^n$ in cryptography was used in [27] $(K = Z_m)$ and [32] $(K = F_q)$. We say that $g$ is a tame Eulerian element over $K$ if it is a composition of several Jordan - Gauss multiplicative maps over commutative ring $K$. It is clear that it sends variable $x_i$ to a certain monomial term. The decomposition of $g$ into product of Jordan - - Gauss transformation allows us to find the reimage of this transformation of $(K^*)^n$

So, tame Eulerian transformations over $K$ are special elements of $EG_n(K)$. We refer to elements of $ES_n(K)$ as multiplicative Cremona elements. Assume that the order of $K$ is a constant. As it follows from the definition the computation of the value of element from $ES_n(K)$ on the given element of $K^n$ is estimated by $O(n^2)$. The product of two multiplicative Cremona elements can be computed in time $O(n^3)$.

Similarly to the case of commutative ring (see [28]) we introduce a linguistic graph $I = \Gamma(G)$ over finite abelian group $G$ defined as bipartite graph with a point set $P = P_{s,m} = G^{s+m}$ and a line set $L = L_{r,m} = G^{r+m}$ as linguistic incidence structure $I=I_{s,r,m}$ if point $x = (x_1, x_2,\ldots, x_s, x_{s+1}, x_{s+2},\ldots, x_{s+m})$ is incident to line $y = [y_1, y_2,\ldots, y_r, y_{r+1}, y_{r+2},\ldots,y_{r+m}]$ if and only if the following relations hold

$$x_{s+1}^{a(1)}y_{r+1}^{b(1)}=q_1w_1(x_1, x_2,\ldots, x_s, y_1, y_2,\ldots, y_r)$$

$$x_{s+2}^{a(2)}y_{r+2}^{b(2)}=q_2w_2(x_1, x_2,\ldots, x_{s+1}, y_1, y_2,\ldots, y_{r+1})$$

$$\ldots$$

$$x_{s+m}^{a(m)}y_{r+1}^{b(m)}=q_mw_m(x_1, x_2,\ldots, x_{s+m-1}, y_1, y_2,\ldots, y_{r+m-1})$$

where $q_j$, $j = 1, 2,\ldots, m$ are elements of $G$, $w_i$ are words in characters $x_i$ and $y_j$ from $G$ and parameters $a(i)$, $b(i)$ are mutually prime with $d = |G|$. Brackets and parenthesis allow us to distinguish points from lines similarly to the case of linguistic graphs over commutative rings.

We define colours $\rho((p))$ and $\rho([l])$ of the point $(p)$ and the line $[l]$ as the tuple of their first coordinates of kind $a = (p_1, p_2,\ldots, p_s)$ or $a = (l_1, l_2,\ldots, l_r)$ and introduce well defined operator $N(v; a)$ of computing the neighbour of vertex $v$ of colour $a \in G^s$ or $a \in G^r$. Similarly to the case of linguistic graph over commutative ring we define colour jump operator $J(p, a)$, $a \in G^s$ on partition set $P$ and $J(l, a)$, $a \in G^r$ on partition set $L$ by conditions $J(p, a) =(a_1, a_2,\ldots, a_s, p_{1+s}, p_{2+s},\ldots, p_{s+n})$ and $J(l, a)=[a_1, a_2,\ldots, a_r, l_{1+r}, l2_{+r},\ldots, l_{r+m}]$.

If $G' > G$ then we can consider graph $I(G')$ of type $(r, s, m)$ with partition sets $P'=(G')^{m+s}$ and $L' = (G')^{m+r}$ given by the same equations with $q_i$ from $G$. Note that group $G'$ can be an infinite one. Let $x_1, x_2,\ldots, x_n$ be the list of variables. We define $G < x_1, x_2,\ldots, x_s >$ as a totality of monomial terms with coefficients from $G$ of kind $gx_1^{a(1)}x_2^{a(2)}\ldots x_n^{a(n)}$, where $a(i)$, $i = 1, 2,\ldots, n$ are elements of $Z_d$, $d = |G|$. We introduce ${}^sB_s(G)$ as $(G < x_1, x_2,\ldots, x_s >)^s$ and ${}^rB_s$ as $G(< x_1, x_2,\ldots, x_s >)^r$. Element $(f_1, f_2,\ldots, fs)$ from ${}^sB_s(G)$ can be identified with the endomorphism $x_1 \rightarrow f_1, x_2 \rightarrow f_2,\ldots, x_s \rightarrow f_s$ of $G < x_1, x_2,\ldots, x_s >$ as a group with the operation given via the following rule $gx_1^{a(1)}x_2^{a(2)}\ldots x_s^{a(s)}\times hx_1^{b(1)}x_2^{b(2)}\ldots x_s^{b(s)}=ghx_1^{a(1)+b(1)}x_2^{a(2)+b(2)}\ldots x_s^{a(s)+b(s)}$.

We assume that $G = K^*$ for the commutative ring $K$. Endomorphism $H \in ES_s(K)$ acts naturally on ${}^rBS_s(K^*)$. The result of action of $H$ on $G$ from ${}^rBS_s(K^*)$ will be written as $G(H)$ or simply $GH$.

We consider the concept of time dependent linguistic graph over commutative group $K^*$.

Let $L_{s,r,m}(K^*) = L(K^*)$ be variety of all linguistic graphs of type $(s, r, m)$ over $K^*$. $F(L_{s,r,m}(K^*)) = F(L(K^*))$ stands for the free semigroup over the alphabet $L(K^*)$. We interpret word $(I(1), I(2),\ldots, I(l)) = F(L)$ as time dependent linguistic graph $I_t(K^*)$ on interval $[1; l]$ and refer to $j$ of $I(j)$ as time parameter. We think that there is a function, given by some Oracle, which establishes coefficients $q_i = q_i(t)$ from $K^*$, $a(i, j) = a(i, j)(t)$ from $Z_d$, $i = 1, 2,\ldots, m$, $j =1, 2,\ldots, m$. Product of $(I(1), I(2),\ldots, I(l))$ with $(I'(1), I'(2),\ldots, I'(p))$ is time dependent graph (shortly t.d.g.) $(I(1), I(2),\ldots, I(l), I(l+1); I'(l+2),\ldots, I'(l+p))$.

Let us define special subsemigroup ${}^sST_r(K^*)$. We consider totality ${}^sST_r(K^*)$ of tuples of kind ${}^tu = u = (H_1, G_1, G_2, H_2, H_3, G_3, G_4, H_4,\ldots, H_{2t-1}, G_{2t-1}, G_{2t}, H_{2t}, H_0)$ where $H_i$ and $G_i$ are elements of ${}^sB_s(G)$ and ${}^rB_s(G)$ respectively of various *rank* $t$, $t \geq 0$. We refer to such tuple ${}^tu$ as symbolic strings of type $(s; r)$ and rank $t = r(u)$.

We define a product of $u = (H_1, G_1, G_2, H_2, H_3, G_3, G_4, H_4,\ldots, H_{2t-1}, G_{2t-1}, G_{2t}, H_{2t}, H_0)$ and

$$v = (\widetilde{H}_1, \widetilde{G}_1, \widetilde{G}_2, \widetilde{H}_2, \widetilde{H}_3, \widetilde{G}_3, \widetilde{G}_4, \widetilde{H}_4, \ldots, \widetilde{H}_{2k-1}\widetilde{G}_{2k-1}, \widetilde{G}_{2k}, \widetilde{H}_{2k}, \widetilde{H}_0)$$

as

$$w = u = (H_1, G_1, G_2, H_2, H_3, G_3, G_4, H_4, \ldots, H_{2t-1}, G_{2t-1}, G_{2t}, H_{2t}, \widetilde{H}_1H_0, \widetilde{G}_1H_0, \widetilde{G}_2H_0, \widetilde{H}_2H_0, \widetilde{H}_3H_0, \widetilde{G}_3H_0, \widetilde{G}_4H_0, \widetilde{H}_4H_0, \ldots, \widetilde{H}_{2k-1}H_0, \widetilde{G}_{2k-1}H_0, \widetilde{G}_{2k}H_0, \widetilde{H}_{2k}H_0, \widetilde{H}_0H_0)$$

So, $r(w) = r(u) + r(v)$.

It is easy to see that this products converts ${}^sST_r(K^*)$ into a semigroup. The totality of symbolic strings of length 1 forms subsemigroup which is isomorphic to $ES_s(K)$. The unity of

$^sST_r(K^*)$ is $(H_0)$ where $H_0$ is the unity of semigroup $ES_s(K)$

Let us consider the pair $(^tu, I_t)$ such that $u_t$ is element of $^sST_r(K^*)$ of rank $t$ and $I_t \epsilon F(L_{r,s,m}(K))$ of length $t$.

Selected time dependent linguistic graph $I = I_t$ from $L_{s,r,m}(K^*)$ defined on the interval $[1, t]$. Let us expand $K^*$ for $R = K^* < x_1,x_2,..., x_{s+m} >$. This change instantly converts t.d.g. $I_t = (I(1), I(2),..., I(t))$ into $I'_t =(I'(1), I'(2),..., I'(t))$ from $F(L_{s,r,m}(R))$. It is easy to see that this products converts $^sST_r(K^*)$ into a semigroup. The totality of symbolic strings of length 1 forms subsemigroup which is isomorphic to $ES_s(K)$. The unity of $^sST_r(K^*)$ is $(H_0)$ where $H_0$ is the unity of semigroup $ES_s(K)$.

We will construct time dependent walk $W(^tu, I_t)$ with colour jumps in the $I't(R)$ which starts in the graph $I(1)$ with selection of initial point $v_0 = (x_1, x_2,..., x_{s+m})$ from $R^{s+m}$. Further construction of the walk is prescribed by symbolic string $u$. During initial time interval (0; 1] we have to compute $J(v_0;H_1) =v_1$, $N(v_1,G_1) = v_2$, $J(v_2;G_2) = v_3$ and $N(v_3;H_2) = v_4$ in the graph $I'(1)$. Doing these computations we use only multiplication of $K^* < x_1, x_2,..., x_{s+m} >$.

Next step corresponds to time interval (1; 2]. We treat the output $v_4$ of computations within interval (0; 1] as point of the graph $I'(2)$.

Now we compute $J(v_4,H_3) = v_5$, $N(v_5,G_3) = v_6$, $J(v_6,G_4) = v_7$ and $N(v_7;H_4) = v_8$ in the graph $I'(2)$.

Continuation of this process subdivided into t steps to the last four vertexes of graph $I'(t)$ given by the list $J(v_{4t-4},H_{2t-1}) = v_{4t-3}$, $N(v_{4t-3},G_{2t-1}) = v_{4t-2}$, $J(v_{4t-2},G_{2t}) = v_{4t-1}$ and $N(v_{4t-1},H_{2t}) = v_{4t}$.

Finally, we compute $v_{4t+1} = J(v_{4t},H_0)$ from $^sB_s(R)$ in the graph $I'(t)$. Noteworthy that output $v_{4t+1}$ is a tuple $(^1H_0,^2H_0,...,^sH_0, F_{s+1}, F_{s+2},..., F_{s+m})$ where $H_0 = (^1H_0, ^2H_0,..., ^sH_0)$, $F_j$ are elements of $K^* < x_1, x_2,..., x_{s+m} >$. The walk $W(t^u, I_t)$ defines the map $\eta(^tu; I_t) =^{s,r}\eta_m$ given by the rule $x_1 \rightarrow {}^1H_0$, $x_2 \rightarrow {}^2H_0,...$, $x_s \rightarrow {}^sH_0$, $x_{s+1} \rightarrow F_{s+1}$, $x_{s+2} \rightarrow F_{s+2},...$, $x_{s+m} \rightarrow F_{s+m}$ from $E_{s+m}(K)$. Let us consider these maps in formal way. We consider a direct product $^{s,r}D_m(K^*)$ of $^sST_r(K^*)$ and $F(L_{r,s,m}(K^*))$ and its subdirect product $^{s,r}SW_m(K^*)$ formed by elements of kind $(^tu, I_t)$.

**Lemma 2.1.** *The $\eta =^{s,r} \eta_m = \eta_m$ is the homomorphism of semigroup of $^{s,r}SW_m(K^*)$ into $ES_n(K)$, $n = s + m$.*

We refer to $^{s,r}SW_m(K^*)$ as space of symbolic walks of type $(s, r)$ and say that $\eta$ is a compression map of this space. We refer to $\eta$ $(^{s,r}SW_m(K^*) =^{s,r} S_m(K^*)$ as chain transition subsemigroup of $ES_{s+m}(K)$ of type $(s, r)$ and to $\eta$ $(u, I_t)$ as chain transition of time dependent linguistic graph $I_t$ with symbolic trace $u$.

Let $^{s,r}GW_m(K^*)$ be subsemigroup of $^{s,r}SW_m(K^*)$ formed by pairs $(^tu, I_t)$ for which $^tu = u$ is a symbolic strings of kind $(H_1, G_1, G_2, H_2, H_3, G_3, G_4, H_4,..., H_{2t-1}, G_{2t-1}, G_{2t}, H_{2t}, H_0)$ where $H_0$ is an element of $EG_n(K)$.

**Lemma 2.2**. *The map $\eta$ induces homomorphism $\tilde{\eta}$ of $^{s,r}GW_m(K^*)$ into $EG_{s+m}(K)$.*

We refer to $\tilde{\eta}(^{s,r}GW_m(K^*))=^{s,r}G_m(K^*)$ as chain transition group of type $(s, r,m)$.

Assume that $\tilde{\eta}(^tu, I_t) = F$ is written in its standard form, $s = O(1)$ and $r = O(1)$. The knowledge of some reimage $\tilde{\eta}$ of kind $(^tu, I_t)$ and $\tilde{H}_0 = (H_0)^{-1}$ allow us to compute $F^{-1}(y)$ in given $y$ in time $O(tn^2)$.

In fact we can form the reverse string $v = (H_{2t}\tilde{H}_0, G_{2t}\tilde{H}_0, G_{2t-1}\tilde{H}_0, H_{2t-1}\tilde{H}_0, H_{2t-2}\tilde{H}_0, G_{2t-2}\tilde{H}_0, G_{2t-3}\tilde{H}_0, H_{2t-3}\tilde{H}_0,..., H_2\tilde{H}_0, G_2\tilde{H}_0, G_1\tilde{H}_0, H_1\tilde{H}_0, \tilde{H}_0)$ and check that $\eta(^tu, I_t)\eta(^tv, \tilde{I}_t), (\tilde{I}_t) = (I(t), I(t-1),..., I(1)$ is an identity map.

Let us consider the data $D$ consisting of symbolic walk $(^tu, I_t)$, where $I_t$ is time dependent graph of type $(s, r,m)$, element $^tu$ *of* $^sGT_r(K^*)$, and two lists of Jordan - Gauss generators of $EG_{s+m}(K)$ formed by $G_1, G_2,..., G_{t(1)}$ and $F_1, F_2,..., F_{t(2)}$ with $t(1) \geq 1$, $t(2) \geq 1$. We say that element $F =G_1G_2...G_{t(1)}\eta(^tu, I_t)F_1F_2,...,F_{t(2)}$ written in its standard form has inverting accelerator $D$. Noteworthy that knowledge of $D$ allows us to find $F^{-1}$ in its standard form in polynomial time in variable $n = m + s$. Pairs of kind $(F,D)$ can be used instead of products of Jordan - Gauss elements for the constructions of public key cryptosystems introduced in [27, 31].

## 3. Special Homomomrphisms of Time Dependent Graphs and Protocols of Noncommutative Cryptography

Let us consider time dependent linguistic graph $I_t = (I(1), I(2),..., I(t))$ over group $K^*$ of type $(r, s, m)$ and parameter $n$, $n < m$. We can define another time dependent linguistic graph $\mu_n(I_t) = (\tilde{I}(1), \tilde{I}(2),..., \tilde{I}(t))$ where $\tilde{I}(j)$, $j =1, 2,..., t$ is obtained from $I(j)$ by deleting the last coordinates $x_{n+s+1}$, $x_{n+s+2},...$, $x_{m+s}$ of points and $y_{n+s+1}$, $y_{n+s+2},...$, $y_{m+s}$ of lines and cancellation of the last $n$ - $m$ equations in the definition of $I_t$. The map $\mu_n$ is the homomorphism of semigroups $F(L_{s,r,m}(K^*))$ onto $F(L_{s,r,n}(K^*))$.

It induces the homomorphism $\pi_n$ of ${}^sST_r(K^*) \times F(L_{s,r,m}(K^*))$ onto ${}^sST_r(K^*) \times F(L_{s,r,n}(K^*))$ acting by the rule $\pi_n(u, I_t) = (u, \mu_n(I_t))$. It is clear that $\pi({}^{s,r}SW_m(K^*) = {}^{s,r}SW_n(K^*)$.

Composition of $\pi_n$ and ${}^{s,r}\eta_n$ defines homomorphism of ${}^{s,r}SW_m(K^*)$ onto ${}^{s,r}S_n(K^*)$

In fact, the diagram formed by maps

$\pi : s,rSW_m(K^*) \rightarrow {}^{s,\,r}SW_n(K^*)$, ${}^{s,r}\eta_m : {}^{s,r}SW_m(K^*) \rightarrow {}^{s,r} S_m(K^*)$,

${}^{s,r}\eta_n : {}^{s,r}SW_n(K^*) \rightarrow {}^{s,r} S_n(K^*)$, $\tau_n : {}^{s,r} S_m(K^*) \rightarrow {}^{s,r} S_n(K^*)$

where $\tau_n$ is the restriction of endomorphism of $K^* < x_1, x_2, \ldots, x_{m+s} >$ on $K^* < x_1, x_2, \ldots, x_{n+s} >$ given by its values on $x_1, x_2, \ldots, x_{n+s}$, is the commutative one.

TAHOMA PROTOCOL (tahoma stands for the abbreviation of "tame homomorphism")

Alice selects positive integers $s, r, m$ and $n, n < m$ together with commutative ring $K$ with the unity. Assume that $m = O(n)$ and $m > \alpha n$ where $\alpha > 1, s \geq 1, r \geq 1, s = 0(1), r = O(1)$. Alice considers semigroup ${}^{s,r}SW_m(K^*)$ and takes its elements $c_1 = ({}^{t(1)}u_1, {}^1I_{t(1)})$, $c_2 = ({}^{t(2)}u_2, {}^2I_{t(2)}), \ldots, c_{k(1)} = ({}^{t(k(1)}u_{t(k(1))}, {}^{k(1)}I_{t(k(1))})$ where $k(1) \geq 2$, $k(1)=O(1)$ , $t(i) \geq 2, i = 1, 2, \ldots, k(1)$.

Additionally, she takes $d_1 = ({}^tu, I_t)$, $I_t = (I(1), I(2), \ldots, I(t))$, $t \geq 2$ from ${}^{s,r}GW_m(K^*)$ with ${}^tu = (H_1, G_1, G_2, H_2, \ldots, H_{4t-1}, G_{4t-1}, H_{4t}, H_0)$ where $H_0$ is Jordan - Gauss element of $EG_s(K)$. She computes $H_0^{-1}, {}^tu' = rev({}^tu), I_t' = (I(t), I(t), \ldots, I(1))$ and $d_1' = ({}^tu', I_t')\cdot$

Alice computes $d_1c_1d_1', d_1c_2d_1', \ldots, d_1c_{k(1)}d_1'$ in the semigroup ${}^{s,r}SW_m(K^*)$. She applies ${}^m\eta$ to these elements and gets $z_1 = \eta_m(d_1c_1d_1'), z_2 = \eta_m(d_1c_2d_1'), \ldots,$ $z_{k(1)}\eta_m(d_1c_{k(2)}d_1'$

Alice takes some Jordan Gauss generators $J_1, J_2, \ldots, J_{k(2)}$, $k(2) \geq 1$, from $EG_{m+s}(K)$ and computes their inverses $J_1', J_2', \ldots, J_{k(2)}'$ and $J_1\ J_2 \ldots\ J_{k(2)}$ together with $J^{-1}$. She forms $a_1 = Jz_1J^{-1}$, $a_2 = Jz_2J^{-1}, \ldots, a_{k(1)} = Jz_{k(1)}J^{-1}$.

Alice computes $\tilde{c}_1 = \eta_n(c_1), \tilde{c}_2 = \eta_n(c_2), \ldots, k(1) = \eta_n(c_{k(1)})\cdot$

She takes $d_2 = ({}^{t'}v, \tilde{I}_{t'})$ from ${}^{s,r}GW_n(K^*)$, where $\tilde{I}_t$ has type $(s, r, n)$, $v = (H_1', G_1', G_2', H_2', \ldots, H_{4t'-1}', G_{4t'-1}', G_{4t'}',$ $H_{4t'}', H_0')$ and forms $rev(d_2) = d_2'$. Alice constructs $y_1 = \eta_n(d_2c_1'd_2'), y_2 = \eta_n(d_2c_2'd_2'), \ldots,$ $y_{k(1)} = \eta_n(d_2c_{k(1)}'d_2')$

She takes some Jordan Gauss generators $G_1, G_2, \ldots, G_{k(3)}$, $k(3) \geq 1$ from $EG_{n+s}(K)$ and computes their inverses $G_1', G_2', \ldots, G_{k(3)}'$ and $G = G_1G_{2k(3)}$ with $G^{-1}$. Alice forms $b_1 = Gy_1G^{-1}$, $a_2 = Gy_2G^{-1}, \ldots, b_{k(1)} = Gy_{k(1)}G^{-1}$.

She sends pairs $(a_i, b_i)$, $i = 1, 2, \ldots, k(1)$ to Bob.

Bob takes tuple $(j(1), j(2), \ldots, j(q))$, $q = O(1)$, $q \geq 2$ where $j(i) \in \{1, 2, \ldots, k(1)\}$ such that $|\{j((1), j(2), \ldots, j(q)\}| \geq 2$. He forms $a = a_{j(1)}a_{j(2)} \ldots a_{j(q)}$ and sends it to Alice. Bob computes $b = b_{j(1)}b_{j(2)} \ldots b_{j(q)}$ and keeps it safely in his private storage.

Alice computes ${}^1a = J^{-1}aJ$, ${}^2a = {}_m(rev(d_1))^1a\eta_m(d_1)$, $\tau_n({}^2a) = {}^1 b$, ${}^2b = \eta_n(d_2)({}^2b)\eta_n(rev(d_2)$ and collision element $b$ as $G({}^2b)G^{-1}$. Note that b is an element $ES_{n+s}(K)$.

**Remark 3.1.** *The security of protocol rests on the complexity of problem of decomposition of element from $ES_n(K)$ in the composition of generators. This problem is an intractable one even in the case of the usage Turing machine jointly with Quantum computer.*

## 4. Examples of Sparse Graphs and Protocol based Cryptosystems

Well known linguistic graph $A(k;K)$ over commutative ring $K$ [27, 28] of type $(1, 1, n - 1)$ is given by equations $x_2 - y_2 = y_1x_1$, $x_3 - y_3 = x_1y_2$, $x_4 - y_4 = y_1x_3$, $x_5 - y_5 = x_1y_4, \ldots, x_k - y_k = y_1x_{k-1}$ in the case of even $k$. We consider linguistic graph $A(k, K^*)$ over commutative group $K^*$ of type (1, 1, k - 1) given by equations $x_2/y_2 = y_1x_1$, $x_3/y_3 = x_1y_2$, $x_4/y_4 = y_1x_3$, $x_5/y_5 = x_1y_4, \ldots, x_k/y_k = y_1x_{k-1}$.

We define class of time dependent graphs $DA_T(k, K^*)$, $T \geq 1$, $k \geq 2$ given by equations $x_2^{a(1,t)}y_2^{b(1,t)} = y_1^{c(1,t)}x_1^{d(1,t)}$, $x_3^{a(2,t)}y_3^{b(2,t)} = x_1^{c(2,t)}y_2^{d(2,t)}$, $x_4^{a(3,t)}y_4^{b(3,t)} = y_1^{c(3,t)}x_2^{d(3,t)}$, $x_5^{a(4,t)}y_5^{b(4,t)} = x_1^{c(4,t)}y_4^{d(4,t)}, \ldots, x_k^{a(k-1,t)}y_k^{b(k-1,t)} = y_1^{c(k-1,t)}x_{k-1}^{d(k-1,t)}$ with $a(i, t), b(i, t), c(i, t), d(i, t)$ from $Z_d - 0$, $d = |K^*|$, $i = 1, 2, \ldots, k - 1$, $t = 1, 2, \ldots, T$ such that $a(i)$ and $b(i)$ are mutually prime with $d$. The graph depends on data $D$ given by parameters $(a(i, t), b(i, t), c(i, t), d(i, t))$, $t \in [1; T]$, $i = 1, 2, \ldots, k - 1$. These graphs were used for the implementation of the protocol together with Jordan - Gauss transformations of kind $J: x_1 \rightarrow qx_1^{m(1)}x_2^{m(2)} \ldots x_k^{m(k)}$, $x_i \rightarrow x_i$, $i = 2, 3, \ldots, k$. In [8] the output of implemented protocol from $ES_{n+1}(K)$

is used for the construction of polynomial encryption map of plaintext space $K^{n^{\alpha}}, \alpha > 1$, which has exponential degree and density. The execution speed is $O(n^{\alpha+2})$. The map is constructed in terms of linguistic graph $A(n^{\alpha};K)$. It is implemented in the case of finite fields of characteristic 2 and $K = Z_{2^l}, l \geq 2$. The security of this cryptosystem rests on the security of the protocol.

## 5. Conclusions

We suggest the method of generation transformations of semigroup ${}^{n}ES(K)$ and group ${}^{n}EG(K)$, where $K$ is finite commutative ring, in terms of time dependent linguistic graphs over commutative group $K^*$. The method can be used for generation of subsemigroups ${}^{n}S<{}^{n}ES(K)$ or subgroups ${}^{n}EG(K)$.

Homomorphisms of time dependent linguistic graphs induce the homomorphisms of corresponding generated semigroups or groups. These effectively computable homomorphisms between two semigroups (or groups) can be used for the data preparation for Postquantum Tahoma Protocol. Its security rests on the complexity of word decomposition problem for subsemigroup of ${}^{n}ES(K)$.

The concept of linguistic graphs over commutative group is traditionally used in graph based cryptography for generation of encryption maps from affine Cremona group $CG_n(K)$. We suggest combination of Tahoma Protocol with output from ${}^{n}ES(K)$ and symmetric protocol based on transformation of $K^n$ defined in terms of linguistic graph over commutative ring $K$. Illustrating example uses known graph $A(n, K)$ for creation of transformation of $K^n$ and time depending analog of graph $A(n, K^*)$ for generation of data for Tahoma protocol. Other examples reader can find in [32].

## 6. References

[1] J. Ding, J. E. Gower, D. S. Schmidt, Multivariate Public Key Cryptosystems. Springer, Advances in Information Security, vol. 25, 2006.

[2] L. Goubin, J. Patarin, B.-Y. Yang, Multivariate Cryptography, Encyclopedia of Cryptography and Security, 2nd Ed., 2011, 824-828.

[3] F. Kipchuk, et al., Investigation of Availability of Wireless Access Points based on Embedded Systems, in VI International Scientific and Practical Conference Problems of Infocommunications. Science and Technology, 2019, pp. 246–250. doi: 10.1109/PICST47496.2019.9061551.

[4] A Myasnikov, V. Shpilrain, A. Ushakov, Noncommutative Cryptography and Complexity of Group-theoretic Problems, Amer. Math Soc. 2011.

[5] J. A. Lopez Ramos, et al., Group Key Management based on Semigroup Actions, Journal of Algebra and its Applications, vol.16 , 2019.

[6] V. Ustimenko, On semigroups of multivariate transformations constructed in terms of time dependent linguistic graphs and solutions of Post Quantum Multivariate Cryptography, Cryptology ePrint Archive, 1466, 2021.

[7] V. Sokolov, P. Skladannyi, H. Hulak, Stability Verification of Self-Organized Wireless Networks with Block Encryption, in Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3137, 2022, pp. 227–237.

[8] L. Sakalauskas, P. Tvarijonas, A. Raulynaitis, Key Agreement Protocol (KAP) Using Conjugacy and Discrete Logarithm Problema in Group Representation Level, Informatica, vol. 18, no. 1, 2007, pp. 115–124.

[9] V. Shpilrain, A. Ushakov, The Conjugacy Search Problem in Public Key Cryptography: Unnecessary and Insufficient, Applicable Algebra in Engineering, Communication and Computing, vol. 17, iss. 3–4, 2006, pp. 285–289.

[10] D. Kahrobaei, B. Khan, A Non-Commutative Generalization of ElGamal Key Exchange Using Polycyclic Groups, in IEEE GLOBECOM Global Telecommunications Conf., 2006. doi: 10.1109/GLOCOM.2006.

[11] A. Myasnikov, V. Shpilrain, A. Ushakov, Group-based Cryptography. Berlin, BirkhäuserVerlag, 2008.

[12] Z. Cao, New Directions of Modern Cryptography. Boca Raton: CRC Press, Taylor & Francis Group, 2012.

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

[14] I. Anshel, M. Anshel, D. Goldfeld, An Algebraic Method for Public-Key

Cryptography. Math. Res. Lett., vol. 6, no. 3–4, 1999, pp. 287–291.

[15] S. R. Blackburn, S. D. Galbraith, Cryptanalysis of Two Cryptosystems based on Group Actions, in: Advances in Cryptology—ASIACRYPT, Lecture Notes in Computer Science, vol. 1716, 1999, pp. 52–61.

[16] C Ko, et al., New Public-Key Cryptosystem using Braid Groups. In: Advances in Cryptology—CRYPTO 2000, Santa Barbara, CA. Lecture Notes in Computer Science, vol. 1880, 2000, pp. 166–183.

[17] G. Maze, C. Monico, J. Rosenthal, Public Key Cryptography based on Semigroup Actions. Adv. Math. Commun., vol. 1, no. 4, 2007, pp. 489–507.

[18] P. H. Kropholler, et al., Properties of Certain Semigroups and Their Potential as Platforms for Cryptosystems, Semigroup Forum, vol. 81, 2010, pp. 172–186.

[19] J. A. Lopez Ramos, et al., Group key Management based on Semigroup Actions, Journal of Algebra and its applications, vol. 16, 2019.

[20] G. Kumar, H. Saini, Novel Noncommutative Cryptography Scheme Using Extra Special Group, Security and Communication Networks, 2017. doi: 10.1155/2017/9036382.

[21] A. Ben-Zvi, A. Kalka, B. Tsaban, Cryptanalysis via Algebraic Span, in: Advances in Cryptology CRYPTO 2018, 38th Annual International Cryptology Conference, part I, vol. 10991, 2018, 255274.

[22] V. Roman'kov, Cryptanalysis of a New Version of the MOR Scheme, 2019. arXiv:1911.00895.

[23] V. Ustimenko, On New Symbolic Key Exchange Protocols and Cryptosystems based on Hidden Tame Homomorphism, Dopovidi. NAS of Ukraine, no. 10, 2018, pp. 26–36.

[24] V. Ustimenko, On Semigroups of Multiplicative Cremona Transformations and New Solutions of Post Quantum Cryptography, Cryptology ePrint Archive, vol. 133, 2019.

[25] V. Ustimenko, On New Multivariate Cryptosystems based on Hidden Eulerian Equations, Reports of Nath Acad of Sci, Ukraine, 2017, pp. 17–24.

[26] V. Ustimenko, On Computations with Double Schubert Automaton and Stable Maps of Multivariate Cryptography, 2021. arXiv:2108.08288.

[27] Max Noether, Luigi Cremona, Mathematische Annalen 59, 1904.

[28] I. Shafarevich, On Some Infinite Dimension Groups II, Izv. Akad. Nauk SSSR Ser. Mat., vol. 45, no. 1, 1981, pp. 214–226.

[29] V. Ustimenko, On New Multivariate Cryptosystems based on Hidden Eulerian Equations over Finite Fields, Cryptology ePrint Archive, 093, 2017.

[30] V. Ustimenko, Graphs in Terms of Algebraic Geometry, Symbolic Computations and Secure Communications in Post-Quantum world, UMCS Editorial House, Lublin, 2022.

[31] A. Bessalov, et al., Analysis of 2-Isogeny Properties of Generalized form Edwards Curves, in: Proceedings of the Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 2746, 2020, pp. 1–13.

[32] D. Moldovyan, N. 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, pp 183–194.