On Multivariate Maps of High Degree for the Post Quantum Protection of Virtual Organizations

Vasyl Ustimenko[1,2,3] and Tymoteusz Chojecki[1]

[1] University of Marie Curie-Sklodowska in Lublin, 5 Plac Marii Curie-Skłodowskiej str., Lublin, 20-031, Poland
[2] Institute of Telecommunications and the Global Information Space of the National Academy of Sciences of Ukraine, 13 Chokolivsky boul., Kyiv, 02000, Ukraine
[3] Royal Holloway University of London, Egham Hill, Egham TW20 0EX, UK

Abstract

The intersection of Commutative and Multivariate cryptography contains studies of cryptographic applications of subsemigroups and subgroups of affine Cremona semigroups defined over finite commutative ring K with the unit. We consider two special families of subsemigroups in a semigroup of all endomorphisms of $K[x_1, x_2, \ldots, x_n]$. They can be used in Post Quantum Cryptography for the development of key exchange protocols of Noncommutative Cryptography with output presented as multivariale map of high degree and density. The security of these schemes is based on a complexity of Conjugacy Power Problem. Suggested schemes can be converted in protocol based cryptosystems of El Gamal type and used for post quantum protection of Virtual Organisations in Global Information Space. Algorithms are implemented in the cases of finite fields of characteristic 2 and arithmetic rings Z_m, $m=2n$, $n=8,16,32$.

Keywords

Multivariate transformations, virtual organization, knowledge base, noncommutative cryptography, multivariate cryptography, graph based cryptography.

CEUR-WS.org/Vol-3288/short14.pdf

1. Introduction

NIST 2017 tender starts the standardisation process of possible Post-Quantum Public keys aimed for purposes to be:

- Encryption tools.
- Tools for digital signatures [1].

In July 2020 the Third round of the competition was started. In the category of Multivariate Cryptography (MC) remaining candidates are easy to observe [2].

For the first task multivariate algorithm were not selected, single multivariate candidate is Rainbow Like Unbalanced Oil and Vinegar (RUOV) In fact RUOV algorithm is investigated as appropriate instrument for the second task [3, 4].

2. Post Quantum, Multivariate and Noncommutative Cryptography and Virtual Organizations

Noteworthy that all multivariate NIST candidates were presented by multivariate rule of degree bounded by constant (2 or 3) of kind $x_1 \to f_1(x_1, x_2, \ldots, x_n)$, $x_2 \to f_2(x_1, x_2, \ldots, x_n)$, ..., $x_n \to f_n(x_1, x_2, \ldots, x_n)$.

In fact RUOV is given by quadratic system of polynomial equations. During Third Round of NIST project [5] some crypto analytical instruments for breaking ROUV were found. So, all multivariate algorithms-candidates were rejected during the project and first four winners were announced in July, 2022. All of them are within the area of Lattice based Cryptography.

We think that these NIST outcomes motivate investigations of alternating options in

CPITS-2022: Cybersecurity Providing in Information and Telecommunication Systems, October 13, 2022, Kyiv, Ukraine
EMAIL: vasulustimenko@yahoo.pl (V. Ustimenko); tymoteusz.chojecki@umcs.pl (T. Chojecki)
ORCID: 0000-0002-2138-2357 (V. Ustimenko); 0000-0002-3294-2794 (T. Chojecki)
© 2022 Copyright for this paper by its authors.
Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).
CEUR Workshop Proceedings (CEUR-WS.org)

Multivariate Cryptography oriented on encryption tools and conducting digital signatures.

(a) To work with plainspace F_q^n and its transformation G of linear degree cn, $c > 0$ on the level of stream ciphers or public keys.

(b) To use protocols of Noncommutative Cryptography with platforms of multivariate transformations for the secure elaboration of multivariate map G from $End(F_q[x_1, x_2, \ldots, x_n])$ of linear or superlinear degree and density bounded below by function of kind cn^r, where $c>0$ and $r>1$.

Recall that density is the number of all monomial term in standard form $x_i \rightarrow g_i(x_1, x_2, \ldots, x_n)$, $i = 1,2,\ldots,n$ of G, where polynomials g_1 are given via the lists of monomial terms in the lexicographical order.

Solution of task (b) can be used for the control access to the portal B of virtual organisation (knowledge base, virtual decision making centre, etc.) via secure communications of portal administrator (Alice) and public user (Bob).

Assume that the information in B is presented in binary alphabet. So we can identify characters of this alphabet with elements of finite field F_q, $q=256$. Portal has a search engine. So, we can assume that the size of the information through the portal is practically unlimited.

Assume that some secure tools are used to protect the entrance of B. To enter the system user need a password which is a tuple E of length n written in alphabet F_q. It has to be changed regularly with the usage of certain period Δ.

We suggest the following access control scheme. Alice and Bob use several session of Postquantum Secure Protocols of Noncommutative Cryptography based on a subsemigroup S of $End\ F_q\ [x_1, x_2, \ldots, x_n]$ to elaborate multivariate map G from S of kind $x_i \rightarrow f_i(x_1, x_2, \ldots, x_n)$, $i = 1,2,\ldots,n$ of degree bounded below by cn, $c>0$ and density bounded below by dn^r where c, d are positive constants and $r > 2$.

The standard form of G can be unknown. This map could be non bijective one. It has to be given with a polynomial algorithm of computation the value of G in given tuple $P = (p_1, p_2, \ldots, p_n)$.

Alice use some pseudorandom generator of tuples for the creation of $P = (p_1, p_2, \ldots, p_n)$ and sends it to Bob via open channel. She enters password $E = G(p_1, p_2, \ldots, p_n)$ to secure the portal.

Bob also computes the tuple E and enters the system. We can assume that data storage B contains a pseudorandom (or genuinely random, obtained via quantum computations) matrix of rows $M_i = (m_{i,1}, m_{i,2}, \ldots, m_{i,n})$, $i \in J$ for some "potentially infinite" set J.

So, Alice and Bob can periodically compute $G(M_i)$ and use this tuple as entrance password.

Additionally they can use G for symmetric communication via one time pad.

Alice writes her plaintext $P=(p_1, p_2, \ldots, p_n)$ from F_q^n. She computes $P + G(M_i)$ and sends it to Bob. He knows M_i as well. So, Bob restores the plaintext.

Surely instead of *one time pad* correspondents can use *other* stream cipher with periodical change of password.

It is naturally to consider more general case of arbitrarily commutative ring K instead of finite field F_q. We will use Algebraic Graphs to generate highly nonlinear automorphisms of $K[x_1, x_2, \ldots, x_n]$ over commutative ring.

For creation of M_i, $i \in J$ ontological technologies can be used. We use files obtained by ontological instruments presenting for example key words of texts with the relations between them in the form of graph (trees or other diagrams). One can combine ontological extraction with hashing technologies to make digests of documents of appropriate size.

We hope that this new application of technologies for special ontological extractions will motivate further research in this important direction.

The task is new because of postquantum protocols with outputs in the form of highly nonlinear map of affine map of K^n to itself appear very recently.

We present one of them below.

3. Multivariate Platforms of Noncommutative Cryptography and Their Applications

Regular algebraic graph $A(n, q) = A(n, F_q)$ is an important object of *Extremal Graph Theory*. In fact we can consider more general graphs $A(n, K)$ defined over arbitrary commutative ring K.

This graph is a 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). It is convenient to use brackets and parenthesis to distinguish tuples from P and L.

So, $(p) = (p_1, p_2, \ldots, p_n) \in P_n$ and $[l] = [l_1, l_2, \ldots, l_n] \in L_n$. The incidence relation $I = A(n,K)$ (or corresponding bipartite graph I) can be given by

condition $p\ I\ l$ if and only if the equations of the following kind hold:

$$p_2 - l_2 = l_1p_1$$
$$p_3 - l_3 = p_1l_2,$$
$$p_4 - l_4 = l_1p_3,$$
$$p_5 - l_5 = p_1l_4, \ldots ,$$
$$p_n - l_n = p_1l_{n-1}$$

for odd n and $p_n - l_n = l_1p_{n-1}$ for even n.

They were intensively used for the constructions of LDPC codes for satellite communications and cryptographic algorithms.

In the case of $K=F_q$, $q > 2$ of odd characteristic graphs $A(n, F_q)$, $n > 1$ form a family of small world graphs because their diameter is bounded by linear function in variable n. We can consider an infinite bipartite graph $A(K)$ with points $(p_1, p_2, \ldots, p_n, \ldots)$ and lines $[l_1, l_2, \ldots, l_n, \ldots]$. If K, $|K| > 2$ is an integrity then $A(K)$ is a tree and $A(n, K)$, $n=2,3,\ldots$ is its algebraic approximation of large girth.

We refer to the first coordinates $p_1=\dot{\rho}((p))$ and $l_1=\dot{\rho}([l])$ as colors of vertices of $A(K)$ (or $A(n, K)$). It is easy to check that each vertex v of the graph has a unique neighbor $N_a(v)$ of selected colour a. So the walk of length $2k$ from vertex $(0,0,\ldots)$ will be given by the sequence $\boldsymbol{w}$ of colours of its elements $b_1, a_1, b_2, a_2, \ldots, b_k, a_k$.

It will be the walk without repetition of edges if $0 \neq a_1$, $a_i \neq a_{i+1}$ and $b_i \neq b_{i+1}$ for $i=1, 2,\ldots, k-1$. So we can identify walks from 0 point of even length point with sequence of kind w. Let $w'=(b'_1, a'_1, b'_2, a'_2, \ldots, b'_s, a'_s)$.We define the composition u of w and w' as the sequence $u=(b_1, a_1, b_2, a_2, \ldots, b_k, a_k, b'_1 + a_k, a_k + a'_1, b'_2 + a_k, \ldots, b'_s + a_k, a'_s + a_k)$. If w and w' are paths and $b'_1 + a_k \neq b_k$ then u is also a path.

Let $B_P(K)$ be a semigroup of all walks with this operation. One can identify empty string with the unity of $B_P(K)$.We use term *branching semigroup* for $B_P(K)$.

3.1. Group Family

Let us take graph $A(n, K)$ together with $A(n, K[x_1, x_2, \ldots, x_n])$. For each element w from $B_P(K)$ we consider a walk $\Delta(w)$ in $A(n, K[x_1, x_2, \ldots, x_n])$ with starting point $(x_1, x_2, \ldots, x_n)$ where x_i are generic elements of $K[x_1, x_2, \ldots, x_n]$ and special colors of vertices $x_1 + b_1$, $x_1 + a_1$, $\ldots$, $x_1 + b_k$, $x_1 + a_k$. Let $p'=dest(\Delta(w))$ be a destination, i. e. a final point of this walk. The destination has coordinates $(x_1 + a_k, f_1(x_1, x_2), f_2(x_1, x_2, x_3), \ldots, f_{n-1}(x_1, x_2, \ldots, x_n)$ where f_1 are elements of $K[x_1, x_2, \ldots, x_n]$. We consider the transformation ${}^n\acute{\eta}(w)$ of $P=K^n$ defined bythe rule $x_1 \rightarrow x_1 + a_k$, $x_2 \rightarrow f_1(x_1, x_2)$, $x_3 \rightarrow f_2(x_1, x_2, x_3)$, $\ldots$, $x_n \rightarrow f_{n-1}(x_1\ x_2, \ldots, x_n)$.This transformation is bijective map of K^n to itself. It is an element of affine Cremona group $CG(K^n)$ of elements from $Aut(K[x_1, x_2, \ldots, x_n])$ acting naturally on K^n. The inverse for this map is ${}^n\acute{\eta}(w)^{-1}$ which coincides with ${}^n\acute{\eta}(w')$ for $w' =Rev(w)=(-a_t, b_1-a_t, a_2-a_t, b_2-a_t, \ldots, b_t-a_t)$.We refer to $Rev(w)$ as reverse string for w from $B_P(K)$.

Proposition 2.1.1 [6]. *The map ${}^n\acute{\eta}$ from $B_P(K)$ to $CG(K^n)$ is a homomorphism of the semigroup into group.*

We refer to ${}^n\acute{\eta}$ as compression map and denote ${}^n\acute{\eta}(B_P(K))$ as $GA(n, K)$. Degree of element g of Cremona group $CG(K^n)$ of kind $x_i \rightarrow g_i(x_1, x_2, \ldots, x_n)$ is the maximal degree of polynomials g_i.

Theorem 2.1.1 [7]. *The maximal degree of multivariate element g* from *GA(n, K) equals 3*.

It means that subgroup G of kind $TGA(n,K)T^{-1}$ where T is an element of $AGL_n(K)$ can be used efficiently as a platform for the implementation of protocols of Noncommutative Cryptography.

3.2. Semigroup Family

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

$$\begin{aligned} &x_1 \rightarrow \mu_1 x_1^{\,a(1,1)} x_2^{\,a(1,2)} \ldots x_m^{\,a(1,n)}, \\ &x_2 \rightarrow \mu_2 x_1^{a(2,1)} x_2^{\,a(2,2)} \ldots x_n^{\,a(2,n)}, \\ &\ldots \\ &x_n \rightarrow \mu_n x_1^{\,a(n,1)} x_2^{\,a(n,2)} \ldots x_n^{\,a(n,n)}, \end{aligned} \qquad (1)$$

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

3.3. Two Platforms in a Tandem

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.

1. Twisted Diffie-Hellman protocol.

Let S be *an abstract semigroup* which has some invertible elements.

Alice and Bob share element $g \in S$ and pair of invertible elements h, h^{-1} from *this semigroup.*

Alice takes positive integer $t = k_A$ and $d = r_A$ and forms $h^{-d}gh^d = g_A$. Bob takes $s = k_B$ and $p = r_B$ and forms $h^{-p}g^sh^p = g_B$. They exchange g_A and g_B and compute collision element X as ${}^Ag = h^{-d}g_B{}^th^d$ and ${}^Bg = h^{-p}g_A{}^s h^p$ respectively.

2. Inverse twisted Diffie-Hellman protocol.

Let S be a group.

Correspondents follow the scheme 1 with the inverse element $g \in {}^nEG(K)$ and Alice sends $h^{-d}g^{-t}h^d = g_A$ to Bob and she gets $h^{-p}g^sh^p = g_B$ from him. They use the same formulae for ${}^Ag$ and ${}^Bg$. But in the new version these elements are mutual inverses. Alice has X but Bob possesses X^{-1}.

Both schemes can be *implemented with the multivariate platforms* $S=TGA(n,K)T^{-1}$ and ${}^nES(K)$.

Algorithm 2.3.1. Correspondents executes pairs of directed twisted DH protocols with platforms $P_1 = {}^nES(K)$ and $P_2 = TGA(n,K)T^{-1}$. Assume that they have outputs H and X.

Each of correspondents have HX of linear degree $\Theta(n)$ and density $\Theta(n^4)$.

They can compute standard form of $G=HX$**,** or use two step procedure to compute $G(p)$ as ${}^1p = H(p)$ and ${}^2p = X({}^1p)$.

Remark 2.3.1 The density of HX is the number of monomial terms of this map in its standard form. It is function of the length of reimage of X under the homomorphism $\acute{\eta}'$ sending u from $B_P(K)$ to $T^n\acute{\eta}(u)T^{-1}$. It depends on $d(HX)=d(X)=l(\acute{\eta}'^{-1}(X))$.

Parameter $d(X)$ depends on k_A, k_B, r_A, r_B, $\acute{\eta}'^{-1}(g)$, $\acute{\eta}'^{-1}(h)$ and linear transformation T of the protocol with the platform $TGA(n,k)T^{-1}$ [8, 9].

Thus, adversary does not able to estimate $d(HX)$.

Results of computer simulation demonstrate connection between $d(HX)$ in the case of field F_q of characteristic 2.

Table 1 corresponds to the case of sparse matrix T eith $2n-1$ no zero entries. Table 2 reflects the case of the matrix with n^2 nonzero entries**.**

Algorithm 2.3.2. Correspondents executes pairs of inverse twisted DH protocols with platforms $P_1 = {}^nES(K)$ and $P_2 = TGA(n,K)T^{-1}$. Assume that Alice has outputs H and X, Bob has H^{-1} and X^{-1} from P_1 and P_2 respectively**.** Correspondents use space of plaintexts $(K^*)^n$ and space of ciphertexts K^n.

Alice and Bob encrypt via HX and $H^{-1}X^{-1}$ and decrypt via XH and $X^{-1}H^{-1}$.

Remark 2.3.2. *In the case of inverse protocols. The access control does not use the extraction of information from knowledge base B. Alice enters the access password P and sends HX(P) it to Bob. He restores the P and enters B.*

Alternatively Bob enters the access password P andsends $H^{-1}X^{-1}(P)$ to *Alice. She restores P and puts as entrance rule to the system.*

Table 1

Density of the map HX of linear degree induced by the graph $\boldsymbol{A(n, F_{2^{32}})}$, case I

	Length of the walk *d(HX)*				
n	**16**	**32**	**64**	**128**	**256**
16	5623	5623	5623	5623	5623
32	53581	62252	62252	62252	62252
64	454375	680750	781087	781087	781087
128	3607741	6237144	9519921	10826616	10826616

Table 2

Density of the map of linear degree induced by the graph $\boldsymbol{A(n, F_{2^{32}})}$, case II

	Length of the walk *d(HX)*				
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

Usage of transformations of kind HX as in algorithm 2 in the form of public key was considered in [10] and [11]. Classical approach of Multivariate Cryptography are presented in [12]. Ideas of fast developing Noncommutative Cryptography reader can find in [13]–[28].

4. Conclusions

Multivariate Cryptography started from studies of bijective transformations G of a vector space $(F_q)^n$. as possible encryption tools. One can increase number of variables n in the equation of kind $G(x) = b$ and rewrite the condition of existence of solution for this equation in the form $G'(y) = b'$ where G' is quadratic transformation of $V = (F_q)^m$ where m is essentially larger than n, y and b' are vectors from V.

The complexity of initial and rewritten systems of equations are essentially differs. Anyway this possibility motivates studies of quadratic maps as tools for Public Key Cryptography.

All algorithms of Multivariate Cryptography under NIST investigation were based on quadratic equations and were not selected as finalists. The first four winners of the NIST competition are described in term of Lattice based Cryptography.

We have to mention that NIST project compares implementations of some public keys as products of Software Engineering. On the level of Theoretical Computer Science all 5 classic direction of Post Quantum Cryptography inclusive Multivariate Cryptography have future perspectives because they are based on known NP-hard problems. One of such problems is about finding solution of nonlinear system of $m = m(n)$ equations in n variables.

We already mention that restriction on the case of quadratic equations is not well motivated. Outcomes of NIST project motivates for search of efficient and secure public keys based on multivariate transformation of unbounded degrees of affine space K^n defined over finite commutative ring K.

Noteworthy that some efficient public keys over finite fields and arithmetical rings Z_m are suggested in [10] and [11]. They use no bijective transformations of K^n of unbounded linear degree $d(n)$. *Crypto analytical instruments for breaking these* algorithms are not founded yet. Other idea to use hard problems of Noncommutative Cryptography in case of platform-semigroups of multivariate transformations is explored in this paper.

5. References

[1] Post-Quantum Cryptography: Call for Proposals, https://csrc.nist.gov/.

[2] V. Grechaninov, et al., Formation of Dependability and Cyber Protection Model in Information Systems of Situational Center, in Workshop on Emerging Technology Trends on the Smart Industry and the Internet of Things, vol. 3149, 2022, pp. 107–117.

[3] 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, July 7, 2020, vol. 2746, pp. 1–13.

[4] A. Bessalov, et al., Implementation of the CSIDH Algorithm Model on Supersingular Twisted and Quadratic Edwards Curves, in Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3187, no. 1, 2022, pp. 302–309.

[5] A. C. François, Xavier Standaert, Eurocrypt 2021, LNCS 12696, 40th Annual International Conference on the Theoryand Applications of Cryptographic Techniques, part I, 2021.

[6] V. Ustimenko, On the Extremal Graph Theory and Symbolic Computations, Dopovidi National Academy of Sci, Ukraine, no. 2, 2013, pp. 42–49.

[7] V. Ustimenko, A. Wroblevska, On the key exchange with nonlinear polynomial maps of stable degree, Annalles UMCS Informatica AI X1, 2, 2011, pp. 81–93.

[8] M. Klisowski, V. Ustimenko, On the Comparison of Cryptographical Properties of Two Different Families of Graphs with Large Cycle Indicator, Mathematics in Computer Science, vol. 6, no. 2, 2012, pp. 181–198.

[9] V. Ustimenko, M. Klisowski, On Noncommutative Cryptography with Cubical Multivariate Maps of Predictable Density, in Computing Conference, Londone, vol. 2, Part of Advances in Intelligent Systems and Computing (AISC), volume 998, 2019, pp. 654–674.

[10] V. Ustimenko, On New Multivariate Cryptosystems based on Hidden Eulerian Equations, Dopov. Nath Acad of Sci, Ukraine, no. 5, 2017, pp 17–24.

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

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

[13] 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.

[14] 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.

[15] 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.

[16] D. Kahrobaei, B. Khan, A non-commutative generalization of ElGamal key exchange using polycyclic groups, in IEEE GLOBECOM Global Telecommunications Conference [4150920], 2006. doi: 10.1109/glocom.2006.
[17] Z. Cao, New Directions of Modern Cryptography. Boca Raton: CRC Press, Taylor & Francis Group, 2012.
[18] B. Fine, et al., Aspects of Non abelian Group Based Cryptography: A Survey and Open Problems, arXiv:1103.4093.
[19] A. Myasnikov, V. Shpilrain, A. Ushakov, Non-commutative Cryptography and Complexity of Group-theoretic Problems. American Mathematical Society, 2011.
[20] I. Anshel, M. Anshel, D. Goldfeld, An Algebraic Method for Public-Key Cryptography, Math. Res. Lett. 6(3–4), 1999, pp. 287–291.
[21] S. R. Blackburn, S. D. Galbraith, Cryptanalysis of Two Cryptosystems based on Group Actions, in Advances in Cryptology—ASIACRYPT'99. Lecture Notes in Computer Science, vol. 1716, 1999, pp. 52–61.
[22] P. H. Kropholler, et al., Properties of Certain Semigroups and Their Potential as Platforms for Cryptosystems, Semigroup Forum 81, 2010, pp. 172–186.
[23] J. A. Lopez Ramos, et al., Group Key Management based on Semigroup Actions, Journal of Algebra and Its Applications, vol. 16, 2019.
[24] A. G. Myasnikov, A. Roman'kov, A Linear Decomposition Attack, Groups Complex. Cryptol., vol. 7, no. 1, 2015, pp. 81–94.
[25] V. A. Roman'kov, A Nonlinear Decomposition Attack, Groups Complex. Cryptol., vol. 8, no. 2, 2016, pp. 197–207.
[26] V. Roman'kov, An improved version of the AAG cryptographic protocol, Groups, Complex., Cryptol, 11, No. 1 (2019), 35-42.
[27] A. Ben-Zvi, A. Kalka, B. Tsaban, Cryptanalysis via Algebraic Span, in Advances in Cryptology, CRYPTO, 38th Annual International Cryptology Conference, part I, vol. 10991, 2018, pp. 255–274.
[28] B. Tsaban, Polynomial-time solutions of computational problems in noncommutative-algebraic cryptography, J. Cryptol. 28, No. 3 (2015), 601-622.