UDC 519.1, 514.128

Extremal graph theory and generation of quadratic multivariate transformations of Algebraic Post-Quantum Cryptography

Vasyl Ustymenko[1], Aneta Wróblewska[3] and Oleksandr Pustovit[2]

[1] *Royal Holloway University of London, United Kingdom.*
[2] *Institute of telecommunications and global information space, Kyiv, Ukraine*
[3] *University of Maria Curie-Skłodowska, Lublin, Poland*

Abstract
We introduce large groups of quadratic transformations of a vector space over the finite fields defined via symbolic computations with the usage of algebraic constructions of Extremal Graph Theory. They can serve as platforms for the protocols of Noncommutative Cryptography. The modifications of these symbolic computations in the case of large fields of characteristic two allow us to define quadratic bijective multivariate public keys such that the inverses of public maps has a large polynomial degree. We suggest the usage of constructed protocols for the private delivery of quadratic encryption maps instead of the public usage of these transformations.

Keywords: Multivariate Cryptography, Extremal Graph Theory, Quadratic multivariate rules, Noncommutative Cryptography

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

Introduction: On Post Quantum, Multivariate and Noncommutative Crytography

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. PQC is subdivided into Coding based Cryptography, Multivariate Cryptography, Noncommutative Cryptography, Hash based Cryptography. Isogeny based Cryptography and Lattice based Cryptography.

Each of these six areas is based on the complexity of certain *NP* - hard problem. Noteworthy that fundamental assumption of cryptography that there are no polynomial-time algorithms for solving any *NP*-hard problem remains valid. So all six directions are well justified theoretically.

The tender of US National Institute of Standartisation Technology (NIST, 2017) is dedicated to the standardisation process of possible real life Post-Quantum Public keys. Already selected in July of 2022 four cryptosystems are developed via methods of Lattice based Cryptography. This fact motivates researchers from other four core areas of Post Quantum Cryptography to continue design of new cryptographical primitives. Noteworthy that during the NIST project an interesting results on cryptanalysis of Unbalanced Rainbow Oil and Vinegar digital signatures schemes were found (see [1], [2], [3]). This scheme is defined via quadratic multivariate public rule, which refers to MiniRank problem. Examples of previously knowm multivariate quadratic public keas reader can find in classical monographs [4], [5], [6]

Graph based multivariate public keys with bijective encryption maps generated via special walks on incidence graph of projective geometry were proposed in [7] this year. It can be count as attempt to combine methods of Coding based and Multivariate Cryptographies.

Classical multivariate public rule is a transformation of n-dimensional vector space over finite field F_q which move vector $(x_1, x_2, \ldots, x_n)$ to the tuple $(g_1(x_1, x_2, \ldots, x_n), g_2(x_1, x_2, \ldots, x_n), \ldots, g_n(x_1, x_2, \ldots, x_n))$, where polynomials g_i are given in their standard forms, i. e. lists of monomial terms in the lexicographical order. The degree of this transformation is the maximal value of $deg(g_i)$. Traditionally public rule has degree 2 or 3.

We use the known family of graphs $D(n, q)$ and $A(n.q)$ of increasing girth (see [8], [9] and further references) and their analogs $D(n, K)$ and $A(n, K)$ defined over finite commutative ring K with unity for the construction of our public keys. Noteworthy to mention that for each prime power q, $q > 2$ graphs $D(n, q)$, $n = 2, 3,...$ form a family of graphs of large girth (see [8]). There is well defined projective limit of these graphs which is a q-regular forest. In fact if K is an integral domain both families $A(n, K)$ and $D(n, K)$ are approximations of infinite dimensional algebraic forests. Cubical transformation groups $GA(n, K)$ and $GD(n, k)$ of K^n (see [10], [11]), were used for the design of key exchange protocols of Noncommutative Cryptography (see [12], [13], [11]), elements of this groups were used for the creation of stream ciphers.

1. On graphs, groups and quadratic maps with the inverses of high degree

Let K be a commutative ring .We define $A(n, K)$ as bipartite graph with the point set $P=K^n$ and line set $L=K^n$ (two copies of a Cartesian power of K are used). We will use brackets and parenthesis to distinguish tuples from P and L. So $(p)=(p_1, p_2, \dots, p_n) \in P_n$ and $[l]=[l_1, l_2, \dots, l_n] \in L_n$. The incidence relation $I=A(n,K)$ (or corresponding bipartite graph I) is given by condition $p\ I\ l$ if and only if the equations of the following kind hold. $p_2 - l_2=l_1p_1, p_3 - l_3= p_1 l_2, p_4 - l_4 = l_1p_3, p_5 - l_5 = p_1 l_4, \dots, p_n - l_n = p_1 l_{n-1}$ for odd n and $p_n - l_n = l_1 p_{n-1}$ for even n. We can consider an infinite bipartite graph $A(K)$ with points $(p_1, p_2, \dots, p_n, \dots)$ and lines $[l_1, l_2, \dots, l_n, \dots]$. We proved that for each odd n girth indicator of $A(n, K)$ is at least $2n+2$.

Another incidence relation $I= D(n, K)$ is defined below. The following interpretation of a family of graphs $D(n. K)$ in case of general commutative ring K is convenient for the computations. Let us use the same notations for points and lines as in previous case of graphs $A(n, K)$.

Points and lines are elements of two copies of the affine space over K. Point $(p)=(p_1, p_2, \dots, p_n)$ is incident with the line $[l]=[l_1, l_2, \dots, l_n]$ if the following relations between their coordinates hold: $p_2 - l_2=l_1p_1$, $p_3 - l_3= p_1 l_2$, $p_4 - l_4 = l_1p_3$, ..., $l_i-p_i=p_1l_{i-2}$ if i congruent to 2 or 3 modulo 4, $l_i-p_i=l_1p_{i-2}$ if i congruent to 1 or 0 modulo 4.

Let $\Gamma(n, K)$ be one of graphs $D(n, K)$ or $A(n, K)$. The graph $\Gamma(n, K)$ has so called linguistic colouring ρ of the set of vertices. We assume that $\rho(x_1, x_2, \dots, x_n)=x_1$ for the vertex x (point or line) given by the tuple with coordinates $x_1, x_2, \dots, x_n$. We refer to x_1 from K as the colour of vertex x. It is easy to see that each vertex has a unique neighbour of the chosen colour. Let N_a and J_a be operators of taking the neighbour with colour a and jump operator changing the original colour of point or line for new colour a from K. Let $[y_1, y_2, \dots, y_n]$ be the line y of $\Gamma(n, K[y_1, y_2, \dots, y_n])$ and $(\alpha(1), \alpha(2), \dots, \alpha(t))$ and $(\beta(1), \beta(2), \dots, \beta(t))$ are the sequences of colours of the length at least 2. We form $(\beta^*(1), \beta^*(2), \dots, \beta^*(t))=(y_1+\beta(1), y_1+\beta(2), \dots, y_1+ \beta(t))$ and consider the sequence ${}^0v=y$, ${}^1v=J_{\alpha(1)}({}^0v)$, ${}^2v=N_{\beta^*(1)}({}^1v)$, ${}^3v=N_{\alpha(2)}({}^2v)$, ${}^4v=N_{\beta^*(2)}({}^3v)$, … , ${}^{2t-2}v=N_{\beta^*(t-1)}({}^{2t-3}v)$, ${}^{2t-1}v=N_{\alpha(t)}({}^{2t-2}v)$, ${}^{2t}v=J_{\beta^*(t)}({}^{2t-1}v)$.

Assume that $v={}^{2t}v=[v_1, v_2, \dots, v_n]$ where v_i are from $K[y_1, y_2, \dots, y_n]$. We consider bijective quadratic transformation $g(\alpha(1), \alpha(2), \dots, \alpha(t), \beta(1), \beta(2), \dots, \beta(t))$, $t \geq 2$ of affine space K^n of kind $y_1 \to y_1 + \beta(t)$, $y_2 \to v_2(y_1, y_2)$, $y_3 \to v_3(y_1, y_2, y_3)$, … , $y_n \to v_n(y_1, y_2, \dots, y_n)$.

It is easy to see that $g(\alpha(1), \alpha(2), \dots, \alpha(t), \beta(1), \beta(2), \dots, \beta(t))\bullet g(\gamma(1), \gamma(2), \dots, \gamma(s), \sigma(1), \sigma(2), \dots, \sigma(t))= g(\alpha(1), \alpha(2), \dots, \alpha(t), \gamma(1), \gamma(2), \dots, \gamma(s), \beta(1), \beta(2), \dots, \beta(s), \sigma(1)+\beta(t), \sigma(2)+\beta(t), \dots, \sigma(s)+ \beta(t))$.

Theorem 1 (see [11] and further references**)** *Bijective transformations of kind* $g(\alpha(1), \alpha(2), \dots, \alpha(t), \beta(1), \beta(2), \dots, \beta(t))$, $t \geq 2$ *generate a stable subgroup* ${}^2G(\Gamma(n, K))$ *of transformations of* K^n *of degree 2.*

Remark *In the case of two quadratic transformations of K^n of ''general position'' their composition will have degree 4.*

We associate with the sequence $\alpha(1), \alpha(2), \dots, \alpha(t), \beta(1), \beta(2), \dots, \beta(t)$ another quadratic transformation $h=H(\alpha(1), \alpha(2), \dots, \alpha(t), \beta(1), \beta(2), \dots, \beta(t))$ constructed via the sequence of vertices ${}^0v$, ${}^1v$, ${}^2v$, , … , ${}^{2t-2}v=N_{\beta^*(t-1)}({}^{2t-3}v)$, ${}^{2t-1}v=N_{\alpha(t)}({}^{2t-2}v)$. We compute ${}^{2t}v=J_{a(t)}({}^{2t-1}v)=v$ where $a(t)=(y_1)^2 + \beta(t)$ and define h as the quadratic map $y_i \to v_i$, $i=1, 2, \dots, n$.

Theorem 2 (see [16]) *Let K be the finite field F_q, $q=2^r$. Then transformation $h=h(\alpha(1), \alpha(2), \dots, \alpha(t), \beta(1), \beta(2), \dots, \beta(t))$ is a quadratic transformation of the vector space $(F_q)^n$. The* *polynomial degree of its inverse transformation is at least* 2^{r-1}.

2. Protocols and cryptosystems

2.1. Twisted Diffie-Hellman protocol with the platform $^2G(\Gamma(n, Fq)), q>2$

Let $^2G(\Gamma(n, F_q))=G$ be the transformation group of Theorem 1. So the following twisted Diffie – Hellman protocol of Noncommutative Cryptography is feasible.

Alice and Bob will use elements of $Y= \tau G\tau^{-1}$ where $\tau \in AGL_n(F_q)$. They take element $x = g(\alpha(1), \alpha(2),\dots , \alpha(t), \beta(1), \beta(2) , ..., \beta(t)), t \geq 2$ from Y and representative $y=(g(\gamma(1), \gamma(2),\dots \gamma(s), \sigma(1), \sigma(2), ..., \sigma(s))$ from this group and makes them public. We assume that $\alpha(i)\neq \alpha(i+1), \beta(i)\neq \beta(i+1), i=1,2, ..., t-1, \gamma(i)\neq \gamma(i+1), \alpha(i)\neq \sigma(i+1),), i=1,2, ..., s-1$.

Alice selects rather big numbers $k(A)$ and $r(A)$. She sends $x(A)= y^{r(A)}x^{k(A)}y^{-r(A)}$ written in its standard form to Bob.

Bob selects his numbers $k(B)$ and $r(B)$. He forms the standard form of $x(B)= y^{r(B)}x^{k(B)}y^{-r(B)}$ and sends it to Alice.

Correspondents Alice and Bob computes the collision map C as $y^{r(A)}x(B)^{k(A)}y^{-r(A)}$ and $y^{r(B)}x(A)^{k(A)}y^{-r(A)}$. Noteworthy that C is a quadratic map from the group of kind y_n $y_1\to c_1(y_1, y_2,\dots, y_n), y_2\to c_2(y_1, y_2,\dots,),\dots, y_n\to c_n(y_1, y_2,\dots, y_n)$. One can take tuples ^iC of nonzero coefficients of taken in the lexicographical order and form the concatenation ***c*** of them.

Remark *It is easy to see that the complexity of the protocol coincides with the complexity of the computation of the composition of two quadratic transformations of n-dimensional vector space and equals* $O(n^7)$.

2.2. Stream cipher supported by the protocol

Correspondents Alice and Bob can choose potentially infinite parameter m, $m\geq l(n)$ where $l(n)$ is the length of vector c.

After the completion of the presented above protocol they concatenate tuple c of $[m/([l(n)]+1)$ and form the vector $b= b(c)=(b_1, b_2, ..., b_m)$ containing first m coordinates of obtained tuple. They take coordinates of b in the reverse order and form vector b^* of length m.

They select parameter t, $t\geq n$ of size $O(1)$. Let $^tb=(\alpha(1), \alpha(2),\dots , \alpha(t))$ and $^tb^*=(\beta(1), \beta(2) , ... , \beta(t))$ be vectors formed by t first coordinates of b and b^* and consider the recurrent usage of a composition of ^1T, $h=h(\alpha(1), \alpha(2),\dots , \alpha(t), \beta(1), \beta(2) , ..., \beta(t))$ of Theorem 2 and ^2T , where ^1T and ^2T are linear transformation sending y_1 to $b_1y_1+b_2y_2+\dots+b_my_m$ and $b^*_1y_1+b^*_2y_2+\dots+b^*_m$ respectively and leaving of coordinates y_i, $i=2, 3,\dots, m$.

So, correspondents work with the space of plaintexts (F_q). They can agree on the parameter t via open channel. The password $b(c)$ is computed via vector c of length $O(n^3)$. Plaintext is converted into ciphertext via usage of two sparse linear operators with complexity $O(m)$**,** two operators of changing colour of complexity $O(1)$ and several operators of taking neighbour of chosen colour with complexity $O(m)$. So fast encryption/decryption procedure takes time $O(m)$.

Remark *Multivariate map* $^1T\ h\ ^2T$ *has inverse of polynomial degree at least* 2^{r-1}. *So if* $r \geq 16$ *then the stream cipher is resistant to a differential linearisation attacks. We implement the case with* $r=32$.

2.3. Quadratic Multivariate Public Key

Alice selects finite field F_q, $q=2^r$**,** dimension n of the vector space over F_q, ^1T and ^2T from $AGL_n(F_q)$ defined by matrices with most entries distinct from zero. She chooses parameter $t=O(n)$, elements $\alpha(1), \alpha(2),\dots , \alpha(t), \beta(1), \beta(2) , ..., \beta(t)$ for which $\alpha(i)\neq \alpha(i), \beta(i) \neq\beta(i+1), i=1, 2, ..., n$ and compute the standard form of $F= {}^1Th(\alpha(1), \alpha(2),\dots , \alpha(t), \beta(1), \beta(2) , ..., \beta(t))^2T$.

She presents F of kind $y_i\to f(y_1, y_2, ..., y_n)$, $i=1, 2, ..., n$ as public map. Public user Bob use this transformation to encrypt his plaintext p in time $O(n^3)$. Alice knows the decomposition $^1T\ h\ ^2T$ and sequences $\alpha(i)$ and $\beta(i)$, $i=1, 2\dots , t$. It allows her to decrypt in time $O(n^2)$.

Remark (the periodic privatization of public rule) Alice creates bijective G according presented above method. Together with Bob she executes algorithm 2.1 to elaborate the collision map and sends $C+G$ to his partner. So correspondents can use ”public key rule” G in a private mode. The usage of G just $t(n)=[n^2/2]$

times for the message encryption or electronic signatures times does not allow adversary to make the restoration of *G*. After the exchange of *t(n)* vectors correspondents can start the new session of the execution of procedures 2.1 and 2.2.

2.4. Remark on the implementation

We use computer simulation to generate maps of kind $y = \tau_1 h=h(\alpha(1), \alpha(2),\dots , \alpha(t), \beta(1), \beta(2) , \dots, \beta(t))\ \tau_2(x)$ related to graphs $A(n, K)$ and $D(n, K)$, K is one of the commutative rings: Boolean ring h $B(32)$, modular ring Z_q, $q=2^{32}$ and finite field F_q, $q=2^{32}$.

We have implemented three cases of invertible affine transformations:

1) τ_1 and τ_2 are identities, this is just evaluation of time execution of core quadratic transformation,

2) τ_1 and τ_2 are of kind $x_1 \rightarrow x_1 + a_2 x_2 + a_3 x_3 + \dots + a_n x_n$ (linear time of computing execution of τ_1 and τ_2),

3) $\tau_1 = A_1x+b_1$ and $\tau_2 = A_2x+b_2$, nonsingular matrices A_1, A_2 have nonzero entries and column vectors b_1, b_2 with mostly all coordinates differ from zero

Standard forms of the maps in the cases 2 and 3.

The program is written in C++ and compiled with the gcc compiler. We used an average PC with processor Pentium 3.00 GHz, 2GB memory RAM and system Windows 7.

Tables 1–6 presents the time of encryption with symmetric algorithm and three different commutative rings.

Table 1
Generation time for the map (ms) $D(n,F_2^{32})$, case I

	length of the the path (2t-2)				
n	**16**	**32**	**64**	**128**	**256**
16	10	22	30	50	98
32	60	138	289	590	1189
64	1042	2259	4831	9983	20267
128	15819	33844	74338	160211	331893

Table 2
Generation time for the map (ms) $D(n,F_2^{32})$, case II

	length of the path (2t-2)				
n	**16**	**32**	**64**	**128**	**256**
16	25	45	97	209	417
32	281	645	1369	2813	5709
64	3226	8394	19451	41565	85780
128	55072	139364	357359	824163	1758056

Table 3
Generation time for the map (ms) $D(n,F_2^{32})$, case III

	length of the word				
n	**16**	**32**	**64**	**128**	**256**
16	71	136	263	518	1030
32	1220	2324	4535	8962	17824
64	21884	40412	77476	151587	299839
128	453793	812136	152678	2946017	5792884

Table 4
Generation time for the map (ms) $A(n,F_2^{32})$, case I

	length of the word				
n	**16**	**32**	**64**	**128**	**256**
16	4	11	22	46	93
32	53	130	286	597	1230
64	992	298	4642	10065	20931
128	15642	33487	74242	167452	364704

Table 5
Generation time for the map (ms) $A(n,F_2^{32})$, case II

	length of the word				
n	**16**	**32**	**64**	**128**	**256**
16	18	57	125	257	538
32	306	786	1773	3758	7713
64	3190	8856	23228	53193	113146
128	54029	137191	368458	950847	2164035

Table 6
Generation time for the map (ms) $A(n,F_2^{32})$, case III

	length of the word				
n	**16**	**32**	**64**	**128**	**256**
16	73	146	285	573	1145
32	1266	2417	4698	9265	18403
64	22142	40945	78549	153781	304237
128	460198	819495	1532275	2970741	5836936

Conclusions

Recall that multivariate public rule is a transformation of n-dimensional affine space over commutative ring K with unity which move a tuple $(x_1, x_2, \dots, x_n)$ to the tuple $(g_1(x_1, x_2, \dots, x_n), g_2(x_1, x_2, \dots, x_n), \dots, g_n(x_1, x_2, \dots, x_n))$, where polynomials g_i from $K[x_1, x_2, \dots, x_n]$ are given in their standard forms, i.e. lists of monomial terms in the lexicographical order. We are working in the area of intersection of Multivariate and Noncommutative Cryptographies. So groups formed by multivariate transformations are important for us and the following algebraic terminology is useful to interprete our results on Theoretical Computer Science.

Affine Cremona Group ${}^nCG(K)$ is defined as automorphism group of polynomial ring $K[x_1, x_2, \dots, x_n]$ over the commutative ring K. It is an important object of Algebraic Geometry (see Max Noether paper [14] about mathematics of Luigi Cremona - prominent figure in Algebraic Geometry in XIX). Element of the group σ can be given via its values on variables, i. e. as the rule $x_i \rightarrow f_i(x_1, x_2, \dots, x_n)$, $i=1, 2, \dots, n$. This rule induces the map σ': $(a_1, a_2, .., a_n) \rightarrow (f_1(a_1, a_2, .., a_n), f_2(x_1, x_2, \dots, x_n), \dots, f_n(x_1, x_2, \dots, x_n))$.

Results about subgroups of ${}^nCG(K)$ (or subsemigroups of ${}^nCS(K)$) such that computation of the superposition of arbitrary n elements can be completed for polynomial time can be used as so called platforms of Noncommutative Cryptography.

Let us assume that element σ is given via so called standard form, i. e. some of monomial terms listed in the lexicographical order.

We say the piece of information T is a *trapdoor accelerator* for nonlinear σ if the knowledge of T allows us to compute the reimage of given value b in time $O(n^2)$ (see [15]). If T can be given in a form of tuple $(a_1, a_2, \dots, a_{f(n)})$, $a_i \in K$ we say that σ has *affine trapdoor accelerator.*

Of course it is just an instrument to search for practical trapdoor functions for which without knowledge of secret T the computation of reimage in polynomial time is impossible.

The existence of theoretical trapdoor functions is closely related to the open conjecture that $P \neq NP$.

The following *inverse problem* is an interesting for applications. Assume that σ_n is a family of quadratic or cubic elements of ${}^nCG(K)$ given in the standard form and it has hidden trapdoor accelerator. Find some trapdoor accelerator for this map.

Noteworthy that somebody has to find an algorithm to compute the reimages of σ_n in time $O(n^2)$. Note if $\sigma^{-1}{}_n$ is known in its standard form then it gives the computation of reimage in time $O(n^3)$ and $O(n^4)$ in cases of degree *2* and *3*. *The following statement is instantly follows from Theorem 1.*

Corollary 1 *For each commutative ring K with unity and* $n \geq 2$ *there is a subgroup* $X_n(K)$ *of degree 2 in* ${}^nCG(K)$ *such that each its nonlinear representative has an affine trapdoor accelerator and each tuple* $(a_1, a_2, .., a_{n2s})$, $s \geq 2$ *with nonzero coordinatess can serve as a trapdoor accelerator of quadratic representative of this subgroup.*

Another construction which satisfies to this statement the reader can find in [7]. From Theorem 2 we deduce the following statement.

Corollary 2 *Let K be the finite field* F_q, $q=2^r$. *Then there is a quadratic transformation of the vector space* $(F_q)^n$ *with affine accelerator such that polynomial degree of the inverse transformation is at least* 2^{r-1}.

These propositions insure existence of important platform of Noncommutative Cryptography, which can be used in various protocols and El. Gamal Cryptosystems (see [12]-[15] and [17]-[27]). Important feature of the multivariate platforms is their description as tansformations groups which does not use generators and relations.

References

[1] 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..

[2] 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.

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

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

[5] Jintai Ding, Albrecht Petzolt, Dieter S. Schmidt, Multivariate Public Key Cryptosystems, Springer, ADIS, vol.80, 2020.

[6] N. Koblitz, Algebraic aspects of cryptography, Springer (1998), 206 p.

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

[8] F.Lazebnik V. Ustimenko and A.J.Woldar, A new series of dense graphs of high girth, Bulletin of the AMS 32 (1) (1995), 73-79.

[9] V. A. Ustimenko On the extremal graph theory and symbolic computations, Dopovidi National Academy of Sci, Ukraine, 2013, No. 2, p. 42-49.

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

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

[12] Alexei G. Myasnikov, Vladimir Shpilrain, Alexander Ushakov. Non-commutative Cryptography and Complexity of Group-theoretic Problems, AMS, 2011

[13] 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.

[14] 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.

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

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

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

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

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

[20] 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).

[21] 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)

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

[23] 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.

[24] J.A. Lopez Ramos, J. Rosenthal, D. Schipani and R. Schnyder, Group key management based on semigroup actions, Journal of Algebra and its applications, 2017, vol.16(08):1750148.

[25] 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

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

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