On Extremal Algebraic Graphs and implementations of new Multivariate Cryptosystems

Ustimenko V. O [1,2], Pustovit O. S. [2]

[1]Royal Holloway, University of London

[2]Institute of telecommunication and global information space, NAS of Ukraine

E - mail: vasylustimenko@yahoo.pl, sanyk_set@ukr.net

Funding: This research is partially supported by the Fellowship of British Academy for Researchers at Risk 2022

Extremal algebraic graphs were traditionally used for the construction of stream ciphers of multivariate nature (see [6] and further references or [7]). We introduce the first graph based multivariate public keys with bijective encryption maps. NIST 2017 tender starts the standardisation process of possible Post-Quantum Public keys aimed for purposes to be (I) encryption tools, (II) tools for digital signatures (see [1]).

In July 2020 the Third Round of the competition started. In the category of Multivariate Cryptography (MC) remaining candidates are easy to observe. For the task (I) multivariate algorithm was not selected, single multivariate candidate is "The Rainbow Like Unbalanced Oil and Vinegar" (RUOV) digital signature method. As you see RUOV algorithm was investigated as appropriate instrument for the task (II). Due to this investigation RUOV was not selected for the next 4th round of NIST competition. In 2022 first 4 winners of the NIST competition were selected. So NIST certification do not select any of algorithm of Multivariare Cryptography.

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

In fact RUOV is given by quadratic system of polynomial equations. We think that NIST outcomes motivate investigations of alternative options in Multivariate Cryptography oriented on encryption tools for:
(a) the work with the space of plaintexts $(F_q)^n$ and its transformation G of linear degree cn, $c>0$ on the level of stream ciphers or public keys
(b) the usage of protocols of Noncommutative Cryptography with platforms of multivariate transformations for the secure elaboration of multivariate map G from $End(F_q[x_1, x_2, \dots, x_n])$ of linear or superlinear degree and density bounded below by function of kind cn^r, where $c>0$ and $r>1$.

We hope that these alternative options together with classical multivariate public key approach are able to bring reliable encryption algorithms.

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

We use the known family of small world graphs $A(n, q)$ (see [2], [3] and further references) and their analogs $A(n, K)$ defined over finite commutative ring K with unity for the construction of cubic multivariate public keys. Noteworthy to mention that for each prime power q, $q>2$ graphs $A(n, q)$, $n=2, 3, \dots$ form a family of large girth (see [3]), there is well defined projective limit of these graphs which is a q-regular tree.

Further we obfuscate the encryption maps of these public keys via the combination of them with Eulerian transformation of K^n.

We also use the new extraction technique to combine these public keys of degree 3 or linear degree $\alpha(n)$, $\alpha >0$ with postquantum protocols of Noncommutative Cryptography with the implementations on platform of Eulerian multivariate maps. We show that extraction technique can be used for the

conversion of graph based symmetric ciphers to protocol based asymmetric algorithms of El Gamal type.

In the talk we present the known mathematical definitions of algebraic geometry for further usage of them as instruments of Multivariate Cryptography. In particular definitions of affine Cremona semigroup of endomorphisms of multivariate ring $K[x_1, x_2,..., x_n]$ defined over commutative ring K, Eulerian transformations and affine Cremona group ${}^nCG(K)$ are presented there.

We present the idea of Eulerisation of bijective map from affine Cremona semigroup, i.e. the usage of a composition of Eulerian transformation with the element of ${}^nCG(K)$. The concept of *trapdoor accelerator* of the transformation from affine Cremona semigroup ${}^nCS(K)$ will be given as a piece of information which allows computation of reimage of the map in time $O(n^2)$.

This is a weaker version of the definition of trapdoor one way function. The definition of the trapdoor accelerator is independent from the conjecture $P \neq NP$ of the Complexity theory.

We formulate some statements on the existence of the trapdoor accelerator with the restrictions on the degrees on maps and their inverses for families of elements of the affine Cremona group ${}^nCG(K)$. Similar statements for toric transformations of ${}^nCS(K)$ which restrictions on $(K^*)^n$ are injective will be also given.

The description of linguistic graphs $A(n, K)$ and some their properties will be given together withdescription of subgroups and subsemigroups of ${}^nCS(K)$ defined via walks in graphs $A(n, K)$ and $A(n, K[x_1, x_2, ..., x_n])$. Some statements about degrees of elements of these semigroups are already obtained. Proofs of these statements are based on explicite constructions. Several examples of cryptographic applications of proven statements will be presented.

We discuss the implementation of twisted Diffie-Hellman protocol based on the platform semigroup ${}^{n}ES(K)$ of Eulerian transformations. Security of this protocol rests on the well known Conjugacy Power Search Problem (CPSP, see [4]) in the case of semigroup of Eulerian transformations.

We discuss the implementation of *tame homomorphism protocol* of [5] based on the canonical homomorphism of parabolic subgroup ${}^{n}P_{m}(K)$ onto ${}^{n}ES(K)$ for $m>n$. Security of this protocol rests on the complexity of the Word Decomposition Search Problem for the case of group ${}^{m}ES(K)$. The output of both protocols is the collision element from ${}^{m}ES(K)$.

Protocol output is used for the ''privatisation'' of earlier presented multivariate public keys with public rules from ${}^{n}CS(K)$. This process converts public rule to the protocol based El Gamal type cryptosystem. Its security rests on the security of the corresponding protocol.

Two different methods are used for this purpose. The first one is safe delivery method which allows to transfer the public rule created by Alice to her partner Bob. The second method uses new idea of extraction the private password from the output of the protocol. So both correspondents use it for private key encryption of the public key.

Noteworthy that extraction method can be used for the conversion of symmetric stream ciphers of multivariate nature with encryption maps of nonpolynomial density to El Gamal type cryptosystems. In this case there are no options to use the encryption rule on the public key mode and linearisation attacks are not feasible.

More general idea to combine stream cipher of multivariate nature with the space of ciphertexts K^{n} with the output of the protocol based in computations in subgroups of affine Cremona semigroup ${}^{m}CS(K)$ will be also presented. The

combination is established via open logical scheme of key extraction given in terms of Predicates Calculus.

Finally we present the option of faster trapdoor accelerators with execution time $O(n^{\alpha})$, $1<\alpha<2$ instead of $O(n^2)$.

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. V. Ustimenko., *On the extremal graph theory and symbolic computations*, Reports of Nath Acad of Sci, of Ukraine, 2013, No. 2, p. 42-49.
3. V. Ustimenko, *On new results on Extremal Graph Theory, Theory of Algebraic Graphs and their applications in Cryptography and Coding Theory*, Reports of Nath Acad of Sci, of Ukraine, No. 4, p. 42-49.
4. Alexei G. Myasnikov; Vladimir Shpilrain; Alexander Ushakov, *Non-commutative Cryptography and Complexity of Group-theoretic Problems*, Amer. Math Soc. 2011.
5. V. Ustimenko, *On new symbolic key exchange protocols and cryptosystems based on hidden tame homomorphism*, Reports of. Nath. Acad. Sci. of Ukraine, 2018, n 10, pp. 26-36.
6. M. Polak, U. Roman'czuk, V. Ustimenko and A. Wryblewska, *On the applications of Extremal Graph Theory to Coding Theory and Cryptography*, Electronic Notes in Discrete
7. V. Ustimenko, Graphs in terms of Algebraic Geometry, symbolic computations and secure communications in Post-Quantum world, UMCS Editorial House, Lublin, 2022, 198 p.