ON THE NEW APPLICATIONS OF ALGEBRAIC GRAPH THEORY TO MULTIVARIATE CRYPTOGRAPHY

V.A. Ustimenko[1], U. Romańczuk-Polubiec[2], A. Wróblewska[1], M. Polak[1]

[1] The University of Maria Curie Sklodowska, Institute of Mathematics,
pl. Marii Curie-Skiodowskiej 1, 20-031 Lublin, Poland,
vasyl@hektor.umcs.lublin.pl, awroblewska@hektor.umcs.lublin.pl, monika.katarzyna.plak@gmail.com
[2] The Independent Polish Researcher, urszula_romanczuk@yahoo.pl

Presented research of authors is partially supported through the project "Scientific fellowships for PhD students working in research teams", which is realized by Self-Ggovernment of the of Lubelskie Voivodeship and Regional Operational Programme Department of the Marshal's Office of Lubelskie Voivodeship in Lublin, Poland, within the framework of Sub-measure 8.2.2 Regional Innovation Strategies, Measure 8.2 Transfer of knowledge, Priority VIII Regional human resources for the economy Human Capital Operational Programme co-financed by European Social Fund and state budget. The authors team together with the firm LabSQL.pl collaborate on the above project.

The RSA is one of the most popular cryptosystems. It is based on number factorisation problem and Euler Theorem. Peter Shor discovered that factorisation problem can be effectively solved with the usage of theoretical quantum computer. It means that RSA could not be a security tool in the future postquantum era. One of the research directions which can lead to a postquantum secure public key is the Multivariate Cryptography which uses a polynomial maps of affine space K^n defined over a finite commutative ring into itself as encryption tools (see [1]). This is a young promising research area with the current lack of known cryptosystems with the proven resistence against attacks with the use of Turing machines. Other important direction of Postquantum Cryptography is the studies of Elliptic Curves cryptosystems.

Applications of Algebraic Graph Theory to Multivariate Cryptography were observed in our talks at Erdos Centennial (2013, Budapest) and Central European Conference on Cryptology 2014 (Alfred Renyi Institute, Budapest) [2, 3]. This talk was devoted to algorithms based on bijective maps of affine spaces into itself. Applications of algebraic graphs to cryptography started from symmetric algorithms based on explicit constructions of extremal graph theory and their directed analogue (see survey [4, 5]). The main idea is to convert an algebraic graph in finite automaton and use the preudorandom walks on the graph as encryption tools. This approach can be also used for the key exchange protocols. Nowadays the idea of "symbolic walks" on algebraic graphs when the walk on the graph depends on parameters given as special multivariate polynomials in variables depending from plainspace vector brings several public key cryptosystems. Other source of graphs suitable for cryptography is connected with finite geometries and their flag system (see [4], [11] and further references).

Our presentation at DIMA 2015 includes new cryptoalgorithms in terms of Algebraic Combinatorics which use non bijective transformations of K^n.

Multivariate cryptography started from studies of potential for the special quadratic encryption multivariate bijective map of K^n, where K is an extention os finite field F_q of characteristic 2. One of the first such cryptosystems were proposed by Imai and Matsumoto, cryptanalysis for this system was invented by J. Patarin. The survey on various modifications of this algorithm and corresponding cryptanalysis the reader can find in [1]. Bijective multivariate sparse encryption maps of rather high degree based on walks in algebraic graphs were proposed in [6].

One of the first usage of non bijective map of multivariate cryptography was in *oil and vinegar* crytosystem proposed in [7] and analysed in [8]. Nowadays this general idea is strongly supported by publication [9] devoted to security analysis of direct attacks on modified unbalanced oil and vinegar systems. It looks like such systems and rainbow signatures schemes may lead to promising Public Key Schemes of Multivariate Encryption defined over finite fields. Non bijective multivariate

sparse encryption maps of degree 3 and ≥ 3 based on walks on algebraic graphs $D(n, K)$ defined over general commutative ring and their homomorphic images were proposed in [10].

The new cryptosystems with non bijective multivariate encryption maps on the affine space ${Z_m}^n$ into itself will be presented. It uses the plainspace ${Z_m^*}^n$, where $n = k(k-1)/2$, $k \geq 2$ can be arbitrary natural number. The private key space is formed by sequence of general multivariate polynomials from $Z_m[x_1, x_2, \ldots, x_{k-1}]$ and sequence of parameters l_i, $i = 1, 2, \ldots, k-1$ which are mutually prime with $\phi(m)$. The properties of the encryption map depends heavily on the prime factorisation of m. This non bijective encryption map is the deformation of special computation generated by Schubert automaton of "$k-1$ dimensional projective geometry" over Z_m. This method does not use the partition of variables into groups, non bijective nature of the map caused by zero devisors of composite integer m. In fact the idea of multiple "hidden RSA" is used.

This algorithm is a modification of public key cryptosystem based on the computation of Tits automaton in the case of finite projective geometry [11], which were presented at the conference ALCOMA 2015.

The talk is dedicated to the memory of D. A. Suprunenko whose research is an inspirational example of multifaceted work in Pure and Applied Mathematics in areas of Algebra and Discrete Mathematics.

References

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

2. Polak M., Romańczuk U., Ustimenko V., Wróblewska A. On the applications of Extremal Graph Theory to Coding Theory and Cryptography // Erdős Centennial, Proceedings of Erdős Centennial (EP 100). Electronic Notes in Discrete Mathematics. 2013. V. 43. P. 329–342.

3. Ustimenko V. A. Explicit constructions of extremal graphs and new multivariate cryptosystems // Studia Scientiarum Mathematicarum Hungarica, Special issue "Proceedings of The Central European Conference, 2014, Budapest" (to appear in 2015).

4. Ustimenko V. A. Graphs with Special Arcs and Cryptograph // Acta Applicandae Mathematicae. 2002. V. 71. No 2. P. 117–153.

5. Ustimenko V. On the extremal graph theory for directed graphs and its cryptographical applications // In: T. Shaska, W.C. Huffman, D. Joener and V. Ustimenko. Advances in Coding Theory and Cryptography. Series on Coding and Cryptology. 2007. V. 3. P. 181–200.

6. Ustimenko V. On Multivariate Cryptosystems Based on Computable Maps with Invertible Decompositions // Annales of UMCS. Informatica (special issue "Proceedings of International Conference Cryptography and Security Systems"). 2014. V. 14. P. 7–18.

7. Patarin J. The Oil i Vinegar digital signatures // Dagstuhl Workshop on Cryptography. 1997.

8. Kipnis A., Shamir A. Cryptanalisis of the Oil and Vinegar Signature Scheme // Advances in Cryptology, Crypto 96. Lecture Notes in Computer Science. 1996. V. 1462. P. 257–266.

9. Bulygin S., Petzoldt A., Buchmann J. Towards provable security of the unbalanced oil and vinegar signature scheme under direct attacks // In "Progress in Cryptology, INDOCRYPT", eds.: Guang Gong, KishanChand Gupta editors, Lecture notes in Computer Science. 2010. V. 6498. P. 17–32.

10. Romańczuk-Polubiec U., Ustimenko V. On two windows multivariate cryptosystem depending on random parameters // Algebra and Discrete Mathematics. 2015. V. 19. No. 1. P. 101–129.

11. Ustimenko V. A. On the flag geometry of simple group of Lie type and Multivariate Cryptography // Algebra and Discrete Mathematics. 2015. V. 19. No 1. P. 130–144.