МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ТАРАСА ШЕВЧЕНКА

III МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

ПРОБЛЕМИ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ (PCSITS)

12 червня 2020 року

Збірник матеріалів доповідей та тез

Київ – 2020

УДК 004.056.55:004.032:004.93

V.G. Krasilenko, D.V. Nikitovich, A.A. Lazarev
Vinnytsia National Technical University

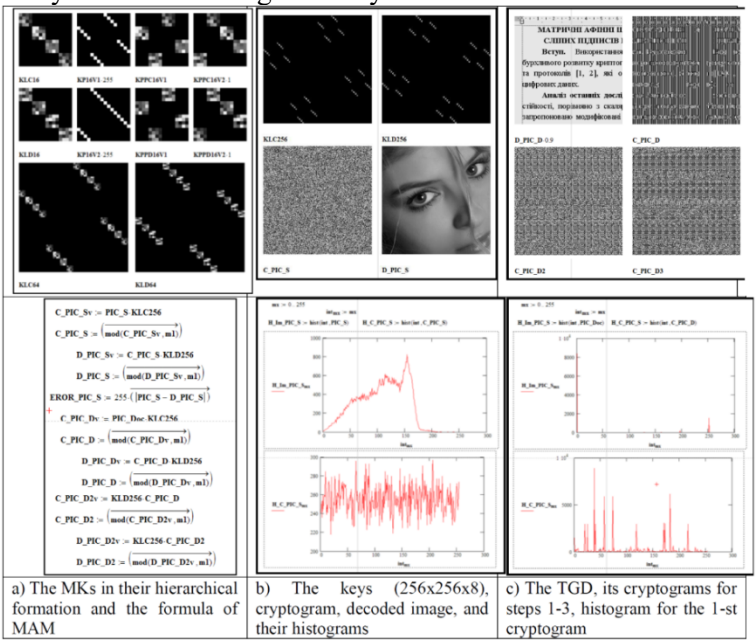
MULTI-FUNCTIONAL PARAMETRIC (MFP) MATRIX-ALGEBRAIC MODELS (MAM) OF CRYPTOGRAPHIC TRANSFORMATIONS (CTs) WITH OPERATIONS BY MODULO AND THEIR MODELING

Introduction, **analysis of recent publications, formulation of the problems.** In the era of electronic communications, the need to transmit and cryptographic transformations (CTs) specific text and graphic documents (TGDs) in the form of table data, 2-D, 3-D, 4-D arrays, drawings, diagrams, resolutions has essentially increased [1-7]. In identification, biometric systems, intelligent management it is necessary to transmit in encrypted form a large number of various images. Many TGDs contain restricted access information that should be reported to government agencies, in a timely manner and in encrypted form, to transmit over communication channels, providing only authorized access, to certify their digital signatures. Authorized access many resources can be provided with appropriate technologies of cryptography and measures with the issuance of certificates and access keys. For such security purposes, methods and tools for CTs of images [1-9] and procedures and protocols for the formation of keys and their exchange [1, 10-11] are used, but among their variety [1-9] only a small part is devoted to methods and algorithms oriented on matrix models [11-18] and tools. At the same time, the emergence of parallel matrix (image-type) processors [3, 8] contributed to the reorientation in the study of image CTs and the creation and models of matrix type (MT) [11-21]. That is why the search and research of new matrix models (MM) of CT, improvement of existing matrix ciphers and means for their realization are an actual strategic task. In works [12, 13] more generalized matrix algorithms for CTs of images and so-called matrix affine-permutation algorithms (MAPA) [15] based on of more generalized matrix affinity ciphers (MACs), as modifications of known affine ciphers [14], were proposed. The results of simulation

[11-14] of processes of CTs of color images [18] on the basis of such models have shown their significant advantages such as: greater stability, increase in speed. In work [13] on the basis of MACs the algorithm and the procedure for creating a digital blind signature (DBS) is proposed on the TGD, and the results of simulation. The results of modeling algorithms for creating a 2D key are also known [10]. Paper [11] is devoted to creation of DBS on TGD, but on the basis of other models of matrix type. One of the main components of MAPA [15], is matrix permutation model (MM_P), which has obvious simplicity. Further application and improvement of matrix-type ciphers based on such MM_P is highlighted in papers [16, 17, 19, 20]. Their basic operations are elemental multiplication, matrix addition and matrix permutation models (MM_P) with multiplication matrices. But the disadvantage of these works is the large size of the matrix keys (MK) and the lack of demonstration of their effective work with blocks in the form of matrices, which split multi-page data. However, as shown in papers [16, 17], the CTs on their basis, without additional operations, do not modify histograms of TGDs. At the same time, for most of the above-mentioned works, there is a common significant disadvantage, especially for work related to MAC [14, 18], MAPA [15] and the like [11-13, 17, 19-21], which requires the use of at least two MK, if implemented in models multiplicative and additive matrix components. Therefore, the search to improve especially the multi-step MAC, MAPA [15] while maintaining stability and other characteristics, in order to reduce the number of MKs to one, and their experimental verification is a necessary urgent task. Therefore, in order to increase the cryptographic stability of CT of such TGDs, it is necessary to search for improvements for MFP MAM, including by expanding their functional capabilities while maintaining unified matrix operations and procedures [22]. Thus, the purpose of this section is development and further modification, universalization and generalization of MFP MAM for the CT in order to improve their characteristics and sustainability, and simulation, testing the created models on real information objects (IO) that will allow evaluating their parameters, possibilities and application features.

The essence of the proposed MFP MAM for CT is to apply matrix multiplication procedures to the corresponding 8-bit MK of the same dimension (KLC256, KLD256) for matrix size NxN, as sets of bytes or 8-bit images (PIC_S, PIC_Doc, see Fig. 1) using multiplication and add operations by modulo. As can be seen from Fig. 1 – 5, the results of the simulation of the processes of direct and inverse CT TGD with a dimension of 256x256 confirmed the correct operation of models when applying the correct keys (Fig. 4) and wrong (Fig. 5). MK had a hierarchical structure, the dimension of 256x256 and consisted of a block matrix of 16x16 units with each unit size of 16x16, and each of the blocks (KLC16, KLD16) had 4 sub-blocks of 4x4 elements. Using matrices of permutations **P** of types K, KP16V1, KP16V2, allow arbitrary permutations of blocks and sub-blocks, as shown in Fig. 1. Blocks KLC, KLD and full keys are mutually inverse matrices when multiplying them by the corresponding modulo. The essential difference between the proposed MKs is that both the blocks themselves in the entire matrix and sub-blocks, and elements in them can be mixed, and their structures are similar to the permutations matrix. Thus, the cryptographic block processing is accompanied by simultaneous mixing blocks and sub-blocks, as well as their elements (Fig. 2 – 4). But the analysis of entropy, TGD histograms and their cryptograms shown in Fig. 1 confirms the following. For TGD, in contrast to a human image, even several iterative multiplications of a data matrix (DM) by MK may not be enough for high-quality encryption, especially when using one same MK. Therefore, we proposed two new multifunctional parametric MAM CTs, the main conceptual idea of which is based on the use of additional scalar or vector keys (VK) as parameters influencing the degrees of the matrices MD and MK modulo in which they are presented in models of matrix multiplications, as well as the shape or type of permutation matrices or their blocks and the degrees to which they are raised. At each iterative step, depending on the VK, different MKs are formed. Fragments of the processes of formation of matrices P, cyclic MK and their components, as well as the MAM formula for direct and inverse CT and verification using parametric MK are shown in Fig. 2. In Fig. 3 shows the appearance of some parametric MK. The

simulation results of CTs of TGDs based on parametric MAM and MK for cases of correct and, accordingly, incorrect MK, are shown in Fig. 4 and 5. The appearance of the initial histograms after the CT confirms that even for the selected TGD-specific histogram, the proposed models give better results. The power of the set of possible keys has increased by an order of magnitude (more than 10^{300} !!), and as the estimates show, only the power of a plurality of mini-blocks (8x8 8-bit) is of the order of more than 10^{150}. Thus, the models stability has increased significantly.



a) The MKs in their hierarchical formation and the formula of MAM

b) The keys (256x256x8), cryptogram, decoded image, and their histograms

c) The TGD, its cryptograms for steps 1-3, histogram for the 1-st cryptogram

Fig. 1. Fragments of Mathcad windows with the results of MK formation and simulation of MFP MAM CT: cryptograms, decoded images, histograms

Without the knowledge of keys, it is impossible to restore MD and, as shown in [13, 15], even with the dimension of MK, equal to 32x32, the stability of models is ensured [13, 15], and we have the keys of 256x256 8-bit elements, which gives a substantial strength! For the MAM there is an urgent need to form a whole range of permutation matrixes (MPs) from the main MK, which would satisfy a number of requirements. In [23, 24] only the main MK of the

general type, but not the series (flow) of the MP, was considered, the purpose of this paper is to study the processes for forming the flow of MP for MAM CT, checking their properties.

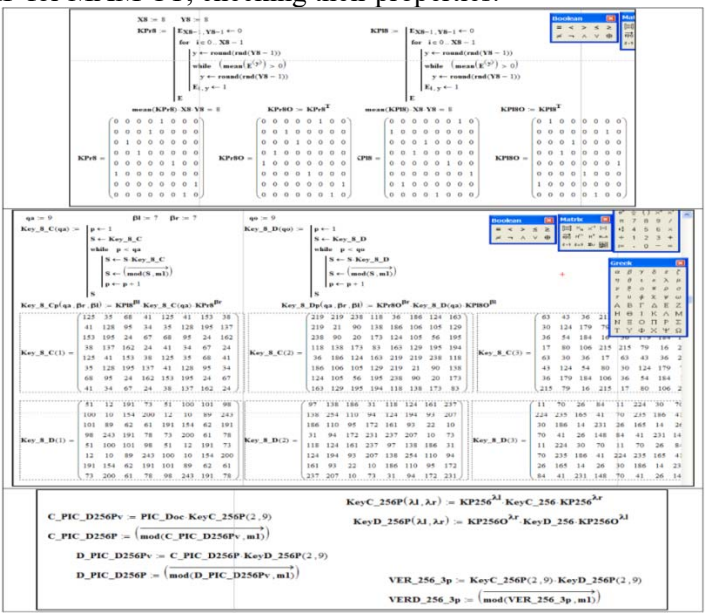


Fig. 2. Fragments of modeling of the processes of forming matrices **P**, cyclic parametric **MK**, their constituents, as well as MFP MAM formulas for encryption, decryption and verification

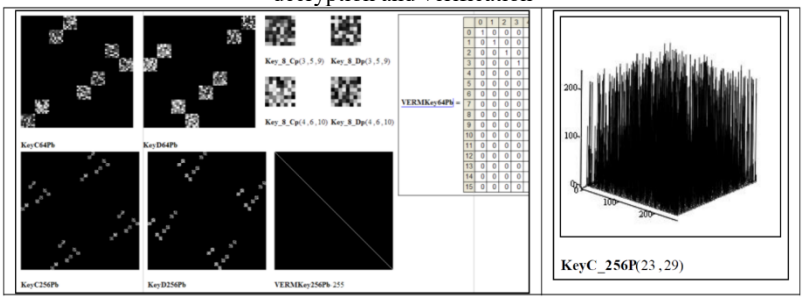


Fig. 3. The appearance of some parametric MKs, their component hierarchical blocks, and the unity- matrix (at checking) in different formats (2D, 3D, and digital)

The conclusions: New models with modular operations for MD, images, are proposed and considered. The results of their simulation are presented on the example CT over images, which testify to their

correct work, convenience (only 1 procedure and one in essence MK!), adaptability to formats, multi-functionality (combination of operations of block replacements-permutations, interchangeability of cyclic iterations procedures and matrix substitutions in modulus with convenient choice of parameters and management of transformations and key shapes) and efficiency (orientation to matrix processors). The aspects of matrix algebraic procedures and operations by modulo and creation of MK are considered. The results of simulation of direct and inverse CT, their verification confirmed the adequacy of parametric generalized MAM, their convenience, multi-functionality, efficiency for use. They are implemented both programmatically and with matrix processors, have high speed and stability of transformations and adapt to the CT over image of different formats.

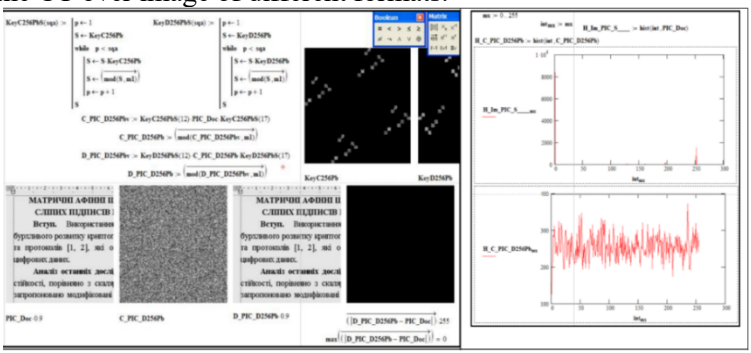


Fig. 4. Results of simulation of CT TGD on the basis of parametric MAM and MK with the correct keys (1 experiment) and histogram TGD and cryptograms (right)

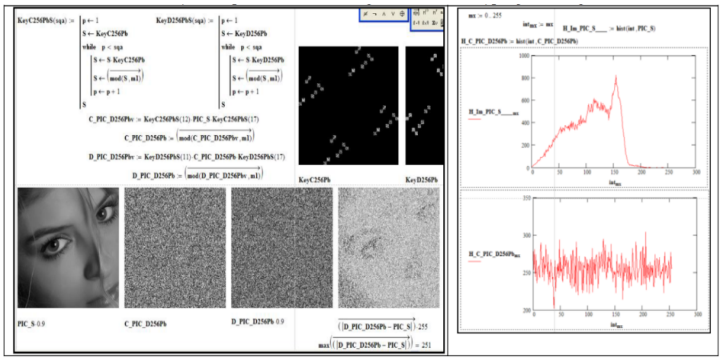


Fig. 5. Results of simulation of CT TGD on the basis of parametric MAM and MK with wrong keys (2 experiments) and TGD histograms and cryptograms (right)

References

1. Yemets V. Modern cryptography. Basic concepts / V. Yemets, A. Melnyk, R. Popovich. – Lviv: Baku, 2003. – 144 p.
2. Khoroshko V.O. Methods and means of information protection: Teaching. manual / V.O. Khoroshko, A.O. Chetkov – K .: Junior, 2003. – 502 p.
3. Korkishko T.A. Algorithms and Processors of Symmetric Block Encryption: Scientific Edition / T.A. Korkishko, A.O. Melnik, V.A. Melnik. – Lviv: Baku, 2003. – 168 p.
4. Rashkevich Yu.M. Affine transformations in modifications of the RSA image encryption algorithm / Yu.M. Rashkevich, A.M. Kovalchuk, D.D. Peleshko // Automatics. Automation. Electrotechnical complexes and systems. – 2009. – No. 2 (24). – pp. 59-66.
5. Deergha Rao K. A New and Secure Cryptosyce for Image Encryption and Decryption / K. Deergha Rao, K. Praveen Kumar, P.V. Murali Krishna // IETE Journal of research. – 2011. – Vol. 57. – Issue 2. – pp. 165-171.
6. Han Shuihua. An Asymmetric Image Encryption Based on Matrix Transformation / Han Shuihua, Yang Shuangyuan // Ecti Transactions on Computer and Information Technology. – 2005 – Vol.1, No.2. – pp. 126-133.
7. Chin-Chen Chang. A new encycle algorithm for image cryptosystems / Chin-Chen Chang, Min-Shian Hwang, Tung-Shou Chen // Journal of Systems and Software. – 2001. – No. 58. – pp. 83-91.
8. Krasilenko V.G. Algorithms and architecture for high-precision matrix-matrix multipliers based on optical four-digit alternating arithmetic / V.G. Krasilenko // Measuring and computing engineering in technological processes. – 2004. – №1. – pp. 13-26.
9. Krasilenko V.G. A noise-immune crptographis information protection method for facsimile information transmission and the realization algorithms / V.G. Krasilenko, A.I. Nikolsky, V. F. Bardaschenko // Proc. SIEE, 2006. – Vol. 6241. – pp. 316-322.
10. Krasilenko V.G. Algorithms for the formation of two-dimensional keys for matrix algorithms of cryptographic transformations of images and their modeling / V.G. Krasilenko, V. I. Yatskovsky, R. A. Yatskovskaya // Systems of information processing. – 2012. – Exp. 8. – pp. 107-110.
11. Krasilenko V.G. Simulation of Blind Electronic Digital Signatures of Matrix Type on Confidential Text-Graphic Documentation / V.G. Krasilenko, R. O. Yatskovskaya, S. K. Grabovlyak, // I International Scientific-Methodical Conference Vinnytsya: VNAU, 2012. – pp. 103-107.
12. Krasilenko V.G. Modifications of the RSA system for creation of matrix models and algorithms for encryption and decryption of images on its basis / V.G. Krasilenko, S.K. Grabovliak // Systems of information processing. – Kh.: KhUPPS, 2012. – Vol. 8. – pp. 102-106.
13. Krasilenko V.G., Matrix Affine Ciphers for the Creation of Digital Blind Signatures for Text-Graphic Documents / V.G. Krasilenko, S.K. Grabovlyak // Systems of information processing. – Kh.: KhUPPS, 2011. – Vol. 7 (97). – pp. 60 – 63.

14. Krasilenko V.G. Modeling of Matrix Cryptographic Protection Algorithms / V.G. Krasilenko, Yu.A. Flavitskaya // Bulletin of the National University of Lviv Polytechnic "Computer Systems and Networks". – 2009. – No. 658. – pp. 59-63.

15. Krasilenko V.G. Matrix affine and permutation ciphers for encryption and decryption of images / V.G Krasilenko, S.K. Grabovlyak // Systems of information processing. – Kh.: KhUPPS, 2012. – Vo. 3 (101). – t. 2. – pp. 53-62.

16. Krasilenko V.G. Matrix models of cryptographic transformations of images with matrix-bit-map decomposition and mixing and their modeling / V.G. Krasilenko, D.V. Nikitovich // Materials of 68 NTC "Modern Information Systems and Technologies. Informational security". – Odessa, ONAT them O.P.Popova, 2013. – pp. 139-143.

17. Krasilenko V.G. Cryptographic transformations of images based on matrix models of permutations with matrix-bit-map decomposition and their modeling / V.G. Krasilenko, V.M. Dubchak // Bulletin of Khmelnitsky National University. Technical sciences. – 2014. – No. 1. – pp. 74-79.

18. Krasilenko, V.G. Modeling of Matrix Affine Algorithms for the Encryption of Color Images / V.G. Krasilenko, K.V. Ogorodnik, Yu.A. Flavitskaya // Computer technologies: science and education: abstracts of reports v VseUkr. sci. conf. – K., 2010. – pp. 120-124.

19. Krasilenko V.G. Modeling and research of cryptographic transformations of images based on their matrix-bit-map decomposition and matrix models of permutations with verification of integrity / V.G. Krasilenko, D.V. Nikitovich // Electronics and Information Technologies: – Lviv, 2016. – Vo. 6. – pp. 111-127.

20. Krasilenko V.G. Simulation of cryptographic transformations of color images based on matrix models of permutations with spectral and bit-map decompositions / V.G. Krasilenko, D.V. Nikitovich // Computer-integrated technologies: education, science, production: – Lutsk:, – 2016. – No. 23. – pp. 31-36.

21. Krasilenko V.G. Modeling cryptographic transformations of color images with verification of the integrity of cryptograms based on matrix permutation models / V.G. Krasilenko, D.V. Nikitovich // Materials of the scientific and practical Internet conference "Problems of modeling and development of information systems". – Drohobych: DDPU them. I. Franko, 2016. – pp. 128-136.

22. Krasilenko V.G. Cryptographic transformations (CTs) of color images based on matrix models with operations on modules / V.G. Krasilenko, D.V. Nikitovich // Modern methods, information and software management systems for organizational and technical complexes: a collection of reports of the All-Ukrainian Internet conference (May 11, 2016). – Lutsk:, 2016. – pp. 41-43.

23. Krasilenko V.G. Modeling Protocols for Matching a Secret Matrix Key for Cryptographic Transformations and Matrix-type Systems / V.G. Krasilenko, D.V. Nikitovich // Systems of information processing. – 2017 – Vo. 3 (149). – pp. 151-157.

24. Krasilenko V.G. "Modeling of multi-stage and multi-protocol protocols for the harmonization of secret matrix keys" / V.G. Krasilenko, D.V. Nikitovich // Computer-integrated technologies: education, science, production: scientific journal. – Lutsk: LNTU, 2017. – Vo. 26. – P. 111-120.