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, A.A. Lazarev, D.V. Nikitovich
Vinnytsia National Technical University
nikitovych@i.ua

MODELS OF MATRIX BLOCK AFFINE-PERMUTATION CIPHERS (MBAPCs) FOR CRYPTOGRAPHIC TRANSFORMATIONS AND THEIR RESEARCH

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. The emergence of parallel algorithms, and especially the matrices of multiprocessor means, requires the creation of appropriate matrix-algebraic models (MAM), matrix-type systems (MT) for CT. The promise of the MAM, its modifications for the CT is evidenced by the ability to check the integrity of the cryptograms and the presence of distortions in them [19, 21], increasing the crypto-stability and expanding their functionality for very specific characteristic histograms of scanned TGDs, as experimentally shown in [22]. The generalization of the MAM to a matrix-block view is necessary in terms of the versatility of block algorithms and independence on data volumes. Thus, the actual purpose of this section is the development of block modifications of

the MAPCs with a minimum length of 2048 bits, with the possibility of choosing its parameters and cyclic or block keys of similar length, their simulation on real information objects (IO) and demonstration, evaluation of their advantages, characteristics and durability, application possibilities.

Presentation of research results. The proposed CT algorithm for encryption consists of the following steps: 1) the partition of IO into blocks in the form of matrices with a dimension 2mx2m, where m = 4, 5, 6, ... and with element-bytes in a digital format that at m = 4 is equivalent to the length of the block 256x8 = 2024 bits; 2) the permutation of the bytes of each current block using the current key, which is formed synchronously as the power of the main according to the parametric model, the argument of which is index block, 3) matrix affine or affine-permutation transformations (MAPTs) of matrix of bytes of current keys, the same as on stage 2 or similar, but according to another parametric model, 4) concatenation of the received blocks for the formation of cryptogram of IO. The decryption process has the following steps: 1) decomposing the cryptograms on blocks, 2) reversing the MAPT blocks based on the reversed current keys; 3) reversing bytes of blocks by current keys (vectors); 4) concatenating the transformed blocks into the restored IO. Blocking MAPS modeling was done with Mathcad. Mathcad windows with formulas for modeling the CT of the image by the algorithm of block MAPTs are shown in Fig. 1-4. The random bitmap KPX (256x256x1) of permutations formed in any way is used for permutations of bytes in each kp-th blocks (256 component vector VID (C_VID) or matrix C_M_V (16x16) with 8-bit numbers). It can be uniquely represented in the form of a matrix of M_V (16x16) bytes, which is either its parametric (power) model and is used for MAPTs in the next stage. The essence of MAPT is to apply to matrices-B, as a collection of bytes (8-bit PIC_S, PIC_Doc images), procedures on-element matrix multiplication by the corresponding 8-bit MKs (direct or inverse) of the same dimensions (Key0, Key0_O or Key_C (qa), Key_C (qo), Key_CN (qs), depending on the parameters and the formation modules of which are shown in Fig. 2, 3) using the multiplication and modulo operations. As can be seen from Fig. 4, 5, the simulation results of the processes

of direct and reverse CT TGDs and images with the dimension of 256x256 elements are confirmed the correct work of the models.

The cryptographic blocks processing is accompanied by the simultaneous mixing of their elements and their subsequent replacements, but, as it was shown by researches with histograms of images, TGDs and their cryptogram, shown in Fig. 4, for TGDs, in contrast to the image of a person, several iterative multiplications of the data matrix (MD) on the MK to the left or right may not be sufficient, especially with the application of the same MK. Therefore, in order to improve the algorithm, we propose to apply different current MKs to the blocks. Thus, the idea and essence of parametric block MAP-ciphers of CT is to use the functional dependencies of their parameters on block indices and additional scalar-vector keys (VK).

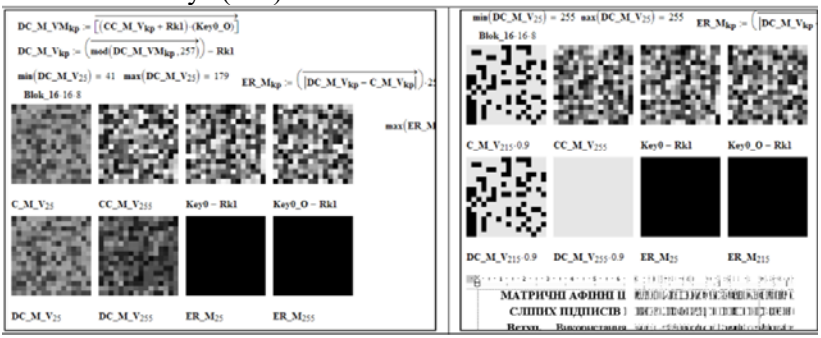

Figure 1. The results of the CT and the form of the current keys and blocks before and after the CT, the difference verification matrix-blocks: left – for the 1-st image, right – for the TGD

```
Key_C(qa) :=                    Key_C_O(qo) :=
p ← 1                           p ← 1
S ← Key0                        S ← Key0_O
while p < qa                    while p < qo
    S ← [(S)·(Key0)]                S ← [(S)·(Key0_O)]
    S ← (mod(S, m1))                S ← (mod(S, m1))
    p ← p + 1                       p ← p + 1
S                               S
```

Module of current MK generation	Generation of current reversed MK

Figure 2. Fragments of Mathcad windows with modules of MK formation

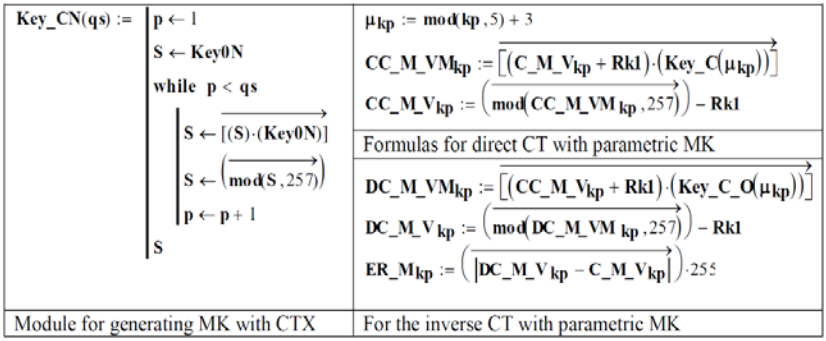

Figure 3. Fragments of Mathcad windows with modules for the MK formation and the CT formulas

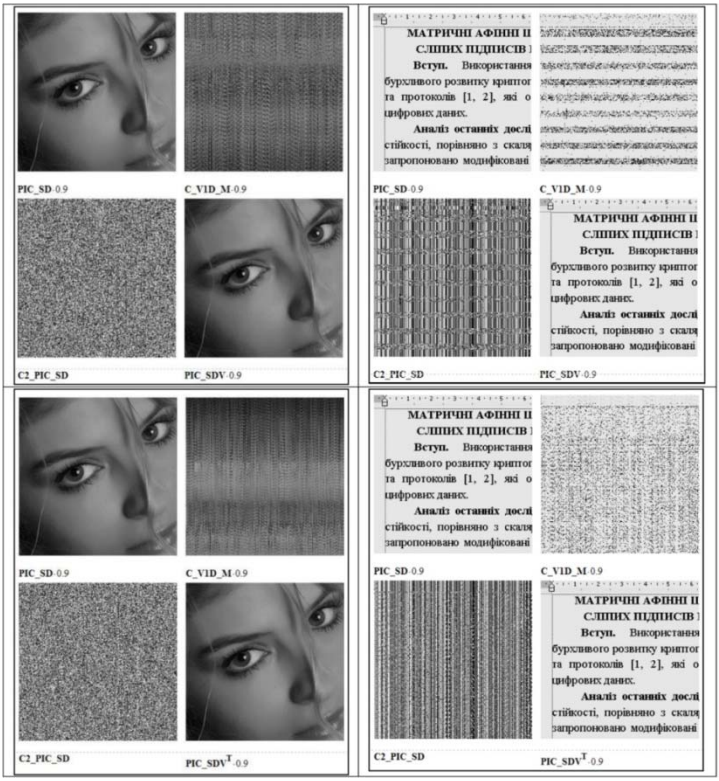

Figure 4. Fragments of Mathcad windows with the results of CT modeling the matrix block APC.

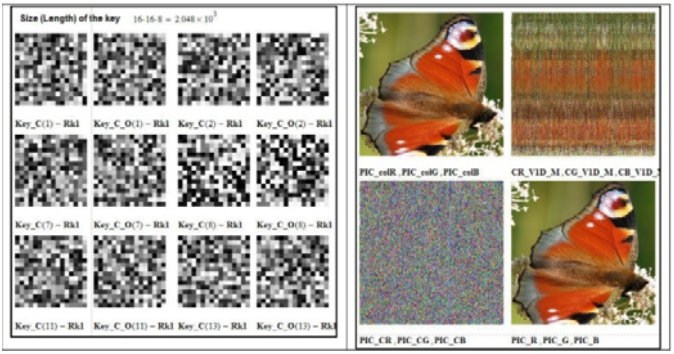

Figure 5. The form of the parametric current MK (right) and the CT of a color image (left)

The analysis of histograms before and after the CT confirms that the proposed models give better results. The TGD entropy was 0.738, and the cryptogram entropy increased 10.62 times and became equal to 7.837. The entropy of cryptogram has become almost equal to 8 bits per element: 7,997 (- 0.04%!). Without knowledge of MK it is impossible to restore MD and, as was shown in [13, 15], already with a dimension of 32x32 MK of type **P**, the stability is ensured, and with keys 16x16 8-bit elements, gives a substantial strength (256!). The power of the set of possible keys has increased by an order of magnitude more than 10^{300}!!. Therefore, the stability has increased significantly. 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 papers [23, 24] only the main MK of the general type, but not the series of MP, was considered, the purpose of paper is to study the processes for forming the flow of MP for CTs, checking their the properties.

The conclusions: New parametric block matrix-algebraic models for CTs are proposed and modulated. The results of their simulation are presented on the example of direct and inverse CTs over images, which testify to their correct performance and efficiency. Considered aspects of creating current MK. Models can be implemented with matrix processors and have high speed, stability of transformations.

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. 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 ISMC: 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: a collection of scientific works. – Lviv: Lviv Ivan Franko National University, 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: sciences. journ – Lutsk: Lutsk Publishing House. nats tech Un., – 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 abstracts of reports of the All-Ukrainian scientific and practical Internet conference (May 11, 2016). – Lutsk: RVB of Lutsk National Technical University, 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. – Mode of access: http://ki.lutsk-ntu.com.ua/node/134/section/27

37. ***G. Iashvili, M. Iavich*** 297
DEVELOPMENT OF USER-FRIENDLY SECURITY CERTIFICATE GENERATION MECHANISMS

38. ***M. Iavich, A. Gagnidze, G. Iashvili*** 301
INTEGRATION OF QUANTUM RANDOM NUMBER GENERATORS TO DIGITAL SIGNATURE SCHEMES

39. ***V.G. Krasilenko, D.V. Nikitovich, A.A. Lazarev*** 306
MULTI-FUNCTIONAL PARAMETRIC (MFP) MATRIX-ALGEBRAIC MODELS (MAM) OF CRYPTOGRAPHIC TRANSFORMATIONS (CTS) WITH OPERATIONS BY MODULO AND THEIR MODELING

40. ***V.G. Krasilenko, A.A. Lazarev, D.V. Nikitovich*** 314
MODELS OF MATRIX BLOCK AFFINE-PERMUTATION CIPHERS (MBAPCs) FOR CRYPTOGRAPHIC TRANSFORMATIONS AND THEIR RESEARCH

41. ***E. Machusky*** 322
QUANTUM INFORMATION LIMITATIONS OF ARTIFICIAL INTELLIGENCE

42. ***С.С. Бучик, Р.І. Гатченко*** 326
ШЛЯХИ ЗАПОБІГАННЯ ШАХРАЙСТВУ БАНКІВСЬКИХ СИСТЕМ ЗА ДОПОМОГОЮ МАШИННОГО НАВЧАННЯ

43. ***А.О. Нашкерський, А.О. Фесенко, В.А. Швець*** 329
ХАРАКТЕРИСТИКА IP-ТЕЛЕФОНІЇ ТА АТАК

44. ***В.В. Мохор, В.В. Цуркан*** 332
СТРУКТУРНІ ЕЛЕМЕНТИ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ