Modeling of a Cryptographic Protocol for Matching a Shared Secret Key-Permutation of Significant Dimension with its Isomorphic Representations

Volodymyr Saiko [1], Vladimir Krasilenko [2], Svitlana Kiporenko [2], Illia Chikov [2] and Diana Nikitovych [2]

[1] Taras Shevchenko National University of Kyiv, 60 Volodymyrska Street, Kyiv, 01033, Ukraine
[2] Vinnytsia National Agrarian University, st. Sonyachna, 3, Vinnytsia, 21008 Vinnytsia Oblast, Ukraine

Abstract

A protocol for agreement by user parties of secret keys-permutations of significant dimension and their new isomorphic matrix representations is proposed. Features and advantages of such representations are considered. The need to create such secret permutation keys to improve the cryptographic stability of matrix affine-permutation ciphers and other cryptosystems of the new matrix type is well-founded. The results of modeling the basic procedures of the proposed key agreement protocol in the form of an isomorphic permutation of a significant dimension, namely the processes of generating permutation matrices and their degrees, are given. Model experiments of the protocol as a whole, including accelerated methods of raising permutations to significant degrees, were performed. Such methods use sets of fixed permutation matrices, which are degrees of the underlying permutation matrix, and all these matrices are given in their isomorphic representations. The values of the fixed exponents correspond to the corresponding weights of the digits of the binary or other code representations of the selected random numbers. The results of simulation modeling demonstrated the adequacy and advantages of isomorphic representations of the processes of functioning of matrix-algebraic models of cryptographic transformations and the proposed secret key-permutation agreement protocol.

Keywords [1]

Matrix-algebraic model, matrix representations, isomorphic permutation key, cryptogram, cryptographic transformations, affine-permutation cipher, protocol, matrix-type cryptosystem.

1. Introduction, overview and analysis of publications

Introduction. Generalization of known cryptosystems [1-14] with scalar-type data formats to the cases of matrix-tensor formats, emergence and research of a new class of matrix-type cryptosystems (MTC) [15-18] based on their matrix-algebraic models (MAM) of cryptographic transformations (CT) 2D (3D) - arrays, images (Is), which have a number of significant advantages, contributed to the intensification of MTC, MAM research and the demonstration of a number of new improvements and applications [11-14, 16, 18, 19-21]. MAMs in their hardware implementations are more easily displayed on matrix processors, have extended functionality, improved crypto-resistance, allow checking the integrity of cryptograms of black and white, color images [16, 18-20], and the presence of distortions in them [16], create block ones [17], parametric [18], multi-page [18] models with their significant stability [16, 18]. Secret key generation protocols for known non-matrix type ciphers were considered in [2, 6, 12, 22-29], and for matrix type ciphers were partially considered in our previous works, including in works [30, 31], where some improved matrix modifications of known key matching protocols were proposed. Generalized MAM, matrix affine and affine-permutation ciphers (MAPCs),

Information Technology and Implementation (IT&I-2023), November 20-21, 2023, Kyiv, Ukraine

EMAIL: vgsaiko@gmail.com (A. 1); krasvg@i.ua (A. 2); kiporis11@ukr.net (A. 3); ilya95chikov@gmail.com (A. 4); diananikitovych@gmail.com (A. 5)
ORCID: 0000-0002-3059-6787 (A. 1); 0000-0001-6528-3150 (A. 2); 0000-0001-5045-5052 (A. 3); 0000-0002-2128-5506 (A. 4); 0000-0002-8907-1221 (A. 5)

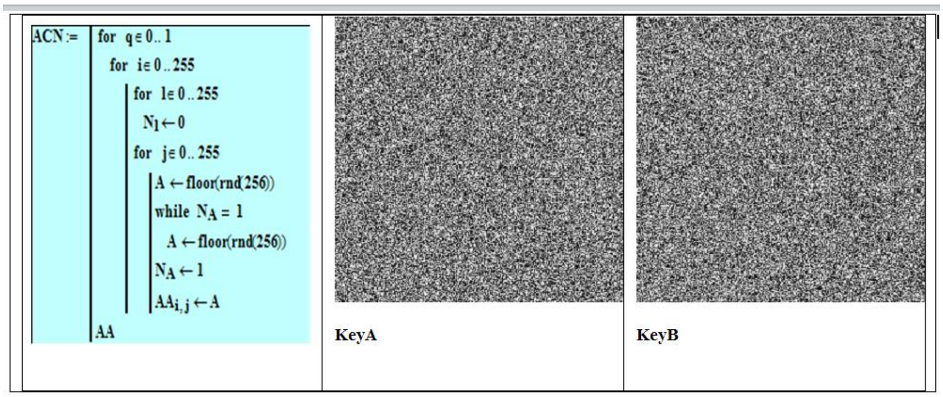
their modifications were studied and used in the creation of blind and other improved digital signatures in [18]. For CT in matrix models of permutations (MM_P), with their basic procedures of matrix multiplication and some other element-by-element modulo operations on matrices, byte matrices formed from rows, columns, vectors, which in unitary or other codes display symbols, codes, bytes, must be multiplied by the permutation matrix (PM). Procedures for rearranging bits, bytes or their groups are the most common and mandatory for almost all known and newly created algorithms and ciphers. To increase the entropy of cryptograms images with their CT based on MM_P and change their histograms, the decomposition of R, G, B components and their bit slices and several matrix keys (MKs) of the PM type are necessary [16, 18, 21, 30]. A number of such pseudo-random (current, step-by-step, frame-by-frame) MKs, which would meet the requirements and be quickly generated, is also needed for masking, CT of video files or stream of blocks from files, images with their significant sizes.

Formulation of the problem. Thus, there is a need for the MAM to form a number of MKs of the PM-type that would satisfy a number of requirements from the main MK. Since the issue of matching the main MK (MMK) of a general type, but not the sequence of PMs, was considered in [30, 31], and the methods of generating a stream of MKs-permutations from the main MK were partially considered in [31], but only for bit MPs of small sizes (256*256), then the purpose of the work is to propose and investigate a protocol for the coordination of a secret (main) MK in the form of an PM of significant dimensions, i.e., an main PM (MPM), to improve and adapt the type and structure of a MPM of such or even greater dimensions to the images format and to fast hardware solutions, to model this protocol and the process of formation flow of PMs from such a MPM for MAM CT in MT systems. In addition, the above review and analysis of publications allows to determine another important task, namely the need to develop and model such MAM CTs, which would be best suited for implementation based on vector-matrix multipliers (VMMs), as well as to determine the characteristics and indicators of such models and implementations.

2. Presentation of the main material and research results.

An overview of MT ciphers, especially multifunctional parametric block ciphers [17], their analysis shows that it is advisable to use isomorphism of various representations of permutations (matrices or vectors) that act as a master key (MK) and block or step-by-step, round MKs to achieve the goal of PM-type, i.e. sub-keys (SKs), which are matrices of permutations of P (its powers!) or vectors isomorphic to them. It is known from the works [15, 16, 17, 18] that with CT based on the basis of matrix affine-permutation ciphers (MAPCs) and vector affine-permutation ciphers (VAPCs), cryptograms for some types of text-graphic documents (TGD) and images (I), especially for block-based MAMs, when using one personal computer (PC) for all blocks are insufficient in terms of stability, however, a number of PCs created from MPM solve this problem. And that is why the aspect of coordinating the secret MPM of the PM-type with a significant dimension is important. Let's consider the situation when for M blocks with a length of 256*256 bytes, presented in the form of a matrix of a black and white image, it is necessary to rearrange all bytes in accordance with PM. In this case, PM in the generally accepted form should be square with N*N elements ("0" or "1"), where N=2^{16}=65536. The power of the set of possible such PMs, i.e. their number, is estimated as N!=65536!, which gives colossal values for this N.

But each byte address of the block can be represented by two bytes indicating two coordinates (row and column) of the block. This gives us the opportunity to represent any permutation with two blocks (256*256 elements) of bytes, setting in each identical address of these blocks the corresponding senior byte (in the first block) and junior byte (in the second block) coordinates of the new address of the byte selected for permutation. The view of the software module in Mathcad for generating the basic (main) MK (PM) and the view of its components KeyA and KeyB in the format of two black and white images is shown in Fig. 1. Therefore, any PM can be uniquely represented by two matrices of size 256*256, the elements of which take values from the range 0-255, with the peculiarity that each of their 256 gradations of intensity in each of these two matrices (images) is repeated exactly 256 times. The histograms of KeyA and KeyB PM components are shown in Fig. 2 and have the form of horizontal lines, as expected. We note that such an isomorphic representation of the PM in the form of two images gives us the opportunity to use these components KeyA and KeyB as two secret MCs of a general type, for example, as additive and multiplicative keys in the MAPCs or other MAMs. This is evidenced by the results of the simulation of the CT image (Im) of the MAPC using the proposed PM and its components, as keys, shown in Fig. 3 with the matrices of explicit image (Im), intermediates, its cryptograms (Cmap) and verifiable images [31]. And the histograms of explicit image, its cryptograms after each CT with affine components of this PM are shown in Fig. 2.



```
ACN := | for q ∈ 0..1
       |   for i ∈ 0..255
       |     | for l ∈ 0..255
       |     |   N_l ← 0
       |     | for j ∈ 0..255
       |     |   | A ← floor(rnd(256))
       |     |   | while N_A = 1
       |     |   |   A ← floor(rnd(256))
       |     |   | N_A ← 1
       |     |   | AA_i,j ← A
       | AA
```

Figure 1: Software module for generating the basic (main) MK (PM) and the view of KeyA and KeyB components in the format of two black and white images (Mathcad window).

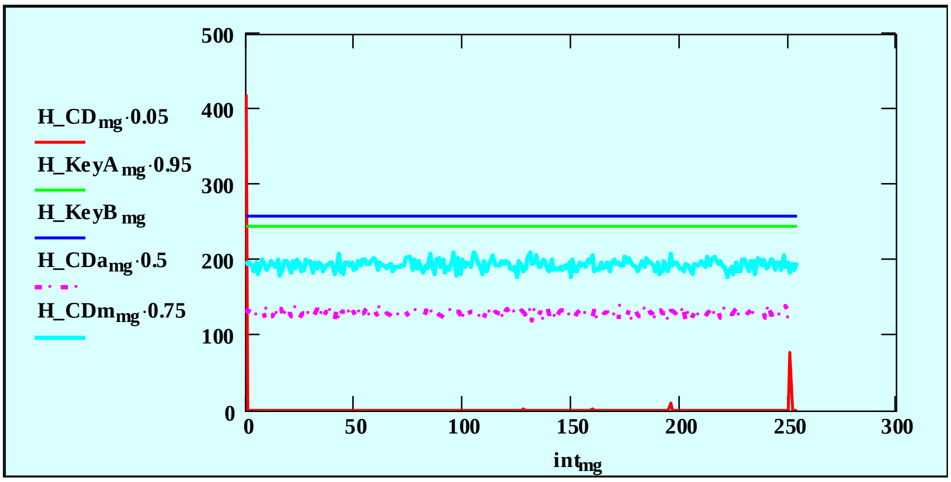
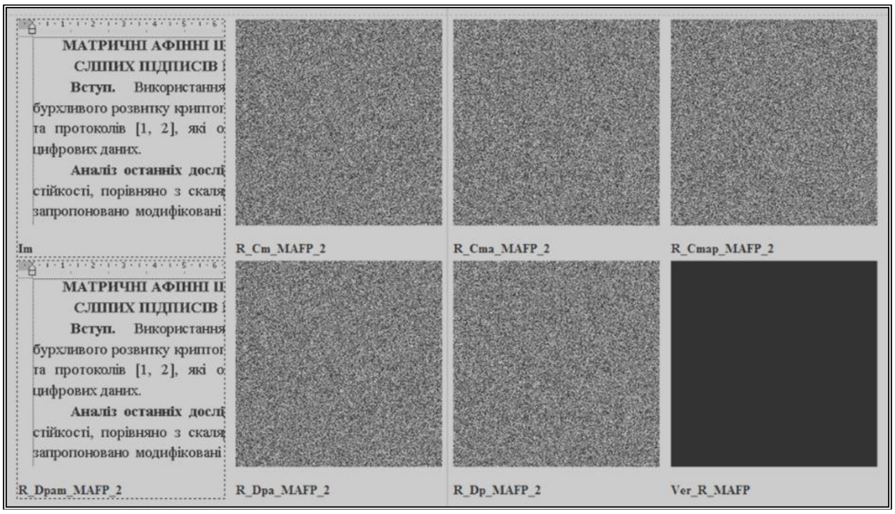


Figure 2: Histograms H_KeyA and H_KeyB, respectively, of the components KeyA and KeyB of PM, the histogram H_CD of explicit image, the corresponding histograms H_CDa and H_CDm of the cryptogram of the image after additive and multiplicative affine transformations of this image using the same KeyA and KeyB (Mathcad window).



МАТРИЧНІ АФІННІ Ц
СЛІПИХ ПІДПИСІВ
Вступ. Використання
бурхливого розвитку криптог
та протоколів [1, 2], які о
цифрових даних.
Аналіз останніх дослі
стійкості, порівняно з скаля
запропоновано модифіковані

МАТРИЧНІ АФІННІ Ц
СЛІПИХ ПІДПИСІВ
Вступ. Використання
бурхливого розвитку криптог
та протоколів [1, 2], які о
цифрових даних.
Аналіз останніх дослі
стійкості, порівняно з скаля
запропоновано модифіковані

Figure 3: The results of the simulation of MAPC based on PM and its components, as additive and multiplicative MKs. Top row, from left to right: explicit image, after transformations, cryptogram of image after MAPC; bottom row: reconstructed, intermediate and difference (right) images of TGD.

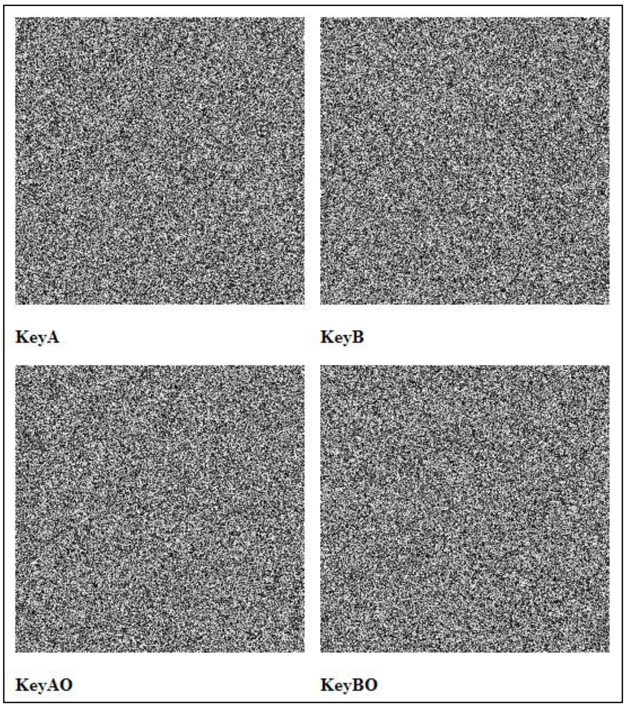
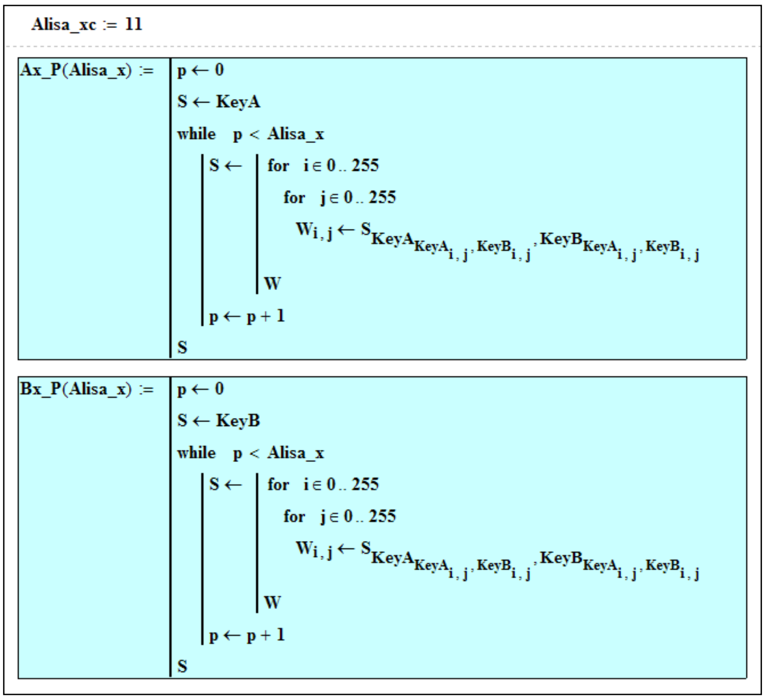


Figure 4: View (2D) of known generated PMs: top (forward), bottom (reverse) permutations.

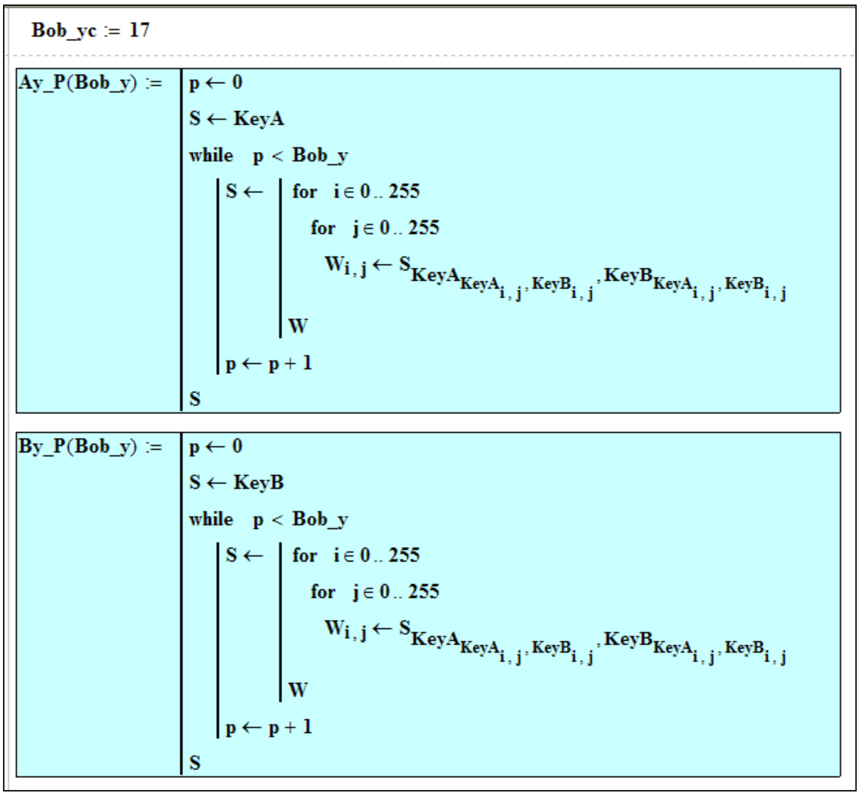


```
Alisa_xc := 11

Ax_P(Alisa_x) :=  p ← 0
                  S ← KeyA
                  while  p < Alisa_x
                      S ←  for  i ∈ 0..255
                              for  j ∈ 0..255
                                  $W_{i,j} \leftarrow S_{KeyA_{KeyA_{i,j},KeyB_{i,j}},KeyB_{KeyA_{i,j},KeyB_{i,j}}}$
                           W
                      p ← p + 1
                  S

Bx_P(Alisa_x) :=  p ← 0
                  S ← KeyB
                  while  p < Alisa_x
                      S ←  for  i ∈ 0..255
                              for  j ∈ 0..255
                                  $W_{i,j} \leftarrow S_{KeyA_{KeyA_{i,j},KeyB_{i,j}},KeyB_{KeyA_{i,j},KeyB_{i,j}}}$
                           W
                      p ← p + 1
                  S
```

Figure 5: Program modules (copies from Mathcad) displaying the procedure of iterative permutations of the initial permutation matrix PM, isomorphic to the elevation of the permutation matrix PM to the required power (11 !) by side ***x*** (Alisa).

These model experiments confirmed that the CT MAPC with the existing 2 components of the PM give high-quality cryptograms CD_ImAa and CD_ImAm, whose histograms H_CDa and H_CDm are so close to the uniform distribution law that even for image (Im) with an entropy of 0.738, the entropy of cryptograms differs from the theoretical maximum (8 bits) by just a fraction of a percent, going all the way up to 7.99. The results of the simulation of the MAPC and multi-step MAPC for different cases, when the components of affine transformations are first performed in a different sequence and with different or one MK from the PM, and then permutation using the PM, or vice versa, also proved similar qualitative CTs, when applying the proposed representations of the PM. But for all modifications of the MAM with such PMs, the power of the set of which is estimated by a significant value N! = (256*256)!, the issue of agreeing the session secret MPM is paramount.

Here is an analogy with the Diffie-Hellman protocol. In Fig. 5-8 show the results of modeling these two steps of the protocol for the agreement of the secret MC in Mathcad, and Fig. 9-10 shows the obtained intermediate and resulting secret MPM in the isomorphic representation of images. The parties do not know the degrees of the other party, but the MPs obtained by them are identical, which can be seen from Fig. 10. In this way, raising MPMs (N*N binaries, where N=2^{16} !) to a power is equivalently replaced by fast permutations, which, moreover, can be even more accelerated for significant powers due to the use of some basic set of fixed (fixed powers of MPM) and their specific sequence, which provides significant advantages due to the acceleration of the calculation of degrees of MPM, the simplicity of possible implementations and the reduction of costs.



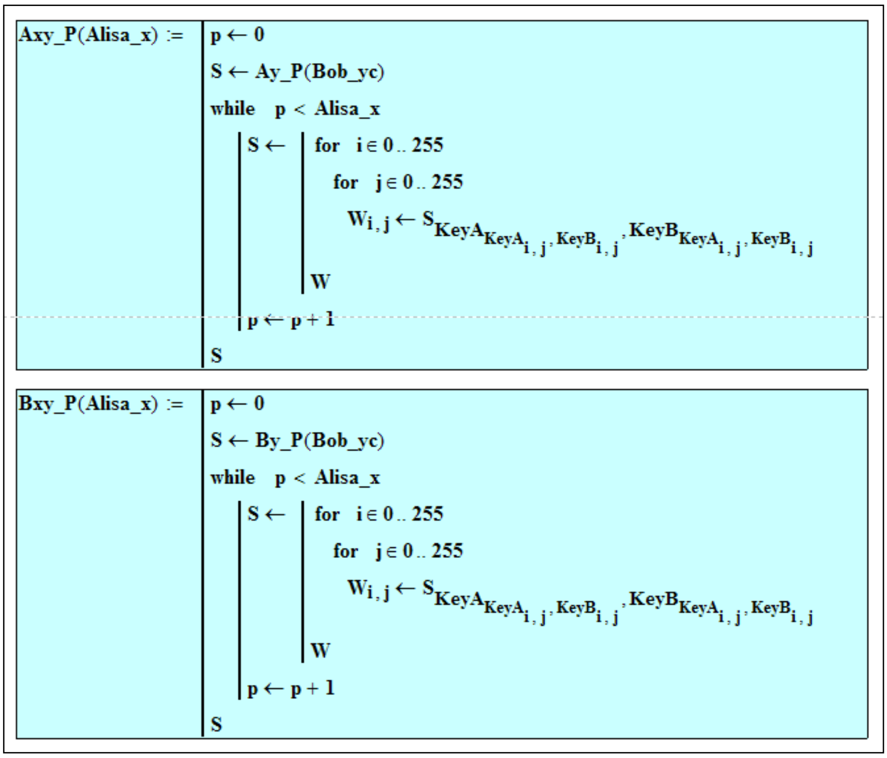
```
Bob_yc := 17

Ay_P(Bob_y) :=  p ← 0
                S ← KeyA
                while  p < Bob_y
                    S ←  for  i ∈ 0..255
                             for  j ∈ 0..255
                                 W_{i,j} ← S_{KeyA_{KeyA_{i,j},KeyB_{i,j}},KeyB_{KeyA_{i,j},KeyB_{i,j}}}
                         W
                    p ← p + 1
                S

By_P(Bob_y) :=  p ← 0
                S ← KeyB
                while  p < Bob_y
                    S ←  for  i ∈ 0..255
                             for  j ∈ 0..255
                                 W_{i,j} ← S_{KeyA_{KeyA_{i,j},KeyB_{i,j}},KeyB_{KeyA_{i,j},KeyB_{i,j}}}
                         W
                    p ← p + 1
                S
```

Figure 6: Program modules (copies from Mathcad) displaying the procedure of iterative permutations of the initial permutation matrix PM, isomorphic to the elevation of the permutation matrix PM to the required power (17 !) by side ***y*** (Bob).

In accordance with the MP protocol, values of significant dimensions must be multiplied many times, that is, raised to a power. And the degrees to which the parties raise these isomorphically presented MPs must be significant enough to ensure the necessary crypto-resistance against random attacks. Therefore, taking into account the necessity and expediency of using the above-mentioned accelerated methods of raising matrices to a power, we show an adequate isomorphic transformation of this procedure into some sequence of fixed permutations.

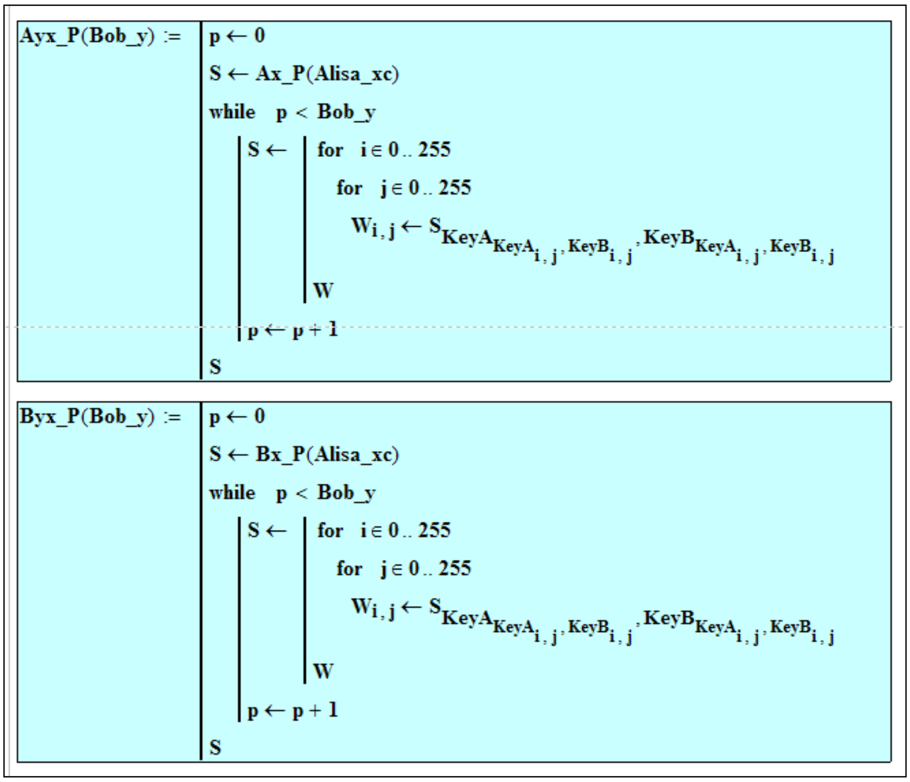
Depending on the code in which the value of the degree is given, appropriate permutations are selected from the formed set of fixed MPs, the degrees of which correspond to the corresponding weights of the digits of the binary or other code representations of the selected random numbers: ***xc*** (Alisa) and ***yc*** (Bob). The results of these simulations, the corresponding formulas, procedures, key fragments are shown in Fig. 11-12. A comparison of matrix elements in Fig. 12 highlights their equality.

Using the developed functional parametric models of the CT with the help of a secret MK (PM), agreed with the proposed protocol, shown above, a check of the correctness of their synthesis and adequacy of the models was performed by means of direct and reverse CT image, which was shown in Fig. 1-3. The results obtained by modeling in Mathcad confirm the correctness of the protocol, and the stability analysis, which will be presented in more detail in the report, shows the impossibility of attacks due to the huge number of possible PMs.



```
Axy_P(Alisa_x) :=
    p ← 0
    S ← Ay_P(Bob_yc)
    while  p < Alisa_x
        S ← | for  i ∈ 0 .. 255
            |     for  j ∈ 0 .. 255
            |         $W_{i,j} \leftarrow S_{KeyA_{KeyA_{i,j},KeyB_{i,j}},KeyB_{KeyA_{i,j},KeyB_{i,j}}}$
            | W
        p ← p + 1
    S

Bxy_P(Alisa_x) :=
    p ← 0
    S ← By_P(Bob_yc)
    while  p < Alisa_x
        S ← | for  i ∈ 0 .. 255
            |     for  j ∈ 0 .. 255
            |         $W_{i,j} \leftarrow S_{KeyA_{KeyA_{i,j},KeyB_{i,j}},KeyB_{KeyA_{i,j},KeyB_{i,j}}}$
            | W
        p ← p + 1
    S
```

Figure 7: Program modules (copies from Mathcad) reflecting the procedure of iterative permutations in the new PM obtained from ***y***, isomorphic to the elevation to the required power (11 !) by side ***x*** (Alisa).



```
Ayx_P(Bob_y) :=
    p ← 0
    S ← Ax_P(Alisa_xc)
    while  p < Bob_y
        S ← | for  i ∈ 0 .. 255
            |     for  j ∈ 0 .. 255
            |         $W_{i,j} \leftarrow S_{KeyA_{KeyA_{i,j},KeyB_{i,j}},KeyB_{KeyA_{i,j},KeyB_{i,j}}}$
            | W
        p ← p + 1
    S

Byx_P(Bob_y) :=
    p ← 0
    S ← Bx_P(Alisa_xc)
    while  p < Bob_y
        S ← | for  i ∈ 0 .. 255
            |     for  j ∈ 0 .. 255
            |         $W_{i,j} \leftarrow S_{KeyA_{KeyA_{i,j},KeyB_{i,j}},KeyB_{KeyA_{i,j},KeyB_{i,j}}}$
            | W
        p ← p + 1
    S
```

Figure 8: Program modules (copies from Mathcad) reflecting the procedure of iterative permutations in the new PM obtained from ***x***, isomorphic to the elevation to the required power (17 !) by side ***y*** (Bob).

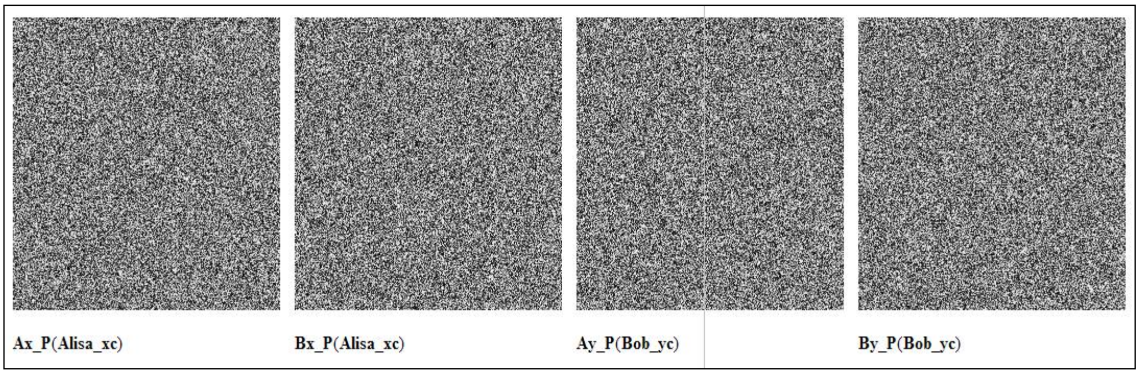
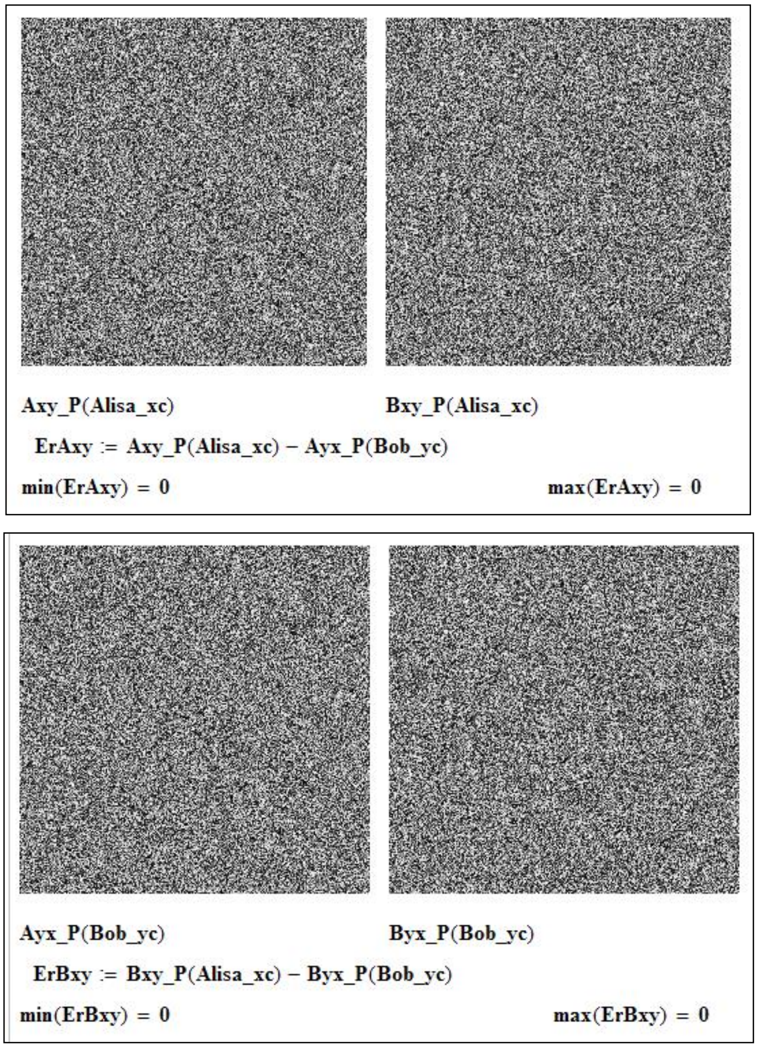


Figure 9: New PMs received by the parties (each in the form of their two components) after the first step of the protocol, those that are forwarded to the other party.



ErAxy := Axy_P(Alisa_xc) − Ayx_P(Bob_yc)

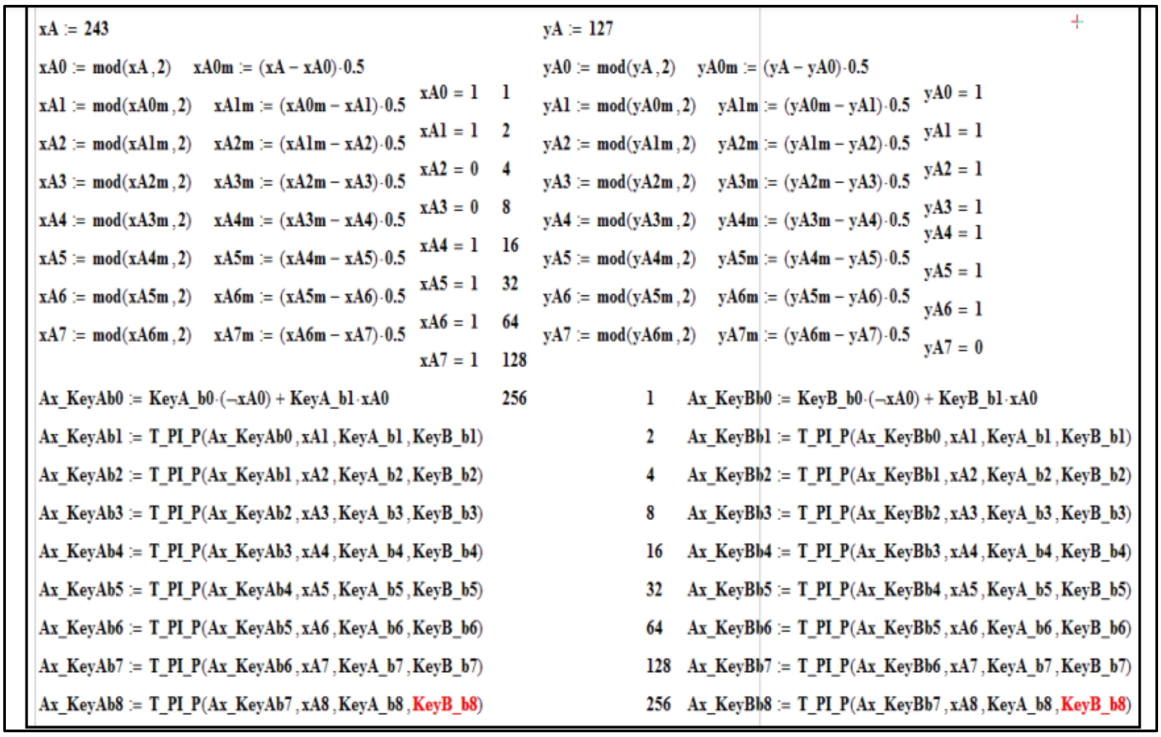
min(ErAxy) = 0 max(ErAxy) = 0

ErBxy := Bxy_P(Alisa_xc) − Byx_P(Bob_yc)

min(ErBxy) = 0 max(ErBxy) = 0

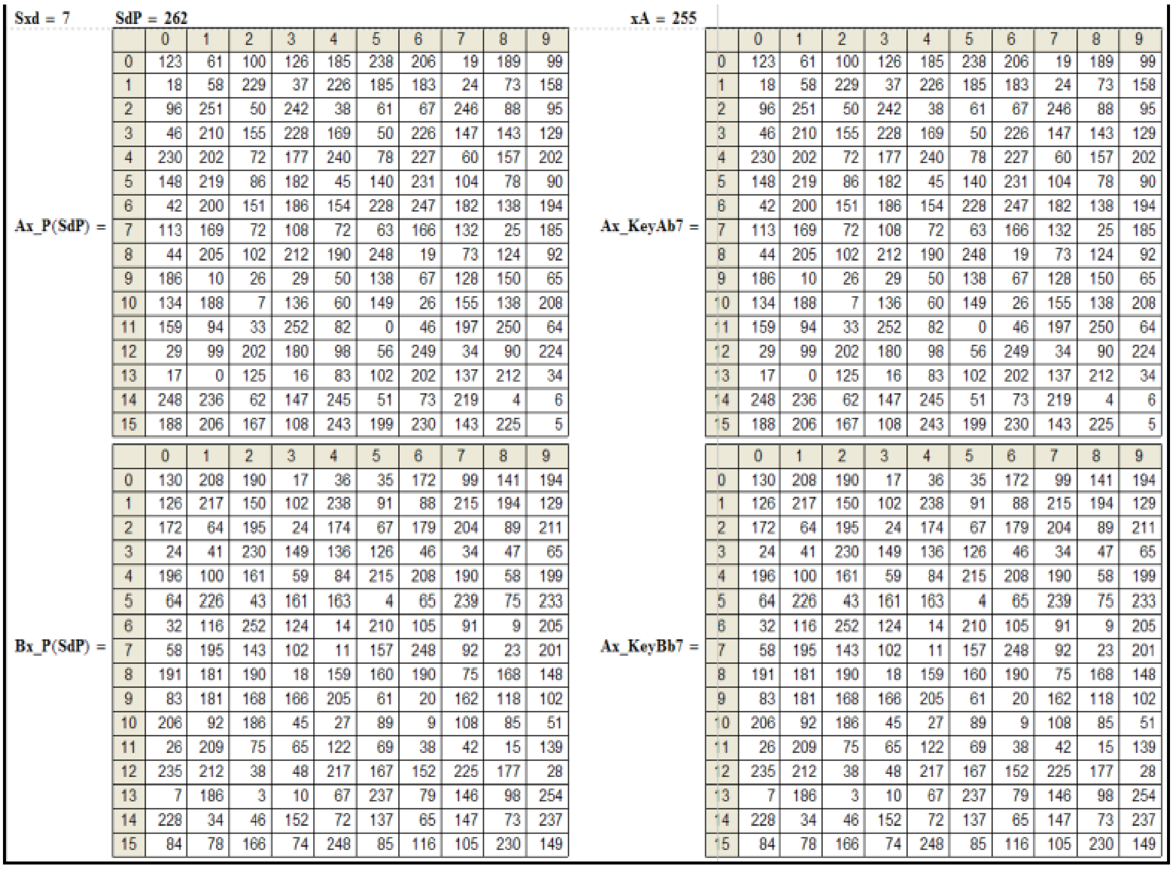
Figure 10: The participants of the session received identical new PMs (each in the form of their two components) after the second step of the protocol, i.e. essentially one secret PM.

Although the initial MPM is known to both parties, the protocol allows without knowledge of the secret degrees being chosen sides, form a secret key, PM in a similar isomorphic form in a time proportional to the number fixed permutations. In addition, stability analysis taking into account the power of the set formed by this the protocol of the relevant PM of significant dimensions showed the impossibility of carrying out attacks as a result of a huge set of possible MPs, which is estimated by the value (2^{16})!



```
xA := 243                                                       yA := 127

xA0 := mod(xA,2)    xA0m := (xA − xA0)·0.5                      yA0 := mod(yA,2)    yA0m := (yA − yA0)·0.5
                                              xA0 = 1   1                                                     yA0 = 1
xA1 := mod(xA0m,2)   xA1m := (xA0m − xA1)·0.5                    yA1 := mod(yA0m,2)   yA1m := (yA0m − yA1)·0.5
                                              xA1 = 1   2                                                     yA1 = 1
xA2 := mod(xA1m,2)   xA2m := (xA1m − xA2)·0.5                    yA2 := mod(yA1m,2)   yA2m := (yA1m − yA2)·0.5
                                              xA2 = 0   4                                                     yA2 = 1
xA3 := mod(xA2m,2)   xA3m := (xA2m − xA3)·0.5                    yA3 := mod(yA2m,2)   yA3m := (yA2m − yA3)·0.5
                                              xA3 = 0   8                                                     yA3 = 1
xA4 := mod(xA3m,2)   xA4m := (xA3m − xA4)·0.5                    yA4 := mod(yA3m,2)   yA4m := (yA3m − yA4)·0.5
                                              xA4 = 1   16                                                    yA4 = 1
xA5 := mod(xA4m,2)   xA5m := (xA4m − xA5)·0.5                    yA5 := mod(yA4m,2)   yA5m := (yA4m − yA5)·0.5
                                              xA5 = 1   32                                                    yA5 = 1
xA6 := mod(xA5m,2)   xA6m := (xA5m − xA6)·0.5                    yA6 := mod(yA5m,2)   yA6m := (yA5m − yA6)·0.5
                                              xA6 = 1   64                                                    yA6 = 1
xA7 := mod(xA6m,2)   xA7m := (xA6m − xA7)·0.5                    yA7 := mod(yA6m,2)   yA7m := (yA6m − yA7)·0.5
                                              xA7 = 1   128                                                   yA7 = 0

Ax_KeyAb0 := KeyA_b0·(¬xA0) + KeyA_b1·xA0               256        1    Ax_KeyBb0 := KeyB_b0·(¬xA0) + KeyB_b1·xA0
Ax_KeyAb1 := T_PI_P(Ax_KeyAb0,xA1,KeyA_b1,KeyB_b1)                 2    Ax_KeyBb1 := T_PI_P(Ax_KeyBb0,xA1,KeyA_b1,KeyB_b1)
Ax_KeyAb2 := T_PI_P(Ax_KeyAb1,xA2,KeyA_b2,KeyB_b2)                 4    Ax_KeyBb2 := T_PI_P(Ax_KeyBb1,xA2,KeyA_b2,KeyB_b2)
Ax_KeyAb3 := T_PI_P(Ax_KeyAb2,xA3,KeyA_b3,KeyB_b3)                 8    Ax_KeyBb3 := T_PI_P(Ax_KeyBb2,xA3,KeyA_b3,KeyB_b3)
Ax_KeyAb4 := T_PI_P(Ax_KeyAb3,xA4,KeyA_b4,KeyB_b4)                 16   Ax_KeyBb4 := T_PI_P(Ax_KeyBb3,xA4,KeyA_b4,KeyB_b4)
Ax_KeyAb5 := T_PI_P(Ax_KeyAb4,xA5,KeyA_b5,KeyB_b5)                 32   Ax_KeyBb5 := T_PI_P(Ax_KeyBb4,xA5,KeyA_b5,KeyB_b5)
Ax_KeyAb6 := T_PI_P(Ax_KeyAb5,xA6,KeyA_b6,KeyB_b6)                 64   Ax_KeyBb6 := T_PI_P(Ax_KeyBb5,xA6,KeyA_b6,KeyB_b6)
Ax_KeyAb7 := T_PI_P(Ax_KeyAb6,xA7,KeyA_b7,KeyB_b7)                 128  Ax_KeyBb7 := T_PI_P(Ax_KeyBb6,xA7,KeyA_b7,KeyB_b7)
Ax_KeyAb8 := T_PI_P(Ax_KeyAb7,xA8,KeyA_b8,KeyB_b8)                 256  Ax_KeyBb8 := T_PI_P(Ax_KeyBb7,xA8,KeyA_b8,KeyB_b8)
```

Figure 11: Formulas and procedures (copies from Mathcad windows) used for modeling isomorphic formation accelerated processes of degrees of matrix permutations by sides.



Sxd = 7   SdP = 262   xA = 255

Ax_P(SdP) =

	0	1	2	3	4	5	6	7	8	9
0	123	61	100	126	185	238	206	19	189	99
1	18	58	229	37	226	185	183	24	73	158
2	96	251	50	242	38	61	67	246	88	95
3	46	210	155	228	169	50	226	147	143	129
4	230	202	72	177	240	78	227	60	157	202
5	148	219	86	182	45	140	231	104	78	90
6	42	200	151	186	154	228	247	182	138	194
7	113	169	72	108	72	63	166	132	25	185
8	44	205	102	212	190	248	19	73	124	92
9	186	10	26	29	50	138	67	128	150	65
10	134	188	7	136	60	149	26	155	138	208
11	159	94	33	252	82	0	46	197	250	64
12	29	99	202	180	98	56	249	34	90	224
13	17	0	125	16	83	102	202	137	212	34
14	248	236	62	147	245	51	73	219	4	6
15	188	206	167	108	243	199	230	143	225	5

Ax_KeyAb7 =

	0	1	2	3	4	5	6	7	8	9
0	123	61	100	126	185	238	206	19	189	99
1	18	58	229	37	226	185	183	24	73	158
2	96	251	50	242	38	61	67	246	88	95
3	46	210	155	228	169	50	226	147	143	129
4	230	202	72	177	240	78	227	60	157	202
5	148	219	86	182	45	140	231	104	78	90
6	42	200	151	186	154	228	247	182	138	194
7	113	169	72	108	72	63	166	132	25	185
8	44	205	102	212	190	248	19	73	124	92
9	186	10	26	29	50	138	67	128	150	65
10	134	188	7	136	60	149	26	155	138	208
11	159	94	33	252	82	0	46	197	250	64
12	29	99	202	180	98	56	249	34	90	224
13	17	0	125	16	83	102	202	137	212	34
14	248	236	62	147	245	51	73	219	4	6
15	188	206	167	108	243	199	230	143	225	5

Bx_P(SdP) =

	0	1	2	3	4	5	6	7	8	9
0	130	208	190	17	36	35	172	99	141	194
1	126	217	150	102	238	91	88	215	194	129
2	172	64	195	24	174	67	179	204	89	211
3	24	41	230	149	136	126	46	34	47	65
4	196	100	161	59	84	215	208	190	58	199
5	64	226	43	161	163	4	65	239	75	233
6	32	116	252	124	14	210	105	91	9	205
7	58	195	143	102	11	157	248	92	23	201
8	191	181	190	18	159	160	190	75	168	148
9	83	181	168	166	205	61	20	162	118	102
10	206	92	186	45	27	89	9	108	85	51
11	26	209	75	65	122	69	38	42	15	139
12	235	212	38	48	217	167	152	225	177	28
13	7	186	3	10	67	237	79	146	98	254
14	228	34	46	152	72	137	65	147	73	237
15	84	78	166	74	248	85	116	105	230	149

Ax_KeyBb7 =

	0	1	2	3	4	5	6	7	8	9
0	130	208	190	17	36	35	172	99	141	194
1	126	217	150	102	238	91	88	215	194	129
2	172	64	195	24	174	67	179	204	89	211
3	24	41	230	149	136	126	46	34	47	65
4	196	100	161	59	84	215	208	190	58	199
5	64	226	43	161	163	4	65	239	75	233
6	32	116	252	124	14	210	105	91	9	205
7	58	195	143	102	11	157	248	92	23	201
8	191	181	190	18	159	160	190	75	168	148
9	83	181	168	166	205	61	20	162	118	102
10	206	92	186	45	27	89	9	108	85	51
11	26	209	75	65	122	69	38	42	15	139
12	235	212	38	48	217	167	152	225	177	28
13	7	186	3	10	67	237	79	146	98	254
14	228	34	46	152	72	137	65	147	73	237
15	84	78	166	74	248	85	116	105	230	149

Figure 12: Fragments of the keys formed after the second step, which testify to the adequacy of the accelerated algorithms of the isomorphic formation of degrees of matrix permutations by sides.

3. Conclusions

The relevance and necessity of creating secret permutation keys to increase the cryptographic stability of matrix affine permutation ciphers and other cryptosystems of the new matrix type are substantiated. A protocol for agreeing a secret key in the form of isomorphic representations of permutation matrixs of significant dimensions was proposed, model experiments were performed that confirmed the adequacy of the functioning of the models and the proposed protocol and methods of permutation matrixs generation, their advantages. The models are simple, convenient, adaptable for various format and color images, implemented by matrix processors, have high efficiency, stability, and speed.

4. References

[1] B. Schneier, Applied cryptography. Protocols, algorithms, source texts in C language, Triumph, 2002.

[2] M. Wenbo, Modern cryptography. Theory and practice, Williams House, 2005.

[3] N. Fergusson, B. Schneier, Practical cryptograph,Williams House, 2005.

[4] A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, “Handbook of Applied Cryptography.” CRC Press, 1997, 794 p.

[5] D. Bernstein, J. Buchmann, and E. Dahmen, “Post-Quantum Cryptography.” Springer-Verlag, Berlin-Heidelberg, 2009, 245p.

[6] NIST. “Advanced Encryption Standard (AES).” National Institute of Standards and Technology, 2001. [Online]. Available: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

[7] N. A. Gunathilake, W. J. Buchanan, and R. Asif, “Next Generation Lightweight Cryptography for Smart IoT Devices: Implementation, Challenges and Applications,” *IEEE 5th World Forum on Internet of Things (WF-IoT)*, 2019, doi: 10.1109/WF-IoT.2019.8767250. IEEE.

[8] S. Zeadallya, A. K. Das, and N. Sklavos, "Cryptographic technologies and protocol standards for Internet of Things," *Internet of Things*, 2019, doi: 10.1016/j.iot.2019.100075. Elsevier.

[9] B. S. Sumit Singh Dhanda, Poonam Jindal, “Lightweight Cryptography: A Solution to Secure IoT,” *Wireless Personal Communications*, 2020, doi: 10.1007/s11277-020-07134-3. Springer.

[10] A. Hameed and A. Alomary, “Security Issues in IoT: A Survey,” in Proceedings *of 2019 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*, 2019, DOI: 10.1109/3ICT.2019.8910320.

[11] Mcginthy, J. M., & Michaels, A. J. (2019). “Further Analysis of PRNG-Based Key Derivation Functions.” *IEEE Access*, 7, 95978–95986. DOI: 10.1109/access.2019.2928768.

[12] ISO/IEC 18033-4:2011. “Information technology – Security techniques – Encryption algorithms – Part 4: Stream ciphers.” [Online]. Available: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54532.

[13] M. Mahbub, “Progressive researches on IoT security: An exhaustive analysis from the perspective of protocols, vulnerabilities, and preemptive architectonics,” *Journal of Network and Computer Applications*, vol. 168, 2020, doi: 10.1016/j.jnca.2020.102761.

[14] A. R. Sfar, E. Natalizio, Y. Challal, and Z. Chtourou, “A roadmap for security challenges in the Internet of Things,” *Digital Communications and Networks*, vol. 4, no. 2, pp. 118-137, 2018, doi: 10.1016/j.dcan.2017.04.003.

[15] V.G. Krasilenko, S.K. Grabovlyak, “Matrix affine and permutation ciphers for encryption and decryption of images,” *Systems of Information Processing*, vol. 3 (101), pp. 53-62, 2012.

[16] V.G. Krasilenko, D.V. Nikitovich, “Modeling and research of cryptographic transformations of images based on their matrix-bit-map decomposition and matrix models of permutations with verification of integrity,” *Electronics and Information Technologies*, vol. 6, pp. 111-127, 2016.

[17] V.G. Krasilenko, A.A. Lazarev, D.V. Nikitovich, “The Block Parametric Matrix Affine-Permutation Ciphers (BP_MAPCs) with Isomorphic Representations and their Research*,” Actual problems of information systems and technologies*, pp. 270-282, 2020.

[18] V.G. Krasilenko, A.A Lazarev, D.V Nikitovich, “Matrix Models of Cryptographic Transformations of Video Images Transmitted from Aerial-Mobile Robotic Systems. In Control

and Signal Processing Applications for Mobile and Aerial Robotic Systems," *Hershey*, PA: IGI Global, pp. 170-214, 2020.

[19] Xiaoshuai Wu, Tong Qiao, Ming Xu, Ning Zheng, "Secure reversible data hiding in encrypted images based on adaptive prediction-error labeling, *Signal Process*.," vol. 188, 2021. doi: 10.1016/j.sigpro.2021.108200.

[20] P. Puteaux, W. Puech, "A recursive reversible data hiding in encrypted images method with a very high payload," *IEEE Transactions on Multimedia*, vol. 23, pp. 636-650, 2021. doi: 10.1109/TMM.2020.2985537.

[21] B. Girod "The information theoretical significance of spatial and temporal masking in video signals," Proc. of the SPIE Symposium on Electronic Imaging, vol. 1077. Pp. 178–187, 1989.

[22] W. Diffie, and M. E. Hellman, "New Directions in Cryptography", *IEEE Transactions on Information Theory*, Vol. IT22, No. 6, Vol. 22, No. 6, pp. 644-654, 1976.

[23] A.Y. Beletskyi, A.A. Beletskyi, D.A. Stetsenko, "Modified matrix asymmetric cryptographic algorithm of Diffie–Hellman, Artificial Intelligence," no. 3, pp. 697-705, 2010.

[24] Preetika J., Manju V. and Pushpendra R. V., "Secure Authentication Approach Using Diffie-Hellman Key Exchange", *International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT)*, IEEE publisher, 2015.

[25] J. Kannan, M. Mahalakshmi and A. Deepshika, "Cryptographic Algorithm involving the Matrix Qp, Korean J. Math.," 30(3)(2022), 533-538.

[26] A. Deepshika, J. Kannan, M. Mahalakshmi, K. Kaleeswari, "Cryptographic Algorithm Based on Permutation Ciphers," Int. J. Math. And Appl., 11(4)(2023), 1–7.

[27] Saima I. and Ram L. Y., "A Secure File Transfer Using the Concept of Dynamic Random Key, Transaction Id and Validation ey with Symmetric ey Encryption Algorithm", in Proceedings *of First International Conference on Smart System, Innovations and Computing, Smart Innovation, Systems and Technologies. Springer Nature Singapore*, Pte Ltd., pp.271-278, 2018.

[28] Alvarez R., Caballero-Gil C., Santonja J. and Zamora A., "Algorithms for Lightweight key Exchange", In Proceedings *of the 10th International Conference on Ubiquitous Computing and Ambient Intelligence, UCAmI, Springer International Publishing*, pp. 536-543, 2016.

[29] Sagar V., Kumar K., "Symmetric Key Cryptographic Algorithm Using Counter Propagation Network (CPN)," in Proceedings *of the 2014 ACM International Conference on Information and Communication Technology for Competitive Strategies*, 2014, p. 51.

[30] V.G. Krasilenko, D.V. Nikitovich, "Modeling protocols for secret matrix key agreement for cryptographic transformations and matrix-type systems," *Information Processing Systems*, vol. 3 (149), pp. 151-157, 2017.

[31] V.G. Krasilenko, D.V. Nikitovich, "Modeling multistep and multilevel protocols for secret matrix key agreement," *Computer-Integrated Technologies: Education, Science, Production: Scientific Journal, Lutsk*: Lutsk National Technical University, vol. 26, pp. 111-120, 2017.