A Finite Field of Square Matrices of Order 2

Emil Faure[1,2], Anatoly Shcherba[1], Artem Skutskyi[1], and Artem Lavdanskyi[1]

[1] Cherkasy State Technological University, 460 Shevchenko blvd., Cherkasy, 18006, Ukraine
[2] State Scientific and Research Institute of Cybersecurity Technologies and Information Protection, 3 M. Zaliznyak str., Kyiv, 03142, Ukraine

Abstract

This paper focuses on constructing a Galois field of square matrices of order 2 and substantiates a theoretical basis for developing schemes of cryptographic transformation of information, key exchange, and digital signature. This research goal has been achieved by investigating a family of square matrices of order 2 with the commutative operation of matrix multiplication from the general linear group over the prime field of integers modulo. It has been proved that this commutative family of matrices is simultaneously diagonalized. The matrix that performs diagonalization has been calculated. This matrix is common to all matrices of the commutative family. The research has defined the family of matrices forming a Galois field of order with common operations of matrix multiplication and addition. The multiplicative cyclic group of this field has been shown.

Keywords

Finite field, square matrices, commutative family of matrices, diagonalization, key agreement, cryptography

1. Introduction

The theory of finite fields plays one of the key roles in cryptography. Thus, the operations of addition, multiplication, and finding inverse values in symmetric encryption algorithms [1–2] are implemented over an extended finite field $GF\left(2^n\right)$. Algorithms testing simplicity and factorization of integers rely on the theory of finite fields [3], which is the foundation of asymmetric cryptography [4–7]. Finite fields are an integral tool for creating electronic digital signatures, including those based on elliptic curves [8–14].

The recent trends in cryptography indicate that applications of matrix theory in information representation and transformation are expanding. In particular, this approach has already proven its effectiveness in the AES encryption standard [2].

Previous research findings into matrix theory [15] developed a public-key cryptosystem based on commutative semirings of tropical cyclic matrices, where multiplication is the usual addition of numbers, while the usual multiplication of numbers in the tropical semiring is absent.

The study [16] investigated chaotic image encryption technology and the application of matrix semi-tensor product theory.

In the study [17], the authors propose a homomorphic encryption technique based on matrix transformations with shifts, rotations, and transpositions. A recent study [18] proposes a code-based digital signature. The proposed scheme uses the McEliece cryptosystem [19] based on random inverse matrices.

Another major study describes Shamir's three-pass random matrix ciphering mechanism [20] that deploys a three-pass protocol with encryption operators that are random matrices. However, this research was limited by operations on commutative matrices, and uses inverse, circular, and permutation matrices, leaving the matrix fields beyond the scope of the study.

CPITS-2023-II: Cybersecurity Providing in Information and Telecommunication Systems, October 26, 2023, Kyiv, Ukraine
EMAIL: e.faure@chdtu.edu.ua (E. Faure); a.shcherba@chdtu.edu.ua (A. Shcherba); a.b.skutskyi.asp21@chdtu.edu.ua (A. Skutskyi); a.lavdanskyi@chdtu.edu.ua (A. Lavdanskyi)
ORCID: 0000-0002-2046-481X (E. Faure); 0000-0002-3049-3497 (A. Shcherba); 0000-0002-8632-1176 (A. Skutskyi); 0000-0002-1596-4123 (A. Lavdanskyi)

As we have indicated above, finite matrix fields have potential applications in cryptographic schemes used in information transformation, key exchange, and digital signature. In addition, the authors of this research have described potentially effective applications of finite matrix fields in permutation-based data transmission systems [21–24].

The study [25] identifies and investigates families of square matrices of order 2 with the commutative operation of multiplication for solving cryptographic information transformation problems.

Six families of matrices from the general linear group $GL(n,Z_p)$ [26–27] of the order n are defined over the prime field of integers modulo p, for which the multiplication operation is commutative.

In [25], the authors show that one of the families of square matrices of order 2 with the commutative operation of matrix multiplication is the family

$$\Gamma_6=\left\{ t\cdot\begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix}, \begin{array}{c} t,a,b,k\in Z_p, \\ t\neq 0, b\neq 0, \\ a(a+k)-b\neq 0 \end{array} \right\}.$$

with b and k fixed and supplemented with an identity matrix. We denote this family as

$$CGL_{b,k}(2,Z_p)=\left\{ \begin{array}{l} t\cdot\begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix}, s\cdot\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \\ t,s,a,b,k\in Z_p, \\ t,s\neq 0, \\ a(a+k)-b\neq 0 \end{array} \right\}.$$

The study [25] has proved that the matrix family $CGL_{b,k}(2,Z_p)$ is a commutative (abelian) group by multiplication. In addition, the study has shown that the order of the group $CGL_{b,k}(2,Z_p)$ for $D=k^2+4b\neq u^2\in Z_p$ is p^2-1.

Obviously, $a(a+k)-b\neq 0$ if and only if $D=k^2+4b\neq u^2\in Z_p$.

Further, we shall accept that

$$CGL_{b,k}(2,Z_p)=\left\{ \begin{array}{l} t\cdot\begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix}, s\cdot\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \\ t,s,a,b,k\in Z_p, \\ t,s\neq 0, \\ D=k^2+4b\neq u^2\in Z_p \end{array} \right\}.$$

This paper aims to build a Galois field of square matrices of order 2 based on the group of matrices $CGL_{b,k}(2,Z_p)$, thus substantiating a theoretical basis for developing schemes for the cryptographic transformation of information.

2. Diagonalization of Matrices From $CGL_{b,k}(2,Z_p)$

Note that, according to the study [28], permutable matrices of simple structure can be brought into diagonal form simultaneously, that is, by a similarity transformation.

By matrices of simple structure, we mean matrices of order n, which have linearly independent eigenvectors [28]. Since the eigenvectors corresponding to pairwise different characteristic numbers are always linearly independent, a sufficient condition for the matrix to have a simple structure is that all the roots of the characteristic equation are different [28–29].

The characteristic polynomial of the matrix $A=\begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix}\in CGL_{b,k}(2,Z_p)$ is

$$|A-\lambda E|=\begin{vmatrix} a-\lambda & 1 \\ b & a+k-\lambda \end{vmatrix}= ,$$
$$=\lambda^2-(2a+k)\lambda+a(a+k)-b$$

where E is an identity matrix of size $n=2$.

The discriminant of the characteristic equation is $D=(2a+k)^2-4(a^2+ak-b)=k^2+4b$.

If D value is a quadratic nonresidue in the prime field of integers Z_p $(D=k^2+4b\neq u^2\in Z_p)$, the characteristic polynomial has no roots in Z_p. Since the power of the equation is $n=2$, the polynomial is irreducible over the Z_p field.

Consider an irreducible polynomial $f(x)=x^2-D\in Z_p[x]$.

The simple algebraic extension of degree 2 over Z_p is defined as a quadratic field $F_{p^2}=Z_p\left[\sqrt{D}\right]$ [30], where $D=k^2+4b\neq u^2\in Z_p$.

Galois field F_{p^2} has the characteristic p and degree 2 [3].

Remark 1. F_{p^2} is a field of decomposition of characteristic polynomials for matrices from the group $CGL_{b,k}(2,Z_p)$. Eigenvalues of the matrix $tA=t\cdot\begin{pmatrix} a & 1 \\ b & a+k\end{pmatrix}$ over the field $F_{p^2}=Z_p\left[\sqrt{D}\right]$ are

$$\lambda_{1,2}(a,t)=\frac{t}{2}\left(2a+k\pm\sqrt{D}\right),\ t\neq 0. \qquad (1)$$

Thus, for the matrix tA, $t\neq 0$, the characteristic equation is $|tA-\lambda E|=t^2\left|A-\frac{\lambda}{t}E\right|=0$, whence $\lambda_{1,2}(a,t)=t\cdot\lambda_{1,2}(a)$, where $\lambda_{1,2}(a)$ are the eigenvalues of the matrix $A=\begin{pmatrix} a & 1 \\ b & a+k\end{pmatrix}$ over the field $F_{p^2}=Z_p\left[\sqrt{D}\right]$.

If $\lambda(a,t)=\frac{t}{2}\left(2a+k\pm\sqrt{D}\right)$ is one of the roots of the characteristic polynomial irreducible over Z_p, where $\lambda\in F_{p^2}$, then, by Theorem 2.14 from [3], the other root of the equation is $\lambda^p(a,t)=\frac{t}{2}\left(2a+k\mp\sqrt{D}\right)$.

The eigenvalues for the matrix sE are $\lambda_{1,2}(s)=s\neq 0$.

Lemma 1.3.19 from [29] proves that the family of diagonalizable matrices is a commutative family if and only if it is simultaneously diagonalizable. Based on this lemma, we formulate our next remark.

Remark 2. The commutative family of matrices $CGL_{b,k}(2,Z_p)$ over the field $F_{p^2}=Z_p\left[\sqrt{D}\right]$ is simultaneously diagonalizable.

That is, there is a matrix $C=\begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22}\end{pmatrix}$ with elements from F_{p^2} so that for each matrix $A\in CGL_{b,k}(2,Z_p)$ the product $C^{-1}\cdot A\cdot C$ is a diagonal matrix: $C^{-1}\cdot A\cdot C=\begin{pmatrix} \lambda_1(a,t) & 0 \\ 0 & \lambda_2(a,t)\end{pmatrix}$.

Here, we find such a matrix C.

Since $C^{-1}\cdot A\cdot C=\begin{pmatrix} \lambda_1(a,t) & 0 \\ 0 & \lambda_2(a,t)\end{pmatrix}$, then

$$t\begin{pmatrix} a & 1 \\ b & a+k\end{pmatrix}\cdot\begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22}\end{pmatrix}=$$

$$=\begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22}\end{pmatrix}\begin{pmatrix} \lambda_1(a,t) & 0 \\ 0 & \lambda_2(a,t)\end{pmatrix}.$$

After multiplying the matrices and comparing them, we arrive at

$$\begin{cases} t(ac_{11}+c_{21})=c_{11}\lambda_1(a,t), \\ t(bc_{11}+(a+k)c_{21})=c_{21}\lambda_1(a,t), \\ t(ac_{12}+c_{22})=c_{12}\lambda_2(a,t), \\ t(bc_{12}+(a+k)c_{22})=c_{22}\lambda_2(a,t). \end{cases}$$

Considering that $\lambda_{1,2}(a,t)=t\cdot\lambda_{1,2}(a)$, we rewrite the equation system as:

$$\begin{cases} ac_{11}+c_{21}=c_{11}\lambda_1(a), \\ bc_{11}+(a+k)c_{21}=c_{21}\lambda_1(a), \\ ac_{12}+c_{22}=c_{12}\lambda_2(a), \\ bc_{12}+(a+k)c_{22}=c_{22}\lambda_2(a). \end{cases}$$

The last equation system can be transformed into the next one:

$$\begin{cases} (a-\lambda_1(a))c_{11}+c_{21}=0, \\ bc_{11}+(a+k-\lambda_1(a))c_{21}=0, \\ (a-\lambda_2(a))c_{12}+c_{22}=0, \\ bc_{12}+(a+k-\lambda_2(a))c_{22}=0. \end{cases}$$

We take the first eigenvalue of the matrix $tA=t\cdot\begin{pmatrix} a & 1 \\ b & a+k\end{pmatrix}$ as $\lambda_1(a)=\frac{2a+k+\sqrt{D}}{2}$. Then the second eigenvalue of the matrix tA is $\lambda_2(a)=\frac{2a+k-\sqrt{D}}{2}$.

From the first two equations of the system, we have:

$$\begin{cases} c_{21} = \dfrac{k+\sqrt{D}}{2} c_{11}, \\ bc_{11} + \left(\dfrac{k-\sqrt{D}}{2} \right) c_{21} = 0. \end{cases}$$

We shall accept $c_{11} = 1$. Then $c_{21} = \dfrac{k+\sqrt{D}}{2}$ and the first eigenvector of the matrix C is $\overline{e_1} = \begin{pmatrix} 1 \\ \dfrac{k+\sqrt{D}}{2} \end{pmatrix}$.

The second eigenvector of the matrix C can be found similarly from the other two equations of the system: $\overline{e_2} = \begin{pmatrix} 1 \\ \dfrac{k-\sqrt{D}}{2} \end{pmatrix}$.

Then the matrix $C = \begin{pmatrix} 1 & 1 \\ \dfrac{k+\sqrt{D}}{2} & \dfrac{k-\sqrt{D}}{2} \end{pmatrix}$.

Note that the matrix C is independent of a and t values and is common for $CGL_{b,k}\left(2, Z_p\right)$.

Here, we perform a verification to complete the presentation.

$$C^{-1} \cdot A \cdot C = \frac{1}{|C|} \begin{pmatrix} \dfrac{k-\sqrt{D}}{2} & -1 \\ -\dfrac{k+\sqrt{D}}{2} & 1 \end{pmatrix} t \begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix} \times$$

$$\times \begin{pmatrix} 1 & 1 \\ \dfrac{k+\sqrt{D}}{2} & \dfrac{k-\sqrt{D}}{2} \end{pmatrix} =$$

$$= t \begin{pmatrix} \dfrac{2a+k+\sqrt{D}}{2} & 0 \\ 0 & \dfrac{2a+k+\sqrt{D}}{2} \end{pmatrix} =$$

$$= \begin{pmatrix} \lambda_1(a,t) & 0 \\ 0 & \lambda_2(a,t) \end{pmatrix}.$$

Consider the set of nondegenerate diagonal matrices D_λ over the field $F_{p^2} = Z_p\left[\sqrt{D}\right]$:

$$D_\lambda = \left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^p \end{pmatrix}, \lambda \in F_{p^2} \right\}. \qquad (2)$$

Remark 3. The mapping $g(A) = C^{-1} \cdot A \cdot C$ defines a one-to-one correspondence (bijection) between matrices from $CGL_{b,k}\left(2, Z_p\right)$ and diagonal matrices from D_λ. Hence, $g : CGL_{b,k}\left(2, Z_p\right) \leftrightarrow D_\lambda$.

Proof.

Let $A_1, A_2 \in CGL_{b,k}\left(2, Z_p\right)$, $A_1 \neq A_2$, λ_1, λ_1^p and λ_2, λ_2^p are eigenvalues of matrices A_1 and A_2 correspondently.

Then

$$C^{-1} \cdot \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_1^p \end{pmatrix} \cdot C \neq C^{-1} \cdot \begin{pmatrix} \lambda_2 & 0 \\ 0 & \lambda_2^p \end{pmatrix} \cdot C \Leftrightarrow$$

$$\Leftrightarrow \lambda_1 \neq \lambda_2.$$

The number of different matrices of the set D_λ is equal to $p^2 - 1$, which corresponds to the order of the multiplicative abelian group $CGL_{b,k}\left(2, Z_p\right)$.

This implies that the mapping $g = g(A)$ establishes a one-to-one correspondence between $CGL_{b,k}\left(2, Z_p\right)$ and D_λ.

3. Galois Field of Square 2×2 Matrices

We shall use the notation

$$F_{b,k} = \left\{ \begin{array}{c} t \cdot \begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix}, s \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \\ t, s, a, b, k \in Z_p, \\ D = k^2 + 4b \neq u^2 \in Z_p \end{array} \right\}$$

for the matrix family, where p is a prime number and b, k are fixed in Z_p.

Theorem 1. The matrix family $F_{b,k}$ is a Galois field of order p^2 with usual ordinary operations of matrix multiplication and addition.

Proof.

It is obvious that $F_{b,k} = CGL_{b,k}\left(2, Z_p\right) \cup \Theta$, where $\Theta = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

Here, we show that the addition operation is closed in the set $F_{b,k}$.

According to Remarks 2 and 3, there is the same matrix C for random matrices A_1 and A_2 from $F_{b,k}$ that

$$\begin{cases} A_1 = C \cdot \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_1^p \end{pmatrix} \cdot C^{-1}, \\ A_2 = C \cdot \begin{pmatrix} \lambda_2 & 0 \\ 0 & \lambda_2^p \end{pmatrix} \cdot C^{-1}; \end{cases} \Rightarrow$$

$$\Rightarrow A_1 + A_2 = C \cdot \begin{pmatrix} \lambda_1 + \lambda_2 & 0 \\ 0 & \lambda_1^p + \lambda_2^p \end{pmatrix} \cdot C^{-1}.$$

The Galois field $F_{p^2} = Z_p\left[\sqrt{D}\right]$ has a characteristic p. Therefore, due to Proposition 7.1.4 from [30], an equation $\lambda_1^p + \lambda_2^p = (\lambda_1 + \lambda_2)^p$ is satisfied.

Consequently, for $\lambda_3 = \lambda_1 + \lambda_2$: $A_1 + A_2 = C \cdot \begin{pmatrix} \lambda_3 & 0 \\ 0 & \lambda_3^p \end{pmatrix} \cdot C^{-1}$ or $C^{-1} \cdot (A_1 + A_2) \cdot C = \begin{pmatrix} \lambda_3 & 0 \\ 0 & \lambda_3^p \end{pmatrix} \in D_\lambda$. Obviously, $C^{-1} \cdot \Theta \cdot C = \Theta$.

According to Remark 3, there is a single matrix $A_3 \in CGL_{b,k}\left(2, Z_p\right)$, where $C^{-1} \cdot A_3 \cdot C = \begin{pmatrix} \lambda_3 & 0 \\ 0 & \lambda_3^p \end{pmatrix}$, $\lambda_3 \in F_{p^2}$. Therefore, $A_1 + A_2 = A_3 \in F_{b,k}$.

Thus, we can present the matrix family $F_{b,k}$ in the form of a fixed matrix C:

$$F_{b,k} = \left\{ C \cdot \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^p \end{pmatrix} \cdot C^{-1}, \lambda \in F_{p^2} = Z_p\left[\sqrt{D}\right] \right\}.$$

Therefore, $F_{b,k}$ is an algebraic field for ordinary operations on matrices, and its order is p^2.

Corollary 1. The multiplicative group $F_{b,k}^*$ of the finite field $F_{b,k}$ is cyclic, i.e. the group $CGL_{b,k}\left(2, Z_p\right)$ is cyclic.

Corollary 2. The number of primitive elements in the field $F_{b,k}$ is $\varphi\left(p^2 - 1\right)$, where $\varphi(m)$ is the Euler function of m.

4. Conclusion

Thus, this study has shown that the commutative family of matrices

$$CGL_{b,k}\left(2, Z_p\right) = \left\{ \begin{array}{l} t \cdot \begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix}, s \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \\ t, s, a, b, k \in Z_p, \\ t, s \neq 0, \\ a(a+k) - b \neq 0 \end{array} \right\}$$

is simultaneously diagonalizable over the field $F_{p^2} = Z_p\left[\sqrt{D}\right]$.

The matrix performing diagonalization is $C = \begin{pmatrix} 1 & 1 \\ \frac{k + \sqrt{D}}{2} & \frac{k - \sqrt{D}}{2} \end{pmatrix}$. The matrix C does not depend on the values of a or t and is common for $CGL_{b,k}\left(2, Z_p\right)$.

It was also shown that the matrix family $F_{b,k} = CGL_{b,k}\left(2, Z_p\right) \cup \Theta$, where $\Theta = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, forms a Galois field of order p^2 with usual matrix multiplication and addition operations. Consequently, $CGL_{b,k}\left(2, Z_p\right)$ is a multiplicative cyclic group.

The finite field of square 2×2 matrices investigated in this study can be applied to construct new schemes of cryptographic matrix transformations. In addition, the approach used to find the finite field of matrices of order 2 allows extending this approach to the study of square matrices of higher orders. Further research might explore a 3×3 matrix set and attempt to construct the Galois field in it.

5. Acknowledgments

This research was funded by the Ministry of Education and Science of Ukraine under grant 0123U100270.

References

[1] Data Encryption Standard (DES), National Institute of Standards and Technology, U.S. Department of Commerce (1999).

[2] Advanced Encryption Standard (AES), National Institute of Standards and Technology, FIPS 197, US (2001).

[3] R. Lidl, H. Niederreiter, Finite Fields, Encyclopedia of Mathematics and its Applications, 2nd ed., Cambridge University Press (1997).

[4] W. Diffie, M. Hellman, New Directions in Cryptography, IEEE Transactions on Inf. Theory 22(6) (1976) 644–654. doi: 10.1109/TIT.1976.1055638.

[5] R. Rivest, A. Shamir, L. Adleman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of the ACM 21(2) (1978) 120–126. doi: 10.1145/359340.359342.

[6] PKCS #1: RSA Cryptography Specifications Version 2.2, RSA Laboratories (2012).

[7] T. Elgamal, A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, IEEE Transactions Inf. Theory 31(4) (1985) 469–472. doi: 10.1109/TIT.1985.1057074.

[8] IEEE Standard Specifications for Public-Key Cryptography, IEEE (2000). doi: 10.1109/IEEESTD.2000.92292.

[9] A. Bessalov, et al., Analysis of 2-Isogeny Properties of Generalized Form Edwards Curves, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 2746 (2020) 1–13.

[10] A. Bessalov, et al., Multifunctional CRS Encryption Scheme on Isogenies of Non-Supersingular Edwards Curves, in: Workshop on Classic, Quantum, and Post-Quantum Cryptography, vol. 3504 (2023) 12–25.

[11] A. Bessalov, et al., Implementation of the CSIDH Algorithm Model on Supersingular Twisted and Quadratic Edwards Curves, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3187, no. 1 (2022) 302–309.

[12] A. Bessalov, et al., Computing of Odd Degree Isogenies on Supersingular Twisted Edwards Curves, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 2923 (2021) 1–11.

[13] A. Bessalov, V. Sokolov, P. Skladannyi, Modeling of 3- and 5-Isogenies of Supersingular Edwards Curves, in: 2nd International Workshop on Modern Machine Learning Technologies and Data Science, no. I, vol. 2631 (2020) 30–39.

[14] Digital Signature Standard (DSS), National Institute of Standards and Technology, Gaithersburg, MD (2023). doi: 10.6028/NIST.FIPS.186-5.

[15] H. Huang, C. Li, L. Deng, Public-Key Cryptography Based on Tropical Circular Matrices, Appl. Sci. 12(15) (2022). doi: 10.3390/app12157401.

[16] X. Wang, S. Gao, Image Encryption Algorithm for Synchronously Updating Boolean Networks Based on Matrix Semi-Tensor Product Theory, Inf. Sci. 507 (2020) 16–36. doi: 10.1016/j.ins. 2019.08.041.

[17] C. Rupa, Greeshmanth, M. Shah, Novel Secure Data Protection Scheme Using Martino Homomorphic Encryption, J. Cloud Comput. 12(1) (2023) 47. doi: 10.1186/s13677-023-00425-7.

[18] F. Makoui, T. Gulliver, M. Dakhilalian, A New Code-Based Digital Signature Based on the McEliece Cryptosystem, IET Commun. 17(10) (2023) 1199–1207. doi: 10.1049/cmu2.12607.

[19] R. McEliece, A Public-Key Criptosystem Based on Algebraic Coding Theory, DSN Progress Report (1978) 42–44.

[20] F. Dupont, A New Shamir's Three Pass Random Matrix Ciphering Mechanism, J. Comput. Virol. Hacking Tech. (2023). doi: 10.1007/s11416-023-00467-0.

[21] E. Faure, et al., A Method for Reliable Permutation Transmission in Short-Packet Communication Systems, Information Technology for Education, Science, and Technics (2023) 177–195. doi: 10.1007/978-3-031-35467-0_12.

[22] E. Faure, et al., Concept for Using Permutation-Based Three-Pass Cryptographic Protocol in Noisy Channels, Systems, Decision and Control in Energy V (2023) 99–113. doi: 10.1007/978-3-031-35088-7_7.

[23] E. Faure, et al., Permutation-Based Block Code for Short Packet Communication Systems, Sensors 22(14) (2022). doi: 10.3390/s22145391.

[24] J. Al-Azzeh, et al., Permutation-Based Frame Synchronization Method for Data Transmission Systems with Short Packets, Egyptian Inform. J. 23(3) (2022) 529–545. doi: 10.1016/j.eij.2022.05.005.

[25] A. Shcherba, et al., Families of Square Commutative 2x2 Matrices, in: Cybersecurity Providing in Information and Telecommunication Systems (2023).

[26] T. Springer, Linear Algebraic Groups, 2nd ed., Modern Birkhäuser Classic (1998). doi: 10.1007/978-0-8176-4840-4.

[27] A. Baker, Matrix Groups. An Introduction to Lie Group Theory, Springer (2002). doi: 10.1007/978-1-4471-0183-3.

[28] F. Gantmacher, The Theory of Matrices, Reprinted, American Mathematical Society, Providence, RI (1959).

[29] R. Horn, C. Johnson, Matrix Analysis, 2nd ed., Cambridge University Press (2012). doi: 10.1017/CBO9781139020411.

[30] K. Ireland, M. Rosen, A Classical Introduction to Modern Number Theory, Graduate texts in mathematics, 2nd ed., Springer-Verlag, New York (1990).