# Three-Pass Protocol on Permutations: Implementation Example and Security

Emil Faure[1, 2], Anatoly Shcherba[1], Artem Lavdanskyi[1], Mykola Makhynko[3], and Muhabbat Khizirova[4]

[1] *Cherkasy State Technological University, Cherkasy, 18006, Ukraine*
[2] *State Scientific and Research Institute of Cybersecurity Technol. and Inform. Protection, Kyiv, 03142, Ukraine*
[3] *GoodLabs Studio Inc., Toronto, ON M5H 3E5, Canada*
[4] *Almaty University of Power Engineering and Telecommunications named after Gumarbek Daukeyev, Almaty, 050013, Kazakhstan*

**Abstract**

The existing exponentiation-based three-pass cryptographic protocols are not secure against attacks using hypothetic quantum computers. This paper will review the research conducted on the cryptographic security of the three-pass protocol on permutations. An informational message is a permutation $\pi$ of a given length $M$. The operations of cryptographic transformation for the proposed protocol are the operations of multiplying permutations, exponentiation of their disjoint cycles, and the operation of finding a conjugate permutation. The steps for implementing the protocol are described in detail. The protocol uses a permutation $\alpha$, Alice's secret key $\overline{s}$, and Bob's secret keys $\overline{r}$ and $\chi_B$. All disjoint cycles in the permutation $\chi_B$ decomposition have different lengths. The length of all $\alpha$ disjoint cycles is pairwise coprime with the length of $\chi_B$ disjoint cycles. The protocol correctness and single solution are proved. An example of the protocol implementation for $M = 7$ is presented. The Alice's key space size equals the product of $\alpha$ disjoint cycles length. Bob's key space size equals the product of $\alpha$ disjoint cycle length and the number of possible $\chi_B$ permutations with a suitable structure. The protocol resistance to some statistical ciphertext-only attacks has been investigated. It is shown that even if the cryptanalyst is informed about the structure of $\alpha$ and $\chi_B$ cycles, he will not be able to determine permutation $\pi$, neither does this knowledge disclose the keys $\overline{s}$, $\overline{r}$, $\chi_B$ values; the cryptanalyst cannot reduce the size of the potential permutation $\pi$ set to a value less than the size of Alice's key space; even knowing the key $\chi_B$ structure and having checked all possible vector $\overline{r}$ values, the cryptanalyst will not be able to determine the key $\overline{r}$; cryptanalyst will not be able to determine the structure of $\chi_B$ cycles by going through all possible $\overline{r}$ values. The transformation security is based on the complexity of permutation factorization, as well as on the complexity of implementing transformations that are inverse to nonlinear operations based on the identical cycle structure of conjugate permutations. The protocol keys must be changed after being used. Channel error protection must be provided when implementing the protocol.

**Keywords**

Permutation, three-pass protocol, cryptographic strength, security, cryptographic system, operations on permutations, conjugate permutations.



## 1. Introduction

The three-step protocol allows messages to be transmitted securely between two parties without transferring or disclosing either public or private encryption keys [1–5].

The first three-pass protocol was suggested by Adi Shamir in the 1980s, however, the protocol was not published at the time. The three-pass protocol is based on the concept

CPITS-2024: Cybersecurity Providing in Information and Telecommunication Systems, February 28, 2024, Kyiv, Ukraine
EMAIL e.faure@chdtu.edu.ua (E. Faure); a.shcherba@chdtu.edu.ua (A. Shcherba); a.lavdanskyi@chdtu.edu.ua (A. Lavdanskyi); nmakhinko@goodlabs.studio (M. Makhynko); m.khizirova@aues.kz (M. Khizirova)
ORCID: 0000-0002-2046-481X (E. Faure); 0000-0002-3049-3497 (A. Shcherba); 0000-0002-1596-4123 (A. Lavdanskyi); 0000-0002-4064-8894 (M. Makhynko); 0000-0002-2242-7756 (M. Khizirova)

that each party has a private encryption key and a private decryption key. Both parties use their keys independently, to encrypt the message first, and decrypt the message afterward.

The protocol uses the encryption function $E$ and the decryption function $D$. The encryption function and the decryption function may or may not coincide. The encryption function uses an encryption key $e$ to change a plaintext message $m$ into a ciphertext $E(e,m)$. Each encryption key $e$ has a corresponding decryption key $d$, which allows to recovery of the original text using the decryption function $D\big(d,E(e,m)\big)$.

For the encryption function $E$ and the decryption function $D$ to be suitable for the three-pass protocol, the condition $D\left(d,E\big(k,E(e,m)\big)\right)=E(k,m)$ should be fulfilled for any message $m$, any encryption key $e$ with corresponding decryption key $d$, and any independent encryption key $k$. In other words, the first encryption must be decrypted with the key $e$, even if the message is encrypted with the second key $k$. This property is characteristic of the commutative encryption where $E\big(a,E(b,m)\big)=E\big(b,E(a,m)\big)$ for any of the keys $a$ and $b$, and for every message $m$. Commutative encryptions satisfy the equation $D\left(d,E\big(k,E(e,m)\big)\right)=D\left(d,E\big(e,E(k,m)\big)\right)=E(k,m)$.

Suppose Alice wants to send a message to Bob. In this case, the three-pass protocol works as follows [6].

1. Alice selects a private encryption key $s$ and a corresponding decryption key $t$. Alice encrypts the original message $m$ with the key $s$ and sends the ciphertext $E(s,m)$ to Bob.
2. Bob selects a private encryption key $r$ and a corresponding decryption key $q$, encrypts the first message $E(s,m)$ with the key $r$, and sends the doubly encrypted message $E\big(r,E(s,m)\big)$ back to Alice.
3. Alice decrypts the second message with the key $t$. Due to the commutativity property described here $D\left(t,E\big(r,E(s,m)\big)\right)=E(r,m)$, which means that the message is encrypted only with Bob's private key. Alice sends this ciphertext to Bob.
4. Bob decrypts the third message with the key $q$ and receives the original message $D\big(q,E(r,m)\big)=m$.

It should be noted that all the operations involving Alice's private keys $s$ and $t$ are performed by Alice, and all of the operations involving Bob's private keys $r$ and $q$ are performed by Bob. Thus, neither party needs to know the other party's keys.

## 1.1. State of the Art in Three-Pass Cryptoprotocols

Shamir No-Key Protocol [7], which was developed in the 1980s, uses exponentiation modulo a large prime number as both encryption and decryption functions, that is, $E(e,m)=m^e \bmod p$ and $D(d,m)=m^d \bmod p$, where $p$ is a large prime [8]. For any encryption, the exponent $e$ is found within the range $[1,\dots,p-1]$ with $gcd(e,p-1)=1$. The corresponding decryption exponent $d$ is selected such that $de \bmod (p-1)=1$. It follows from Fermat's Little Theorem that $D\big(d,E(e,m)\big)=m^{de} \bmod p=m$. The Shamir protocol has the commutativity property because $E\big(a,E(b,m)\big)=m^{ab} \bmod p=m^{ba} \bmod p=E\big(b,E(a,m)\big)$.

There are many implementations of the Shamir protocol with various encryption methods.

In particular, this protocol can be used for exchanging images securely. Surveys such as that conducted in [9] offer a secure no-key-exchange image-sharing scheme. This scheme uses a Multiple-Parameter Fractional Fourier Transform as a cryptographic algorithm for the three-pass protocol.

Another implementation of the Shamir protocol in quantum cryptography is the quantum three-stage protocol [10], which uses the property of quantum superposition. An improvement to this protocol has been proposed in [11].

The Massey-Omura Cryptosystem [8, 12] was originally proposed by James Massey and Jim K. Omura in 1982 as a possible upgrade over the Shamir protocol. There are two options for implementing the Massey-Omura protocol: the classical one and the elliptical one. The first option is built on the complexity of the discrete logarithm problem, the second option is based on the properties of an elliptic curve.

The Massey-Omura method uses exponentiation in the Galois field $GF(2^n)$ as both the encryption and decryption functions. Thereby, $E(e,m) = m^e \, mod \, p$ and $D(d,m) = m^d \, mod \, p$, where $p = 2^n$. Similar to the Shamir protocol, the exponent $e$ is found within the range $[1, \dots, p-1]$ with $gcd(e, p-1) = 1$. The corresponding decryption exponent $d$ is calculated to ensure $de \, mod(p-1) = 1$. Since the multiplicative group of the Galois field $GF(2^n)$ has order $2^n - 1$, the Lagrange's theorem implies that $D\big(d, E(e,m)\big) = = m^{de} \, mod \, p = m$ for all $m$ in $GF(2^n)$.

The elliptic version of the Massey-Omura cryptosystem provides for the representation of the message $m$ to be transmitted by the point $P_m$ of the elliptic curve $\varepsilon$ above the finite field.

The total number of points on the curve (the order of the elliptic curve) $N$ is calculated and unclassified. Each user of the system chooses a random integer $e: 1 < e < N$, $gcd(e, N) = 1$. Using the Euclid's algorithm, the inverse value $d: de \, mod \, N = 1$ is found. By using $e$ and $d$, and any point $P_m$ on the elliptic curve, it is now possible to calculate $E(e, P_m) = eP_m \, mod \, N$, whereas $D\big(d, E(e, P_m)\big) = deP_m \, mod \, N = P_m$. Calculating point $P_m$ by $eP_m$ is equivalent to solving the discrete logarithm problem for an elliptic curve.

Recently, new studies have emerged that are aimed at developing the three-pass cryptographic protocol, in particular, by applying new transformation algorithms, as well as implementing the protocol in new applications.

The eligibility of the H-Rabin algorithm, which belongs to the class of public key cryptosystems, as a candidate algorithm for the three-pass protocol is studied in [13, 14]. Unlike the well-known RSA and Rabin public key cryptosystems, the H-Rabin's security depends on the complexity of factoring three large prime numbers rather than two.

Other studies [15–18] have considered Vigenere cipher as an algorithm for the cryptographic process. However, to perform a cryptanalysis of this algorithm, it is worth considering the well-known effective methods of attacks on the Vigenère cipher, for example, such as the Kasiski examination [19] and the Friedman test [20].

The authors of the research [21] confirm the efficiency of using the Massey-Omura protocol in the tasks of file protection in Android.

The study [22] uses the Shamir three-pass protocol modified with the ElGamal algorithm for AES key exchange in an ad hoc 802.11 network.

The authors of the study [23] evaluate the effectiveness of the Pohlig-Hellman algorithm [24] for implementing a three-pass protocol.

The authors in [25] prove, that the RSA algorithm can be used as an encryption algorithm in the Shamir three-pass protocol since it has the commutative property required by the three-pass protocol.

In the literature [26], the researchers propose a new method for deniable encryption based on commutative transformations. This method includes the following cryptographic primitives as its three basic components: the Diffie-Hellman public key agreement protocol, the Pohlig-Hellman commutative encryption algorithm, and Shamir's no-key encryption protocol. To perform commutative encryption, the method uses an exponentiation cipher.

Nonetheless, it has been proved in [27] that the used exponentiation cipher is as secure as the discrete logarithm problem is hard. Therefore, the exponentiation-based cryptographic protocols are not secure against attacks using hypothetic quantum computers.

The authors in [27] propose post-quantum implementation of the three-pass no-key encryption protocol. The proposed protocol is based on exponentiation and factorization operations. It involves a larger volume of data transmitted by a communication channel as compared with the Shamir algorithm (10 messages versus 3), as well as a larger number of operations performed by each of the parties.

Further, in the study [28], the authors have developed a post-quantum no-key protocol based on the commutative cipher introduced earlier that 'seems more attractive for practical applications' [29, 30]. This cipher performs transformations of such algebraic structures as vectors and their global right-sided and two-sided units. At the same time, exponentiation remains the encryption operation.

This paper will give an account of a fundamentally new approach to building a three-pass cryptographic protocol. It is based on presenting an informational message as a permutation of numbers $\pi$ of a given length $M$.

A permutation on a set of $M$ elements is a bijective function of a finite set $X$ of size $M$ to itself. The elements of the finite set $X$ will be denoted by non-negative integers from 0 to $M-1$. Then $X=\{0,1,\dots,M-1\}$, while permutation $\pi$ will be denoted as a sequence of elements of the set $X$, wherein each of the numbers $\{0,1,\dots,M-1\}$ is only used once (without gaps or repetitions). The set of all permutations on the set $X$ will be denoted by $S_M$. A similar representation of the information message as a permutation of numbers is used in factorial data coding [31–39], as well as in the cryptographic key exchange method [40]. The operations of cryptographic transformation for the proposed protocol are the operations of multiplying permutations, exponentiation of their disjoint cycles, and the operation of finding a conjugate permutation. The transformation security is based on the complexity of permutation factorization, as well as on the complexity of implementing transformations that are inverse to nonlinear operations based on the identical cycle structure of conjugate permutations.

The purpose of this paper is to study the security of a three-pass cryptographic protocol on permutations against ciphertext-only attacks.

### 1.2. Paper Structure

Section 2 details an outline of the basic concepts for the three-pass protocol on permutations, proves the protocol's correctness and presents a case study for its implementation. Section 3 studies the three-pass protocol cryptographic strength, in particular, key space size and protocol statistical properties due to the application of different approaches to protocol attack based on known cyphertext. Section 4 presents a cryptographic system and describes the principles underlying its functioning. Section 5 discusses the results, summarizes the findings, and concludes the paper.

## 2. The Concept of a Three-Pass Protocol on Permutations

An approach to constructing a three-pass protocol based on permutations was first presented in [41]. An essential feature of the proposed approach is the use of linear and nonlinear operations on permutations, including those on the conjugate permutations.

### 2.1. Three-Pass Protocol Construction

The three-pass protocol includes the following procedures:

- Permutation $\alpha \in S_M$ and its decomposition into a product of disjoint cycles $\alpha = \prod_{i=1}^{n(\alpha)} \alpha_i$ is known to Alice and Bob.
- Alice randomly generates her secret key as a $n(\alpha)$-dimensional vector $\overline{s} = = (s_1, s_2, \dots, s_{n(\alpha)})$, where $0 \le s_i \le l(\alpha_i)-1$, $l(\alpha_i)$ is the cycle $\alpha_i$ order. Next, Alice generates a key permutation $\sigma_A = \prod_{i=1}^{n(\alpha)} \alpha_i^{s_i}$ and its inverse: $\sigma_A^{-1} = \prod_{i=1}^{n(\alpha)} \left(\alpha_{n(\alpha)+1-i}^{s_{n(\alpha)+1-i}}\right)^{-1}$. Alice keeps the vector $\overline{s}$ and permutations $\sigma_A$ and $\sigma_A^{-1}$ secret.
- Bob randomly generates his private key as a $n(\alpha)$-dimensional vector $\overline{r} = = (r_1, r_2, \dots, r_{n(\alpha)})$, where $0 \le r_i \le l(\alpha_i)-1$. Next, Bob forms a key permutation $\sigma_B = \prod_{i=1}^{n(\alpha)} \alpha_i^{r_i}$ and its inverse: $\sigma_B^{-1} = \prod_{i=1}^{n(\alpha)} \left(\alpha_{n(\alpha)+1-i}^{r_{n(\alpha)+1-i}}\right)^{-1}$. In addition, Bob randomly generates a permutation $\chi_B \in S_M$. Bob keeps the vector $\overline{r}$ and permutations $\sigma_B$, $\sigma_B^{-1}$ and $\chi_B$ secret.

**Remark 1.** All disjoint cycles $\chi_{jB}$ in the permutation decomposition $\chi_B = \prod_{j=1}^{n(\chi_B)} \chi_{jB}$ have different length: $l(\chi_{iB}) \ne l(\chi_{jB})$ for $\forall i \ne j$.

**Remark 2.** The length of all disjoint cycles $\alpha_i$ in the permutation decomposition $\alpha = \prod_{i=1}^{n(\alpha)} \alpha_i$ is pairwise coprime with the length of disjoint cycles $\chi_{jB}$ in the permutation decomposition $\chi_B = \prod_{j=1}^{n(\chi_B)} \chi_{jB}$: $gcd\left(l(\alpha_i); l(\chi_{jB})\right) = 1$ for $\forall i, j$.

- To securely transmit permutation $\pi \in S_M$, Alice generates a ciphertext $Y_1 = \sigma_A \cdot \pi$. She sends $Y_1$ to Bob.
- Bob encrypts the received message $Y_1$: $Y_2 = \sigma_B \cdot Y_1 \cdot \chi_B$. He then sends $Y_2$ to Alice.
- Alice forms a permutation $\pi^{-1}$ inverse to $\pi$ and "removes" her key $\sigma_A$: $Y_3 = \sigma_A^{-1} \cdot Y_2 \times \pi^{-1}$. She transmits $Y_3$ to Bob.
- Bob "removes" his key $\sigma_B$: $Y_4 = \sigma_B^{-1} \cdot Y_3$. Next, Bob represents $Y_4$ as a product of

disjoint cycles: $Y_4 = \prod_{k=1}^{n(Y_4)} Y_{k4}$. After that, Bob finds $\prod_{j=1}^{n(\chi_B)} l(\chi_{jB})$ possible permutations $\pi$ from the expression $Y_4 = \prod_{j=1}^{n(\chi_B)} \left(\pi(\chi_{1jB}), \pi(\chi_{2jB}), \dots, \pi\left(\chi_{l(\chi_{jB})jB}\right)\right)$ based on the known $Y_4$ and $\chi_B$. By going through $Y_1 \cdot \pi^{-1} = \prod_{i=1}^{n(\alpha)} \alpha_i^{s_i}$, Bob chooses one correct permutation from $\prod_{j=1}^{n(\chi_B)} l(\chi_{jB})$ possible permutations $\pi$.

## 2.2. Correctness

This section demonstrates that if Alice and Bob perform the above steps, they will implement a three-pass protocol.

Alice calculates $Y_1 = \sigma_A \cdot \pi$. Bob calculates $Y_2 = \sigma_B \cdot Y_1 \cdot \chi_B = \sigma_B \cdot \sigma_A \cdot \pi \cdot \chi_B$. Alice calculates $Y_3 = \sigma_A^{-1} \cdot \sigma_B \cdot \sigma_A \cdot \pi \cdot \chi_B \cdot \pi^{-1}$.

Here, we demonstrate that permutations $\sigma_A$ and $\sigma_B$ commute with each other. The product of $\sigma_A$ and $\sigma_B$ is $\sigma_A \cdot \sigma_B = \prod_{i=1}^{n(\alpha)} \alpha_i^{s_i} \cdot \prod_{i=1}^{n(\alpha)} \alpha_i^{r_i}$. Since the cycles $\{\alpha_i\}$, where $1 \le i \le n(\alpha)$, are pairwise disjoint, we receive

$$\sigma_A \cdot \sigma_B = \prod_{i=1}^{n(\alpha)} \alpha_i^{s_i} \cdot \prod_{i=1}^{n(\alpha)} \alpha_i^{r_i} = \prod_{i=1}^{n(\alpha)} \alpha_i^{s_i+r_i} = \prod_{i=1}^{n(\alpha)} \alpha_i^{r_i+s_i} = \prod_{i=1}^{n(\alpha)} \alpha_i^{r_i} \cdot \prod_{i=1}^{n(\alpha)} \alpha_i^{s_i} = \sigma_B \cdot \sigma_{A.}$$

Hence it follows that:

$$Y_3 = \sigma_A^{-1} \cdot \sigma_B \cdot \sigma_A \cdot \pi \cdot \chi_B \cdot \pi^{-1} = \sigma_A^{-1} \cdot \sigma_A \cdot \sigma_B \times \times \pi \cdot \chi_B \cdot \pi^{-1} = \sigma_B \cdot \pi \cdot \chi_B \cdot \pi^{-1}.$$

Bob calculates $Y_4 = \sigma_B^{-1} \cdot \sigma_B \cdot \pi \cdot \chi_B \cdot \pi^{-1} = \pi \times \chi_B \cdot \pi^{-1}$. It follows from the latter expression that the permutations $Y_4, \chi_B \in S_M$ are conjugate. Therefore, the permutations $Y_4$ and $\chi_B$ are of the same cycle structure: their decompositions into a product of disjoint cycles for any $l$ containing the same number of cycles of length $l$. Since $l(\chi_{iB}) \ne l(\chi_{jB})$ for $\forall i \ne j$, the number of cycles of length $l$ for any $l$ equals to unity. Additionally, $Y_4 = \pi \cdot \chi_B \cdot \pi^{-1} = \pi \cdot \prod_{j=1}^{n(\chi_B)} \chi_{jB} \cdot \pi^{-1}$. If the cycles $\chi_{jB}$ are represented as $\chi_{jB} = \left(\chi_{1jB}, \chi_{2jB}, \dots, \chi_{l(\chi_{jB})jB}\right)$, where $1 \le j \le n(\chi_B)$, then $Y_4 = \pi \cdot \prod_{j=1}^{n(\chi_B)} \left(\chi_{1jB}, \chi_{2jB}, \dots, \chi_{l(\chi_{jB})jB}\right) \cdot \pi^{-1} = \prod_{j=1}^{n(\chi_B)} \left(\pi(\chi_{1jB}), \pi(\chi_{2jB}), \dots, \pi\left(\chi_{l(\chi_{jB})jB}\right)\right)$.

Therefore, the number of possible solutions $\pi$ for the equation $Y_4 = \pi \cdot \chi_B \cdot \pi^{-1}$ with known $Y_4$ and $\chi_B$ is determined by element positions $\chi_{1jB}, \chi_{2jB}, \dots, \chi_{l(\chi_{jB})jB}$ in cycles $\chi_{jB}$ (or elements $\pi(\chi_{1jB}), \pi(\chi_{2jB}), \dots, \pi\left(\chi_{l(\chi_{jB})jB}\right)$ in cycles $\pi(\chi_{jB})$) and equal to $\prod_{j=1}^{n(\chi)} l(\chi_{jB})$.

Here, we prove that only one of the possible $\pi$ values satisfies the condition $Y_1 \cdot \pi^{-1} = \prod_{i=1}^{n(\alpha)} \alpha_i^{s_i}$.

**Theorem 1.** Let $\chi_B^{\overline{\mu}} = \prod_{j=1}^{n(\chi_B)} \chi_{jB}^{\mu_j}$ be for $\chi_B = \prod_{j=1}^{n(\chi_B)} \chi_{jB}$, $\overline{\mu} = (\mu_1, \dots, \mu_{n(\chi)})$. In this case, permutation

$$g_{\overline{\mu}} 3 = \sigma_A \cdot \pi \cdot \chi_B^{\overline{\mu}} \cdot \pi^{-1} \qquad (1)$$

has the cycle representation

$$g_{\overline{\mu}} = \prod_{i=1}^{n(\alpha)} \alpha_i^{\lambda_i} \qquad (2)$$

where $\overline{\lambda} = (\lambda_1, \dots, \lambda_{n(\alpha)})$, $0 \le \lambda_i \le l(\alpha_i) - 1$, if and only if $\overline{\mu} = \overline{0}$ (i.e. $\mu_j = 0$ for $\forall j \in 1, \dots, n(\chi_B)$).

*Proof.*

It is obvious that when $\overline{\mu} = \overline{0}$, we receive $g_{\overline{\mu}} = \sigma_A$.

Here, we assume that $g_{\overline{\mu}} = \prod_{i=1}^{n(\alpha)} \alpha_i^{\lambda_i}$. Then the permutation

$$G_{\overline{\mu}} = \sigma_A^{-1} \cdot g_{\overline{\mu}} = \prod_{i=1}^{n(\alpha)} \left(\alpha_{n(\alpha)+1-i}^{s_{n(\alpha)+1-i}}\right)^{-1} \cdot \prod_{i=1}^{n(\alpha)} \alpha_i^{\lambda_i} = \prod_{i=1}^{n(\alpha)} \alpha_i^{\Lambda_i} \qquad (3)$$

where $0 \le \Lambda_i \le l(\alpha_i) - 1$.

At the same time, it follows from (1) that $G_{\overline{\mu}} = \sigma_A^{-1} \cdot g_{\overline{\mu}} = \pi \cdot \chi_B^{\overline{\mu}} \cdot \pi^{-1}$, and the permutations $G_{\bar{\mu}}$ and $\chi_B^{\overline{\mu}}$ are conjugate and are of identical cycle structure. The conditions of Remark 2 are sufficient for the equation $G_{\overline{\mu}} = \sigma_A^{-1} \cdot g_{\overline{\mu}} = \pi \cdot \chi_B^{\overline{\mu}} \cdot \pi^{-1}$ to be possible only in the case when $\chi_B^{\overline{\mu}} = e = \sigma_A^{-1} \cdot g_{\overline{\mu}}$, where $e$ is the identical permutation, that is, $\sigma_A^{-1} = g_{\overline{\mu}}$.

**Theorem 2.** Only one of $\prod_{j=1}^{n(\chi_B)} l(\chi_{jB})$ possible $\pi$ values satisfies the condition $Y_1 \cdot \pi^{-1} = \prod_{i=1}^{n(\alpha)} \alpha_i^{s_i}$.

*Proof.*

We keep in mind that $Y_4 = \pi(\chi_B)$. With $Y_4$ and $\chi_B$ known, any permutation $\pi$ value that satisfies the equality $Y_4 = \pi \cdot \chi_B^{-\overline{v}}$ will become a solution to the equation $Y_4 = \pi(\chi_B)$. The number of such permutations is equal to the size of the set of possible vectors $\overline{v} = (v_1, \dots, v_{n(\chi)})$, which is $\prod_{j=1}^{n(\chi_B)} l(\chi_{jB})$.

Let $\exists \overline{v_0}$: $Y_4 = \pi \cdot \chi_B^{-\overline{v_0}}$.

Here, we consider all possible permutations

$$Z_{\overline{v_0}-\overline{v}} = Y_4 \cdot \chi_B^{\overline{v}} = \pi \cdot \chi_B^{\overline{v}-\overline{v_0}}$$

and

$$g_{\overline{v_0}-\overline{v}} = Y_1 \cdot Z_{\overline{v_0}-\overline{v}}^{-1} = \sigma_A \cdot \pi \cdot \chi_B^{\overline{v_0}-\overline{v}} \cdot \pi^{-1}$$

for all possible vectors $\overline{v}$.

Due to Theorem 1, there can only be one possible exponent $\overline{v_0} - \overline{v} = 0$ for which permutation $g_{\overline{v_0}-\overline{v}}$ has the cycle representation $g_{\overline{\mu}} = \prod_{i=1}^{n(\alpha)} \alpha_i^{\lambda_i}$.

The maximum number of permutations $\pi$ used in checking $Y_1 \cdot \pi^{-1} = \prod_{i=1}^{n(\alpha)} \alpha_i^{s_i}$ is $\prod_{j=1}^{n(\chi_B)} l(\chi_{jB})$.

## 2.3. Example of the Protocol Implementation

In the following, we consider an example of implementing the three-pass protocol on permutations for length $M = 7$.

Let Alice and Bob choose the following permutation $\alpha = \{3,6,0,2,4,1,5\}$, which decomposes into the product of the following disjoint cycles:

$$\alpha_1 = (0,3,2);$$
$$\alpha_2 = (1,6,5);$$
$$\alpha_3 = (4).$$

Therefore, $n(\alpha) = 3$, while permutation $\alpha$ can be presented as $\alpha = (0,3,2)(1,6,5)$. The permutations length is $l(\alpha_1) = 3$, $l(\alpha_2) = 3$, $l(\alpha_3) = 1$.

Let Alice generate her secret key in the following form:

$$\overline{s} = (2,2,0)$$

Alice calculates key permutation $\sigma_A = \prod_{i=1}^{n(\alpha)} \alpha_i^{s_i}$ and its inverse $\sigma_A^{-1}$:

$(\alpha_1)^2 = (0,3,2)^2 = (0,2,3);$
$(\alpha_2)^2 = (1,6,5)^2 = (1,5,6);$
$(\alpha_3)^0 = (4);$
$\sigma_A = (0,2,3)(1,5,6)(4) = \{2,5,3,0,4,6,1\};$
$\sigma_A^{-1} = \{3,6,0,2,4,1,5\}.$

Let Bob generate his secret key as follows:

$$\overline{r} = (2,1,0)$$

Bob calculates key permutation $\sigma_B = \prod_{i=1}^{n(\alpha)} \alpha_i^{r_i}$ and its inverse $\sigma_B^{-1}$:

$(\alpha_1)^2 = (0,3,2)^2 = (0,2,3);$
$(\alpha_2)^1 = (1,5,6);$
$(\alpha_3)^0 = (4);$
$\sigma_B = (0,2,3)(1,5,6)(4) = \{2,6,3,0,4,1,5\};$
$\sigma_B^{-1} = \{3,5,0,2,4,6,1\}.$

Let Bob form an additional permutation $\chi_B = (0,6)(1,5,3,2,4) = \{6,5,4,2,1,3,0\}$.

Let Alice transmit permutation $\pi = \{3,2,1,6,0,4,5\}$. The permutation inverse to $\pi$ is: $\pi^{-1} = \{4,2,1,0,5,6,3\}$.

Alice forms the ciphertext $Y_1 = \sigma_A \cdot \pi$ and sends it to Bob:

$Y_1 = \{2,5,3,0,4,6,1\}\{3,2,1,6,0,4,5\} = \{0,3,5,1,2,4,6\}$

Bob encrypts the received message $Y_1$: $Y_2 = \sigma_B \times Y_1 \cdot \chi_B$ and sends it to Alice:

$Y_2 = \{2,6,3,0,4,1,5\}\{0,3,5,1,2,4,6\}\{6,5,4,2,1,3,0\} =$
$= \{2,6,3,0,4,1,5\}\{6,4,2,5,3,1,0\} = \{5,4,3,1,0,6,2\}.$

Alice "removes" her encryption key $\sigma_A^{-1}$ using reverse permutation $\pi^{-1}$: $Y_3 = \sigma_A^{-1} \cdot Y_2 \cdot \pi^{-1}$ and sends $Y_3$ to Bob:

$Y_3 = \{3,6,0,2,4,1,5\}\{5,4,3,1,0,6,2\}\{4,2,1,0,5,6,3\} =$
$= \{3,6,0,2,4,1,5\}\{0,3,4,5,6,2,1\} = \{3,2,4,1,5,0,6\}.$

Bob "removes" his key $\sigma_B^{-1}$: $Y_4 = \sigma_B^{-1} \cdot Y_3$:

$Y_4 = \{3,5,0,2,4,6,1\}\{3,2,4,1,5,0,6\} = \{2,0,4,5,6,3,1\}$

Next, Bob represents $Y_4$ as a product of disjoint cycles:

$$Y_4 = \{2,0,4,5,6,3,1\} = (3,5)(0,2,4,6,1)$$

To find $\pi$ value, Bob has to form $\prod_{j=1}^{n(\chi_B)} l(\chi_{jB}) = 2 \cdot 5 = 10$ of possible $\pi$ values and perform a check for each of them. Some of the possible $\pi$ values are given below.

1. $\begin{cases} \pi(0) = 3; \\ \pi(6) = 5; \\ \pi(1) = 0; \\ \pi(5) = 2; \\ \pi(3) = 4; \\ \pi(2) = 6; \\ \pi(4) = 1. \end{cases} \Leftarrow \begin{array}{l} \pi = \{3,0,6,4,1,2,5\}, \\ \pi^{-1} = \{1,4,5,0,3,6,2\}, \\ Y_1 \cdot \pi^{-1} = \\ = \{0,3,5,1,2,4,6\}\{1,4,5,0,3,6,2\} \\ = \\ = (0,3)(1,2,4)(5,6). \end{array}$

2. $\begin{cases} \pi(6) = 3; \\ \pi(0) = 5; \\ \pi(5) = 0; \\ \pi(3) = 2; \\ \pi(2) = 4; \\ \pi(4) = 6; \\ \pi(1) = 1. \end{cases} \Leftarrow \begin{array}{l} \pi = \{5,1,4,2,6,0,3\}, \\ \pi^{-1} = \{5,1,3,6,2,0,4\}, \\ Y_1 \cdot \pi^{-1} = \\ = \{0,3,5,1,2,4,6\}\{5,1,3,6,2,0,4\} \\ = \\ = (0,4,5)(1,3,6,2). \end{array}$

3. $\begin{cases} \pi(0) = 3; \\ \pi(6) = 5; \\ \pi(4) = 0; \\ \pi(1) = 2; \\ \pi(5) = 4; \\ \pi(3) = 6; \\ \pi(2) = 1. \end{cases} \Leftarrow \begin{array}{l} \pi = \{3,2,1,6,0,4,5\}, \\ \pi^{-1} = \{4,2,1,0,5,6,3\}, \\ Y_1 \cdot \pi^{-1} = \\ = \{0,3,5,1,2,4,6\}\{4,2,1,0,5,6,3\} \\ = \\ = (0,2,3)(1,5,6). \end{array}$

Out of the formed possible $\pi$ values, the structure of the product $Y_1 \cdot \pi^{-1}$ is the same as that of $\alpha$, and each $Y_1 \cdot \pi^{-1}$ cycle is an exponent of the $\alpha$ cycle for only one value of $\pi = \{3,2,1,6,0,4,5\}$. This is how Bob determines that the message having been delivered is $\pi = \{3,2,1,6,0,4,5\}$.

Here, we consider an example where the lengths of permutation $\alpha$ cycles are not coprime with the lengths of permutation $\chi_B$ cycles. Let $\alpha = \{3,6,5,2,4,0,1\} = (0,3,2,5)(1,6)$, and $\chi_B = \{5,2,4,0,1,6,3\} = (0,5,6,3)(1,2,4)$.

Let Alice and Bob generate secret keys in the following form: $\overline{s} = (3,1,0)$, $\overline{r} = (2,1,0)$. Then $\sigma_A = \{5,6,3,0,4,2,1\}$, $\sigma_B = \{2,6,0,5,4,3,1\}$.

Let Alice transmit the permutation $\pi = = \{2,6,4,3,1,5,0\}$. Its reverse permutation is $\pi^{-1} = \{6,4,0,3,2,5,1\}$. Then the messages $Y_1 - Y_4$ are as follows:

$Y_1 = \{3,1,4,0,6,2,5\}$;
$Y_2 = \{0,4,1,5,6,3,2\}$;
$Y_3 = \{5,1,3,0,6,2,4\}$;
$Y_4 = \{3,6,5,2,1,0,4\} = (1,6,4)(0,3,2,5)$.

Here, we give the $\pi$ values such that the cycle structure of the product $Y_1 \cdot \pi^{-1}$ coincides with that of $\alpha$, and each $Y_1 \cdot \pi^{-1}$ cycle is a power of $\alpha$ cycle.

4. $\begin{cases} \pi(4) = 1; \\ \pi(1) = 6; \\ \pi(2) = 4; \\ \pi(0) = 0; \\ \pi(5) = 3; \\ \pi(6) = 2; \\ \pi(3) = 5. \end{cases}$ $\pi = \{0,6,4,5,1,3,2\}$, $\pi^{-1} = \{0,4,6,5,2,3,1\}$, $Y_1 \cdot \pi^{-1} = = \{3,1,4,0,6,2,5\}\{0,4,6,5,2,3,1\} = = (0,3,2,5)(1,6)$.

5. $\begin{cases} \pi(4) = 1; \\ \pi(1) = 6; \\ \pi(2) = 4; \\ \pi(6) = 0; \\ \pi(3) = 3; \\ \pi(0) = 2; \\ \pi(5) = 5. \end{cases}$ $\pi = \{2,6,4,3,1,5,0\}$, $\pi^{-1} = \{6,4,0,3,2,5,1\}$, $Y_1 \cdot \pi^{-1} = = \{3,1,4,0,6,2,5\}\{6,4,0,3,2,5,1\} = = (0,5,2,3)(1,6)$.

6. $\begin{cases} \pi(4) = 1; \\ \pi(1) = 6; \\ \pi(2) = 4; \\ \pi(3) = 0; \\ \pi(0) = 3; \\ \pi(5) = 2; \\ \pi(6) = 5. \end{cases}$ $\pi = \{3,6,4,0,1,2,5\}$, $\pi^{-1} = \{3,4,5,0,2,6,1\}$, $Y_1 \cdot \pi^{-1} = = \{3,1,4,0,6,2,5\}\{3,4,5,0,2,6,1\} = = (1,6)$.

Thus, the given example shows that if the lengths of permutation $\alpha$ cycles are not coprime with the lengths of permutation $\chi_B$ cycles, a situation may arise when Bob will not be able to determine the permutation $\pi$ value.

# 3. Protocol Security

The analysis of the proposed three-pass protocol security embraced the following areas:

1. Keyspace size.
2. Distributions of $Y_1$, $Y_2$, $Y_3$, $Y_4$ values depending on $\pi$ values.
3. Distributions of $Y_1$, $Y_2$, $Y_3$ values depending on $\overline{s}$, $\overline{r}$, and $\chi_B$ values.
4. Number of possible permutations $\pi$ satisfying the equation $Y_1 = \sigma_A \cdot \pi$ when $Y_1$ value and $\alpha$ cycle structure are known.
5. Number of key pairs $\sigma_B$, $\chi_B$ satisfying equation $Y_3 = \sigma_B \cdot \pi \cdot \chi_B \cdot \pi^{-1}$.
6. Distribution of $Y_3 = \sigma_B \cdot \pi \cdot \chi_B \cdot \pi^{-1}$ cycle structures in case of checking all possible $\sigma_B$ values.

## 3.1. Key Space Size

The size of Alice's key space is determined by the number of possible keys $\overline{s} = (s_1, s_2, \dots, s_{n(\alpha)})$ and equals to $\prod_{i=1}^{n(\alpha)} l(\alpha_i)$.

The size of Bob's key space is determined by the number of possible keys $\overline{r} = (r_1, r_2, \dots, r_{n(\alpha)})$ and $\chi_B$ and equals to $\prod_{i=1}^{n(\alpha)} l(\alpha_i) \cdot N(\chi_B)$, where $N(\chi_B)$ is the number of possible $\chi_B = \prod_{j=1}^{n(\chi_B)} \chi_{jB}$ permutations, $l(\chi_{iB}) \neq l(\chi_{jB})$ for $\forall i \neq j$.

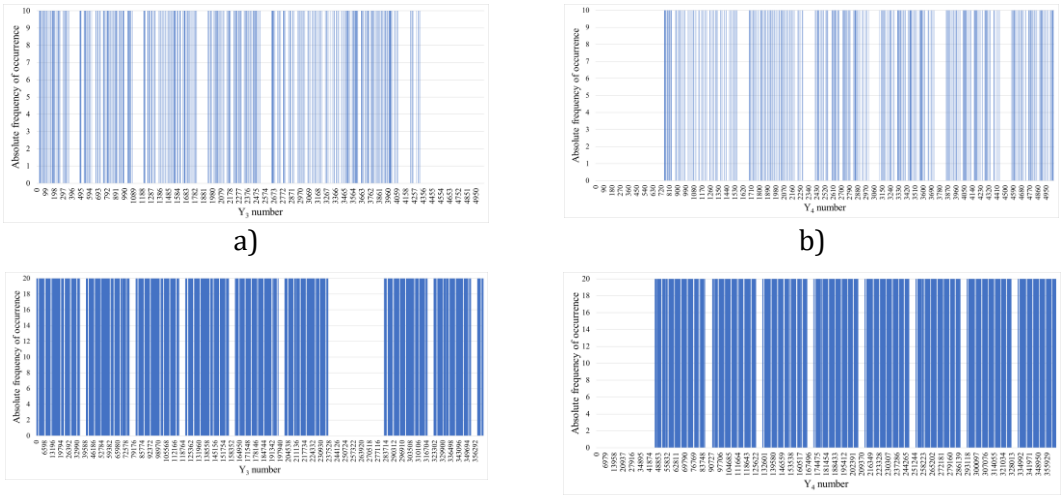
Thus, the size of the key space for the three-pass protocol is equal to $\prod_{i=1}^{n(\alpha)} l^2(\alpha_i) \cdot N(\chi_B)$.

## 3.2. Distributions of $Y_1$, $Y_2$, $Y_3$, $Y_4$ Values Depending on $\pi$ Values

The current study experimentally found absolute frequencies of permutations $Y_1, Y_2, Y_3$, $Y_4$ values occurrence for $M = 7$ and $M = 9$ at fixed values $\alpha, s, r, \chi_B$ as a result of checking all possible values of $\pi$. For $M = 7$, we accepted $\alpha = \{5,4,2,1,3,6,0\} = (0,5,6)(1,4,3)$, $\overline{s} = (1,2)$, $\overline{r} = (2,1)$, $\chi_B = \{6, 5, 4, 2, 1, 3, 0\} = (0,6)(1,5,3,2,4)$. For $M = 9$, we accepted $\alpha = \{5,8,4,1,7,6,0,2,3\} = (0,5,6)(1,8,3)(2,4,7)$, $\overline{s} = (1,2,1)$, $\overline{r} = (2,1,1)$, $\chi_B = \{7,5,8,6,1,2,0,3,4\} = (0,7,3,6)(1,5,2,8,4)$.

The statistical analysis has determined that $Y_1$ and $Y_2$ are distributed uniformly over the set of all possible values of permutation of length $M$ with an absolute frequency of any of $M!$ permutation occurrence equal to unity.

Figure 1 shows the distribution of absolute frequencies of $Y_3$ and $Y_4$ values occurrence. The numbers of possible permutations in the form of Lehmer code [42] are plotted along the x-axis.




a) b)

c) d)

**Figure 1:** Diagrams of absolute frequency distribution for $Y_3$ and $Y_4$ values as a result of checking all $\pi$: a) $Y_3$ for $M = 7$; b) $Y_4$ for $M = 7$; c) $Y_3$ for $M = 9$; d) $Y_4$ for $M = 9$

The diagrams above demonstrate that $Y_3$ and $Y_4$ values are distributed uniformly; however, they are distributed on the subsets of all possible permutation values with length $M$, rather than on the set. The absolute frequencies of permutations occurrence from these subsets are equal to 10 for $M = 7$ and to 20 for $M = 9$, and the sizes of the specified subsets are equal to $7!/10$ and $9!/20$.

**Theorem 3.** Non-zero absolute frequencies of permutations $Y_3$ and $Y_4$ occurrence are equal to the product of the lengths of the permutation $\chi_B$ cycles: $\prod_{j=1}^{n(\chi_B)} l(\chi_{jB})$.

*Proof.*

Here, we consider $Y_4 = \pi \cdot \chi_B \cdot \pi^{-1} = \pi(\chi_B)$. By decomposing $\chi_B$ into a product of disjoint cycles, we shall receive $Y_4 = \pi(\chi_B) = \pi\left(\prod_{j=1}^{n(\chi_B)} \chi_{jB}\right) = \prod_{j=1}^{n(\chi_B)} \pi(\chi_{jB})$ or $Y_4 = = \prod_{j=1}^{n(\chi_B)} \left(\pi(\chi_{1jB})\pi(\chi_{2jB}) \dots \pi\left(\chi_{l(\chi_{jB})jB}\right)\right)$. Substituting all possible $M!$ values of $\pi$ into the latter expression gives $M!$ various sets of permutations

$$\left(\pi(\chi_{11B})\pi(\chi_{21B}) \dots \pi(\chi_{l(\chi_{1B})1B})\right) \times$$
$$\times \left(\pi(\chi_{12B})\pi(\chi_{22B}) \dots \pi(\chi_{l(\chi_{2B})2B})\right) \cdot \dots \times$$
$$\times \left(\pi(\chi_{1n(\chi_B)B})\pi(\chi_{2n(\chi_B)B}) \dots \pi\left(\chi_{l\left(\chi_{n(\chi_B)B}\right)n(\chi_B)B}\right)\right).$$

However, the circular shift of the elements in the cycle does not alter the permutation itself. This implies that the products of all circular shifts for cycles $\pi(\chi_{jB})$ produce the same permutation $Y_4$. The number of such cases is equal to the product of permutation $\chi_B$ cycle lengths: $\prod_{j=1}^{n(\chi_B)} l(\chi_{jB})$.

Since $Y_3 = \sigma_B \cdot Y_4$, such a transformation is a bijection of one set of permutations into another. The distribution of absolute permutation frequencies remains unaltered with precision to their value.

Priorly, we have demonstrated that the $Y_4$ cycle structure corresponds to the $\chi_B$ structure.

Now, we consider the cycle structure of permutation $Y_3$ subsets with non-zero absolute frequencies for $M = 7$ and $M = 9$.

Table 1 summarizes the results.

Here, we determine the value that is a multiple of the permutation number for each structure with nonzero frequency.

Let $l_1, l_2, \dots, l_q$ be all possible different lengths of cycles $\alpha_i$, where $1 \le i \le n(\alpha)$, and $f_1, f_2, \dots, f_q$ be the corresponding numbers of such cycles. Herewith, $q$ is the number of cycles

$\alpha_i$ of different lengths. To present cycles $\alpha_i$ we use denotation $\alpha_i = (\alpha_{1i}, \alpha_{2i}, \dots, \alpha_{l(\alpha_i)i})$.

**Table 1**
The cycle structure of permutation $Y_3$ subsets with non-zero absolute frequencies for $M = 7$ and $M = 9$

| $\mathbf{M = 7}$ | | $\boldsymbol{M = 9}$ | |
|---|---|---|---|
| **Permutation $Y_3$ cycle structure** | **Number of permutations $Y_3$ of the specified cycle structure** | **Permutation $Y_3$ cycle structure** | **Number of permutations $Y_3$ of the specified cycle structure** |
| 1, 2, 2, 2 | 18=2!×3² | 1, 2, 2, 2 | 18=2! ×3² |
| 1, 1, 2, 3 | 72=4×18 | 1, 1, 2, 3 | 72=4×18 |
| 2, 5 | 108=6×18 | 2, 5 | 108=6×18 |
| 3, 4 | 72=4×18 | 3, 4 | 72=4×18 |
| 1, 1, 1, 4 | 54=3×18 | 1, 1, 1, 4 | 54=3×18 |
| 1, 6 | 180=10×18 | 1, 6 | 180=10×18 |
| Total | 504=28×18 | Total | 504=28×18 |

**Definition 1.** Multiplicity of permutation $\alpha$ is the number

$$L(\alpha) = f_1! \cdot f_2! \cdot \ldots \cdot f_q! \cdot l_1^{f_1} \cdot l_2^{f_2} \cdot \ldots \cdot l_q^{f_q}$$

**Theorem 4.** Number $N(Y_3)$ of permutations $Y_3$ with a defined cycle structure is a multiple of the value $L(\alpha)$.

*Proof.*

Let $Y_3$ be one permutation out of those being represented as $Y_3 = \sigma_B \cdot \pi(\chi) = \sigma_B \cdot \pi \cdot \chi \cdot \pi^{-1}$, where $\chi$, $\sigma_B$ are fixed permutations of the given structure.

Permutation $\pi$ specifies the forwarded message. Note that permutation $\alpha_i \cdot \pi$ belongs to the set $\{\pi\}$ of all possible forwarded messages. Then the permutation

$$Y_3' = \sigma_B \cdot (\alpha_i \cdot \pi) \cdot \chi \cdot (\alpha_i \cdot \pi)^{-1} =$$
$$= \alpha_i \cdot \sigma_B \cdot \pi \cdot \chi \cdot \pi^1 \cdot \alpha_i^{-1} = \alpha_i \cdot Y_3 \cdot \alpha_i^{-1}$$

is conjugate to $Y_3$ and has an identical to $Y_3$ cycle structure.

Therefore, the number $N(Y_3)$ of all possible permutations of $Y_3$ is a multiple of the number $l_i$, which implies that this number is also a multiple of the product $l_1^{f_1} \cdot l_2^{f_2} \cdot \ldots \cdot l_q^{f_q}$.

Here, we will demonstrate the divisibility $N(Y_3)$ by the product of factorials $f_1! \cdot f_2! \cdot \ldots \cdot f_q!$.

We shall start with $l_1 = l_2 = l$ and determine the permutation

$$\beta = \begin{pmatrix} \alpha_{11} & \alpha_{21} & \ldots & \alpha_{l1} & \alpha_{12} & \alpha_{22} & \ldots & \alpha_{l2} \\ \alpha_{12} & \alpha_{22} & \ldots & \alpha_{l2} & \alpha_{11} & \alpha_{21} & \ldots & \alpha_{l2} \end{pmatrix}$$

With a given message $\pi$, permutation $\beta \cdot \pi$ is among the set of $\{\pi\}$ possible messages. In this case the permutation

$$Y_3'' = \sigma_B \cdot (\beta \cdot \pi) \cdot \chi \cdot (\beta \cdot \pi)^{-1} =$$
$$= \beta \cdot \sigma_B \cdot \pi \cdot \chi \cdot \pi^1 \cdot \beta^{-1} = \beta \cdot Y_3 \cdot \beta^{-1}$$

is conjugate to $Y_3$ and has an identical to $Y_3$ cycle structure.

Similarly, if the number of permutations of length $l$ among cycles $\alpha_i$ is equal to $f$, we shall consider the permutation

$$\gamma = \begin{pmatrix} \alpha_{11} & \ldots & \alpha_{l1} & \alpha_{12} & \ldots & \alpha_{l2} & \ldots & \alpha_{1f} & \ldots & \alpha_{lf} \\ \alpha_{1t_1} & \ldots & \alpha_{lt_1} & \alpha_{1t_2} & \ldots & \alpha_{lt_2} & \ldots & \alpha_{1t_f} & \ldots & \alpha_{lt_f} \end{pmatrix}$$

where $\{t_1, t_2, \ldots t_f\}$ is permutation of numbers of the selected cycles $\alpha_i$.

With a given message $\pi$, permutation $\gamma \cdot \pi$ is among the set of $\{\pi\}$ possible messages. In this case the permutation

$$Y_3''' = \sigma_B \cdot (\gamma \cdot \pi) \cdot \chi \cdot (\gamma \cdot \pi)^{-1} =$$

$$= \gamma \cdot \sigma_B \cdot \pi \cdot \chi \cdot \pi^1 \cdot \gamma^{-1} = \gamma \cdot Y_3 \cdot \gamma^{-1}$$

is conjugate to $Y_3$, from whence $N(Y_3)$ is a multiple of $f!$ which is the number of possible index permutations $\{t_1, t_2, \dots t_f\}$.

Consequently, $N(Y_3)$ is divided into $L(\alpha) = f_1! \times \dots \cdot f_q! \cdot l_1^{f_1} \cdot \dots \cdot l_q^{f_q}$.

**Consequence.** If the lengths of all cycles $\alpha_i$ are equal to $l$, and their number is equal to $f$, then the number of $N(Y_3)$ permutations with a certain cycle structure is a multiple of $L(\alpha) = f! \cdot l^f$.

The experimental studies have shown that $Y_3$ cycle structures given in Table 1, as well as the distribution of absolute frequencies of permutations according to these structures are invariant relative to $\alpha$, $\overline{s}$, $\overline{r}$, $\chi_B$ selection provided their cycle structure is preserved. The subsets of permutations $Y_3$ with non-zero absolute frequencies do not coincide, although they do intersect.

Thus, even if the cryptanalyst is informed about the structure of $\alpha$ and $\chi_B$ cycles, knowledge of the cycle structure of permutation $Y_3$ will not enable him to determine permutation $\pi$, neither does this knowledge disclose the keys $\overline{s}$, $\overline{r}$, $\chi_B$ values.

### 3.3. Distributions of $Y_1$, $Y_2$, $Y_3$ Values Depending on $\overline{s}$, $\overline{r}$, and $\chi_B$ Values

In this section, we shall consider the effect that the vector $\overline{s}$ value has on the distribution of $Y_1$, $Y_2$, $Y_3$ values.

The vector $\overline{s}$ only impacts the $Y_1$, $Y_2$ values.

Since $Y_1 = \sigma_A \cdot \pi$, for a constant value of $\pi$, the vector $\overline{s}$ value determines $Y_1$. The transformation $\pi \leftrightarrow Y_1$ is bijective. The size of the $Y_1$ values set is determined by Alice's key space size as $\prod_{i=1}^{n(\alpha)} l(\alpha_i)$. $Y_1$ is uniformly distributed over the entire set of its values.

The transformation $Y_1 \leftrightarrow Y_2$ is bijective and depends on the $\overline{r}$ and $\chi_B$ values. Therefore, with constant $\overline{r}$ and $\chi_B$, the size of the $Y_2$ values set is determined by Alice's key space size. $Y_2$ is uniformly distributed over the entire set of its values.

Now, we shall consider the effect that the vector $\overline{r}$ value has on the distribution of $Y_1$, $Y_2$, $Y_3$ values.

The vector $\overline{r}$ only impacts the $Y_2$, $Y_3$ values.

Since $Y_2 = \sigma_B \cdot Y_1 \cdot \chi_B$, for constant $\pi$, $\overline{s}$ and $\chi_B$ the vector $\overline{r}$ value determines $Y_2$. The transformation $\pi \leftrightarrow Y_2$ is bijective. The size of the $Y_2$ values set is determined by the size of the vector $\overline{r}$ values set as $\prod_{i=1}^{n(\alpha)} l(\alpha_i)$. $Y_2$ is uniformly distributed over the entire set of its values.

The transformation $Y_2 \leftrightarrow Y_3$ is bijective and depends on the $\overline{s}$ and $\pi$ values. Therefore, with constant $\overline{s}$ and $\pi$, the size of the $Y_3$ values set is determined by the size of the vector $\overline{r}$ values set. $Y_3$ is uniformly distributed over the entire set of its values.

Next, we shall consider the effect that the $\chi_B$ value has on the distribution of $Y_1$, $Y_2$, $Y_3$ values.

The value $\chi_B$ only impacts the $Y_2$ and $Y_3$ values.

Since $Y_2 = \sigma_B \cdot Y_1 \cdot \chi_B$, for constant $\pi$, $\overline{s}$, and $\chi_B$, the vector $\overline{r}$ value determines $Y_2$. The transformation $\pi \leftrightarrow Y_2$ is bijective. The size of the $Y_2$ values set is determined by the size of the permutation $\chi_B$ values set as $\prod_{i=1}^{n(\chi_B)} l(\chi_{Bi})$. $Y_2$ is uniformly distributed over the entire set of its values.

The transformation $Y_2 \leftrightarrow Y_3$ is bijective and depends on the $\overline{s}$ and $\pi$ values. Therefore, with constant $\overline{s}$ and $\pi$, the size of the $Y_3$ values set is determined by the size of the permutation $\chi_B$ values set. $Y_3$ is uniformly distributed over the entire set of its values.

Note that Bob's key space is defined by a pair of values, $\overline{r}$ and $\chi_B$. Its size is equal to the product of the sizes of the $\overline{r}$ and $\chi_B$ values, $\prod_{i=1}^{n(\alpha)} l(\alpha_i) \cdot \prod_{i=1}^{n(\chi_B)} l(\chi_{Bi})$.

The obtained theoretical results have been confirmed by experimental studies.

### 3.4. Number of Possible Permutations $\pi$ Satisfying the Equation $Y_1 = \sigma_A \cdot \pi$ when $Y_1$ Value and $\alpha$ Cycle Structure are Known

This test determines the possibility for a cryptanalyst to increase his knowledge about the permutation $\pi$ based on the known $Y_1$ and known $\alpha$ cycle structure.

Defining $\sigma_A = Y_1 \cdot \pi^{-1}$ by going through possible values of permutation $\pi$ followed by analyzing $\sigma_A$ and selecting those values $\pi$ for which $\sigma_A = \prod_{i=1}^{n(\alpha)} \alpha_i^{s_i}$, where $\overline{s} = (s_1, s_2, \dots, s_{n(\alpha)})$ is possibly Alice's key, is equivalent to calculation $\pi = \sigma_A^{-1} \cdot Y_1$.

By going through possible keys $\overline{s} = = (s_1, s_2, \dots, s_{n(\alpha)})$, a set of possible $\pi$ values can be obtained. The number of such values corresponds to Alice's key $\overline{s}$ space size and equal to $\prod_{i=1}^{n(\alpha)} l(\alpha_i)$.

Thus, the cryptanalyst can shrink the size of the potential permutations $\pi$ set from $M!$ to $\prod_{i=1}^{n(\alpha)} l(\alpha_i)$, and to determine these permutations, but he cannot reduce the size of the potential permutations set to a value less than the size of Alice's key space. Nevertheless, the specified property should be taken into account when choosing the conversion parameters.

In particular, as shown in [40], $\prod_{i=1}^{n(\alpha)} l(\alpha_i) \to max$ on condition that $l(\alpha_i) \to e$ for $\forall i$. Thus, to achieve the maximum size of Alice's key space, the permutation $\alpha$ must be formed as a product of disjoint cycles of length three. Under these conditions, the size of the possible permutation $\alpha$ values equals $\mu(\alpha) = = \frac{\left(\sum_{i=1}^{n(\alpha)} l(\alpha_i)\right)!}{3^{n(\alpha)}}$.

## 3.5. Number of Key Pairs $\sigma_B$, $\chi_B$ Satisfying Equation $Y_3 = \sigma_B \cdot \pi \cdot \chi_B \cdot \pi^{-1}$

Here, we consider the possibility for a cryptanalyst to find Bob's key by the known value of $\overline{r}$ and known value of $Y_3$ assuming that the cycle structure of the key $\chi_B$ is known to the cryptanalyst.

Since permutations $\pi(\chi_B) = \pi \cdot \chi_B \cdot \pi^{-1}$ and $\chi_B$ are conjugate, the cryptanalyst can perform a search for all permutations $\sigma_B = \prod_{i=1}^{n(\alpha)} \alpha_i^{r_i}$ and all permutations $\pi(\chi_B)$ with the $\chi_B$ cycle structure, and identify pairs $\{\sigma_B; \pi(\chi_B)\}$ that satisfy equation $Y_3 = = \sigma_B \cdot \pi(\chi_B)$. The latter is equivalent to the following:

- Search for all $\sigma_B$ values and calculate $\pi(\chi_B) = (\sigma_B)^{-1} \cdot Y_3$ with its subsequent check for compliance with the $\chi_B$ structure.
- Search for all $\pi(\chi_B)$ values and calculate $\sigma_B = Y_3 \cdot \left(\pi(\chi_B)\right)^{-1}$ with its subsequent check for compliance with the $\sigma_B = \prod_{i=1}^{n(\alpha)} \alpha_i^{r_i}$ structure.

Experimental studies indicate that there may be several pairs of $\{\sigma_B; \pi(\chi_B)\}$. For instance, for $M = 7$, $\alpha = \{5,4,2,1,3,6,0\} = (0,5,6)(1,4,3)$, $\overline{s} = (1,2)$, $\overline{r} = (2,1)$, $\chi_B = \{6, 5, 4, 2, 1, 3, 0\} = (0,6)(1,5,3,2,4)$, and $\pi = \{2,4,5,6,3,0,1\}$ the $Y_3$ value is equal to $Y_3 = = \{5,2,4,3,6,1,0\}$.

However, the equation $Y_3 = \sigma_B \cdot \pi(\chi_B)$ is satisfied by pairs $\begin{cases}\sigma_B = \{6,4,2,1,3,0,5\};\\ \pi(\chi_B) = \{6,2,1,4,0,3,5\}\end{cases}$ and $\begin{cases}\sigma_B = \{0,4,2,1,3,5,6\};\\ \pi(\chi_B) = \{5,2,1,4,6,3,0\}.\end{cases}$ This indicates that even knowing the key $\chi_B$ structure and having checked all possible vector $\overline{r}$ values, the cryptanalyst will not be able to determine the key $\overline{r}$.

## 3.6. Distribution of $Y_3 = \sigma_B \cdot \pi \cdot \chi_B \cdot \pi^{-1}$ Cycle Structures in Case of Checking All Possible $\sigma_B$ Values

Such an analysis can be carried out by a cryptanalyst to determine the key $\chi_B$ structure.

Here, we shall consider the cycle structure of the product $\sigma_B^{-1} \cdot Y_3$ result with non-zero absolute frequencies for $M = 7$, $M = 9$, and $M = 12$ with the fixed $\alpha$, $\overline{s}$, $\chi_B$, $\pi$ values given above, and all possible $\overline{r}$ values. For $M = 12$, we accept $\alpha = \{5,4,8,1,3,6,0,2,7,11,9,10\} = = (0,5,6)(1,4,3)(2,8,7)(9,11,10)$, $\overline{s} = (1,2,1,2)$, $\overline{r} = (2,1,2,1)$, $\chi_B = \{5,11,10,6,1,9,4,8,0,2,7,3\} = (0,5,9,2,10,7,8)(1,11,3,6,4)$. **Error! Reference source not found.** summarizes the results.

The analysis of the results from **Error! Reference source not found.** shows that after checking all possible $\sigma_B$ values, there are several $\sigma_B^{-1} \cdot Y_3$ structures that can be used as $\chi_B$ structure. According to the requirements specified in Remark 1 and Remark 2, for $M = 7$ these structures contain cycles of length 2 and 5; 1 and 6; for $M = 9$ these structures will be 2 and 7; 4 and 5; 1 and 8; for $M = 12$ the structures will be 1, 2, 4, and 5; 2 and 10; 4 and 8; 5 and 7; 1 and 11.

**Table 2**
Cycle structure of permutation $\sigma_B^{-1} \cdot Y_3$ subsets with non-zero absolute frequencies for $M = 7$, $M = 9$, and $M = 12$

| $M = 7$ | | $M = 9$ | | $M = 12$ | |
|---|---|---|---|---|---|
| Permutation $\sigma_B^{-1} \cdot Y_3$ cycle structure | Number of permutations $\sigma_B^{-1} \cdot Y_3$ of the specified cycle structure | Permutation $\sigma_B^{-1} \cdot Y_3$ cycle structure | Number of permutations $\sigma_B^{-1} \cdot Y_3$ of the specified cycle structure | Permutation $\sigma_B^{-1} \cdot Y_3$ cycle structure | Number of permutations $\sigma_B^{-1} \cdot Y_3$ of the specified cycle structure |
| 1, 1, 2, 3 | 2 | 1, 2, 2, 4 | 1 | 1, 1, 2, 2, 3, 3 | 2 |
| 2, 5 | 2 | 1, 2, 3, 3 | 3 | 1, 2, 2, 7 | 3 |
| 3, 4 | 2 | 1, 1, 2, 5 | 2 | 1, 1, 1, 2, 3, 4 | 1 |
| 1, 1, 1, 4 | 1 | 2, 7 | 2 | 1, 2, 3, 6 | 10 |
| 1, 6 | 2 | 1, 1, 3, 4 | 4 | 1, 2, 4, 5 | 2 |
| | | 3, 6 | 4 | 1, 1, 2, 8 | 5 |
| | | 4, 5 | 2 | 2, 10 | 8 |
| | | 1, 1, 1, 6 | 1 | 1, 3, 3, 5 | 3 |
| | | 1, 8 | 8 | 1, 3, 4, 4 | 2 |
| | | | | 1, 1, 3, 7 | 5 |
| | | | | 3, 9 | 8 |
| | | | | 1, 1, 4, 6 | 5 |
| | | | | 4, 8 | 2 |
| | | | | 1, 1, 5, 5 | 1 |
| | | | | 5, 7 | 4 |
| | | | | 6, 6 | 2 |
| | | | | 1, 1, 1, 9 | 2 |
| | | | | 1, 11 | 16 |
| Total | 9 | Total | 27 | Total | 81 |

Thus, the cryptanalyst will not be able to determine the structure of $\chi_B$ cycles by going through all possible $\sigma_B$ values and determining $\sigma_B^{-1} \cdot Y_3$ from the equation $Y_3 = \sigma_B \cdot \pi \cdot \chi_B \cdot \pi^{-1}$ with known $\alpha$ and $Y_3$.

# 4. Cryptographic System and Its Work

The three-pass protocol can be implemented in a cryptographic system with a block diagram shown in Figure 2.

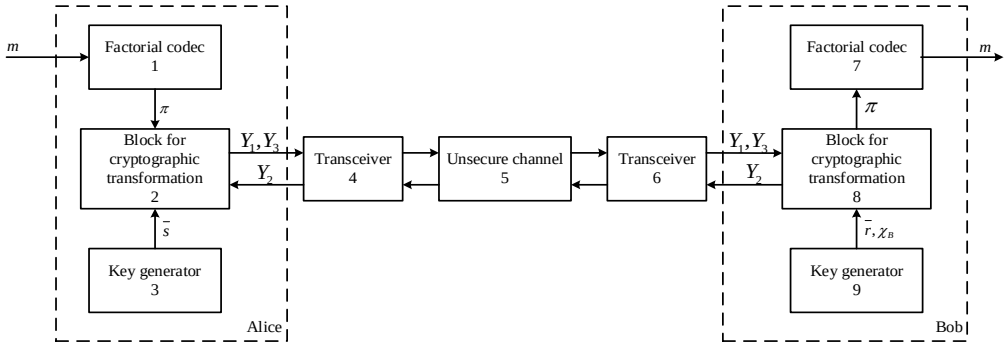



**Figure 2**: Block diagram of a cryptographic system that implements a three-pass protocol

Data exchange between Alice and Bob is carried out by transceivers 4 and 6 through an open unprotected duplex (or half-duplex) communication channel 5. Permutation $\alpha$ is known to Alice and Bob. Alice and Bob have factorial codecs 1 and 7, cryptographic transformation blocks 2 and 8, and private key generators 3 and 9 at their disposal. Let Alice create an open message $m$. Then codecs 1 and 7, respectively, transform message $m$ to permutation $\pi$ and inverse to it. These transformations depend on the shared key. Factorial codec 1 forms a codeword $\pi$ that enters the block of cryptographic

transformation 2. On the receiving side, the cryptographic transformation block 8 issues a codeword to codec 7, which converts it into the message $m$.

Private key generators 3 and 9 are independent generators based on random or pseudorandom processes. Private key generator 3 generates the signal $\overline{s}$. Requirements for the structure of this vector are described above. In cryptographic transformation block 2, Alice forms the permutations $\sigma_A$ and $\sigma_A^{-1}$ and keeps them secret.

Private key generator 9 generates signals $\overline{r}$ and $\chi_B$ and sends them to cryptographic transformation block 8. Requirements for $\overline{r}$ and $\chi_B$ structures are described above. In cryptographic transformation block 8, Bob forms permutations $\sigma_B$ and $\sigma_B^{-1}$ and keeps them secret.

To securely transmit permutation $\pi$, cryptographic transformation block 2 forms a signal $Y_1 = \sigma_A \cdot \pi$ and transmits it to the transceiver 4.

Bob's cryptographic transformation block 8, having received a signal $Y_1$ from transceiver 6, forms signal $Y_2 = \sigma_B \cdot Y_1 \cdot \chi_B$ and sends it to Alice via transceiver 6.

Alice's cryptographic transformation block 2, having received a signal $Y_2$ from transceiver 4, forms signal $Y_3 = \sigma_A^{-1} \cdot Y_2 \cdot \pi^{-1}$ and sends it to Bob via transceiver 4.

Having received the signal $Y_3$, Bob's cryptographic transformation block 8 forms value $Y_4$ and calculates the transmitted permutation $\pi$ value. After that, the permutation $\pi$ is outputted to factorial codec 7 for decoding and issuing the message to Bob.
The signal $\alpha$ may be either publicly available or generated by Alice's or Bob's key generator.

## 5. Discussion and Conclusions

This investigation was undertaken to evaluate the cryptographic strength of the three-pass protocol on permutations against various types of attacks. The results of this investigation show that the considered attacks do not allow a cryptanalyst to reduce the volume of the possible key search variants below Alice and Bob's key spaces.

At the same time, it is worth considering the following limitations while implementing the three-pass protocol on permutations.

1. Selecting permutations is realized about Remark 1 and Remark 2:
   - All disjoint cycles in the permutation $\chi_B$ decomposition into a product of disjoint cycles has different lengths.
   - The lengths of all disjoint cycles in the permutation $\alpha$ decomposition are pairwise coprime with all lengths of disjoint cycles in the permutation $\chi_B$ decomposition.
2. Alice and Bob perform different operations and use different numbers of cryptographic keys. Accordingly, the time required to perform these operations by Alice and Bob may differ.
3. The keys must be changed after being used, at least the key $\sigma_A$. Hence, Bob, having decrypted permutation $\pi$, can easily calculate Alice's private encryption key $\sigma_A$. To achieve this, Bob has to calculate the permutation $\pi^{-1}$ and then perform the procedure $\sigma_A = Y_1 \cdot \pi^{-1}$.

In addition, for the three-pass protocol to operate correctly, it is necessary to ensure that errors are absent in the permutation after receiving it from the communication channel. Otherwise, further transformation of the value received from the channel will be impossible or, if an error in the communication channel transforms the transmitted permutation into another permutation, such an error will not be detected, leading to distortions in the received message.

The developed protocol can be used both in information transmission systems using factorial coding with data recovery by permutation, and in traditional systems that do not use factorial codes. In the latter case, it is necessary to additionally include the bijection function of the information block and permutation in the data transfer protocol, as shown in the example of the implemented data transfer system.

## Acknowledgments

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

## References


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

[2] A. Bessalov, et al., Modeling CSIKE Algorithm on Non-Cyclic Edwards Curves, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3288 (2022) 1–10

[3] 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.

[4] 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.

[5] 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) 3039.

[6] B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd ed. (1996).

[7] B. Oktaviana, A. Utama Siahaan, Three-Pass Protocol Implementation in Caesar Cipher Classic Cryptography, IOSR, 18(04) (2016) 26–29.

[8] A. Menezes, P. Van Oorschot, S. Vanstone, Handbook of ч'applied Cryptography. Boca Raton: CRC Press (1997).

[9] J. Lang, A No-Key-Exchange Secure Image Sharing Scheme Based on Shamir's Three-Pass Cryptography Protocol and the Multiple-Parameter Fractional Fourier Transform, Opt. Express 20(3) (2012) 2386.

[10] Y. Kanamori, S.-M. Yoo, Quantum Three-Pass Protocol: Key Distribution Using Quantum Superposition States (2010).

[11] D. Nguyen, S. Kim, A Quantum Three Pass Protocol with Phase Estimation for Many Bits Transfer, International Conference on Advanced Technologies for Communications (ATC) (2019) 129–132.

[12] J. Massey, J. Omura, Method and Apparatus for Maintaining the Privacy of Digital Messages Conveyed by Public Transmission, US4567600A.

[13] D. Rachmawati, M. Budiman, An Implementation of the H-rabin Algorithm in the Shamir Three-Pass Protocol, 2nd International Conference on Automation, Cognitive Science, Optics, Micro Electro-Mechanical System, and Information Technology (ICACOMIT) (2017) 28–33.

[14] D. Rachmawati, M. Budiman, A Cryptocompression System based on H-Rabin Public Key Encryption Algorithm and Elias Gamma Codes, International Conference of Science, Technology, Engineering, Environmental and Ramification Researches, Medan, Indonesia (2018) 1910–1914.

[15] P. Khasanah, N. Gunawan, R. Rahim, Three-pass Protocol Scheme on Vigenere Cipher to Avoid Key Distribution, J. Critical Rev. 7(1) (2020) 68–71.

[16] A. Subandi, et al., Three-Pass Protocol Implementation in Vigenere Cipher Classic Cryptography Algorithm with Keystream Generator Modification, Adv. Sci. Technol. Eng. Syst. J. 2(5) (2017) 1–5.

[17] D. Rachmawati, A. Sharif, R. Sianipar, A Combination of Vigenere Algorithm and One Time Pad Algorithm in the Three-Pass Protocol, MATEC Web Conf. 197 (2018).

[18] R. Rahim, et al., Enhancement Three-Pass Protocol Security with Combination Caesar Cipher and Vigenere Cipher, J. Physics: Conference Series 1402(6) (2019) 066045.

[19] F. Kasiski, Geheimschriften und die Dechiffrirkunst. E.S. Mittler und Sohn (1863).

[20] W. Friedman, The Index of Coincidence and its Applications in Cryptanalysis. Laguna Hills, Calif: Aegean Park Press, (1987).

[21] D. Rachmawati, M. Andri Budiman, M. Adib Rikzan, Analysis of File Security with Three-Pass Protocol Scheme Using

Massey-Omura Algorithm in Android, J. Phys. Conf. Ser., 1235(1) (2019) 012075.
[22] A. Badawi, M. Zarlis, S. Suherman, Impact three Pass Protocol Modifications to Key Transmission Performance, J. Phys. Conf. Ser., 1235(1) (2019), 012050.
[23] R. Rahim, Applied Pohlig-Hellman Algorithm in Three-Pass Protocol Communication, J Appl Eng Science 16(3) (2018) 424–429.
[24] M. Hellman, S. Pohlig, Exponentiation Cryptographic Apparatus and Method, US4424414A.
[25] D.Rachmawati, M. Budiman, Using the RSA as an Asymmetric Non-Public Key Encryption Algorithm in the Shamir three-Pass Protocol, J. Theor. Appl. Inf. Technol. 96(17) (2018) 5663–5673.
[26] N. Nguyen, et al., No-Key Protocol for Deniable Encryption, Information Systems Design and Intelligent Applications 672 (2018) 96–104.
[27] N. Moldovyan, A. Moldovyan, V. Shcherbacov, Post-quantum No-key Protocol, Buletinul Academiei de Stiinte a Republicii Moldova, Matematica 85(3) (2017) 115–119.
[28] A. Moldovyan, D. Moldovyan, N. Moldovyan, Post-quantum Commutative Encryption Algorithm, Comput. Sci. J. Moldova 81(3) (2019) 299–317.
[29] D. Moldovyan, et al., Post-quantum Commutative Encryption Algorithm, Context-Aware Systems and Applications, and Nature of Computation and Communication 298 (2019) 205–214.
[30] N. Minh, et al., Post-quantum Commutative Deniable Encryption Algorithm, Intelligent Computing in Engineering 1125 (2020) 993–1005.
[31] E. Faure, Factorial Coding with Data Recovery, Visnyk Cherkaskogo Derzhavnogo Tehnologichnogo Universitetu 2 (2016) 33–39.
[32] E. Faure, Factorial Coding with Error Correction, Radio Electron. Comput. Sci. Control 3 (2017) 130–138.
[33] J. Al-Azzeh, et al., Telecommunication Systems with Multiple Access Based on Data Factorial Coding, Int. J. Commun. Antenna Propagation 10(2) (2020) 102–113.
[34] E. Faure, A. Shcherba, B. Stupka, Permutation-Based Frame Synchronisation Method for Short Packet Communication Systems, 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS) (2021) 1073–1077.
[35] J. Al-Azzeh, et al., Permutation-Based Frame Synchronization Method for Data Transmission Systems with Short Packets, Egyptian Inform. J. (2022).
[36] J. Al-Aazzeh et al., Efficiency Assessment of the Permutation-Based Frame Synchronization Method, Int. J. Commun. Antenna Propagation (IRECAP) 13(4) (2023).
[37] A. Lavdanskyi, et al., Accelerating Operations on Permutations Using Graphics Processing Units, in Inf. Technol. Educ. Sci. Technics 178 (2023) 3–12.
[38] E. Faure, et al., Concept for Using Permutation-Based Three-Pass Cryptographic Protocol in Noisy Channels, Systems, Decision and Control in Energy V 481 (2023) 99–113.
[39] E. Faure, et al., A Method for Reliable Permutation Transmission in Short-Packet Communication Systems, Information Technology for Education, Science, and Technics 178 (2023) 177–195.
[40] E. Faure, et al., Cryptographic Key Exchange Method for Data Factorial Coding, CEUR Workshop Proceedings, Vol. 2654 (2020) 643–653.
[41] A. Shcherba, E. Faure, O. Lavdanska, Three-Pass Cryptographic Protocol Based on Permutations, IEEE 2nd International Conference on Advanced Trends in Information Theory (ATIT) (2020) 281–284.
[42] D. Lehmer, Teaching Combinatorial Tricks to a Computer, Proceedings of Symposia in Applied Mathematics 10 (1960) 179–193.