Tatra Mt. Math. Publ. **91** (2025), 69–92
DOI: 10.2478/tmmp-2025-0018

TATRA MOUNTAINS
Mathematical Publications

A PUBLIC KEY CRYPTOSYSTEM USING MATRIX OVER THE FINITE RING

Gayrat Juraev[1] — Alisher Mavlonov[2,3]

[1]Information Security, National University of Uzbekistan, Tashkent, UZBEKISTAN

[2]Computer Science, Urgench State University, Urgench, UZBEKISTAN

[3]Institute of Mathematics, Slovak Academy of Sciences, Štefánikova 49, Bratislava, SLOVAKIA

ABSTRACT. This paper is the first of two complementary papers. In this paper, we present a novel algorithm in the field of cryptography, an area that has garnered significant attention from researchers. Our algorithm is based on matrix calculus over finite rings, enabling efficient encryption and decryption processes without requiring additional computational resources. A key feature of this approach is its formulation of a mathematical problem involving the solution of a system of nonlinear equations, which significantly enhances the system's security and complexity. Furthermore, we provide a detailed mathematical proof of the algorithm's correctness.

1. Introduction

In the context of rapidly advancing computational capabilities and the anticipated emergence of quantum computing, the development of secure cryptographic algorithms remains a critical objective. Traditional cryptographic methods face increasing challenges due to enhanced computational power and evolving attack techniques [1]. This environment necessitates the exploration of novel cryptographic approaches. Post-quantum cryptography, in particular, has gained attention for its potential to ensure security against quantum adversaries and to contribute additional advantages that may shape the future direction of cryptographic research and practice [2].

© 2025 Mathematical Institute, Slovak Academy of Sciences.
2020 Mathematics Subject Classification: 94A60, 11T71, 68P25.
Keywords: matrix, finite ring, algorithm, public-key cryptosystem.
Supported by the "Fund for Financing Science and Innovation Support" Contract No 52. Coordinator of the Fund is Agency for Innovative Development under the Minstry of Higher Education, Science and Innovations of the Republic of Uzbekistan.
Licensed under the Creative Commons BY-NC-ND 4.0 International Public License.

Another well-known challenge in the field is the development of efficient public-key encryption algorithms. At present, three cryptosystems are primarily recognized for addressing both encryption and digital signature tasks: RSA, ElGamal, and Rabin. However, the efficiency of most of these systems is considerably lower than that of symmetric cryptosystems. Consequently, their application is typically limited to encrypting relatively small amounts of data.

Public-key algorithms are distinguished by the one-way functions upon which they are based. Nevertheless, not all one-way functions are suitable for constructing public-key cryptosystems [3] or for implementing secure communication protocols in practical information systems [4]. Therefore, the design and analysis of one-way functions remain active areas of research.

A one-way function is a function $y = f(x)$ such that, for any x in its domain, the value $f(x) = y$ is easy to compute, but finding the corresponding x for any y in its range is computationally infeasible and requires solving a difficult problem.

One-way functions form the foundation of asymmetric cryptography, primarily due to the key distribution problem among users. While symmetric encryption algorithms provide high performance, they have a significant drawback: the number of keys that need to be distributed among users grows rapidly. If there are k users, the number of keys required is $k(k-1)/2$. In asymmetric cryptosystems, however, the number of keys equals the number of users.

The Hill cipher, introduced by Lester S. Hill in 1929, was the first matrix-based cipher algorithm [5, 6]. It is a polygraphic cipher that uses linear transformations to encrypt data. As a block cipher, the plaintext is split into blocks of equal size. The encryption key in the Hill cipher is an $n \times n$ non-singular matrix, where n represents the block size. Although nearly a century has passed since this cipher was created, this field remains relevant, and specialists continue to develop algorithms based on various matrices [7–9]. Researchers are exploring the Affine plane and modifying the Affine Hill Cipher to create public-key cryptosystems [10]. Similar to ECC, they also utilize discrete logarithms in group multiplication to design public-key cryptosystems [11]. Additionally, a public-key cryptosystem based on noncommutative groups has been developed, incorporating concepts such as ring matrices [12–15], special matrices [16–18], and matrix decomposition techniques [19]. The structures formed on these matrices are typically noncommutative.

In this paper, we design a one-way function based on a matrix formed using algebraic parameters. Using this function, we develop a trapdoor function [20] based on the complexity of solving a system of nonlinear equations.

2. Development of a basic matrix-based data encryption and decryption algorithm

In the area of modern cryptography, numerous algorithms based on matrix operations have already been developed, and new ones continue to be proposed. For example, studies [21, 22] explored a multivariate post-quantum encryption algorithm grounded in matrix algebra. However, this algorithm was later analyzed and successfully cryptanalyzed, as reported in [23]. A more recent approach is presented in [24], which addresses key challenges such as reducing public key size, improving computational efficiency, and enhancing resistance to structural attacks in multivariate cryptographic schemes.

In our previous researches [2, 25], we examined key challenges in quantum computing and cryptographic systems, focusing on the impact of quantum algorithms on contemporary encryption methods. We also considered alternative cryptographic approaches, such as matrix-based asymmetric encryption over finite rings. Building upon these findings, the proposed method utilizes matrix operations to improve both security and computational efficiency, supporting its potential for practical application.

This algorithm is designed to work in one mode: 64-bit mode — in this mode the algorithm runs on a 64-bit platform, it uses module values:

$$N = 2^{64}, \quad p = 2^8, \quad q = 2^{56}.$$

Why we chose this mode? The architecture of modern 64-bit processors and digital signal processors (DSPs) offers high performance with low power consumption, primarily due to advanced parallelism and optimized internal structures. These processors feature an internal bus architecture that includes a program bus, multiple data read buses, data write buses, and auxiliary buses for peripherals and direct memory access (DMA) controllers. This design enables the execution of up to three data read operations and two data write operations in a single clock cycle. Simultaneously, the DMA controller can handle up to two independent data transfer operations without involving the central processor, further enhancing throughput. These capabilities significantly reduce latency for encryption and decryption operations, ensuring minimal delays in signal processing. Additionally, modern 64-bit processors can execute all fundamental arithmetic and logical operations — such as multiplication, division, addition, subtraction, and bitwise operations — within a single machine cycle, thanks to advanced pipelining techniques. These features make the 64-bit mode ideal for implementing cryptographic algorithms, where high speed and low latency are critical. Based on these considerations, this algorithm consists of public and private key parameters as well as general computational parameters, which are as follows:

$S_{16\times16}$, $d_{3\times9}$, $\gamma_{8\times1}$, $\lambda_{6\times1}$, $\tau_{36\times1}$, $k_{2\times1}$ — the public key of the algorithm.

$T_{16\times16}$, $U_{8\times1}$, $\eta_{16\times1}$, $\xi_{8\times1}$, $\rho_{8\times1}$, $m_{8\times1}$ — the private key of the algorithm.

σ, Δ – the general parameters of the algorithm.

These key parameters form a trapdoor structure and ensure that, without knowledge of the private key, recovering the plaintext is infeasible. We will sequentially generate them using the following steps.

2.1. Parameters of algorithm

1. Elements are selected

$$u_{8\times1}\ (0 < u_i < N), \quad i = 0\dots7, \quad u_j = 0 \bmod 2, \quad j = 0\dots6, \quad u_7 = 1 \bmod 2.$$

$U_{8\times8}$ matrix is formed from them:

$$U_{8\times8} = \begin{bmatrix} u_7 & u_0 & u_1 & u_2 & u_3 & u_4 & u_5 & u_6 \\ u_5 & u_6 & u_7 & u_0 & u_1 & u_2 & u_3 & u_4 \\ u_6 & u_7 & u_0 & u_1 & u_2 & u_3 & u_4 & u_5 \\ u_4 & u_5 & u_6 & u_7 & u_0 & u_1 & u_2 & u_3 \\ u_3 & u_4 & u_5 & u_6 & u_7 & u_0 & u_1 & u_2 \\ u_2 & u_3 & u_4 & u_5 & u_6 & u_7 & u_0 & u_1 \\ u_1 & u_2 & u_3 & u_4 & u_5 & u_6 & u_7 & u_0 \\ u_0 & u_1 & u_2 & u_3 & u_4 & u_5 & u_6 & u_7 \end{bmatrix} \mod N, \tag{1}$$

here, the elements $u_0, u_1, \dots u_7$ are chosen such that the design of the $U_{8\times8}$ matrix is formed in a way that the operations in formulas (2) and (3) can always be performed.

2. σ — parameter values are calculated, inverse of the determinant of a matrix $U_{8\times1}$ by mod N,

$$\sigma = |U_{8\times8}|^{-1} \mod N, \tag{2}$$

here, the value of σ always exists because the determinant of $U_{8\times8}$ is an odd number.

3. Matrix $G'_{8\times8}$ an adjoint of a matrix of $U_{8\times8}$,

$$G'_{8\times8} = \mathrm{Adj}(U_{8\times8})^T \mod N, \tag{3}$$

here, Adj() — an adjoint of a matrix, T — transpose operator

4. $m_{8\times1}, k_{2\times1}$ integers are randomly selected, satisfying the conditions

$$0 < m_i < N, \quad 0 < k_j < N$$

and

$$m_0 = 1 \bmod 2, \quad m_2 = 1 \bmod 2, \quad k_0 = 1 \bmod 2, \quad k_1 = 0 \bmod 2$$

here

$$i = 0\dots7, \quad j = 0, 1.$$

Choosing the values m_0, m_2 and k_0, k_1 in this way ensures that μ_0 and μ_3

calculated using formulas (4), (5), are odd, μ_2 is even and formula (6) is always satisfied. Then the parameter values are calculated $\mu_{16\times 1}$ according to the formulas:

$$\begin{bmatrix} \mu_0 \\ \mu_2 \\ \mu_4 \\ \mu_6 \\ \mu_8 \\ \mu_{10} \\ \mu_{12} \\ \mu_{14} \end{bmatrix} = G'_{8\times 8} \cdot \begin{bmatrix} m_0 \\ m_1 k_1 \\ m_2 k_1 \\ m_3 k_1 \\ m_4 k_1 \\ m_5 k_1 \\ m_6 k_1 \\ m_7 k_1 \end{bmatrix} \mod N, \tag{4}$$

$$\begin{bmatrix} \mu_1 \\ \mu_3 \\ \mu_5 \\ \mu_7 \\ \mu_9 \\ \mu_{11} \\ \mu_{13} \\ \mu_{15} \end{bmatrix} = G'_{8\times 8} \cdot \begin{bmatrix} m_0 k_0 \\ m_1 \\ m_2 \\ m_3 \\ m_4 \\ m_5 \\ m_6 \\ m_7 \end{bmatrix} \mod N. \tag{5}$$

5. The parameter value is calculated Δ, which is the inverse of the determinant $B_{16\times 16}$,

$$\Delta = \sigma^{-14} \cdot (\mu_0 \mu_3 - \mu_1 \mu_2)^{-1} \mod N. \tag{6}$$

6. Integers are randomly selected $\rho_{8\times 1}, (0 < \rho_i < q,\ i = 0..7)$ elements are calculated, $R_{16\times 1}$ using formulas:

$$R_{16\times 1} = \begin{bmatrix} \Delta^{-1} \cdot (\rho_0 - \mu_0) \\ \Delta^{-1} \cdot (\rho_0 k_0 - \mu_1) \\ (\rho_1 - \mu_2) \\ (\rho_1 k_0 - \mu_3) \\ \Delta^{-1} \cdot (\rho_2 - \mu_4) \\ \Delta^{-1} \cdot (\rho_2 k_0 - \mu_5) \\ (\rho_3 - \mu_6) \\ (\rho_3 k_0 - \mu_7) \\ \Delta^{-1} \cdot (\rho_4 - \mu_8) \\ \Delta^{-1} \cdot (\rho_4 k_0 - \mu_9) \\ (\rho_5 - \mu_{10}) \\ (\rho_5 k_0 - \mu_{11}) \\ \Delta^{-1} \cdot (\rho_6 - \mu_{12}) \\ \Delta^{-1} \cdot (\rho_6 k_0 - \mu_{13}) \\ (\rho_7 - \mu_{14}) \\ (\rho_7 k_0 - \mu_{15}) \end{bmatrix} \mod N. \tag{7}$$

7. A matrix $B_{16\times16}$ is formed based on the given structure. The matrix $A'_{16\times16}$ is assigned the transposed value of the matrix's $B_{16\times16}$ algebraic complements,

$$B_{16\times16} = \begin{bmatrix} \mu_0 & \mu_1 & 0 & 0 & \dots & \dots & 0 & 0 \\ \mu_2 & \mu_3 & 0 & 0 & \dots & \dots & 0 & 0 \\ \mu_4 & \mu_5 & \sigma & 0 & \dots & \dots & 0 & 0 \\ \mu_6 & \mu_7 & 1 & \sigma & \dots & \dots & 0 & 0 \\ \mu_8 & \mu_9 & 1 & 1 & \dots & \dots & 0 & 0 \\ \mu_{10} & \mu_{11} & 1 & 1 & \dots & \dots & 0 & 0 \\ \mu_{12} & \mu_{13} & 1 & 1 & \dots & \dots & 0 & 0 \\ \mu_{14} & \mu_{15} & 1 & 1 & \dots & \dots & 0 & 0 \\ \mathrm{pr}_0 & \mathrm{pr}_1 & 1 & 1 & \dots & \dots & 0 & 0 \\ \mathrm{pr}_2 & \mathrm{pr}_3 & 1 & 1 & \dots & \dots & 0 & 0 \\ \mathrm{pr}_4 & \mathrm{pr}_5 & 1 & 1 & \dots & \dots & 0 & 0 \\ \mathrm{pr}_6 & \mathrm{pr}_7 & 1 & 1 & \dots & \dots & 0 & 0 \\ \mathrm{pr}_8 & \mathrm{pr}_9 & 1 & 1 & \dots & \dots & 0 & 0 \\ \mathrm{pr}_{10} & \mathrm{pr}_{11} & 1 & 1 & \dots & \dots & 0 & 0 \\ \mathrm{pr}_{12} & \mathrm{pr}_{13} & 1 & 1 & \dots & \dots & \sigma & 0 \\ \mathrm{pr}_{14} & \mathrm{pr}_{15} & 1 & 1 & \dots & \dots & 1 & \sigma \end{bmatrix} \mod N, \tag{8}$$

$$A'_{16\times16} = \mathrm{Adj}(B_{16\times16})^T \mod N, \tag{9}$$

here, Adj() — an adjoint of a matrix, T — transpose operator.

8. A matrix $A_{16\times16}$ is formed from the elements $A'_{16\times16}$ as follows:

$$A_{16\times16} = \begin{bmatrix} \Delta a'_{00} & \Delta a'_{01} & 0 & 0 & \dots & 0 & \dots & 0 & 0 \\ \Delta a'_{10} & \Delta a'_{11} & 0 & 0 & \dots & 0 & \dots & 0 & 0 \\ \Delta a'_{20} & \Delta a'_{21} & \Delta a'_{22} & 0 & \dots & 0 & \dots & 0 & 0 \\ \Delta a'_{30} & \Delta a'_{31} & \Delta a'_{32} & \Delta a'_{33} & 0 & 0 & \dots & 0 & 0 \\ \Delta a'_{40} & \Delta a'_{41} & \Delta a'_{42} & \Delta a'_{43} & \Delta a'_{44} & 0 & \dots & 0 & 0 \\ \Delta a'_{50} & \Delta a'_{51} & \Delta a'_{52} & \dots & \Delta a'_{55} & 0 & \dots & 0 & 0 \\ \Delta a'_{60} & \Delta a'_{61} & \Delta a'_{62} & \dots & \Delta a'_{66} & 0 & \dots & 0 & 0 \\ \Delta a'_{70} & \Delta a'_{71} & \Delta a'_{72} & \dots & \Delta a'_{77} & 0 & \dots & 0 & 0 \\ \Delta a'_{80} & \dots & \Delta a'_{87} & a'_{88} & 0 & \dots & \dots & 0 & 0 \\ \Delta a'_{90} & \dots & \Delta a'_{97} & a'_{98} & \Delta a'_{99} & 0 & \dots & 0 & 0 \\ \vdots & \dots & \vdots & \vdots & \vdots & \ddots & \ddots & \dots & \vdots \\ \Delta a'_{150} & \dots & \dots & a'_{158} & \dots & \ddots & \ddots & a'_{1514} & \Delta a'_{1515} \end{bmatrix} \mod N. \tag{10}$$

9. Randomly are chosen these parameters $\eta_0, \eta_1, \dots, \eta_{15}$ and $\beta_0, \beta_1, \dots, \beta_{15}$ according to these conditions: $1 < \eta_0, \eta_1, \dots, \eta_{15} < q$, $1 < \beta_0, \beta_1, \dots, \beta_{15} < q$

$$\left| \begin{bmatrix} \eta_0 & \eta_1 & \eta_2 & \eta_3 \\ \eta_4 & \eta_5 & \eta_6 & \eta_7 \\ \eta_8 & \eta_9 & \eta_{10} & \eta_{11} \\ \eta_{12} & \eta_{13} & \eta_{14} & \eta_{15} \end{bmatrix} \right| \neq 0 \bmod 2, \tag{11}$$

$$\left|\begin{bmatrix} \eta_1 & \eta_2 & \eta_3 & \eta_4 \\ \eta_5 & \eta_6 & \eta_7 & \eta_8 \\ \eta_9 & \eta_{10} & \eta_{11} & \eta_{12} \\ \eta_{13} & \eta_{14} & \eta_{15} & \eta_0 \end{bmatrix}\right| \neq 0 \bmod 2. \tag{12}$$

10. A matrix $O_{16\times 16}$ is formed based on the given structure:

$$\begin{array}{ccccc} 1 < o_{ij} < N & \text{for} & i = 0 \ldots 7, & j = 0 \ldots 15, \\ o_{ij} = 0 & \text{for} & i = 8 \ldots 15, & j = 0 \ldots 6, \\ 0 < o_{ij} < 2^{11} & \text{for} & i = 8 \ldots 15, & j = 7 \ldots 15, \end{array} \tag{13}$$

$$\left|\begin{bmatrix} o_{88} & o_{89} & \ldots & o_{815} \\ o_{98} & o_{99} & \ldots & o_{915} \\ \vdots & \vdots & \ddots & \vdots \\ o_{158} & o_{159} & \ldots & o_{1515} \end{bmatrix}\right| \neq 0 \bmod 2, \tag{14}$$

$$|O_{16\times 16}| \neq 0 \bmod 2. \tag{15}$$

11. Value of the elements of $\tau_i, i = 0 \ldots 35$ are calculated:

$$\begin{bmatrix} \tau_0 & \tau_1 & \ldots & \tau_8 \end{bmatrix} = \begin{bmatrix} \beta_0 & \beta_1 & \beta_2 & \beta_3 \end{bmatrix} \begin{bmatrix} o_{127} & o_{128} & \ldots & o_{1215} \\ o_{137} & o_{138} & \ldots & o_{1315} \\ o_{147} & o_{148} & \ldots & o_{1415} \\ o_{157} & o_{158} & \ldots & o_{1515} \end{bmatrix} \bmod q, \tag{16}$$

$$\begin{bmatrix} \tau_9 & \tau_{10} & \ldots & \tau_{17} \end{bmatrix} = \begin{bmatrix} \beta_4 & \beta_5 & \beta_6 & \beta_7 \end{bmatrix} \begin{bmatrix} o_{127} & o_{128} & \ldots & o_{1215} \\ o_{137} & o_{138} & \ldots & o_{1315} \\ o_{147} & o_{148} & \ldots & o_{1415} \\ o_{157} & o_{158} & \ldots & o_{1515} \end{bmatrix} \bmod q, \tag{17}$$

$$\begin{bmatrix} \tau_{18} & \tau_{19} & \ldots & \tau_{26} \end{bmatrix} = \begin{bmatrix} \beta_8 & \beta_9 & \beta_{10} & \beta_{11} \end{bmatrix} \begin{bmatrix} o_{127} & o_{128} & \ldots & o_{1215} \\ o_{137} & o_{138} & \ldots & o_{1315} \\ o_{147} & o_{148} & \ldots & o_{1415} \\ o_{157} & o_{158} & \ldots & o_{1515} \end{bmatrix} \bmod q, \tag{18}$$

$$\begin{bmatrix} \tau_{27} & \tau_{28} & \ldots & \tau_{35} \end{bmatrix} = \begin{bmatrix} \beta_{12} & \beta_{13} & \beta_{14} & \beta_{15} \end{bmatrix} \begin{bmatrix} o_{127} & o_{128} & \ldots & o_{1215} \\ o_{137} & o_{138} & \ldots & o_{1315} \\ o_{147} & o_{148} & \ldots & o_{1415} \\ o_{157} & o_{158} & \ldots & o_{1515} \end{bmatrix} \bmod q. \tag{19}$$

12. $\xi_0, \xi_1, \ldots, \xi_7, \gamma_0, \gamma_1, \ldots, \gamma_7$ integers in the interval $0 < \xi_0, \xi_1, \ldots, \xi_7, \gamma_0, \gamma_1, \ldots, \gamma_7 < N$ are selected as element values. The remaining elements of the matrix $G_{16\times 16}$ are defined as follows:

$$\begin{aligned} &g_{08} = g_{115} = \xi_0, \quad g_{09} = g_{18} = \xi_1, \quad g_{010} = g_{19} = \xi_2, \quad g_{011} = g_{110} = \xi_3, \\ &g_{012} = g_{111} = \xi_4, \quad g_{013} = g_{112} = \xi_5, \quad g_{014} = g_{113} = \xi_6, \quad g_{015} = g_{114} = \xi_7, \end{aligned} \tag{20}$$

$$\begin{bmatrix} g_{28} \\ g_{29} \\ g_{210} \\ g_{211} \\ g_{212} \\ g_{213} \\ g_{214} \\ g_{215} \end{bmatrix} = \begin{bmatrix} o_{88} & o_{98} & \ldots & o_{158} \\ o_{89} & o_{99} & \ldots & o_{159} \\ o_{810} & o_{910} & \ldots & o_{1510} \\ o_{811} & o_{911} & \ldots & o_{1511} \\ o_{812} & o_{912} & \ldots & o_{1512} \\ o_{813} & o_{913} & \ldots & o_{1513} \\ o_{814} & o_{914} & \ldots & o_{1514} \\ o_{815} & o_{915} & \ldots & o_{1515} \end{bmatrix}^{-1} \begin{bmatrix} \gamma_0 \\ \gamma_1 \\ \gamma_2 \\ \gamma_3 \\ \gamma_4 \\ \gamma_5 \\ \gamma_6 \\ \gamma_7 \end{bmatrix} \mod N, \tag{21}$$

$$\begin{bmatrix} g_{38} \\ g_{39} \\ g_{310} \\ g_{311} \\ g_{312} \\ g_{313} \\ g_{314} \\ g_{315} \end{bmatrix} = \begin{bmatrix} o_{88} & o_{98} & \ldots & o_{158} \\ o_{89} & o_{99} & \ldots & o_{159} \\ o_{810} & o_{910} & \ldots & o_{1510} \\ o_{811} & o_{911} & \ldots & o_{1511} \\ o_{812} & o_{912} & \ldots & o_{1512} \\ o_{813} & o_{913} & \ldots & o_{1513} \\ o_{814} & o_{914} & \ldots & o_{1514} \\ o_{815} & o_{915} & \ldots & o_{1515} \end{bmatrix}^{-1} \begin{bmatrix} \gamma_7 \\ \gamma_0 \\ \gamma_1 \\ \gamma_2 \\ \gamma_3 \\ \gamma_4 \\ \gamma_5 \\ \gamma_6 \end{bmatrix} \mod N, \tag{22}$$

$$\begin{bmatrix} g_{48} \\ g_{49} \\ g_{410} \\ g_{411} \\ g_{412} \\ g_{413} \\ g_{414} \\ g_{415} \end{bmatrix} = \begin{bmatrix} o_{88} & o_{98} & \ldots & o_{158} \\ o_{89} & o_{99} & \ldots & o_{159} \\ o_{810} & o_{910} & \ldots & o_{1510} \\ o_{811} & o_{911} & \ldots & o_{1511} \\ o_{812} & o_{912} & \ldots & o_{1512} \\ o_{813} & o_{913} & \ldots & o_{1513} \\ o_{814} & o_{914} & \ldots & o_{1514} \\ o_{815} & o_{915} & \ldots & o_{1515} \end{bmatrix}^{-1} \begin{bmatrix} \gamma_6 \\ \gamma_7 \\ \gamma_0 \\ \gamma_1 \\ \gamma_2 \\ \gamma_3 \\ \gamma_4 \\ \gamma_5 \end{bmatrix} \mod N, \tag{23}$$

$$\begin{bmatrix} g_{58} \\ g_{59} \\ g_{510} \\ g_{511} \\ g_{512} \\ g_{513} \\ g_{514} \\ g_{515} \end{bmatrix} = \begin{bmatrix} o_{88} & o_{98} & \ldots & o_{158} \\ o_{89} & o_{99} & \ldots & o_{159} \\ o_{810} & o_{910} & \ldots & o_{1510} \\ o_{811} & o_{911} & \ldots & o_{1511} \\ o_{812} & o_{912} & \ldots & o_{1512} \\ o_{813} & o_{913} & \ldots & o_{1513} \\ o_{814} & o_{914} & \ldots & o_{1514} \\ o_{815} & o_{915} & \ldots & o_{1515} \end{bmatrix}^{-1} \begin{bmatrix} \gamma_5 \\ \gamma_6 \\ \gamma_7 \\ \gamma_0 \\ \gamma_1 \\ \gamma_2 \\ \gamma_3 \\ \gamma_4 \end{bmatrix} \mod N, \tag{24}$$

$$\begin{bmatrix} g_{68} \\ g_{69} \\ g_{610} \\ g_{611} \\ g_{612} \\ g_{613} \\ g_{614} \\ g_{615} \end{bmatrix} = \begin{bmatrix} o_{88} & o_{98} & \dots & o_{158} \\ o_{89} & o_{99} & \dots & o_{159} \\ o_{810} & o_{910} & \dots & o_{1510} \\ o_{811} & o_{911} & \dots & o_{1511} \\ o_{812} & o_{912} & \dots & o_{1512} \\ o_{813} & o_{913} & \dots & o_{1513} \\ o_{814} & o_{914} & \dots & o_{1514} \\ o_{815} & o_{915} & \dots & o_{1515} \end{bmatrix}^{-1} \begin{bmatrix} \gamma_4 \\ \gamma_5 \\ \gamma_6 \\ \gamma_7 \\ \gamma_0 \\ \gamma_1 \\ \gamma_2 \\ \gamma_3 \end{bmatrix} \bmod N, \tag{25}$$

$$\begin{bmatrix} g_{78} \\ g_{79} \\ g_{710} \\ g_{711} \\ g_{712} \\ g_{713} \\ g_{714} \\ g_{715} \end{bmatrix} = \begin{bmatrix} o_{88} & o_{98} & \dots & o_{158} \\ o_{89} & o_{99} & \dots & o_{159} \\ o_{810} & o_{910} & \dots & o_{1510} \\ o_{811} & o_{911} & \dots & o_{1511} \\ o_{812} & o_{912} & \dots & o_{1512} \\ o_{813} & o_{913} & \dots & o_{1513} \\ o_{814} & o_{914} & \dots & o_{1514} \\ o_{815} & o_{915} & \dots & o_{1515} \end{bmatrix}^{-1} \begin{bmatrix} \gamma_3 \\ \gamma_4 \\ \gamma_5 \\ \gamma_6 \\ \gamma_7 \\ \gamma_0 \\ \gamma_1 \\ \gamma_2 \end{bmatrix} \bmod N, \tag{26}$$

$$\begin{aligned} g_{8i} &= p \cdot (-g_{0i} \bmod q), \quad i = 0 \dots 7, \\ g_{8j} &= p \cdot (\eta_{j-8} - g_{0j} \bmod q), \quad j = 8 \dots 11, \\ g_{8k} &= p \cdot (\beta_{k-12} - g_{0k} \bmod q), \quad k = 12 \dots 15, \end{aligned} \tag{27}$$

$$\begin{aligned} g_{9i} &= p \cdot (-g_{1i} \bmod q), \quad i = 0 \dots 7, \\ g_{9j} &= p \cdot (\eta_{j-4} - g_{1j} \bmod q), \quad j = 8 \dots 11, \\ g_{9k} &= p \cdot (\beta_{k-8} - g_{1k} \bmod q), \quad k = 12 \dots 15, \end{aligned} \tag{28}$$

$$\begin{aligned} g_{10i} &= p \cdot (-g_{2i} \bmod q), \quad i = 0 \dots 7, \\ g_{10j} &= p \cdot (\eta_j - g_{2j} \bmod q), \quad j = 8 \dots 11, \\ g_{10k} &= p \cdot (\beta_{k-4} - g_{2k} \bmod q), \quad k = 12 \dots 15, \end{aligned} \tag{29}$$

$$\begin{aligned} g_{11i} &= p \cdot (-g_{3i} \bmod q), \quad i = 0 \dots 7, \\ g_{11j} &= p \cdot (\eta_{j+4} - g_{3j} \bmod q), \quad j = 8 \dots 11, \\ g_{11k} &= p \cdot (\beta_k - g_{3k} \bmod q), \quad k = 12 \dots 15, \end{aligned} \tag{30}$$

$$\begin{aligned} g_{12i} &= p \cdot (-g_{4i} \bmod q), \quad i = 0 \dots 11, \\ g_{12j} &= p \cdot (\eta_{j-11} - g_{4j} \bmod q), \quad j = 12 \dots 15, \end{aligned} \tag{31}$$

$$\begin{aligned} g_{13i} &= p \cdot (-g_{5i} \bmod q), \quad i = 0 \dots 11, \\ g_{13j} &= p \cdot (\eta_{j-7} - g_{5j} \bmod q), \quad j = 12 \dots 15, \end{aligned} \tag{32}$$

$$\begin{aligned} g_{14i} &= p \cdot (-g_{6i} \bmod q), \quad i = 0 \dots 11, \\ g_{14j} &= p \cdot (\eta_{j-3} - g_{6j} \bmod q), \quad j = 12 \dots 15, \end{aligned} \tag{33}$$

$$\begin{aligned} g_{15i} &= p \cdot (-g_{7i} \bmod q), \quad i = 0 \dots 11, \\ g_{15j} &= p \cdot (\eta_{j+1} - g_{7j} \bmod q), \quad j = 12 \dots 14, \\ g_{1515} &= p \cdot (\eta_0 - g_{715} \bmod q). \end{aligned} \tag{34}$$

13. As a result, the structure of the matrix $G_{16\times16}$ takes the following form:

$$G_{16\times16} = \begin{bmatrix} g'_{00} & g'_{01} & \cdots & g'_{07} & g_{08} & \cdots & g_{015} \\ g'_{10} & g'_{11} & \cdots & g'_{17} & g_{18} & \cdots & g_{115} \\ \vdots & \ddots & \cdots & \cdots & \cdots & \cdots & \vdots \\ g'_{70} & g'_{71} & \cdots & g'_{77} & g_{78} & \cdots & g_{715} \\ g_{80} & g_{81} & \cdots & \cdots & \cdots & g_{814} & g_{815} \\ \vdots & \ddots & \cdots & \cdots & \cdots & \cdots & \vdots \\ g_{150} & g_{151} & \cdots & \cdots & \cdots & g_{1514} & g_{1515} \end{bmatrix} \bmod N. \tag{35}$$

14. Value of the parameters of λ_0, λ_1, λ_2, λ_3, λ_4, λ_5 is calculated:

$$\begin{aligned} &\lambda_0 = \textstyle\sum g_{2i}o_{i7} \bmod N, \quad \lambda_1 = \sum g_{3i}o_{i7} \bmod N, \quad \lambda_2 = \sum g_{4i}o_{i7} \bmod N, \\ &\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad i = 8\ldots15, \\ &\lambda_3 = \textstyle\sum g_{5i}o_{i7} \bmod N, \quad \lambda_4 = \sum g_{6i}o_{i7} \bmod N, \quad \lambda_5 = \sum g_{7i}o_{i7} \bmod N, \\ &\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad i = 8\ldots15. \end{aligned} \tag{36}$$

15. Inverse of the matrix $O_{16\times16}$ is calculated modulo N,

$$T_{16\times16} = O^{-1}_{16\times16} \bmod N. \tag{37}$$

16. The matrix $S_{16\times16}$ is calculated by multiplying the matrices $A_{16\times16}, G_{16\times16}$ and $O_{16\times16}$,

$$S_{16\times16} = A_{16\times16} \cdot G_{16\times16} \cdot O_{16\times16} \bmod N. \tag{38}$$

17. The matrix elements of $d_{3\times9}$ are calculated using the following formula:

$$\begin{aligned} &d_{00} = o_{87} + o_{97} + o_{107} + o_{117}, && d_{01} = o_{88} + o_{98} + o_{108} + o_{118}, \\ &d_{02} = o_{89} + o_{99} + o_{109} + o_{119}, && d_{03} = o_{810} + o_{910} + o_{1010} + o_{1110}, \\ &d_{04} = o_{811} + o_{911} + o_{1011} + o_{1111}, && d_{05} = o_{812} + o_{912} + o_{1012} + o_{1112}, \\ &d_{06} = o_{813} + o_{913} + o_{1013} + o_{1113}, && d_{07} = o_{814} + o_{914} + o_{1014} + o_{1114}, \\ &d_{08} = o_{815} + o_{915} + o_{1015} + o_{1115}, \\ &d_{10} = o_{127} + o_{137}, && d_{11} = o_{128} + o_{138}, && d_{12} = o_{129} + o_{139}, \\ &d_{13} = o_{1210} + o_{1310}, && d_{14} = o_{1211} + o_{1311}, && d_{15} = o_{1212} + o_{1312}, \\ &d_{16} = o_{1213} + o_{1313}, && d_{17} = o_{1214} + o_{1314}, && d_{18} = o_{1215} + o_{1315}, \\ &d_{20} = o_{147} + o_{157}, && d_{21} = o_{148} + o_{158}, && d_{22} = o_{149} + o_{159}, \\ &d_{23} = o_{1410} + o_{1510}, && d_{24} = o_{1411} + o_{1511}, && d_{25} = o_{1412} + o_{1512}, \\ &d_{26} = o_{1413} + o_{1513}, && d_{27} = o_{1414} + o_{1514}, && d_{29} = o_{1415} + o_{1515}, \end{aligned} \tag{39}$$

here, the elements of the $d_{3\times9}$ matrix, based on formula (13), take values in the interval

$$0 \le d_{ij} < 2^{13}.$$

2.2. Encryption process

1. The plaintext is divided into blocks of 100 bytes in length, and each block is further divided into sub-blocks as follows and assigned to the corresponding elements of the $X_{16\times1}$ matrix, according to the following rule:

$$X_{16\times1} = \begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ x_{15} \end{bmatrix}, \tag{40}$$

here,

— the elements $x_0, x_1, \ldots, x_6$ are assigned the initial 64 bits of the block,

— the elements $x_7, x_8, \ldots, x_{14}$ is assigned the initial 40 bits of the block,

— the element x_{15} is assigned the initial 32 bits of the block.

2. The matrix $Y_{16\times1}$ is calculated using the following formula:

$$Y_{16\times1} = S_{16\times16} \cdot X_{16\times1} \bmod N, \tag{41}$$

here, in (41) — function is a one-way function, meaning it is easy to calculate the value of $Y_{16\times1}$, but it is difficult to determine the value of $X_{16\times1}$ because the inverse of $S_{16\times16}$ does not exist.

3. v_0, v_1, v_2 — the parameter values are calculated, for $i = 1 \ldots 8$,

$$\begin{aligned} v_0 &= \sum d_{0i} x_{i+7} \bmod N, \\ v_1 &= \sum d_{1i} x_{i+7} \bmod N, \\ v_2 &= \sum d_{2i} x_{i+7} \bmod N. \end{aligned} \tag{42}$$

Here, as given in relations (13), (39) and (40), the values

$$v_0,\ v_1 \quad \text{and} \quad v_2 \quad \text{are 56-bit long.}$$

4. A matrix $C_{16\times1}$ is formed from $Y_{16\times1}$, $X_{16\times1}$ matrix elements according to the following rule:

$$\left[\begin{array}{c}
y_0 + k_0 y_1 \\
(k_1 y_0 + y_1) \oplus (v_0 v_1 v_2 \bmod N) \\
\sigma\big(\sigma y_2 - (\lambda_0 x_7 + \gamma_0 x_8 + \gamma_1 x_9 + \gamma_2 x_{10} + \gamma_3 x_{11} + \gamma_4 x_{12} \\
+\gamma_5 x_{13} + \gamma_6 x_{14} + \gamma_7 x_{15})\big) \bmod N \oplus \big(\mathrm{not}(v_0) v_1 v_2 \bmod N\big) \\
\sigma\big(y_2 + \sigma y_3 - (\lambda_1 x_7 + \gamma_7 x_8 + \gamma_0 x_9 + \gamma_1 x_{10} + \gamma_2 x_{11} + \gamma_3 x_{12} \\
+\gamma_4 x_{13} + \gamma_5 x_{14} + \gamma_6 x_{15})\big) \bmod N \oplus \big(\mathrm{not}(v_1) v_0 v_2 \bmod N\big) \\
\sigma\big(y_2 + y_3 + \sigma y_4 - (\lambda_2 x_7 + \gamma_6 x_8 + \gamma_7 x_9 + \gamma_0 x_{10} + \gamma_1 x_{11} + \gamma_2 x_{12} \\
+\gamma_3 x_{13} + \gamma_4 x_{14} + \gamma_5 x_{15})\big) \bmod N \oplus \big(\mathrm{not}(v_2) v_0 v_1 \bmod N\big) \\
\sigma\big(y_2 + y_3 + y_4 + \sigma y_5 - (\lambda_3 x_7 + \gamma_5 x_8 + \gamma_6 x_9 + \gamma_7 x_{10} + \gamma_0 x_{11} + \gamma_1 x_{12} \\
+\gamma_2 x_{13} + \gamma_3 x_{14} + \gamma_4 x_{15})\big) \bmod N \oplus \big(\mathrm{not}(v_0 v_1) v_2 \bmod N\big) \\
\sigma\big(y_2 + y_3 + y_4 + y_5 + \sigma y_6 - (\lambda_4 x_7 + \gamma_4 x_8 + \gamma_5 x_9 + \gamma_6 x_{10} + \gamma_7 x_{11} \\
+\gamma_0 x_{12} + \gamma_1 x_{13} + \gamma_2 x_{14} + \gamma_3 x_{15})\big) \bmod N \oplus \big(\mathrm{not}(v_0 v_2) v_1 \bmod N\big) \\
\sigma\big(y_2 + y_3 + y_4 + y_5 + y_6 + \sigma y_7 - (\lambda_5 x_7 + \gamma_3 x_8 + \gamma_4 x_9 + \gamma_5 x_{10} + \gamma_6 x_{11} \\
+\gamma_7 x_{12} + \gamma_0 x_{13} + \gamma_1 x_{14} + \gamma_2 x_{15})\big) \bmod N \oplus \big(\mathrm{not}(v_1 v_2) v_0 \bmod N\big) \\
\frac{\Delta(y_2 + y_3 + y_4 + y_5 + y_6 + y_7 + \sigma y_8) \bmod N}{p} - (\tau_0 x_7 + \tau_1 x_8 + \tau_2 x_9 + \tau_3 x_{10} \\
+\tau_4 x_{11} + \tau_5 x_{12} + \tau_6 x_{13} + \tau_7 x_{14} + \tau_8 x_{15}) \bmod q \oplus \mathrm{not}(v_1) \\
\frac{(y_2 + y_3 + y_4 + y_5 + y_6 + y_7 + y_8 + \sigma y_9) \bmod N}{p} - (\tau_9 x_7 + \tau_{10} x_8 + \tau_{11} x_9 + \tau_{12} x_{10} \\
+\tau_{13} x_{11} + \tau_{14} x_{12} + \tau_{15} x_{13} + \tau_{16} x_{14} + \tau_{17} x_{15}) \bmod q \oplus v_1 \\
\frac{\Delta(y_2 + y_3 + y_4 + y_5 + y_6 + y_7 + y_8 + y_9 + \sigma y_{10}) \bmod N}{p} + \sigma y_2 - (\tau_{18} x_7 + \tau_{19} x_8 + \tau_{20} x_9 \\
+\tau_{21} x_{10} + \tau_{22} x_{11} + \tau_{23} x_{12} + \tau_{24} x_{13} + \tau_{25} x_{14} + \tau_{26} x_{15}) \bmod q \oplus \mathrm{not}(v_2) \\
\frac{(y_2 + y_3 + y_4 + y_5 + y_6 + y_7 + y_8 + y_9 + y_{10} + \sigma y_{11}) \bmod N}{p} + (y_2 + \sigma y_3) - (\tau_{27} x_7 + \tau_{28} x_8 \\
+\tau_{29} x_9 + \tau_{30} x_{10} + \tau_{31} x_{11} + \tau_{32} x_{12} + \tau_{33} x_{13} + \tau_{34} x_{14} + \tau_{35} x_{15}) \bmod q \oplus v_2 \\
\frac{\Delta(y_2 + y_3 + y_4 + y_5 + y_6 + y_7 + y_8 + y_9 + y_{10} + y_{11} + \sigma y_{12}) \bmod N}{p} + (y_2 + y_3 + \sigma y_4) \bmod q \\
\frac{(y_2 + y_3 + y_4 + y_5 + y_6 + y_7 + y_8 + y_9 + y_{10} + y_{11} + y_{12} + \sigma y_{13}) \bmod N}{p} + (y_2 + y_3 + y_4 + \sigma y_5) \bmod q \\
\frac{\Delta(y_2 + y_3 + y_4 + y_5 + y_6 + y_7 + y_8 + y_9 + y_{10} + y_{11} + y_{12} + y_{13} + \sigma y_{14}) \bmod N}{p} + (y_2 + y_3 + y_4 \\
+y_5 + \sigma y_6) \bmod q \\
\frac{(y_2 + y_3 + y_4 + y_5 + y_6 + y_7 + y_8 + y_9 + y_{10} + y_{11} + y_{12} + y_{13} + y_{14} + \sigma y_{15}) \bmod N}{p} + (y_2 + y_3 + y_4 \\
+y_5 + y_6 + \sigma y_7) \bmod q
\end{array}\right], \quad (43)$$

here,

— not() is the logical inversion operation,

— $\oplus$ is the logical operation of addition modulo 2.

This trapdoor function presented in (43) is based on the complexity of solving a system of nonlinear equations without knowing the private key. The nonlinearity is ensured by the XOR operation in the system and the multiplication of terms dependent on the unknowns v_0, v_1, v_2.

5. By concatenating the elements of the $C_{16\times 1}$ matrix, the corresponding block of cipher text is formed:

$$\mathit{Cipherblock} = C_0 \cup C_1 \cup \cdots \cup C_{15}. \quad (44)$$

2.3. Decryption process

Before the decryption process begins, matrices $A_{4\times4}$ and $B_{4\times4}$ are formed based on the $\eta_{16\times1}$ elements:

$$A_{4\times4} = \begin{bmatrix} \eta_1 & \eta_2 & \eta_3 & \eta_4 \\ \eta_5 & \eta_6 & \eta_7 & \eta_8 \\ \eta_9 & \eta_{10} & \eta_{11} & \eta_{12} \\ \eta_{13} & \eta_{14} & \eta_{15} & \eta_0 \end{bmatrix}^{-1} \bmod q, \tag{45}$$

$$B_{4\times4} = \begin{bmatrix} \eta_0 & \eta_1 & \eta_2 & \eta_3 \\ \eta_4 & \eta_5 & \eta_6 & \eta_7 \\ \eta_8 & \eta_9 & \eta_{10} & \eta_{11} \\ \eta_{12} & \eta_{13} & \eta_{14} & \eta_{15} \end{bmatrix}^{-1} \bmod q. \tag{46}$$

The following steps are then performed on each ciphertext block:

1. The corresponding ciphertext block is divided into blocks of length 120 bytes and the values of these blocks are passed in turn to the $C_{16\times1}$ matrix as a matrix element according to the following rule:

$$C_{16\times1} = \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{15} \end{bmatrix}, \tag{47}$$

here,

— every element of $c_0, c_1, \ldots, c_7$ is assigned the initial 64 bits of the ciphertext block,

— every element of $c_8, c_9, \ldots, c_{15}$ is assigned the initial 56 bits of the ciphertext block.

2. The matrix $F_{16\times1}$ elements $f_{12}, f_{13}, f_{14}, f_{15}$ are calculated using the following formula:

$$\begin{bmatrix} f_{12} \\ f_{13} \\ f_{14} \\ f_{15} \end{bmatrix} = A_{4\times4} \cdot \begin{bmatrix} c_{12} + \rho_4 c_0 \\ c_{13} + \rho_5 c_0 \\ c_{14} + \rho_6 c_0 \\ c_{15} + \rho_7 c_0 \end{bmatrix} \bmod q. \tag{48}$$

3. Calculated.

$$\psi_1 = f_{12} + f_{13} \bmod q, \tag{49}$$

$$\psi_2 = f_{14} + f_{15} \bmod q. \tag{50}$$

4. The matrix $F_{16\times 1}$ elements f_8, f_9, f_{10}, f_{11} are calculated using the following formula:

$$\begin{bmatrix} f_8 \\ f_9 \\ f_{10} \\ f_{11} \end{bmatrix} = B_{4\times 4} \cdot \begin{bmatrix} c_8 \oplus \mathrm{not}(\psi_1) + \rho_0 c_0 \\ c_9 \oplus \psi_1 + \rho_1 c_0 \\ c_{10} \oplus \mathrm{not}(\psi_2) + \rho_2 c_0 \\ c_{11} \oplus \psi_2 + \rho_3 c_0 \end{bmatrix} \bmod q. \tag{51}$$

5. Calculated.

$$\psi_0 = f_8 + f_9 + f_{10} + f_{11} \bmod N. \tag{52}$$

6. The other elements of the matrix $F_{16\times 1}$ are calculated as follows:

$$\begin{bmatrix} f_0 \\ f_1 \\ f_2 \\ f_3 \\ f_4 \\ f_5 \\ f_6 \\ f_7 \end{bmatrix} = \begin{bmatrix} m_0 c_0 \\ m_1 c_1 \oplus (\psi_0\psi_1\psi_2 \bmod N) \\ m_2 c_1 \oplus (\psi_0\psi_1\psi_2 \bmod N) \\ m_3 c_1 \oplus (\psi_0\psi_1\psi_2 \bmod N) \\ m_4 c_1 \oplus (\psi_0\psi_1\psi_2 \bmod N) \\ m_5 c_1 \oplus (\psi_0\psi_1\psi_2 \bmod N) \\ m_6 c_1 \oplus (\psi_0\psi_1\psi_2 \bmod N) \\ m_7 c_1 \oplus (\psi_0\psi_1\psi_2 \bmod N) \end{bmatrix} + \begin{bmatrix} \sigma u_7 & \sigma u_0 & u_1 & u_2 & u_3 & u_4 & u_5 & u_6 \\ \sigma u_5 & \sigma u_6 & u_7 & u_0 & u_1 & u_2 & u_3 & u_4 \\ \sigma u_6 & \sigma u_7 & u_0 & u_1 & u_2 & u_3 & u_4 & u_5 \\ \sigma u_4 & \sigma u_5 & u_6 & u_7 & u_0 & u_1 & u_2 & u_3 \\ \sigma u_3 & \sigma u_4 & u_5 & u_6 & u_7 & u_0 & u_1 & u_2 \\ \sigma u_2 & \sigma u_3 & u_4 & u_5 & u_6 & u_7 & u_0 & u_1 \\ \sigma u_1 & \sigma u_2 & u_3 & u_4 & u_5 & u_6 & u_7 & u_0 \\ \sigma u_0 & \sigma u_1 & u_2 & u_3 & u_4 & u_5 & u_6 & u_7 \end{bmatrix}$$

$$\times \begin{bmatrix} -(\xi_0 f_8 + \xi_1 f_9 + \xi_2 f_{10} + \xi_3 f_{11} + \xi_4 f_{12} + \xi_5 f_{13} + \xi_6 f_{14} + \xi_7 f_{15}) \\ -(\xi_1 f_8 + \xi_2 f_9 + \xi_3 f_{10} + \xi_4 f_{11} + \xi_5 f_{12} + \xi_6 f_{13} + \xi_7 f_{14} + \xi_0 f_{15}) \\ c_2 \oplus \big(\mathrm{not}(\psi_0)\psi_1\psi_2 \bmod N\big) \\ c_3 \oplus \big(\mathrm{not}(\psi_1)\psi_0\psi_2 \bmod N\big) \\ c_4 \oplus \big(\mathrm{not}(\psi_2)\psi_0\psi_1 \bmod N\big) \\ c_5 \oplus \big(\mathrm{not}(\psi_0\psi_1)\psi_2 \bmod N\big) \\ c_6 \oplus \big(\mathrm{not}(\psi_0\psi_2)\psi_1 \bmod N\big) \\ c_7 \oplus \big(\mathrm{not}(\psi_1\psi_2)\psi_0 \bmod N\big) \end{bmatrix} \bmod N. \tag{53}$$

7. The matrix $Z_{16\times 1}$ is calculated,

$$Z_{16\times 1} = T_{16\times 1} \cdot F_{16\times 1} \bmod N. \tag{54}$$

8. By concatenating $Z_{16\times 1}$ matrix elements, a corresponding block of plaintext is formed,

$$\textit{Plaintext block} = z_0 \cup z_1 \cup \cdots \cup z_{15}. \tag{55}$$

3. Proof of the correctness of the algorithm

To prove the correctness of the above data encryption algorithm, it is necessary to show the fulfillment of the

$$X_{16\times1} = Z_{16\times1} \text{ equality.}$$

Based on expressions (38), (9) and (10) of the "Algorithm parameters" item, expression (41) takes the following form:

$$\begin{aligned} B_{16\times16}\cdot Y_{16\times1} &= B_{16\times16}\cdot S_{16\times16}\cdot X_{16\times1} \\ &= B_{16\times16}\cdot A_{16\times16}\cdot G_{16\times16}\cdot O_{16\times16}\cdot X_{16\times1} \bmod N. \end{aligned} \tag{56}$$

If denoted by the $H_{16\times1}$ expression $O_{16\times16}\cdot X_{16\times1} \bmod N$, then (56) takes the following form:

$$H_{16\times1} = O_{16\times16}\cdot X_{16\times1} \bmod N, \tag{57}$$

$$B_{16\times16}\cdot Y_{16\times1} = B_{16\times16}\cdot A_{16\times16}\cdot G_{16\times16}\cdot H_{16\times1} \bmod N. \tag{58}$$

Taking into account the last equalities, to prove correctness it is required to establish the validity of the $H_{16\times1} = F_{16\times1}$ equality. This is done as follows.

Expression (57) is reduced to the form (60), taking into account the conditions given in (13),

$$\begin{array}{llll} h_0 = \sum_0^{15} o_{0i}x_i \bmod N, & h_1 = \sum_0^{15} o_{1i}x_i \bmod N, \\ h_2 = \sum_0^{15} o_{2i}x_i \bmod N, & h_3 = \sum_0^{15} o_{3i}x_i \bmod N, \\ h_4 = \sum_0^{15} o_{4i}x_i \bmod N, & h_5 = \sum_0^{15} o_{5i}x_i \bmod N, \\ h_6 = \sum_0^{15} o_{6i}x_i \bmod N, & h_7 = \sum_0^{15} o_{7i}x_i \bmod N, \\ h_8 = \sum_7^{15} o_{8i}x_i \bmod N, & h_9 = \sum_7^{15} o_{9i}x_i \bmod N, \\ h_{10} = \sum_7^{15} o_{10i}x_i \bmod N, & h_{11} = \sum_7^{15} o_{11i}x_i \bmod N, \\ h_{12} = \sum_7^{15} o_{12i}x_i \bmod N, & h_{13} = \sum_7^{15} o_{13i}x_i \bmod N, \\ h_{14} = \sum_7^{15} o_{14i}x_i \bmod N, & h_{15} = \sum_7^{15} o_{15i}x_i \bmod N. \end{array} \tag{59}$$

It should be noted that here the elements

$$h_0,\, h_1,\, \ldots,\, h_7$$

take values in the

$$0 < h_0,\, h_1,\, \ldots,\, h_7 < N \quad \text{interval,}$$

and the elements

$$0 < h_8,\, h_9,\, \ldots,\, h_{15} < q.$$

take values in the interval.

Expressing (58) in the form of systems of linear equations, we obtain:

$$\begin{cases}
\mu_0 y_0 + \mu_1 y_1 = \sum_0^{15} g_{0i} h_i \bmod N,\\
\mu_2 y_0 + \mu_3 y_1 = \sum_0^{15} g_{1i} h_i \bmod N,\\
\mu_4 y_0 + \mu_5 y_1 + \sigma y_2 = \sum_0^{15} g_{2i} h_i \bmod N,\\
\mu_6 y_0 + \mu_7 y_1 + y_2 + \sigma y_3 = \sum_0^{15} g_{3i} h_i \bmod N,\\
\mu_8 y_0 + \mu_9 y_1 + \sum_2^3 y_i + \sigma y_4 = \sum_0^{15} g_{4i} h_i \bmod N,\\
\mu_{10} y_0 + \mu_{11} y_1 + \sum_2^4 y_i + \sigma y_5 = \sum_0^{15} g_{5i} h_i \bmod N,\\
\mu_{12} y_0 + \mu_{13} y_1 + \sum_2^5 y_i + \sigma y_6 = \sum_0^{15} g_{6i} h_i \bmod N,\\
\mu_{14} y_0 + \mu_{15} y_1 + \sum_2^6 y_i + \sigma y_7 = \sum_0^{15} g_{7i} h_i \bmod N,\\
\mathrm{pr}_0 y_0 + \mathrm{pr}_1 y_1 + \sum_2^7 y_i + \sigma y_8 = \Delta^{-1} \sum_0^{15} g_{8i} h_i \bmod N,\\
\mathrm{pr}_2 y_0 + \mathrm{pr}_3 y_1 + \sum_2^8 y_i + \sigma y_9 = \sum_0^{15} g_{9i} h_i \bmod N,\\
\mathrm{pr}_4 y_0 + \mathrm{pr}_5 y_1 + \sum_2^9 y_i + \sigma y_{10} = \Delta^{-1} \sum_0^{15} g_{10i} h_i \bmod N,\\
\mathrm{pr}_6 y_0 + \mathrm{pr}_7 y_1 + \sum_2^{10} y_i + \sigma y_{11} = \sum_0^{15} g_{11i} h_i \bmod N,\\
\mathrm{pr}_8 y_0 + \mathrm{pr}_9 y_1 + \sum_2^{11} y_i + \sigma y_{12} = \Delta^{-1} \sum_0^{15} g_{12i} h_i \bmod N,\\
\mathrm{pr}_{10} y_0 + \mathrm{pr}_{11} y_1 + \sum_2^{12} y_i + \sigma y_{13} = \sum_0^{15} g_{13i} h_i \bmod N,\\
\mathrm{pr}_{12} y_0 + \mathrm{pr}_{13} y_1 + \sum_2^{13} y_i + \sigma y_{14} = \Delta^{-1} \sum_0^{15} g_{14i} h_i \bmod N,\\
\mathrm{pr}_{14} y_0 + \mathrm{pr}_{15} y_1 + \sum_2^{14} y_i + \sigma y_{15} = \sum_0^{15} g_{15i} h_i \bmod N.
\end{cases} \tag{60}$$

Substituting in place of parameters $\gamma_{8\times 1}$, $\lambda_{6\times 1}$, $\tau_{36\times 1}$ system of equations (43) respectively, expressions (16), (17), (18), (19), (21), (22), (23), (24), (25) and (36) we obtain:

$$\begin{cases}
c_0 = y_0 + k_0 y_1 \bmod N,\\
c_1 \oplus (v_0 v_1 v_2 \bmod N) = k_1 y_0 + y_1 \bmod N,\\
c_2 \oplus \big(\mathrm{not}(v_0) v_1 v_2 \bmod N\big) = \sigma\left(\sigma y_2 - \sum_8^{15} g_{2i} h_i\right) \bmod N,\\
c_3 \oplus \big(\mathrm{not}(v_1) v_0 v_2 \bmod N\big) = \sigma\left(y_2 + \sigma y_3 - \sum_8^{15} g_{3i} h_i\right) \bmod N,\\
c_4 \oplus \big(\mathrm{not}(v_2) v_0 v_1 \bmod N\big) = \sigma\left(\sum_2^3 y_i + \sigma y_4 - \sum_8^{15} g_{4i} h_i\right) \bmod N,\\
c_5 \oplus \big(\mathrm{not}(v_0 v_1) v_2 \bmod N\big) = \sigma\left(\sum_2^4 y_i + \sigma y_5 - \sum_8^{15} g_{5i} h_i\right) \bmod N,\\
c_6 \oplus \big(\mathrm{not}(v_0 v_2) v_1 \bmod N\big) = \sigma\left(\sum_2^5 y_i + \sigma y_6 - \sum_8^{15} g_{6i} h_i\right) \bmod N,\\
c_7 \oplus \big(\mathrm{not}(v_1 v_2) v_0 \bmod N\big) = \sigma\left(\sum_2^6 y_i + \sigma y_7 - \sum_8^{15} g_{7i} h_i\right) \bmod N,\\
c_8 \oplus \mathrm{not}(v_1) = \frac{\Delta(\sum_2^7 y_i + \sigma y_8) \bmod N}{p} - (\beta_0 h_{12} + \beta_1 h_{13} + \beta_2 h_{14} + \beta_3 h_{15}) \bmod q,\\
c_9 \oplus v_1 = \frac{(\sum_2^8 y_i + \sigma y_9) \bmod N}{p} - (\beta_4 h_{12} + \beta_5 h_{13} + \beta_6 h_{14} + \beta_7 h_{15}) \bmod q,\\
c_{10} \oplus \mathrm{not}(v_2) = \frac{\Delta(\sum_2^9 y_i + \sigma y_{10}) \bmod N}{p} + \sigma y_2 - (\beta_8 h_{12} + \beta_9 h_{13} + \beta_{10} h_{14} + \beta_{11} h_{15}) \bmod q,\\
c_{11} \oplus v_2 = \frac{(\sum_2^{10} y_i + \sigma y_{11}) \bmod N}{p} + (y_2 + \sigma y_3) - (\beta_{12} h_{12} + \beta_{13} h_{13} + \beta_{14} h_{14} + \beta_{15} h_{15}) \bmod q,\\
c_{12} = \frac{\Delta(\sum_2^{11} y_i + \sigma y_{12}) \bmod N}{p} + (y_2 + y_3 + \sigma y_4) \bmod q,\\
c_{13} = \frac{(\sum_2^{12} y_i + \sigma y_{13}) \bmod N}{p} + (y_2 + y_3 + y_4 + \sigma y_5) \bmod q,\\
c_{14} = \frac{\Delta(\sum_2^{13} y_i + \sigma y_{14}) \bmod N}{p} + (y_2 + y_3 + y_4 + y_5 + \sigma y_6) \bmod q,\\
c_{15} = \frac{(\sum_2^{14} y_i + \sigma y_{15}) \bmod N}{p} + (y_2 + y_3 + y_4 + y_5 + y_6 + \sigma y_7) \bmod q.
\end{cases} \tag{61}$$

Carrying out the appropriate transformations on the equations of system (61), we obtain the following expression:

$$
\begin{cases}
c_0 = y_0 + k_0 y_1 \bmod N, \\
c_1 \oplus v_0 v_1 v_2 = k_1 y_0 + y_1 \bmod N, \\
(\sigma\mu_4 y_0 + \sigma\mu_5 y_1 + c_2) \oplus \big(\mathrm{not}(v_0) v_1 v_2\big) = \sigma\left(\mu_4 y_0 + \mu_5 y_1 + \sigma y_2\right) \\
-\sigma \sum_8^{15} g_{2i} h_i \bmod N, \\
(\sigma\mu_6 y_0 + \sigma\mu_7 y_1 + c_3) \oplus \big(\mathrm{not}(v_1) v_0 v_2\big) = \sigma\left(\mu_6 y_0 + \mu_7 y_1 + y_2 + \sigma y_3\right) \\
-\sigma \sum_8^{15} g_{3i} h_i \bmod N, \\
(\sigma\mu_8 y_0 + \sigma\mu_9 y_1 + c_4) \oplus \big(\mathrm{not}(v_2) v_1 v_0\big) = \sigma\left(\mu_8 y_0 + \mu_9 y_1 + \sum_2^3 y_i + \sigma y_4\right) \\
-\sigma \sum_8^{15} g_{4i} h_i \bmod N, \\
(\sigma\mu_{10} y_0 + \sigma\mu_{11} y_1 + c_5) \oplus \big(\mathrm{not}(v_0 v_1) v_2\big) = \sigma\left(\mu_{10} y_0 + \mu_{11} y_1 + \sum_2^4 y_i + \sigma y_5\right) \\
-\sigma \sum_8^{15} g_{5i} h_i \bmod N, \\
(\sigma\mu_{12} y_0 + \sigma\mu_{13} y_1 + c_6) \oplus \big(\mathrm{not}(v_0 v_2) v_1\big) = \sigma\left(\mu_{12} y_0 + \mu_{13} y_1 + \sum_2^5 y_i + \sigma y_6\right) \\
-\sigma \sum_8^{15} g_{6i} h_i \bmod N, \\
(\sigma\mu_{14} y_0 + \sigma\mu_{15} y_1 + c_7) \oplus \big(\mathrm{not}(v_1 v_2) v_0\big) = \sigma\left(\mu_{14} y_0 + \mu_{15} y_1 + \sum_2^6 y_i + \sigma y_7\right) \\
-\sigma \sum_8^{15} g_{7i} h_i \bmod N, \\
\left(\Delta \sum_0^1 r_i y_i + \sum_0^1 \mu_i y_i + c_8\right) \oplus \mathrm{not}(v_1) = \frac{\Delta(p \sum_0^1 r_i y_i + \sum_2^7 y_i + \sigma y_8) \bmod N}{p} \\
+ \sum_0^1 \mu_i y_i - \sum_0^3 \beta_i h_{i+12} \bmod q, \\
\left(\sum_0^1 r_{i+2} y_i + \sum_0^1 \mu_{i+2} y_i + c_9\right) \oplus v_1 = \frac{(p \sum_0^1 r_{i+2} y_i + \sum_2^8 y_i + \sigma y_9) \bmod N}{p} \\
+ \sum_0^1 \mu_{i+2} y_i - \sum_4^7 \beta_i h_{i+8} \bmod q, \\
\left(\Delta \sum_0^1 r_{i+4} y_i + \sum_0^1 \mu_{i+4} y_i + c_{10}\right) \oplus \mathrm{not}(v_2) = \frac{\Delta(p \sum_0^1 r_{i+4} y_i + \sum_2^9 y_i + \sigma y_{10}) \bmod N}{p} \\
+ \sum_0^1 \mu_{i+4} y_i + \sigma y_2 - \sum_8^{11} \beta_i h_{i+4} \bmod q, \\
\sum_0^1 r_{i+6} y_i + \sum_0^1 \mu_{i+6} y_i + c_{11} \oplus v_2 = \frac{(p \sum_0^1 r_{i+6} y_i + \sum_2^{10} y_i + \sigma y_{11}) \bmod N}{p} \\
+ \sum_0^1 \mu_{i+6} y_i + y_2 + \sigma y_3 - \sum_{12}^{15} \beta_i h_i \bmod q, \\
\Delta \sum_0^1 r_{i+8} y_i + \sum_0^1 \mu_{i+8} y_i + c_{12} = \frac{\Delta(p \sum_0^1 r_{i+8} y_i + \sum_2^{11} y_i + \sigma y_{12}) \bmod N}{p} \\
+ \sum_0^1 \mu_{i+8} y_i + \sum_2^3 y_i + \sigma y_4 \bmod q, \\
\sum_0^1 r_{i+10} y_i + \sum_0^1 \mu_{i+10} y_i + c_{13} = \frac{(p \sum_0^1 r_{i+10} y_i + \sum_2^{12} y_i + \sigma y_{13}) \bmod N}{p} \\
+ \sum_0^1 \mu_{i+10} y_i + \sum_2^4 y_i + \sigma y_5 \bmod q, \\
\Delta \sum_0^1 r_{i+12} y_i + \sum_0^1 \mu_{i+12} y_i + c_{14} = \frac{\Delta(p \sum_0^1 r_{i+12} y_i + \sum_2^{13} y_i + \sigma y_{14}) \bmod N}{p} \\
+ \sum_0^1 \mu_{i+12} y_i + \sum_2^5 y_i + \sigma y_6 \bmod q, \\
\sum_0^1 r_{i+14} y_i + \sum_0^1 \mu_{i+14} y_i + c_{15} = \frac{(p \sum_0^1 r_{i+14} y_i + \sum_2^{14} y_i + \sigma y_{15}) \bmod N}{p} \\
+ \sum_0^1 \mu_{i+14} y_i + \sum_2^6 y_i + \sigma y_7 \bmod q.
\end{cases}
\tag{62}
$$

Taking into account equalities (60), expression (62) takes the following form:

$$\begin{cases} c_0 = y_0 + k_0 y_1 \bmod N, \\ c_1 \oplus (v_0 v_1 v_2 \bmod N) = k_1 y_0 + y_1 \bmod N, \\ \sigma\mu_4 y_0 + \sigma\mu_5 y_1 + c_2 \oplus \big(\mathrm{not}(v_0) v_1 v_2 \bmod N\big) = \sigma \sum_0^{15} g_{2i} h_i - \sigma \sum_8^{15} g_{2i} h_i \bmod N, \\ \sigma\mu_6 y_0 + \sigma\mu_7 y_1 + c_3 \oplus \big(\mathrm{not}(v_1) v_0 v_2 \bmod N\big) = \sigma \sum_0^{15} g_{3i} h_i - \sigma \sum_8^{15} g_{3i} h_i \bmod N, \\ \sigma\mu_8 y_0 + \sigma\mu_9 y_1 + c_4 \oplus \big(\mathrm{not}(v_2) v_1 v_0 \bmod N\big) = \sigma \sum_0^{15} g_{4i} h_i! - \sigma \sum_8^{15} g_{4i} h_i \bmod N, \\ \sigma\mu_{10} y_0 + \sigma\mu_{11} y_1 + c_5 \oplus \big(\mathrm{not}(v_0 v_1) v_2 \bmod N\big) = \sigma \sum_0^{15} g_{5i} h_i - \sigma \sum_8^{15} g_{5i} h_i \bmod N, \\ \sigma\mu_{12} y_0 + \sigma\mu_{13} y_1 + c_6 \oplus \big(\mathrm{not}(v_0 v_2) v_1 \bmod N\big) = \sigma \sum_0^{15} g_{6i} h_i - \sigma \sum_8^{15} g_{6i} h_i \bmod N, \\ \sigma\mu_{14} y_0 + \sigma\mu_{15} y_1 + c_7 \oplus \big(\mathrm{not}(v_1 v_2) v_0 \bmod N\big) = \sigma \sum_0^{15} g_{7i} h_i - \sigma \sum_8^{15} g_{7i} h_i \bmod N, \\ \Delta \sum_0^1 r_i y_i + \sum_0^1 \mu_i y_i + c_8 \oplus \mathrm{not}(v_1) = \frac{\Delta\Delta^{-1} \sum_0^{15} g_{8i} h_i \bmod N}{p} + \sum_0^{15} g_{0i} h_i - \sum_0^3 \beta_i h_{i+12} \bmod q, \\ \sum_0^1 r_{i+2} y_i + \sum_0^1 \mu_{i+2} y_i + c_9 \oplus v_1 = \frac{\sum_0^{15} g_{9i} h_i \bmod N}{p} + \sum_0^{15} g_{1i} h_i - \sum_4^7 \beta_i h_{i+8} \bmod q, \\ \Delta \sum_0^1 r_{i+4} y_i + \sum_0^1 \mu_{i+4} y_i + c_{10} \oplus \mathrm{not}(v_2) = \frac{\Delta\Delta^{-1} \sum_0^{15} g_{10i} h_i \bmod N}{p} + \sum_0^{15} g_{2i} h_i \\ - \sum_8^{11} \beta_i h_{i+4} \bmod q, \\ \sum_0^1 r_{i+6} y_i + \sum_0^1 \mu_{i+6} y_i + c_{11} \oplus v_2 = \frac{\sum_0^{15} g_{11i} h_i \bmod N}{p} + \sum_0^{15} g_{3i} h_i - \sum_{12}^{15} \beta_i h_{i+8} \bmod q, \\ \Delta \sum_0^1 r_{i+8} y_i + \sum_0^1 \mu_{i+8} y_i + c_{12} = \frac{\Delta\Delta^{-1} \sum_0^{15} g_{12i} h_i \bmod N}{p} + \sum_0^{15} g_{4i} h_i \bmod q, \\ \sum_0^1 r_{i+10} y_i + \sum_0^1 \mu_{i+10} y_i + c_{13} = \frac{\sum_0^{15} g_{13i} h_i \bmod N}{p} + \sum_0^{15} g_{5i} h_i \bmod q, \\ \Delta \sum_0^1 r_{i+12} y_i + \sum_0^1 \mu_{i+12} y_i + c_{14} = \frac{\Delta\Delta^{-1} \sum_0^{15} g_{14i} h_i \bmod N}{p} + \sum_0^{15} g_{6i} h_i \bmod q, \\ \sum_0^1 r_{i+14} y_i + \sum_0^1 \mu_{i+14} y_i + c_{15} = \frac{(\sum_0^{15} g_{15i} h_i) \bmod N}{p} + \sum_0^{15} g_{7i} h_i \bmod q. \end{cases} \tag{63}$$

Let us take the last 4 equations from (63) and replace the parameters

$$g_{ij} \ (i = 12 \ldots 15, \ \ j = 0 \ldots 15)$$

in them with expressions (31), (32), (33) and (34). As a result we get:

$$\begin{cases} (\Delta r_8 + \mu_8) y_0 + (\Delta r_9 + \mu_9) y_1 + c_{12} = \eta_1 h_{12} + \eta_2 h_{13} + \eta_3 h_{14} + \eta_4 h_{15} \bmod q, \\ (r_{10} + \mu_{10}) y_0 + (r_{11} + \mu_{11}) y_1 + c_{13} = \eta_5 h_{12} + \eta_6 h_{13} + \eta_7 h_{14} + \eta_8 h_{15} \bmod q, \\ (\Delta r_{12} + \mu_{12}) y_0 + (\Delta r_{13} + \mu_{13}) y_1 + c_{14} = \eta_9 h_{12} + \eta_{10} h_{13} + \eta_{11} h_{14} + \eta_{12} h_{15} \bmod q, \\ (r_{14} + \mu_{14}) y_0 + (r_{15} + \mu_{15}) y_1 + c_{15} = \eta_{13} h_{12} + \eta_{14} h_{13} + \eta_{15} h_{14} + \eta_0 h_{15} \bmod q. \end{cases} \tag{64}$$

Taking into account expressions (7), expression (64) takes the following form:

$$\begin{bmatrix} c_{12}+\rho_4(y_0+k_0y_1) \\ c_{13}+\rho_5(y_0+k_0y_1) \\ c_{14}+\rho_6(y_0+k_0y_1) \\ c_{15}+\rho_7(y_0+k_0y_1) \end{bmatrix} = \begin{bmatrix} \eta_1 & \eta_2 & \eta_3 & \eta_4 \\ \eta_5 & \eta_6 & \eta_7 & \eta_8 \\ \eta_9 & \eta_{10} & \eta_{11} & \eta_{12} \\ \eta_{13} & \eta_{14} & \eta_{15} & \eta_0 \end{bmatrix} \cdot \begin{bmatrix} h_{12} \\ h_{13} \\ h_{14} \\ h_{15} \end{bmatrix} \bmod q. \tag{65}$$

Substituting the resulting expression (65) into the right side of (48) we obtain:

$$\begin{bmatrix} f_{12} \\ f_{13} \\ f_{14} \\ f_{15} \end{bmatrix} = A_{4\times 4} \cdot \begin{bmatrix} \eta_1 & \eta_2 & \eta_3 & \eta_4 \\ \eta_5 & \eta_6 & \eta_7 & \eta_8 \\ \eta_9 & \eta_{10} & \eta_{11} & \eta_{12} \\ \eta_{13} & \eta_{14} & \eta_{15} & \eta_0 \end{bmatrix} \cdot \begin{bmatrix} h_{12} \\ h_{13} \\ h_{14} \\ h_{15} \end{bmatrix} \bmod q. \tag{66}$$

Thus, we get the equality,

$$\begin{bmatrix} f_{12} \\ f_{13} \\ f_{14} \\ f_{15} \end{bmatrix} = \begin{bmatrix} h_{12} \\ h_{13} \\ h_{14} \\ h_{15} \end{bmatrix} . \tag{67}$$

The proof of equality is carried out as follows:

$$\begin{bmatrix} f_8 \\ f_9 \\ f_{10} \\ f_{11} \end{bmatrix} = \begin{bmatrix} h_8 \\ h_9 \\ h_{10} \\ h_{11} \end{bmatrix} . \tag{68}$$

Let's take the 9th, 10th, 11th and 12th equations from the system of equations (63) and replace the parameters $l_{ij}(i = 8 \dots 11, j = 0 \dots 15)$ in them with expressions (27), (28), (29) and (30). As a result we get:

$$\begin{cases} (\Delta r_0+\mu_0)y_0+(\Delta r_1+\mu_1)y_1+c_8 \oplus \text{not}(v_1)=\eta_0h_8+\eta_1h_9+\eta_2h_{10}+\eta_3h_{11} \bmod q, \\ (r_2+\mu_2)y_0+(r_3+\mu_3)y_1+c_9 \oplus v_1=\eta_4h_8+\eta_5h_9+\eta_6h_{10}+\eta_7h_{11} \bmod q, \\ (\Delta r_4+\mu_4)y_0+(\Delta r_5+\mu_5)y_1+c_{10} \oplus \text{not}(v_2)=\eta_8h_8+\eta_9h_9+\eta_{10}h_{10}+\eta_{11}h_{11} \bmod q, \\ (r_6+\mu_6)y_0+(r_7+\mu_7)y_1+c_{11} \oplus v_2=\eta_{12}h_8+\eta_{13}h_9+\eta_{14}h_{10}+\eta_{15}h_{11} \bmod q. \end{cases} \tag{69}$$

Taking into account expressions (7), expression (68) takes the following form:

$$\begin{bmatrix} c_8 \oplus \text{not}(v_1)+\rho_0c_0 \\ c_9 \oplus v_1+\rho_1c_0 \\ c_{10} \oplus \text{not}(v_2)+\rho_2c_0 \\ c_{11} \oplus v_2+\rho_3c_0 \end{bmatrix} = \begin{bmatrix} \eta_0 & \eta_1 & \eta_2 & \eta_3 \\ \eta_4 & \eta_5 & \eta_6 & \eta_7 \\ \eta_8 & \eta_9 & \eta_{10} & \eta_{11} \\ \eta_{12} & \eta_{13} & \eta_{14} & \eta_{15} \end{bmatrix} \cdot \begin{bmatrix} h_8 \\ h_9 \\ h_{10} \\ h_{11} \end{bmatrix} \bmod q. \tag{70}$$

The equalities of

$$f_8=h_8, \quad f_9=h_9, \quad f_{10}=h_{10}, \quad f_{11}=h_{11},$$

the equalities

$$\psi_1=v_1, \quad \psi_2=v_2 \quad \text{is true.}$$

In this case, we substitute the last expression into expression (51) and get

$$\begin{bmatrix} f_8 \\ f_9 \\ f_{10} \\ f_{11} \end{bmatrix} = B_{4\times 4} \cdot \begin{bmatrix} \eta_0 & \eta_1 & \eta_2 & \eta_3 \\ \eta_4 & \eta_5 & \eta_6 & \eta_7 \\ \eta_8 & \eta_9 & \eta_{10} & \eta_{11} \\ \eta_{12} & \eta_{13} & \eta_{14} & \eta_{15} \end{bmatrix} \cdot \begin{bmatrix} h_8 \\ h_9 \\ h_{10} \\ h_{11} \end{bmatrix} \bmod q. \tag{71}$$

So we got equality

$$f_8 = h_8, \quad f_9 = h_9, \quad f_{10} = h_{10}, \quad f_{11} = h_{11}. \tag{72}$$

By virtue of equalities

$$f_0 = h_0, \quad f_1 = h_1, \quad f_2 = h_2, \quad f_3 = h_3, \quad f_4 = h_4, \quad f_5 = h_5, \quad f_6 = h_6, \quad f_7 = h_7,$$

the equality $\psi_0 = v_0$ holds. Considering expressions (63), (4) and (5), you can perform the following actions over expression (53):

$$\begin{bmatrix} f_0 \\ f_1 \\ f_2 \\ f_3 \\ f_4 \\ f_5 \\ f_6 \\ f_7 \end{bmatrix} = \begin{bmatrix} \sigma u_7 & \sigma u_0 & u_1 & u_2 & u_3 & u_4 & u_5 & u_6 \\ \sigma u_5 & \sigma u_6 & u_7 & u_0 & u_1 & u_2 & u_3 & u_4 \\ \sigma u_6 & \sigma u_7 & u_0 & u_1 & u_2 & u_3 & u_4 & u_5 \\ \sigma u_4 & \sigma u_5 & u_6 & u_7 & u_0 & u_1 & u_2 & u_3 \\ \sigma u_3 & \sigma u_4 & u_5 & u_6 & u_7 & u_0 & u_1 & u_2 \\ \sigma u_2 & \sigma u_3 & u_4 & u_5 & u_6 & u_7 & u_0 & u_1 \\ \sigma u_1 & \sigma u_2 & u_3 & u_4 & u_5 & u_6 & u_7 & u_0 \\ \sigma u_0 & \sigma u_1 & u_2 & u_3 & u_4 & u_5 & u_6 & u_7 \end{bmatrix} \cdot \begin{bmatrix} \mu_0 y_0 + \mu_1 y_1 - \sum_0^7 \xi_i f_{i+8} \\ \mu_2 y_0 + \mu_3 y_1 - (\sum_1^7 \xi_i f_{i+7} + \xi_0 f_{15}) \\ \sigma(\mu_4 y_0 + \mu_5 y_1) + c_2 \oplus \mathrm{not}(\psi_0)\psi_1\psi_2 \\ \sigma(\mu_6 y_0 + \mu_7 y_1) + c_3 \oplus \mathrm{not}(\psi_1)\psi_0\psi_2 \\ \sigma(\mu_8 y_0 + \mu_9 y_1) + c_4 \oplus \mathrm{not}(\psi_2)\psi_0\psi_1 \\ \sigma(\mu_{10} y_0 + \mu_{11} y_1) + c_5 \oplus \mathrm{not}(\psi_0\psi_1)\psi_2 \\ \sigma(\mu_{12} y_0 + \mu_{13} y_1) + c_6 \oplus \mathrm{not}(\psi_0\psi_2)\psi_1 \\ \sigma(\mu_{14} y_0 + \mu_{15} y_1) + c_7 \oplus \mathrm{not}(\psi_1\psi_2)\psi_0 \end{bmatrix} \bmod N. \tag{73}$$

Taking into account (61), (64), we calculate the expression (73).

By virtue of equalities (20), we obtain:

$$\begin{bmatrix} f_0 \\ f_1 \\ f_2 \\ f_3 \\ f_4 \\ f_5 \\ f_6 \\ f_7 \end{bmatrix} = \sigma \cdot U_{8\times 8} \cdot G'_{8\times 8} \cdot \begin{bmatrix} h_0 \\ h_1 \\ h_2 \\ h_3 \\ h_4 \\ h_5 \\ h_6 \\ h_7 \end{bmatrix} \bmod N. \tag{74}$$

By virtue of expression (3), the following holds:

$$\begin{bmatrix} f_0 \\ f_1 \\ f_2 \\ f_3 \\ f_4 \\ f_5 \\ f_6 \\ f_7 \end{bmatrix} = \sigma \cdot \sigma^{-1} \cdot E_{8\times 8} \cdot \begin{bmatrix} h_0 \\ h_1 \\ h_2 \\ h_3 \\ h_4 \\ h_5 \\ h_6 \\ h_7 \end{bmatrix} \bmod N. \tag{75}$$

So we got equality

$$f_1 = h_1,\ \ f_2 = h_2,\ \ f_3 = h_3,\ \ f_4 = h_4,\ \ f_5 = h_5,\ \ f_6 = h_6,\ \ f_7 = h_7. \qquad (76)$$

From expressions (67), (72) and (76) it is clear that the equalities

$$\begin{array}{lll} f_1 = h_1, & f_2 = h_2, & f_3 = h_3, \\ f_4 = h_4, & f_5 = h_5, & f_6 = h_6, \\ f_7 = h_7, & f_8 = h_8, & f_9 = h_9, \\ f_{10} = h_{10}, & f_{11} = h_{11}, & f_{12} = h_{12}, \\ f_{13} = h_{13}, & f_{14} = h_{14}, & f_{15} = h_{15} \end{array}$$

are fulfilled, as required to be proven. Thus, the mathematical correctness of the asymmetric data encryption algorithm has been proven.

4. Results and discussion

The complexity of the newly developed asymmetric algorithm is based on the mathematical hardness of solving systems of nonlinear multivariate equations over a finite ring. This provides a foundation for ensuring the security of the system.

By substituting $y_0, y_1, \ldots, y_{15}$ from (41) into the encryption function (43) and v_0, v_1, v_2 from (42), we obtain a system of nonlinear equations expressed in terms of the public parameters, where the plaintext variables $x_0, x_1, \ldots, x_{15}$ appear as unknowns. Thus, the problem of recovering the plaintext from the ciphertext or in other words, the complexity of the system, is directly related to the hardness of solving nonlinear systems of equations over a finite ring.

The cryptanalysis of this system and the corresponding results will be presented in our forthcoming publications.

To evaluate the proposed asymmetric cryptosystem, we developed a software using the Python programming language. The implementation was tested on a computer equipped with CPU Ryzen 7 5700G, 64 GB RAM and 1 TB SSD.

The experimental results are summarized in Table 1. For different input data sizes, the ciphertext length increased by approximately 20 %, which is consistent across all tested cases. This confirms the correctness of the encryption-decryption process and the predictable overhead of the system.

The performance results demonstrate that encryption and decryption are computationally efficient. For example, encrypting 1 MB of data required approximately 5 seconds, while decrypting it back required 4 seconds. For larger data sizes (100 MB), the encryption took around 501 seconds and decryption

TABLE 1. Performance analysis of the developed algorithm (CPU Ryzen 7 5700 G, DDR 64 GB, SSD 1 TB)

Data length (bytes)	1 048 576	5 242 880	10 485 760	104 857 600
Encrypted text (bytes)	1 258 380	6 291 542	12 582 920	125 829 140
Change in ciphertext size (%)	Increased by 20 %	Increased by 20 %	Increased by 20 %	Increased by 20 %
Time spent for encryption (seconds)	5	25	50	501
Time spent for decryption (seconds)	4	19	39	383
Total time (minutes)	$\frac{3}{20}$	$\frac{11}{15}$	$1\frac{29}{60}$	$14\frac{11}{15}$

about 383 seconds. The total time required to process 100 MB was approximately 15 minutes.

These results indicate that the proposed system is not only theoretically secure but also practically feasible. The computational complexity grows linearly with respect to the input data size and the obtained performance confirms that the system can be implemented with high speed in practice for secure data transmission.

5. Conclusions

Our research began with exploring cryptographic problems, specifically the challenges of finding the inverse of parameterized matrices over finite rings. We believe these problems form the foundation for developing innovative cryptographic algorithms resistant to quantum computers. As we investigated the unique characteristics of finding the inverse of a matrix over finite rings, we observed that it is not possible to compute the inverse in the same way for all matrices. The complexity of these mathematical problems provides the basis for creating cryptographic primitives. During our paper, we meticulously developed the algorithm parameters, ensuring both security and practicality by designing them using algebraic operations. Based on these parameters, we constructed encryption and decryption functions. Finally, we mathematically proved the correctness of the developed algorithm.

Acknowledgement. The authors are thankful to Agency for Innovative Development under the Ministry of Higher Education, Science and Innovations of the Republic of Uzbekistan, for the support by "Fund for Financing Science and Innovation Support" Contract No 52.

REFERENCES

[1] KAUR, R.—GABRIJELČIČ, D.—KLOBUČAR, T.: *Artificial intelligence for cybersecurity: Literature review and future research directions*, Information Fusion **97** (2023), Article (KAUR2023101804).

[2] JURAEV, G. U.—MAVLONOV, A. B.: *Delving into potential asymmetric cryptographic algorithms for the post-quantum era*, In: 2024 IEEE 25th International Conference of Young Professionals in Electron Devices and Materials (EDM). IEEE, 2024, pp. 2510–2513.

[3] KASHEFI, E.—KERENIDIS, I.: *Statistical zero knowledge and quantum one-way functions*, Theoret. Comput. Sci. **378** (2007), no. 1, 101–116.

[4] ADAMS, C.—FARRELL, S.: *Rfc2510: internet X. 509 Public Key Infrastructure Certificate Management Protocols*, March 1999.

[5] HILL, L.: *Cryptography in an algebraic alphabet*, Amer. Math. Monthly **36** (1929), no. 6, 306–312.

[6] HILL L.: *Concerning certain linear transformation apparatus of cryptography*, Amer. Math. Monthly **38** (1931), no. 3, 135–154.

[7] LEELA D.—SHAW, S-M.—NANDAKISHORE S. —ARUNAKUMARI, M.—SAI, M. G.—MAHABOOB, B.: *Matrix applications in cryptography*, In: AIP Conference Proceedings, International Conference on Recent Advances in Materials and Manufacturing, ICRAMM 2023.

[8] NASERI, A. R.—ABBASI, A.—ATANI, R. E.: *A new public key cryptography using M_q matrix*, J. Math. Modeling **11** (2023), no. 4, 681–693

[9] HONG, M.—CHEE, W. L.: *Hill cipher modifications and dynamic cryptosystem design*, In: Proc. - 2023 7th International Conference on Cryptography, Security and Privacy, CSP 2023, pp. 176–180.

[10] SUNDARAYYA, P.—VARA PRASAD, M. G.: *A public key cryptosystem using Affine Hill Cipher under modulation of prime number*, J. Inf. Optim. Sci. textbf40 (2019), no. 4, 919–930.

[11] MESHRAM, C,—LI, X.: *New efficient key authentication protocol for public key cryptosystem using DL over multiplicative group*, J. Inf. Optim. Sci. **39** (2018), no. 2, 391–400.

[12] EZHILMARAN, D.—MUTHUKUMARAN, V.: *Key exchange protocol using decomposition problem in near ring*, Gazi Univ. J. Sci. **29** (2016), no. 1, 123–127.

[13] KRISHNA, A. V. N.—NARAYANA, A. H.—VANI, K. M.: *A novel approach with matrix based public key cryptosystems*, J. Discret. Math. Sci. Cryptogr. **20** (2017), no. 2, pp. 407–412.

[14] KARATAS, Z. Y.—LUY, E.—GONEN, B.: *Public key cryptosystem based on matrices*, Int. J. Comput. Appl. **182** (2019), no. 42, 47–50.

[15] YUMMAN, M.—SHAH, T.—HUSSAIN, I.: *Asymmetric cryptosystem on matrix algebra over a chain ring*, Symmetry **13** (2021), no. 45, 1–11.

[16] M. MAXRIZAL: *Public key cryptosystem based on singular matrix*, Trends Sciences **19** (2022), no. 3, p. 2147.

[17] AHMED, MD. H.—TANTI, J.—PUSHP, S.: *A public key cryptosystem using cyclotomic matrices*, Coding Theory — Recent Adv. New Perspect. Appl. (2021), 86–132.

[18] SREE PARVATHI, P. M.—SRINIVASAN, C .: *Matrix Lie group as an algebraic structure for NTRU like cryptosystem*, J. Discret. Math. Sci. Cryptogr. **23** (2020), no. 7, 1455–1464.

[19] LIU, J.—ZHANG, H.—JIA, J.: *Cryptanalysis of schemes based on polynomial symmetrical decomposition*, Chinese J. Electron. **26** (2017), no. 6, 1139–1146.

[20] AUERBACH, B.—GÜNTHER, C. U.—PIETRZAK, K.: *Trapdoor memory-hard functions*, In: Advances in Cryptology — EUROCRYPT 2024. 43rd Annual international conference on the theory and applications of cryptographic techniques, Zurich, Switzerland, May 26–30, 2024; Proceedings. Part III, pp. 315–344.

[21] TAO, C.—DIENE, A.—TANG, S.—DING, J.: *Simple matrix scheme for encryption*, In: Gaborit, P., ed. Post-Quantum Cryptography (PQCrypto 2013), Lecture Notes in Computer Science, Vol 7932. Springer-Verlag, Berlin, 2013. pp. 231–242.

[22] TAO, C.—XIANG, H.—PETZOLDT, A.—DING, J.: *Simple matrix a multivariate public key cryptosystem (MPKC) for encryption*, Finite Fields Appl. **35** (2015), 352–368.

[23] C. GU: *Cryptanalysis of simple matrix scheme for encryption*, IACR Cryptol. ePrint Arch. *2016* (2016), p. 1075.

[24] MOLDOVYAN, A. A.—MOLDOVYAN, D. N.—MOLDOVYAN, N. A.: *A new approach to the development of multivariate cryptography algorithms*, Cryptography **2** (2023), p. 54. (In Russian)

[25] MAVLONOV, A.: *Investigation of the possibility of using matrix multiplication in asymmetric cryptographic systems*, Academic research in educational sciences, **2** (2021), no. 10, 89–93.

Received September 1, 2025
Revised September 19, 2025
Accepted September 19, 2025
Publ. online September 30, 2025

Gayrat Juraev
Department of Information Security
Applied Mathematics and
Intellectual Technologies
National University of Uzbekistan
University
100174 – ashkent
UZBEKISTAN
E-mail: gjuraev@mail.ru

Alisher Bagbekovich Mavlonov
Department of Computer Science
Faculty of Physics and Mathematics
Urgench State University
Kh. Alimdjan str.
220100 – Urgench
UZBEKISTAN

Institute of Mathematics
Slovak Academy of Sciences
Štefánikova 49
Bratislava 814 73
SLOVAKIA
E-mail: mavlonosher@gmail.com