BAREKENG: Journal of Mathematics and Its Applications
March 2026 Volume 20 Issue 1 Page 0657–0672
P-ISSN: 1978-7227 E-ISSN: 2615-3017
https://doi.org/10.30598/barekengvol20iss1pp0657-0672

A NOVEL PUBLIC-KEY CRYPTOGRAPHY SCHEME UTILIZING SKEW CIRCULANT MATRICES WITH GENERALIZED ALTERNATING FIBONACCI

Sapto Mukti Handoyo[1*], **Sugi Guritman**[2], **Jaharuddin**[3]

[1,2,3] *Applied Mathematics Study Program, School of Data Science, Mathematics, and Informatics, IPB University*
Jln. Raya Dramaga, Kampus IPB Dramaga, Bogor, 16680, Indonesia

*Corresponding author's e-mail: ** ***saptomukti@apps.ipb.ac.id***

Article Info

Article History:

Received: 1st May 2025
Revised: 3rd July 2025
Accepted: 4th August 2025
Available online: 24th November 2025

Keywords:

Determinant;
Hill cipher;
Inverse;
Public-key cryptography;
Skew circulant matrices.

ABSTRACT

Circulant and skew circulant matrices play a significant role in various applications, especially in cryptography. Their determinants and inverses can be used in the decryption process. In classical cryptography, the Hill cipher is known to be susceptible to known-plaintext attacks and requires matrix-based key transmission. This study introduces a new public-key cryptography scheme that combines the Hill cipher with the ElGamal technique, utilizing skew circulant matrices with generalized alternating Fibonacci numbers. These numbers provide a pattern that simplifies the explicit formulas of the determinant and inverse of the matrices. The proposed scheme is the first of its kind to use these matrices and numbers for public-key cryptography. Explicit formulas for the determinant and inverse of these matrices are derived using elementary row and column operations. The proposed scheme is resistant to the discrete logarithm problem, known-plaintext, and brute-force attacks and requires only the transmission of key parameters. The implementation of the scheme has been tested using Wolfram Mathematica. In practice, the computational time of the scheme is significantly faster than three other related schemes, with up to 500 times faster in encryption and 17 times faster in decryption.

How to cite this article:

S. M. Handoyo, S. Guritman, and Jaharuddin, "A NOVEL PUBLIC-KEY CRYPTOGRAPHY SCHEME UTILIZING SKEW CIRCULANT MATRICES WITH GENERALIZED ALTERNATING FIBONACCI", BAREKENG: J. Math. & App., vol. 20, iss. 1, pp. 0657-0672, Mar, 2026.

Journal homepage: *https://ojs3.unpatti.ac.id/index.php/barekeng/*
Journal e-mail: *barekeng.math@yahoo.com; barekeng.journal@mail.unpatti.ac.id*

Research Article · Open Access

1. INTRODUCTION

Circulant and skew circulant matrices are matrices that have a good structure, so that they are easy to construct or generate. An $n \times n$ circulant matrix is a matrix in which the entries in the i-th row is the result of a circular shift to the right of the entries in the $(i-1)$-th row for $i = 2,3, \dots, n$. A skew circulant matrix is similar to a circulant matrix, but all entries below the main diagonal are multiplied by -1 [1]. These matrices are widely applied in cryptography [2]-[7], coding theory [8], signal processing [9], differential equation [10],[11], and others [12]-[15].

Cryptography is a field that studies encryption schemes for securing communication. An encryption scheme consists of two main processes: encryption and decryption. Encryption is a process that transforms an original message, known as plaintext, into a secret message, referred to as ciphertext. Decryption is the reverse process of encryption. Both processes require the use of a key. According to [16], cryptography can be classified into two types: symmetric-key and asymmetric-key (or public-key) cryptography. Symmetric-key cryptography uses the same key for encryption and decryption, while public-key cryptography uses different keys. In public-key cryptography, the two different keys are the public key for encryption and the private key for decryption. A well-known example of symmetric-key cryptography is the Hill cipher. However, the Hill cipher is vulnerable to a known plaintext attack. Some of the new public-key cryptography schemes based on Hill and Affine-Hill ciphers have been developed utilizing several types of key matrices and are secure against known plaintext attack [17],[18]. In addition, a new public-key cryptography based on the Hill cipher can be constructed using other approaches that utilize RSA cryptography [19]. Other new public-key cryptography also uses matrices with different approaches [20]-[22]. Furthermore, the ElGamal technique can also be integrated into public-key cryptography schemes based on these ciphers. Notable examples of key matrices used in these schemes include generalized Fibonacci matrices with the Hill cipher [23], generalized Fibonacci matrices with the Affine-Hill cipher [24], M_q matrices with the Hill cipher [25], and others [26],[27]. These schemes that utilize the ElGamal technique derive their security from the hardness of the discrete logarithm problem and can reduce the time complexity of key transmission of the Hill cipher.

The determinant and inverse of circulant and skew circulant matrices have potential applications in the decryption process because their determinant and inverse formulas can be derived explicitly, thus allowing for fast computation during the decryption process. Based on the well-known formulas for computing the determinant and inverse of the matrices in [28], a major challenge lies in the inefficiency of applying these formulas when the matrix size n becomes very large. However, if the entries of the matrices follow a simple pattern, the formulas can be significantly simplified, allowing for better explicit formulas. Such simplifications are expected to significantly reduce the computational time of both the determinant and the inverse of the matrices. Several studies have explored explicit formulas for the determinant and inverse of circulant matrices, including those involving alternating Fibonacci numbers [29] and other numbers [30],[31]. Similarly, research on the determinant and inverse of skew circulant matrices has been conducted for various numbers [32]-[35]. In this paper, we use skew circulant matrices with generalized alternating Fibonacci numbers to develop a novel public-key cryptography scheme over $\mathbb{Z}_r$ based on the Hill cipher and the ElGamal technique, where r is a prime number. The scheme proposed in this research is expected to reduce the computational time for encryption and decryption than other similar schemes in [23], [24] and [25].

The objectives of this research are: (1) to explicitly formulate the determinant and inverse of $A_{n,p,q}$ over $\mathbb{Z}_r$, where r is a prime number; (2) to develop a public-key cryptography scheme based on the Hill cipher and the ElGamal technique using these matrices; (3) analyze the security of the proposed scheme theoretically involving the discrete logarithm problem, brute force attack, and known plaintext attack; and (4) compare the computational time of the proposed scheme by measuring execution time of the encryption and decryption of the proposed scheme with three other schemes presented in [23], [24] and [25].

2. RESEARCH METHODS

2.1 Determinant and Inverse Formulations

In this subsection, we present some mathematical background related to skew circulant matrices and the generalized alternating Fibonacci sequence.

Definition 1. [1] *Let $S = \{s_i\}_{i=1}^{n}$ be a finite sequence of numbers. A skew circulant matrix is written as follows*

$$\tilde{C} = \begin{pmatrix} s_1 & s_2 & \cdots & s_{n-1} & s_n \\ -s_n & s_1 & s_2 & \cdots & s_{n-1} \\ -s_{n-1} & \ddots & \ddots & \ddots & \vdots \\ \vdots & \cdots & -s_n & s_1 & s_2 \\ -s_2 & -s_3 & \cdots & -s_n & s_1 \end{pmatrix},$$

and is denoted by $\tilde{C} = \mathrm{SCirc}(S)$.

The eigenvalues of $\tilde{C}$ defined in Definition 1 are well-known and formulated in the following lemma.

Lemma 1. [28] *Let $\tilde{C} = \mathrm{SCirc}(S)$ and $S = \{s_i\}_{i=1}^{n}$. Suppose λ_k are the eigenvalues of $\tilde{C}$ for $k = 0,1,\dots,n-1$. Then,*

$$\lambda_k = \sum_{j=0}^{n-1} s_j \left(\psi\omega^k\right)^j,$$

where $\omega = e^{\frac{2\pi}{n}i} = cos\left(\frac{2\pi}{n}\right) + i\, sin\left(\frac{2\pi}{n}\right) \in \mathbb{C}$ and $i = \sqrt{-1} \in \mathbb{C}$.

According to Lemma 1, it is clear that

$$\det(\tilde{C}) = \prod_{k=0}^{n-1} \sum_{j-0}^{n-1} s_j \left(\psi\omega^k\right)^j. \tag{1}$$

Moreover, the inverse of $\tilde{C}$ are also well-known and formulated in the following theorem.

Theorem 1. [28] *Let $\tilde{C} = SCirc(S)$ and $S = \{s_i\}_{i=1}^{n}$. Suppose λ_k are the eigenvalues of $\tilde{C}$ for $k = 0,1,\dots,n-1$. Then,*

$$\tilde{C}^{-1} = \mathrm{SCirc}(b_0, b_1, b_2, \dots, b_{n-1}),$$

where $b_j = \frac{1}{n}\sum_{k=0}^{n-1} \mu_k \left(\psi\omega^k\right)^{-j}$ for $j = 0,1,2,\dots,n-1$, and $\mu_k = \begin{cases} 0, \lambda_k = 0 \\ \frac{1}{\lambda_k}, \lambda_k \neq 0 \end{cases}$.

Definition 2. *A generalized alternating Fibonacci sequence $\mathcal{F}_{p,q} = \left\{a_{j,p,q}\right\}_{j=0}^{n}$ is defined recursively as*

$$a_{j,p,q} = -pa_{j-1,p,q} + qa_{j-2,p,q},$$

where $a_{0,p,q} = 0$, $a_{1,p,q} = 1$, for $j = 2,3,\dots,n$.

The sequence $\mathcal{F}_{p,q}$ defined in Definition 2 is more general than the sequence defined in [29]. We use this sequence as entries of the skew circulant matrix defined as follows.

Definition 3. *A skew circulant matrix $A_{n,p,q}$ of size $n \times n$ with generalized alternating Fibonacci entries $\mathcal{F}_{p,q} = \left\{a_{j,p,q}\right\}_{j=1}^{n}$ is defined as*

$$A_{n,p,q} = \mathrm{SCirc}\left(\mathcal{F}_{p,q}\right) = \mathrm{SCirc}\left(a_{1,p,q}, a_{2,p,q}, \dots, a_{n,p,q}\right),$$

where $p, q, n \in \mathbb{N}$ and $n \geq 2$.

The determinant and inverse of a matrix can be computed by simplifying its matrix form using elementary row and column operations. Elementary row operations on a matrix A are described as [36]:

1. the entries of the i-th row are interchanged with the entries of the j-th row, denoted as $E_{ij}, i \neq j$;
2. the entries of the i-th row are multiplied by a constant $k \neq 0$, denoted as $E_{i(k)}$; and
3. the entries of i-th row are replaced with the sum of the entries of the i-th row with k times the entries of the j-th row, denoted as $E_{ij(k)}$, $i \neq j$.

Elementary column operations are described in the same way as elementary row operations, but the word "row" is replaced with "column" and denoted as K_{ij}, $K_{i(l)}$, and $K_{ij(l)}$ [36]. If elementary row and column operations are applied to a matrix X to obtain a matrix Y, then Y can be expressed as in the following theorem.

Theorem 2. [36] *Let X be a matrix and I be the identity matrix of the same size. If Y is a matrix obtained by applying a series of elementary row and column operations $E_1, E_2, \dots, E_n$ and $K_1, K_2, \dots, K_n$ on X, then there exists nonsingular matrix P and Q such that $Y = PXQ$, where $P = E_n E_{n-1} \dots E_1(I)$ and $P = K_n K_{n-1} \dots K_1(I)$.*

The relationship between the determinant of a matrix and the elementary row and column operations can be stated in the following theorem.

Theorem 3. [36] *Let X be an $n \times n$ matrix and k be a constant. Then, the following statements hold:*

1. $\det\left(E_{i(k)}(X)\right) = k \det(X), k \neq 0$;
2. $\det\left(E_{ij}(X)\right) = -\det(X), i \neq j$; and
3. $\det\left(E_{ij(k)}(X)\right) = \det(X), i \neq j$.

These statements are analogous to elementary column operations.

We utilize the matrix $A_{n,p,q}$ defined in Definition 3 over $\mathbb{Z}_r$, where $p, q, n \in \mathbb{N}$, r is a prime number, and $n \geq 2$. We compute the determinant and inverse of $A_{n,p,q}$ over $\mathbb{Z}_r$ by first transforming it into a diagonal matrix using elementary row and column operations, and applying Theorem 2 and Theorem 3, rather than computing them using Eq. (1) and Theorem 1.

2.2 Construction of A New Public-Key Cryptography Scheme

In this subsection, we present some mathematical background related to the Hill cipher and the ElGamal encryption technique.

Let K be an $n \times n$ key matrix, and $M_i \in \mathbb{Z}_r^m$ and $C_i \in \mathbb{Z}_r^m$ be the plaintext and ciphertext blocks of size $1 \times m$, respectively. The encryption and decryption transformations of the Hill cipher are given by [23]

$$C_i = M_i K \pmod{r},$$

and

$$M_i = C_i K^{-1} \pmod{r},$$

respectively, where r is a prime number such that $\gcd(\det(K), r) = 1$.

The ElGamal technique belongs to public-key cryptography and can be described as follows [16].

1. Public Key Generation
   Let party B be the message recipient. Party B performs the following steps:
   a. generates a safe prime r;
   b. chooses a generator α of $\mathbb{Z}_r^*$;
   c. chooses a private key $d \in \mathbb{Z}$, where $1 \leq d < \phi(r)$;
   d. computes $\beta = \alpha^d \pmod{r}$; and
   e. sends the public key (r, α, β) to the sender of the message.
2. Encryption
   Let party A be the sender of the message and has received the public key (r, α, β) from party B. Suppose an original message is represented as $m \in \mathbb{Z}_r$. Party A performs the following steps:
   a. chooses a secret random number $e \in \mathbb{Z}$, where $1 \leq e < \phi(r)$;
   b. computes $\gamma = \alpha^e \pmod{r}$ and $\delta = m \cdot \beta^e \pmod{r}$; and
   c. sends the ciphertext $(\gamma \quad \delta) \in \mathbb{Z}_r^2$ to party B.
3. Decryption
   Party B uses private key d to decrypt ciphertext $(\gamma \quad \delta)$ by computing $m = \gamma^{-d} \cdot \delta \pmod{r}$.

In our proposed public-key cryptography scheme, we utilize the matrix $A_{n,p,\lfloor n/2 \rfloor}$ over $\mathbb{Z}_r$ as the key matrix K in the Hill cipher, while the encryption technique employs the ElGamal technique, where $p, n \in \mathbb{N}$, r is a prime number, $r > 256$, and $n \geq 2$. The security aspects analyzed in our proposed scheme include the discrete logarithm problem, brute force attack, and known plaintext attack. Then, the computation time is compared with the schemes in [23], [24], and [25] using Wolfram Mathematica.

3. RESULTS AND DISCUSSION

3.1 Explicit Formulas for Determinant and Inverse of $A_{n,p,q}$

We present the following theorem, which provides explicit formulas for the determinant and inverse of the skew circulant matrices $A_{n,p,q}$ with generalized alternating Fibonacci numbers as their entries over $\mathbb{Z}_r$, where r is a prime number.

Theorem 4. *Let $A_{n,p,q} = \mathrm{SCirc}(\mathcal{F}_{p,q})\ (mod\, r)$ be a $n \times n$ skew circulant matrix with generalized alternating Fibonacci numbers $\mathcal{F}_{p,q} = \{a_{j,p,q}\}_{j=1}^{n}\ (mod\, r)$ as its entries, where $p, q, n \in \mathbb{N}$, $n \geq 2$ and r is a prime number. Then,*

$$det(A_{n,p,q}) = x_{n,p,q}^{n-2} - a_{n,p,q}s_{2,p,q}\ (mod\, r), \tag{2}$$

and if $gcd(det(A_{n,p,q}), r) = 1$, then

$$A_{n,p,q}^{-1} = [det(A_{n,p,q})]^{-1}\ \mathrm{SCirc}(s_{1,p,q}, s_{2,p,q}, s_{3,p,q}, \dots, s_{n,p,q})\ (mod\, r), \tag{3}$$

where $x_{n,p,q} = -pa_{n,p,q} + qa_{n-1,p,q} + 1$, $s_{1,p,q} = \frac{det(A_{n,p,q})+(-1)^{n-2}q^{n-1}a_{n,p,q}^{n-2}}{x_{n,p,q}}$, $s_{2,p,q} = px_{n,p,q}^{n-2} + q\sum_{j=1}^{n-2}(-1)^j a_{n-1-j,p,q}q^j a_{n,p,q}^{j-1}x_{n,p,q}^{n-2-j}$, *and* $s_{j,p,q} = (-1)^{j-2}q^{j-2}a_{n,p,q}^{j-3}x_{n,p,q}^{n-j}$ *for* $j = 3,4, \dots, n$.

Proof. Since

$$\det(A_{2,p,q}) = a_{1,p,q}^2 - a_{2,p,q}(-a_{2,p,q})\ (\mathrm{mod}\, r) = 1 + p^2\ (\mathrm{mod}\, r),$$

$$A_{2,p,q}^{-1} = [\det(A_{2,p,q})]^{-1}\begin{pmatrix} 1 & p \\ -p & 1 \end{pmatrix}\ (\mathrm{mod}\, r),$$

$$\begin{aligned}\det(A_{3,p,q}) = {} & a_{1,p,q}(a_{1,p,q}^2 + a_{2,p,q}a_{3,p,q}) - a_{2,p,q}(-a_{1,p,q}a_{3,p,q} + a_{2,p,q}^2) \\ & + a_{3,p,q}(a_{3,p,q}^2 + a_{1,p,q}a_{2,p,q})\ (\mathrm{mod}\, r)\end{aligned}$$

$$\Leftrightarrow \det(A_{3,p,q}) = p^6 + 3p^4q - 2p^3 + 3p^2q^2 - 3pq + q^3 + 1\ (\mathrm{mod}\, r),$$

and

$$\begin{aligned} & A_{3,p,q}^{-1} \\ = [\det(A_{3,p,q})]^{-1} & \begin{pmatrix} 1 - p^3 - pq & p - p^4 - 2p^2q - q^2 & -q \\ q & 1 - p^3 - pq & p - p^4 - 2p^2q - q^2 \\ -p + p^4 + 2p^2q + q^2 & q & 1 - p^3 - pq \end{pmatrix}\ (\mathrm{mod}\, r),\end{aligned}$$

then it is clear that Eqs. (2) and (3) hold for $n = 2$ and $n = 3$. However, for the case $n \geq 4$, the proof is carried out through a sequence of elementary row and column operations applied to $A_{n,p,q}$ as follows.

$$\begin{aligned} B_1 &= E_{(n-2)n(-q)}E_{(n-2)(n-1)(p)} \cdots E_{46(-q)}E_{45(p)}E_{35(-q)}E_{34(p)}E_{24(-q)}E_{23(p)}(A_{n,p,q}) \\ &= \begin{pmatrix} 1 & -p & \cdots & a_{n-1,p,q} & a_{n,p,q} \\ 0 & x_{n,p,q} & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ -(-p)^2 - q & -a_{4,p,q} & \cdots & 1 & -p \\ p & -(-p)^2 - q & \cdots & -a_{n,p,q} & 1 \end{pmatrix}, \end{aligned}$$

$$B_2 = E_{n1(-p)}E_{(n-1)1(q)}E_{(n-1)n(p)}(B_1)$$

$$= \begin{pmatrix} 1 & -p & (-p)^2+q & \cdots & a_{n-1,p,q} & a_{n,p,q} \\ 0 & x_{n,p,q} & qa_{n,p,q} & \cdots & 0 & 0 \\ 0 & 0 & x_{n,p,q} & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & x_{n,p,q} & qa_{n,p,q} \\ 0 & -q & -q(-p) & \cdots & -qa_{n-2,p,q} & x_{n,p,q}-qa_{n-1,p,q} \end{pmatrix},$$

$$B_3 = K_{n1(-a_{n,p,q})} \dots K_{31(-a_{3,p,q})} K_{21(-a_{2,p,q})}(B_2)$$

$$= \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & x_{n,p,q} & qa_{n,p,q} & \cdots & 0 & 0 \\ 0 & 0 & x_{n,p,q} & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & x_{n,p,q} & qa_{n,p,q} \\ 0 & -q & -q(-p) & \cdots & -qa_{n-2,p,q} & x_{n,p,q}-qa_{n-1,p,q} \end{pmatrix},$$

$$B_4 = E_{(n-1)\left(\frac{1}{x_{n,p,q}}\right)} \dots E_{3\left(\frac{1}{x_{n,p,q}}\right)} E_{2\left(\frac{1}{x_{n,p,q}}\right)}(B_3)$$

$$= \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & y_{n,p,q} & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & y_{n,p,q} \\ 0 & -q & -q(-p) & \cdots & -qa_{n-2,p,q} & x_{n,p,q}-qa_{n-1,p,q} \end{pmatrix},$$

$$B_5 = K_{n(n-1)(-y_{n,p,q})} \dots K_{43(-y_{n,p,q})} K_{32(-y_{n,p,q})}(B_4) = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & g_{1,p,q} & g_{2,p,q} & \cdots & g_{n-2,p,q} & d_{n,p,q} \end{pmatrix},$$

where

$$d_{n,p,q} = 1 - pa_{n,p,q} - y_{n,p,q}g_{n-2,p,q},\ y_{n,p,q} = qa_{n,p,q}/x_{n,p,q},$$

$$g_{1,p,q} = -q \text{ and } g_{j,p,q} = -qa_{j,p,q} - y_{n,p,q}g_{j-1,p,q} \text{ for } j = 2,3,\dots,n-2, \text{ and}$$

$$g_{n-2,p,q} = q\sum_{j=1}^{n-2}\left[-a_{j,p,q}\left(-y_{n,p,q}\right)^{n-2-j}\right].$$

Then, by applying Theorem 3, we obtain that

$$d_{n,p,q} = \det(B_5) = \frac{1}{x_{n,p,q}^{n-2}}\det\left(A_{n,p,q}\right) \Leftrightarrow \det\left(A_{n,p,q}\right) = x_{n,p,q}^{n-2}d_{n,p,q}$$

$$\Leftrightarrow \det\left(A_{n,p,q}\right) = x_{n,p,q}^{n-2}\left(1 - pa_{n,p,q} - y_{n,p,q}g_{n-2,p,q}\right) = x_{n,p,q}^{n-1} - q\sum_{j=0}^{n-2}(-1)^j a_{n-1-j,p,q}\left(qa_{n,p,q}\right)^j x_{n,p,q}^{n-2-j}.$$

Moreover, we apply a series of elementary row operations on B_5 as follows.

$$B = E_{n(n-1)(-g_{n-2,p,q})} \cdots E_{n3(-g_{2,p,q})} E_{n2(-g_{1,p,q})}(B_5) = \begin{pmatrix} 1 & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & d_{n,p,q} \end{pmatrix}.$$

Consequently, based on Theorem 2, there exists nonsingular matrices P and Q, where

$$P=\frac{1}{x_{n,p,q}}\begin{pmatrix} x_{n,p,q} & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 1 & -1 & \cdots & 0 & 0 \\ 0 & 0 & 1 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 & -1 \\ 1 & 0 & 0 & 0 & \cdots & 1 & 1 \\ z_{1,p,q} & z_{2,p,q} & z_{3,p,q} & z_{4,p,q} & \cdots & z_{n-1,p,q} & z_{n,p,q} \end{pmatrix},$$

and

$$Q=\begin{pmatrix} 1 & h_{2,p,q} & h_{3,p,q} & h_{4,p,q} & \cdots & h_{n-1,p,q} & h_{n,p,q} \\ 0 & 1 & -y_{n,p,q} & \left(-y_{n,p,q}\right)^2 & \cdots & \left(-y_{n,p,q}\right)^{n-3} & \left(-y_{n,p,q}\right)^{n-2} \\ 0 & 0 & 1 & -y_{n,p,q} & \cdots & \left(-y_{n,p,q}\right)^{n-4} & \left(-y_{n,p,q}\right)^{n-3} \\ 0 & 0 & 0 & 1 & \cdots & \left(-y_{n,p,q}\right)^{n-5} & \left(-y_{n,p,q}\right)^{n-4} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & -y_{n,p,q} & \left(-y_{n,p,q}\right)^2 \\ 0 & 0 & 0 & 0 & \cdots & 1 & -y_{n,p,q} \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix},$$

such that $B=PA_{n,p,q}Q$, where

$$h_{2,p,q}=p \text{ and } h_{j,p,q}=-a_{j,p,q}-y_{n,p,q}h_{j-1,p,q} \text{ for } j=3,4,\dots,n,$$

$$z_{1,p,q}=\frac{x_{n,p,q}}{a_{n,p,q}}\left(d_{n,p,q}-1\right),\ z_{2,p,q}=q, \text{ and } z_{j,p,q}=\left(-y_{n,p,q}\right)z_{j-1,p,q} \text{ for } j=3,4,\dots,n-1.$$

Since $B=PA_{n,p,q}Q$, then $A_{n,p,q}^{-1}=QB^{-1}P$. Note that

$$QB^{-1}=\begin{pmatrix} 1 & h_{2,p,q} & h_{3,p,q} & \cdots & h_{n-1,p,q} & h_{n,p,q}/d_{n,p,q} \\ 0 & 1 & -y_{n,p,q} & \cdots & \left(-y_{n,p,q}\right)^{n-3} & \left(-y_{n,p,q}\right)^{n-2}/d_{n,p,q} \\ 0 & 0 & 1 & \cdots & \left(-y_{n,p,q}\right)^{n-4} & \left(-y_{n,p,q}\right)^{n-3}/d_{n,p,q} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -y_{n,p,q}/d_{n,p,q} \\ 0 & 0 & 0 & \cdots & 0 & 1/d_{n,p,q} \end{pmatrix}.$$

We know that $A_{n,p,q}^{-1}$ is also a skew circulant matrix based on Theorem 1. Thus, we can construct $A_{n,p,q}^{-1}$ by simply computing one of the rows of $QB^{-1}P$. In this case, we compute only the last row. Consequently,

$$A_{n,p,q}^{-1}=QB^{-1}P=\left[\det\left(A_{n,p,q}\right)\right]^{-1}\operatorname{SCirc}\left(s_{1,p,q},s_{2,p,q},\dots,s_{n-1,p,q},s_{n,p,q}\right)\ (\operatorname{mod} r).$$

and

$$\det\left(A_{n,p,q}\right)=x_{n,p,q}^{n-2}-a_{n,p,q}s_{2,p,q}\ (\operatorname{mod} r).$$

■

Eqs. (2) and (3) are computationally fast, as the determinant and its inverse leverage the same numbers in their computations. In this context, $s_{2,p,q}$ is used to compute both the determinant and the inverse. The determinant is used to compute $s_{1,p,q}$, while $a_{n,p,q}$ and $x_{n,p,q}$ are used to compute the determinant and $s_{j,p,q}$ for $j=1,2,\dots,n$. Below, we present a simple example of the use of the explicit formulas contained in Theorem 4.

Example 1. Suppose $n=4$, $p=3$, $q=6$, and $r=257$. Then,

$$\mathcal{F}_{p,q}=\left\{a_{j,p,q}\right\}_{j=1}^{4}\ (\operatorname{mod} 257)=\{1,-3,15,-63\}\ (\operatorname{mod} 257)=\{1,254,15,194\},$$

$$x_{4,3,6}=-3a_{4,3,6}+6a_{3,3,6}+1=-3\cdot 194+6\cdot 15=-491,$$

$$s_{2,3,6} = 3x_{4,3,6}^2 + 6\sum_{j=1}^{2}(-1)^j a_{3-j,3,6} 6^j a_{4,3,6}^{j-1} x_{4,3,6}^{2-j},$$

$$= 3 \cdot (-491)^2 - 6 \cdot 254 \cdot 6 \cdot (-491) + 6 \cdot 1 \cdot 6^2 \cdot 194$$

$$\Leftrightarrow s_{2,3,6} = 5254851,$$

$$\det(A_{4,3,6}) = x_{4,3,6}^2 - a_{4,3,6} s_{2,3,6} = (-491)^2 - 194 \cdot 5254851$$

$$\Leftrightarrow \det(A_{4,3,6}) = -1019200013,$$

$$s_{1,3,6} = \frac{\det(A_{4,3,6}) + (-1)^2 6^3 a_{4,3,6}^2}{x_{4,3,6}} = \frac{-1019200013 + 6^3 \cdot 194^2}{-491} = 2059207,$$

$$s_{3,3,6} = -6x_{4,3,6} = -6 \cdot (-491) = 2946,$$

$$s_{4,20,25} = 6^2 a_{4,3,6} = 36 \cdot 194 = 6984,$$

Thus, according to Theorem 4, the determinant of $A_{4,3,6}$ over $\mathbb{Z}_{257}$ is

$$\det(A_{4,3,6}) = -1019200013 \pmod{257} = 50,$$

Furthermore, we obtain that

$$[\det(A_{4,3,6})]^{-1} \pmod{257} = 50^{-1} \pmod{257} = 36,$$

$$A_{4,3,6}^{-1} = [\det(A_{4,3,6})]^{-1}\,\mathrm{SCirc}(s_{1,3,6}, s_{2,3,6}, s_{3,3,6}, s_{4,3,6}) \pmod{257}$$

$$= 36 \cdot \mathrm{SCirc}(2059207{,}5254851{,}2946{,}6984) \pmod{257}$$

$$= 36\begin{pmatrix} 2059207 & 5254851 & 2946 & 6984 \\ -6984 & 2059207 & 5254851 & 2946 \\ -2946 & -6984 & 2059207 & 5254851 \\ -5254851 & -2946 & -6984 & 2059207 \end{pmatrix} \pmod{257}.$$

So, based on Theorem 4, the inverse of $A_{4,3,6}$ over $\mathbb{Z}_{257}$ is

$$A_{4,3,6}^{-1} = \begin{pmatrix} 59 & 20 & 172 & 78 \\ 179 & 59 & 20 & 172 \\ 85 & 179 & 59 & 20 \\ 237 & 85 & 179 & 59 \end{pmatrix}.$$

3.2 Public-Key Cryptography Scheme Based on Hill Cipher with $A_{n,p,q}$ Matrix and ElGamal Technique

The novel public-key cryptography scheme proposed in this research can be presented as follows.

1. Public Key Generation
   Let party B be the message recipient. Party B performs the following steps:
   a. generates a safe prime r;
   b. chooses a generator α of $\mathbb{Z}_r^*$;
   c. chooses a private key $d \in \mathbb{Z}$, where $1 \leq d < \phi(r)$;
   d. computes $\beta = \alpha^d \pmod r$; and
   e. sends the public key (r, α, β) to the sender of the message.

2. Encryption
   Let party A be the sender of the message (or plaintext) and has received the public key (r, α, β) from party B. Suppose the plaintext is represented as $M = (M_1 \quad M_2 \quad \ldots \quad M_N)$, where $M_i \in \mathbb{Z}_r^n$ is a block matrix of the plaintext of M. Party A performs the following steps:
   a. chooses a secret random number $e \in \mathbb{Z}$, where $1 \leq e < \phi(r)$;
   b. computes $p = \alpha^e \pmod r$ and $n = \beta^e \pmod r$;
   c. computes the key matrix $A_{n,p,\lfloor n/2 \rfloor}$ over $\mathbb{Z}_r$;
   d. encrypts M by computing $C_i = M_i A_{n,p,\lfloor n/2 \rfloor} \pmod r \in \mathbb{Z}_r^n$; and
   e. sends $(p \quad C)$ to party B.

3. Decryption
   Party B uses private key d and $(p \quad C)$ to decrypt the ciphertext. Party B performs the following steps:
   a. computes $n = p^d \pmod r$;
   b. computes $A^{-1}_{n,p,\lfloor n/2 \rfloor}$ over $\mathbb{Z}_r$ using Theorem 4; and
   c. decrypts ciphertext by computing $M_i = C_i A^{-1}_{n,p,\lfloor n/2 \rfloor} \pmod r$.

The overall procedure of the public-key cryptography scheme proposed in this study is summarized in the flowchart in Fig. 1 below.

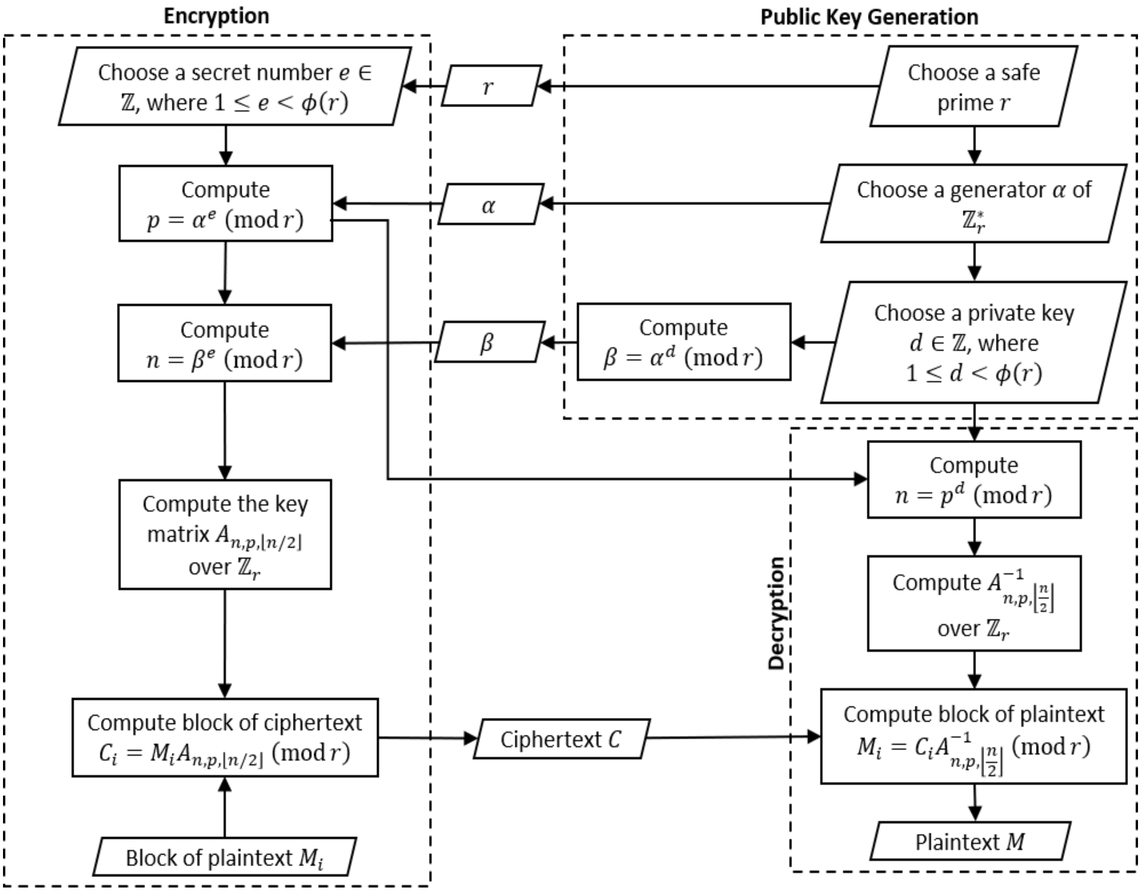

Encryption
Public Key Generation
Choose a secret number $e \in \mathbb{Z}$, where $1 \le e < \phi(r)$
r
Choose a safe prime r
Compute $p = \alpha^e \pmod r$
α
Choose a generator α of $\mathbb{Z}_r^*$
Compute $n = \beta^e \pmod r$
β
Compute $\beta = \alpha^d \pmod r$
Choose a private key $d \in \mathbb{Z}$, where $1 \le d < \phi(r)$
Compute $n = p^d \pmod r$
Compute the key matrix $A_{n,p,\lfloor n/2 \rfloor}$ over $\mathbb{Z}_r$
Decryption
Compute $A^{-1}_{n,p,\lfloor \frac{n}{2} \rfloor}$ over $\mathbb{Z}_r$
Compute block of ciphertext $C_i = M_i A_{n,p,\lfloor n/2 \rfloor} \pmod r$
Ciphertext C
Compute block of plaintext $M_i = C_i A^{-1}_{n,p,\lfloor \frac{n}{2} \rfloor} \pmod r$
Block of plaintext M_i
Plaintext M

Figure 1. Flowchart of the Public-Key Cryptography Scheme Proposed in This Study

This scheme is based on the ElGamal encryption technique, so only the key parameters are transmitted. Unlike conventional ElGamal, which encrypts individual characters, this scheme encrypts entire plaintext block matrices as it is based on the Hill cipher.

3.3 Security and Computational Aspects

The security and computational aspects of the proposed scheme are presented in this section. We begin by discussing the security aspect.

1. Discrete Logarithm Problem

   The matrix $A^{-1}_{n,p,q}$ is generated by computing the value of n, which depends on the publicly known value of p and the private key d. Consequently, an adversary must determine d to obtain $A^{-1}_{n,p,q}$. The value of d can be determined by solving the equation $\beta = \alpha^d \pmod r$, which corresponds to the discrete logarithm problem [16]. This problem is regarded as computationally infeasible if r is a sufficiently very large prime number. To ensure security, the size of r must be in the range of 1024 bits to 4096 bits [37].

2. Brute Force Attack

An adversary attempts to search through all possible $n \times n$ key matrices over $\mathbb{Z}_r$. In this case, there are r^{n^2} possible $n \times n$ matrices over $\mathbb{Z}_r$. Moreover, the set of all invertible $n \times n$ matrices over $\mathbb{Z}_r$ with matrix multiplication, forms the general linear group denoted by $GL_n(r)$. The order of $GL_n(r)$ is given by $|GL_n(r)| = \prod_{k=0}^{n-1}\left(r^n - r^k\right)$ [38].

Example 2. Let $r = 257$ and $n = 50$. Then, there are $r^{n^2} = 257^{2500} \approx 6.80468973864327 \times 10^{6024}$ possible matrices. The number of invertible 50×50 matrices over $\mathbb{Z}_{257}$ can be computed as follows.

$$|GL_{50}(257)| = \prod_{k=0}^{49}\left(257^{50} - 257^k\right) \approx 6.77810932179867 \times 10^{6024}.$$

Therefore, an adversary would need to check approximately $6.77810932179867 \times 10^{6024}$ possible invertible matrices to get the key matrix $A_{50,p,\lfloor 30/2 \rfloor}$.

3. Known Plaintext Attack

Suppose an adversary has access to n distinct plaintext and ciphertext pairs, namely $(M_1, C_1), (M_2, C_2), \dots, (M_n, C_n)$, where $M_i = (m_{i1} \quad m_{i2} \quad \cdots \quad m_{in})$ and $C_i = (c_{i1} \quad c_{i2} \quad \cdots \quad c_{in})$ for $1 \leq i \leq n$. Let the matrices $M_P = \left(m_{ij}\right)$ and $C_P = \left(c_{ij}\right)$. If M_P is invertible, then the adversary can get the key matrix $A_{n,p,\lfloor n/2 \rfloor}$ as by compute

$$A_{n,p,\left\lfloor \frac{n}{2} \right\rfloor} = M_P^{-1} C_P.$$

If M_P is not invertible, then the adversary must obtain another set of n distinct plaintext and ciphertext pairs until an invertible M_P is found. However, the values of e, n, and p used in the current encryption differ from those used in the next encryption. As a result, the entries of the key matrix $A_{n,p,\lfloor n/2 \rfloor}$ in the current encryption will also differ from those in the next encryption. Therefore, the adversary cannot reuse the key matrix from one session to decrypt ciphertexts in subsequent communications.

We present a simple illustration of the proposed public-key cryptography scheme as follows.

Example 3. Let party A be the sender of the message and party B be the recipient of the message. Below, we present the steps taken by each party.

1. Public Key Generation by Party B

The following are the steps taken by party B:

a. generates a safe prime $r = 2 \cdot 431 + 1 = 863$, where $s = 431$ is a prime;

b. $r - 1 = 862$ has two prime factors, 2 and s, so $\alpha = 145$ can be chosen as the generator of $\mathbb{Z}_{863}^*$ since $\alpha^s \pmod r = 145^{431} \pmod{863} = 862 \neq 1$;

c. chooses a private key $d = 494$;

d. computes $\beta = \alpha^d \pmod r = 145^{494} \pmod{863} = 601$; and

e. sends the public key $(863,145,601)$ to party A.

2. Encryption by Party A

Party A encrypts and sends the message “Hello!!!” to B with the following steps:

a. chooses a secret random number $e = 32$;

b. computes $p = \alpha^e \pmod r = 145^{32} \pmod{863} = 110$;

c. computes $n = \beta^e \pmod r = 601^{32} \pmod{863} = 3$;

d. converts the message “Hello!!!” into ASCII decimal as follows

$$M = (72 \quad 101 \quad 108 \quad 108 \quad 111 \quad 33 \quad 33 \quad 33);$$

e. partitioning the plaintext M into

$M_1 = (72 \quad 101 \quad 108)$, $M_2 = (108 \quad 111 \quad 33)$, and $M_3 = (33 \quad 33 \quad 0)$;

f. computes the matrix $A_{3,110,1}$ over $\mathbb{Z}_{863}$, so that we obtain that

$$A_{3,110,1} = \mathrm{SCirc}(1{,}753{,}19) \pmod{863};$$

g. encrypts M by computing $C_i = M_i A_{3,110,1} \pmod{863}$, so that we get that

$C_1 = (540 \quad 485 \quad 722)$, $C_2 = (766 \quad 549 \quad 231)$, and $C_3 = (269 \quad 718 \quad 449)$.

Then,

$$\begin{aligned} C &= (540 \;\; 485 \;\; 722 \;\; 766 \;\; 549 \;\; 231 \;\; 269 \;\; 718 \;\; 449) \\ &= (3 \quad \text{g̰} \quad \text{˒} \quad \text{˽} \quad \text{ȥ} \quad \text{ç} \quad \text{č} \quad \text{ˏ} \quad \text{ǁ}) \end{aligned}$$

h. sends $(p \quad C)$ to B.

3. Decryption by Party B

Party B uses private key d and $(p \quad C)$ to decrypt the ciphertext, with the following steps:

a. computes $n = p^d \pmod r) = 110^{494} \pmod{863} = 3$;

b. computes the matrix $A_{3,110,1}^{-1}$ over $\mathbb{Z}_{863}$ using Theorem 4, so that we obtain that

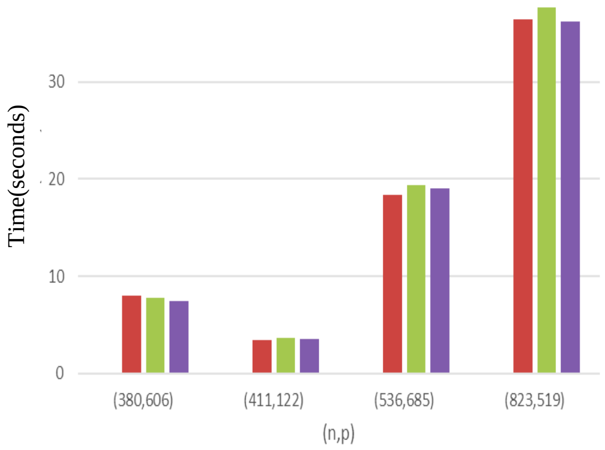
$$A_{3,110,1}^{-1} = \mathrm{SCirc}(655,422,318) \pmod{863}; \text{ and}$$

c. decrypts the ciphertext by computing $M_i = C_i A_{3,110,1}^{-1} \pmod{863}$, so that we get that $M_1 = (72 \quad 101 \quad 108)$, $M_2 = (108 \quad 111 \quad 33)$, and $M_3 = (33 \quad 33 \quad 0)$.

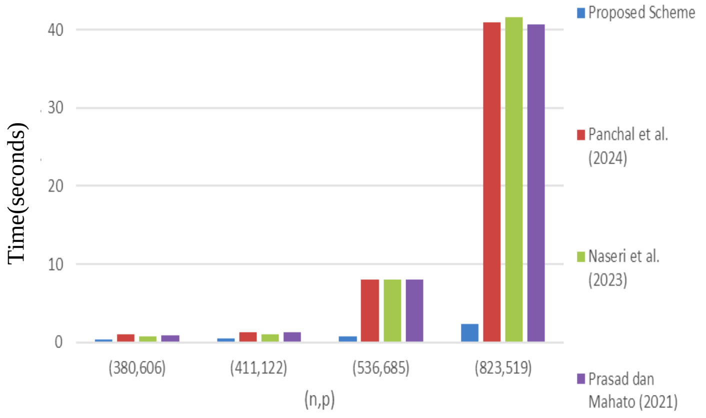
Consequently,

$$M = (72 \quad 101 \quad 108 \quad 108 \quad 111 \quad 33 \quad 33 \quad 33 \quad 0) = (H \quad e \quad l \quad l \quad o \quad ! \quad ! \quad ! \quad).$$

The computation time of the public key cryptographic scheme in this study is compared with that proposed in [23], [24] and [25]. Let the public key $(r, \alpha, \beta) = (983,398,950)$ and the plaintext message M of size $1 \times 3n$ be randomly chosen. The following shows a comparison of the encryption and decryption computation time (seconds) in Fig. 2 and Table 1.



(a)



(b)

Figure 2. Computational Time of the Scheme Proposed in This Study and the Scheme Proposed in [23], [24] and [25] for (a) Encryption and (b) Decryption

Table 1. Computational Time of the Scheme Proposed in This Study and the Scheme Proposed in [23], [24] and [25] for Encryption and Decryption

Scheme	n	p	Encryption Time (seconds)	Decryption Time (seconds)
Proposed in This Study	380	606	0.0216616	0.3207920
	411	122	0.0311113	0.4348070
	536	685	0.0383450	0.7648180
	823	519	0.0916562	2.3837900
Panchal *et al*. (2024)	380	606	7.9686200	0.9513410
	411	122	3.4424300	1.2794100
	536	685	18.3427000	8.0722700
	823	519	36.4818000	40.9020000
Naseri *et al*. (2023)	380	606	7.7517200	0.7795170
	411	122	3.6590300	1.0309300
	536	685	19.3314000	7.9729200
	823	519	37.6896000	41.5998000
Prasad and Mahato (2021)	380	606	7.3933300	0.9437380
	411	122	3.5223600	1.2257400
	536	685	18.9975000	7.9653500
	823	519	36.2777000	40.6545000

As seen in Fig. 2 and Table 1, the computation time of encryption and decryption across all tested schemes tends to increase as the size of the matrix increases. However, the scheme proposed in this study is able to perform encryption and decryption significantly faster than the three other schemes. Specifically, the proposed scheme achieves encryption approximately 478.36 times faster than the scheme in [23], 495.44 times faster than that in [24], and 504.14 times faster than that in [25] when $n = 536$ and $p = 685$. For decryption, the proposed scheme is approximately 17.16 times faster than the scheme in [23], 17.05 times faster than that in [24], and 17.45 times faster than that in [25] when $n = 823$ and $p = 519$.

The computation time of the scheme proposed in this study is significantly faster than the schemes in [23], [24] and [25] for both encryption and decryption. This advantage arises from the structure of the matrix $A_{n,p,\lfloor n/2 \rfloor}$ over $\mathbb{Z}_r$, which is easy to construct, as it depends only on the first n terms of the second-order relation $\mathcal{F}_{p,\lfloor n/2 \rfloor}$ over $\mathbb{Z}_r$. Furthermore, the matrix $A^{-1}_{n,p,\lfloor n/2 \rfloor}$, used in decryption, can also be computed efficiently using Theorem 1, whereas the matrices in the three other schemes are more complex to construct and compute.

4. CONCLUSION

The main conclusions of this research are as follows:

1. The determinant and the inverse of the matrix $A_{n,p,q} \pmod r$, where $n, p, q \in \mathbb{N}$, $n \geq 2$, and r is a prime number, are explicitly formulated in one theorem using elementary row and column operations. The explicit formulas allow for highly efficient computation by reusing the same numerical information.
2. The matrix $A_{n,p,\lfloor n/2 \rfloor} \pmod r$, where $n, p \in \mathbb{N}$, $n \geq 2$, and r is a prime number, along with its determinant and inverse, are used to construct a new public-key cryptography based on the Hill cipher and ElGamal technique. The decryption does not require transmitting the complete key matrix but only its key parameters, thus significantly reducing the computational complexity. The encryption and decryption are performed on blocks of plaintext instead of single plaintext characters.

3. The primary security of the proposed scheme lies in the hardness of the discrete logarithm problem. Specifically, recovering the private key d and the matrix size n is computationally infeasible for an adversary if r is chosen to be a very large prime (e.g., 1024 to 4096 bits). The scheme is resistant to known plaintext attack, since the values of e, n, and p always change, resulting in distinct key matrices $A_{n,p,\lfloor n/2 \rfloor}$ for each session. Furthermore, the scheme is also resistant to brute force attack since an adversary would have to exhaustively try all invertible square matrices over $\mathbb{Z}_r$, which is computationally impractical.
4. The proposed scheme can perform encryption up to 478.36 times faster than the scheme in [23], 495.44 times faster than that in [24], and 504.14 times faster than that in [25]. For decryption, the proposed scheme can perform up to 17.16 times faster than the scheme in [23], 17.05 times faster than that in [24], and 17.45 times faster than that in [25]. This remarkable efficiency is mainly due to the simpler construction of the matrix $A_{n,p,\lfloor n/2 \rfloor}$ and the availability of an explicit formula for computing its determinant and inverse, which enables rapid operations that surpass the other three schemes, and the matrices used in these three schemes are more difficult to construct.

Author Contributions

First Author: Conceptualization, methodology, writing-original draft, software, validation, and visualization. Second Author: Resources, formal analysis, supervision, validation. Third Author: Writing-review & editing, supervision, validation. All authors discussed the results and contributed to the final manuscript.

Funding Statement

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Acknowledgment

The authors have no acknowledgments to declare.

Declarations

The authors declare that they have no conflicts of interest to report study.

REFERENCES

[1] P. J. Davis, *CIRCULANT MATRICES*. New York: John Wiley & Sons, 1979.

[2] U. R. Bodasingi and S. Gunupuru, “NEW DIGITAL SIGNATURE SCHEME BASED ON RSA USING CIRCULANT MATRIX,” *SN Comput Sci*, vol. 4, no. 3, p. 275, 2023. doi: https://doi.org/10.1007/s42979-023-01694-4.

[3] M. Sever, “A NTRU TYPE CRYPTOSYSTEM BASED ON CIRCULANT MATRICES,” *Turkish Journal of Science*, vol. 9, no. 3, pp. 207–215, 2024.

[4] A. Pandey, I. Gupta, and D. Kumar Singh, “IMPROVED CRYPTANALYSIS OF A ELGAMAL CRYPTOSYSTEM BASED ON MATRICES OVER GROUP RINGS,” *Journal of Mathematical Cryptology*, vol. 15, no. 1, pp. 266–279, 2020. doi: https://doi.org/10.1515/jmc-2019-0054.

[5] B. Amutha and R. Perumal, “PUBLIC KEY EXCHANGE PROTOCOLS BASED ON TROPICAL LOWER CIRCULANT AND ANTI CIRCULANT MATRICES,” *AIMS Mathematics*, vol. 8, no. 7, pp. 17307–17334, 2023. doi: https://doi.org/10.3934/math.2023885.

[6] Maxrizal, I. G. N. Y. Hartawan, P. Jana, and B. Desy Aniska Prayanti, “MODIFIED PUBLIC KEY CRYPTOSYSTEM BASED ON CIRCULANT MATRIX,” *J Phys Conf Ser*, vol. 1503, no. 1, p. 12007, 2020. doi: https://doi.org/10.1088/1742-6596/1503/1/012007.

[7] X. Zhang, X. Jiang, Z. Jiang, and H. Byun, “ALGORITHMS FOR SOLVING A CLASS OF REAL QUASI-SYMMETRIC TOEPLITZ LINEAR SYSTEMS AND ITS APPLICATIONS,” *Electronic Research Archive*, vol. 31, no. 4, pp. 1966–1981, 2023. doi: https://doi.org/10.3934/era.2023101.

[8] S. UÇAR and N. YILMAZ ÖZGÜR, “RIGHT CIRCULANT MATRICES WITH GENERALIZED FIBONACCI AND LUCAS POLYNOMIALS AND CODING THEORY,” *Balıkesir Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, vol. 21, no. 1, pp. 306–322, 2019. doi: https://doi.org/10.25092/baunfbed.547188.

[9] G. G. Garayar-Leyva, H. Osman, J. J. Estrada-López, and O. Moreira-Tamayo, “SKEW-CIRCULANT-MATRIX-BASED HARMONIC-CANCELING SYNTHESIZER FOR BIST APPLICATIONS,” *Sensors*, vol. 22, no. 8, p. 2884, 2022. doi: https://doi.org/10.3390/s22082884.

[10] K.-Y. Lu, “DIAGONAL AND CIRCULANT OR SKEW-CIRCULANT SPLITTING PRECONDITIONERS FOR SPATIAL FRACTIONAL DIFFUSION EQUATIONS,” *Computational and Applied Mathematics*, vol. 37, no. 4, pp. 4196–4218, Sep. 2018. doi: https://doi.org/10.1007/s40314-017-0570-6.

[11] M.-Z. Zhu, Y.-E. Qi, and G.-F. Zhang, “ON CIRCULANT AND SKEW-CIRCULANT PRECONDITIONED KRYLOV METHODS FOR STEADY-STATE RIESZ SPATIAL FRACTIONAL DIFFUSION EQUATIONS,” *Linear and Multilinear Algebra*, vol. 69, no. 4, pp. 719–731, Mar. 2021. doi: https://doi.org/10.1080/03081087.2019.1617230.

[12] Z. Liu, X. Qin, N. Wu, and Y. Zhang, “THE SHIFTED CLASSICAL CIRCULANT AND SKEW CIRCULANT SPLITTING ITERATIVE METHODS FOR TOEPLITZ MATRICES,” *Canadian Mathematical Bulletin*, vol. 60, no. 4, pp. 807–815, Dec. 2017. doi: https://doi.org/10.4153/CMB-2016-077-5.

[13] Z. Liu, F. Zhang, C. Ferreira, and Y. Zhang, “ON CIRCULANT AND SKEW-CIRCULANT SPLITTING ALGORITHMS FOR (CONTINUOUS) SYLVESTER EQUATIONS,” *Computers & Mathematics with Applications*, vol. 109, pp. 30–43, Mar. 2022. doi: https://doi.org/10.1016/j.camwa.2022.01.027.

[14] I. Dokuzova and D. Razpopov, “FOUR-DIMENSIONAL ALMOST EINSTEIN MANIFOLDS WITH SKEW-CIRCULANT STUCTURES,” *Journal of Geometry*, vol. 111, no. 1, p. 9, Apr. 2020. doi: https://doi.org/10.1007/s00022-020-0521-z.

[15] Y. Wei, Y. Zheng, and Z. Jiang, “SKEW-CIRCULANT MATRIX AND CRITICAL POINTS OF POLYNOMIALS,” *Journal of Mathematical Inequalities*, no. 4, pp. 1427–1431, 2023. doi: https://doi.org/10.7153/jmi-2023-17-93 https://doi.org/10.7153/jmi-2023-17-93.

[16] A. Menezes, P. C. van Oorschot, and S. A. Vanstone, *HANDBOOK OF APPLIED CRYPTOGRAPHY*. Florida: CRC Press, 1996.

[17] M. K. Viswanath and M. R. Kumar, “A PUBLIC KEY CRYPTOSYSTEM USING HIIL’S CIPHER,” *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 18, no. 1–2, pp. 129–138, 2015. doi: https://doi.org/10.1080/09720529.2014.962856.

[18] P. Sundarayya and G. Vara Prasad, “A PUBLIC KEY CRYPTOSYSTEM USING AFFINE HILL CIPHER UNDER MODULATION OF PRIME NUMBER,” *Journal of Information and Optimization Sciences*, vol. 40, no. 4, pp. 919–930, 2019. doi: https://doi.org/10.1080/02522667.2018.1470751.

[19] R. K. Hasoun, S. Faris Khlebus, and H. K. Tayyeh, “A NEW APPROACH OF CLASSICAL HILL CIPHER IN PUBLIC KEY CRYPTOGRAPHY,” *International Journal of Nonlinear Analysis and Applications*, vol. 12, no. 2, pp. 1071–1082, 2021. doi: https://doi.org/10.22075/ijnaa.2021.5176.

[20] Z. Y. Karatas, E. Luy, and B. Gonen, “PUBLIC KEY CRYPTOSYSTEM BASED ON MATRICES,” *Int J Comput Appl*, vol. 182, no. 42, pp. 47–50, Feb. 2019. doi: https://doi.org/10.5120/ijca2019918432.

[21] A. V. N. Krishna, A. H. Narayana, and M. K. Vani, “A NOVEL APPROACH WITH MATRIX BASED PUBLIC KEY CRYPTO SYSTEMS,” *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 20, no. 2, pp. 407–412, Feb. 2017. doi: https://doi.org/10.1080/09720529.2015.1085738.

[22] M. Kumari and J. Tanti, “CRYPTOGRAPHY USING MULTINACCI BLOCK MATRICES,” *International Journal of Nonlinear Analysis and Applications*, vol. 14, no. 10, pp. 57–65, 2023. doi: 10.22075/ijnaa.2023.29918.4295.

[23] J. Panchal, H. Chandra, and A. Singh, “A NEW PUBLIC KEY CRYPTOGRAPHY USING GENERALIZED FIBONACCI MATRICES,” *Surveys in Mathematics and its Applications*, vol. 19, pp. 301–316, 2024.

[24] K. Prasad and H. Mahato, “CRYPTOGRAPHY USING GENERALIZED FIBONACCI MATRICES WITH AFFINE-HILL CIPHER,” *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 25, no. 8, pp. 2341–2352, 2021. doi: https://doi.org/10.1080/09720529.2020.1838744.

[25] A. R. Naseri, A. Abbasi, and R. E. Atani, “A NEW PUBLIC KEY CRYPTOGRAPHY USING M_Q MATRIX,” *Journal of Mathematical Modeling*, vol. 11, no. 4, 2023.

[26] K. Prasad, M. Kumari, and H. Mahato, “A MODIFIED PUBLIC KEY CRYPTOGRAPHY BASED ON GENERALIZED LUCAS MATRICES,” *Communications in Combinatorics and Optimization*, vol. 10, no. 3, pp. 665–679, 2025.

[27] V. Billore and N. Patel, “CRYPTOGRAPHY UTILIZING THE AFFINE-HILL CIPHER AND EXTENDED GENERALIZED FIBONACCI MATRICES,” *Electron J Math Anal Appl*, vol. 11, no. 2, pp. 1–11, 2023. doi: https://doi.org/10.21608/ejmaa.2023.295792.

[28] R. E. Cline, R. J. Plemmons, and G. Worm, “GENERALIZED INVERSES OF CERTAIN TOEPLITZ MATRICES,” *Linear Algebra Appl*, vol. 8, no. 1, pp. 25–33, 1974. doi: https://doi.org/10.1016/0024-3795(74)90004-4.

[29] S. Guritman, “SIMPLE FORMULATIONS ON CIRCULANT MATRICES WITH ALTERNATING FIBONACCI,” *Communications of the Korean Mathematical Society*, vol. 38, no. 2, pp. 341–354, 2023.

[30] F. YEŞİL BARAN, “THE EIGENVALUES OF CIRCULANT MATRICES WITH GENERALIZED TETRANACCI NUMBERS,” *Gümüşhane Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, vol. 11, no. 2, pp. 417–423, 2021. doi: https://doi.org/10.17714/gumusfenbil.830575.

[31] Y. Gong, Z. Jiang, and Y. Gao, “ON JACOBSTHAL AND JACOBSTHAL-LUCAS CIRCULANT TYPE MATRICES,” *Abstract and Applied Analysis*, vol. 2015, pp. 1–11, 2015. doi: https://doi.org/10.1155/2015/418293.

[32] Y. Wei, Y. Zheng, Z. Jiang, and S. Shon, “DETERMINANTS, INVERSES, NORMS, AND SPREADS OF SKEW CIRCULANT MATRICES INVOLVING THE PRODUCT OF FIBONACCI AND LUCAS NUMBERS,” *Journal of Mathematics and Computer Science*, vol. 20, no. 1, pp. 64–78, 2019. doi: https://doi.org/10.22436/jmcs.020.01.08.

[33] J. Yao and J. Sun, “EXPLICIT DETERMINANTS AND INVERSES OF SKEW CIRCULANT AND SKEW LEFT CIRCULANT MATRICES WITH THE PELL-LUCAS NUMBERS,” *Journal of Advances in Mathematics and Computer Science*, vol. 26, no. 2, pp. 1–16, 2018. doi: https://doi.org/10.9734/JAMCS/2018/38768.

[34] Z. Jiang and Y. Wei, “SKEW CIRCULANT TYPE MATRICES INVOLVING THE SUM OF FIBONACCI AND LUCAS NUMBERS,” *Abstract and Applied Analysis*, vol. 2015, pp. 1–9, 2015. doi: https://doi.org/10.1155/2015/951340.

[35] Y. Zheng and S. Shon, “EXACT DETERMINANTS AND INVERSES OF GENERALIZED LUCAS SKEW CIRCULANT TYPE MATRICES,” *Appl Math Comput*, vol. 270, pp. 105–113, Nov. 2015. doi: https://doi.org/10.1016/j.amc.2015.08.02.

[36] P. Lancaster and M. Tismenetsky, *THE THEORY OF MATRICES WITH APPLICATIONS*, 2nd ed. San Diego: Academic Press, 1985.

[37] T. S. Fun and A. Samsudin, "AN EFFICIENT ELGAMAL ENCRYPTION SCHEME BASED ON POLYNOMIAL MODULAR ARITHMETIC IN $\mathbb{F}_2^n$," in *ICCST 2017*, R. Alfred, H. Lida, A. Ibrahim, and Y. Lim, Eds., Singapore: Springer, 2018, pp. 99–107. doi: https://doi.org/10.1007/978-981-10-8276-4_10.

[38] N. Jacobson, *BASIC ALGEBRA I*, 2nd ed. New York: Dover Publications, Inc, 2009.