International Journal of Advances in Applied Sciences (IJAAS)
Vol. 15, No. 1, March 2026, pp. 293~302
ISSN: 2252-8814, DOI: 10.11591/ijaas.v15.i1.pp293-302

A novel circulant matrix-based McEliece framework for secure digital communication

Ravikumar Inakoti[1], James Stephen Meka[2], Padala Venkata Gopala Durga Prasad Reddy[1]
[1]Department of Computer Science and Systems Engineering, Andhra University, Visakhapatnam, India
[2]Dr. B. R. Ambedkar Chair, Andhra University, Visakhapatnam, India

Article Info

Article history:

Received Apr 24, 2025
Revised Dec 23, 2025
Accepted Jan 1, 2026

Keywords:

Circulant matrix
Code-based cryptosystem
Cryptography
Data communication
McEliece

ABSTRACT

McEliece cryptosystem is old and well-explored post-quantum cryptography system that offers superior security against quantum attacks. Though the system holds great potential and superior security, the challenge associated with large key sizes has made system impractical for most applications. The first challenge against McEliece cryptosystem remains its large key sizes, which make system impractical, especially when implementing internet of things (IoT) and mobile communication applications. Overcoming challenges and retaining superior security still remains an issue to explore. This paper presents investigation into use of circulant matrices for McEliece encryption system to achieve a considerable reduction in key sizes and enhance fast encryption processes. The use of circulant matrices' inherent properties boosts performance without focusing much on system's security. In addition, the paper presents security evaluation process for modified communication system to determine and mitigate weaknesses that might arise, considering use of sophisticated encryption systems. Findings and results explore use of circulant matrices, which achieve great reductions in key sizes and improve efficiency of process. Security evaluation reports that proper scrambling techniques are efficient at mending the vulnerabilities associated with circulant matrix structures. A modified McEliece cryptosystem using circulant matrices offers superior data communication, balancing both strong security and efficient computational processes, making system ideal for use in recent communication systems.

Corresponding Author:

Ravikumar Inakoti
Department of Computer Science and Systems Engineering, Andhra University
Visakhapatnam, Andhra Pradesh, India
Email: ravirk1228@gmail.com

1. INTRODUCTION

The security of data is paramount during end-to-end data communication and data storage. To ensure safe delivery of data transferred over the internet, cryptography has been widely used to transform the data into a non-readable content that can only be reverted to its initial by an authorized user. With the continuous adoption of internet technology, data communication experiences a large increase in security attack especially when wireless channels are employed for communication. To address the security challenges in data communications and ensure data integrity, numerous cryptographic algorithms were developed [1]. These algorithms have proved promising in preventing various forms of attacks.

However, majority of these cryptosystems can be easily broken by the existence of quantum computing. Quantum computers are highly computation-intensive and capable of employing algorithms like Shor's and Grover's [2], [3] to accelerate the execution of tasks. With the evolution and advancement in

quantum computing, promising cryptographic algorithms like Rivest-Shamir-Adleman (RSA) and Diffie-Hellman algorithms have proven to be vulnerable, thus necessitating the need for other post quantum solutions. Primitive based solutions well-suited for mathematical problems are required. These solutions may still be very difficult for the quantum computer to solve. Code-based cryptography, multivariate, lattice-based schemes are some techniques that can inherently resist attacks by the quantum computer.

Code-based encryption approach represents one of the most viable options for cryptography following quantum computing, or encryption systems immune to attacks by quantum computers. The McEliece and Niederreiter encryption schemes are two examples [4], [5]. It has been established in [6] that the fundamental issue in the schemes is the efficiency of decoding the linear block codes, which is considered a nondeterministic polynomial-time (NP)-complete problem. In code-based cryptography, the common encryption schemes are McEliece encryption scheme, Niederreiter encryption scheme. Recently, the hybrid McEliece encryption scheme (HyMES) was explained [7]. Like the RSA encryption scheme, the conventional McEliece system of information encryption for secure information communication fails to capture the attention of researchers, users, and industries, as the magnitude of the generation matrix used in the public key of the approach is relatively enormous. However, the vulnerability associated with the conventional encryption schemes like RSA and Diffie-Hellman algorithms when used on quantum computing has made it one of the focuses of research in quantum security.

One of the major focuses on the conventional McEliece system of encryption is reduction in the magnitude of the system key. For example, Fathalla and Azab [8] investigated the notion of employing compact representation of the shared matrix of the conventional McEliece system of information encryption. The research in [9], [10] proposed quasi-cyclic (QC) alternant along with the quasi-dyadic (QD) Goppa codes to reduce the magnitude of the conventional McEliece scheme of information encryption, which they succeeded in reducing it from several hundred thousand bits to 20 kilobits. The purpose of those constructs is to use first row permutations to produce the entire matrix. Additionally, those constructions enable message encryption using only the initial row of the matrix rather than the entire matrix. In both scenarios, the binary parameters remain secure even after multiple attacks.

Other methods proposed to deplete the magnitude of the shared key of the traditional McEliece information encryption scheme include “algebraic geometric (AG) codes” [11], “generalized Reed-Solomon (GRS) codes” [12], “low-density parity check (LDPC) codes” [13], “Reed-Muller (RM) codes” [14], “low-rank parity check (LRPC) codes” [15], and many more that allow for shorter shared keys, have been demonstrated through various codes. The majority of these variations have been successfully cryptanalyzed, even though the original McEliece cryptosystem is still secure [16], [17]. The alternative codes must be treated with caution because of their excessive structure, even with their promising features. Polar coding was initially intended to be a method, akin to previous Pinsker and Massey schemes, for increasing the cutoff rate of sequential decoding. The secret to raising the cutoff rate is to take a vector channel (whether it’s naturally occurring or purposefully produced), split it up into multiple interrelated subsidiary channels, and then apply a separate ordered decoder on every subchannel. Polar coding was initially intended to be a low-complexity recursive channel combining and splitting operation of this kind, with the goal of being employed as internal code in a composite scheme with external convolutional coding and ordered decoding.

Nevertheless, the initial goal of increasing the cutoff rate to channel capacity was actually achieved without the need for an outer code because the polar inner code proved to be so successful [18]. With the continuous growth in the field of quantum computing, there is need for more robust schemes that will be difficult for the quantum systems to break. In this paper, a modified McEliece public key encryption system with high level of security to produce a secure communication scheme based on polar code, which can prevent Brickel’s attack during communication. The objectives of this paper are summarized as follows:

- Create a modified form of McEliece cryptosystem that uses circulant matrices to make its public key smaller. This will reduce a major weakness of McEliece cryptosystem, its large public key size. The idea will help in improving the usage of McEliece cryptosystem in situations where limited storage capacity would not allow all its cryptograms to be transmitted.
- To examine the security of the McEliece cryptosystem based on circulant matrices against both classic and quantum attacks. This involves scrutinizing the ability of circulant matrices, complemented by scrambling and permutation matrices, to ensure the security of confidential message transmission.
- To analyze and compare the effectiveness of the McEliece system based on a circulant matrix with the McEliece system. In this area, we plan to test and analyze the speed of encryption and decryption, the time required for generating a key, and, most importantly, the effectiveness and efficiency added by the use of a circulant matrix.

The rest of the document is structured as follows: section 2 describes several research papers which are closely related to code-based encryption schemes, section 3 provides information about the traditional McEliece algorithm and basic principles about circulant matrices. Section 4 presents the proposed circulant

matrix-based McEliece cryptosystem in this paper. Section 5 of this paper presents the security analysis and comparison of the proposed circulant matrix-based McEliece cryptosystem, and lastly, section 6 of this paper draws a conclusion on the circulant matrix-based McEliece cryptosystem.

2. RELATED WORK

One of the first and longest-lasting public-key encryption schemes is the McEliece system for information encoding, created in the year 1978 by Robert J. McEliece. Its defense against quantum attacks, which come from its use of error-correcting codes, has enticed a significant interest by numerous entities in the cryptography world. The McEliece cryptosystem is thoroughly covered in this literature review, which also explores its recent developments, security features, implementation difficulties, and theoretical underpinnings. The McEliece cryptosystem was introduced by Robert J. McEliece, who also suggested using algebraic coding theory for public-key encryption. It describes the fundamental ideas and draws attention to its possible benefits over alternative encryption techniques. Maduni *et al.* [19] examine a McEliece cryptosystem variation that can guarantee that encoding utilized as the shared generated key is no more similar to the permutation of the secret/unshared code. As a result, the adoption of traditional code families, such as Reed-Solomon codes, which have been long-standing exclusions from the conventional McEliece system of information encoding due to safety concerns, may be given another look. This elevated the public key's security level. The primary benefits of the suggested approach are these because it is widely recognized that these categories of encodings can result in a decrease in magnitude of the shared keys or, comparably, an increase in information decoding resistivity.

New parameters for the conventional McEliece and Niederreiter cryptosystems are proposed [20], guaranteeing baseline security across all investigated threats. The modified settings take into consideration the improved threat, the recently added binary Goppa code list decoding approach, and the option to employ code sequences that aren't multiple of two. For the same level of security, the resulting shared-key lengths are significantly shorter compared to prior parameter settings selection. To further clarify on the nature of the conventional McEliece cryptosystem's quantum resistance, the authors examine potential quantum attacks and suggest defense strategies. Puneyani and Bhat [21] demonstrated execution of a conventional McEliece system of information encryption on a field-programmable gate array (FPGA), guaranteeing the security guidelines provided by the European Telecommunications Standards Institute for the next wave of encryption systems that are robust to quantum resistance. Employing a shared key with a byte length of 2,097,152, the suggested implementation by the authors offers quantum security with bits beyond 128. The suggested system is built around a hardware and software settings that makes use of an AX14 lite interface to link an ARM Cortex-A53 core to a coprocessor. The state-of-the-art comprehensive overview, component-by-component algorithmic description, and implementation of this cryptosystem are presented [22]. Different McEliece cryptosystem attacks are covered in separate sections. Aside from simulation of the cryptosystem on different extension degrees, the authors also present experimental results using Goppa codes. The authors concluded the results and the different implementation-related issues based on the simulations that were run.

The modern variants of the classical cryptosystems put forth by Harold Niederreiter (1986) and Robert J. McEliece (1978) are examined [23]. Five different code-based shared key systems of information encryption have been thoroughly reviewed. It is demonstrated that there are serious problems with several contemporary expositions of traditional McEliece and Niederreiter systems of information encryption. It has been demonstrated, in particular, that XGRS encryption systems, which bases itself on the broadened Reed-Solomon code, contain multiple flaws and is not as secure against the information set decoding attack as it is supposed to be. It is demonstrated that both the shared and unshared encryption keys occupy a significant quota of storage and that key generation and decryption in contemporary cryptosystems take a long time.

A novel code-based digital signature built on the McEliece system of information encryption is proposed [24]. Algorithms for the construction of shared key, signing, and authentication are shown. The public key is created by the key generation algorithm using random inverse matrices. Compared to the CFS scheme, the signing algorithm is less complex and takes less computing time to sign a document. Forgeries can be recognized by the verification algorithm. It is demonstrated that the suggested scheme is resistant to structural attacks using public keys.

Birhanu *et al.* [25] employ an irregular code version of the QC-LDPC and the quasi-cyclic moderate-density parity-check (QC-MDPC) in place of Goppa code, which is used in tandem to address previous bottlenecks in the system. Results obtained by the proposed method also confirmed that the length of the shared key was appropriately shortened. The fact that this release of the McEliece cryptosystem is more resistant to message-resend threats is another benefit over the previous iteration. Sutradhar [26] focuses on the development of indistinguishability under adaptive chosen ciphertext attack 2 (IND-CCA2) secure version of the conventional McEliece system of information encryption. The authors employ the S-repetition encryption of S/2 different information with a single typical permutation, which contradict the S-repetition

encryption of single information in other modification. New McEliece system of information encryption, with its foundation on punctured RM codes are [27]. They effectively demonstrate the inefficacy of well-known security threats on the suggested RM code-based McEliece cryptosystem, including the Minder-Shokrollahi, Chizhov-Borodin, and square code attacks. In order to guard against the aforementioned attacks on the suggested RM code-based cryptosystems, the authors devised an ideal puncturing scheme. Specifically, they determined the precise areas of puncturing positions where the generator matrix's least amount of punctured columns could be found.

3. PRELIMINARIES

The working of convention McEliece cryptosystem and circulant matrix are described in this section.

3.1. The McEliece cryptosystem

Robert J. McEliece created the McEliece cryptosystem, a public-key encryption algorithm, in 1978. In contrast to numerous other public-key encryption algorithms that depend on discrete logarithm problems or factorization difficulties, McEliece is based on the challenge of decoding error-correcting codes, which are frequently utilized in digital communications. The McEliece cryptosystem relies on Goppa code, permutation matrix, and an invertible matrix to scramble the plaintext and conceal a secret key. The corresponding codeword generated is finally permuted before transmitted through the transmission channel. The plain text from the sender is first scrambled, and the generated codeword is permuted. A set of bits up to t from the codeword are flipped, with t representing the error correction code of the generated codeword. The public key of McEliece cryptosystem is a combination of non-singular 'k' by 'k' scramble matrix, a 'k' by 'n' generator matrix, and 'n by n' permutation matrix. The encryption and decryption process of the McEliece cryptosystem is given as follows.

3.1.1. Private key generation

The private key of the McEliece cryptosystem is a combination of the generator matrix 'G', the scrambling matrix 'S', and the random permutation matrix 'P'. The generator matrix is given as shown in (1).

$$G_{kxn} = \left(I_k \middle| P'_{kx(n-k)}\right) \tag{1}$$

Where 'I_k' is an identity matrix of dimension k by k, and P' is a random permutation matrix of dimension '$kx(n-k)$'. The parity check matrix of the linear code is obtained as shown in (2). The private key is 'S_k' is the combination of the matrices 'G', 'S', and 'P'.

$$H_{n-k(n)} = \left(T'^{T} \middle| I_{(n-k)}\right) \tag{2}$$

3.1.2. Public key generation

The public key consists of 'k' by 'n' matrix G′ defined by 'G. S. P' and error correcting capability t. The encryption process of the McEliece cryptosystem is as follows: given a message m $\in F_k^2$, a random error vector e $\in F_2^n$ is chosen with a weight w≤t and compute corresponding encrypted message as (3).

$$y = mG' + e \tag{3}$$

To decrypt the encrypted message, the following is computed as shown in (4).

$$yP^{-1} = mSG + eP^{-1} \tag{4}$$

Since 'P' is a permutation matrix, '$P^{-1} = P^T$' is equally a permutation matrix as such, the vector 'eP^{-1}' has the same weight as e. Therefore, 'mS' can be obtained by decoding 'yP^{-1}'. Finally, 'mS' can be multiplied by S^{-1} as $(mS)\,S^{-1}$ to obtain m.

3.2. Circulant matrix

Circulant matrix is a matrix in which each row relative to the previous row vector is rotated one element to the right [28]. The product of circulant matrices is also a circulant matrix and commutative [29]. Matrix A is a circulant matrix with entries generated from the n-vector $\{r1, r2, \ldots, rn\}$ by cyclically permuting its entries, and is of the form as shown in (5).

$$A = \begin{bmatrix} r_1 & r_2 & \cdots & r_N \\ r_N & r_1 & \cdots & r_{N-1} \\ \vdots & \vdots & \vdots & \vdots \\ r_2 & r_3 & \ldots & r_1 \end{bmatrix} \quad (5)$$

For example, we define the circulant matrix generated by three elements as shown in (6).

$$Circ_3(\alpha, \beta, \gamma) = \begin{bmatrix} \alpha & \beta & \gamma \\ \gamma & \alpha & \beta \\ \beta & \gamma & \alpha \end{bmatrix} \quad (6)$$

The block circulant of circulant matrix ($Circi$) is an $\mathrm{M} \times \mathrm{M}$ matrix for every $i = 1, 2, \ldots, N$. Then $\{Circ1, Circ2, \ldots, CircN\}$ generates an $\mathrm{N\,M} \times \mathrm{N\,M}$ blocks circulant matrices. An example of a block circulant matrix ($\mathrm{Circ_B}$) for 'A' defined as shown in (7) to (9).

$$Let\ M = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 8 \end{bmatrix};\ then \quad (7)$$

$$Circ_B = Circ\ (X, Y, Z) = \begin{bmatrix} X & Y & Z \\ Z & X & Y \\ Y & Z & X \end{bmatrix} \quad (8)$$

We have,

$$X = Circ\ (1,2,3) = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix}; Y = Circ\ (4,5,6) = \begin{bmatrix} 4 & 5 & 6 \\ 6 & 4 & 5 \\ 5 & 6 & 4 \end{bmatrix};$$
$$Z = Circ(7,8,9) = \begin{bmatrix} 7 & 8 & 9 \\ 9 & 7 & 8 \\ 8 & 9 & 7 \end{bmatrix} \quad (9)$$

4. MATERIALS AND METHOD

In this section, the circulant matrix-based McEliece crypto system is presented in detail. The proposed method uses the structure of the traditional McEliece scheme but introduces the circulant matrices to improve the efficacy of storage and computation. The McEliece cryptosystem is based on the difficulty of decoding random linear codes, often using Goppa codes, which makes it resistant to quantum-based attacks. Using circulant matrices allows for a reduction in key size, enhancing the system's practicality. The proposed system consists of three phases, which include key generation phase, encryption phase, and decryption phase.

4.1. Key generation phase

In the McEliece cryptosystem, key generation involves creating a public and private key pair through a Goppa code (or a comparable error-correcting code) and applying random transformations to conceal its structure. By using circulant matrices, storage requirements for the generator matrix are minimized, as the entire matrix can be generated from just one row. To generate the private and public key, a code parameter n representing code length, k representing the dimension of the code parameter, and error correction capability t is chosen. After choosing the parameters, the binary Goppa code c, with a generator matrix 'G' of size k x n is chosen.

i) Primary key generation: to construct the private key, a generator matrix 'G' is created for the chosen Goppa code, structured as a circulant matrix. For example, a vector $\mathrm{v} = \{\mathrm{v}_0, \mathrm{v}_1, \mathrm{v}_2, \ldots, \mathrm{v}_{\mathrm{n}-1}\}$ is chosen to generate a circulant matrix 'G' by rotating v row by row. In addition to G, two secret matrices 'S' and 'P' representing a random invertible k×k matrix used to permutate the plain text and a random permutation matrix of size n×n that scrambled the order of the code bits are defined. The private key is then generated to compose the triple $(\mathrm{G}, \mathrm{S}, \mathrm{P})$ as shown in (10).

$$S_k = (G, S, P) \quad (10)$$

Where 'G' is the generator matrix of Goppa code in circulant matrix form, 'S' is the scrambling matrix to mask the structure of 'G' and 'P' is the permutation matrix to disguise the arrangement of the code.

ii) Public key generation: the public key G′ is computed as shown in (11).

$$G' = SGP \tag{11}$$

Because ‘G’ is circulant, it requires much less storage space. G′is published as a public key, while (G, S, P) are kept private.

4.2. Encryption phase

To encrypt a message m using the public key G′ generated in the key generation phase, ‘m’ is represented as a binary vector of length ‘k’. The encoded message ‘c’ is computed by multiplying the plain message m with the public key G′ and adding a random error vector ‘e’ of weight ‘t’ with exactly ‘t’ random bits set to 1 as shown in (12).

$$c = mG' + e \tag{12}$$

The error vector e complicates the decoding process without access to the private key, thus safeguarding the ciphertext's security.

4.3. Transmit the ciphertext

The final encrypted output, denoted as 'c' is sent from the sender to the receiver over the communication channel. This ciphertext 'c' now contains the original message fully encoded through the encryption algorithm, combined with a deliberately added random error vector for enhanced security. This transmission step completes the encryption phase, ensuring the message remains protected until proper decryption with the shared key occurs at the receiver's end.

4.4. Decryption phase

In this phase, the primary key (G, S, P) is used to decrypt the ciphertext ‘c’. The first step in this phase is to undo the permutation applied during the encryption by computing ‘cP^{-1}’ as shown in (13).

$$c' = cP^{-1} = (mG' + e)\,P^{-1} = mSG + eP^{-1} \tag{13}$$

After removing the permutation, the scrambling matrix is inverted by multiplying c' by S^{-1} as shown in (14).

$$S^{-1}c' = S^{-1}(mSG + eP^{-1}) = mG + eP^{-1}S^{-1} \tag{14}$$

The step yields a scrambled codeword with minor error, which can be resolved during error correction phase.

4.5. Error correction

To correct errors in the scrambled codeword, the error-correcting algorithm for Goppa code associated with ‘G’ is used to decode ‘mG’ and rectify any error introduced by ‘e’. The retrieved ‘m’ is decoded residual errors are removed from the codeword. The error-correcting algorithm consists of the following steps.

i) Syndrome calculation: in this stage, the syndrome is determined to detect the presence and location of errors. The syndrome s offers essential information regarding the positions of the errors and is calculated as shown in (15).

$$s = cH^T \tag{15}$$

Here, H represents the parity-check matrix related to the Goppa code, and H^T is its transpose. $s=eH^T$ because $mG'^{H^T} = 0$ if $s = 0$, then no errors are present and if $s \neq 0$, it indicates the presence of error.

ii) Error locator polynomial calculator: in this phase, the error location is determined by calculating the error locator polynomial σ(x) using the syndrome computed in the syndrome calculation phase. The error locator polynomial helps identify the error locations, which is defined as shown in (16).

$$\sigma(x) = \prod_{i=1}^{t}(1 - xX_i) \tag{16}$$

Where X_i are the locations of the errors in the received vector. To determine the error locator polynomial σ(x), we use a Patterson syndrome-based decoding algorithm specifically designed for Goppa codes. For example, consider a simple scenario with two errors located at position X_1 and X_2, the error locator polynomial would be represented as shown in (17).

$$\sigma(x) = (1 - xX_1)(1 - xX_2) = 1 - (X_1 + X_2)x + X_1X_2x^2 \tag{17}$$

The coefficients of σ(x) can be determined from the syndrome vector 's'.

iii) Solving the error locator polynomial: once the error locator polynomial $\sigma(x)$ is obtained, the next step is to solve it to identify the error positions. Finding the roots of $\sigma(x) = 0$ reveals the locations X_i of the errors. These roots can be found through different algebraic methods tailored to the finite field utilized by the Goppa code. For example, $if\ \sigma(x) = 1 - xX1$ for a single error at position X_1, solving $\sigma(x) = 0$ immediately gives $x = X_1$.

iv) Calculating the error magnitude: after pinpointing error positions, error magnitudes can be determined. In Goppa codes, errors are generally binary (0 or 1), meaning the error vector e has non-zero values only at the specified error locations. The error vector e is constructed by setting the identified error position as 1. When multiple errors are present, each identified position in the vector is assigned a value of 1, with all other positions left as 0.

v) Correcting the errors and retrieving the original message: in this phase, the errors in the received ciphertext 'c' are corrected using the identified error vector 'e' as shown in (18).

$$c - e = mG' \tag{18}$$

This produces the codeword 'mG', which allows us to recover the original message 'm' by applying standard decoding methods used for linear codes.

4.6. Security analysis of the McEliece cryptosystem

An analysis of the McEliece cryptosystem using circulant matrices evaluates its resilience against various attacks, and more specifically, those which are enabled by properties of circulant matrices. Although improving storage efficiency, there are particular difficulties introduced by the use of circulant matrices. The McEliece cryptosystem, being a standard approach, takes advantage of the difficulty of randomly decoding linear codes.

More specifically, for a randomly selected generator matrix 'G', the task of randomly linear code decoding (decoding a randomly linear code, namely finding the initial message and the error added) without the private key is difficult. Goppa codes are chosen due to their improved error correction and resilience to efficient decoding algorithms and, more specifically, to those introduced by quantum threats. In the McEliece cryptosystem, security against potential attacks is achieved by utilizing the arrangement of Goppa code and two private transformations: firstly, by applying an invertible random matrix S for disturbing the initial message, and secondly by utilizing a permutation matrix P for randomly rearranging code positions. Adopting circulant matrices in the McEliece cryptosystem alters the public key G′, requiring a careful assessment of any vulnerabilities related to circulant matrix characteristics.

4.7. Security of the circulant matrix based McEliece crypto system

First of all, the use of circulant matrices helps to minimize the size of the key. It also imposes a pattern on the generator matrix that might affect security. In this section, we examine the primary types of attacks in detail, focusing particularly on how the utilization of a circulant matrix influences them.

4.7.1. Structural attack

This type of attack tries to find patterns in the public key G′ to figure out the private key. Since a circulant matrix G has a repeating, circular structure, an attacker might use this to try and rebuild the matrix. To stop this, a random permutation matrix is used to mix up the circular pattern of G, making it hard to see the structure. Also, another random matrix 'S' is used to mix up each row of the generator matrix G, hiding the circulant pattern even more. As a result, the public key G′ = SGP doesn't show the circulant nature of G, making this type of attack less effective.

4.7.2. Known plaintext attack

In a known-plaintext attack, an adversary may obtain pairs of plaintexts and ciphertext messages and try to utilize this data to retrieve the private key. For example, let's assume the attacker possesses the message m and its corresponding ciphertext 'c' is as shown in (19).

$$c = mG' + e \tag{19}$$

Where 'e' is an error vector of a known weight 't'. If an attacker gathers enough pairs (m, c), they could attempt to solve for G′. However, since G prime equals SGP, they still need to separate out 'S' and 'P', which is hard to do because matrix operations are complex and there are extra errors. The security comes from how hard it is to decode a linear code and find the exact error vector 'e' without knowing the private key matrices 'S' and 'P'.

4.7.3. Decoding attack

A decoding attack tries to get the original message m by solving the equation $c = mG' + e$ directly. In this process, both m and e need to be found when G' and c are known. The problem is hard because decoding a random linear code is an NP-hard task, which is why McEliece cryptosystem is secure. Even though using a circulant matrix for G might make its structure easier to guess, the matrices 'S' and 'P'mix up the structure, hiding it from attackers. The Stern algorithm and other information-set decoding methods are among the best ways to try and solve this problem. However, these methods are not practical for large code sizes like n =2,048 without knowing private key matrices 'S' and 'P'. The code parameters n and t are chosen so that even the best decoding methods would need too much computing power, even for quantum computers.

4.7.4. Quantum attack

Quantum computers can solve certain math problems much faster than regular computers, sometimes thousands or millions of times quicker. A prominent example is Shor's algorithm, which efficiently addresses the integer factorization problem, rendering RSA and ECC susceptible to quantum attacks. However, decoding random linear codes (the foundation of the McEliece cryptosystem) remains challenging even for quantum computers. Grover's algorithm, known for accelerating brute-force search, is not particularly effective in this context, as the decoding problem does not easily allow for brute-force approaches. In the McEliece cryptosystem, the decoding problem remains difficult because of the vast number of possible error vectors e, which Grover's algorithm alone cannot efficiently reduce.

4.7.5. Dual-code attack

In dual-code attacks, an adversary tries to leverage information from the dual code of the public code, which consists of vectors orthogonal to all codewords in G'. With circulant matrices, the structure of the dual code may be more predictable. The scrambling provided by S and P preserves the randomness of the public code G' and its dual, ensuring that dual-code attacks are no more effective than they are against the traditional McEliece cryptosystem.

5. PERFORMANCE COMPARISON OF TRADITIONAL MCELIECE AND THE CIRCULANT MATRIX-BASED MCELIECE

The performance evaluation of the McEliece cryptosystem utilizing circulant matrices versus the traditional McEliece cryptosystem centers on three key factors: key size, encryption and decryption speed, and security level is shown in Table 1. The McEliece cryptosystem achieves significant advantages over conventional public key cryptography in both key size and encryption speed by implementing circulant matrices, making it very practical. The circulant matrix structure also introduces minor vulnerability to some attack types; however, using sufficient scrambling methods along with proper parameter selection allows for the security of the system to remain intact. Thus, it provides a good balance between security and performance, useful for applications where storage and computational resources need to be minimal, for example, internet of things (IoT) devices and mobile Apps.

Table 1. Comparison of traditional McEliece and the circulant matrix-based McEliece

Metric	Traditional McEliece	Circulant matrix-based McEliece	Improvement factor
Public key size	~256 KB	~256 bytes	~1,000x reduction
Encryption speed	O(k×n)	O(nlogn)	Faster encryption with FFT
Decryption speed	Comparable	Comparable	Similar
Security level	Very strong	Strong, slight theoretical risk if unscrambled	Practically comparable

6. CONCLUSION

This is a paper describing an alternative implementation of the McEliece cryptographic algorithm that utilizes circulant matrix representations. One of the weaknesses associated with using this type of system is that it often requires very large, complex key sizes to provide high levels of security. The authors of this paper discuss how various properties of circulant matrices allow for the development of smaller key size while still providing adequate protection for messages sent via secure channels. By decreasing the key sizes associated with the McEliece cryptographic algorithm, the authors believe their work will allow for improved adoption of the algorithm in contemporary digital devices, including those connected to the IoT, as well as mobile devices using wireless networks. Although concerns regarding weaknesses in circulant structures persist, the use of private permutations and scrambling matrices minimizes these risks. This offers the security of the system against both regular and quantum attacks. Future research could improve this method

by choosing better parameters and testing it in real-world situations. Given the rising threats posed by quantum computing, continued exploration of structured but secure cryptographic frameworks is essential to ensure long-term data security.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Ravikumar Inakoti	✓	✓	✓	✓	✓	✓		✓	✓	✓			✓	
James Stephen Meka		✓				✓		✓	✓	✓	✓	✓		
Padala Venkata Gopala		✓				✓		✓	✓	✓	✓	✓		
Durga Prasad Reddy														

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

The authors confirm that data supporting the findings of this study are available within the article.

REFERENCES

[1] M. L. -García and E. C. -Navarro, "Post-quantum authentication framework based on iris recognition and homomorphic encryption," *IEEE Access*, vol. 13, pp. 155015–155030, 2025, doi: 10.1109/ACCESS.2025.3605676.
[2] E. Bindal and A. K. Singh, "Secure and compact: a new variant of McEliece cryptosystem," *IEEE Access*, vol. 12, pp. 35586–35596, 2024, doi: 10.1109/ACCESS.2024.3373314.
[3] K. Iwamura and A. A. A. M. Kamal, "Secure user authentication with information theoretic security using secret sharing-based secure computation," *IEEE Access*, vol. 13, pp. 9015–9031, 2025, doi: 10.1109/ACCESS.2025.3526632.
[4] H. A. Sharath, J. Vrindavanam, S. Dana, and S. N. Prasad, "Quantum-resilient cryptography: a survey on classical and quantum algorithms," *IEEE Access*, vol. 13, pp. 172854–172877, 2025, doi: 10.1109/ACCESS.2025.3612982.
[5] O. Alibrahim, "Unveiling Samsung quantum Galaxy: securing smartphones with quantum and post-quantum cryptography," *IEEE Access*, vol. 13, pp. 73202–73218, 2025, doi: 10.1109/ACCESS.2025.3563826.
[6] Z. Z. Sun *et al.*, "Quantum blockchain relying on quantum secure direct communication network," *IEEE Internet of Things Journal*, vol. 12, no. 10, pp. 14375–14385, 2025, doi: 10.1109/JIOT.2025.3526443.
[7] J. O. D. Moral, A. D. iOlius, G. Vidal, P. M. Crespo, and J. E. Martinez, "Cybersecurity in critical infrastructures: a post-quantum cryptography perspective," *IEEE Internet of Things Journal*, vol. 11, no. 18, pp. 30217–30244, 2024, doi: 10.1109/JIOT.2024.3410702.
[8] E. Fathalla and M. Azab, "Beyond classical cryptography: a systematic review of post-quantum hash-based signature schemes, security, and optimizations," *IEEE Access*, vol. 12, pp. 175969–175987, 2024, doi: 10.1109/ACCESS.2024.3485602.
[9] K. Wang, J. Dong, S. Wang, Z. Yuan, L. Sha, and F. Xiao, "RSAKA-VDT: designing reliable and provably secure authenticated key agreement scheme for vehicular digital twin networks," *IEEE Transactions on Vehicular Technology*, vol. 74, no. 8, pp. 12330–12346, 2025, doi: 10.1109/TVT.2025.3552481.
[10] X. Ren *et al.*, "Building resilient Web 3.0 infrastructure with quantum information technologies and blockchain: an ambilateral view," *Proceedings of the IEEE*, vol. 112, no. 11, pp. 1686–1715, 2024, doi: 10.1109/JPROC.2024.3520803.
[11] K. S. Shim, B. Kim, and W. Lee, "Research on quantum key, distribution key and post-quantum cryptography key applied protocols for data science and web security," *Journal of Web Engineering*, vol. 23, no. 6, pp. 813–830, 2024, doi: 10.13052/jwe1540-9589.2365.
[12] B. Choudhury, A. Hota, M. Karmakar, S. Saha, A. Nag, and S. Nandi, "A comprehensive survey on pre versus post quantum security schemes for 5G-enabled IoT applications," *IEEE Access*, vol. 13, pp. 159305–159333, 2025, doi: 10.1109/ACCESS.2025.3608623.
[13] S. Bajrić, "Enabling secure and trustworthy quantum networks: current state-of-the-art, key challenges, and potential solutions," *IEEE Access*, vol. 11, pp. 128801–128809, 2023, doi: 10.1109/ACCESS.2023.3333020.
[14] J. Zhang, F. Zhang, and X. Huang, "Theory and applications of sequentially threshold public-key cryptography: practical private key safeguarding and secure use for individual users," *IEEE Transactions on Information Forensics and Security*, vol. 20, pp. 3220–3233, 2025, doi: 10.1109/TIFS.2025.3552202.
[15] H. Wen *et al.*, "Secure optical image communication using double random transformation and memristive chaos," *IEEE Photonics Journal*, vol. 15, no. 1, pp. 1–11, 2023, doi: 10.1109/JPHOT.2022.3233129.

[16] M. El-Hadedy, A. Abelian, K. Lee, B. N. Cheng, and W.-M. Hwu, "ANUBIS: hybrid FPAA-FPGA architecture for entropy-based true random number generation in secure UAV communication," *IEEE Embedded Systems Letters*, vol. 17, no. 3, pp. 164–167, 2025, doi: 10.1109/LES.2024.3510365.
[17] M. A. Khan *et al.*, "An improvised certificate-based proxy signature using hyperelliptic curve cryptography for secure UAV communications," *IEEE Transactions on Intelligent Transportation Systems*, vol. 26, no. 4, pp. 5264–5275, 2025, doi: 10.1109/TITS.2024.3524575.
[18] A. Giorgetti *et al.*, "Generalized quantum-assisted digital signature service in an SDN-controlled quantum-integrated optical network," *Journal of Optical Communications and Networking*, vol. 17, no. 2, pp. A155--A164, 2025, doi: 10.1364/JOCN.534089.
[19] P. K. Maduni, I. Byun, J. Seo, and K. Ko, "Hybrid quantum-safe cryptographic scheme with secure key exchange and signature scheme," *IEEE Access*, vol. 13, pp. 147650–147665, 2025, doi: 10.1109/ACCESS.2025.3600068.
[20] Y. Hariprasad, S. S. Iyengar, and N. K. Chaudhary, "Securing the future: advanced encryption for quantum-safe video transmission," *IEEE Transactions on Consumer Electronics*, vol. 71, no. 1, pp. 140–153, 2025, doi: 10.1109/TCE.2024.3473542.
[21] V. Puneyani and K. V Bhat, "Quantum-resistant blockchain protocols for secure transactions," *IEEE Access*, vol. 13, pp. 108984–108991, 2025, doi: 10.1109/ACCESS.2025.3581955.
[22] K. B. A. Kumar, L. S. Mohith, K. Jain, P. Krishnan, N. Venkatachalam, and R. Buyya, "Post-quantum cryptography-based multimedia encryption communication scheme in IoT consumer electronics," *IEEE Transactions on Consumer Electronics*, vol. 71, no. 2, pp. 4995–5006, 2025, doi: 10.1109/TCE.2025.3572949.
[23] S. Hussain, A. Tufail, H. A. A. G. Naim, M. A. Khan, and G. Barb, "Evaluation of computationally efficient identity-based proxy signatures," *IEEE Open Journal of the Computer Society*, vol. 6, pp. 846–861, 2025, doi: 10.1109/OJCS.2025.3573638.
[24] A. Sharma and S. Rani, "Post-quantum cryptography (PQC) for IoT-consumer electronics devices integrated with deep learning," *IEEE Transactions on Consumer Electronics*, vol. 71, no. 2, pp. 4925–4933, 2025, doi: 10.1109/TCE.2025.3569904.
[25] S. L. Birhanu, M. Ghadimi, Y. Hai, P. Seeling, R. Bassoli, and F. H. P. Fitzek, "A survey of continuous variable quantum key distribution in quantum communication," *IEEE Access*, vol. 13, pp. 166027–166061, 2025, doi: 10.1109/ACCESS.2025.3610519.
[26] K. Sutradhar, "A quantum cryptographic protocol for secure vehicular communication," *IEEE Transactions on Intelligent Transportation Systems*, vol. 25, no. 5, pp. 3513–3522, 2024, doi: 10.1109/TITS.2023.3322728.
[27] R. Zhang, L. Zhang, K.-K. R. Choo, and T. Chen, "Dynamic authenticated asymmetric group key agreement with sender non-repudiation and privacy for group-oriented applications," *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 1, pp. 492–505, 2023, doi: 10.1109/TDSC.2021.3138445.
[28] V. Kumar *et al.*, "Design of secure and efficient framework for vehicular digital twin networks using ECC," *IEEE Access*, vol. 12, pp. 194352–194366, 2024, doi: 10.1109/ACCESS.2024.3511654.
[29] D. S. C. Putranto, R. W. Wardhani, H. T. Larasati, and H. Kim, "Space and time-efficient quantum multiplier in post quantum cryptography era," *IEEE Access*, vol. 11, pp. 21848–21862, 2023, doi: 10.1109/ACCESS.2023.3252504.

BIOGRAPHIES OF AUTHORS

Ravikumar Inakoti is pursuing his Ph.D. in the Department of Computer Science and Systems Engineering at Andhra University, Visakhapatnam, and completed his M.Tech. in 2015 from Pydah College of Engineering. He worked as an assistant professor in the Department of Computer Science and Engineering at Welfare Institute of Technology and Management, Visakhapatnam, India. His research interests include wireless sensor networks, big data analytics, computer networks, network security, and MANETs. He can be contacted at email: ravirk1228@gmail.com.

James Stephen Meka is a respected academician, currently serving as the national chair professor at the Dr. B.R. Ambedkar Chair, Andhra University, under the Ministry of Social Justice and Empowerment, Government of India. Academically, he holds a Ph.D. in Computer Science and Systems Engineering from Andhra University, along with multiple Master's degrees in MCA and M.Phil. (CS), M.Div., M.B.A., and M.Tech. (CST). He can be contacted at email: jamesstephenm@gmail.com.

Padala Venkata Gopala Durga Prasad Reddy is a senior professor in the Department of Computer Science and Systems Engineering, Andhra University, Visakhapatnam, India, where he previously worked as a Vice-Chancellor. He produced more than 60 Ph.D's and published more than 250 quality research articles. He owns more than 15 patents and 3 copyrights. His research interests include machine learning, artificial intelligence, IoT, and wireless networks. He can be contacted at email: prasadreddy.vizag@gmail.com.