

Mathematical foundations of code-based cryptography for quantum-resistant systems

Khursheed Alam [‡]

Department of Mathematics & Data Science

The A. H. Siddiqi Centre for Advanced

Research in Applied Mathematics & Physics (CARAMP)

Sharda University

Greater Noida 201310

Uttar Pradesh

India

Supriya Maheshwari [†]

Department of Mathematics

Noida Institute of Engineering and Technology

Greater Noida 201310

Uttar Pradesh

India

A. K. Singh [§]

Department of Mathematics

RBS Engineering Technical Campus

Khandari

Agra 282002

Uttar Pradesh

India

Masood Alam ^{*}

Department of Mathematics & Information Technology

Centre for Preparatory Studies

Sultan Qaboos University

Muscat 123

Sultanate of Oman

[‡] E-mail: khursheed.alam@sharda.ac.in

[†] E-mail: supriya.maheshwari@niet.co.in

[§] E-mail: aksinghrbs@yahoo.com

^{*} E-mail: malam@squ.edu.om (Corresponding Author)

Abstract

This paper looks at the theoretical bases of code-based cryptographic techniques, specifically looking to determine if they can be used as a method to develop new post-quantum resistant systems. To do this we look at linear block codes, Hamming distance, and Goppa codes as the base in which to create secure communications. These are then used to build the McEliece and Niederreiter cryptosystems, where we illustrate the dependence on the computational difficulty of solving the Syndrome Decoding Problem (SDP), and the General Decoding Problem (GDP). Using both analytical methods, and by providing examples using numbers, we demonstrate how an intentional introduction of errors, and their subsequent correction, form the basis of encrypting information, and decrypting information. This is done to ensure that confidentiality, and robustness are provided. We also perform a comparison of these systems with RSA and ECC, and demonstrate that while the classical systems are compromised by Shor's Algorithm, the code-based systems have exponential hardness. Figures and Tables help to visually understand the complexity analysis of these systems, the flow of encryption, and the process of error correction. Our results support our conclusion that McEliece and Niederreiter are viable candidate post-quantum cryptographic systems, as they are able to provide efficient, reliable, and provably secure alternatives to current systems.

Subject Classification: 94A60.

Keywords: Niederreiter cryptosystem, Goppa codes, Syndrome decoding, General decoding problem, Quantum resistance, Error correction codes.

1. Introduction

The emergence of quantum computers will create major challenges to the current state-of-art classical cryptographic schemes (RSA, ECC) based on Shor's quantum algorithms to factor and find discrete logarithms that are much faster than any classical algorithm. The fear that a quantum computer can break all classical cryptography schemes has stimulated the research of post-quantum cryptography and new cryptographic primitives based on computational problems that cannot be solved by a quantum machine with reasonable resources. Among the candidates of new cryptographic primitives we find the code-based cryptography which are based on the inherent hardness of decoding random linear codes. Code-based cryptography transforms an error correcting code traditionally used for reliable data transmission into a basis for secure data encryption. The goal is achieved through the intentional insertion of errors during the encoding process and using the low complexity of decoding a well-defined class of structured codes (Goppa codes), for example the schemes McEliece and Niederreiter, to ensure robustness and confidentiality of the encrypted message. In contrast to other number theoretic approaches, their security relies on decoding problems in NP, and therefore they remain resistant to both classical and quantum attacks.

The first non-number-theory based public-key cryptosystem was created by McEliece [8]. McEliece used algebraic coding theory (binary Goppa codes)

to create a resistant-to-all-known-attacks encryption system. The scheme depends on the difficulty of solving the syndrome-decoding-problem which is NP-complete. Although it has a very large public key size, the McEliece scheme is currently considered to be the best candidate to replace RSA in quantum-resistant cryptography. In addition to exploring post-quantum cryptography on FPGAs using isogeny of elliptic curves, Koziel et al. [6] demonstrated the hardware feasibility of cryptographic primitives beyond code-based schemes. Although their work does not directly relate to code-based cryptography, it is important because it demonstrates the hardware optimization requirements to implement PQC and thus provides useful comparisons with McEliece-type systems. Fritzmann, Sigl, and Sepúlveda [2] focused on developing tightly-coupled hardware accelerators to maximize PQC performance. Since they did not develop their accelerators for code-based cryptography, this paper illustrates how the design of processors and/or hardware accelerators can help alleviate the high-performance costs associated with the large key-sizes and computational requirements of PQC algorithms such as McEliece. Chen and Chou [1] implemented the Classic McEliece scheme on the ARM Cortex-M4, which is a very limited microcontroller platform. This study showed that even though the large key sizes of McEliece are inefficient from a performance standpoint, it can still be effectively deployed on resource-constrained embedded systems, such as those found in Internet-of-things and low-power/low-cost devices. Their study focused on optimizing performance and selecting parameters securely. Zhao et al. [10] proposed an optimized hardware platform that was both smaller and much faster than the traditional CRYSTALS-Dilithium PQC system. In spite of not being code-based, their work shows the impact of optimizing code-based systems for use in PQC systems by demonstrating how to dramatically improve all PQC systems through the use of hardware optimization techniques. The improvements shown in this paper provide a benchmark for comparing the efficiency of McEliece and Niederreiter with other code-based PQC systems. Koufopoulou et al. [5] evaluated the security and reliability of countermeasures used to protect code-based PQC systems from fault injection attacks and reliability testing. Gao et al. [3] have developed graph neural networks (GNNs) to predict Quality of Results (QoR) in High-Level Synthesis (HLS) workflows. Although this paper has a design automation focus, the results are very important for the development of PQC systems because they allow for better models of the performance of cryptographic circuits that may implement McEliece-like systems. Ghashghaei et al. [4] demonstrated how PQC systems (including code-based systems) could be included as part of a secure communication framework along with QKD and illustrated the potential of post-quantum systems to play a significant role in the implementation of future secure networks. Liu et al. [7] developed hardware optimizations of the MPCITH and Picnic3 signature schemes that were part of the PQC landscape. These may be viewed as non-code based; however, their findings demonstrate the challenges in optimizing hardware common to all PQC families, therefore, research on improving the performance of McEliece-based encryption is very

important. Redhu and Narwal [9] conducted an exploratory study of the development and growth of code-based cryptography. The study was comprised of both a bibliometric and research trend analysis with respect to where code-based cryptography fits into the larger PQC research community. The study was useful for providing insight into the history of research concerning McEliece, Niederreiter and other related codes and how they continue to be important components of the PQC family of algorithms since their introduction in 1978. The study also demonstrated the focus of the research effort has shifted from theoretical constructs to developing efficient solutions that can be deployed.

2. Mathematical Background:

2.1 Linear Block Codes

Linear block codes form the mathematical foundation of code-based cryptography and error correction [8]. An $[n, k, d]$ code is a block code of length n , dimension k , and minimum Hamming distance d . Such a code encodes k -symbol messages into n -symbol codewords over a finite field F_q , where the redundancy allows error detection and correction. The generator matrix G of size $k \times n$ maps a message vector $u \in F_q^k$ into a codeword $c = uG$. The entire code can thus be written as

$$C = \{uG: u \in F_q^k\} \quad (1)$$

Complementarily, the parity-check matrix H of size $(n - k) \times n$ characterizes the same code by the orthogonality condition:

$$H \cdot c^T = 0 \quad (2)$$

ensuring that every valid codeword lies in the null space of H . Together, G and H provide algebraic tools to encode messages efficiently and to detect and correct transmission errors by computing syndromes.

2.2 Hamming Distance & Error Correction

$$d(x, y) = |\{i: x_i \neq y_i\}| \quad (3)$$

$$\text{Error correction capability: } t = \left\lfloor \frac{(d-1)}{2} \right\rfloor \quad (4)$$

2.3. Goppa Codes

Goppa codes are a special family of linear error-correcting codes that play a central role in code-based cryptography due to their strong error-correcting capability and resistance against structural attacks [8, 9]. They are defined using two algebraic ingredients: an irreducible polynomial $g(x)$ of degree t over F_2 , and a support set $L = \{L_1, L_2, \dots, L_n\}$ of distinct elements from F_{2^m} such that $g(L_i) \neq 0$ for all i . The binary Goppa code constructed from these parameters is given by

$$C(L, g) = \left\{ c \in F_2^n : \sum_{i=1}^n \frac{c_i}{x - L_i} \equiv 0 \pmod{g(x)} \right\} \quad (5)$$

This definition means that a codeword $\mathbf{c}$ is valid if the rational function formed by combining its components with the support set reduces to zero modulo $g(x)$. Goppa codes are linear, with parameters $[n, k \geq n - mt, d \geq 2t + 1]$, and are capable of correcting up to t errors. Their algebraic structure not only allows efficient decoding (via Patterson's algorithm) but also makes them excellent candidates for post-quantum cryptography, as exploited in the McEliece cryptosystem.

3. Code-Based Cryptography

3.1 McEliece Cryptosystem

Key generation: $G' = SGP$ (6)

where S is invertible, P is a permutation.

Encryption: $c = mG' + e$ (7)

Decryption: decode with secret structure.

3.2 Niederreiter Cryptosystem

The Niederreiter cryptosystem is a code-based public-key encryption scheme closely related to McEliece but formulated in terms of parity-check matrices rather than generator matrices. Instead of publishing a scrambled generator matrix, the public key in Niederreiter is a scrambled and permuted parity-check matrix H' derived from a secret code (often a binary Goppa code). To encrypt, a plaintext is represented as a binary error vector e of fixed Hamming weight, and the ciphertext is computed as the syndrome

$$c = H' \cdot e^t \quad (8)$$

Decryption proceeds by applying the secret permutation and scrambling inverses to recover the syndrome with respect to the original code's parity-check matrix H , after which efficient decoding algorithms (e.g., Patterson's algorithm) can recover the error vector e , which represents the plaintext. Compared with McEliece, the Niederreiter scheme generally produces smaller public keys and ciphertexts, while relying on the same hard problem: decoding a general linear code. Its equivalence in security but improved efficiency has made Niederreiter one of the main alternatives considered in post-quantum cryptography.

3.3 Security Assumptions

Hardness of Syndrome Decoding Problem (SDP) and General Decoding Problem (GDP).

The security of code-based cryptosystems such as McEliece and Niederreiter relies on the computational hardness of decoding problems in coding theory. The first key assumption is the Syndrome Decoding Problem (SDP): given a parity-check matrix $H \in \mathbb{F}_q^{(n-k) \times n}$, a syndrome $s \in \mathbb{F}_q^{(n-k)}$, and an integer t , the task is to find a vector $e \in \mathbb{F}_q^n$ Hamming weight at most t such that

$$H \cdot e^t = s \quad (9)$$

This problem is known to be NP-complete in the worst case, even over the binary field, making it resistant to efficient classical and quantum algorithms. A more general formulation is the General Decoding Problem (GDP): given a generator matrix G , a received word y , and an integer t , the goal is to find a codeword $c = uG$ within Hamming distance t of y . Both SDP and GDP encapsulate the challenge of distinguishing structured codes (like Goppa codes) from random linear codes and correcting errors without knowledge of secret structure. While advances such as information set decoding (ISD) provide the best-known attacks, their exponential complexity ensures that, with sufficiently large parameters, code-based cryptosystems remain secure even against quantum adversaries.

4. Quantum-Resistance Analysis

The quantum-resistance of code-based cryptography stems from the fact that the underlying decoding problems (SDP and GDP) remain intractable even in the presence of quantum algorithms [8, 9]. Unlike RSA and elliptic-curve cryptography (ECC), which are efficiently broken by Shor's algorithm through polynomial-time factoring and discrete logarithm solutions, no analogous quantum algorithm is known for syndrome or general decoding. In fact, both problems are provably NP-complete, and their hardness persists regardless of quantum speedups. The best classical and quantum attacks rely on Information Set Decoding (ISD), a family of algorithms that attempt to guess a set of positions free of errors and decode accordingly. While quantum variants of ISD achieve slight improvements (mainly quadratic speedups similar to Grover's algorithm), the overall complexity remains exponential in code length. Lattice-based methods do not offer a significant advantage in terms of the efficient solution to SDP/GDP. Consequently, using appropriately-chosen parameters, code-based schemes (like McEliece and Niederreiter) still possess robust security assurances against both classical and quantum adversaries, so are therefore the most likely candidate for post-quantum cryptographic applications.

A comparative summary of the security characteristics, key sizes, ciphertext expansion, and quantum resistance of McEliece, Niederreiter, RSA, and ECC is presented in Table 1.

Table 1
Comparative Security and Efficiency of Classical and Code-Based Cryptosystems

Scheme	Key Size	Ciphertext Expansion	Quantum Security Basis
McEliece	Large	Moderate	Decoding NP-complete
Niederreiter	Smaller	Moderate	Same as above
RSA	Small	Small	Broken by Shor
ECC	Very small	Small	Broken by Shor

5. Numerical Illustrations

Let us take McEliece example with the binary $[7, 4]$ Hamming code.

5.1. *Encryption:*

$$\text{Generator Matrix } G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \quad (1)$$

Scrambling matrix S (invertible 4×4):

$$S = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix} \quad (2)$$

Permutation Matrix (Permutes Columns)

$$P = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \quad (3)$$

Public Generator Matrix

$$G' = SGP = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \end{bmatrix} \quad (4)$$

$$\text{Message: } m = [1, 0, 1, 1] \quad (5)$$

$$\text{Error vector: } e = [0, 0, 0, 0, 0, 1, 0] \quad (6)$$

$$\text{Ciphertext: } c = mG' + e \pmod{2} = [1, 0, 1, 1, 0, 1, 1] \quad (7)$$

$$\text{So the encrypted message is: } c = [1, 0, 1, 1, 0, 1, 1] \quad (8)$$

5.2. *Decryption:***(i) Recall Parameters:**

$$\text{Ciphertext received: } c = [1, 0, 1, 1, 0, 1, 1] \quad (9)$$

Secret matrices:

 S (scrambling) P (permutation)

Original Hamming code structure.

(ii) Remove Permutation: We know ciphertext is:

$$c = mG' + e, G' = SGP \quad (10)$$

$$\text{First, undo permutation with } P^{-1}: c' = cP^{-1} \quad (11)$$

This brings the codeword back into the structure of the underlying Hamming code.

- (iii) **Syndrome Calculation:** Define **parity-check matrix** H for $[7,4]$ Hamming code:

$$H = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \quad (12)$$

$$\text{Now compute the syndrome: } s = Hc'^T \pmod{2} \quad (13)$$

If $s = [0,0,0]$: no error.

Otherwise, s points to the error location.

- (iv) **Error Correction:** Suppose $s = [0,1,1]$.

This corresponds to a lookup table entry that identifies bit 6 as erroneous.

$$\text{Correct the error: } c'' = c' + e_{\text{pos}} \quad (14)$$

- (v) **Recover Message:** Now c'' is a valid Hamming codeword:

$$\text{Multiply by } S^{-1} \text{ to remove scrambling: } mG = S^{-1} + c'' \quad (15)$$

Finally, extract the original message bits: $m = [1,0,1,1]$

The decoding process corrects the error and recovers:

- (v) **Result:** The decoding process corrects the error and recovers:

$$m = [1,0,1,1]$$

6. Results and Discussion:

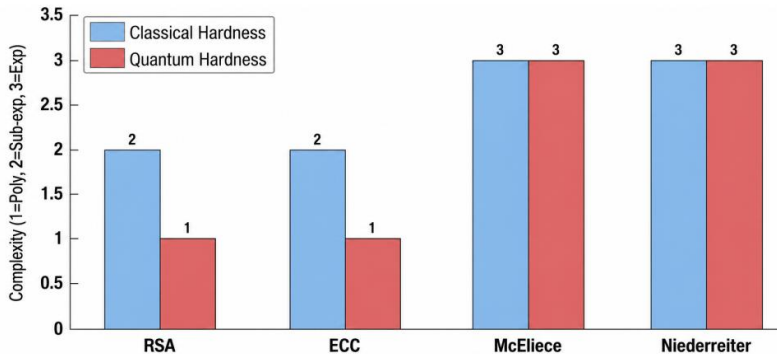


Figure 1
Classical vs Quantum Complexity of Cryptosystems

The Figure 1 compares the computational complexity of breaking major cryptosystems under both classical **and** quantum settings. On the left, RSA and ECC are shown to have sub-exponential classical hardness (blue bars labeled “2”), meaning they are difficult but not intractable for sufficiently large keys; however, under quantum attacks with **Shor’s algorithm**, their complexity drops dramatically to polynomial time (red bars labeled “1”), making them insecure in a post-quantum world. On the right, the McEliece and Niederreiter code-based cryptosystems exhibit exponential hardness (blue bars labeled “3”) under

classical attacks, and importantly, this remains unchanged even with quantum adversaries (red bars also labeled “3”). This illustrates the quantum resilience of code-based systems, highlighting why McEliece and Niederreiter are considered strong candidates for post-quantum cryptography, unlike RSA and ECC which collapse under quantum algorithms.

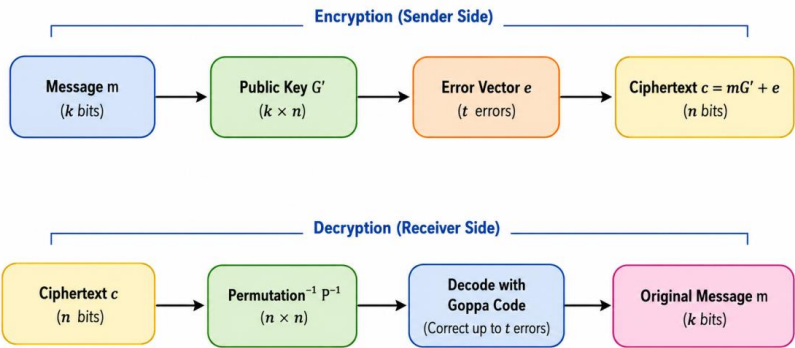


Figure 2
McEliece Encryption / Decryption Block Diagram

As shown in the Figure 2, block diagrams are used to show the encryption and decryption flow of McEliece for the messages. In the top portion of the encryption section, the plaintext message is first encoded by the public generator matrix G' , as an example of a plaintext m . Then a small amount of error e is randomly selected and added to the encoded plaintext message so that the resulting message $c = mG' + e$ represents a scrambled version of the codeword to make it difficult to decrypt without access to the secret key. The bottom row of the decryption portion shows the legitimate decoder, who has been given the private key, applying the inverse permutation P^{-1} to unscramble columns of the scrambled codeword; then he or she will use a fast algorithm for Goppa code decoding to remove the intentionally introduced errors e ; and finally the process of descrambling will yield the original plaintext message m . As illustrated in this diagram, the McEliece scheme achieves post-quantum security through the combination of structured error correcting codes with intended noise to achieve confidentiality.

The Figure 3 displays the basic error detection/ correction steps of Hamming /Goppa codes using a step by step example. The first row is the original valid codeword of a series of bits. An error occurred during transmission at one location shown in the second row, with the erroneous bit identified by the label "Error detected" and the rest of the bits being unaltered. Using the Syndrome Decoding method or the Error-Correction Algorithm (for Hamming Codes), or other methods built into both Hamming and Goppa codes, the system will identify the erroneous bit and correct it. The third row is the corrected codeword, which has been restored back to its original state. In essence, this depicts how Linear Error Correcting Codes are capable of detecting

and correcting errors that occur during data transmission; they allow for the establishment of secure communication systems and provide the mathematical basis for code based encryption methods.

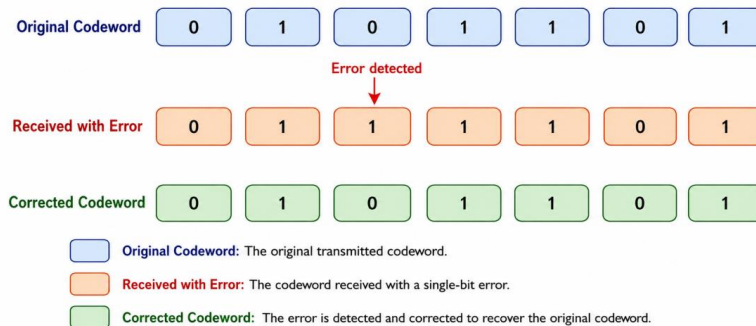


Figure 3
Error Correction in Hamming/Goppa Codes

6. Conclusion

This research demonstrates the long-term viability of code based cryptographic techniques as the foundation for post-quantum security; specifically McEliece and Niederreiter cryptosystems which utilize linear block codes (and Goppa codes) to create an encrypted message with embedded random errors so that the security of the system is based upon the difficulty of solving the SDP and GDP problems. It has been demonstrated through comparative analysis that while RSA and ECC will be insecure when they are subjected to quantum computers, code based ciphers have exponential computational complexity against both quantum and classical attacks. Figures and numerical examples demonstrate the capability of these systems to correct errors, provide workflow examples of the encryption process and their resistance to attack from a quantum computer. While cryptography moves towards the post-quantum era, it can now be demonstrated that code based techniques are not only theoretically sound but also practical and offer scalable and secure solutions to the communication systems of the future.

References

- [1] M.-S. Chen and T. Chou, "Classic McEliece on the ARM Cortex-M4," *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, vol. 2021, no. 3, pp. 125–148 (2021), doi: 10.46586/tches.v2021.i3.125-148.
- [2] T. Fritzmann, G. Sigl, and J. Sepúlveda, "RISQ-V: Tightly coupled RISC-V accelerators for post-quantum cryptography," *IACR Trans.*

- Cryptogr. Hardw. Embed. Syst.*, vol. 2020, no. 4, pp. 239–280 (2020), doi: 10.13154/tches.v2020.i4.239-280.
- [3] M. Gao, J. Zhao, Z. Lin, and M. Guo, “Hierarchical source-to-post-route QoR prediction in high-level synthesis with GNNs,” in *Proc. Design, Automation & Test in Europe Conf. Exhibition (DATE)*, pp. 1–6 (2024), doi: 10.23919/DATE58400.2024.10546555.
- [4] F. R. Ghashghaei, Y. Ahmed, N. Elmrabit, and M. Yousefi, “Enhancing the security of classical communication with post-quantum authenticated-encryption schemes for the quantum key distribution,” *Computers*, vol. 13, no. 7, Art. no. 163 (2024), doi: 10.3390/computers13070163.
- [5] A.-A. Koufopoulou, K. Xevgeni, A. Papadimitriou, M. Psarakis, and D. Hely, “Security and reliability evaluation of countermeasures implemented using high-level synthesis,” in *Proc. IEEE 28th Int. Symp. On-Line Testing and Robust System Design (IOLTS)*, pp. 1–8 (2022), doi: 10.1109/IOLTS56730.2022.9897824.
- [6] B. Kozziel, R. Azarderakhsh, M. Mozaffari Kermani, and D. Jao, “Post-quantum cryptography on FPGA based on isogenies on elliptic curves,” *IEEE Trans. Circuits Syst. I, Reg. Pap.*, vol. 64, no. 1, pp. 86–99 (2017), doi: 10.1109/TCSI.2016.2611561.
- [7] G. Liu, K. Jia, P. Wei, and L. Ju, “High-performance hardware implementation of MPCitH and Picnic3,” *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, vol. 2024, no. 2, pp. 190–214 (2024), doi: 10.46586/tches.v2024.i2.190-214.
- [8] R. J. McEliece, “A public-key cryptosystem based on algebraic coding theory,” *JPL DSN Progress Report*, vol. 42-44, pp. 114–116 (1978).
- [9] R. Redhu and E. Narwal, “An exploratory analysis of the evolution and trends of code-based cryptography,” *J. Discrete Math. Sci. Cryptogr.*, vol. 28, no. 3, pp. 959–972 (2025), doi: 10.47974/JDMSC-2236.
- [10] C. Zhao, N. Zhang, H. Wang, B. Yang, W. Zhu, Z. Li, M. Zhu, S. Yin, S. Wei, and L. Liu, “A compact and high-performance hardware architecture for CRYSTALS-Dilithium,” *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, vol. 2022, no. 1, pp. 270–295 (2022), doi: 10.46586/tches.v2022.i1.270-295.

Received January, 2026