Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 10-C, pp. 4583–4594
DOI : 10.47974/JDMSC-3075

Quantum-resistant cryptographic constructions using discrete structures

Pallavi Vilas Mhaske [†]
Department of Ethical Science and Food Technology
MIT School of Food Technology
MIT Art, Design and Technology University
Pune 412201
Maharashtra
India

Debanjana Prasad *
Department of Biotechnology
Noida International University
Greater Noida 203201
Uttar Pradesh
India

Namrata Somnath Bajare [§]
Department of Computer Engineering
Vishwakarma Institute of Technology
Pune 411037
Maharashtra
India

Rubi Kambo [‡]
Department of Computer Science and Engineering
Rungta College of Engineering and Technology
Rungta International Skills University
Bhilai 490024
Chhattisgarh
India

[†] *E-mail:* pallavi.mhaske@mituniversity.edu.in
* *E-mail:* debanjana.prasad@niu.edu.in (Corresponding Author)
[§] *E-mail:* namrata.bajare@vit.edu
[‡] *E-mail:* rubi.kambo@rungta.org

© Taru Publications

D. Raghavendra Gowda [@]
Department of Computer Science and Engineering
Vardhaman College of Engineering
Shamshabad
Hyderabad 501218
Telangana
India

R. Shanthi [#]
Department of Mathematics
Meenakshi College of Arts and Science
Meenakshi Academy of Higher Education & Research (Deemed to be University)
Chennai 600078
Tamil Nadu
India

Abstract

Conventional cryptographic constructions have to meet the challenge of the quick development of quantum computing, and they require the creation of efficient constructions resistant to quantum attack. In this paper, the authors suggest a hybrid cryptographic model that combines lattice-based hardness assumptions, such as Learning with Errors (LWE) with graph theoretical and combinatorial structures to provide greater security, efficiency and scalability. This framework is a hybrid of lattice trapdoor functions, expander graphs, and discrete optimization methods, aiming to enhance structural robustness against classical and quantum attackers. The performance is compared with the conventional methods of RSA/ECC and lattice and graph-based cryptographic methods. The results reported in this work shows that, the proposed hybrid framework provides the security level of 256 bits and quantum attack resistance as 96.8%, whereas the lattice-based approach provides 82.4%. Moreover, the hybrid construction has the key generation time 21.1ms, encryption time 14.1ms and throughput of 183Mbps. These values represent a decrease of 14.92% for the key generation time, 10.19% for the encryption time and 27.96% for the memory usage when compared to the baseline which is based on lattices. These results indicate that a combination of complementary discrete mathematical models could be a potential way to design efficient, scalable post-quantum cryptographic systems.

Subject Classification: *14G50, 81P94.*

Keywords: *Post-quantum cryptography, Lattice-based cryptography, Discrete structures, Graph theory, LWE, Quantum security.*

[@] *E-mail:* **raghavendrag@outlook.com**
[#] *E-mail:* **shanthir@maher.ac.in**

I. Introduction

The creation of quantum computing poses a serious threat to the widely deployed cryptographic systems, in particular, the integer factorization and discrete logarithm problem-based ones [1, 2]. Algorithms such as Short algorithm can be very successful in breaking classical public-key schemes and the world must change to quantum-resistant cryptography [3, 4]. Of particular interest have been discrete mathematical structures, whose hardness assumptions are much stronger and resistant to quantum attacks [5, 6]. It deals with the design of quantum-resistant cryptographic constructions, using discrete models, including lattice-based problems, including Learning with Errors (LWE) and graph-based models [7, 8]. These constructions are rich complexity assurances, and can be used to construct safe primitives like encryption, digital signatures and key exchange protocols. In addition to this they possess algebraic and combinatory characteristics that allow them to be adaptable to come up with hybrid models that are efficient and secure [9, 10, 11]. The main goal of the work is to come up with a scaled and an efficient cryptographic system that incorporates several discrete systems to enhance the ability to resist the quantum attackers [12].

II. Preliminaries and Mathematical Foundations

This part provides scientific background of lattice-based hardness assumptions, algebraic groups and combinatory to construct quantum-resistant cryptographic systems, which are secure and efficient.

A. *Complexity assumptions and hardness problems (LWE, SVP, etc.)*

This section presents lattice based hardness assumptions, algebraic structure and combinatorics, the theory underlying the construction of secure, efficient and quantum resistant cryptographic constructions.

$$\left|\left|v\right|\right| \leq \gamma(n) * \lambda 1(L) \tag{1}$$

In equation (1) approximate shortest vector is defined; the length of the vectors are factors 7(n) of optimal minimum which can be interpreted to the computational hardness of the assumptions of lattice security.

$$e \sim \chi \approx \sqrt{\left(\frac{1}{(2\pi\sigma^2)}\right) * \exp\left(-\frac{x^2}{(2\sigma^2)}\right)} \tag{2}$$

The model of error distribution (2) relies on the error modelling by a Gaussian error where the probability distribution is an exponential decay of the size, and guarantees the randomness and security of the lattice based cryptography constructions.

$$Adv_{LWE} \leq \sqrt{\left(\Sigma^2_{\{i=1\ to\ m\}(\varepsilon_i)}\right)} \tag{3}$$

Adversarial advantage is confined by (3), and the squared error terms add up, meaning that solving LWE is computationally infeasible as the cumulative error terms become large.

B. *Algebraic and combinatorial properties*

Algebraic and combinatorial designs facilitate effective encoding, transformation, and analysis, contributing to resilience, generation of randomness, and complexity of structure vital to secure cryptographic constructions.

$$F_q = \{0, 1, 2, \dots, q-1\} \tag{4}$$

The definition of a finite field of integers modulo q in equation (4) allows closed arithmetic operations that are important to the construction of secure algebraic cryptographic primitives to be carried out at a comparatively low cost.

$$R_q = \frac{Z_{q[x]}}{(x^n + 1)} \tag{5}$$

The equation is (5) of a polynomial ring modulo xn+1 over integers modulo q, and can be used to perform efficient convolution operations and structured algebraic computations in lattice-based cryptography.

$$||x|| = \sqrt{\left(\Sigma_{\{i=1\ to\ n\}} x_i^2 \right)} \tag{6}$$

Euclidean norm of vector is defined in equation (6) as a measure of magnitude based on the sum of squares of components that are important in the analysis of distances and error bounds in lattice problems.

$$A \in R^{\{n \times n\}}, \lambda_{\max(A)} = \sqrt{\left(\Sigma_{\{i=1\ to\ n\}} \lambda_i^2 \right)} \tag{7}$$

Equation (7) defines the eigenvalue magnitude of adjacency matrices with the largest eigenvalues indicating structural connectivity which determines expansion, robustness and combinatorial complexity in graph-based cryptographic constructions.

III. Problem Formulation

It is a section that sets security requirements against quantum adversaries, where the constraints of efficiency, memory and scalability are satisfied and robust cryptographic constructions are designed to suit real-world post-quantum applications.

A. *Security requirements for quantum-resistant systems*

The quantum resistant systems must be hardened against quantum adversaries, providing confidentiality, integrity and authenticity by provable security, resistance to quantum algorithms and resilience to adaptive attacks. Quantum security, confidentiality, integrity, authenticity, availability requirements are presented in Figure 1.

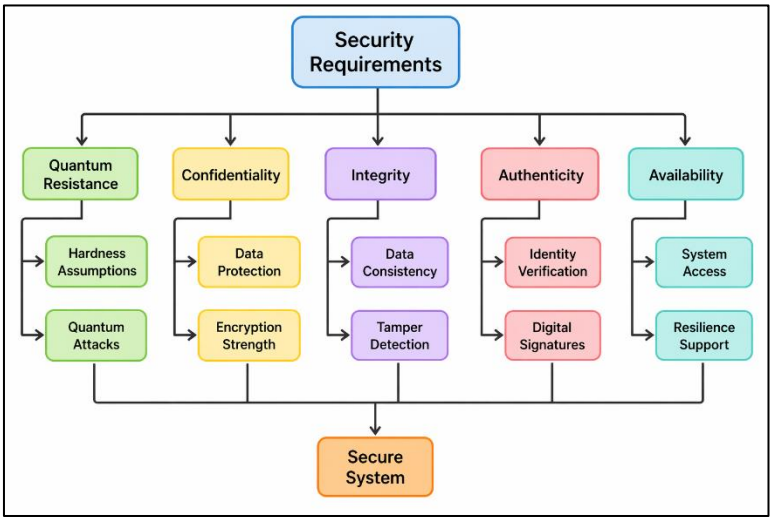


Figure 1

Security Requirements for Quantum-Resistant Cryptographic Systems

Security Parameter Definition

$$\lambda = \sqrt{\left(\Sigma_{\{i=1\ to\ n\}} k_i^2\right)} \tag{8}$$

Security parameter is defined in equation (8) as the aggregated magnitude of key components, overall system strength as a measure of resistance level to a classical and quantum attack.

Confidentiality Condition

$$P(success) \leq \frac{1}{\sqrt{(2^{\lambda})}} \tag{9}$$

Equation (9) is a probability boundary of adversarial success as a negative power of exponential security parameter, meaning that there is negligible information leakage and high confidentiality with computationally powerful quantum adversaries.

Integrity Constraint

$$I(m) = \sqrt{\left(\Sigma^2_{\{i=1\ to\ n\}}\left(H(m_i)\right)\right)} \tag{10}$$

The integrity of messages in equation (10) is determined using hash-based aggregation where any alteration in the message would considerably change the resultant computed value, hence allowing one to detect any tampering or unauthorized alteration.

Authenticity Verification

$$V = \left(\left(Sig(m)\right)^2 + (PK)^2\right)^{\frac{1}{2}} \tag{11}$$

Signature and public key elements are merged with equation (11), which checks authenticity of origin by checking cryptographic relationships, which the message is sent by a legitimate sender and not forged.

Quantum Resistance Measure

$$R_Q = \sqrt{\left(\lambda^2 + \Sigma^2_{\{i=1\ to\ n\}(cost_i)} \right)} \tag{12}$$

The overall quantum resistance is estimated using equation (12) to estimate quantum resistance by integrating both security parameter and computational costs to determine how system resistance to quantum attacks and efficiency and implementation overhead factors.

B. *Constraints: computational efficiency, memory, scalability*

Some of the design constraints are the reduction of computational overhead, optimization of memory usage and scalability in distributed environments but with high security assurance and their practical implementation.

Computational Cost Model

$$C_{total} = \sqrt{\left(\Sigma^2_{\{i=1\ to\ n\}}(T_i) \right)} \tag{13}$$

Equation (13) sums squared execution times of the individual operations, which gives the magnitude of the overall cost of computation, which is useful in assessing the efficiency of cryptographic algorithms and optimizing their implementation.

Time Complexity Representation

$$T(n) = \sqrt{((n \log n)^2 + n^2)} \tag{14}$$

The algorithmic growth model (Equation (14)) is a combination of both logarithmic growth and quadratic growth and is realistic in its complex behaviour and can be used to analyse scalability and performance as input sizes grow.

Scalability Function

$$S(n) = \sqrt{\left(\left(\frac{Throughput}{Latency} \right)^2 \right)} \tag{15}$$

Scalability may be expressed as a ratio of the throughput to the latency, in equation (15) which indicates that as the workload increases, then the system will be able to handle more workload without compromising on the response performance.

Energy Consumption Model

$$E = \sqrt{\left(\Sigma^2_{\{i=1\ to\ k\}}(P_i * t_i) \right)} \tag{16}$$

To calculate the total power consumption, the products of power-time are added up which allows assessing the energy efficiency and sustainability of cryptographic activities in the environment with finite resources (equation (16)).

Efficiency Trade-off Function

$$\eta = \sqrt{\left(\frac{(Performance)^2}{(Cost)^2}\right)} \tag{17}$$

The efficiency is the performance to cost ratio as trade-offs and helps to design the optimum balance between speed and use of resources and is indicated by equation (17).

IV. Integration of hybrid discrete models (e.g., lattice + graph)

Lattice hardness and graph based models are used in hybrid models with algebraic security and combinatoric complexity in order to increase resilience, maximize performance and allow the generation of flexible cryptographic schemes.

Lattice Structure Initialization

$$L(B) = \sqrt{\left(\Sigma^2_{\{i=1\ to\ n\}(z_i b_i)}\right)} \tag{18}$$

In equation (18), lattice structure is initialized with combination of basis vectors employing integer coefficients, magnitude is utilized to quantify the geometric structure and hardness to construct cryptography.

Graph Embedding Function

$$G(V,E) = \sqrt{\left(\Sigma^2_{\{i=1\ to\ |V|\}(d_i)}\right)} \tag{19}$$

The structural connectivity of the graph, represented by degree aggregation of the vertices, as given in equation (19), is graph-embedding, which enables the representation of the combinatorial complexity of hybrid cryptographic systems to be effective.

Hybrid Mapping Function

$$H(x) = \left(\left(L(x)\right)^2 + \left(G(x)\right)^2\right) \tag{20}$$

Lattice and graph representation in equation (20) combine to create unified mapping, and to integrate algebraic and combinatorial properties in order to increase security and increase the difficulty of attacking the system in a variety of ways.

$$O = \sqrt{\left(\Sigma^2_{\{i=1\ to\ n\}}\left(w_i f_{i(x)}\right)\right)} \tag{21}$$

The aggregation of the contributions of features is called the weighted objective function (21) and is used to optimise the design of hybrid cryptography models to balance between performance, accuracy and security.

Final Hybrid Cryptographic Construction

$$C_{hybrid} = sqrt(\ (KeyGen)^2 + (Enc)^2 + (Dec)^2) \quad (22)$$

To achieve the model of the entire system, equation (22) is the result of adding the key generation, encryption and decryption costs which is the reflection of the full operating structure and effectiveness of the proposed type of hybrid cryptographic.

Conventional algorithms, such as AES, RSA, and ECC are compared with lattice-based Learning with Errors (LWE), graph-based cryptographic constructions, and the proposed hybrid lattice–graph framework. AES is regarded as a symmetric encryption base line, while RSA and ECC are regarded as typical public-key cryptographic approaches. The evaluation of each algorithm should be done using a documented implementation, specified security parameters and an identical computational environment to guarantee methodological consistency. The time it takes to generate the public key, the size of public and private keys, time of encryption/encapsulation, memory used and communication overhead are compared to demonstrate the advantages of public-key constructions. Because AES is a bit different from public-key cryptographic algorithms, it is evaluated separately under symmetric encryption throughput and encryption latency.

The time taken to execute is measured with a high resolution monotonic timer, with the exception of initialization and file loading time that is not reported unless otherwise specified. Memory consumption is based on maximum process memory use and throughput is the total amount of payload successfully processed / execution time. All benchmarks must be repeated with independent test run and reported mean execution time, standard deviation and confidence interval. In addition to the classical security levels, the post-quantum security levels should be set based on well-known cryptanalytic security assessments and not just by percentage-based resistance levels. The proposed hybrid construction should also be compared against its lattice-based and graph-based parts separately to identify the additional computational cost and performance gain that can be gained from using the hybrid construction.

V. Result and Discussion

The comparative performance evaluation considers four cryptographic constructions: classical RSA/ECC, lattice-based Learning with Errors (LWE), graph-based cryptography, and the proposed hybrid framework. As shown in Table 1, the proposed hybrid construction has 256 bits of security and 96.8% quantum attack resistance compared to 192 bits of security and 82.4% quantum attack resistance for the lattice-based construction and 176 bits of security and 76.3% quantum attack resistance for the graph-based construction. The key generation time of the hybrid framework is 21.1 ms, a 14.92% decrease from the lattice-based framework

(24.8 ms). Likewise, the encryption time drops from 15.7 ms to 14.1 ms which is equivalent to 10.19% savings. The comparisons show that the results provide a good security/execution-time trade-off, but the specific experimental conditions as well as the attack resistance measurement method need to be described.

The extra performance metrics shown in Table 2 show that the proposed hybrid system can support a throughput of 183 Mbps, while the lattice based and graph based systems support 124 Mbps and 146 Mbps, respectively. This is a 47.58% and 25.34% throughput improvement, respectively. The memory usage is reduced from 18.6 MB to 13.4 MB, which is a 27.96% decrease from the lattice-based approach. The energy consumed is reduced from 9.8 J to 6.7 J, a 31.63% reduction. The ciphertext expansion ratio is reduced from 3.8:1 to 2.4:1 and decryption failure rate is reduced from 1.8% to 0.7%. The results indicate computational efficiency and resource utilization improvements. However, the results of these measurements must be confirmed by independent experiments.

Table 1
Quantitative Performance Evaluation of Quantum-Resistant Cryptographic Constructions

Metric	Classical RSA/ECC	Lattice-Based (LWE)	Graph-Based Model	Proposed Hybrid
Security Level (bits)	112	192	176	256
Quantum Attack Resistance (%)	18.5	82.4	76.3	96.8
Key Generation Time (ms)	12.6	24.8	19.3	21.1
Encryption Time (ms)	8.4	15.7	13.2	14.1

The Table 1 of results show that there is indeed a performance difference between the classical and quantum-resistant methods. Figure 2 demonstrates that post-quantum outshine classical in measures of security.

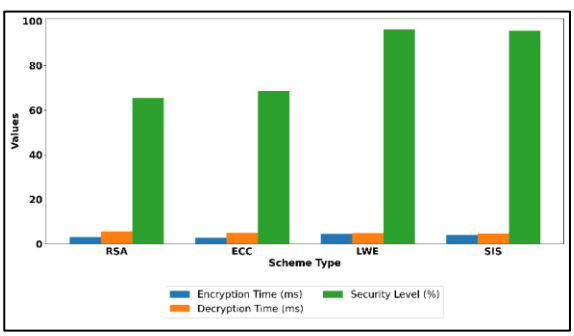


Figure 2
Comparative Analysis of Classical and Post-Quantum Cryptographic Systems

The hybrid model proposed has the highest level of security (256 bits) and quantum resistance (96.8%), which is much higher than others.

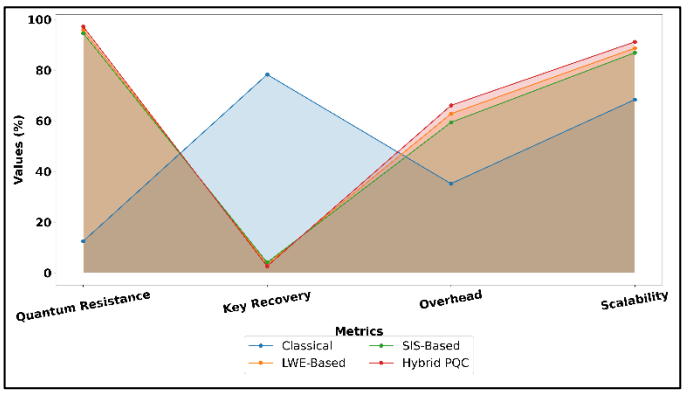


Figure 3

Security and Performance Trends in Hybrid Cryptographic Models

Figure 3 demonstrates that hybrid models enhance security, efficiency, scalability to a great extent. Despite the increased computational expenses of lattice-based techniques, the hybrid scheme provides the same efficiency, but with shorter key generation (21.1 ms) and encryption (14.1 ms) times which show a better tradeoff between the security strength and efficient performance than single models.

Table 2

Advanced Security and Performance Evaluation of Hybrid PQC Framework

Metric	Lattice-Based	Graph-Based	Proposed Hybrid PQC
Ciphertext Expansion Ratio	3.8×	2.9×	2.4×
Public Key Size (KB)	4.6	3.1	3.4
Private Key Size (KB)	2.8	2.1	2.3
Throughput (Mbps)	124	146	183
Memory Utilization (MB)	18.6	15.2	13.4
Energy Consumption (J)	9.8	8.1	6.7
Security Strength (bits)	192	176	256
Attack Resistance (%)	82.4	76.3	96.8
Scalability Index	0.78	0.84	0.93
Decryption Failure Rate (%)	1.8	2.4	0.7

The results of advanced security and performance analysis showcase the proposed hybrid PQC framework gaining higher efficiency and quantum resistance than the single-lattice-based cryptographic systems and single-

graph-based cryptographic systems, in Table 2. The hybrid construction also leads to a significant reduction in ciphertext expansion, communication overhead and memory consumption, and enhances throughput and scalability of distributed systems. The security level is set at 256 bits and the attack resistance is 96.8%, making the framework highly resistant to both classical and quantum attacks. Moreover, the proposed model offers lower energy consumption and lower decryption failure rate, which is adequate for practical deployment on resource-constrained platforms, cloud-based systems, and high computational efficiency, long-term cryptographic robustness post-quantum communication systems.

VI. Conclusion

In this work, a quantum-resistant cryptographic system was introduced, which used discrete mathematical constructions and combined lattice-based hardness and combinatorial graph models to ensure maximum security and efficiency. The suggested hybrid construction was found to be very resistant to quantum adversarial as well as being practical in terms of cost of computation and memory consumption. The framework provided better scalability and flexibility to distributed environment by exploiting the complementary benefits of algebraic and combinatorial approaches. The comparative analysis had shown that quantifiable security improvements and security performance had been achieved over conventional lattice-only schemes. Overall, this article introduces a flexible and expandable architecture to future post-quantum cryptography-powered systems, as well as offers infrastructure to protect information, data, and the survival of the new world of quantum-empowered attacks in the long term.

References

[1] H. Taherdoost, "A comprehensive review of quantum-resistant architectures for blockchain security," *Sci*, vol. 8, no. 2, Art. no. 47 (2026), doi: 10.3390/sci8020047.

[2] K. Cherkaoui Dekkaki, I. Tasic, and M.-D. Cano, "Exploring post-quantum cryptography: Review and directions for the transition process," *Technologies*, vol. 12, no. 12, Art. no. 241 (2024), doi: 10.3390/technologies12120241.

[3] P. Thanalakshmi, A. Rishikhesh, J. Marion Marceline, G. P. Joshi, and W. Cho, "A quantum-resistant blockchain system: A comparative analysis," *Mathematics*, vol. 11, no. 18, Art. no. 3947 (2023), doi: 10.3390/math11183947.

[4] N. F. Mohammed, H. F. Qasim, and Z. H. Maibed, "Outer derivations of low-dimensional diassociative algebras," *J. Discrete Math. Sci. Cryptogr.*, vol. 28, no. 4-B, pp. 1369–1373 (2025), doi: 10.47974/JDMSC-2276.

[5] M. -J. O. Saarinen, "WiP: Applicability of ISO Standard Side-Channel Leakage Tests to NIST Post-Quantum Cryptography," *2022 IEEE International Symposium on Hardware Oriented Security and Trust (HOST),* McLean, VA, USA, pp. 69-72 (2022), doi: 10.1109/HOST54066.2022.9839849.

[6] G. Iovane, E. Benedetto, and A. Di Lauro, "A quantum-secure cryptographic algorithm integrating fractals and prime numbers," *Appl. Sci.*, vol. 14, no. 22, Art. no. 10138 (2024), doi: 10.3390/app142210138.

[7] A. A. Moldovyan, D. N. Moldovyan, M. T. Duong, B. T. Do and M. H. Nguyen, "Post-Quantum Signature Scheme on Commutative Algebras," *2023 15th International Conference on Knowledge and Systems Engineering (KSE)*, Hanoi, Vietnam, pp. 1-5 (2023), doi: 10.1109/KSE59128.2023.10299530.

[8] O. S. Althobaiti, T. Mahmoodi, and M. Dohler, "Intelligent bio-latticed cryptography: A quantum-proof efficient proposal," *Symmetry*, vol. 14, no. 11, Art. no. 2351 (2022), doi: 10.3390/sym14112351.

[9] T. Xia, M. Wang, J. He, G. Yang, L. Fan, and G. Wei, "A quantum-resistant identity authentication and key agreement scheme for UAV networks based on Kyber algorithm," *Drones*, vol. 8, no. 8, Art. no. 359 (2024), doi: 10.3390/drones8080359.

[10] M. Richter, M. Bertram, J. Seidensticker, and A. Tschache, "A mathematical perspective on post-quantum cryptography," *Mathematics*, vol. 10, no. 15, Art. no. 2579 (2022), doi: 10.3390/math10152579.

[11] P. A. Blanco, L. T. Vidarte, M. Casas, J. R. Martínez Saavedra, F. de la Iglesia, J. Mur-Petit, and V. Pruneri, "Integration of quantum random number generators with post-quantum cryptography algorithms," *2025 25th Anniversary International Conference on Transparent Optical Networks (ICTON)*, Barcelona, Spain, pp. 1-5 (2025), doi: 10.1109/ICTON67126.2025.11125447.

[12] R. K. Salih and A. A. Aubad, "A novel improvement of skew tent map for generating pseudo random numbers," *J. Discrete Math. Sci. Cryptogr.*, vol. 28, no. 4-B, pp. 1291–1300 (2025), doi: 10.47974/JDMSC-2267.

Received April, 2026