

# **Journal of Discrete Mathematical Sciences & Cryptography**

Volume 29, Number 9-B, September 2026

*Special Issue on*

**Discrete Mathematical Approaches to Modern  
Cryptography and Secure Authentication**

*Guest Editor*

**Altaf Osman Mulani**

Published by :



*Guest Editor*

**Altaf Osman Mulani**

Department of Electronics & Telecommunication Engineering

SKN Sinhgad College of Engineering

Pandharpur 413304

Maharashtra

India

E-mail: [altaaf.mulani@sknscoe.ac.in](mailto:altaaf.mulani@sknscoe.ac.in)

## FOREWORD

This special issue titled “*Discrete Mathematical Approaches to Modern Cryptography and Secure Authentication*” brings together a focused collection of research that draws on discrete mathematical structures, including algebraic, combinatorial, and graph-theoretic structures, to address pressing challenges in the design of secure authentication and encryption systems for today’s networked and device-driven world.

The papers selected for this issue trace a coherent line of inquiry, beginning with a comparative evaluation of authentication techniques, weighing trade-offs between security strength, computational efficiency, and scalability across resource-constrained environments. Building on this foundation, subsequent contributions propose lightweight hybrid encryption schemes for secure data transmission, designed to operate efficiently under strict computational and power constraints.

A central theme of this issue is the application of elliptic curve cryptography (ECC) and related algebraic structures. Contributions in this area introduce fusion frameworks that integrate ECC-based authentication with dynamic session tokenization and rolling hash integrity verification, providing layered protection against session hijacking and data tampering. Related work extends ECC into secure multi-party computation over discrete algebraic structures, demonstrating how classical number-theoretic and algebraic tools can be adapted for collaborative and privacy-preserving computation.

Anticipating the challenges posed by future computing paradigms, this issue also includes research on hybridized, quantum-contingent cryptographic constructs, exploring how discrete mathematical techniques can be adapted to withstand the vulnerabilities that quantum computing may introduce to classical cryptographic assumptions. Complementing these algebraic approaches, a graph-theoretic contribution applies chromatic graph coloring to the problem of minimum-key distribution, offering an elegant combinatorial solution to secure key management in distributed and wireless environments.

Together, these contributions showcase the richness of discrete mathematics as a foundation for cryptographic innovation, spanning algebraic structures, graph theory, and combinatorial optimization, and demonstrate its continued relevance in confronting both present-day and emerging security challenges.

This special issue is an outcome of the International Conference on Intelligent Computing and Vision Technologies 2025 (ICICVT-25), held at SKN Sinhgad College of Engineering, Pandharpur on 12 and 13 December 2025. The conference received more than 200 research papers covering diverse areas including cryptography, security, intelligent computing, artificial intelligence, machine vision, data science, and emerging computational technologies. All submitted papers underwent a rigorous peer-review process, following which only the most relevant and high-quality 21 research papers were selected for publication in this special issue. The selected papers present innovative approaches, methodologies, and applications addressing contemporary challenges in intelligent computing and vision technologies.

We extend our sincere appreciation to all authors for their valuable contributions, to the reviewers for their insightful comments and dedicated efforts, and to the editorial team for their continuous support throughout in bringing out this special issue. We are particularly thankful to Professor B. K. Dass, Chief Editor, for his constant support and encouragement during the publication process in the *Journal of Discrete Mathematical Sciences & Cryptography*, published by Taru Publications, New Delhi.

We are confident that this special issue will serve as a valuable reference for researchers, practitioners, and students working at the intersection of discrete mathematics and cryptography, and that it will inspire further advances in the theory and application of secure authentication systems.

*Guest Editor :*

**Altaf Osman Mulani**

# Journal of Discrete Mathematical Sciences & Cryptography

Volume 29, Number 9-B, September 2026

*Special Issue on*

## Discrete Mathematical Approaches to Modern Cryptography and Secure Authentication

### CONTENTS

|                                                                                                                                                                                                                                                                          |           |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| A. O. MULANI, K. R. CHAUDHARI, V. V. DESHMUKH, N. NARKHEDE,<br>V. B. LOBO AND P. G. GAWANDE<br>Fuzzy line graphs and their intuitionistic extension :<br>Mathematical properties and applications                                                                        | 3503–3512 |
| M. GHAMANDE, V. N. AHER, G. V. GHULE, P. D. DESHPANDE,<br>K. KSHIRSAGAR AND S. V. GAIKWAD<br>Hybridized lightweight quantum-contingent cryptographic<br>constructs for fortifying device trust in the expanding IoT<br>perimeter                                         | 3513–3522 |
| G. V. GHULE, P. D. DESHPANDE, S. V. GAIKWAD, K. KSHIRSAGAR,<br>M. GHAMANDE AND R. S. POL<br>A lightweight fusion framework for IoT security : Integrating<br>ECC-based authentication, dynamic session tokenization, and<br>rolling hash integrity                       | 3523–3532 |
| V. UDAY KUMAR, N. K. MANIKANDAN, C. KAUSHIK, P. ANUSHA,<br>P. M. GOUD, L. PALLAVI, K. SARANYA AND S. MALEMPATI<br>Spatial omics-informed graph neural networks for metabolic<br>flux estimation in microbial communities                                                 | 3533–3542 |
| K. K. KUMAR, R. KULKARNI, S. KAYALVIZHI, D. SHARMA,<br>S. PUSHPARANI, Y. TONDEPU, G. MOUNICA AND B. S. RAO<br>A novel fuzzy graph based cryptographic framework for<br>secure communication in computer and electronic systems<br>using discrete mathematical structures | 3543–3552 |
| P. V. SHINDE, M. PATIL, R. S. PACHADE, V. RANE, A. O. MULANI<br>AND M. RANA<br>Fuzzy algebraic structure based cryptographic key generation                                                                                                                              | 3553–3562 |

|                                                                                                                                                                                                                                                                                 |           |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| A. O. MULANI, S. JAGADEESH, S. S. SALUNKHE, K. SHIVASHANKER,<br>P. G. GAWANDE AND S. M. SHUKLA<br>Fuzzy domination in graphs and its applications to<br>cryptographic key generation                                                                                            | 3563–3572 |
| V. N. AHER, M. GHAMANDE, P. D. DESHPANDE, G. V. GHULE,<br>K. KSHIRSAGAR AND R. S. POL<br>Performance evaluation of IoT authentication techniques :<br>Balancing security, efficiency, and scalability                                                                           | 3573–3582 |
| N. DUDIKI, N. MANJUNATHAN, A. H. PRASAD, S. REVATHI,<br>R. N. RAVIKUMAR, M. CHANDAN, V. BALAJI AND N. S. R. P. KUMAR<br>Fuzzy algebra-based cryptographic key generation models for<br>secure communication systems                                                             | 3583–3592 |
| S. KALLI, V. S. J. R. K. PADMINIVALLI, S. R. S. V. BALA, V. L. PRIYA,<br>B. SRINIVAS, M. THOLKAPIYAN, R. N. RAVIKUMAR AND<br>P. V. L. R. N. S. SUDHA<br>Discrete algebraic channel modeling and information-theoretic<br>security bounds for quantum key distribution protocols | 3593–3602 |
| N. S. RAMIREDDY AND K. B. PRAKASH<br>Elliptic curve cryptography based lightweight mutual<br>authentication with zero-knowledge proof for industrial<br>Internet of Things networks                                                                                             | 3603–3611 |
| S. D. KUMAR, S. SIVAPRAKASH, P. IYAPPAN, S. THAMIZHARASAN,<br>K. C. ARUN AND S. P. MANIKANDAN<br>Algebraic lattice decomposition techniques for AI-assisted<br>security evaluation of cryptographic schemes                                                                     | 3613–3622 |
| M. S. KOBAN, S. S. GADADHE, D. YEWALE AND K. S. GADGIL<br>Elliptic curve cryptography based secure multi-party<br>computation over discrete algebraic structures                                                                                                                | 3623–3632 |
| N. PARVEEN, K. U. NISA, P. GAYATRI, K. N. BHARGAVI, P. LALITHA,<br>K. C. ARUN, M. SANGEETHA AND A. SRUTHI<br>Finite field algebraic coding theory for enhanced physical layer<br>security in wireless communication networks                                                    | 3633–3641 |
| P. D. DESHPANDE, G. V. GHULE, M. GHAMANDE, K. KSHIRSAGAR,<br>S. V. GAIKWAD AND R. S. POL<br>Cryptographic framework for secure data transmission in IoT<br>networks using lightweight hybrid encryption                                                                         | 3643–3652 |
| Z. H. CHOUDHURY, R. R. KALANGI, K. K. RAO, P. KATKAM,<br>R. T. ANANDAM, A. SUNDARAM, W. T. CHEMBIAN AND I. ATHAL<br>Discrete algebraic ring signatures on elliptic curves for<br>privacy-preserving blockchain transaction authentication                                       | 3653–3661 |

|                                                                                                                                                                                                                                                                  |           |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| N. KRISHNAVENI, B. S. SAMANTHA, P. GAYATHRI,<br>S. S. SUBRAMANIAN, V. AMMISETTY, D. SARANYA, V. R. GERA AND<br>T. M. AMIRTHALAKSHMI<br>Homomorphic encryption over polynomial rings for<br>privacy-preserving healthcare data analytics in cloud<br>environments | 3663–3672 |
| M. S. KOBAN, S. KHEDKAR, D. YEWALE AND S. S. GADADHE<br>Chromatic graph coloring-based minimum-key distribution<br>for secure wireless sensor networks                                                                                                           | 3673–3682 |
| K. SHRISHA, T. V. S. VIVEK, R. R. KALANGI, R. S. BABU,<br>M. MANIMARAN, D. VETRITHANGAM, V. VINITHA AND D. GEORGE<br>A mathematical hybrid lattice–elliptic curve encryption model<br>for lightweight IoT security                                               | 3683–3692 |
| S. SIVAPRAKASH, S. D. KUMAR, S. THAMIZHARASAN, P. IYAPPAN,<br>W. T. CHEMBIAN AND K. SONY<br>Discrete graph spectral framework for dynamic malware<br>detection in software-defined networks                                                                      | 3693–3702 |
| S. MEKALA, K. BHARGAVI, R. T. ANANDAM, A. KULKARNI,<br>G. MANIKANDAN, T. M. AMIRTHALAKSHMI, T. S. REDDY AND<br>V. BALAJI<br>Graph-theoretic zero-knowledge authentication scheme for<br>decentralized identity management                                        | 3703–3712 |