Journal of Discrete Mathematical Sciences & Cryptography

Volume 29, Number 10-A, October 2026

Special Issue on

Advances in Discrete Mathematics and Secure Network Technologies (Part-A)

Guest Editors

Ramesh Chandra Poonia

Ankur Goyal

Amol Dhumane

Raja Kumar Rajaboina

K Rajendra Prasad

Arul Kumar Natarajan

Published by :



Guest Editors

Ramesh Chandra Poonia
Department of Computer Science
CHRIST (Deemed to be University)
Ghaziabad 201003
Uttar Pradesh
India
E-mail: rameshcpoonia@gmail.com

Ankur Goyal
Symbiosis Institute of Technology
Pune Symbiosis International Deemed University
Pune 412115
Maharashtra
India
ankur.goyal@sitpune.edu.in

Amol Dhumane
Symbiosis Institute of Technology
Pune Symbiosis International Deemed University
Pune 412115
Maharashtra
India
Email: amol.dhumane@sitpune.edu.in

Raja Kumar Rajaboina
Department of Computer Science and Engineering
Rajeev Gandhi Memorial College of Engineering and Technology
Nandyal 518501
Andhra Pradesh
India
E-mail: rajakumar.rajaboina@gmail.com

K. Rajendra Prasad
Department of Computer Science and Engineering
Amity School of Engineering & Technology
Amity University
Hyderabad 500108
Telangana
India
Email: krprgm@gmail.com

Arul Kumar Natarajan
Department of Cybersecurity
School of Computing
Samarkand International University of Technology
Samarkand 140100
Uzbekistan
Email: arul.natarajan@siut.uz

Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 10-A, pp. iii-iv
DOI : 10.47974/JDMSC-29-10-A-Foreword

FOREWORD

This special issue entitled "*Advances in Discrete Mathematics and Secure Network Technologies*" brings together a comprehensive collection of research papers on current trends in discrete mathematics, algebra, combinatorics, cryptography, coding theory, and secure network technologies. This special issue contains articles that address various aspects of modern discrete mathematics and its applications in cybersecurity. Special attention has been paid to graph theory, algebraic structures, finite fields, finite groups, polynomial rings, combinatorial designs, Boolean functions, hypergraphs, semigroups, and discrete optimization. At the same time, these mathematical tools are applied to various modern cryptographic schemes, including lightweight cryptography, elliptic- and hyperelliptic-curve cryptography, lattice- and isogeny-based cryptography, homomorphic cryptography, threshold cryptography, zero-knowledge proofs, secure multiparty computation, and post-quantum cryptography.

This special issue consists of selected research papers that were presented at the International Conference on Sustainable Computing and Management (SUSCOM-2026) organized by Sri Balaji College of Engineering & Technology, Jaipur, Rajasthan, India, from June 26-27, 2026. The conference received an overwhelming response with more than 760 research submissions, out of which 90 high-quality papers were carefully selected for publication in this special issue, which are being published in three parts : JDMSC 29#10-A, JDMSC 29#10-B and JDMSC 29#10-C, with 30 papers each, covering a wide range of innovative concepts. The conference provided a valuable forum for researchers, educators, and practitioners to exchange ideas and share recent developments in sustainable computing, mathematical sciences, cybersecurity, intelligent technologies, and interdisciplinary research.

© Taru Publications

We would like to extend our sincere thanks to all the authors for their valuable contributions and to all the reviewers for their constructive feedback and comments. In particular, we would like to thank Prof. B. K. Dass, Chief Editor, for his consistent guidance and support throughout the publication process of this special issue of *Journal of Discrete Mathematical Sciences and Cryptography*, published by Taru Publications, New Delhi.

We believe that the research findings presented in this special issue will offer valuable insights to researchers, academics, and practitioners working in discrete mathematics, cryptography, coding theory, cybersecurity, and secure networking technologies.

Guest Editors :
Ramesh Chandra Poonia
Ankur Goyal
Amol Dhumane
Raja Kumar Rajaboina
K. Rajendra Prasad
Arul Kumar Natarajan

Journal of Discrete Mathematical Sciences & Cryptography

Volume 29, Number 10-A, October 2026

Special Issue on

Advances in Discrete Mathematics and Secure Network Technologies (Part-A)

CONTENTS

D. Balaji, T. Singh, N. M. Shinde, R. K. Tripathi, V. Dhanalakshmi and K. Nikhila
Chaotic polynomial sequences for high-entropy stream ciphers 3713–3725

S. S. Aladakatti, B. V. Ramana, V. U. Bansude, S. P. Katake, M. Keerthana and S. C. Agrawal
Cryptographic indexing schemes for encrypted scientific databases 3727–3738

S. Vhatkar, R. Mane, S. Kaulgud, A. B. Marathe, A. A. Maha and Z. Aalam
Graph-partition-based attack mitigation in dense mesh networks 3739–3749

K. Rohini, C. G. Rajput, M. Verghese, M. Singh, S. Goyal and S. Purohit
Code-based signature schemes for long-term archival documents 3751–3763

M. Alfiras, M. H. Aldulaimi, M. M. Ranade, G. Tiwari, M. Vinitha, E. Asadbek and S. Ibragimova
Topological simplification methods for large-scale knowledge graphs 3765–3775

S. J. Modi, K. S. Bhosale, A. G. Said, S. N. Ajani, A. Bhansali and P. N. Sripada
Probabilistic analysis of threshold cryptography for cloud storage 3777–3790

M. Alfiras, M. Thamizhsudar, A. Gaurav, M. S. Pawar, M. Chhabra and S. Sabirov
Number-theoretic foundations of attribute-based encryption schemes 3791–3801

S. Gayathri, V. Swathi, M. H. Aldulaimi, S. Kasimova, Q. Hayitov and E. Bekmurod
Graph-theoretic approaches to post-quantum cryptographic protocols 3803–3814

A. R. Alex, B. Sule, M. Jagga, B. Vamalatha, S. Goyal and G. Tiwari
Algebraic structures for lightweight block cipher design 3815–3826

O. Al Rawi, M. Thamizhsudar, N. Nivetha, V. V. Patel, M. M. Ranade, A. Abduvokhidov and S. Sabirov
Number-theoretic foundations of post-quantum cryptographic protocols 3827–3838

V. V. Patel, S. Goyal, P. Lavanya, R. Adhau, S. Punwatkar and S. Pandey
Error-correcting code embedding for confidential edge storage 3839–3850

H. U. Karne, P. K. Yadav, V. M. Dabhi, R. Snehaa, M. Vinitha and M. Chhabra
Graph-theoretic approaches to lightweight block cipher design 3851–3862

P. V. Kashid, S. Khurana, S. Gupta, S. S. Kulkarni, S. Loganathan and D. Balaji
Algebraic curve constructions for lightweight key establishment 3863–3874

A. K. Bhanja, M. A. Kumar, G. V. Shrimant, T. S. Rani, M. I. Patel and D. Balaji
Algebraic frameworks for transparent cryptographic systems 3875–3886

M. H. Molawade, P. Sharma, K. Tejesh, S. Goyal, V. M. Dabhi and Y. Hasan
Lattice-based homomorphic encryption for privacy-preserving medical analytics 3887–3898

R. Shrivastav, P. Gaikwad, R. Thangjam, G. V. Kumar, A. P. Kharade and P. P. Kale
Lightweight post-quantum cryptography for energy-constrained wireless sensor networks 3899–3912

M. K. Assudani, S. S. Shriyal, P. Sharma, N. Mounika, S. Goyal and V. M. Dabhi
Secure cross-border medical data exchange using post-quantum cryptography 3913–3924

Y. D. Jadhav, J. Suryavanshi, P. Shrivastava, P. A. Upadhye, M. Jagga and K. Parimala
Algebraic cryptographic primitives for secure IoT data aggregation 3925–3936

M. H. Molawade, D. Pisal, P. M. Patare, S. O. Ahire, S. Guha and S. Goyal
Homomorphic encryption–enabled AI processing for IoT security 3937–3949

A. B. Ubale, V. Kotkar, S. D. Joshi, M. S. Patil, P. K. Yadav and V. S. N. Kumar
AI-driven early warning systems for IoT cyber threats 3951–3961

A. B. Raut, A. B. Thakare, S. T. Surase, B. K. Kiran, S. R. Shaikh and M. B. Diwate
Graph homomorphisms and applications to network coding 3963–3972

S. Gayathri, L. R. Desai, B. Vamalatha, H. Sharma, M. D. Venkata and M. Jagga
Hamiltonicity conditions in random graph models 3973–3983

M. M. Ranade, S. Gayathri, G. Tiwari, V. Swathi, S. Goyal and R. Kumar
Dominating sets in hierarchical sensor networks 3985–3996

A. R. Khatoon, M. W. A. Khan, H. M. H. Tariq and T. Khan
A lightweight block cipher based on combinatorial substitution structures 3997–4007

D. Kumar, K. Sairam, V. S. N. Kumar, D. Balaji, L. Verma and P. D. Morey
Algebraic construction of secure S-boxes using finite fields 4009–4019

P. Sharma, M. R. Mani, M. M. Zade, I. D. Bhavani, R. Snehaa and K. Rohini
Cryptographic protocols based on graph isomorphism hardness 4021–4032

N. Govil, K. Keerthika, S. Sobti, M. Sruthi, D. Raupov and A. K. Bhuvaneswari
Applications of group actions in symmetric cryptosystems 4033–4044

H. M. H. Tariq, T. Khan, A. R. Khatoon and M. W. A. Khan
Semiring-based models for secure data aggregation 4045–4054

J. P. Tiwari, D. Balaji, S. M. Karve, M. Dixit, P. P. Kale and B. Prashanthi
Ideal structure of polynomial rings over finite fields 4055–4064

M. W. A. Khan, A. R. Khatoon, H. M. H. Tariq and T. Khan
Post-quantum cryptographic schemes using lattice problems 4065–4074