Journal of Discrete Mathematical Sciences & Cryptography

Volume 29, Number 10-B, October 2026

Special Issue on

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

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-B, pp. iii-iv
DOI : 10.47974/JDMSC-29-10-B-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-B, October 2026

Special Issue on

Advances in Discrete Mathematics and Secure Network Technologies (Part B)

CONTENTS

K. Madhura, B. Sule, S. S. Sarpal, A. K. Bhuvaneswari, S. Goyal and Y. B. Adhyaru
Boolean function optimization for stream cipher design 4075–4085

T. Khan, H. M. H. Tariq, M. W. A. Khan and A. R. Khatoon
Homomorphic encryption based on modular arithmetic structures 4087–4096

R. Shrivastav, L. R. Desai, S. Khurana, L. Ravilla, S. Goyal and F. Hasan
Chaos-based image encryption using discrete maps 4097–4107

D. Y. Sakhare, Y. S. Lonkar, M. Raghavendra, S. R. Sree, S. Loganathan and P. P. Kale
Cryptographic hash functions derived from expander graphs 4109–4119

S. Sonawane, D. Motwani, V. Chitre, A. Nerurkar, V. Bhosale and R. Deolekar
Linear approximation attacks on reduced-round block ciphers 4121–4131

M. Kaur, G. Kaur, D. S. Kumar, S. N. Ajani, R. Dhulipudi and R. A. Padgilwar
Algebraic attacks on multivariate public key cryptosystems 4133–4143

N. Wankhade, A. Gaurav, S. S. Reddy, N. Varshney, M. Ernazarov, B. Madaminov and P. S. Lahane
Combinatorial design theory for the development of threshold secret sharing schemes in cloud-based environments 4145–4155

P. R. Patil, S. Verma, V. Lobo, A. M. Gojare, N. Kamble and S. S. Rajpurohit
Cryptanalysis of permutation-based image encryption algorithms 4157–4167

A. A. Patil, N. J. Vispute, U. B. Goradiya, P. Wagde, S. N. Ambekar and S. Verma
Fault injection attacks on finite field arithmetic implementations 4169–4178

M. Thamizhsudar, T. A. Wani, S. Kaur, M. S. Heera, B. Anandkumar and V. Satyanarayana
Number-theoretic transformations in public key encryption 4179–4188

T. A. Wani, A. K. Bhuvaneswari, S. S. Shriyal, Tusha, Y. B. Adhyaru and A. Baxrom
Modular forms and their role in cryptographic constructions 4189–4199

S. S. Rajpurohit, A. A. Patil, N. J. Vispute, U. B. Goradiya, P. Wagde and S. N. Ambekar
Secure pairing-based cryptographic protocols 4201–4211

R. S. M. Joshitta, S. S. Gaikwad, S. Goyal, N. Mohan, S. Suganya and N. S. Bajare
Ring-theoretic analysis of error-correcting codes 4213–4224

A. Srividya, S. Goyal, Y. Hasan, S. S. Pawale, S. Meylikulov, C. R. Vaghela and U. Musaev
Boolean function analysis for enhancing nonlinearity and resistance against linear and differential cryptanalysis 4225–4236

K. Madhura, B. Vijay, A. Chaudhary, V. Bibhu, S. Buriyev and M. Latipova
Statistical attacks on pseudorandom number generators 4237–4247

T. A. Wani, N. M. Patel, K. Navya, S. N. Ajani, P. Goyal and S. S. Pawale
Algebraic graph theory in secure communication design 4249–4259

S. S. Aladakatti, V. V. Patel, R. R. Papalkar, H. B. Magar, V. Yadav and S.Farhan
Discrete logarithm problem in hyperelliptic curve groups 4261–4272

S. A. Thanekar, D. R. Anekar, R. Suryawanshi, A. N. Nawathe, Y. Shepal, M. G. Ovhal and M. Gulhane
Matrix group representations in cryptographic transformations 4273–4288

P. Dubey, D. A. Meshram, R. A. Kulkarni, A. V. Surana, K. Khairnar, K. Ghuge and C. D. Kokane
Torsion subgroups and their cryptographic implications 4289–4298

V. Yadav, A. P. Kharade, Tusha, L. Ravilla, C. G. Rajput and G. Bathla
Enumeration and classification of self-dual codes over finite rings with applications in cryptographic systems 4299–4308

V. V. Kimbahune, C. D. Sukte, N. Deshpande, U. Raut, S. Chavan, A. S. Gaikwad and C. D. Kokane
Discrete algebraic methods in secure distributed systems 4309–4320

B. S. Panigrahi, R. K. Singh, P. Madan, N. Ramu, A. Chaudhary and M. I. Patel
Efficient scalar multiplication techniques on elliptic curves 4321–4331

S. Gupta, P. Reddy, U. Bhardwaj, M. R. Babu, R. Sowmya and B. P. Mishra
Authentication schemes using combinatorial key distribution 4333–4345

M. Shkoukani, N. Gain, V. V. Patel, M. R. Ghogare, B. Vamalatha and P. S. Kshirsagar
Elliptic curve cryptography over binary extension fields 4347–4356

S. B. Patil, S. V. Joshi, T. N. Pawase, V. G. Kale, D. B. Patil and A. B. Rajmane
Secure data hiding via discrete wavelet transform techniques 4357–4368

R. A. Kapgate, D. Raju, C. R. Vaghela, N. S. Balan, A. Barde and K. C. Pidugu
Isogeny-based cryptosystems for post-quantum security 4369–4381

S. Rungta, N. Raj, N. Mounika, V. K. Patil, M. T. Jadhav and C. R. Vaghela
Combinatorial approaches to privacy-preserving data mining 4383–4395

M. S. Reddy, F. Hasan, S. Gupta, S. P. Chaudhary, M. S. Pawar and S. Islam
Efficient scalar multiplication algorithms on elliptic curves over prime fields for resource-constrained cryptographic devices 4397–4406

B. Prabhakar, T. Singh, N. Sao, K. Sairam, S. N. Patil and R. V. Patil
Threshold cryptography for distributed ledger systems 4407–4416

S. C. Cholke, A. Garg, V. Swathi, T. Sharma, K. D. Parmar and P. N. Sripada
Secure routing in wireless networks using dominating sets 4417–4428