

Journal of Discrete Mathematical Sciences & Cryptography

Volume 28, Number 8, December 2025

Special Issue on

Cryptography and Secure Intelligent Systems : Biometrics, Blockchain, Homomorphic Encryption, and FinTech Security

Guest Editors

Chirag Joshi

Gaurav Kumawat

Neeraj Kumar Verma

Sarvesh Kumar

Published by :



Guest Editors

Chirag Joshi

Department of Data Science and Engineering
Manipal University Jaipur
Jaipur
Rajasthan
India
E-mail: chirag.joshi@jaipur.manipal.edu

Gaurav Kumawat

Department of Data Science and Engineering
Manipal University Jaipur
Jaipur
Rajasthan
India
E-mail: gaurav.kumawat@jaipur.manipal.edu

Neeraj Kumar Verma

Department of Data Science and Engineering
Manipal University Jaipur
Jaipur
Rajasthan
India
E-mail: neeraj.verma@jaipur.manipal.edu

Sarvesh Kumar

Amity Institute of Information Technology
Amity University, Patna
Patna
Bihar
India
E-mail: skumar8@ptn.amity.edu

FOREWORD

This special issue titled “*Cryptography and Secure Intelligent Systems: Biometrics, Blockchain, Homomorphic Encryption, and FinTech Security*” presents cutting-edge research connecting discrete mathematics, cryptography, secure AI, and modern digital systems. The selected papers of this special issue arises from contributions submitted to the International Conference on Innovations in Data Science (ICIDS 2024) held at Manipal University Jaipur, Jaipur on 28–29 November 2024. Out of over 320 submitted manuscripts, only 19 papers from researchers covering a wide range of innovative concepts have been selected for publication in this issue.

Each contribution demonstrates how mathematical modeling, non-invertible transformations, private-key mechanisms, and encrypted computation strengthen the trustworthiness of today’s interconnected digital infrastructures.

Together, the works address challenges such as identity protection, secure digital transactions, encrypted model aggregation, and safeguarding financial platforms from sophisticated cyber threats. They illustrate how cryptographic primitives—ranging from lattice-based schemes and polynomial encodings to zero-knowledge proofs and homomorphic encryption—provide robust solutions to risks such as replay attacks, data exposure, unauthorized access, and fraud. These studies collectively show that advancing digital security requires both theoretical depth and system-level innovation.

We extend sincere gratitude to all authors, reviewers, and the editorial team, and especially to Professor B. K. Dass, Chief Editor, for his invaluable guidance during the publication process in the *Journal of Discrete Mathematical Sciences and Cryptography*, published by Taru Publications, New Delhi.

We hope this issue serves as a meaningful resource for researchers and practitioners working toward secure, privacy-preserving intelligent systems.

Guest Editors :

Chirag Joshi

Gaurav Kumawat

Neeraj Kumar Verma

Sarvesh Kumar

Journal of Discrete Mathematical Sciences & Cryptography

Volume 28, Number 8, December 2025

Special Issue on

Cryptography and Secure Intelligent Systems : Biometrics, Blockchain, Homomorphic Encryption, and FinTech Security

CONTENTS

S. KHANDELWAL, K. RAMI, H. VYAWAHARE, A. S. GAHLOT, R. VYAS AND G. KUMAWAT Secure vein biometrics authentication based on multimodal artificial template and cryptographic salts	2915–2931
G. KUMAWAT, T. KANT, V. BHARDWAJ, M. KUMAR, A. RASHID AND M. T. B. OTHMAN Cryptographic protocols for passwordless systems with enhanced security	2933–2944
G. M. UPADHYAY, M. JOSHI, S. SHANKER, ANU, A. K. PHOGAT AND P. VATS A private key cryptographic framework for preventing replay attacks and digital signature verification in securing blockchain networks	2945–2954
A. K. SHARMA, N. BABBAR, P. PAL, N. K. VERMA AND R. K. SAINI AI-powered framework for real-time dark web monitoring and cybersecurity threat detection	2955–2966
N. BABBAR, A. K. SHARMA, R. K. SAINI AND N. K. VERMA Mathematical foundations of secure AI : Homomorphic encryption for distributed learning systems	2967–2975
S. K. JHA, S. VERMA, S. GUPTA, K. K. KUMAR, D. KAPILA AND S. MOHAPATRA Cybersecurity in FinTech : Strategies for protecting digital finance from cyber threats and ensuring secure transactions	2977–2987

A. TIWARI, S. C. ADDIMULAM, N. DUBEY, K. K. KUMAR, D. KAPILA AND K. JAIN Cybersecurity in voice over IP (VoIP) systems : Protecting communication networks from threats, vulnerabilities, and cyber attacks	2989–2999
S. SAXENA, S. SRIVASTAVA, D. DUDEJA, C. T. D. PRAVINA, N. KAPILA AND P. NAROOKA Enhancing cybersecurity measures in virtual reality and augmented reality environments : Challenges, risks, and solutions	3001–3011
P. NAROOKA, D. SHARMA, M. T. BASU, V. KUMAR, S. C. ADDIMULAM, N. KAPILA AND N. K. VERMA Deepfake detection : A new frontier in cybersecurity for protecting digital identities, preventing misinformation, and ensuring data integrity	3013–3023
A. MALSARIA, C. JOSHI, S. BASU AND N. SHARMA Secure chaotic cryptography for optical image encryption in pervasive devices using Lorenz-based DRPE, hybrid RSA-AES, and blockchain trust anchoring	3025–3037
V. P. SINGH, S. S. BISWAS, B. ALANKAR AND S. TANWEER Cryptographic modeling and discrete structures for intrusion detection in Ethereum smart contracts	3039–3048
G. M. UPADHYAY, N. TEWARI, S. SHANKER, A. K. PHOGAT, A. MISRA AND T. MALCHE Analysis of the robustness and cryptographic security of a DCT-based image watermarking scheme	3049–3058
M. KUMAR, B. AHMED, M. SHUJA, K. DHIMAN, A. M. A. QUTEISHAT, A. QTAISHAT AND V. BHARDWAJ LCE-AIoT : A lightweight cryptographic algorithm for resource-constrained AIoT devices	3059–3069
S. SHARMA, P. RATHI, R. K. POPLI, SUSHAMA AND P. VATS Algebraic graph models for secure distributed networks and cryptographic systems	3071–3080
P. VATS, S. K. BUDHANI, D. K. SRIVASTAVA, S. L. YADAV, S. K. GUPTA AND A. K. SAINI Secure key exchange and digital signatures via elliptic curves and discrete mathematical principles	3081–3089

VIRENDER, N. SHARMA AND S. SONI Quantum-resistant hierarchical consensus protocol (QRHCP) for enhanced security in blockchain networks	3091–3100
S. SHARMA, P. SHARMA, S. SHANKER, P. VELUVALI, S. TANWAR AND P. VATS A PKI-integrated cryptographic framework for deepfake detection via facial micro-expression analysis	3101–3109
A. K. SAINI, M. WADHWA, R. K. POPLI, M. L. SAINI, S. KUMAR AND P. VATS Combinatorial algebra and cryptographic graph structures for cluster-based hybrid intrusion detection in IoT networks	3111–3120
A. CHAURASIA, A. K. SHARMA AND S. K. SHARMA Post quantum cryptography for blockchain security using CRYSTALS-Dilithium authentication	3121–3132
INDEX OF VOLUME 28 (2025)	3133–3153