

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

Volume 27, Number 2-B, March 2024

*Special Issue on*

**Advancements in Intelligent Encryption Systems and its Applications (Part-B)**

*Guest Editors*

**Dinesh Goyal**

**Pranav Dass**

**Anil Kumar**

**Gajanand Sharma**

**Carlos M. Travieso- Gonzalez**

Published by:



*Guest Editors*

**Dinesh Goyal**

Department of Computer Science and Engineering  
Poornima Institute of Engineering & Technology  
Jaipur  
Rajasthan  
India  
E-mail: dinesh.goyal@poornima.org

**Pranav Dass**

Department of Computer Science  
Shyam Lal College  
University of Delhi  
New Delhi  
India  
E-mail: pdasscs@shyamlal.du.ac.in

**Anil Kumar**

Department of Computer Engineering  
Poornima Institute of Engineering and Technology  
Jaipur  
Rajasthan  
India  
E-mail: anilkumar@poornima.org

**Gajanand Sharma**

Department of Computer Engineering  
JECRC University  
Jaipur  
Rajasthan  
India  
E-mail: gajanan.sharma@gmail.com

**Carlos M. Travieso-Gonzalez**

Department of Signals and Communication  
University of Las Palmas de Gran Canaria  
Spain  
E-mail: carlos.travieso@ulpgc.es

## FOREWORD

The digital era has underscored the necessity for resilient and fortified communication protocols. While traditional encryption methodologies remain indispensable, they confront escalating hurdles posed by evolving cyber threats and burgeoning data intricacies. This special issue endeavours to probe into the strides made in intelligent encryption systems and their capacity to redefine data security amidst these challenges.

The fusion of computational intelligence (CI) and machine learning (ML) presents promising avenues for crafting adaptive, self-learning, and efficient encryption frameworks. These frameworks hold the promise of bolstering security by dynamically adjusting to emergent threats and vulnerabilities. Intelligent encryption systems have the potential to outmatch the security efficacy of static traditional methods. Furthermore, with their capacity to assimilate and adapt to fluctuating data volumes and complexities, intelligent systems can proficiently fortify extensive datasets and diverse communication channels, thus augmenting the scalability of the system.

The objective of this special issue intends to bring together research and advancements done in the field of computational intelligence and machine learning. Researcher can contribute more towards the recent advancement in this field related to computational intelligence in cloud computing.

Under the 5th edition of our International Conference on Information Management and Machine Intelligence (ICIMMI-2023), held on 14-16 Dec 2023, at Poornima Institute of Engineering & Technology, Jaipur, Rajasthan, India, in association with Asia University, Taiwan; IIIT Nagpur and NUST,

Namibia, we had received 129 papers out of which, after peer review, 30 papers are now being published in Part A and 29 in Part B of this Special Issue.

The guest editors of this special issue would like to express their gratitude to authors for sharing their valuable research and publication partner for their approval regarding the special issue of the esteemed journal. Guest editors especially thank Prof. B. K. Dass, Chief Editor who supported us in bringing out the Special Issue/s on “**Advancements in Intelligent Encryption Systems and its Applications**” of selected peer reviewed, high quality papers, in “Journal of Discrete Mathematical Sciences & Cryptography” published by Taru Publications, New Delhi.

*Guest Editors:*

**Dinesh Goyal**

**Pranav Dass**

**Anil Kumar**

**Gajanand Sharma**

**Carlos M. Travieso- Gonzalez**

# Journal of Discrete Mathematical Sciences & Cryptography

Volume 27, Number 2-B, March 2024

*Special Issue on*

## Advancements in Intelligent Encryption Systems and its Applications

### CONTENTS

|                                                                                                                                                                                                                 |         |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
| U. UPADHYAY, A. KUMAR, S. ROY AND U. RAWAT<br>Balancing innovation and privacy : A machine learning perspective                                                                                                 | 547–557 |
| K. D. SINGH, P. D. SINGH, G. L. SAINI, D. PANWAR AND D. GOYAL<br>Cryptographic security for IoT : Leveraging Feistel-permutation network for enhanced encryption                                                | 559–568 |
| D. GOYAL, F. SHETH, P. MATHUR AND A. K. GUPTA<br>Discrete mathematical models for enhancing cybersecurity : A mathematical and statistical analysis of machine learning approaches in phishing attack detection | 569–599 |
| S. K. SHARMA AND A. KUMAR<br>A cellular automata approach for extending data privacy and security of edge computing                                                                                             | 601–612 |
| A. PAL, D. GOYAL, S. SHARMA, S. MATHUR, J. KUMAWAT AND G. SHARMA<br>Proposed approach for securing VANET by detection and avoidance of Sybil attack                                                             | 613–623 |
| H. V. TAIWADE AND P. B. AMBHORE<br>Hybrid bioinspired approach for secret sharing algorithm and ownership transfer optimization in cloud based models                                                           | 625–637 |
| K. M. PATIL<br>Some applications of trace of powers of matrices to graph theory, algebra and combinatorics                                                                                                      | 639–650 |
| K. A. SUTARIA AND N. B. DESAI<br>On the relations between antitrace, row/column sum of elements and generalized horadam sequence associated with a matrix                                                       | 651–663 |

|                                                                                                                                                                                                                                 |         |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
| S. KOMALA AND U. MARY<br>Burning, edge burning & chromatic burning classification of<br>some graph family                                                                                                                       | 665–674 |
| V. D. GOWDA, Y. N. SUNITHA, S. V. CHAKRASALI, K. D. V. PRASAD,<br>P. SARMA AND M. RAHMAN<br>Mathematical analysis of wavelet-based multi-image<br>compression in medical diagnostics                                            | 675–687 |
| P. SRILATHA, S. P. BENDALE, M. SINGH, N. CHAKOLE, G. M. DHOTE<br>AND N. SHELKE<br>Machine intelligence security : A methodological blend of<br>fuzzy logic in industry 4.0 algorithms                                           | 689–701 |
| D. GOYAL, A. KUMAR, Y. GANDHI AND V. KHETANI<br>Securing wireless sensor networks with novel hybrid<br>lightweight cryptographic protocols                                                                                      | 703–714 |
| J. CHANDWANI, G. DHOPAVKAR, M. TATIYA, N. CHAKOLE,<br>S. V. KULKARNI AND N. SHELKE<br>Security-aware analytical framework : A mathematical model<br>and machine learning for dynamical system control in secure<br>environments | 715–727 |
| D. DHABLIYA, S. KUNCHE, S. DINGANKAR, S. S. DARI, R. DHABLIYA<br>AND V. KHETANI<br>Blockchain technology as a paradigm for enhancing cyber<br>security in distributed systems                                                   | 729–740 |
| V. DESHPANDE, D. KHUBALKAR, A. DHABLIA, M. J. PASHA,<br>D. DHABLIYA AND Y. GANDHI<br>Enhancing financial transaction security with lightweight<br>cryptographic algorithms                                                      | 741–751 |
| S. S. DARI, D. DHABLIYA, A. DHABLIA, S. DINGANKAR, M. J. PASHA<br>AND S. N. AJANI<br>Securing micro transactions in the Internet of Things with<br>cryptography primitives                                                      | 753–762 |
| M. PALIWAL, P. SONI, R. KUMAR, A. GOYAL, M. MALIK AND<br>B. GOYAL<br>Chaotic map-based selective image encryption via diffusion<br>and confusion                                                                                | 763–773 |
| D. SHARMA, C. PRABHA, A. GOYAL, M. MALIK AND R. KUMAR<br>Enhanced security of EMI using an edge-based steganography<br>with four-layered cryptography                                                                           | 775–784 |
| V. K. VERMA, M. V. C. VARMA, A. JALA, R. K. GUPTA AND<br>P. DADHEECH<br>The fusion of quantum chaos and nonlinear dynamics in<br>securing image encryption                                                                      | 785–795 |

|                                                                                                                                                                                                           |         |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
| A. JULIAN, G. I. MARY, S. SELVI, M. RELE AND M. VAITHIANATHAN<br>Blockchain based solutions for privacy-preserving authentication and authorization in networks                                           | 797–808 |
| S. V. JOSHI, N. R. WAGH, J. R. R. KUMAR, D. DONGRE, N. RIZVI AND M. BHOWMIK<br>Mitigating DDoS attacks with an intrusion detection and prevention system based on 2-player Bayesian game theory           | 809–820 |
| I. DE, A. K. AGARWAL, B. BHUSHAN, A. KALNAWAT, P. MATHURKAR AND A. GARG<br>Implementing multi-factor authentication (MFA) for robust network access security                                              | 821–832 |
| J. MANTE-KHURPADE, M. DHOTAY, P. PATIL, S. KULKARNI, S. BUDHAVALÉ AND S. IKHAR<br>Enhancing data privacy in wireless sensor network using homomorphic encryption                                          | 833–842 |
| R. V. MAHADIK, S. C. HEMBADE, S. S. SORTE, D. KHUBALKAR, A. INGLE AND S. THORAT<br>Lightweight authenticated key management mechanism for enhanced data transmission in the Internet of Things framework  | 843–854 |
| U. B. AHER, A. A. BHOSLE, P. PALSODKAR, S. B. PATIL, N. KOUL AND P. MANGE<br>Secure data sharing in collaborative network environments for privacy-preserving mechanisms                                  | 855–865 |
| P. K. SRIVASTAVA, A. K. SRIVASTAVA, R. R. BUDARAJU, R. K. YELLAPRAGADA, S. ATTULURI AND S. MOHAPATRA<br>A holistic mathematical cyber security model in fog resource management in computing environments | 867–877 |
| H. S. OHAL, M. P. FATANGARE, M. S. AWARE, P. U. NEHETE, N. G. DONGRE AND P. M. KOTHOKE<br>Enhancing IoT security using lightweight key management with PRESENT for resource-constrained devices           | 879–888 |
| A. K. SINGHA, S. KUNDU, H. P. SINGH, L. S. SONGARE AND P. K. TIWARI<br>Measuring network security in the cloud : A roadmap for proactive defense                                                          | 889–902 |
| A. SANAP, S. S. MALWADE, R. BHOSALE, A. KARANDIKAR, A. A. BAKARE AND V. LANGOTE<br>Privacy-preserving authentication and authorization in networks using blockchain                                       | 903–914 |