WORKSHOP ON POST-QUANTUM CRYPTOGRAPHY-I

(Design and Analysis of Quantum Safe Public Key Cryptosystems)

13 April – 17 April 2024

Organized by

Department of Mathematics and Computing

Indian Institute of Technology (Indian School of Mines), Dhanbad-826004

Objective: The primary objective of organizing this workshop is to advance knowledge and skills in post-quantum cryptography, specifically focusing on code-based cryptographic techniques. The workshop aims to provide a comprehensive understanding of post-quantum cryptographic algorithms and their practical implementations. Participants will engage in hands-on learning, coding theory knowledge, and real-world case studies, ensuring a seamless transition from theory to practice. The workshop also emphasizes networking and collaboration, creating a platform for knowledge exchange and discussions on industry challenges and best practices. By the end of the workshop, participants will be prepared to address the cryptographic difficulties caused by quantum computing and contribute to ongoing research and innovation in this important field. Certificates of completion will be awarded, recognizing participants for their commitment to advancing their expertise in post-quantum cryptography.

Eligibility: All interested individuals, including researchers from the research laboratory, industry personnel, and faculty and students from recognised technical institutes and universities, are welcome to participate in this workshop. Students majoring in relevant subjects and those with a basic understanding of cryptography and coding who are keen to learn about the inner workings of post-quantum technology are encouraged to apply.

Boarding & Lodging: Boarding and lodging will be provided by the organizers. Accommodation will be provided to all the outstation participants in the student hostel of the institute. Those who want to stay in the IIT (ISM) guest house need to pay as per the rules, subject to availability.

Course Registration Fee:

Category	Course Fee (Indian Participants)	Course Fee (Foreign Participants)
UG/PG Students	Rs. 1500/-	USD 50
Research Scholars	Rs. 3000/-	USD 100
Faculty Members, Industry Personnels and Scientists	Rs. 5000/-	USD 150

The registration fee has to be paid through NEFT in the following given account on/before **10/04/2024:**
Name: Registrar IIT(ISM) Dhanbad
A/C: 0986101024892
IFSC: CNRB0000986
Bank name: CANARA BANK
Branch: SARAIDHELA, DHANBAD, JHARKHAND

Registration:
The registration form is given on the next page and can be downloaded from IIT(ISM) website: www.iitism.ac.in Please send the scanned copy of the registration form to abhay@iitism.ac.in

Dr. Abhay Kumar Singh (Coordinator)
Department of Mathematics and Computing
IIT(ISM), Dhanbad – 826 004
Email: abhay@iitism.ac.in
Phone No.: 8986696177

Dr. Pramod Kumar Kewat (Co- Coordinator)
Department of Mathematics and Computing
IIT(ISM), Dhanbad – 826 004
Email: pramodk@iitism.ac.in
Phone No.: 9471191836

Speakers (Tentative)
Prof. Udaya Parampalli, University of Melbourne, Australia
Prof. Patric Sole, Aix- Marseille University, France
Prof. Han Mao Kiah, NTU Singapore
Prof Vaneet Aggarwal, Purdue University, USA
Prof Eitan Yaakobi, Israel Institute of Technology, Technion, Israel
Prof Hai Q Dinh, Kent State University, OHIO, USA
Prof Nitin Saxena, IIT Kanpur, India
Prof Marco Baldi, Marche Polytechnic University, Italy
Prof Philip Gaborit, CNRS, France
Prof. Bimal Roy, ISI Kolkata, India
Prof Abhay K Singh, IIT(ISM) Dhanbad, india
Prof P K Kewat, IIT(ISM) Dhanbad, India
Prof Sourabh Mukhopadhyay, IIT Kharagpur, India

Tentative Areas to be covered are:

Coding Theory: Linear codes, cyclic codes, Quasi-cyclic codes, BCH codes, Reed-Solomon codes, Generalized Reed-Solomon codes, classical Goppa codes, Reed-Muller codes, LDPC and MDPC codes, QC-LDPC/MDPC codes, Encoding algorithms, General Decoding algorithms and their NP-completeness, Decoding algorithms of the specific codes, Information-Set Decoding algorithms..

Cryptography: Private-Key and Public-Key Encryption, IND-CPA and IND-CCA security, Key-Encapsulation Mechanism, Digital Signature Scheme, Zero-Knowledge Identification Scheme, Fiat-Shamir Transform.

Code-based Cryptography: McELliece Cryptosystem, Niederreiter cryptosystem, Alekhnovich Cryptosystem, GPT cryptosystem, NIST submissions: classic McEliece, BIKE and HQC, Hash and Sign, Zero-Knowledge Identification Scheme, Security analysis: Structural and non-structural attacks.

REGISTRATION FORM

Five Days Workshop on

ON POST-QUANTUM CRYPTOGRAPHY-I (Design and Analysis of Quantum Safe Cryptosystems)

Organized by Department of Mathematics and Computing, IIT(ISM) Dhanbad

13 April – 17 April 2024

1. Name: .....
(In Block letters)

2.Designation: .....

3. Institution / Organization: .....

4. Address for Communication: .....

5. Mobile No: .....

6. E-mail: .....

7. Gender: Male / Female / Other .....

8. Date of birth and Age: .....

9. Aadhar Card No: .....

10. Highest educational qualification with specialization: .....

11. Accommodation: Yes / No.

12. Local Participant: Yes / No.

13. Payment Details:

Bank Name :

NEFT Reference No:

Date of transfer:

Amount:

Payment receipt attached: Yes / No

DECLARATION

The information provided by me is true to the best of my knowledge. I agree to abide by the rules and regulations governing the organizing committee. If selected, I shall attend the program for the entire duration.

Place: **Signature of the Applicant with date**