IEEE
IITI Student Branch

Indian Institute of Technology Indore
organizes

Next-Gen Cybersecurity: Preparing for the Post-Quantum Era

In association with

Dept. of Computer Science and Engineering
Indian Institute of Technology Indore
and
IEEE Student Branch, IIT Indore

July 1-2, 2025

About IIT Indore

IIT Indore is in Indore, which takes pride in being the cleanest city in India. It was established in 2009 with the motto of 'ज्ञानम सर्वजनहिताय (Knowledge is for the well-being of everyone)'. It belongs to the IIT family, which is known to provide the best education in Engineering and Technology across India. IIT Indore has made relentless efforts to provide the best platform for education and research in several areas of science and technology.

About the Workshop

The Cybersecurity workshop is meant for skill development training on quantum-secure algorithms for encryption and authentication schemes. It is an effort to improve the research productivity of promising PG and PhD students from universities and colleges. This program aims to provide opportunities to acquire specialized research skills.

Course Benefits

- Certificates will be issued to the participants on successful completion of the course.
- Course materials and stationery/ consumable items will be provided to the participants based on availability.

About the Speakers

Experts from academia **(IITK, IITM, IISc, ISI, IIIT, RRU, UNSW Sydney, University of Waterloo)** will deliver talks and a few hands-on training sessions will be conducted.

Number of seats: 100

Brief description of the workshop

This workshop will make the participants familiar with the recent advances in Post Quantum Cryptography (PQC) primitives. With the advent of quantum computers, present-day Public Key Cryptography Primitives are rendered vulnerable. This will compromise the confidentiality and integrity of digital communications on the Internet and elsewhere. This workshop will focus on how to develop cryptographic systems pertaining to encryption and authentication that are secure against both quantum and classical computers, and can interoperate with existing communications protocols and IoT networks.

Targeted Participants

BTech/MTech/MS/Ph.D. students/faculty members of ECE/CSE/EE or any other specialization relevant to the area of IoT, Cybersecurity, Cryptography, Hardware Security, Quantum Computing, and other relevant areas.

Registration fee:

Indian Student (UG): ₹ 250
Indian Student (PG/PhD): ₹ 500
Indian Faculty: ₹ 1000
Industry Professional: ₹ 2000

IEEESTUDENTBRANCH

Make payment through QR code.

Limited seats are available.

Registration link: https://docs.google.com/forms/d/1twE2KseJE3-vvaWBD3DL6jEkGh92KfnI5FW6-nheAKI/edit
Last date for Registration: June 30, 2025 (12pm, IST).

Organizing Chair:

Dr. Bodhisatwa Mazumdar
Associate Professor
Department of CSE, IIT Indore

Contact: pqcw@iiti.ac.in

Workshop Schedule

Day 1: PQC Foundations and Applications

1. **Keynote Talk "Why PQC?":** *Prof. Bimal Kumar Roy*, TCG CREST and ISI Kolkata.
2. **SIDH is Dead: Not Isogeny-Based Cryptography:** *Dr. Surbhi Shaw*, IISc Bangalore.
3. **Multivariate and Code-Based Cryptography: Construction, Current Landscape, and Challenges:** *Dr. Jayashree Dey*, IIT Madras.
4. **Lattice-Based Cryptography:** *Dr. Meenakshi Kansal*, RRU, Gandhinagar.
5. **IoT Security in Post-Quantum Era**: *Dr. Subhra Mazumdar* *and* *Dr. Ayan Mondal*, IIT Indore.

Day 2: PQC Foundations and Applications

6. **Concrete Security Analysis of Lattice-based Reductions:** *Dr. Subhadip Singha*, University of Waterloo.
7. **Post Quantum Cryptography for Blockchains:** *Dr. Sushmita Ruj*, UNSW Sydney.
8. **Efficient Hardware Implementation of Lattice-Based Cryptographic Algorithms:** *Dr. Debopriya Basu Roy*, IIT Kanpur.
9. **TBD:** *Dr. Dibyendu Roy, IIIT Vadodara (Gandhinagar Campus).*
10. **Hash-based Signature Schemes :** *Dr. Bodhisatwa Mazumdar*, IIT Indore.
11. **Tutorial/Evaluation: TBD.**