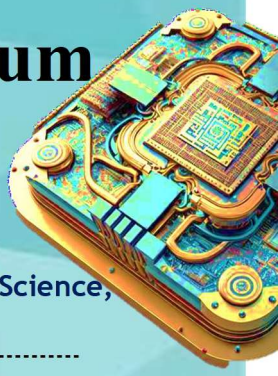
Quantum Threats & Post-Quantum Defences Workshop



(28-29 November 2024)

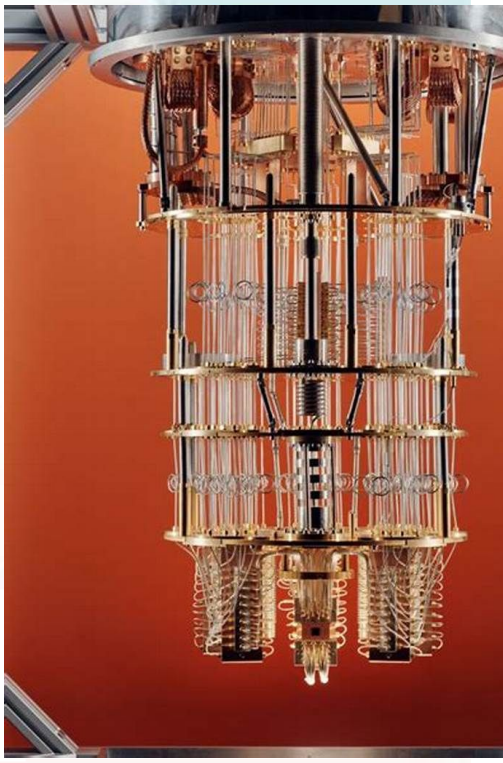
Conducted by CR Rao Advanced Institute of Mathematics, Statistics and Computer Science, University of Hyderabad Campus, Prof.CR Rao Road, Hyderabad-500054.

ABOUT CR RAO AIMSCS

CR Rao AIMSCS is engaged in cutting edge research and academics in the areas of mathematics, statistics, computer science and interdisciplinary fields, and provides a forum for national and international experts from different fields to meet and address problems of mutual interest. This is done through Centers of Excellence in (1) Mathematical Sciences, (2) Statistics (3) Computer Science and its allied areas such as Data Science, Cyber Security, Artificial Intelligence, Blockchain technology, Wireless Communication & IoT security, and Quantum & post-Quantum technology. The institute's mission includes advancing mathematical sciences through workshops, conferences, and courses, supporting doctoral research, and providing consultancy to researchers, government, and industry.

ABOUT WORKSHOP

The Quantum Threats & Post-Quantum Defenses Workshop focuses on addressing the emerging challenges posed by quantum computing to current cryptographic systems and exploring resilient solutions. It serves as a platform for researchers, industry experts, and policymakers to discuss quantum threats to traditional cryptography and to develop strategies for post-quantum cryptographic defenses. The program includes sessions on theoretical advances, practical implementations of post-quantum algorithms, and strategies for transitioning to quantum-resistant systems. It also emphasizes collaboration and innovation to ensure secure communication in a quantum-enabled future.



TOPICS TO BE COVERED

- **PQC: Encryption scheme based on LWE**
- **Lattice based Signatures**
- **Quantum Cryptanalysis**
- **Quantum Systems: QRNG, QKD**
- **Implementations & Demos**

Coordinator: Mrs Neelima Jampala, neelima.jampala@crraoaimscs.res.in

Quantum Threats & Post-Quantum Defenses Workshop
28-29, Nov 2024

28-Nov-2024

Time	Topic	Speaker
9:30 am – 10:00	**Inaugural session**	
10.00 am –11.15 am	Introduction to SIS and LWE problems (ring and module variants) Discrete gaussian distribution over lattice and rejection sampling	Dr. Mahavir Jhawar Ashoka University
11.15 am – 11.45	**Tea Break**	
11.45 am – 1.00 pm	Encryption scheme based on LWE and its variants	Dr. Mahavir Jhawar Ashoka University
1.00 pm – 2.00 pm	**Lunch**	
2.00 pm – 3.15 pm	Quantum Cryptography	Dr Kannan Srinathan, IIIT Hyderabad
3.15 pm – 3.45 pm	**Tea Break**	
3.45 pm – 5.00 pm	Quantum Cryptanalysis of PKE using Shor's algorithm (Attack on RSA)	Dr Kannan Srinathan, IIIT Hyderabad

29-Nov-2024

Time	Topic	Speaker
10.00 am –11.15 am	Signature scheme based on lattice (Hah-and-sign Fiat shamir with Abort)	Dr. Mahavir Jhawar Ashoka University
11.15 am – 11.45	**Tea Break**	
11.45 am – 1.00 pm	Advancements in True Random Number Generators with Quantum Entropy Sources	Col. Kapil Jaiswal, Quantum AI
1.00 pm – 2.00 pm	**Lunch**	
2.00 pm – 3.15 pm	Review of QKD Technologies & Experimentation Challenges	Col. Kapil Jaiswal, Quantum AI
3.15 pm – 3.45 pm	**Tea Break**	
3.45 pm – 5.00 pm	Discussion and Conclusions	