NATIONAL INSTRUCTIONAL WORKSHOP on CRYPTOLOGY : LATTICE BASED CRYPTOGRAPHY (NIWC 2024)

(1-5 July 2024)

Organized by

Department of Mathematics

Motilal Nehru National Institute of Technology Allahabad

&

Cryptology Research Society of India

Venue

Motilal Nehru National Institute of Technology Allahabad, Prayagraj-211004 (U.P.)

ABOUT THE INSTITUTE

Motilal Nehru National Institute of Technology, Allahabad (MNNIT) was established as one of the seventeen Regional Engineering Colleges of India in the year 1961. On June 26, 2002 MNREC was transformed into the National Institute of Technology fully funded by Government of India. The Institute now offers nine B.Tech., twenty four M.Tech. Degree Programmes, MCA, MBA, M.Sc. (Mathematics and Scientific Computing) and Master of Social Work (M.S.W.) programmes also register candidates for the Ph.D. degree. The Institute has been recognized by the Government of India as one of the centers for the Quality Improvement Programme for M.Tech. and Ph.D. It is an institute with total commitment to quality and excellence in academic pursuits and is among one of the leading institutes in India.

ABOUT THE DEPARTMENT

The Department of Mathematics came into existence w.e.f., 1st April 2003; prior to this, it constituted a section of the Department of Applied Sciences & Humanities. The department offers core courses at the undergraduate level and several advanced courses at post graduate level. The department also enrolls candidates for the Ph.D. programme. There is widespread interaction between the Mathematics department and various Engineering departments in the field of teaching and research. The Department of Mathematics started a full-time M.Sc. in Mathematics & Scientific Computing program since 2008 and admission is done through JAM (Joint admission in M.Sc.) conducted by IIT.

ABOUT CRYPTOLOGY RESEARCH SOCIETY OF INDIA

Set up in 2001, CRSI is a scientific assembly made up of academicians, researchers, specialists, students, and institutions who are interested in promoting the science and technology of Cryptology and Data security and related theory and applications in India. The CRSI has been founded for:

- Supporting and promoting research activities in cryptology and data security in India.
- To arrange lectures, discussions, workshops, seminars, conferences, etc. to motivate and guide the young Indian researchers in the field of cryptology and data security.
- Organizing the annual events INDOCRYPT- the International Conference on Cryptology and Security, the National Workshop on Cryptology and National Instructional Workshop on Cryptology.

OBJECTIVE OF THE WORKSHOP

Cryptology (mathematical techniques related to aspects of information security and cryptanalysis) is developing rapidly and its popularity is increasing daily in information sciences, particularly in network, banking, mail, and information security-related activities. CRSI (Cryptology Research Society of India) organizes this workshop every year, in cooperation with an Indian institution, to reach students nationwide and provide them with a platform to explore the opportunities in Cryptology and related fields of study and research. This workshop aims to systematically expose the students and faculty of Mathematics & Engineering, as well as industry executives, to the basic understanding of Cryptology, post-quantum cryptography, network security, and other related information security issues and applications. Lattice-based cryptography is an important candidate to withstand against quantum computers. Participants will be benefited by understanding the basics of hard lattice problems and designing cryptographic primitives with the security relying on hard lattice problems.

ELIGIBILITY

Students, Faculty, and Industry Executives.
Participants familiar with the area of Algebra / Number Theory / Cryptography / Information Security are preferred.

RESOURCE PERSONS

Resource persons from various IITs, ISI, DRDO and other reputed organizations will be delivering the expert lectures.

List of tentative speakers are

- Prof. Bimal Roy, ISI Kolkata, General Secretory CRSI
- Dr. N Rajesh Pillai, Scientist H, Director SAG, DRDO New Delhi
- Dr. Bhupendra Singh, Scientist F, CAIR, DRDO, Bangalore
- Dr. Indivar Gupta, Scientist F, SAG DRDO, New Delhi
- Dr. Dhananjay Day, IIIT Lucknow
- Dr. Angshuman Karmakar, IIT Kanpur
- Dr. Vishal Saraswat, Bosch Global Software Technologies Pvt. Ltd. (BGSW), Bengaluru, India.
- Dr. Rajeev Anand Sahu, Bosch Global Software Technologies Pvt. Ltd. (BGSW), Bengaluru, India.
- Dr. Mahaveer Jhawar, Ashoka University
- Dr. Shashank Singh, IISER Bhopal
- Dr. Sonika Singh, CMP Degree College, University of Allahabad
- Prof. Shiv Datt Kumar, MNNIT Allahabad
- Dr. Sahadeo Padhye, MNNIT Allahabad
- Dr. Shashank Srivastava, MNNIT Allahabad

TOPICS TO BE COVERED

- Mathematical foundation to Cryptography
- Overview of Symmetric and Asymmetric key Cryptography
- Cryptography in Cyber Security and Network Security
- Overview of Code-based, Hash-based, Multivariate-based, and Lattice-based PQC
- Lattice hard problems: CVP, SVP, SIS, LWE,LWR etc.
- Reductions of Lattice Problems
- Lattice-based Encryptions
- Lattice-based Digital Signatures
- Cryptographic Primitives using LWE
- NIST finalist of Lattice-based Schemes
- Fully Homomorphic Encryption
- Secret Sharing and Multiparty Computation

REGISTRATION DETAILS

Industry Executive/Officer/Faculty : ₹ 3540 /- *
Student / Research scholar : ₹ 2360 /- *

* 18% GST included

(50% of Registration fee is waived for CRSI members)

Registration fee may be paid through online/NEFT/UPI

For Registration and Payment 👉 Click Here

Last Date of Registration : 15-05-2024

Note - Limited seats available. Selection is based on first come first serve basis.

BOARDING & LODGING

Registration fee includes meals during the workshop. Lodging of the participants will be arranged at the institute guest house/hostels on payment basis.

ADVISORY COMMITTEE

- Prof. R S Verma, Director MNNIT Allahabad
- Dr. N. Rajesh Pillai, Scientist-H, Director SAG, DRDO New Delhi
- Prof. Bimal Roy, ISI Kolkata, General Secretary of CRSI
- Prof. R Balasubramanian, IMSC Chennai, President of CRSI
- Prof. L K Mishra, Dean Academic, MNNIT Allahabad
- Prof. H S Goyal, Dean P and D, MNNIT Allahabad
- Prof. R S Yadav, MNNIT Allahabad
- Prof. O P Vyas, IIIT Allahabad
- Prof. R P Shukla, Allahabad University
- Prof. Ramji Lal, Former Professor, Allahabad University
- Dr. Brajesh Sharma, Allahabad University

ORGANIZING COMMITTEE

- Prof. R S Verma (Patron)
- Prof. Shiv Datt Kumar (Chairman)
- Dr. Sahadeo Padhye (Convener)
- Prof. Pitam Singh (Coordinator)
- Dr. Gorakh Nath, Head, Mathematics Dept.
- Dr. Bhupendra Singh, CAIR, DRDO, Bangalore (Mentor CRSI & Coordinator)
- Dr. V R Komma, MED
- Prof. Pankaj Srivastava
- Prof. Mukesh Kumar
- Dr. Pramod Kumar Yadav
- Dr. B Vasu
- Dr. Surabhi Tiwari
- Dr. Supriya Yadav
- Dr. Shubham Gupta
- Dr. Prashant Majee
- Dr. Naren Bag

STUDENT COMMITTEE

- Mr. Ramakant Kumar
- Mr. Rohitkumar R Upadhyay
- Mr. Shubham Khurana
- Mr. Jitender
- Mr. Dev Karan Singh
- Mr. Tushar Singh
- Mr. Aneesh Kumar
- Ms. Nitisha Yadav
- Ms. Sonu Bai
- Ms. Shristi Srivastava
- Ms. Ritika Omar

CONTACT DETAILS

For any query, one may contact to

Dr Sahadeo Padhye
Convener, NIWC-2024
Department of Mathematics
Motilal Nehru National Institute of Technology Allahabad
Prayagraj - 211004

Email: niwc2024@gmail.com
Contact- +91-9453256043