



Institute for Development and Research in Banking Technology

(Established by Reserve Bank of India)

Castle Hills, Road No. 1, Masab Tank, Hyderabad-57, India.

e-Programme on

INTRODUCTION TO POST-QUANTUM CRYPTOGRAPHY

June 21 – 24, 2022

Introduction

The advent of quantum computing threatens to break most popular public-key cryptosystems such as RSA and ECC, which are currently in use. Post-quantum cryptography is an alternative to classical public-key cryptography because it is secure against quantum attacks and quantum secure. Post-quantum cryptography refers to develop cryptographic systems that are resistant to attacks by both classical and quantum computers, to keep information assets secure even after a large-scale quantum computer has been built. This program discusses the different families of post-quantum cryptography.

Objective

This program aims to offer a platform for the participants learn about different post-quantum cryptography algorithms and their applicability in banking sector.

Contents

- Introduction to Post-quantum cryptography
- Lattice based Cryptography
- Lattice-based Zero-Knowledge Proofs
- Code-based Cryptography
- Isogeny-based Cryptography
- Hash-based Cryptography
- Multivariate Cryptography

Mode of Teaching

Online teaching plus learning inputs through reading material, videos, webinars, assignments, quizzes, online interactions and clarifications. Each e-Programme will have four live webinars and course material will be made available in advance for study.

Who Can Participate?

Officers of Banks / Financial Institutions / Insurance Sector who work in Development team including developers, testers, architects, DevOps engineer, managers, and support engineers.

End Use:

After completion of this program, the participants will understand post-quantum cryptography algorithms and how to implement these techniques in banking sector to secure information and data.

Programme Coordinator:

Dr. P. Syam Kumar, Assistant Professor, IDRBT

e-mail: psyamkumar@idrbt.ac.in

Fees:

For Indian Participants

- RRBs & Coop Banks: Rs. 17,700/- (Rs. 15,000/- + 18% GST)
- All Other Banks & Financial Institutions: Rs. 23,600/- (Rs. 20,000/- + 18% GST)

For International participants

- US \$ 310 (per participant, All inclusive)

Bank Account Details for Remittance of Fees

The fees for this e-programme can be remitted to the following accounts:

For Indian Participants

Account Name : IDRBT
Bank & Branch : Axis Bank Limited, Humayun Nagar, Mehdiapatnam, Hyderabad
Account No. : 426010100018823
MICR Code : 500211012
IFSC Code : UTIB0000426

For International participants

Receiver's Correspondent Bank : JP Morgan Chase, New York, USA
Swift Code : CHASUS33XXX
Fed Wire Routing Number : ABA 021000021
Beneficiary Bank & Branch : Axis Bank Ltd., Mumbai, India
Account Number : 0011407376
Beneficiary Bank Swift Code : AXISINBB

Ultimate Beneficiary

Account Name : IDRBT
Customer ID : 030021632
Account No. : 426010100018823
Bank & Branch : Axis Bank Ltd., Jubilee Hills, Hyderabad, India. (AXISINBB030)

Nominations

Banks may nominate any number of participants to these e-Programmes, which may be accepted on a first-cum-first-served basis. While nominating, please provide the details of the participants (Name, Designation, Bank, Mobile No/Phone No, email address, fees billing address, GST No. of the Bank).

Apart from nominations by banks, staff members of banks can self-nominate themselves for these e-Programmes by providing their employee credentials and paying the programme fee latest by **June 20, 2022**.

How to Register

The nominations for these e-Programmes, and queries if any, may please be sent to eprogram@idrbt.ac.in. Please visit <https://www.idrbt.ac.in/eprogrammes> for more details about these programmes.

e-Programmes in June 2022

S. No.	Name of the e-Programme	Date	e-Programme Coordinator	Last Date for Nomination
1	Privacy Preserving Machine Learning for Banks	06 – 09	Dr. V. Ravi	June 03, 2022
2	Distributed Ledger Technology and Banking Applications	06 – 09	Dr. N. V. Narendra Kumar	June 03, 2022
3	5G Use Cases and IoT Applications for Banks	06 – 10	Dr. V. N. Sastry	June 03, 2022
4	Threats to Digital Payment Ecosystem	07 – 10	Dr. Susmita Mandal	June 06, 2022
5	Technologies for Financial Inclusion	07 – 10	Dr. M.V.N.K. Prasad	June 06, 2022
6	Emerging AI/ML Technologies	13 – 16	Dr. Mridula Verma	June 10, 2022
7	Workshop on Registration Authority Operations	14 – 17	Dr. N. P. Dhavale	June 13, 2022
8	Privacy and Security Risks in Machine Learning	14 – 17	Dr. Rajarshi Pal	June 13, 2022
9	RBI Guidelines on Cyber Security	20 – 23	Dr. Dipanjan Roy	June 17, 2022
10	Introduction to Containers	21 – 24	Dr. P. Syam Kumar	June 20, 2022
11	Targeted Attacks - Detecting in Early Stages	21 – 24	Dr. B. M. Mehtre	June 20, 2022
12	API Development	Jun 28 – Jul 01	Dr. V. Radha	June 27, 2022