



— LABORATORY PROFILE —

POST-QUANTUM & AI
SECURITY LAB

PQS

Research and national outreach in post-quantum cryptography — code-based encryption and signature schemes, blockchain security, and the security of connected systems.

OUTREACH ACTIVITIES

RECORD OF ENGAGEMENTS

00 · WORKSHOP ORGANISED

FROM	TO	PROGRAMME	COORDINATOR	BENEFICIARY / VENUE	PARTICIPANTS
26.05.2025	30.05.2025	Cybersecurity and Its Practices	Dr. Debasish Bera	Barrackpore Police Commissionerate, West Bengal, India	25

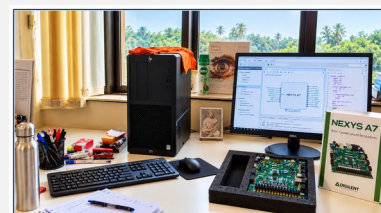
01-05 · INVITED TALKS & RESOURCE-PERSON ENGAGEMENTS

01	"Code-based Post-Quantum Cryptosystem: Encryption and Signature" National Instructional Workshop on Cryptology: Code-based Cryptography (NIWC-23) · Dept. of Mathematics, IIT (BHU)	05-07 July 2023 INVITED TALK
02	"Code-based Post-Quantum Cryptosystem" Intl. Conference on Quantum Information and Quantum Technology (QIQT-2023) · organised by IISER Kolkata (online)	02 June 2023 INVITED TALK
03	"Code-based Signature Schemes" CEP on Post-Quantum Cryptography · organised by CAIR, DRDO, Bangalore (mixed mode)	13-17 June 2022 INVITED TALK
04	"Blockchain and Post-Quantum Cryptography: Code-based Cryptography" Online FDP on Cyber Security and Blockchain Technology · Dept. of CSE, IIIT Bhagalpur	24 Dec. 2021 INVITED TALK
05	Resource person · "Internet of Things with Blockchain — Applications and Challenges" Faculty Development Programme · Velalar College of Engineering, Erode, Tamil Nadu	01-06 Feb. 2021 FDP

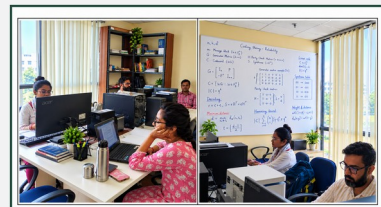
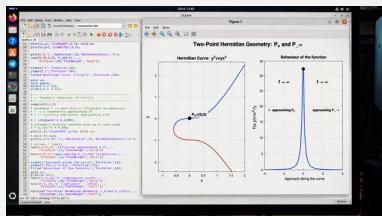
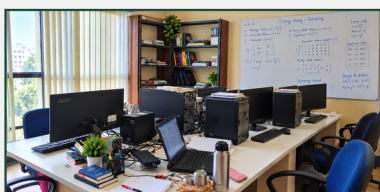
PQC HARDWARE EQUIPMENTS

FPGA PROTOTYPING PLATFORM

01	Digilent Nexys A7 · Artix-7 FPGA Board Artix-7 based FPGA development board for hardware prototyping of post-quantum cryptographic designs
02	Computer Systems Host computer systems for FPGA design entry, simulation and synthesis, connected to the Nexys A7 board



NEXYS A7 · ARTIX-7 FPGA WORKBENCH



LAB COORDINATORS

Dr. Debasish Bera

Post-Quantum Security (PQS) Lab · IIIT Kalyani

Dr. Bhaskar Biswas

Post-Quantum Security (PQS) Lab · IIIT Kalyani

FOCUS AREAS

Code-based cryptography
Digital signatures
Blockchain security
IoT & network security
Quantum-safe migrationSCAN FOR MORE
INFORMATION



LAB 01 — SPONSORED RESEARCH LABORATORY

PQC & AI LAB

Post-Quantum Cryptography Laboratory



ONGOING PROJECT

Design and Development of Post-Quantum Cryptography (PQC) Algorithms and Security Analysis — code-based

SPONSOR

TTDF, TCOE India, Department of Telecommunications, Government of India

SANCTIONED COST

₹ 109.28 L

TOTAL SPONSORED FUNDING

₹ 263.22 L

Four projects · Government of India agencies

ONGOING

₹ 109.28 L

COMPLETED

₹ 153.94 L

COMPLETED PROJECTS

THREE · ₹ 153.94 L

01	Development of code-based PQC algorithms and its security analysis Sponsored by CAIR, DRDO, Bangalore	₹ 49.98 L
02	Development of code-based PQC signature scheme and its security analysis Sponsored by CAIR, DRDO, Bangalore	₹ 48.96 L
03	Development of cryptanalytic tools for Hamming-metric post-quantum schemes, and design of selected post-quantum code-based cryptosystems Sponsored by SAG, DRDO, New Delhi	₹ 55.00 L

SANCTIONED COST BY PROJECT

₹ IN LAKH

PQC algorithms & security analysis TTDF · TCOE · DoT — ongoing	109.28
Cryptanalytic tools, Hamming metric SAG, DRDO — completed	55.00
Code-based PQC algorithms CAIR, DRDO — completed	49.98
Code-based signature scheme CAIR, DRDO — completed	48.96

SPONSORING AGENCIES

TTDF · TCOE India

Department of Telecommunications,
Govt. of India

CAIR, DRDO

Bangalore

SAG, DRDO

New Delhi

CO-ORDINATORS

Dr. Bhaskar Biswas

bhaskar@iiitkalyani.ac.in

Dr. Debasish Bera

debasish@iiitkalyani.ac.in

RESEARCH FOCUS

- Code-based encryption schemes
- Code-based digital signatures
- Cryptanalytic tooling, Hamming metric
- Security analysis & proofs
- Quantum-safe migration



Scan for institute
and lab information
www.iiitkalyani.ac.in

PATRON

Director, IIIT KALYANI
Kalyani, Nadia, West Bengal

LAB MEMBERS

PH.D. RESEARCH SCHOLARS

SUPERVISOR Dr. Debasish Bera

5 SCHOLARS

SCHOLAR	DEPARTMENT	FELLOWSHIP / CATEGORY
Soumik Biswas	ECE	Project JRF
Sourabh Biswas	CSE	Project-JRF
Saptaparna Kundu	CSE	Visvesvaraya PhD Scheme
Asim Sarkar	CSE	T.A
Aniket Deb	CSE	Project JRF

SUPERVISOR Dr. Bhaskar Biswas

1 SCHOLAR

SCHOLAR	DEPARTMENT	FELLOWSHIP / CATEGORY
Sayantan Chatterjee	CSE	Project SRF

B.TECH / M.TECH INTERNS Looking for interested candidates to join us in the lab