acm India Council

IITB TRUST LAB
DIGITAL : SECURE : RESPONSIBLE

ACM SUMMER SCHOOL ON CRYPTOGRAPHY

REPORT

2025

A summer of ideas, insights, and innovation.

IIT BOMBAY TRUST LAB

This summer school brought together students and researchers from across the nation, to explore the foundations and frontiers of modern cryptography.

2 June

Perfect Security & Hardness Assumptions
Instructor: Aishwarya T (IIT Madras)

The opening day set a strong foundational tone by introducing participants to the fundamental question: what does it mean for a system to be secure? The instructor guided the cohort through the evolution of cryptographic thinking—from ancient ciphers like the Caesar and Vigenère, to the formal notion of perfect secrecy.

Through the lens of Shannon's work, participants explored the one-time pad, and how this method of encryption is perfectly secure. These classical examples served not only as historical context but also as springboards into the rigorous definitions and limitations of perfect security.

A theoretical exercise session followed, where students worked through formal models of adversaries and security guarantees, setting the stage for deeper explorations in the coming days. This initial day ensured all attendees—regardless of prior exposure—had a conceptual base to understand modern cryptographic tools and methods.

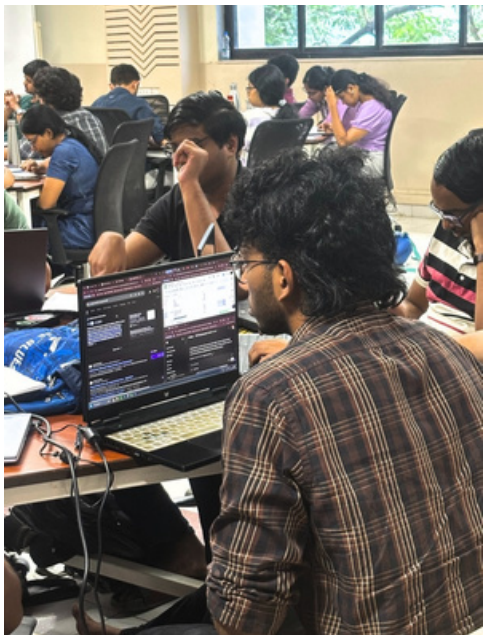
3 June

Secure Communication I.a – PRG, PRF & Semantic Security
Instructor: Aishwarya T (IIT Madras)

This session introduced the core building blocks of modern cryptography: pseudorandom generators (PRGs) and pseudorandom functions (PRFs). Participants learned how these primitives are used to achieve semantic security, ensuring that encrypted messages reveal no meaningful information to adversaries.

The session also explored how to extend encryption securely to multiple messages, laying the groundwork for robust symmetric-key encryption schemes.

Lab: Symmetric Key Encryption Tutorial (OpenSSL) Instructors: Ravi Prakash & Priyanshu Singh (IIT Bombay)



This hands-on lab introduced students to OpenSSL, a widely used open-source toolkit for implementing cryptographic protocols.

Participants learned to perform encryption and decryption using symmetric key algorithms, focusing on block ciphers, key management, and modes of operation. The session emphasised practical skills, bridging theoretical concepts with real-world cryptographic tools.

4 June

Structured Hardness & Lattices
Instructor: Rajendra Kumar (IIT Delhi)

This session introduced mathematical lattices and the Learning With Errors (LWE) problem, a cornerstone of post-quantum cryptography. Students explored how structured hardness assumptions like LWE differ from generic ones, and why they remain hard even for quantum computers.

The session also covered short-integer solutions and basic cryptographic constructions built from LWE, highlighting their relevance in designing future-proof encryption systems.

Secure Communication II – Public-Key Encryption
Instructor: Rajendra Kumar (IIT Delhi)

This session focused on asymmetric encryption, key generation, and semantic security in the public-key setting. It explained how confidentiality is maintained without shared keys. RSA and ECC, two types of PKE, are used in secure emails and digital certificate, and are crucial for designing secure digital ID systems.

The session focused on the principles of public-key encryption, highlighting how it differs from symmetric-key schemes. Core constructions like RSA and LWE-based encryption were discussed, along with their security assumptions. In the exercise session, students explored theoretical attacks on RSA and applied their understanding of LWE to analyze post-quantum security.

5 June

Lab: PKE Tutorial (OpenSSL & OpenSSH)
Instructors: Archisman Dutta & Adwaiya Srivastav (IITB Trust Lab)

Hands-on labs included generating key pairs, encrypting messages, and understanding SSH authentication via public keys. It demystified the tools developers use for secure system access. Setting up GitHub or server access with SSH keys mirrors these lessons.

Using OpenSSH and OpenSSL, students learned to implement key cryptographic protocols in practice. The lab focused on generating key pairs, encrypting data, and understanding how public-key authentication works in secure communication tools like SSH.

Secure Communication I.b – MACs, Signatures, Hash Functions
Instructor: Rajendra Kumar (IIT Delhi)

This session focused on ensuring data integrity and authenticity using cryptographic tools like Message Authentication Codes (MACs), digital signatures, and hash functions. Students examined key properties such as collision resistance and unforgeability, learning how these tools protect messages from tampering and impersonation in real-world systems.

6 June

Secure Communication III – Homomorphic Encryption Instructor: Monosij Maitra (IIT Kharagpur)

This session focussed on how Fully Homomorphic Encryption (FHE) allows computations on encrypted data without decrypting it. FHE is crucial as it enables privacy-preserving data analysis, so places like hospitals which deal with highly sensitive information can compute on encrypted patient data without ever seeing it.

Lab: Signatures & Hash Functions Instructors: Archisman Dutta & Adwaiya Srivastav (IITB Trust Lab)

A practical session to implement and verify digital signatures, hash integrity checks, and understand potential attack vectors. Students worked with code to experience how cryptographic integrity works. Students used signature tools to verify file downloads, simulating how secure package managers like `apt` and `pip` validate updates.

7 June

Advanced Primitives Instructor: Monosij Maitra (IIT Kharagpur)

This session explored advanced cryptographic primitives, including functional encryption and attribute-based encryption. These emerging tools enable fine-grained access control, allowing decryption only under specific conditions or user attributes. The lecture highlighted their potential in privacy-preserving systems and secure data sharing.

To keep the session engaging, the instructor included in-lecture exercises with small prizes for correct answers, encouraging active participation and reinforcing key concepts in real time.

9 June

Proof systems I: IP, ZK
Instructor: Vineet Nair (Arithmic Labs)

This session introduced the concept of interactive proofs, where a verifier interacts with a prover to be convinced of a statement's validity. Students learned about languages, relations, and how interactive protocols expand the power of verification beyond static proofs. Foundational examples like the sum-check protocol and matrix multiplication proof were covered to illustrate the core ideas.

The session also touched on proofs in the random oracle model and traced the development of succinct proofs, leading to modern SNARKs (Succinct Non-interactive Arguments of Knowledge). The historical context helped participants understand the motivation behind zero-knowledge and verifiable computation.

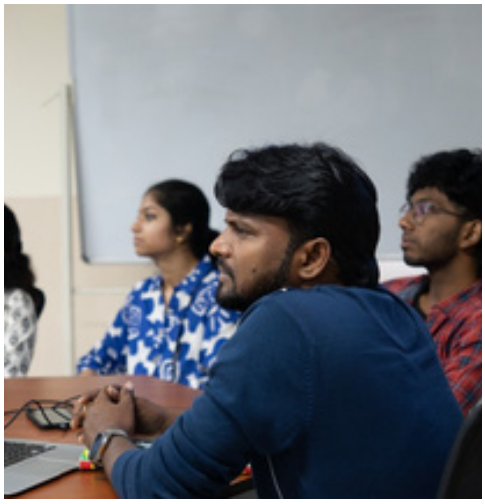
Also covered were foundational concepts in interactive proofs and Zero-Knowledge Proofs (ZKPs), which allow verification without revealing secrets.

Lab: Fully Homomorphic Encryption
Instructor: Vineet Nair (Arithmic Labs)

A lab component introduced students to Fully Homomorphic Encryption (FHE), allowing them to experiment with performing computations on encrypted data—an emerging area linked closely with verifiable and privacy-preserving protocols.

10 June

Proof Systems II – SNARGs
Instructor: Saravanan Vijayakumaran (IIT Bombay)



This session focused on Succinct Non-Interactive Arguments (SNARGs), which offer short, efficiently verifiable proofs—crucial for scaling zero-knowledge systems. Students examined how SNARGs balance proof size, verification speed, and security, making them practical for applications like blockchain and privacy-preserving protocols.

Lab: Circom for ZK Circuits
Instructor: Saravanan Vijayakumaran (IIT Bombay)

In the accompanying lab, participants used Circom, a domain-specific language for writing zero-knowledge circuits. They built and debugged basic ZK applications, gaining hands-on experience with real-world tools used in privacy-focused cryptographic systems.

11 June

Basics of MPC
Instructor: Ashish Choudhury (IIIT Bangalore)

This session introduced the basics of Secure Multi-Party Computation (SMPC), which enables parties to jointly compute a function over their private inputs without revealing them. Students learned about secret-sharing techniques, focusing on Shamir's secret sharing, and how they form the basis for MPC protocols.

The lecture covered key protocols like BGW and Maurer's protocol, which use secret-sharing to securely evaluate functions. It concluded with an introduction to Yao's garbled circuits, a powerful technique for two-party computation. These foundational tools gave participants insight into how privacy can be preserved even in collaborative computation.

Lab: BGW and Yao's garbled circuits
Instructor: Bhavadharini V (IITB Trust Lab)

Participants worked together to implement and analyze protocols like BGW and Yao's garbled circuits, reinforcing their understanding of secure computation.

These hands-on activities emphasised teamwork, protocol design, and real-world problem-solving in privacy-preserving settings. The session served as a practical wrap-up, allowing students to consolidate their learning and engage with the material more deeply.

12 June

Applied MPC
Instructor: Nishat Koti (Aztec Labs)

This session explored real-world applications of Multi-Party Computation (MPC), demonstrating how theoretical protocols are adapted for practical use. Topics included privacy-preserving machine learning, secure shuffling, anonymous broadcasting, and secure graph computation. Through these examples, students saw how MPC enables collaborative computation without sacrificing privacy.

Lab: MPC Protocol
Instructor: Nishat Koti (Aztec Labs)

In the accompanying lab, participants designed simple MPC protocols tailored to specific use cases such as voting, finance, and auctions. The session also discussed practical deployment challenges and optimisations, bridging the gap between academic research and real-world privacy-preserving technologies.

13 June

Basics of Blockchain Technology
Instructor: Nitin Singh (IBM Research)

This session introduced the fundamentals of blockchain technology and its deep ties to cryptography. Students learned how blockchains function as distributed ledgers and how cryptographic tools like hash functions, digital signatures, and consensus mechanisms ensure their security and integrity.

The session also explored how cryptography enables privacy within blockchain systems, including the use of techniques like zero-knowledge proofs and secure transactions. It provided a high-level view of how cryptographic primitives are applied in real-world decentralized systems.

IITB TRUST LAB

DIGITAL : SECURE : RESPONSIBLE

acm India Council

ACM SUMMER SCHOOL ON CRYPTOGRAPHY

A summer of ideas, insights, and innovation.