ACM Summer School IITB Trust Lab 2025

DAY 1 — 02 June 2025

Welcome to ACM Summer School IIT Bombay Trust Lab 2025 — 09:00AM 09:30AM
Chethan Kamath (IITB) & Venkata Koppula (IITD)

Perfect security and its limitations, hardness assumptions, modelling adversaries — 09:30AM 11:00AM
Aishwarya T (IITM)

Tea Break — 11:00AM to 11:15AM

Perfect security and its limitations, hardness assumptions, modelling adversaries — 11:15AM 12:45PM
Aishwarya T (IITM)

Lunch Break — 12:45PM to 2:00PM

Perfect security and its limitations, hardness assumptions, modelling adversaries — 02:00PM 03:30PM
Aishwarya T (IITM)

Tea Break — 03:30PM to 04:00PM

Group exercise — 04:00PM 05:00PM
Bhavadharini V (Trust Lab)

DAY 2 — 03 June 2025

Secure communication I.a: PRG & one-time semantic security (SS), PRF & many-time SS — 09:30AM 11:00AM
Aishwarya T (IITM)

Tea Break — 11:00AM to 11:15AM

Secure communication I.a: PRG & one-time semantic security (SS), PRF & many-time SS — 11:15AM 12:45PM
Aishwarya T (IITM)

Lunch Break — 12:45PM to 2:00PM

Lab sessions: SKE tutorial (OpenSSL) — 02:00PM 03:30PM
Ravi Prakash and Priyanshu Singh (IITB)

Tea Break — 03:30PM to 04:00PM

Lab sessions: SKE tutorial (OpenSSL) — 04:00PM 05:00PM
Ravi Prakash and Priyanshu Singh (IITB)

DAY 3 — 04 June 2025

Structured hardness assumptions, basic lattices, LWE — 09:30AM 11:00AM
Rajendra Kumar (IITD)

Tea Break — 11:00AM to 11:15AM

Structured hardness assumptions, basic lattices, LWE — 11:15AM 12:45PM
Rajendra Kumar (IITD)

Lunch Break — 12:45PM to 2:00PM

Secure Communication II: Public-key encryption (PKE) — 02:00PM 03:30PM
Ravi Prakash and Priyanshu Singh (IITB)

Tea Break — 03:30PM to 04:00PM

Group exercise — 04:00PM 05:00PM
Priyanshu Singh and Ravi Prakash (IITB)

DAY4 — 05 June 2025

Secure communication I.b: MAC, digital signatures and hash functions — 09:30AM 11:00AM
Rajendra Kumar (IITD)

Tea Break — 11:00AM to 11:15AM

Secure communication I.b: MAC, digital signatures and hash functions — 11:15AM 12:45PM
Rajendra Kumar (IITD)

Lunch Break — 12:45PM to 2:00PM

Lab sessions: PKE tutorial (OpenSSL + OpenSSH) — 02:00PM 03:30PM
Archisman Dutta and Adwaiya Srivastav (IITB Trust Lab)

Tea Break — 03:30PM to 04:00PM

Lab sessions: PKE tutorial (OpenSSL + OpenSSH) — 04:00PM 05:00PM
Archisman Dutta and Adwaiya Srivastav (IITB Trust Lab)

DAY 5 — 06 June 2025

Secure communication III: homomorphic PKE, FHE etc — 09:30AM 11:00AM
Monosij Maitra (IITKGP)

Tea Break — 11:00AM to 11:15AM

Secure communication III: homomorphic PKE, FHE etc — 11:15AM 12:45PM
Monosij Maitra (IITKGP)

Lunch Break — 12:45PM to 2:00PM

Lab sessions: Signatures and hash functions — 02:00PM 03:30PM
Archisman Dutta and Adwaiya Srivastav (IITB Trust Lab)

Tea Break — 03:30PM to 04:00PM

Lab sessions: Signatures and hash functions — 04:00PM 05:00PM
Archisman Dutta and Adwaiya Srivastav (IITB Trust Lab)

Dinner — 07:00PM to 08:00PM

ACM Summer School IITB Trust Lab 2025

DAY 6 — 07 June 2025

Advanced primitives
Monosij Maitra (IITKGP)
09:30AM 11:00AM

Tea Break 11:00AM to 11:15AM

Advanced primitives
Monosij Maitra (IITKGP)
11:15AM 12:45PM

Lunch Break 12:45PM to 2:00PM

Lab sessions: FHE tutorial (OpenFHE)
Archisman Dutta and Adwaiya Srivastav (IITB Trust Lab)
02:00PM 03:30PM

Tea Break 03:30PM to 04:00PM

Lab sessions: FHE tutorial (OpenFHE)
Archisman Dutta and Adwaiya Srivastav (IITB Trust Lab)
04:00PM 05:00PM

DAY 7 — NO LECTURES — 08 June 2025

DAY 8 — 09 June 2025

Proof systems I: IP, ZK
Vineet Nair (Arithmic Labs)
09:30AM 11:00AM

Tea Break 11:00AM to 11:15AM

Proof systems I: IP, ZK
Vineet Nair (Arithmic Labs)
11:15AM 12:45PM

Lunch Break 12:45PM to 2:00PM

Proof systems I: IP, ZK
Vineet Nair (Arithmic Labs)
02:00PM 03:30PM

Tea Break 03:30PM to 04:00PM

Group exercise
Priyanshu Singh and Ravi Prakash (IITB)
04:00PM 05:00PM

DAY 9 — 10 June 2025

Proof Systems II: SNARGs
Saravanan Vijayakumaran (IITB)
09:30AM 11:00AM

Tea Break 11:00AM to 11:15AM

Proof Systems II: SNARGs
Saravanan Vijayakumaran (IITB)
11:15AM 12:45PM

Lunch Break 12:45PM to 2:00PM

Lab sessions: Circom
Saravanan Vijayakumaran (IITB)
02:00PM 03:30PM

Tea Break 03:30PM to 04:00PM

Lab sessions: Circom
Saravanan Vijayakumaran (IITB)
04:00PM 05:00PM

DAY 10 — 11 June 2025

Basics of MPC
Ashish Choudhury (IIITB)
09:30AM 11:00AM

Tea Break 11:00AM to 11:15AM

Basics of MPC
Ashish Choudhury (IIITB)
11:15AM 12:45PM

Lunch Break 12:45PM to 2:00PM

Basics of MPC
Ashish Choudhury (IIITB)
02:00PM 03:30PM

Tea Break 03:30PM to 04:00PM

Group exercise
Bhavadharini V (IITB Trust Lab)
04:00PM 05:00PM

DAY 11 — 12 June 2025

Applied MPC
Nishat Koti (Aztec Labs)
09:30AM 11:00AM

Tea Break 11:00AM to 11:15AM

Applied MPC
Nishat Koti (Aztec Labs)
11:15AM 12:45PM

Lunch Break 12:45PM to 2:00PM

Applied MPC
Nishat Koti (Aztec Labs)
02:00PM 03:30PM

Tea Break 03:30PM to 04:00PM

Group exercise
Bhavadharini V (IITB Trust Lab)
04:00PM 05:00PM

DAY 12 — 13 June 2025

Crypto for crypto
Nitin Singh (IBM Research)
09:30AM 11:00AM

Tea Break 11:00AM to 11:15AM

Crypto for crypto
Nitin Singh (IBM Research)
11:15AM 12:45PM

Lunch Break 12:45PM to 2:00PM

Conclusion