ICTS | INTERNATIONAL CENTRE for THEORETICAL SCIENCES

TATA INSTITUTE OF FUNDAMENTAL RESEARCH

Bangalore Probability Seminar

Title : Cryptographic proofs for privacy and integrity

Speaker : Chaya Ganesh (Indian Institute of Science, Bengaluru)

Date : Monday, 24 February 2025

Time : 2:00 PM (IST)

Abstract : A common denominator of conventional financial systems, trusted execution environments (like SGX), blockchain technology, and ZK-rollups is the promise of *computational integrity* -- doing the right computation on potentially secret inputs, even when there is no trust.

In this talk, we will define computational integrity and show how one can verify the correctness of a computation much more efficiently than having to re-perform the computation. We will introduce the notion of succinct proof systems that allow a prover to convince a verifier about the correctness of computation such that verification is exponentially faster than the computation itself, and zero-knowledge where the verifier learns nothing beyond the truth of the statement.

Venue : Madhava Lecture Hall
Zoom Link: https://us02web.zoom.us/j/88670406480
Meeting ID: 886 7040 6480