Time: 3:30 PM, Date: 24th October

Venue: KD 102 (CSE building)

Title: Two-party cryptography beyond computational assumptions: Some old and new results

Abstract:

The impossibility of information-theoretic or unconditional security under classical communication is already established for many two-party cryptographic primitives, including but not limited to coin flipping, bit commitment, and oblivious transfer. In this talk, we first discuss the known limits of information-theoretic security using quantum communication and propose the novel framework of stochastic switching that uses stochastic semidefinite programming to develop simple protocols for tasks such as Rabin oblivious transfer [1]. We also discuss some of the reductions that can be used to develop secure Rabin oblivious transfer and propose some lower bounds on its overall security [2]. We conclude by briefly discussing the insufficiency of standalone security from the perspective of (in)composability of weak coin flipping [3].

[1] Akshay Bansal and Jamie Sikora. "Breaking barriers in two-party quantum cryptography via stochastic semidefinite programming." arXiv preprint arXiv:2304.13200 (2023).

[2] Akshay Bansal, James T. Peat, Jiawei, Wu, Jamie Sikora, and Erika Andersson. "Towards better oblivious transfer protocols."

[3] Jiawei Wu, Yanglin Hu, Akshay Bansal, and Marco Tomamichel. "On the composable security of weak coin flipping." arXiv preprint arXiv:2402.15233 (2024).