Title: Device-independent Quantum Cryptography.

Abstract: Device-independent (DI) quantum cryptographic protocols are such that the honest parties are classical and interact with untrusted quantum devices by providing classical inputs and obtaining classical outputs from the devices.

Existing DI protocols in the literature for Quantum Key Distribution (QKD) between Alice and Bob assume that the devices shared between them do not communicate with each other once Alice and Bob start interacting with the devices. This may be a stringent and hard-to-implement assumption in the real world with adversarial devices. We present a first DI protocol for QKD that allows for linear (in the number of bits of the shared key) leakage between the devices and the adversary, allowing for a more practical implementation.

Oblivious Transfer (OT) is a very important cryptographic primitive that allows for secure Multi-Party Computation (MPC). We present a first DI protocol for OT that allows the cheating party full control over the devices shared between Alice and Bob. Our protocol is composable and hence allows for its use inside larger cryptographic protocols. Our protocol is presented in the bounded-storage model, where the long-term quantum memory is bounded.

The talk is based on:

1) R. Jain and S. Kundu. A direct product theorem for quantum communication complexity with applications to device-independent QKD. SIAM Journal on Computing (SICOMP), 2025. FOCS 2021. QIP 2022. ArXiv:2106.04299.

2) R. Batra, S. Chakraborty, R. Jain, and U. Kapshikar. A robust and composable device-independent
protocol for oblivious transfer using (fully) untrusted quantum devices in the bounded storage model.
QCrypt, 2025. ArXiv:2404.11283.