CT Advanced Computing Center (CACC) Security Seminar Series 2022-2023

Speaker: Hasan Iqbal
Date: Wednesday, November 30, 2022
Time:12 - 1:30pm
Location: ITE 401
Remote Access:https://uconn-cmr.webex.com/uconn-cmr/j.php?MTID=mab3ad0ebcb3b99da6167c8cc0c6807ee
Meeting number: 2624 433 7779
Password: XMuqTTej533

Quantum Key Distribution (QKD)

Quantum key distribution (QKD) is a cryptographic system that can generate a shared secret between two communicating parties, Alice and Bob, even when the adversary, Eve has unlimited computational capabilities. However, as working with quantum resources is hard, we strive to design protocols and choose resources carefully so that we get good performance in terms of noise-tolerance and efficiency. High-dimensional(HD) QKD has been getting attention recently as it serves that goal. In this talk, we cover a brief overview of HD-QKD and our recent contribution to this area. We discuss in detail an extension of the BB84 protocol. In particular, we derive an analytical proof of security that does not require numerical optimizations. Our new approach allows us to evaluate the performance of the protocol beyond dimension 7, which was a limitation of prior work. Along the way, we also derive and prove a new continuity bound for quantum entropy which is useful in cryptographic applications.

UCONN

CACC