NJIT

Department of Computer Science

Cryptographically Secure Systems for Modern Applications

Anrin Chakraborti
Duke University

Hosted by Reza Curtmola

Date: Wednesday, January 18, 2023
Coffee: 2:15 PM – 2:30 PM
Time: 2:30 PM – 3:30 PM
Location: GITC 4402 (4th floor Seminar Lecture Hall)
WebEx Link: https://njit.webex.com/njit/j.php?MTID=m73cc9aca43fd92f0265c35bfa3961d76

http://cs.njit.edu/seminars

Abstract:
Modern applications and computing platforms come with their share of privacy concerns. One way to address these concerns is by using tailor-made cryptographic tools. This talk will demonstrate how new application settings influence theoretical developments by presenting designs of cryptographically secure systems for : i) collaborative threat detection, and ii) deniable data storage. The first part of the talk presents a new cryptographic tool, namely a distance-aware private set intersection protocol, which has applications in collaborative threat detection and blacklisting by mutually untrusting parties. The second part of the talk introduces deniable storage systems: an evolution of full disk encryption systems that additionally provide plausible deniability of data possession even when encryption keys and metadata are leaked. Finally, the talk concludes by discussing potential applications of cryptographic theory to build secure infrastructures for intelligent transportation and machine learning.

Bio:
Anrin Chakraborti is a postdoctoral researcher at Duke University working with Professor Michael Reiter. He obtained his PhD in Computer Science from Stony Brook University where he was advised by Professor Radu Sion. His current research aims to address privacy concerns in cloud computing, collaborative computing, and end-to-end encrypted systems through applications of cryptographic theory. His work has appeared at several top-tier computer security and privacy conferences, and he has co-authored two monographs on secure cloud computing.