NJIT

Department of Computer Science

Space Jammed: Cryptography against Space-Bounded Adversaries

Jiaxin Guan
New York University

Hosted by: Reza Curtmola

Date: Tuesday, March 4, 2025
Coffee: 2:15 PM – 2:30 PM
Time: 2:30 PM – 3:30 PM (Eastern Time (US and Canada)
Location: GITC 4402 (4th floor Seminar Lecture Hall)

Zoom Link: https://njit-edu.zoom.us/j/98945613501?pwd=MrLEGbGBYmXarZhl2LdBbRVPu3iFhH.1.

Abstract:

Traditional cryptographic frameworks typically assume adversaries are limited by computational power. In contrast, this talk explores cryptographic constructions against space-bounded adversaries, where constraints are placed on the adversaries' storage capacity. This paradigm enables unconditionally secure protocols and previously unattainable security notions.

We begin by revisiting Maurer's Bounded Storage Model (CRYPTO '92), where we impose memory limitations on adversaries instead of computational constraints throughout the attack. Leveraging Raz's lower bound on parity learning (FOCS '16), we show constructions of various cryptographic protocols that achieve information-theoretic security, making them resilient to adversaries with unbounded computational power.

In the second part of the talk, we explore how combining computational assumptions with space constraints unlocks powerful new cryptographic primitives, ones that are unachievable with computational assumptions alone. Specifically, we show how to construct encryption schemes that guarantee privacy even if the adversary retrieves the decryption keys at a later time, and signature schemes where the adversary cannot produce a valid signature on any message, even one it has seen signed before. We present these constructions in the context of Incompressible Cryptography, a novel framework where adversaries can use an arbitrary amount of memory during protocol execution but are bounded by their long-term storage.

Bio:

Jiaxin Guan is an Assistant Professor / Faculty Fellow at New York University. His research focuses on the foundations of cryptography, in particular the space-constrained aspects of cryptography. His work explores topics such as the Bounded Storage Model, incompressible cryptography, space lower bounds, and streaming functional encryption. He received his PhD in 2023 from Princeton University, where he was advised by Mark Zhandry.