NJIT

# Department of Computer Science

## User-Centric Privacy via Cryptography

Yanxue Jia
Purdue University

**Hosted by: Zephyr Yao**

**Date:** Friday, January 31, 2025
**Coffee:** 11:15 AM – 11:30 AM
**Time:** 11:30 AM – 12:30 PM (Eastern Time (US and Canada)
**Location:** GITC 4402 (4th floor Seminar Lecture Hall)

**Zoom Link:** https://njit-edu.zoom.us/j/97248902716?pwd=cbvZFU5S7xYa6a3rKcqKUcz0SXmKRm.1

**Abstract:**
While concerns about data privacy are growing, people are often compelled to surrender sensitive data for the convenience of services. Moreover, providing clear privacy risk assessments to inform users about how their data will be utilized is becoming increasingly challenging. To overcome this dilemma, my research leverages secure multi-party computation to enable people to enjoy gains without exposing their sensitive data.

In this talk, I will present highly efficient secure two-party computation solutions for key scenarios involving end-to-end communication and set operations. Specifically, while communication content is protected, leaking metadata—that is, who communicated with whom, when, and the extent of their interactions—still poses significant privacy risks. To address this, I leverage two non-colluding servers to assist users in their communications while protecting their metadata. In addition, private set operations reveal the operation results while hiding the other items, making them valuable for privacy-preserving data collaboration scenarios. My work unifies diverse private set operations into a framework, and further designs private set union protocols with both stronger security and better performance. Finally, I will outline my future research directions, which include developing privacy-preserving data management systems based on the results of my previous research and advancing cryptographic techniques to support compute-intensive scenarios.

**Bio:**
Yanxue Jia is a post-doctoral researcher in the Department of Computer Science at Purdue University. She earned her Ph.D. in Computer Science from Shanghai Jiao Tong University in 2022. She is an applied cryptographer and her current research focuses on secure (multi-party) computation, blockchains, and provable security. She is dedicated to advancing cryptography to solve security and privacy issues in existing as well as emerging real-world applications. Her work has been published at top-tier conferences, such as USENIX Security, ACM CCS, and Asiacrypt. She has also served as a Program Committee member for conferences, such as ACM CCS and FC.