NJIT

<u>Department of Computer Science</u>

Going From Strength to Strength: Synergizing Formal Methods and Cryptography

Ning Luo
Northwestern University

Hosted by Martin Kellogg

Date: Monday, February 5, 2024
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=m4a39156fef6ec31471230f73adc5a7ff

<u>Abstract:</u>

As our reliance on digital techniques grows, ensuring the reliability and security of software becomes more crucial than ever. In this talk, I will discuss my research on synergizing cryptography and formal methods to achieve next-generation security and reliability of software. I will explain how to integrate cryptography into formal methods and enable software verification even without access to the software's source code. I will also demonstrate how to liberate the workforce from the complexity of cryptography-related implementation by applying formal methods to cryptography. Altogether, I will show that a never-before-seen combination of cryptography and formal methods is not only possible but also a necessary component in developing secure and reliable software for the future.

<u>Bio:</u>

Ning Luo is a postdoctoral fellow in the computer science department at Northwestern University. She received her Ph.D. in Computer Science from Yale University in Dec 2022. Ning's research combines formal methods, automated reasoning, programming language, and cryptography to achieve security, verifiability, and confidentiality in practical and challenging scenarios. She is a recipient of EECS Rising Stars (2023), a CCS Distinguished Paper Award (2022) and Roberts Innovation Award (2023).