VICEROY NORTHWEST INSTITUTE FOR CYBERSECURITY EDUCATION AND RESEARCH

CySER Virtual Seminar

Feng-Hao Liu
EECS, WSU

Cryptography in the Presence of Quantum Computing: New Opportunities and Research Directions

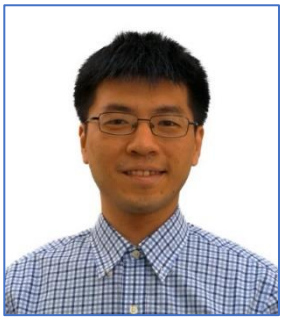
Nov. 13, 2023, 3:10 – 4PM Pacific

Team Link: Click here to join the meeting
Meeting ID: 290 931 227 452| Passcode: CouAD8
Call in (audio only) +1 509-498-6399 | Phone Conference ID: 997 608 206#

Abstract:

Quantum computing poses significant threats to traditional public-key cryptosystems, rendering many existing security structures insecure. The steady advancement in building large-scale quantum computers in recent years underscores the imminent nature of these threats. This shifting landscape has sparked extensive and dynamic research aimed at devising new cryptographic methods for the post-quantum era. In this talk, I will discuss new research directions along this goal, ranging from basic public-key encryption (PKE) to advanced fully homomorphic encryption (FHE), and substantial applications. Particularly, I will present the crypto basics following NIST's current efforts in standardizing post-quantum PKE. Then I will describe how to expand the scope to achieve and improve further advanced crypto capabilities, including fully homomorphic encryption (FHE), and a compelling subset of its applications.

Bio:



Feng-Hao Liu is an associate professor at the School of Electrical Engineering and Computer Science at WSU. He received a PhD in Computer Science from Brown University in 2013 and then joined the Maryland Cybersecurity Center at University of Maryland as a postdoctoral researcher from 2013 – 2015. In 2015, he joined Florida Atlantic University as an assistant professor and then became an associate professor in 2021. In 2023, he joined WSU as an associate professor. His research interests span the realms of post-quantum and lattice-based cryptography, fully homomorphic encryption, multiparty computation, tamper/leakage-resilient designs, and the foundational aspects of cryptography. With a focus on advancing the research frontier, he aspires to devise novel mathematical and analytical techniques. The ultimate goal is to realize cyberspace security and trustworthiness, especially in outsourced environments and in the face of potential threats from quantum computers. His research is supported by an NSF CRII award and an NSF CAREER Award. He has made significant contributions to the field, publishing multiple papers in esteemed venues such as Crypto, Eurocrypt, Journal of Cryptology, CCS, among others.