DEPARTMENT OF COMPUTER SCIENCE

TEXAS TECH
Whitacre College of Engineering

Software and Hardware Design for Cybersecurity in Post-Quantum and AI Era

Tuy Nguyen, Ph.D.
Northern Arizona University
Monday, February 24, 2025
10:00 a.m.
Holden 106

Abstract: The increasing number of data breaches and cyberattacks in the United States, culminating in the highest recorded figures in 2023 and 2024, underscores a critical security challenge. This challenge is further amplified by the growing reliance on data for training artificial intelligence (AI) algorithms, raising concerns about the protection of both sensitive data and the trained models themselves. In response to these evolving threats, the National Institute of Standards and Technology (NIST) initiated a process in 2016 to standardize quantum-resistant cryptographic algorithms. This effort has led to the selection of lattice-based algorithms in August 2024 as benchmarks for future security standards.

This talk explores efficient design methodologies to enhance data security. We will then delve into the design and optimization of lattice-based algorithms, considering both software and hardware implementations. Furthermore, we will investigate techniques for seamlessly integrating post-quantum cryptography with artificial intelligence, enabling highly secure and accurate AI training on encrypted data protected by post-quantum cryptographic al-gorithms. Finally, we will explore applications of cybersecurity and AI in various domains, such as autonomous systems and smart healthcare.

Bio: Tuy Nguyen received the Ph.D. degree in Information and Communication Engineering from Inha University, South Korea, in 2019. He is currently an Assistant Professor in the School of Informatics, Computing, and Cyber Systems at Northern Arizona University. Prior to this appointment, he held a Post-Doctoral Fellowship and a Lectureship in the Department of Electrical and Computer Engineering at Inha University. From August 2019 to April 2021, he worked as a Senior Research Engineer at Conextt Inc., South Korea. His research interests encompass the software and hardware design, implementation, and optimization of cryptography, homomorphic encryption, error correction codes, and applied artificial intelligence.

Dr. Nguyen's research team has developed highly secure and accurate federated learning systems operating on encrypted data. The team has also integrated cryptography, error correction codes, and artificial intelligence into applications for IoT communications, autonomous systems, and smart healthcare. His research has been supported by grants from the National Science Foundation, Army Research Laboratory, Department of Defense, Arizona Commerce Authority, and the State of Arizona Technology and Research Initiative. Dr. Nguyen is committed to mentoring students in research, as demonstrated by more than 20 coauthored publications with undergraduate, graduate, and students in his courses, along with numerous research awards received by his team.