Department of Electrical Engineering
香港城市大學
City University of Hong Kong

VILLANOVA UNIVERSITY

CityU Architecture Lab for Arithmetic and Security (CALAS) Seminar Series

Design and Implementation of Lightweight Post-Quantum Cryptography: From Algorithmic Derivation to Architectural Innovation

Dr. Jiafeng (Harvest) XIE, Assistant Professor
Department of Electrical and Computer Engineering, Villanova University

Abstract:

Post-quantum cryptography (PQC) has recently drawn significant attention from various communities, along with the rapid advancement in building large-scale quantum computers. Apart from the National Institute of Standards and Technology (NIST) PQC standardization process targeting general-purpose algorithms, the research community is also looking for lightweight PQC for specific applications. In this talk, I will follow this trend to introduce the design and implementation of a promising lightweight PQC, the Ring-Binary-Learning-with-Errors (RBLWE)-based encryption scheme. Specifically, this talk stands from the hardware implementation perspective, covering algorithmic derivation and architectural innovation. A series of novel algorithms and architectures will be covered in this talk. I hope that this talk will attract more research on the lightweight PQC development and further possible standardization.

Biography:

Dr. XIE is currently an Assistant Professor in the Department of Electrical and Computer Engineering, Villanova University. His research interests include cryptographic engineering, hardware security, post-quantum cryptography, and digital design for large-scale computing systems. Dr. Xie has served as technical committee member for many reputed conferences such as HOST, ICCAD, and DAC. He is also currently serving as Associate Editor for IEEE Transactions on VLSI Systems, Microelectronics Journal, and IEEE Access. He also will be serving as Associate Editor for IEEE Transactions on Circuits and Systems-II starting 2024. He received the IEEE Access Outstanding Associate Editor for the year of 2019. He also received the 2022 IEEE Philadelphia Section Merrill Buckley Jr. Student Project Award and the Best Paper Award from IEEE International Symposium on Hardware Oriented Security and Trust 2019 (HOST'19).

18 Oct 2023 (Wed), 4:00pm, G6501 & https://cityu.zoom.us/j/96742093029