Hardware Acceleration for Post-Quantum Cryptography: Algorithmic Derivation, and Architectural Innovation

Time: December 14, 2022

Abstract: Post-quantum cryptography (PQC) has drawn significant attention from various communities recently as the existing public-key cryptosystems such as Rivest Shamir Adleman (RSA) and Elliptic Curve Cryptography (ECC) are proven to be vulnerable to the large-scale quantum computers executing Shor’s algorithm. The National Institute of Standards and Technology (NIST) has already started the PQC standardization process, and hardware acceleration for PQC algorithms is one of the recent focused topics. In this talk, I follow this trend to introduce several interesting methods to accelerate the PQC algorithms on the hardware platform. Specifically, this talk will present the hardware implementation methods from the aspects of both algorithmic derivation and architectural innovation. Implementation techniques for a lightweight PQC scheme is also covered in this talk. I hope that this talk will facilitate more research to help the PQC standardization and further development.

Speaker: 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 VLSI design of neural network 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 Microelectronics Journal and IEEE Access. He also served as Associate Editor for IEEE Transactions on Circuits and Systems-II: Express Briefs. 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).

Contact: Dr. Jiafeng (Harvest) Xie (jiafeng.xie@villanova.edu)
Department of Electrical and Computer Engineering, Villanova University