Po-Jen Chen

+886-978-215-272 · mooseedsheeran@gmail.com · /in/pojenchen1123

Research Interest

My research goal is to provide flexible and cost-effective solutions from the viewpoint of architecture. Recently I have worked on implementing the public-key generator for post-quantum cryptography, that is, cryptosystems deployed in classical computers conjectured to be secure against attacks from large-scale quantum computers.

Education

Master of EECS | Digital Integrated Circuit Design Sep. 2019 – Feb. 2022 (expected)
Graduate Institute of Electronics Engineering, National Taiwan University *Taiwan*

- Advisors: *Prof.* Tsung-Te Liu, *Prof.* Tung Chou
- Thesis: VLSI Implementation for the First LUP-Based Systemizer with Early Abortion on FPGA (in progress)
- GPA: 4.2/4.3

Bachelor of EECS | Electrical Engineering Sep. 2015 – Jun. 2019
National Taiwan University *Taiwan*

- GPA: 3.9/4.3

Professional Experiences

Research Assistant of CITI, Academia Sinica Jul. 2020 – Present
Project: FPGA-based Implementation of Post-Quantum Cryptosystem

- Implemented an early-abort algorithm on FPGA for the public-key generation of Classic McEliece, one of the finalists in the Round 3 NIST PQC Standardization Process.
- Designed a LUP (decomposition) Gaussian elimination flow over systolic line architecture.

Teaching Assistant | Post-Quantum Cryptography Spring 2021

- Gave sample solutions to Quiz and Midterm and Evaluated students' coding performances of PQC algorithms' on developed tools, such as Cortex M4, Cortex A7, Cortex A53, and Cortex A72.

Teaching Assistant | Computer Architecture Spring 2020

- Designed fair, yet challenging, homework problems that deepen students' understanding of the subjects.
- Held office hours and grading.

Teaching Assistant | Scientific Research and Academic Career Fall 2020

- Helped Students develop critical thinking skills through discussions and writing practices.

Undergraduate Research in EECS Lab, NTU Mar. 2018 – Aug. 2019
Project: Power Side-Channel Attacks, VLSI Design of Galois Field Arithmetic Logic Unit

- Proposed a hybrid modular arithmetic architecture with high hardware utilization and low energy cost.
- Designed an energy-efficient elliptic curve cryptography processor avoiding attacks from simple power analysis.

Projects and Experiences

Computer-Aided Vlsi System Design Sep. 2019 – Jan. 2020

- Title: Motion Estimation/Compensation (MEMC)

Digital Signal Processing in Vlsi Design Mar. 2019 – Jun. 2019

- Title: Parallelism Factor of 2D Convolution Circuit in 28-nm CMOS Technology

Badminton Team Leader Jul. 2017 – Jun. 2018

Publication

L. -Y. Yeh, **P. -J. Chen**, C. -C. Pai and T. -T. Liu, "An Energy-Efficient Dual-Field Elliptic Curve Cryptography Processor for Internet of Things Applications," in *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 67, no. 9, pp. 1614-1618, Sept. 2020, doi: 10.1109/TCSII.2020.3012448.

Skills

Programming Languages: Verilog, Matlab, Python, SageMath, Bash
Developer Tools: Quartus, Vivado, NC-Verilog, iVerilog, Design Compiler, Innovus