PO-JEN **CHEN**

☎ (+886) 978-215-272 | ✉ mooseedsheeran@gmail.com

Research Interests

My research goal is to provide flexible and cost-efficient 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

Graduate Institute of Electronics Engineering, National Taiwan University (NTU)

Taipei, Taiwan

M.S. in Digital Integrated Circuit Systems — *Sep. 2019 – Jan. 2022 (expected)*

- **Thesis**: First FPGA-Based Early-Aborting Systemizer in Classic McEliece Applied with LU Decomposition
- **Advisor**: *Prof. Tsung-Te Liu*, *Prof. Tung Chou*
- **GPA**: overall: **4.21/4.30**

National Taiwan University (NTU)

Taipei, Taiwan

B.S. in Electrical Engineering — *Sep. 2015 – Jun. 2019*

- **GPA**: overall: **3.90/4.30**, last 60: **4.09/4.30**

Research Experiences

Research Assistant

Taipei, Taiwan

Research Center for Information Technology Innovation, Academia Sinica — *Jul. 2020 – Present*

- **Project**: FPGA-based Implementation of Post-Quantum Cryptosystem
- **Advisor**: *Prof. Tung Chou*, *Prof. Ruben Niederhagen*, *Prof. Jakub Szefer*
- Implemented three early-abort methods on FPGA for the public-key generation of Classic McEliece, one of the finalists in the Round 3 NIST PQC Standardization Process.
- Designed a hardware-friendly LUP-based (decomposition) Gaussian elimination flow over systolic line architecture.
- Proposed an overlapping elimination flow to enhance the utilization rate of the systolic line.
- Introduced logic reduction to the majority of processors in the systolic line architecture.
- Outperformed the prior key generator hardware designs by up to over 2.8x in runtime and 3.6x in time-area efficiency.

Undergraduate Research

Taipei, Taiwan

EECS Lab, NTU — *Mar. 2018 – Aug. 2019*

- **Project**: Power Side-Channel Attacks, VLSI Design of Galois Field Arithmetic Logic Unit
- **Advisor**: *Prof. Tsung-Te Liu*
- Funded by **Ministry of Science and Technology (MOST) for undergraduate research projects**.
- 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.
- Achieves 51.6% and 50.5% lower energy consumption for each $GF(p)$ and $GF(2^m)$ ECPM operation, respectively.

Publication † indicates equal contribution

[1] Ling-Yu Yeh†, **Po-Jen Chen**†, Chen-Chun Pai, and Tsung-Te Liu. An energy-efficient dual-field elliptic curve cryptography processor for internet of things applications. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 67(9):1614–1618, 2020.

Teaching Experiences

Teaching Assistant

Taipei, Taiwan

Scientific Research and Academic Career | *Prof. Hsiao-Wen Chung* — *Fall 2021*

- Helped the professor deal with classroom affairs, such as setup of distance learning.
- Reviewed and commented students' feedback for each class.

Teaching Assistant

Taipei, Taiwan

Post-Quantum Cryptography | *Prof. Bo-Yin Yang* — *Spring 2021*

- Gave sample solutions to Quiz and Midterm and corrected students' test papers.
- Maintained the "Final Project Reminder" for students and provided sample formats in terms of coding, presenting and reporting.
- Evaluated students' coding performances of PQC algorithms on developed tools, such as Cortex M4, Cortex A7, Cortex A53, and Cortex A72.
- Wrote a preliminary"Final Project Document", including problem description, sample format, tools' instructions, and Q&A.

Teaching Assistant
Taipei, Taiwan

Scientific Research and Academic Career | *Prof. Hsiao-Wen Chung* — *Fall 2020*

- Helped students develop critical thinking skills through discussions and writing practices.
- **Won NTU Excellent Teaching Assistants**.

Teaching Assistant
Taipei, Taiwan

Computer Architecture | *Prof. Tsung-Te Liu* — *Spring 2020*

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

Honors & Awards

2021	**Excellent Teaching Assistants [*link*]**, NTU	*Taipei, Taiwan*
2021	**Certificate of design completion, Finalist**, Integrated Circuit Design Contest (Cell-based, Graduate Level)	*Taiwan*
2020	**Finalist**, Integrated Circuit Design Contest (Cell-based, Graduate Level)	*Taiwan*
2019	**Finalist**, Integrated Circuit Design Contest (Cell-based, Undergraduate Level)	*Taiwan*
Jul. 2018 – Feb, 2019	**Funded**, Ministry of Science and Technology Project for Undergraduate Students	*Taiwan*

Selected Projects & Extracurricular Activity

Motion Estimation/Compensation (MEMC)
Taipei, Taiwan

Course Final Project of "**Computer-Aided Vlsi System Design**" — *Sep. 2019 – Jan. 2020*

- Adopted down sampling for image pixels, shrunk search range within matching blocks, and early skipping for min-max error.
- Scheduled truncated pixels of separated images into one SRAM and parallelized the computation with 4 process elements.

Miller's Algorithm in Pairing-Based Cryptography
Taipei, Taiwan

Course Final Project of "**Cryptography**" — *Sep. 2019 – Jan. 2020*

- Surveyed algorithmic improvements to decrease the complexity of Miller's algorithm.

Baby-Step Giant-Step Attack on Diffie-Hellman Key Exchange Protocol
Taipei, Taiwan

Course Final Project of "**Integrated Circuits Design Laboratory**" — *Mar. 2019 – Jun. 2019*

- Organized the architect and instructed team members to accomplish encryption/decryption (DES) and key-exchange protocol (DHKE).
- Implemented Montgomery multiplication/division for arithmetic computation over Galois field.
- **Fabricated in 180-nm CMOS technology and validated with measurement results**.

Frequency Analysis System
Taipei, Taiwan

Summer Training in *EECS Lab*, NTU — *Jul. 2019 – Aug. 2019*

- Employed "transposed" finite impulse response filter to shorten the critical path and reduce the number of adders.
- Exploited radix-2^2 16-point FFT to reduce the multiplicative complexity.
- Searched the main frequency with "folding" architect to share datapath logic.

5-Stage Pipelined MIPS
Taipei, Taiwan

Course Final Project of "**Digital System Design**" — *Mar. 2018 – Jun. 2018*

- Extended pipelined multiplication/division to shorten critical path and carried Booth's multiplication algorithm to facilitate recursive computation.
- Exploited the advantage of locality through multi-levels of caches with different read/write policies.

Badminton Team Leader
Taipei, Taiwan

Electrical Engineering Dept. at NTU — *Jul. 2017 – Jun. 2018*

- Shared my passion to team members and built a heartwarming badminton community.
- Held a badminton contest for College of Electrical Engineering and Computer Science at NTU, and organized over 5 nationwide or school-wide games.
- Provided guidance in every game and led our team to win 4 trophies.

Technical Skills

Programming Languages: Verilog, MATLAB, Python, SageMath, Bash, LaTeX

Developer Tools: Quartus, Vivado, NC-Verilog, iVerilog, nWave, Design Compiler, Innovas, Git