PO-JEN (Peter) **CHEN**

No. 5, Aly. 32, Ln. 282, Pingdong Rd., Pingzhen Dist., Taoyuan City, Taiwan (R.O.C.)

(+886) 978-215-272 | mooseedsheeran@gmail.com | pojenchen.github.io

Research Interests

VLSI Design for Secure Primitives or Digital Signal Processing, Chip Security, Secure Microarchitectures, Cryptography

Education

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

Taipei, Taiwan

M.S. in Electronics Engineering — *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. Tsung-Te Liu*, *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 the systolic line architecture.
- Deployed an overlapping elimination flow to enhance the utilization rate of the systolic line.
- Employed the logic reduction to the majority of processors in the systolic line architecture.
- Outperformed the prior key generator hardware designs by up to 2.8x in runtime and 3.6x in time-area efficiency.

Graduate Research Assistant

Taipei, Taiwan

Energy-Efficient Circuits and Systems Lab, NTU — *Sep. 2019 – Jun. 2020*

- **Advisor**: *Prof. Tsung-Te Liu*
- Conducted a survey on post-quantum cryptography (lattice-based, code-based, and isogeny-based), which secures data against both quantum and classical computers.
- Conducted a survey on pairing-based cryptography, which enabling many new cryptographic protocols that had not previously been feasible.
- Surveyed algorithmic improvements to decrease the complexity of Miller's algorithm.

Undergraduate Research Assistant

Taipei, Taiwan

Energy-Efficient Circuits and Systems Lab, NTU — *Mar. 2018 – Aug. 2019*

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

Publication † indicates equal contribution

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.

Preprint

Po-Jen Chen, Tung Chou, Sanjay Deshpande, Norman Lahr, Ruben Niederhagen, Jakub Szefer and Wen Wang, "A Complete FPGA Implementation of Classic McEliece." (Aiming at TCHES, Volume 2022, Issue 3)

Teaching Assistantship

Teaching Assistant — *Taipei, Taiwan*

Course Title: Scientific Research and Academic Career | *Prof. Hsiao-Wen Chung* — *Fall 2020, Fall 2021*

- Reviewed and provided comments to students' assignments for each class.
- Facilitated students to develop critical thinking skills through peer discussions and writing practices.
- **Won NTU Excellent Teaching Assistants**.

Teaching Assistant — *Taipei, Taiwan*

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

- Provided sample solutions to Quiz and Midterm and marked students' papers.
- Evaluated students' coding performances of PQC algorithms on developed tools, i.e. Cortex M4, Cortex A7, Cortex A53, and Cortex A72.
- Documented a "Final Project Guideline", including problem description, sample formats, tools' instructions, and Q&A.

Teaching Assistant — *Taipei, Taiwan*

Course Title: 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 graded students' assignments and papers.

Selected Experiences

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.

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**.

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 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.

Awards & Funding

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*
2018 – 2019	**Funding**, Ministry of Science and Technology Project for Undergraduate Students	*Taiwan*

Technical Skills

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

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

Referees

Dr. Tsung-Te Liu
Associate Professor, National Taiwan University
+886-2-33661818
ttliu@ntu.edu.tw

Dr. Tung Chou
Assistant Researcher, CITI, Academia Sinica
+886-2-2787-2300 #2345
blueprint@citi.sinica.edu.tw

Dr. Bo-Yin Yang
Research Fellow/Professor, IIS, Academia Sinica
+886-2-2788-3799 #1731
byyang@iis.sinica.edu.tw

Dr. Hsiao-Wen Chung
Professor, National Taiwan University
+886-2-33663628
chunghw@ntu.edu.tw