Cheng-Jhih Shih

+886 928 634 949 | @ cs861324@gmail.com | LinkedIn | GitHub | Google Scholar

Education

National Taiwan University — Taipei, Taiwan

M.Sc. in Computer Science and Information Engineering; ***GPA: 4.04/4.30*** — *Sep 2020 – Nov 2023*

B.Sc. in Computer Science and Information Engineering; ***GPA: 3.92/4.30*** — *Sep 2016 – Jun 2020*

Awards & Achievements

NTUEE-1975 Innovation and Entrepreneurship Fund Award: Awarded to outstanding individuals or teams within the College of EECS. Recognizes achievements in innovation, creativity, exceptional research papers, top competition performances, and other categories as determined by the evaluation committee.

Future Tech Award: Received from the National Science and Technology Council R.O.C. Among 501 entries, the award recognized 80 outstanding technologies for their 'scientific breakthrough' and 'industrial applicability,' revitalizing the field of technological innovation.

NTU Quantum Computing and Information Program (Completed): Completed the program by taking 6 required credits in quantum computing courses and a minimum of 9 credits from other electives, including Linear Algebra, Algorithms, etc.

Research Experience

National Taiwan University — Taipei, Taiwan

Research Assistant — *Jan 2020 – Jan 2022*

- "Emerging Technology Design Automation in the Post-Moore Era" project led by Prof. Shih-Hao Hung, Prof. Jie-Hong Roland Jiang, and Prof. Chung-Yang Huang.
- Performed research on quantum computations, including accelerated simulated quantum annealing using Tensor Cores, and prototyped large-scale circuit-based simulations on NVMe.

Academia Sinica — Taipei, Taiwan

Research Assistant — *Jul 2020 – Aug 2020*

- Wrote ARM assembly code for Cortex-M4 processors in the field of post-quantum cryptography and co-authored two publications on CHES with instructors and fellow interns.
- Advisor: Prof. Bo-Yin Yang

Selected Publications

[1] Shih, Cheng Jhih, Hung, S. H., Chen C. W., Perng, C. F., Kao. M. C. & Shih, C. S., "A Heterogeneous Computing Framework for Accelerating Fully Homomorphic Encryption", International Symposium on Mobile Internet Security (**MobiSec**), Dec 2023

[2] Beullens, W., Chen, M. S., Hung, S. H., Kannwischer, M. J., Peng, B. Y., Shih, Cheng Jhih, & Yang, B. Y., "Oil and vinegar: Modern parameters and implementations", IACR Transactions on Cryptographic Hardware and Embedded Systems (**TCHES**), Vol. 2023 No. 3

[3] Chung, Y. H., Shih, Cheng Jhih, & Hung, S. H., "Accelerated Simulated Quantum Annealing with GPU and Tensor Cores", **ISC High Performance**, May 2022

[4] Chung, C. M. M., Hwang, V., Kannwischer, M. J., Seiler, G., Shih, Cheng Jhih, & Yang, B. Y., "NTT multiplication for NTT-unfriendly rings: New speed records for Saber and NTRU on Cortex-M4 and AVX2", IACR Transactions on Cryptographic Hardware and Embedded Systems (**TCHES**), Volume 2021, Issue 2 (**Best Artifact Award**)

[5] Alkim, E., Cheng, D. Y. L., Chung, C. M. M., Evkan, H., Huang, L. W. L., Hwang, V., Li, C. L. T., Niederhagen, R., Shih, Cheng Jhih, Wälde, J., & Yang, B. Y., "Polynomial Multiplication in NTRU Prime: Comparison of Optimization Strategies on Cortex-M4", IACR Transactions on Cryptographic Hardware and Embedded Systems (**TCHES**), Volume 2021, Issue 1

[6] Shih, Cheng Jhih, "A Hardware/Software Co-Design Framework for FPGA-based Fully Homomorphic Encryption", advised by Prof. Shih-Hao Hung, **Master's Thesis**

Conference Presentations

Shih, Cheng Jhih, "A Heterogeneous Computing Framework for Accelerating Fully Homomorphic Encryption", International Symposium on Mobile Internet Security (**MobiSec**), Dec 2023

Work Experience

Wistron New Taipei City, Taiwan
Software Engineer *Feb 2022 – Jul 2023*

- Collaboration between Wistron and MIT CSAIL to develop a **homomorphic encryption accelerator on FPGA**, enabling privacy preserving computations.
- Collaborators: Prof. Daniel Sanchez and Prof. Srini Devadas

National Taiwan University Taipei, Taiwan
Teaching Assistant *May 2022 – Jun 2022*

- Course: AI Accelerator, Lecturer: Prof. Hsiang-Tsung Kung

Teaching Assistant *Sep 2020 – Jan 2021*

- Course: Computer Architecture, Lecturer: Prof. Shih-Hao Hung

System Administrator *Feb 2018 – Jan 2020*

- Conducted regular hardware inspections and performed software updates for classroom computers (Reborn Cards), along with maintaining online printing services (PaperCut) and wireless projectors (AirServer).

ASUS AICS Cloud Team Taipei, Taiwan
Software Engineer *Jul 2018 – Aug 2018*

- Deployed ASUS services to the cloud through Kubernetes while ensuring a certain level of durability and scalability.

Selected Projects

UOV: Unbalanced Oil and Vinegar *GitHub*

- A multivariate signature scheme submitted to "NIST Post-Quantum Cryptography: Digital Signature Schemes".
- I was in charge of the FPGA implementation. The design allocates systolic arrays for tasks such as Gaussian elimination and polynomial evaluation, paired with a controller to carry out KeyGen, Sign and Verify. The AES128 and SHAKE256 modules are included and adjusted to be consistent with the result of software implementations.

Hardware Accelerator for Computing on Encrypted Data (Wistron & MIT CSAIL Collaboration)

- Modified and synthesized F1 on the Xilinx Alveo U280 board.
- Integrated the FPGA framework with the Lattigo fully homomorphic encryption (FHE) library to leverage KeyGen/Enc/Dec functions, providing end-to-end FHE inference demonstrations.
- Integrated the FHE compiler with the FPGA framework to create an easy-to-use interface.
- Prototyped multi-FPGA accelerator designs for FHE.

Quantum-Inspired Computations *GitHub*

- Researched and implemented quantum-inspired computation algorithms to solve Ising problems.
- Accelerated algorithms using CUDA for GPUs and OpenCL for FPGAs.

Research Interests

High-Performance Computation, Computer Architecture, Computer Systems

- Topics: Post Quantum Cryptography, Homomorphic Encryption, Quantum Computation

Skills

C/C++, Python, Go, SQL, MATLAB, R, CUDA, OpenCL, HLS, Verilog, Assembly