Weihang Tan

Linkedin: www.linkedin.com/in/weihangtan/
Homepage: wtan.cc

Email : wtan@g.clemson.edu
Mobile : +1-864-624-2991

Academic Positions

- **University of Minnesota, Twin Cities** — Minneapolis, MN
  Postdoctoral Research Associate (Advisor: Dr. Keshab K. Parhi) — *Jan. 2023 - Dec. 2023*
- **Clemson University** — Clemson, SC
  Graduate Research Assistant (Advisor: Dr. Yingjie Lao) — *Aug. 2018 - Dec. 2022*

Education

- **Clemson University** — Clemson, SC
  Ph.D. in Electrical Engineering; — *Dec. 2022*
- **Clemson University** — Clemson, SC
  Master of Science in Electrical Engineering; — *Aug. 2020*
- **Clemson University** — Clemson, SC
  Bachelor of Science in Electrical Engineering (Cum Laude); — *May 2018*

Skills Summary

- **Programming**: Verilog HDL, C/C++, Python, MATLAB, R
- **Design tools**: Synopsys, HSPICE, VCS, Design Complier, Xilinx Vivado, PyTorch

Research Interest

My research interests include hardware security and VLSI architecture design for fully homomorphic encryption (FHE), post-quantum cryptography (PQC), digital signal processing systems, and privacy-preserving machine learning.

Experience

- **University of Minnesota and Clemson University** — Minneapolis, MN
  Efficient Hardware Accelerators for PQC and FHE — *Nov. 2020 - Present*
  - **Advisors**: Prof. Yingjie Lao (Clemson), Prof. Keshab K. Parhi (UMN), and Prof. Xinmiao Zhang (OSU)
  - **Objective 1**: Design an accelerator for NIST PQC finalist scheme Saber. Develop a modular polynomial multiplier that exploits the FIR filter and systolic array to reduce computational complexity. Parallelize the architecture using fast filtering structure to reduce the latency while maintaining high-speed performance. Successfully implemented the accelerator on the Xilinx Artix-7 FPGA, demonstrating a significantly improved timing performance and area-timing product compared to previous designs.
  - **Objective 2**: Develop a customized and parameterized design for both the CRYSTAL-Kyber and NewHope PQC schemes. Innovate an efficient partly-parallel number theoretic transform (NTT) multi-channel architecture to achieve high throughput and low latency performance.
  - **Objective 3**: Hardware/software co-optimization for BFV homomorphic encryption scheme for privacy-preserving machine learning application. (Ongoing)

  - This work was supported in part by Semiconductor Research Corporation (SRC) Task 2998.001 and NSF: CCF-2243052

- **Clemson University** — Clemson, SC
  Hardware/Algorithm Co-optimization for FHE — *Aug. 2018 - Dec. 2022*
  - **Advisors**: Prof. Yingjie Lao and Prof. Shuhong Gao
  - **Objective 1**: Develop a modular multiplier based on the Karatsuba algorithm for coefficient multiplication. Design a novel algorithm through the exploration of special primes utilized in lattice-based cryptography. The design was successfully implemented using the 32nm ASIC technology node (Synopsys tool). Demonstrated outstanding performance in terms of timing and area efficiency compared to previous works.
  - **Objective 2**: Develop a cutting-edge memory-based NTT-based polynomial multiplier employing a versatile and reconfigurable PE design. Proposed a novel memory addressing scheme that maximizes hardware utilization across a range of PE numbers. This approach achieves significant improvements in both efficiency based on hardware utilization and flexibility.

- **Clemson University** — Clemson, SC
  Swarm Robotics (Creative Inquire, Undergraduate Research) — *Aug. 2017 - Dec. 2017*
  - **Advisor**: Prof. Yongqiang Wang
  - **Contribution**: Took part in algorithm design and implementation in the Micro-controller (Arduino) for swarm robot navigation system.

- **Clemson University** Clemson, SC
  Medical Instrumentation Design (Undergraduate Research) *Aug. 2017 - Dec. 2017*
  - **Advisor**: Prof. Delphine Dean
  - **Objective**: Congenital Hand Deformity Patient Movement Improved by the EMG Signal Control.
  - **Contribution**: Took part in physiological signal (EMG) processing and analysis, simple artificial limb design, and application of bio-sensor.

Honors and Awards

- Pramod Subramanyan **Best PhD Forum Presentation Award**, IEEE Asian Hardware Oriented Security and Trust Symposium (AsianHOST), 2021
- **Student Travel Grant**, National Science Foundation (**NSF**), Conference on Cryptographic Hardware and Embedded Systems (**CHES**), 2019
- Merit Student of **Dean's List**, Clemson University, 2018
- Graduated with Cum Laude (B.S.), Clemson University, 2018
- Merit Student of **President's List** (GPA 4.0 in F17 semester), Clemson University, 2018
- Richard W. Borry Scholarship, Clemson University, 2017
- Merit Student of **President's List** (GPA 4.0 in S17 semester), Clemson University, 2017

Patent

- Keshab K Parhi, Xinmiao Zhang, **Tan, Weihang**, Antian Wang, and Yingjie Lao. Low-latency polynomial modulo multiplication over ring, July 27, 2023. U.S. Patent App. 17/582,560.
- Keshab K. Parhi, **Tan, Weihang**, Sin-Wei Chiu, Antian Wang, and Yingjie Lao, Parallel polynomial modular multiplication using NTT and inverse NTT, Nov. 2, 2023, U.S. Patent App. 18/500,670.

Research Grant (Helped my advisors in writing the proposal)

- Collaborative Research: SHF: Small: Efficient and Scalable Privacy-Preserving Neural Network Inference based on Ciphertext-Ciphertext Fully Homomorphic Encryption - National Science Foundation (NSF): CCF-2243052 & CCF-2243053; April 2023 - March 2026; Total Award amount: $600,000

Selected Publications

[1] **Tan, Weihang**, Benjamin M Case, Gengran Hu, Shuhong Gao, and Yingjie Lao. An ultra-highly parallel polynomial multiplier for the bootstrapping algorithm in a fully homomorphic encryption scheme. *Journal of Signal Processing Systems*, 93(6):643–656, 2021.

[2] **Tan, Weihang**, Benjamin M. Case, Antian Wang, Shuhong Gao, and Yingjie Lao. High-speed modular multiplier for lattice-based cryptosystems. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 68(8):2927–2931, 2021.

[3] **Tan, Weihang**, Sin-Wei Chiu, Antian Wang, Yingjie Lao, and Keshab K Parhi. PaReNTT: Low-latency parallel residue number system and ntt-based long polynomial modular multiplication for homomorphic encryption. *arXiv preprint arXiv:2303.02237 (Accepted by IEEE Transactions on Information Forensics and Security)*, 2023.

[4] **Tan, Weihang**, Gengran Hu, Benjamin Case, Shuhong Gao, and Yingjie Lao. An efficient polynomial multiplier architecture for the bootstrapping algorithm in a fully homomorphic encryption scheme. In *2019 IEEE International workshop on signal processing systems (SiPS)*, pages 85–90. IEEE, 2019.

[5] **Tan, Weihang**, Yingjie Lao, and Keshab K Parhi. KyberMat: Efficient accelerator for matrix-vector polynomial multiplication in CRYSTALS-Kyber scheme via NTT and polyphase decomposition. In *the 42nd IEEE/ACM International Conference on Computer-Aided Design (ICCAD) (Accepted)*. IEEE, 2023.

[6] **Tan, Weihang**, Antian Wang, Yingjie Lao, Xinmiao Zhang, and Keshab K Parhi. Pipelined high-throughput NTT architecture for lattice-based cryptography. In *2021 Asian Hardware Oriented Security and Trust Symposium (AsianHOST)*. IEEE, 2021.

[7] **Tan, Weihang**, Antian Wang, Yunhao Xu, and Yingjie Lao. Area-efficient pipelined VLSI architecture for polar decoder. In *2020 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, pages 352–357. IEEE, 2020.

[8] **Tan, Weihang**, Antian Wang, Xinmiao Zhang, Yingjie Lao, and Keshab K Parhi. High-speed VLSI architectures for modular polynomial multiplication via fast filtering and applications to lattice-based cryptography. *IEEE Transactions on Computers*, 2023.

[9] Antian Wang, **Tan, Weihang**, Yuejiang Wen, and Yingjie Lao. NoPUF: A novel PUF design framework toward modeling attack resistant PUFs. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 68(6):2508–2521, 2021.

[10] Antian Wang, Bingyin Zhao, **Tan, Weihang**, and Yingjie Lao. NNTesting: Neural network fault attacks detection using gradient-based test vector generation. In *2023 60th ACM/IEEE Design Automation Conference (DAC)*, pages 1–6. IEEE, 2023.