Antian Wang, Ph.D. candidate

E-Mail	antianw@g.clemson.edu
Linkedin	www.linkedin.com/in/wangantian
Personal website	https://wangantian.github.io/

Education

2018 – 2024 • **Ph.D. Electrical Engineering (Intelligent System), The Holcombe Department of Electrical and Computer Engineering, College of Engineering, Computing and Applied Sciences, Clemson University SC, U.S.A**
Advisor: Dr. Yingjie Lao
Dissertation title: Hardware-oriented Protection and Acceleration for Machine Learning Application.

2018 – 2021 • **Engineering and Science Education Certificate, Department of Engineering and Science Education, College of Engineering, Computing and Applied Sciences, Clemson University SC, U.S.A**
Eleven Credit Hour courses in Seminar, Pedagogy, Education Research Methods, Professional development, and Practicum.

2013 – 2017 • **B.E. Communication Engineering, Department of Electronic Engineering, College of Information Engineering, Shanghai Maritime University, Shanghai, China.**
Municipal level Outstanding Graduates.
Outstanding Individual of Construction of Study Style.

Research Interest

Design Automation, Cryptographic System Software-Hardware co-design, Privacy-Preserving Machine Learning, Machine Learning Application Hardware Acceleration, VLSI Digital signal processing, Hardware Security, Cybersecurity, Machine Learning Model Security, Engineering Education.

Research Experience

- Design BFV-HPS homomorphic encryption hardware system level implementation over FPGA data acceleration card for homomorphic matrix-vector evaluation. This custom system-level design explores the intermediate schedule features to increase the utilization of computation modules and parallelism opportunities.
- Design a novel Neural Network hardware implementation bit-flip testing and fixing mechanism, relying on discerning classification result disparities between a faulty Neural Network and its original counterpart. The idea is verified for image classification tasks.
- Collaborate on the design of a modular polynomial multiplication architecture, targeting Post-Quantum Cryptography candidates, during the NIST standardization process. Emphasize fast filtering technique for saber, high-parallel NTT/INTT operations, and optimized modular multiplier using Karatsuba algorithm for custom parameters to enhance overall efficiency in resource consumption and timing.
- Design a new PUF architecture, Noisy PUF (NoPUF), by investigating potential reconfiguration structures to incorporate noise. This noisy architecture enhances resistance against modeling attacks and empowers the designer to perform configuration using one-time programming.

Research Grant (Helped my advisor 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

Research Publications

Journal Articles

1 W. Tan, S.-W. Chiu, **A. Wang**, Y. Lao, and K. K. Parhi, "PaReNTT: Low-latency parallel residue number system and NTT-based long polynomial modular multiplication for homomorphic encryption," *IEEE Transactions on Information Forensics Security*, 2023.

2 W. Tan, **A. Wang**, X. Zhang, Y. Lao, and K. K. Parhi, "High-speed vlsi architectures for modular polynomial multiplication via fast filtering and applications to lattice-based cryptography," *IEEE Transactions on Computers*, pp. 1–12, 2023.

3 W. Tan, B. M. Case, **A. Wang**, S. Gao, and Y. Lao, "High-speed modular multiplier for lattice-based cryptosystems," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 68, no. 8, pp. 2927–2931, 2021.

4 **A. Wang**, W. Tan, Y. Wen, and Y. Lao, "NoPUF: A novel puf design framework toward modeling attack resistant PUFs," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 68, no. 6, pp. 2508–2521, 2021.

Conference Proceedings

1 **A. Wang**, B. Zhao, W. Tan, and Y. Lao, "NNTesting: Neural network fault attacks detection using gradient-based test vector generation," in *Proceedings of the 60th Annual Design Automation Conference 2023*, 2023, pp. 1–6.

2 **A. Wang**, W. Tan, and Y. Lao, "Integral sampler and polynomial multiplication architecture for lattice-based cryptography," in *2022 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)*, IEEE, 2022, pp. 1–6.

3 W. Tan, **A. Wang**, Y. Lao, X. Zhang, and K. K. Parhi, "Pipelined high-throughput NTT architecture for lattice-based cryptography," in *2021 Asian Hardware Oriented Security and Trust Symposium (AsianHOST)*, IEEE, 2021, pp. 1–4.

4 W. Tan, **A. Wang**, K. K. Parhi, and Y. Lao, "Area-efficient pipelined VLSI architecture for polar decoder," in *2020 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, IEEE, 2020, pp. 397–402.

Patents

1 K. K. Parhi, W. Tan, S.-W. Chiu, **A. Wang**, and Y. Lao, *Parallel polynomial modular multiplication using NTT and inverse NTT*, U.S. Patent Application 18,500,670, Filed: November 2, 2023.

2 K. K. Parhi, X. Zhang, W. Tan, **A. Wang**, and Y. Lao, *Low latency polynomial modulo multiplication over ring*, US Patent 17,582,560, Filed: January 24, 2022.

Professional activities

Conference Reviewer

AsianHOST • IEEE Asian Hardware Oriented Security and Trust Symposium 2021-2023

Professional activities (continued)

HOST	• IEEE International Symposium on Hardware Oriented Security and Trust	2023-2024
ISCAS	• IEEE International Symposium on Circuits and Systems	2019-2024
ISVLSI	• IEEE Symposium on VLSI	2022
MWSCAS	• IEEE International Midwest Symposium on Circuits and Systems	2020,2022,2023
SiPS	• IEEE International Workshop on Signal Processing Systems	2019-2020

Journal Reviewer

TCAS-I	• IEEE Transactions on Circuits and Systems I: Regular Papers
HaSS	• Journal of Hardware and Systems Security
	• The Journal of Supercomputing
OJCAS	• IEEE Open Journal of Circuits and Systems

Membership

2020–current • IEEE Graduate Student Member

Teaching

Graduate Teaching Assistant at Clemson University

ECE 2090 • Logic and Computing Devices Laboratory 2022 Fall-2023 Fall.

Perform ABET evaluation material collection and provide suggestions for in-class Lab Kit preparation.
Change the simulation software to the latest Logisim Evolution and prepare the usage tutorial.
Perform and update all required lab circuit board building diagrams according to the syllabus. Listed observed common mistakes for future reference.
Enrich lab capstone/final project topics with hints.
Enrollment: 71 students for 23 Fall, 35 students for 23 Spring, 41 students for 22 Fall.

ECE 4590/6590 • Integrated Circuit Design 2023 Fall.

Reformat HSPICE lab to using the Cadence SPECTRE tool.
Introduce Cadence RTL to GDSII workflow.
Enrollment: 25 students.

Graduate Grader Assistant at Clemson University

ECE 2010H	• Logic and Computing Devices	2020 Fall.
ECE 2070	• Basic Electrical Engineering	2019 Fall – 2020 Fall.
ECE 2720	• Computer Organization	2020 Fall – 2021 Fall.
ECE 3300	• Signals, Systems, and Transforms	2022 Spring.
ECE 3710	• Micro-controller Interfacing	2020 Fall – 2021 Fall.
ECE 4090	• Introduction to Linear System	2019 Spring, 2019 Fall.

Teaching (continued)

ECE 4270 • Communication Systems 2021 Spring - 2023 Spring.
Prepare solution and practice problems for Fall semesters.

Miscellaneous Experience

Conference Travel Grant

ISCAS 2022 • ISCAS 2022 Student Participation Grants

Graduate Travel Grant (GTG) from Clemson University Graduate Student Government

2023 Summer • Design Automation Conference (DAC) 2023, San Francisco, CA.
2022 Summer • International Symposium on Circuits and Systems (ISCAS) 2022, Austin, TX, USA.
2021 Fall • Design Automation Conference (DAC) 2021, San Francisco, CA/Virtual, USA.
2021 Spring • International Solid-State Circuits Conference (ISSCC) 2021, virtual, USA.

Course taken at Clemson University

CPSC/ECE 6780 • General Purpose Computation on Graphical Processing Units
CPSC 8400 • Design and Analysis of Algorithms
CPSC 8580 • Security in Emerging Computing and Networking Systems
ECE 6590 • Integrated Circuit Design
ECE 6930 • Algorithms for VLSI Design Automation (currently listed as ECE 6580)
ECE 8010 • Analysis of Linear Systems
ECE 8540 • Analysis of Tracking Systems
ECE 8930 • Hardware and AI
ESED 8000 • Seminar in Engineering and Science Education
ESED 8200 • Teaching Undergraduate Engineering
ESED 8500 • Special Topics in Engineering and Science Education (professoriate)
(currently offered as ESED 8880 Preparing for the Professoriate)
ESED 8610 • Practicum in Engineering, Science and Mathematics Education
ESED 8720 • Action Research in Engineering, Science and Mathematics Education
MATH 8560 • Theory of Error Correcting Codes
MATH 8570 • Cryptography
MATH 8710 • Machine Learning I
MATH 9850 • Blockchains, Security &Privacy
STAT 8010 • Statistical Methods I
STAT 8030 • Regression and Least Squares Analysis

Skills

Programming • C/C++/C#, OpenCL, CUDA, Python, R, Matlab, Verilog HDL, VHDL, LaTeX, SPICE, SPECTRE.

Skills (continued)

Tools	• TensorFlow, PyTorch, Xilinx Vitis, Xilinx Vivado, Cadence (XCELIUM), Synopsys (Verdi, Design Compiler)