

Yicheng Huang

School of Integrated Circuit Science and Engineering, Beihang University, Beijing, China

Email: huangyicheng@buaa.edu.cn | Tel: (+86) 182-2403-6908

Education

Beihang University, Beijing, China

Sep. 2023 – Jan. 2026 (Expected)

- M.S. in Integrated Circuit Science and Engineering

GPA: 3.86/4.0 (Rank: 4/96)

- **Advisor:** Xueyan Wang

Southwest Jiaotong University, Chengdu, China

Sep. 2019 – Jun. 2023

- B.S. in Electronic Science and Technology

GPA: 3.72/4.0 (Rank: 1/84)

- **Advisor:** Zhixiong Di

- **Coursework:** Digital Logic and Computer Composition Principle, Electronic Design Automation, Fundamentals of Digital Integrated Circuit Analysis and Design, Fundamentals of Analog Integrated Circuit Analysis and Design

Research Experience

Area-Optimized Modular Multiplier Design (Under reviewed by *IEEE TCAD* [2])

Feb. 2024 - Present

- **Sponsor:** CCF-Ant Research Fund
- **Key Contributions** (Motivated by the need for area-efficient modular multipliers in homomorphic encryption)
 - Integrated **Karatsuba decomposition** into parallel **NTT-friendly Montgomery Modular Multiplication**(MMM).
 - Developed automated **Karatsuba decomposition optimization search algorithm** to enhance area-efficiency.
 - Implemented the MMM on FPGA, achieving an average of **56% improvement** in **Area/Throughput** vs. SOTAs.

Homomorphic Encryption Processor (published in *DATE 2024* [4])

Apr. 2023 - Apr. 2024

- **Funding Agency:** Beijing Advanced Innovation Center for Future Blockchain and Privacy Computing.
- **Key Contributions:** Designed a fully pipelined multi-point transpose unit for Number Theoretic Transforms (NTT); deployed the NTT IP on Alveo U280 with Xilinx Vitis; and presented as a poster at *DATE 2024*.

ShangMi Algorithm Hardware Accelerator IP (published in *ITC-Asia 2024* [3])

Oct. 2022 - Dec. 2023

- **Funding Agency:** Beijing Advanced Innovation Center for Future Blockchain and Privacy Computing.
- **Key Contributions:** Designed the architecture of hardware IP for elliptic curve cryptography (ECC) and implemented the ECC IP on Xilinx Kintex UltraScale FPGA, achieving 12,000 signatures/sec and 8,000 verifications/sec, supporting SM2, Secp256r1, and Secp256k1 curves.
- **Note:** Received the **Best Paper Nomination Award** at *ITC-Asia 2024*; continued sponsorship by the **CCF-Huawei Populus Grove Fund** (Feb. 2025 - Jan. 2026).

Competition Experience

A Dual-Core System-on-Chip with TEE Support Based on E902 Core

Mar. 2023 - Aug. 2023

- **Award:** National Second Prize in China College IC Competition (T-Head Semiconductor Cup Track)
- **Key Contributions:** Designed and deployed the **System-on-Chip** (SoC) on FPGA; implemented **Mailbox**, **IOPMP** (Input/Output Physical Memory Protection), and **hardware cryptographic accelerator**; built **secure boot mechanisms**; and support **Trusted Execution Environment** (TEE) security feature.

A RISC-V SoC with CNN Accelerator for Marine Bioacoustics Classification

Aug. 2021 - Nov. 2021

- **Award:** National First Prize (**1st Place in Undergraduate Division**) in China Undergraduate Embedded Systems & Chip Design Competition (Chip Design Track)
- **Key Contributions:** Designed FFT IP; deployed the SoC on FPGA; implemented custom RISC-V instructions and wrote IP drivers; conducted Spyglass syntax checks.

Neural Network based SAR Image Compression Accelerator

Mar. 2021 - Aug. 2021

- **Award:** **First Place** in China College IC Competition (T-Head Semiconductor Cup Track)
- **Project Overview:** Designed a neural network based Synthetic Aperture Radar (SAR) image compression accel-

erator and integrated it into the open-source Wujian 100 SoC platform to accelerate the compression task.

- **Key Contributions (Mainly Embedded System Development):** developed C drivers for the accelerator IP; and set up a physical demonstration system.

Publications

- [1] Yuntao Wei, Xueyan Wang, Song Bian, **Yicheng Huang**, Weisheng Zhao, and Yier Jin, "SparseH: Efficient Homomorphic Matrix Multiplication via Sparsity Encoding for Privacy-Preserving Machine Learning," *2025 IEEE/ACM International Conference on Computer Aided Design (ICCAD)* (under review).
- [2] **Yicheng Huang**, Xueyan Wang, Shicheng Ma, Song Bian, Meng Li, Gang Qu and Weisheng Zhao, "KD-Finder: A Karatsuba Decomposition Optimization Finder for NTT-Friendly Montgomery Modular Multiplication", *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* (under review).
- [3] **Yicheng, Huang** and Xueyan, Wang and Tianao, Dai and Jianlei, Yang and Zhaojun, Lu and Xiaotao, Jia and Gang, Qu and Weisheng, Zhao, "LLP-ECCA: A Low-Latency and Programmable Framework for Elliptic Curve Cryptography Accelerators," *2024 IEEE International Test Conference in Asia (ITC-Asia)* (**Best Paper Candidate**)
- [4] Zhenyu, Guan and Yongqing, Zhu and **Yicheng, Huang** and Luchang, Lei and Xueyan, Wang and Hongyang, Jia and Yi, Chen and Bo, Zhang and Jin, Dong and Song, Bian, "ESC-NTT: An Elastic, Seamless and Compact Architecture for Multi-Parameter NTT Acceleration," *2024 Design, Automation & Test in Europe Conference & Exhibition (DATE)*.
- [5] Yuntao Wei, Xueyan Wang, Song Bian, **Yicheng Huang**, Weisheng Zhao, and Yier Jin, "PPGNN: Fast and Accurate Privacy-Preserving Graph Neural Network Inference via Parallel and Pipelined Arithmetic-and-Logic FHE Accelerator," *2024 ACM/IEEE Design Automation Conference (DAC)*.

Honors and Awards

The Merit Student of Beihang University	2024
First Class Graduate Academic Scholarship	2024
2024 ITC-Asia Best Paper Condidate	2024
Outstanding Graduate Student of Southwest Jiaotong University	2023
National Second Prize in China College IC Competition (T-Head Semiconductor Cup Track)	2023
HollySys Scholarship	2022
National First Prize (1st Place in Undergraduate Division) in China Undergraduate Embedded Systems & Chip Design Competition (Chip Design Track)	2021
National Second Prize (<10%) in National Undergraduate Electronics Design Contest	2021
First Place (Top 1%) in China College IC Competition (T-Head Semiconductor Cup Track)	2021
First Class Scholarship at the School Level	2021
Second Class Scholarship at the School Level	2020

Skills

- **Programming:** C, Python, Verilog
- **IC Design**
 - **Tools:** Modelsim, VCS, Design compiler, formality,...
 - **Domain Knowledge:** AMBA, SoC, RISC-V,...
- **Embedded Systems Development**
 - **Hardware:** PCB design and Layout with Altium Designer
 - **Software:** MCU (like STM32, ESP32), FPGA (Xilinx Vitis, Xilinx Vivado and Altera Quartus)
- **Languages:** Chinese (Native), English (CET-6: 523/710, IELTS Preparing)