Jing Tian, Ph.D., Associate Research Fellow

Contact Information

School of Electronic Science and Engineering
Nanjing University
No.163, Xianlin Ave., Nanjing, 210023, P.R.China

Mobile Phone: (+86) 147-5193-0711

Email: tianjing@nju.edu.cn

Research Interests

Very Large Scale Integration (VLSI), Forward Error Correction (FEC), Post-Quantum Cryptography (PQC), Blockchain, Homomorphic Encryption

Education

PhD, School of Electronic Sci. & Eng., Nanjing University, Nanjing, China Aug. 2020

Major: Information and Communication Engineering

Adviser: Prof. Zhongfeng Wang (*ICAIS Lab*)

Thesis: "Optimization and Implementation of Typical Algorithms for Error Correction Coding and Encryption in Modern Communications"

BSEE, School of Electronic Sci. & Eng., Nanjing University, Nanjing, China June 2015

Major: Microelectronics

Research Experience

Aug. 2020 – present: **Associate Research Fellow**, Nanjing University, Nanjing, China

- Proposed a novel FGPA design for the supersingular isogeny key encapsulation (SIKE) protocol (a PQC candidate approved by the NIST) with the best performance among existing works.
- As a team lead, designed a high-speed architecture for the network of HE with AI.
- As a team lead, presented a novel ASIC design for the VDF of blockchain, well adapting to the Chia blockchain.
- As a team lead, developed an ultra-low area and power modular multiplier used for the SM2 standard.
- Deeply involved in the design of efficient FEC codes for the next-generation Ethernet standard.

Sep. 2015 – July 2020: **Ph.D. Student**, Nanjing University, Nanjing, China

- Designed a 21.66 Gbps nonbinary LDPC decoder based on an MLGD algorithm for high-speed communications.
- Introduced a mathematical model to reduce the input data before sending into an NB-LDPC decoder.
- Developed two efficient T-EMS decoding algorithms for NB-LDPC Codes based the mathematical model.
- Devised an optimized trellis-based min-max decoder for NB-LDPC codes, saving more than 1/3 hardware resources without any performance loss.
- Proposed a new data representation for the supersingular isogeny-based PQC and implemented the software for SIKE by adopting the new method.

Honors and Awards

Excellent Graduate, Nanjing University	2020
National Scholarship, China	2019
Excellent Student Award, Nanjing University	2018
Second Prize, Doctoral Fellowship for Excellence, Nanjing University	2018
Kwang-Hua scholarship, Kwang-Hua Education Foundation	2017
Third Prize, China College IC Competition, China	2017
Excellent Graduate, Nanjing University	2015
Moved Youth Olympic Figures, Nanjing University	2014
National Encouragement Scholarship, China	2013

Journal Publications

1. **J. Tian**, B. Wu, and Z. Wang, "High-Speed FPGA Implementation of SIKE Based on An Ultra-Low-Latency Modular Multiplier," submitted to IEEE Transactions on Circuits and Systems I: Regular Papers in Jan. 2021, currently under the 2nd round of review

2. **J. Tian**, P. Wang, Z. Liu, J. Lin, Z. Wang, and J. Großschädl, "Efficient software implementation of the SIKE protocol using new data representation," IEEE Transactions on Computers, pp. 1-1, 2021

3. S. Song, **J. Tian**, J. Lin and Z. Wang, "An Improved Reliability-Based Decoding Algorithm for NB-LDPC Codes," in IEEE Communications Letters, vol. 25, no. 4, pp. 1153-1157, April 2021

4. **J. Tian**, J. Lin, and Z. Wang, "Fast modular multipliers for supersingular isogeny-based post-quantum cryptography," IEEE Transactions on Very Large Scale Integration (VLSI) Systems, pp. 1-13, 2020

5. **J. Tian**, S. Song, J. Lin and Z. Wang, "Optimized Trellis-Based Min-Max Decoder for NB-LDPC Codes," in IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 67, no. 1, pp. 57-61, Jan. 2020

6. S. Song, H. Cui, **J. Tian**, J. Lin and Z. Wang, "A Novel Iterative Reliability-Based Majority-Logic Decoder for NB-LDPC Codes," in IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 67, no. 8, pp. 1399-1403, Aug. 2020

7. **J. Tian**, S. Song, J. Lin and Z. Wang, "Efficient T-EMS Based Decoding Algorithms for High-Order LDPC Codes," in IEEE Access, vol. 7, pp. 50980-50992, 2019

8. W. Li, **J. Tian**, J. Lin and Z. Wang, "Modified GII-BCH Codes for Low-Complexity and Low-Latency Encoders," in IEEE Communications Letters, vol. 23, no. 5, pp. 785-788, May 2019

9. **J. Tian**, J. Lin and Z. Wang, "A 21.66 Gbps Nonbinary LDPC Decoder for High-Speed Communications," in IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 65, no. 2, pp. 226-230, Feb. 2018

Conference Publications

1. X. Hu, Minghao Li, **J. Tian** and Z. Wang, "DARM: A Low-Complexity and Fast Modular Multiplier for Lattice-Based Cryptography," 2021 IEEE International Conference on Application-specific Systems, Architectures and Processors (ASAP), 2021

2. D. Zhu, **J. Tian** and Z. Wang, "Low-Latency Architecture for the Parallel Extended GCD Algorithm of Large Numbers," 2021 IEEE International Symposium on Circuits and Systems (ISCAS), 2021

3. Y. Song, X. Hu, W. Wang, **J. Tian** and Z. Wang, "High-Speed and Scalable FPGA Implementation of the Key Generation for the Leighton-Micali Signature Protocol," 2021 IEEE International Symposium on Circuits and Systems (ISCAS), 2021

4. Y. Song, D. Zhu, **J. Tian**, and Z. Wang, "A High-Speed Architecture for the Reduction in VDF Based on a Class Group," 2020 IEEE International System-on-Chip Conference (SOCC), 2020

5. B. Wu, **J. Tian**, X. Hu and Z. Wang, "A Novel Modular Multiplier for Isogeny-Based Post-Quantum Cryptography," 2020 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), 2020

6. D. Zhu, Y. Song, **J. Tian**, Z. Wang and H. Yu, "An Efficient Accelerator of the Squaring for the Verifiable Delay Function Over a Class Group," 2020 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS), 2020
7. X. Hu, **J. Tian** and Z. Wang, "Fast Permutation Architecture on Encrypted Data for Secure Neural Network Inference," 2020 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS), 2020
8. **J. Tian**, J. Lin and Z. Wang, "Ultra-Fast Modular Multiplication Implementation for Isogeny-Based Post-Quantum Cryptography," 2019 IEEE International Workshop on Signal Processing Systems (SiPS), 2019
9. S. Song, **J. Tian**, J. Lin and Z. Wang, "A Novel Low-Complexity Joint Coding and Decoding Algorithm for NB-LDPC Codes," 2019 IEEE International Symposium on Circuits and Systems (ISCAS), 2019
10. S. Song, **J. Tian**, J. Lin and Z. Wang, "Redundancy-Aided Iterative Reliability-Based Majority-Logic Decoding for NB-LDPC Codes," 2019 IEEE 13th International Conference on ASIC (ASICON), 2019
11. **J. Tian**, J. Lin and Z. Wang, "An Efficient NB-LDPC Decoding Algorithm for Next-Generation Memories," 2018 IEEE International Symposium on Circuits and Systems (ISCAS), 2018
12. **J. Tian**, J. Lin and Z. Wang, "Analysis of the Dual-Threshold-Based Shrinking Scheme for Efficient NB-LDPC Decoding," 2018 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS), 2018
13. S. Song, J. Lin, **J. Tian** and Z. Wang, "A reduced complexity decoding algorithm for NB-LDPC codes," 2017 IEEE 17th International Conference on Communication Technology (ICCT), 2017

Patents

Z. Wang, **J. Tian**, B. Wu. "Device to obtain the result of modular multiplication for supersingular isogeny-based cryptography", China Patent No.202110006918.7

Z. Wang, P. Wang, **J. Tian**, J. Lin. "Hardware architecture and method to compute modular multiplication of supersingular isogeny-based post-quantum cryptography", China Patent No.202110006918.7

Z. Wang, B. Wu, **J. Tian**. "Hardware architecture and method to compute iterative multiplication and addition", China Patent No.202011254262.2

Z. Wang, **J. Tian**, P. Wang, J. Lin. "Method and device to generate public key for the supersingular isogeny key encapsulation protocol", China Patent No.202010412895.5

Z. Wang, **J. Tian**, J. Lin. "A high-performance low-complexity NB-LDPC decoding method", China Patent No.201711499749.5

Z. Wang, **J. Tian**, J. Lin. "A general simplification method suitable for almost all NB-LDPC decoding", China Patent No.201711499748.0

Z. Wang, **J. Tian**, J. Lin. "A high-speed decoder and the decoding method for NB-LDPC codes", China Patent No.201710149925.6

Presentations

”Fast Implementation of Post-Quantum Encryption Protocol Based on Elliptic Curve”, invited talk at CCF China Test Conference, Xi’an, China, 2020

”VLSI design for digital communication”, Technical talk at Sun Yat-Sen University, Guangzhou, China, 2019

”Ultra-Fast Modular Multiplication Implementation for Isogeny-Based Post-Quantum Cryptography”, IEEE International Workshop on Signal Processing Systems (SiPS), Nanjing, China, 2019

”An Efficient NB-LDPC Decoding Algorithm for Next-Generation Memories”, IEEE International Symposium on Circuits and Systems (ISCAS), Florence, Italy, 2018

”Analysis of the Dual-Threshold-Based Shrinking Scheme for Efficient NB-LDPC Decoding”, IEEE Asia Pacific Conference on Circuits and Systems (APCCAS), Chengdu, China, 2018

Professional Activities

Program Committee:
IEEE 21st International Conference on Communication Technology (ICCT) 2021

Technical Reviewer:
Journal:
IEEE Transactions on Circuits and Systems I: Regular Papers, 2018 - present
IEEE Transactions on Circuits and Systems II: Express Briefs, 2017 - present
IEEE Transactions on Very Large Scale Integration (VLSI) Systems
IEEE Transactions on Vehicular Technology
IEEE Transactions on Signal Processing
IEEE Access
China Communications
IET Circuits, Devices Systems
ETRI Journal
Concurrency and Computation: Practice and Experience

Conference:
IEEE International Symposium on Circuits and Systems (ISCAS), 2017 - present
IEEE International Workshop on Signal Processing Systems (SiPS), 2018 - present
IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2018, 2019
IEEE International Conference on Computer and Communications (ICCC), 2019
IEEE Asia Pacific Conference on Circuits and Systems (APCCAS), 2018
IEEE International Conference on Communication Technology (ICCT), 2018
IEEE International Conference on ASIC (ASICON), 2017