Xuanle Ren

Curriculum Vitae

(+86) 186-1833-0780
renxuanle@126.com
renxuanle.github.io

Work Experience

2022.10 – present **Technical Lead/Research Scientist**, *Hash Innovation, Bitmain Inc.*, Shanghai, China.

Work on novel architecture design for zero-knowledge proof (ZKP). Also work on design and optimization for ULSI circuit, through developing novel EDA algorithms/tools for front-end netlist design, back-end placement/routing, and system-technology co-optimization (STCO).

2018.11 – 2022.10 **Technical Lead/Research Scientist**, *DAMO Academy, Alibaba Group*, Shanghai, China.

Lead research on hardware acceleration, algorithm, and application for privacy-preserving computing in Computation Technology Lab. Selected projects include hardware acceleration for fast homomorphic encryption, hardware-algorithm co-design for homomorphic database, TEE design for AI application, and RISC-V TEE design.

2012.9 – 2018.9 **Research Assistant**, *Carnegie Mellon University*, Pittsburgh, PA.

Research focused on developing data-mining techniques for addressing IC security problems. Advised by Prof. Shawn Blanton and Prof. Vitor Grade Tavares (University of Porto).

Education

2012.8 – 2018.9 **Ph.D. in Electrical and Computer Engineering**, *Carnegie Mellon University*, Pittsburgh, PA.

2008.9 – 2012.7 **B.S. in Microelectronics & B.A., Economics**, *Peking University*, Beijing, China.

Publications

Journal

F. Zhang, B. Yang, Y. Zhang, **X. Ren**, S. Bhasin, K. Ren, "Design and evaluation of fluctuating power logic to mitigate power analysis at the cell level", *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD)*, 2021, (CCF-A).

X. Ren, F. Torres, S. Blanton, V. Tavares, "IC protection against JTAG-based attacks", *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD)*, 2019, (CCF-A).

Conference

X. Ren, Z. Chen, Y. Lu, R. Zhong, W. Lu, J. Zhang, Y. Zhang, Z. Gu, H. Wu, X. Zheng, H. Liu, T. Chu, C. Hong, C. Wei, Y. Xie, "CHAM: A customized homomorphic encryption accelerator for fast matrix-vector product", *ACM/IEEE Design Automation Conference (DAC)*, 2023, (CCF-A).

X. Ren[†], L. Su[†], S. Bian[*], S. Wang, F. Li, C. Li, F. Zhang, Y. Xie, "HEDA: Multi-attribute unbounded aggregation over homomorphically encrypted database", *Proceedings of the Very Large Data Bases (VLDB) Endowment*, 2023, (CCF-A).

X. Ren, S. Blanton, V. Tavares, "Detection of IJTAG attacks using LDPC-based feature reduction and machine learning", *IEEE European Test Symposium (ETS)*, 2018.

X. Ren, S. Blanton, V. Tavares, "A learning-based approach to secure JTAG against unseen scan-based attacks", *IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2016.

X. Ren, V. Tavares, S. Blanton, "Detection of illegitimate access to JTAG via statistical learning in chip", *Design, Automation & Test in Europe Conference & Exhibition (DATE)*, 2015, (CCF-B).

X. Ren, M. Martin, S. Blanton, "Improving accuracy of on-chip diagnosis via incremental learning", *IEEE VLSI Test Symposium (VTS)*, 2015.

Preprint

X. Ren, X. Cui, "An enclave-based TEE for SE-in-SoC in RISC-V industry", *Embedded World Exhibition*, 2020.

P. Xie, **X. Ren**, G. Sun, "Customizing trusted AI accelerators for efficient privacy-preserving machine learning", *arXiv:2011.06376*, 2020.

Talks

2022 **Hardware acceleration for fully homomorphic encryption (invited talk)**, *Design Automation Conference*.

Academic Service

Reviewer

2022 **Conference on Cryptographic Hardware and Embedded Systems**.
2018-2020 **International Conference on Computer-Aided Design**.
2019 **IEEE Embedded Systems Letters**.
2019 **International Journal of Electrical and Computer Engineering**.
2018 **Transactions on Emerging Topics in Computing**.
2015-2018 **VLSI Test Symposium**.
2016-2018 **European Test Symposium**.
2016-2017 **International Test Conference**.
2016 **International Symposium on On-Line Testing and Robust System Design**.

Awards

2021 **Shanghai Industrial Elite** , *Shanghai Municipal Commission of Economy and Informatization*.

2018 **Award for Outstanding Self-financed Students Abroad** , *Ministry of Education of China*.

2012-2017 **Carnegie Mellon Porgual Ph.D. Fellowship**, *Carnegie Mellon University, Foundation for Science and Technology in Portugal*.

Computer Skills

Programming Python, C/C++, Tensorflow, PyTorch, MATLAB
Hardware SystemVerilog, FPGA, Design-for-Test
Other LaTeX

Projects

2022.10 – present **Hardware Acceleration for ZKP**, *Bitmain Inc.*.
Zero-knowledge proof is a fundamental technique for building privary-preserving blockchains. However, ZKP algorithms, usually built on large-degree lattice, require quite heavy computation and memory access. Thus, acceleration these algorithms using ASICs becomes necessary. In this work, we study ASIC acceleration for typical ZKP algorithms, and also explore algorithm and hardware co-design, considering that ZKP algorithm is still evolving.

2022.10 – present **ULSI Circuit Optimization**, *Bitmain Inc.*.
Following the Moore's Law, circuit design using ultra large scale integration (ULSI) leads to higher density of transistor, higher performance, and lower power consumption. However, ULSI design poses more challenges that might be addressed using cross-layer co-optimization (such as DTCO and STCO) as well as support of novel, efficient design methodologies and EDA tools. My work is to develop new methods and algorithms to pursue low-power, high-performance circuit design.

2021.9 – 2022.10 **Privacy-preserving Database Using Homomorphic Encryption**, *Alibaba*.
Privacy of outsourced database and subsequent queries should be preserved, such that the cloud provider can neither reverse the database nor the user queries. In this work, we aim to preserve the privacy of database and queries using fully homomorphic encryption (FHE), where both storage and computation are based on ciphertext rather than plaintext. This work has been published in VLDB'2022.

2020.5 – 2022.12 **Hardware Acceleration for Homomorphic Encryption**, *Alibaba*.

Homomorphic Encryption (HE) is a privacy-preserving method that can do computation on encrypted data rather than plaintext. HE computation is commonly 1,000 to 1,000,000 more intensive than computation on plaintext, thus limiting its wide application. In this work, we designed a hardware accelerator supporting FHE computations, and implemented the accelerator using Xilinx FPGA U280. To enable simulation/emulation, we also developed software stack (driver and runtime). The FPGA demonstrates acceleration of neural network inference by more than 200 times. The hardware/software system has been integrated into *Alibaba Ant-Chain All-in-One Machine*. This work has been published in DAC'2023.

2019.5 – 2019.11 **Trusted AI Acceleratiors**, *Alibaba*.

TEE, such as Intel SGX, enables trusted computation within CPUs. However, due to limited memory space and computing power, TEE is not suitable for AI applications which usually involve intensive computations. In this work, we propose to extend the trusted boundary from CPU to AI accelerator, such that both privacy and high performance can be achieved. This extension causes 0.9% to 30% hardware overhead. A paper titled *Customizing Trusted AI Accelerators for Efficient Privacy-Preserving Machine Learning* was reported.

2019.8 – 2020.3 **RISC-V TEE Design**, *Alibaba*.

We designed a light-weight TEE architecture for RISC-V. In addition, Direct-Memory-Access (DMA) is utilized to accelerate data transfer between isolated data enclaves. Compared to existing solutions (e.g., ARM TrustZone), our solution achieves better usability without compromising security.

2013.10 – 2017.12 **IC Intrusion detection Using On-chip Learning**, *Carnegie Mellon University*.

JTAG, the testing interface for IC, is primarily used for manufacturing test, but also used for in-field debug. Hence, JTAG needs to be left intact after manufacturing test, thus providing a backdoor that can be exploited by illegitimate user. Attackers have demonstrated their capability of reverse engineering the system design and dumping credential on-chip data. We improve JTAG security via monitoring real-time JTAG operation, analyzing user behavior using machine learning algorithm, and encrypting the JTAG if a potential attacker is detected. The proposed machine learning detectors are further implemented in *Xilinx* Zynq7000 ZC706 FPGA. This work has been published in DATE'2015, ISVLSI'2016, ETS'2018, and TCAD'2019.

2012.9 – 2013.9 **IC Test and Diagnosis Using Machine Learning**, *Carnegie Mellon University*.

Ensuring lifetime reliability of integrated systems has become a central concern. Although manufacturing tests are performed to help ensure reliability, a chip may still degrade and even fail in the field due to early-life failure and wear-out (also named aging). We proposed to implement on-chip test and diagnosis functionality to ICs, and test the chip periodically. Hence, any potential fault can be detected before fatal consequence occurs. To improve diagnosis accuracy in real-time, we developed a dynamic machine learning algorithm, named dynamic k-nearest-neighbor (k-NN), which can adapt to the test results in real-time. The dynamic k-NN is also implemented in *Xilinx* Zynq7000 ZC706 FPGA. This work has been published in VTS'2015.