# Xuanle Ren

*Curriculum Vitae*

*Hamerschlag Hall 2136*
*5000 Forbes Avenue, Pittsburgh*
*PA 15213, USA*
☎ *(+86) 186-1833-0780*
✉ *renxuanle@126.com*
*staff.org.edu/∼jsmith*

## Experience

2018.11 – 2022.10 **Technical Lead/Research Scientist**, *DAMO Academy, Alibaba Group*, Shanghai, China.
Lead research on privacy-preserving computing and IC security in Computation Technology Lab. Selected projects include hardware acceleration for Homomorphic Encryption, TEE design for AI application, RISC-V TEE design and privacy-preserving database.

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 Tavares (University of Porto).

## Education

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

2012.8 – 2015.5 **M.S. 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.

## Research and Projects

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. A paper titled *Privacy-preserving Storage and Query for Outsourced Database Using Homomorphic Encryption* is in preparation.

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*. A paper titled *H1: Accelerating Linear Computations on Encrypted Data* is in preparation.

2019.5 – 2019.11 **Accelerating AI Computation Using Trusted Execution Environment (TEE)**, *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.

2017.8 – 2018.1 **Intrusion Detection of IEEE P1687 Devices Using Machine Learning**, *Carnegie Mellon University*.

Similar to traditional ICs with a JTAG, a P1687 device also suffers from the risk of being intruded because its testing/debugging process is also operated by the JTAG. However, detection of P1687 intrusion is different from the JTAG, namely, 1) hierarchical network, and 2) simultaneous access to multiple on-chip instruments, and 3) simultaneous execution of multiple commands. We aim to detect possible intrusion to P1687 devices using sequence analyses techniques.

2016.10 – 2017.6 **IC Security via Obfuscation**, *Carnegie Mellon University*.

As ICs are more manufactured in off-shore foundries, the IC/IP may be illegitimately used by untrusted foundries for piracy, overproduction, clone and reverse engineering. Obfuscating the functionality of the IC/IP becomes a popular countermeasure. We aimed to achieve obfuscation through splitting the IC/IP functionality such that a part of the design is manufactured in on-shore foundries. Then we analyzed the feasibility by evaluating the overhead (including latency, area, and power) and test issue.

2015.8 – 2016.8 **Automotive Security**, *Carnegie Mellon University*.

Security is an essential concern for Internet of vehicles (IoV). Attackers have demonstrated their capability of intruding the internal network of a vehicle and controlling the vehicle remotely. We enhanced automotive security through monitoring the internal network of vehicles. Specifically, the traffic of the CAN/FlexRay bus is monitored, and any abnormal traffic or transferred data is reported as a potential security problem.

2015.5 – 2015.8 **IC Design Bug Detection Using Machine Learning**, *Carnegie Mellon University*.

Post-silicon validation is a time-consuming process, especially when a design is modified or upgraded, new tests need to be generated for validating the design. To accelerate the validation, we use machine learning to find tests that can detect bugs more efficiently. Further, more similar tests are generated for validation such that the validation can converge to the expected fault coverage.

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.

2013.2 – 2013.5 **A Pipelined MIPS Design**, *Carnegie Mellon University*.

MIPS is a reduced instruction set computer (RISC) instruction set architecture (ISA). In this project, a MIPS processor was implemented using Verilog. The processor consists in a pipelining structure with five stages, namely fetch, decode, execute, memory-operation and write-back. More features, namely, branch prediction, memory hierarchy and cache coherence, are further implemented in the processor.

2012.9 – 2013.9 **IC Test and Diagnosis Using Dynamic k-NN**, *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.

2011.9 – 2012.6 **$\Sigma$-$\Delta$ ADC Design**, *Peking University*.

This is my undergraduate thesis. A 2nd-order closed-loop $\Sigma$-$\Delta$ ADC read-out circuit for MEMS accelerometer was designed. The circuit is built using XFAB 0.35$\mu m$ CMOS process. Supply source is 3.3V. Sampling frequency is 330MHz. Over-sampling ratio is 330. Effective number of bits (ENOB) is 11. In order to reduce noise, fully-differential structure, correlated-double-sampling (CDS), input common-mode feedback (ICMFB) and output common-mode feedback (OCMFB) are used.

## Computer Skills

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

## 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", *60th 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.

## Academic Service

### Invited talks

2022 **Tutorial on Fully Homomorphic Encryption**, *The 59-th Design Automation Conference.*

### Peer-review for conference/journal papers

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 (100 Total)**, *Shanghai Municipal Commission of Economy and Informatization.*

2018 **Award for Outstanding Self-financed Students Abroad (500 Total)**, *Ministry of Education of China.*

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