

# Shanquan Tian

✉ shanquan.tian@yale.edu • 🌐 caslab.csl.yale.edu/~shanquan  
10 Hillhouse Avenue, Room 523, New Haven, CT 06520

## Work Experience

---

**Google** | Software Engineer March 2023 - Present  
*Sunnyvale, California*

- Worked with Google Core ML - ML Performance and Co-design team
- Focused on LLM infra performance and Hardware/Software Co-design; Conducted analysis and co-design on current and future AI accelerators for Google Large Scale Distributed AI Infrastructure, especially to accommodate emerging Large language Models (LLMs).

**Yale University** | Research Assistant and Teaching Fellow September 2017 - February 2023  
*New Haven, Connecticut*

- Working as a Research Assistant in the field of cloud infrastructure research
- Working as a Teaching Fellow to help lead lab sessions, hold office hours and proctor exams

**Google** | Software Engineering Intern June 2022 - August 2022  
*Sunnyvale, California*

- Worked with Google Technical Infrastructure team
- Contributed to the production codebase which manages millions of node machines of Google Cloud

**Alibaba Cloud (U.S.)** | Research Intern July 2020 - August 2020  
*Sunnyvale, California (Remote)*

- Worked with the cloud heterogeneous acceleration team
- Contributed to the computing acceleration of Alibaba Cloud

## Education

---

**Yale University** Sept. 2017 - Feb. 2023  
*Doctor of Philosophy (Ph.D.), Advisor: Prof. Jakub Szefer*  
Computer Engineering, Department of Electrical Engineering

**Yale University** Sept. 2017 - May 2020  
*Master of Philosophy (M.Phil.) and Master of Science (M.S.)*  
Computer Engineering, Department of Electrical Engineering

**University of Science and Technology of China (USTC)** Sept. 2013 - June 2017  
*Bachelor of Science (B.S.), Applied Physics*

## Peer-reviewed Publications

---

- **Shanquan Tian**, Shayan Moini, Daniel Holcomb, Russell Tessier, and Jakub Szefer. "A Practical Remote Power Attack on Machine Learning Accelerators in Cloud FPGAs" in 2023 Design, Automation and Test in Europe Conference, **DATE'23**, April 2023.
- Ilias Giechaskiel, **Shanquan Tian**, Jakub Szefer. "Cross-VM Covert-and Side-Channel Attacks in Cloud FPGAs" in ACM Transactions on Reconfigurable Technology and Systems, **TRETS**, 2022.
- Ilias Giechaskiel, **Shanquan Tian**, Jakub Szefer. "Cross-VM Information Leaks in FPGA-Accelerated Cloud Environments" in Proceedings of the International Symposium on Hardware Oriented Security and Trust, **HOST'22 (Best Paper Candidate)**, 2022.
- Shayan Moini, **Shanquan Tian**, Daniel Holcomb, Jakub Szefer, and Russell Tessier. "Power Side-Channel Attacks on BNN Accelerators in Remote FPGAs" in IEEE Journal on Emerging and Selected Topics in Circuits and Systems, **JETCAS**, 2021.
- **Shanquan Tian**, Shayan Moini, Adam Wolnikowski, Daniel Holcomb, Russell Tessier, and Jakub Szefer. "Remote Power Attacks on the Versatile Tensor Accelerator in Multi-Tenant FPGAs" in Proceedings of the International Symposium on Field-Programmable Custom Computing Machines, **FCCM'21 (Best Paper Candidate)**, May 2021.
- **Shanquan Tian**, Ilias Giechaskiel, Wenjie Xiong, and Jakub Szefer. "Cloud FPGA Cartography using PCIe Contention"

- in Proceedings of the International Symposium on Field-Programmable Custom Computing Machines, **FCCM'21**, May 2021.
- Shayan Moini, **Shanquan Tian**, Jakub Szefer, Daniel Holcomb, and Russell Tessier. "Remote Power Side-Channel Attacks on BNN Accelerators in FPGAs" in 2021 Design, Automation and Test in Europe Conference, **DATE'21**, February 2021.
- **Shanquan Tian**, Andrew Krzywosz, Ilias Giechaskiel and Jakub Szefer. "Cloud FPGA Security with RO-Based Primitives" in International Conference on Field-Programmable Technology, **FPT'20**, IEEE, 2020.
- Wen Wang, **Shanquan Tian**, Bernhard Jungk, Nina Bindel, Patrick Longa, and Jakub Szefer, "Parameterized Hardware Accelerators for Lattice-Based Cryptography and Their Application to the HW/SW Co-Design of qTESLA", in Proceedings of the Conference on Cryptographic Hardware and Embedded Systems, **CHES'20**, September 2020.
- **Shanquan Tian**, Wenjie Xiong, Ilias Giechaskiel, Kasper Rasmussen and Jakub Szefer. "Fingerprinting Cloud FPGA Infrastructures" in Proceedings of the 2020 ACM/SIGDA International Symposium on Field-Programmable Gate Arrays, **FPGA'20**, ACM, 2020.
- **Shanquan Tian**, Wen Wang and Jakub Szefer. "Merge-Exchange Sort Based Discrete Gaussian Sampler with Fixed Memory Access Pattern" in International Conference on Field-Programmable Technology, **FPT'19**, IEEE, 2019.
- **Shanquan Tian**, and Jakub Szefer. "Temporal Thermal Covert Channels in Cloud FPGAs" in Proceedings of the ACM/SIGDA International Symposium on Field-Programmable Gate Arrays, **FPGA'19**, ACM, 2019.

## Teaching Experience

---

- |   |                           |
|---|---------------------------|
| <b>Teaching Fellow</b>   Yale University, New Haven, CT, USA<br><i>Introduction to Electronics (EENG200)</i>          | Fall 2022                 |
| <b>Teaching Fellow</b>   Yale University, New Haven, CT, USA<br><i>Cloud FPGA (EENG428)</i>                           | Spring 2022               |
| <b>Teaching Fellow</b>   Yale University, New Haven, CT, USA<br><i>Introduction to Computer Engineering (EENG201)</i> | Spring 2020 & Spring 2019 |

## Presentations & Invited Talks

---

- Conference Talks**.....
- Invited talk at FPGA'23, Workshop on Security for Custom Computing Machines (SCCM), "Remote Power Attacks against Machine Learning Accelerators in Cloud FPGAs", Monterey CA, February 2023
  - "Cross-VM Information Leaks in FPGA-Accelerated Cloud Environments" at HOST'22, Washington, D.C., June 2022
  - "Remote Power Attacks on the Versatile Tensor Accelerator" at FCCM'21, virtual, May 2021
  - "Cloud FPGA Cartography using PCIe Contention" at FCCM'21, virtual, May 2021
  - "Cloud FPGA Security with RO-Based Primitives" at FPT'20, virtual, December, 2020
  - "Fingerprinting Cloud FPGA Infrastructures" at FPGA'20, Seaside, CA, USA, February 2020
  - "Merge-Exchange Sort Based Discrete Gaussian Sampler with Fixed Memory Access Pattern" at FPT'19, Tianjin, China, December 2019
  - "Temporal Thermal Covert Channels in Cloud FPGAs" at FPGA'19, Seaside, CA, USA, February 2019
- Hardware Demo**.....
- "Cross-VM Information Leaks in FPGA-Accelerated Cloud Environments", Hardware Demo at the International Symposium on Hardware Oriented Security and Trust (HOST'22), June 2022
  - "Fingerprinting Cloud FPGA Infrastructures", Hardware Demo at the International Symposium on Hardware Oriented Security and Trust (HOST'20), December 2020

## Academic Services

---

- Symposium Organizer for Yale Cloud Computing and FPGA Security Symposium (CCFS) 2022
- Invited reviewer for IEEE Computer Architecture Letters, Springer Journal of Hardware and Systems Security