Yizhuo Tan

PhD Candidate in Computer Science, Yale University
New Haven, CT, USA • yizhuo.tan@yale.edu • +1 203 589 2969
yizhuotan.com • Google Scholar • GitHub

EDUCATION

Yale University, Connecticut, United States *09/2023 – Present*
Ph.D. in Computer Science *Expected graduation: 2028*
Advisors: Prof. Jakub Szefer (now at Northwestern University) and Prof. Yongshan Ding
Area: Quantum Computer Architecture, Quantum Computing Security

University of Science and Technology of China (USTC), Hefei, China *09/2019 – 07/2023*
Bachelor of Science in Physics
Major: Physics (Atomic and Molecular Physics track)
Minor: Computer Science and Technology

TECHNICAL SKILLS

Programming Languages	Python, C, C++, MATLAB, Verilog, LaTeX
Quantum Computing	Qiskit, pytket, Stim, Qiskit Metal, Amazon Braket SDK, COMSOL, Finite Element Analysis
Software & Tools	Mathematica, Blender, Adobe, ANSYS

RESEARCH EXPERIENCE

Doctoral Research / Research Assistant – Yale University *09/2023 – Present*
Advisors: Prof. Jakub Szefer and Prof. Yongshan Ding

Logical Operation Identification in qLDPC Codes

- Developed and implemented likelihood-based inference to identify logical operations from syndrome histories in qLDPC codes, using exact fault marginalization and scalable approximations that reduce computation and memory costs.
- Constructed joint likelihood models to identify individual logical instructions (code automorphisms, T-state injection, and logical Pauli measurements) and logical circuits built from these instructions. The models account for unknown faults, measurement randomness, and classical feedforward during circuit execution.
- Analyzed identification limits arising from insufficient or ambiguous syndrome information, fault timing, and inference approximations. Developed and evaluated refinements for cases with low identification accuracy.

Predictive Reliability Analysis of Superconducting Quantum Processors (EPAR)

- Co-developed EPAR, a framework that predicts layout-dependent robustness of superconducting processors by linking electromagnetic modeling, effective Hamiltonians, and control-pulse response.
- Constructed superconducting circuit models and chip layouts from target Hamiltonians and contributed to layout implementation in Qiskit Metal.
- The framework quantifies deviations between intended and effective qubit connectivity and characterizes the sensitivity of parasitic couplings to local parameter variations.

Private Delegated Quantum Queries (OQRAM)

- Co-designed oblivious QRAM protocols for clients with limited quantum resources, protecting delegated coherent queries through encrypted and shuffled database layouts and quantum-secure address masking.

– Co-developed security and resource analyses for quantum-secure pseudorandom-permutation and quantum one-time-pad variants. Established online quantum communication linear in the combined address and ciphertext register widths and quantified classical database refresh costs.

Pulse-Level Security of Superconducting Processors (QubitHammer)

– Designed and validated pulse-level attacks on IBM and Rigetti superconducting processors under a multi-tenant execution model. Demonstrated state changes across disjoint qubit allocations, including non-adjacent victim qubits, using public control interfaces without elevated privileges.
– Demonstrated that the attacks could bypass the evaluated dynamical-decoupling and active-padding configurations in hardware experiments.
– Implemented Rigetti experiment workflows in Python with Amazon Braket, covering calibration retrieval, hardware execution, and measurement analysis. Released a public demonstration notebook.

Readout Crosstalk in Cloud Quantum Computers

– Characterized correlations among qubit readout outcomes to quantify readout crosstalk and information leakage on superconducting quantum hardware.

Research Visit – Northwestern University *07/2026 – 09/2026*

Host: Prof. Jakub Szefer

– Research on logical-operation identification in qLDPC codes as part of doctoral research.

Undergraduate Research Assistant – USTC (Hefei, China) *09/2021 – 03/2022*

Microscale Nanoscience Laboratory

– Built and aligned optical paths and reflectors for Gaussian boson sampling experiments.
– Assisted in developing and arranging retarder-based optical measurements.

Undergraduate Experimental Project – USTC (Hefei, China) *09/2021 – 12/2021*

Awarded: First Prize, 17th Physical Innovation Research Experimental Paper Competition, USTC *2021*

– Designed ultrasonic phased-array hardware with independently controlled channel phase and drive amplitude for acoustic levitation.
– Modeled acoustic radiation potentials in MATLAB, evaluated fields and particle trajectories in COMSOL, and demonstrated stable levitation and controlled motion.

PUBLICATIONS & PREPRINTS

Peer-reviewed Publications

Navnil Choudhury, **Yizhuo Tan**, Jiaqi Yu, Jakub Szefer, Kanad Basu. “EPAR: Electromagnetic Pathways to Architectural Reliability in Quantum Processors” in Proceedings of the Chips to Systems Conference DAC, 2026. [DOI]

Yizhuo Tan, Navnil Choudhury, Kanad Basu, Jakub Szefer. “QubitHammer: Remotely Inducing Qubit State Change on Superconducting Quantum Computers” in Proceedings of the IEEE International Symposium on Hardware Oriented Security and Trust, HOST, 2026, pp. 151–161. [DOI]

Yizhuo Tan, Jakub Szefer. “I Know What You Are Reading: Evaluating Readout Crosstalk in Cloud-based Quantum Computers” in Proceedings of ACM QSec: Quantum Security and Privacy Workshop @ ACM Conference on Computer and Communications Security, QSec@CCS, 2025. [DOI]

Yizhuo Tan, Hrvoje Kukina, Jakub Szefer. “Securing HHL Quantum Algorithm against Quantum Computer Attacks” in Proceedings of Hardware and Architectural Support for Security and Privacy @ IEEE/ACM International Symposium on Microarchitecture, HASP@MICRO, 2025. [DOI]

Pranet Sharma, **Yizhuo Tan**, Konstantinos-Nikolaos Papadopoulos, Jakub Szefer. "Evaluation of Noise and Crosstalk in Neutral Atom Quantum Computers" in Proceedings of the Quantum-Classical Orchestration for Resilient Engineering Workshop (Q-CORE) at the IEEE International Conference on Quantum Computing and Engineering (QCE), 2025. [DOI]

Yizhuo Tan, Hrvoje Kukina, Jakub Szefer. "Study of Attacks on the HHL Quantum Algorithm" in Proceedings of IEEE Workshop on Quantum IntelLigence, Learning & Security@ IEEE International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications, QUILLS@TPS-ISA, 2024. [DOI]

Yizhuo Tan, Chuanqi Xu, Jakub Szefer. "Exploration of Timing and Higher-Energy Attacks on Quantum Random Access Memory" in Proceedings of the International Conference on Computer-Aided Design, ICCAD, 2024. [DOI]

Preprints & Manuscripts

Yizhuo Tan, Shifan Xu, Yongshan Ding, Jakub Szefer. "Identifying Logical Operations from Syndrome Histories for qLDPC Codes." Manuscript, 2026.

Shifan Xu*, **Yizhuo Tan***, Yongshan Ding, Jakub Szefer. "OQRAM: Oblivious Quantum Random Access Memory for Securing Delegated Quantum Queries." arXiv:2607.27171, 2026. (* Equal contribution.)

TEACHING EXPERIENCE

Teaching Assistant – Yale University

General Physics Laboratory	*Fall 2026*
Introduction to Computer Engineering	*Spring 2025*
Introduction to Electronics	*Fall 2024*

Undergraduate Teaching Assistant – USTC (Hefei, China)

Mechanics B	*Fall 2022*

HONORS & AWARDS

Best Paper, QSec@CCS	*2025*
Best Poster Award – 1st Place, New England Hardware Security Day	*2025*
Silver Award of Excellent Student Scholarship, USTC (Top 2%)	*2022, 2021*
First Prize in 17th Physical Innovation Research Experimental Paper Competition, USTC	*2021*
Scholarship of Yan Jici Talent Program in Physics, USTC (Top 10%)	*2021, 2020*
Second Prize in 6th China Undergraduate Physics Experiment Competition	*2020*
Chen Linyi Scholarship, USTC (Top 1%)	*2020*
Provincial First Prize in 35th Chinese Physics Olympiad	*2018*

SELECTED PRESENTATIONS

IEEE International Symposium on Hardware Oriented Security and Trust (HOST), McLean, VA	*2026*
HASP@58th IEEE/ACM International Symposium on Microarchitecture (MICRO), Seoul, Korea	*2025*
ACM QSec@ACM Conference on Computer and Communications Security (CCS), Taipei, Taiwan	*2025*
Joint March Meeting and April Meeting - Global Physics Summit, Anaheim, CA	*2025*
IEEE Workshop on Quantum IntelLigence, Learning & Security (QUILLS), Washington, DC	*2024*
ACM/IEEE International Conference on Computer-Aided Design (ICCAD), Newark, NJ	*2024*
2nd Quantum Computer Cybersecurity Symposium, New Haven, CT	*2024*