Grace Jia

grace.jia@yale.edu / gjia25.github.io

EDUCATION

Yale University, New Haven, CT. Aug 2022 – Present

Ph.D. in Computer Science.

Selected courses: Big Data Systems, Distributed Systems, Randomized Algorithms, Blockchain

Cornell University, Ithaca, NY. Aug 2018 – May 2022

B.A. in Computer Science, *magna cum laude.* GPA: 3.97/4.00

Selected courses: Cryptography, System Security, Computer Networking, Database Systems

PUBLICATIONS

Grace Jia, Alex Wong, Anurag Khandelwal. "Found in Translation: A Generative Language Modeling Approach to Memory Access Pattern Attacks." In *Proceedings of the 34th USENIX Conference on Security Symposium*, 2025.

Mahdi Soleimani, **Grace Jia,** In Gim, Seung-seob Lee, Anurag Khandelwal. "Wiretapping LLMs: Network Side-Channel Attacks on Public LLM Service," 2025. [In submission]

Mahdi Soleimani, **Grace Jia,** Anurag Khandelwal. "Weave: Efficient and Expressive Oblivious Analytics at Scale." In *Proceedings of the 19th USENIX Conference on Operating Systems Design and Implementation (OSDI), 2025.*

Grace Jia, Rachit Agarwal, Anurag Khandelwal. "Length Leakage in Oblivious Data Access Mechanisms." In *Proceedings of the 33rd USENIX Conference on Security Symposium,* 2024.

PROFESSIONAL EXPERIENCE

Yale Computer Science Department Aug 2022 – Present

Research Assistant *Advisor: Prof. Anurag Khandelwal*

- Implemented **correlated access pattern attack** on confidential computing environments, achieving 70–99% accuracy in predicting private data; now developing efficient mitigations
- Formulated **network side-channel attack on LLM services** with up to 92% accuracy
- Developed Weave system for **oblivious cloud analytics**, improving execution times by 4-10× over prior state-of-the-art

Cornell Computer Science Department Feb 2021 – May 2022

Research Assistant *Advisor: Prof. Rachit Agarwal*

- Designed **length-hiding oblivious access** mechanisms for various leakage scenarios and proved their performance lower bounds
- Developed new analytical framework for length leakage setting and security-performance tradeoff

Palo Alto Networks Summer 2021
Cloud Services Portal Engineer Intern *Santa Clara, CA*

- Deployed **single sign-on feature** using JSON Web Tokens to establish shared Identity and Access Management (IAM) system across all company microservices

Klaviyo Summer 2020
Software Engineer Intern *Boston, MA*

- Scaled up asynchronous task system for **profile CSV exports** using RabbitMQ and Celery, handling greater customer size and demand

Applied Science and Technology Research Institute Summer 2019
Summer Intern *Hong Kong*

- Evaluated statistical and deep learning methods for **fake news classification**

GRANTS & AWARDS

Yale Kwok Family Scholarship Fund	2024
Yale Student Fellowship	2022

TEACHING & SERVICE

Graduate Student Assembly, Yale University. 2025 – Present
Elected representative for Physical Sciences & Engineering Division, 14 departments

Deepfake, Deception, and Disinformation Security Workshop (3D-Sec). Aug 2025
Technical Program Committee Member

CPSC 422: Design & Implementation of Operating Systems, Yale University. 2024 – 2025

CS 2800: Discrete Structures, Cornell University. 2019 – 2020

SKILLS

Languages: Python, C, C++, Rust, OCaml, JavaScript, Java
Software & Development: Git, Linux, PyTorch, Hugging Face, React