Grace Jia

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

RESEARCH INTERESTS

Cloud security, confidential computing, and privacy-preserving AI; currently focused on information leakage from AI/ML services and cloud analytics.

EDUCATION

Ph.D. in Computer Science, Yale University, New Haven, CT. 2022–Present

B.A. in Computer Science, *magna cum laude*, Cornell University, Ithaca, NY. 2018–2022

PUBLICATIONS

Grace Jia, Alex Wong, Anurag Khandelwal. "Found in Translation: A Generative Language Modeling Approach to Memory Access Pattern Attacks." [In submission]

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

Mahdi Soleimani, **Grace Jia,** Anurag Khandelwal. "Weave: Efficient and Expressive Oblivious Analytics at Scale." [In submission]

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

TEACHING

CPSC 422: Design & Implementation of Operating Systems, Yale University. 2024–2025
CS 2800: Discrete Structures, Cornell University. 2019–2020

GRANTS & AWARDS

Yale Kwok Family Scholarship Fund 2024
Yale Student Fellowship 2022

INDUSTRY EXPERIENCE

Cloud Services Portal Engineer Intern @ Palo Alto Networks 2021
Deployed single sign-on feature for establishing shared Identity and Access Management (IAM) system across all company microservices.

Software Engineer Intern @ Klaviyo 2020
Expanded asynchronous task system for CSV exports to scale with customer size and demand.

Intern @ HK Applied Science and Technology Research Institute 2019
Adapted and evaluated deep learning methods for fake news detection.

TECHNICAL SKILLS

Languages & Tools: Python, C/C++, Rust, OCaml, Java; Git, Linux, PyTorch, Hugging Face