

Grace Jia

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

RESEARCH INTERESTS

Cloud security and confidential computing. My focus is currently on preserving data privacy in machine learning (ML) model serving and cloud analytics.

EDUCATION

- 2022 – Present **Ph.D. in Computer Science, Yale University, New Haven, CT.**
- 2018 – 2022 **B.A. in Computer Science, *magna cum laude*, Cornell University, Ithaca, NY.**

PUBLICATIONS

- 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.***
- 2024 **Grace Jia, Rachit Agarwal, Anurag Khandelwal. Length Leakage in Oblivious Data Access Mechanisms. In 33rd USENIX Security Symposium (USENIX Security 24).**

TEACHING

- Spring 2024 *Teaching Fellow for CPSC 422: Design & Implementation of Operating Systems*
- Fall 2019, 2020 *Teaching Assistant for CS 2800: Discrete Structures*

GRANTS & AWARDS

- 2024 *Yale Kwok Family Scholarship Fund*
- 2022 *Yale Student Fellowship*

INDUSTRY

- Summer 2021 *Cloud Services Portal Engineer Intern @ Palo Alto Networks*
Deployed single sign-on feature for team development portal, which laid groundwork for a unified Identity and Access Management (IAM) strategy across all microservices.
- Summer 2020 *Software Engineer Intern @ Klaviyo*
Restructured the asynchronous task system for exporting profile groups to CSVs to handle greater customer size and demand.
- Summer 2019 *Intern @ HK Applied Science and Technology Research Institute*
Evaluated deep learning methods and their effectiveness in fake news detection.

SKILLS

Languages & Software: Python, C, Rust, OCaml, Java; Git, Linux, PyTorch