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 encrypted storage, AI/ML services, and cloud analytics.

EDUCATION

Yale University, New Haven, CT. 2022–Present

Ph.D. in Computer Science.

Graduate courses: Big Data Systems, Distributed Systems, Machine Learning

Cornell University, Ithaca, NY. 2018–2022

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

Advanced 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 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.

PROFESSIONAL EXPERIENCE

Yale Computer Science Department 2022–Present

Research Assistant *Advisor: Prof. Anurag Khandelwal*

- Implemented **deep learning-based access pattern attack** against confidential computing environments, achieving up to 99.9% accuracy by leveraging knowledge of dependent accesses. Now designing unsupervised attack against encrypted search using variational autoencoders and generative adversarial networks.
- Investigated **network side channels of LLM serving systems** exposed by inference optimizations. Provided novel game-based definition to capture security against proposed attacks.
- Contributed to the development of Weave, an **oblivious cloud analytics** platform, proving its security against network and memory access pattern attacks.
  Weave has greater functionality and 4-10× improved execution times over prior state-of-the-art.

Cornell Computer Science Department 2021–2022
Undergraduate Research Assistant *Advisor: Prof. Rachit Agarwal*

- Designed **length-hiding oblivious access** mechanisms for various leakage scenarios and proved their performance lower bounds.
- Presented 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

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

PROJECTS

Offloaded Computer Vision Inference with Rust Kernel Modules 2022

- Prototyped Linux network and camera kernel modules in Rust for an application that sends webcam images to remote server for inference by a computer vision model.
- Eliminated overheads from memory-copy and kernel-user boundary crossing by having network module receive images directly from camera module.

Web App for Automatic Target Detection 2019–2022

- Led effort at CUAir (Cornell Unmanned Air Systems) to port application stack for custom aircraft's computer vision-based automatic target detection system to React and Flask.
- Integrated MySQL database to preserve target data in event of errors and crashes.

SKILLS

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