#### ROHIT NEMA · CURRICULUM VITAE

It Nema

Stanford, CA, USA

🕿 rohit@rohitnema.me | 🖀 rohitnema.me | 🖸 entrohpy | 🛅 rohit-nema | 🎓 Rohit Nema

## **Education**

### **Stanford University**

PhD in Computer Science

• 2nd Year PhD student in the Applied Cryptography Group - Advised by Dan Boneh

### UCLA (University of California, Los Angeles)

B.S. in Computer Science and Mathematics

- GPA: 4.0
- Frank Peters Scholarship Recipient, 2021-22
- Honor Societies: TBP (Tau Beta Pi), UPE (Upsilon Pi Epsilon)

# Publications

2023	Linear-time 2-party secure merge from additively homomorphic encryption, B. H. Falk, R. Nema, R.	
	Ostrovsky. Journal of Computer and System Sciences	JC33 2023
2022	A Linear-Time 2-Party Secure Merge Protocol, B. H. Falk, R. Nema, R. Ostrovsky	CSCML 2022

## Skills

DevOps	AWS, Azure, Docker, Git
Backend	Flask, Golang, REST API, SQL
Frontend	Node.js, Redux, React, HTML, SASS
Programming	Bash, C, C++, LaTeX, OCaml, Python

## Experience\_

### Sandia National Laboratories

R&D Intern

- Helped modernize a threat analytic and intrusion detection tool by supporting cloud computing traffic.
- Developed a smooth workflow between Cloud Service Providers to enable log aggregation and analysis.
- Rewrote dated frontend for a malware repository and multi-tool runner using React for better presentation and accessibility.
- · Participated in discussions on Adversarial Machine Learning and privacy-preserving methods such as Differential Privacy, Homomorphic Encryption, and Secure Multi-party Computation.

## Center for Information and Computation Security (CICS), UCLA

Undergraduate Researcher

- Implemented an efficient and secure method to perform k-means clustering with provable security.
  - Enables two parties to compute on their joint data while hiding their actual data from each other. - Will submit to IEEE S&P 2022.
- Develop a reputation system for peer-to-peer networks with an emphasis on Blockchain with robust fairness and security (against malicious users) guarantees.
  - Novel approach using Markov chains and Google's PageRank algorithm.

## Independent Research (Prof. Rafail Ostrovsky)

Researcher

- Developed and implemented a novel linear-time secure merge algorithm.
- Only requires black-box access to a Group Homomorphic Encryption scheme.
- Asymptotically optimal and beats existing secure-merge protocols in both time and space.
- Introduces clever shuffle algorithm to efficiently create a linked list to obliviously traverse permuted lists.
- · Introduces generalizable technique to convert ciphertexts into secret shares without computing an expensive decryption circuit jointly under MPC.
- To appear in CSCML 2022.

Los Angeles, CA

Livermore, CA

Jun. 2021 - Present

December 2020 - Present

Los Angeles, CA Sept. 2018 - Jun. 2022

Stanford CA

Los Angeles, CA

September 2020 - Present



Sept. 2022



## Stealth Software Technologies Inc.

#### Software Engineer

- Deployed multiple instances of an application on AWS instances with network configured using real-time constructed expander graph.
- Used RabbitMQ to efficiently send and queue messages between instances.
- Implemented a custom flooding algorithm to reduce redundancy in network traffic.

· Automated the entire task with robust error handling.

#### Stealth Software Technologies Inc.

Research Intern

- · Learned cryptography frameworks and languages.
- Analyzed and implemented algorithms for Secure Multi-party Computation for statistics such as Linear Regression and Crosstabs.
- Benchmarked existing secure frameworks to analyze factors such as communication cost and time taken.
- Surveyed existing literature on secure compaction and merge and compared actual running time.

# **Extracurricular Activities**

Stanioru	Dancesport —	Dattroom	Dancing	Club	
Officer					

• Compete in both NDCA and collegiate competitions in International Standard (WTFQV) and Latin (CRSJ)

### **Stanford Cycling Club**

Commodore of Coffee Ride, Team Room Manager

- Organize the weekly beginner-friendly social coffee (and pastries) ride.
- Maintain and manage the team room with various team bikes and tools.

## ACM ICPC at UCLA

Officer, Content Lead

- Create and teach workshops for Competitive Programming and Technical Interview preparation.
- Taught nearly 25-30 regular students Competitive Programming at a beginner-level weekly last Spring.
- Actively deliberate on how to make competitive programming more accessible to UCLA students. Introduce ideas to make content more approachable for students with no prior experience.
- Content Lead for Bruin Quest, a puzzle hunt and one of the biggest collaborations between three clubs under ACM.

#### LA Hacks

Co-Tech Director

- Led a small team in various collaborative projects including teaching the various tools and frameworks used.
- Followed professional coding practice and version control (Git) to manage codebase.
- Used React and SCSS to implement frontend. Developed backend in Go.
- Used industry tools like Docker to containerize micro- services.
- Managed and maintained frameworks used by more than 3000 people every year.

#### MentorSEAS

Mentor

- Mentored incoming freshmen and transfer students to familiarize them with the campus, UCLA Engineering and available resources.
- Organized events both virtually and in-person to foster a sense of community and friendship between students.

## **Projects**

#### **Discord Verification Bot**

Creator & Active Developer

- Built a robust Discord bot in less than 72 hours to verify members on ACM at UCLA's Official Discord server using Node.js, SQLite and Amazon SES for email.
- Verifies users using their UCLA email address and support various commands such as lookup for moderation purposes.
- It currently handles more than 2000 members and features automatic restarting on crash and automatic backups using system cron jobs.
- · Hosted on an AWS EC2 instance.

#### easyBay — ML-powered Advanced Image Search for eBay

#### Co-creator

- Built an iOS app using Google Cloud's Vision API and eBay's Finding and Browse APIs.
- · User could query products based on an image and certain filters.
- The image would be further processed by Google's Vision API to return cropped objects.
- Increased image searching power and accuracy manifold.
- Products were also filtered out based on suspicion analyzed by a trained ML model.

## Los Angeles, CA

Oct. 2018 - Apr. 2020

## Los Angeles, CA

Sept. 2020 - Present

## Hacktech 2019, Caltech

Mar. 2019

### Los Angeles, CA Sept. 2019 - Jun. 2020

## Los Angeles, CA

Jun. - Sept. 2019, Jun. - Aug. 2020

ACM at UCLA

Oct. 2020

Oct. 2019 - Present

Los Angeles, CA

Stanford, CA Dec. 2023 - Present

Stanford CA

June. 2023 - Present

## Listen — Salient Speech-to-text for Meetings and Lecture

- Co-creator
- Created a web app that implements the find functionality for audio files.
- Playback an audio file from any instance of a word you type.
- The app also summarizes the audio file by giving keywords (based on their importance to the context) that acted as an executive summary.
- Made using Jinja, Flask and Python with the Google Cloud Platform for speech-to-text, Natural Language Processing, and Cloud Storage.