Julia Len

jlen@csail.mit.edu • https://julialen.github.io/

Education

Ph.D. in Computer Science Aug 2024
Cornell University
Advisor: Thomas Ristenpart
Thesis: Designing secure-by-default cryptography for computer systems

B.S. in Computer Science Jun 2018
University of California San Diego

Work Experience

University of North Carolina at Chapel Hill, Chapel Hill, NC
- Assistant Professor, Department of Computer Science — Starting **Jul 2025**

MIT CSAIL, Cambridge, MA
- METEOR Postdoctoral Fellow (with Henry Corrigan-Gibbs) — **Sep 2024 – Jul 2025**

Cornell Tech, New York, NY
- Graduate Research Assistant — **Sep 2018 – Aug 2024**

Microsoft Research, Redmond, WA (remote)
- Intern with Cryptography and Privacy Group (with Esha Ghosh and Melissa Chase) — **Feb 2022 – Aug 2022**

Zoom Video Communications, New York, NY (remote)
- Cryptography Intern (with Antonio Marcedone) — **May 2020 – Aug 2020**

Google, Mountain View, CA
- Software Engineering Intern — **Jun 2017 – Sep 2017**
- Engineering Practicum Intern — **Jun 2016 – Sep 2016**

Center for Computational Biology and Bioinformatics, La Jolla, CA
- Data Science Intern — **Sep 2015 – Jun 2017**

Awards & Recognition

- EECS Rising Stars at Georgia Tech — **2023**
- NSF Graduate Research Fellowship — **2018 – 2023**
- Cornell University Graduate School Fellowship — **2018 – 2019**
- UCSD CSE Most Outstanding Undergraduate Researcher — **May 2018**
- Runner Up, Computing Research Association *Outstanding Undergraduate Researcher Award* — **2018**
  - Chosen as one of four runners up in this award that recognizes undergraduate students in North American universities who show outstanding computing research potential.
- Regents Scholarship, UC San Diego — **2013 –2017**
  - Based on academic excellence, it is the most prestigious scholarship awarded to UC undergraduate students.

Publications

1. **OPTIKS: An Optimized Key Transparency System**.
   Julia Len, Melissa Chase, Esha Ghosh, Kim Laine, Radames Cruz Moreno. USENIX Security 2024.
2. **ELEKTRA: Efficient Lightweight multi-dEvice Key TRAnsparency**.
   Julia Len, Melissa Chase, Esha Ghosh, Daniel Jost, Balachandar Kesavan, Antonio Marcedone. CCS 2023.
3. **Context Discovery and Commitment Attacks: How to Break CCM, EAX, SIV, and More**.
   Sanketh Menda, Julia Len, Paul Grubbs, Thomas Ristenpart. Eurocrypt 2023.
4. **Authenticated Encryption with Key Identification**.
   Julia Len, Paul Grubbs, Thomas Ristenpart. Asiacrypt 2022.
5. **Orca: Blocklisting in Sender-Anonymous Messaging**.
   Nirvan Tyagi, Julia Len, Ian Miers, Thomas Ristenpart. USENIX Security 2022.
6. **Partitioning Oracle Attacks**.
   Julia Len, Paul Grubbs, Thomas Ristenpart. USENIX Security 2021.
7. **Fuzzy Message Detection**.
   Gabrielle Beck, Julia Len, Ian Miers, Matthew Green. CCS 2021.
8. **Asymmetric Message Franking: Content Moderation for Metadata-Private End-to-End Encryption**.
   Nirvan Tyagi, Paul Grubbs, Julia Len, Ian Miers, Thomas Ristenpart. Crypto 2019.
9. **Better Than Advertised: Improved Collision-Resistance Guarantees for MD-Based Hash Functions**.
   Mihir Bellare, Joseph Jaeger, Julia Len. CCS 2017.
   (Author names in alphabetical order.)

Preprints

1. **Interoperability in End-to-End Encrypted Messaging**.
   Julia Len, Esha Ghosh, Paul Grubbs, Paul Rösler. *Cryptology ePrint Archive*.
   This paper presents the first investigation into how to design interoperable end-to-end encrypted messaging.

Talks

1. *The Next Generation of Authenticated Encryption*, Charles River Crypto Day, September 2024.
2. *ELEKTRA: Efficient Lightweight multi-dEvice Key TRAnsparency*, CCS 2023.
3. *Interoperability in End-to-End Encrypted Messaging*
   - New York Crypto Day, May 2023
   - University of Maryland Crypto reading group, May 2023
   - Real World Crypto, March 2023
   - SPRAI@UIUC, March 2023
4. *Context Discovery and Commitment Attacks: How to Break CCM, EAX, SIV, and More*, Eurocrypt 2023.
5. *Authenticated Encryption with Key Identification*, Asiacrypt 2022.
6. *Key-committing AEAD*, Crypto Forum Research Group at IETF 110, March 2021.
7. *Partitioning Oracle Attacks*
   - USENIX Security, August 2021
   - 4th Workshop on Attacks in Cryptography, August 2021

- MIT Security Seminar, March 2021
- Stanford Security Lunch, March 2021.
- Real World Crypto, January 2021

8. *Better Than Advertised: Improved Collision-Resistance Guarantees for MD-Based Hash Functions*, CCS 2017.

Service

Academic

- Program Committee: USENIX Security 2025, CATS 2023 (CCS workshop)
- External reviewer: CANS 2021, Crypto 2021, USENIX Security 2021, Crypto 2022, IEEE S&P (Oakland) 2022, Eurocrypt 2022, Asiacrypt 2023

Leadership & Mentorship

- PhD Students at Cornell Tech **Feb 2021 – Feb 2023**
  - Served as the Computer Science departmental representative and then the Co-Social Chair, where I organized weekly social hour gatherings for the Cornell Tech research community.
  - Created a survey to gather data on mental health needs of PhD students at Cornell Tech to present to the campus dean and other administrators, who used the survey results to create better mental health care support for students.
- Cornell High School Programming Contest Mentor **Feb 2021**
  - Volunteered as a mentor at a high school programming contest geared towards getting girls interested in computer science.
- Women PhD Lunch organizer **Nov 2019 – Mar 2020**
  - Single-handedly organized women PhD lunches at Cornell Tech to facilitate discussions on better gender diversity in computing research. This included working with administration to propose a budget and organizing meetings with guest speakers.
- Cornell Computer Science Graduate Organization **Sep 2019 – Jun 2019**
  - Served as the Graduate and Professional Student Assembly representative to keep the organization up-to-date on news and important action items of the broader Cornell Graduate School.
- Cornell Graduate and Professional Student Assembly **Sep 2018 – Jun 2019**
  - Served on the Graduate and Professional Student Assembly to represent the Cornell Computer Science department's interests to the Cornell Graduate School student body.

Teaching Experience

TA for Cornell CS 5830: Cryptography	Summer 2021
TA for Cornell CS 5436: Privacy in the Digital Age	Spring 2021
TA for Cornell CS 5433: Blockchains, Cryptocurrencies, and Smart Contracts	Spring 2020
Tutor for UCSD CSE 107: Introduction to Modern Cryptography	Fall 2017, Winter 2018
Tutor for UCSD CSE 105: Theory of Computability	Spring 2017
Tutor for UCSD CSE 20: Discrete Mathematics	Winter 2017
Head Tutor for UCSD CSE 11: Intro to Object-Oriented Programming in Java	Fall 2016
Tutor for UCSD CSE 30: Computer Organization and Systems Programming	Spring 2016