NOEMI GLAESER

nglaeser@disroot.org
nglaeser.github.io
nglaeser
cryptonoemi
[@ioc.exchange]

EDUCATION

2024

PhD, Computer Science
University of Maryland &
Max Planck Institute for
Security and Privacy (MPI-SP)

2021

MS, Computer Science
University of Maryland

2019

BS, Mathematics
BSCS, Computer Science
University of South Carolina
Honors College
summa cum laude

LANGUAGES

Native (C2)

English, German, Italian

Conversational (A2-B1)

French, Spanish

SUMMARY

I am an applied cryptographer working on the design and analysis of cryptographic protocols. I am looking to span research and practice and work in a collaborative setting. I have extensive experience creating, analyzing, and implementing (in Rust and Python) novel cryptographic protocols and communicating my ideas to various audiences. Besides blockchain applications and discrete-logarithm and elliptic curve cryptography, I have experience with multi-party computation, zero-knowledge proofs, and lattice-based cryptography.

EXPERIENCE

PhD Student, University of Maryland (UMD) & MPI-SP - *2019-2024*

- Published in top-tier security, privacy, and blockchain conferences such as Financial Crypto, ACM CCS, and USENIX Security (see website for full list)
- Developed novel cryptographic protocol for private and secure analytics tailored to epidemiologists' and systems researchers' needs [paper]
- Analyzed and adjusted security of a coin mixing protocol intended for industry deployment [paper]
- Described, implemented, and benchmarked novel protocol for "registration-based" encryption in Python [paper] [code]
- Developed proof-of-concept Rust implementation of novel zero-knowledge proof system [paper] [code]
- Researched, presented, and defended dissertation entitled "Practical Cryptography for Blockchains: Secure Protocols with Minimal Trust"

Research Intern, a16z crypto - *summer 2023*

- Advised portfolio companies on design of cryptographic protocols tailored to their blockchain use cases
- Adapted existing cryptographic primitives to create first non-interactive & private on-chain voting and auction protocol [paper]
- Introduced new zero-knowledge proof/rollup paradigm called "naysayer proofs" which inspired a pitch at the a16z Crypto Startup Accelerator (CSX) and a separate whitepaper [our paper] [blog post]
- Described & evaluated cryptographic approaches to key management on blockchains in an a16z crypto blog post for general audience [X post]

Research Intern, NTT Research, Inc. - *summer 2022*

- Developed & analyzed Throback, a custom threshold signature scheme for Lit Protocol, a decentralized key management network
- Contributor & co-maintainer of open-source Rust implementation of Throback in Hyperledger Labs [code]

Founder & Organizer, UMD CS Graduate Peer Mentoring - *2021-2024*

- Created & coordinated new peer mentoring initiative for CS grad students to support incoming students in grad school transition, develop PhD soft skills, and provide resources & advice. Program became a key piece of student life and department advisory council, serving 88 students this year.

Packet Writer, UMD Girls Talk Math - *2022*

- Communicated complex cryptography concepts (secret sharing, provable security) to high school students [packet]

OTHER PROJECTS

Crypto glossary

- Explaining technical cryptography terms in an accessible way in a publicly-available glossary (https://nglaeser.github.io/crypto-glossary/)

SKILLS

- Deep knowledge of elliptic curve cryptography, discrete-logarithm–based cryptography, blockchain technology
- Experience in multi-party computation, zero-knowledge proofs, lattice-based cryptography, symmetric cryptography
- Experience with Git, Python, Rust, LaTeX, HTML/CSS/JavaScript, Bash, C++
- Excellent written & oral communication, very detail-oriented

SERVICE

Mentor

UMD CS Graduate Peer Mentoring (2021-2024), UMD Iribe Initiative for Inclusion & Diversity in Computing (2020), UofSC McNair Scholar Buddy (2016-2019)

Program Committee

Financial Crypto (2026, 2025, 2024), Information Security Conference (2024), IEEE Security & Privacy - Posters (2023), Network & Distributed Systems Security - Student Support (2023)

External Reviewer

Cryptology and Network Security (2024), Australasian Conference on Information Security & Privacy (2024), IEEE Security & Privacy (2024), IACR Crypto (2023), ACM Computer & Communications Security (2023, 2020), Privacy Enhancing Technologies Symposium (2023.3, 2022.4, 2022.1), IACR Public Key Cryptography (2022)

AWARDS

- NSF Graduate Research Fellowship (2019)
- Phi Beta Kappa Honor Society (2019) - *oldest and most prestigious academic honor society in the US*
- Computational Science Fellowship - Math & Computing, US DOE (2019)