Noemi Glaeser

nglaeser@umd.edu
nglaeser.github.io
nglaeser
cryptonoemi [@ioc.exchange]
0000-0002-6464-2534

Education

Ph.D., Computer Science *expected December 2024*
University of Maryland (UMD), *College Park, MD, USA*
& Max Planck Institute for Security and Privacy (MPI-SP), *Bochum, Germany*
Dissertation: "Practical Cryptography for Blockchains: Secure Cryptographic Protocols with Minimal Trust"
Advisors: Jonathan Katz (UMD) and Giulio Malavolta (MPI-SP)

M.S., Computer Science *May 2021*
University of Maryland, *College Park, MD, USA*
GPA: 3.9/4.0

B.S., Mathematics & B.S.C.S., Computer Science • *summa cum laude* *May 2019*
Minor, Music & Flute performance certificate
University of South Carolina Honors College, *Columbia, SC, USA*
GPA: 4.0/4.0

Advanced Studies High School Diploma *Jun 2015*
Thomas Jefferson High School for Science & Technology, *Alexandria, VA, USA*
#1 public U.S. high school according to Newsweek (2014-2016)
GPA: 4.46/4.0

Publications

* = authors listed in alphabetical order

In submission

[-] **Hot-Cold Threshold Wallet Backups with Proofs of Remembrance**
*S Garg, N Glaeser, A Jain, M Lodder, H Montgomery

[-] **CoVault: Secure, Scalable Analytics of Personal Data**
R De Viti, I Scheff, N Glaeser, B Dinis, R Rodrigues, B Bhattacharjee, A Hithnawi, D Garg, P Druschel

Workshop Papers

[9] **Cicada: A framework for private, non-interactive on-chain auctions and voting**
N Glaeser, I Seres, M Zhu, J Bonneau
Workshop on Cryptographic Tools for Blockchains (CTB 2024) at Eurocrypt 2024

Conference Papers

[8] **Short Paper: Naysayer Proofs**
I Seres, N Glaeser, J Bonneau
FC 2024; also appeared at CTB Workshop 2024

[7] **Universally Composable NIZKs: Circuit-Succinct, Non-Malleable and CRS-Updatable**
*B Abdolmaleki, N Glaeser, S Ramacher, D Slamanig
IEEE CSF 2024

[6] **Efficient Registration-Based Encryption**
*N Glaeser, D Kolonelos, G Malavolta, A Rahimi
ACM CCS 2023

[5] **Foundations of Coin Mixing Services**
*N Glaeser, M Maffei, G Malavolta, P Moreno-Sanchez, E Tairi, SAK Thyagarajan
ACM CCS 2022

[4] **The updated DESGW processing pipeline for the third LIGO/VIRGO observing run**
K Herner, J Annis, A Garcia, M Soares-Santos, D Brout, N Glaeser, N Sherman, R Kessler, R Morgan, A Palmese, F Paz-Chinchon, A Lenon, T Bachmann
Computing in High Energy & Nuclear Physics (CHEP) 2019

[3] **Access control for a database-defined network**
N Glaeser, A Wang
IEEE Sarnoff Symposium 2016

Journal Papers……

[2] **Optical follow-up of gravitational wave triggers with DECam during the first two LIGO/VIRGO observing runs**
K Herner et al.
Astronomy & Computing, Vol 33 (October 2020)

[1] **Prediction and Measurement Update of Fungal Toxin Geospatial Uncertainty using a Stacked Gaussian Process**
K Abdelfatah, J Senn, N Glaeser, G Terejanu
Agricultural Systems, Vol 176 (November 2019)

Other……

[B] **Key distribution on blockchains: the case for registration-based encryption**
N Glaeser
a16zcrypto blog post

[A] **Packet: Cryptographic secret sharing**
N Glaeser
UMD Girls Talk Math summer camp

Talks & Posters

T6. **Invited talk: Mathematically Sharing Secrets**
UMD Girls Talk Math 2021 Spring Event, Virtual

T5. **Poster: Improving bounds on entropy of odd cycle graphs**
UofSC Discovery Day 2019, Columbia, SC, USA

T4. **Talk: Improvements to image processing in the DES-GW pipeline**
2018 Summer Internship in Science & Tech (SIST) Presentation Day, Fermi National Accelerator Laboratory, Batavia, IL, USA

T3. **Talk: Access control for a database-defined network**
Temple University REU Presentations 2016, Philadelphia, PA, USA

T2. **Poster: Access control for a database-defined network**
IEEE Sarnoff Symposium 2016, Newark, NJ, USA
*3rd place Poster Award

T1. **Poster: Generating geographic and temporal heat maps of aflatoxin incidence using regularized linear models**
UofSC Discovery Day 2017, Columbia, SC, USA

Service

Program Committee
FC (2025, 2024), ISC (2024), IEEE S&P Poster PC (2023), NDSS Student Support Committee (2023)

External Reviewer
CANS (2024), ACISP (2024), IEEE S&P (2024), IACR Crypto (2023), ACM CCS (2023, 2020), PETS (2023.3, 2022.4, 2022.1), PKC (2022)

Organizer
UMD CS Graduate Peer Mentoring Program (founder) *fall 2021-present*
UMD Cryptography Reading Group *fall 2020-spring 2021*

Mentor
UMD CS Graduate Peer Mentoring Program *fall 2021-spring 2024*
UMD Iribe Initiative for Inclusion & Diversity in Computing (I4C) *fall 2020*
UofSC McNair Scholar Buddy *fall 2016-spring 2019*

Leadership
UofSC Cybersecurity Club (webmaster) *spring 2018-spring 2019*
Gamecock Math Club/Pi Mu Epsilon Math Honor Society (treasurer) *fall 2017-spring 2019*
UofSC Assoc for Women in Math (co-founder, treasurer, secretary) *spring 2017-spring 2018*

Research Positions

a16z crypto *summer 2023*

Research Intern, supervised by Joseph Bonneau

Conducted fundamental research in cryptographic protocols for blockchains [8,9] and helped portfolio companies with technical research problems. Also wrote an informational post [B] for the company's blog.

NTT Research, Inc. *summer 2022*

Research Intern, supervised by Sanjam Garg

Working on a scheme and formal framework for threshold cryptocurrency wallets in the hot-cold paradigm with strong trust and recovery guarantees (with Linux Foundation & LIT Protocol).

University of Maryland *2019-2020*

Research Assistant

Developing secure multiparty computation (MPC) protocols in novel threat models & deployment environments; studied bounds on query-pattern leakage attacks on encrypted databases.

Inria Sophia Antipolis *summer 2019*

Research Intern

University of South Carolina Mathematics Department *2018-2019*

Science Undergraduate Research Fellowship (SURF)

Investigated tightness of stochastic bounds on cycle graph entropy (poster T5); released an open-source package with cycle graph utilities.

GitHub: nglaeser/graph_cyclone *(Python)* • PyPI: graph-cyclone

University of South Carolina Computer Science Department *2018-2019*

Capstone Computing Project • GitHub

Developed "Open vLab", an educational network virtualization framework for hands-on computing education using Django, OpenFlow, and Javascript.

Fermi National Accelerator Laboratory, Particle Astrophysics *summer 2018*

Grace Hopper Computing Intern • GitHub

Improved efficiency of the Dark Energy Survey's image processing pipeline (Python and Bash) for optical counterparts of gravitational wave events from average 5-8 hrs to 30 min (10-16x speedup). Published in [2,4] and talk T4.

Temple University Computer Science Department *summer 2016*

NSF Research Experience for Undergraduates (REU) • GitHub, website

Implemented an access-control security application in Python and PostgreSQL for the database-defined software-defined network (SDN) controller Ravel. Work presented in [3], T2, & T3.

University of South Carolina Computer Science Department *2016-2018*

Research Assistant / Magellan Scholar

Published in [1] and presented in poster T1.

Awards & Honors

GREPSEC Workshop Grant *2021*

Graduate Research Fellowship, *US National Science Foundation (NSF)* *2019 – 2024*

Phi Beta Kappa Honor Society *2019*

Oldest and most prestigious academic honor society in the US

Computational Science Fellowship (Math & Computing), *US Dept of Energy* *2019, declined*

Outstanding Senior in Mathematics, *UofSC Math Dept* *Spring 2019*

Goldwater Scholarship (Honorable Mention) *2018*

Science Undergraduate Research Fellowship (SURF), *UofSC Honors College* *Fall 2018*

Investigated tightness of stochastic bounds on cycle graph entropy (poster T2); released an open-source package (graph-cyclone) with cycle graph utilities.

Grace Hopper Scholar, *Anita Borg Institute* *2017*

Funding to attend the 2017 Grace Hopper Celebration of Women in Computing

Magellan Scholar Award, *UofSC* *2016*

$2,500 for Computer Science department research

McNair Scholar, *UofSC* *2015-19*

Highest out-of-state merit-based scholarship

Other Achievements

BSides Charleston Capture the Flag (cybersecurity competition), *2nd place* *2018*

BSides Charleston Cryptography Challenge, *1st place* *2017*

MAA Southeastern Math Jeopardy, *3rd place* *2016*

Technical Skills

Strong: *Python* • *LaTeX* • *HTML/CSS/Javascript*
Proficient: *Bash* • *C++* • *Rust*

Languages

Native (C2): English, German, Italian

Conversational proficiency (A2-B1): French, Spanish

Beginner (A1): American Sign Language (ASL)

Selected Coursework

(* denotes honors course; † denotes graduate course.)

Mathematics

Computational Number Theory†

Analysis I* & II*

Algebraic Structures I & II*

Linear Algebra

Ordinary Differential Equations

Discrete Mathematics I

Computer Science

Applied Mechanism Design for Social Good†
Intro to Secure Distributed Computation†
Intro to Quantum Information Processing†
Algos in ML: Guarantees & Analyses†
Applied Crypto & Hostile Govmts (audit)†
Interactive Technologies†
Human Factors in Security & Privacy†
How to Conduct Great Research (seminar)†
Computer & Network security†
Program Analysis & Understanding†
Introduction to Cryptography*
Computer Architecture*
Theory of Computation
Ethical Hacking
Information Security Principles