Noemi Glaeser

nglaeser@umd.edu • nglaeser.github.io
LinkedIn,GitHub: @nglaeser
ORCID: 0000-0002-6464-2534

Education

University of Maryland (UMD), *College Park, MD*   *estimated May 2024*
Max Planck Institute for Security and Privacy (MPI-SP), *Bochum, Germany*
  Ph.D., Computer Science • *Maryland-Max Planck joint program*
  Advisors: Jonathan Katz (UMD) and Giulio Malavolta (MPI-SP)

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

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

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

Current Projects

Key Share Proofs. Threshold signatures optimized to the network architecture used by cryptocurrency exchanges, with efficient proofs of storage of cryptographic keys.

Analysis of Bolt. Formal security analysis of the Bolt [CCS'17] third-party payment protocol.

Publications   * = authors listed in alphabetical order

Preprints

[9].* B. Abdolmaleki, <u>N. Glaeser</u>, S. Ramacher, D. Slamanig. (2022). Universally Composable NIZKs: Circuit-Succinct, Non-Malleable and CRS-Updatable. https://eprint.iacr.org/2023/097.

[8]. R. De Viti, I. Scheff, <u>N. Glaeser</u>, B. Dinis, R. Rodrigues, J. Katz, B. Bhattacharjee, A. Hithnawi, D. Garg, P. Druschel. (2022). CoVault: Secure High-Stakes Analytics. https://arxiv.org/abs/2208.03784.

Conference Papers

[7].* <u>N. Glaeser</u>, D. Kolonelos, G. Malavolta, A. Rahimi. Efficient Registration-Based Encryption.

[6].* <u>N. Glaeser</u>, M. Maffei, G. Malavolta, P. Moreno-Sanchez, E. Tairi, S.A.K. Thyagarajan. Foundations of Coin Mixing Services. ***ACM CCS 2022***. https://eprint.iacr.org/2022/942.

[5]. K. Herner <u>et al.</u> The updated DESGW processing pipeline for the third LIGO/VIRGO observing run. ***Conf. on Computing in High Energy & Nuclear Physics (CHEP)***, 245, 01008. https://doi.org/10.1051/epjconf/202024501008.

[4]. <u>N. Glaeser</u> and A. Wang. Access control for a database-defined network, ***IEEE Sarnoff Symposium 2016***. http://dx.doi.org/10.1109/SARNOF.2016.7846728.

Journal Papers

[3]. K. Herner <u>et al.</u> Optical follow-up of gravitational wave triggers with DECam during the first two LIGO/VIRGO observing runs. ***Astronomy & Computing***, 33, 100425. https://doi.org/10.1016/j.ascom.2020.100425.

[2]. K. Abdelfatah, J. Senn, <u>N. Glaeser</u>, and G. Terejanu. Prediction and Measurement Update of Fungal Toxin Geospatial Uncertainty using a Stacked Gaussian Process. ***Agricultural Systems***, *176*, 102669. https://doi.org/10.1016/j.agsy.2019.102662.

Other

[1]. <u>N. Glaeser</u>. (2021). Cryptographic secret sharing packet, *UMD Girls Talk Math summer camp*. https://github.com/nglaeser/gtm2021/tree/main/packet.

Talks & Posters

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

T5. Improving bounds on entropy of odd cycle graphs (joint work with Joshua Cooper.) Poster, *UofSC Discovery Day 2019*, Columbia, SC.

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

T3. Access control for a database-defined network (joint work with Anduo Wang.) Talk, *Temple University REU Presentations 2016*, Philadelphia, PA.

T2. Access control for a database-defined network (joint work with Anduo Wang.) Poster, *IEEE Sarnoff Symposium 2016*, Newark, NJ.
   *3rd place Poster Award

T1. Generating geographic and temporal heat maps of aflatoxin incidence using regularized linear models (joint work with Gabriel Terejanu.) Poster, *UofSC Discovery Day 2017*, Columbia, SC.

Awards & Honors

GREPSEC Workshop Grant *2021*

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

Phi Beta Kappa Honor Society *2019*

   Oldest and most prestigious academic honor society in the U.S.

Computational Science Fellowship (Math & Computing track), *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 (<u>graph-cyclone</u>) 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

Service

External Reviewer

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*

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*

Mentor

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

Other

Packet Writer, UMD Girls Talk Math	*summer 2021, summer 2022*

Research Experience

a16z crypto   *summer 2023*

Research Intern

Conducting fundamental research in cryptographic protocols for blockchains, helping portfolio companies with technical research problems, writing informational materials for public.

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 (collaboration with the Linux Foundation).

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

Developed "Open vLab", an educational network virtualization framework for hands-on computing education.

> GitHub: SCCapstone/OpenVLab *(Django, OpenFlow, Javascript)*

Fermi National Accelerator Laboratory, Particle Astrophysics *summer 2018*

Grace Hopper Computing Intern

Improved efficiency of the Dark Energy Survey's image processing pipeline for optical counterparts of gravitational wave events from average 5-8 hrs to 30 min (10-16x speedup). Published in [3,5] and talk T4.

> GitHub: SSantosLab/gw_workflow *(Python, Bash)*

Temple University Computer Science Department *summer 2016*

NSF Research Experience for Undergraduates (REU)

Implemented an access-control security application for the database-defined software-defined network (SDN) controller Ravel. Work presented in [4], T2, & T3.

> GitHub: ravel-net/REU-access-control *(Python, PostgreSQL)* • Web: ravel-net.org/

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

Research Assistant / Magellan Scholar

Published in [2] and presented in poster T1.

Memberships

Association for Computing Machinery (ACM)	*2018-*
International Association for Cryptology Research (IACR)	*2019-*

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*
Average: *Bash • C++ • Rust*

Languages

Native proficiency: English, German, Italian

Conversational proficiency: French, 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 Gov'ts (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