Erica Blum | Curriculum Vitae

🌐 cs.umd.edu/~erblum/ ✉ erblum@umd.edu 🎓 scholar.google.com

EDUCATION

University of Maryland College Park — **College Park, MD**
PhD Candidate, Computer Science — *2018 – 2023 (expected)*
Advisor: Jonathan Katz

University of Maryland College Park — **College Park, MD**
MS, Computer Science — *2018 – 2020*

Haverford College — **Haverford, PA**
BS (cum laude), Major: Mathematics, Minor: Computer Science — *2014 – 2018*

PROFESSIONAL EXPERIENCE

Research Intern — **May 2022 – Aug 2022**
NTT Research, Sunnyvale, CA
Began ongoing collaboration on techniques and lower bounds for distributed protocols with balanced communication and optimal communication complexity.

Research Intern — **May 2021 – Aug 2021**
NTT Research, virtual
Developed new tools for constructing monotone boolean circuits for weighted threshold functions, with applications to weighted threshold secret sharing.

Research Intern — **May 2020 – Aug 2020**
Novi (Facebook), virtual
Collaborated with the Libra blockchain research group on new directions in directed acyclic graph (DAG)-based consensus algorithms.

Research Intern — **May 2019 – May 2020**
SRI International, Palo Alto, CA
Conducted research on general adversary cryptographic primitives and applications to federated blockchains.

NSF REU Student — **Summer 2016 & 2017**
University of Connecticut, Storrs, CT
Conducted research on tamper-resistant file storage (Summer 2016) and provable security of blockchain protocols (Summer 2017), leading to a significantly tighter security analysis for a family of proof-of-stake blockchain protocols (including Ouroboros, the protocol used by the Cardano cryptocurrency platform).

CONFERENCE PAPERS

[Asiacrypt'22] Andreea B. Alexandru, Erica Blum, Jonathan Katz, and Julian Loss. "State Machine Replication under Changing Network Conditions". *Advances in Cryptology—**Asiacrypt 2022***. URL: https://eprint.iacr.org/2022/698.

[Asiacrypt'21] Erica Blum, Jonathan Katz, and Julian Loss. "Tardigrade: An Atomic Broadcast Protocol for Arbitrary Network Conditions". *Advances in Cryptology—**Asiacrypt 2021***. URL: https://eprint.iacr.org/2020/142.

[TCC'20] Erica Blum, Jonathan Katz, Chen-Da Liu Zhang, and Julian Loss. "Asynchronous Byzantine Agreement with Subquadratic Communication". *Theory of Cryptography* (***TCC 2020***). URL: https://eprint.iacr.org/2020/851.pdf.

[CRYPTO'20] Erica Blum, Chen-Da Liu Zhang, and Julian Loss. "Always Have a Backup Plan: Fully Secure Synchronous MPC with Asynchronous Fallback". *Advances in Cryptology—**CRYPTO 2020***. URL: https://eprint.iacr.org/2020/740.

[SODA'20] Erica Blum, Aggelos Kiayias, Cristopher Moore, Saad Quader, and Alexander Russell. "The Combinatorics of the Longest-Chain Rule: Linear Consistency for Proof-of-Stake Blockchains". *Proceedings of the Thirty-First Annual ACM-SIAM Symposium on Discrete Algorithms* (***SODA 2020***). URL: https://eprint.iacr.org/2017/241.

[TCC'19] Erica Blum, Jonathan Katz, and Julian Loss. "Synchronous Consensus with Optimal Asynchronous Fallback Guarantees". *Theory of Cryptography* (***TCC 2019***). URL: https://eprint.iacr.org/2019/692.

EPRINTS AND MANUSCRIPTS

[In Submission '22] Erica Blum, Jonathan Katz, Julian Loss, Kartik Nayak, and Simon Ochsenreither. *Abraxas: Throughput-Efficient Hybrid Asynchronous Consensus*. In submission. 2022.

[In Progress '22] Erica Blum, Chen-Da Liu Zhang, Shin'ichiro Matsuo, Elaine Shi, and Yu Xia. *Towards Practical Secret Sharing for Weighted Access Structures*. Unpublished manuscript. 2022.

AWARDS AND HONORS

- 2022 Chainlink Labs PhD Fellowship Honorable Mention
- 2020 NSF GRFP Honorable Mention
- 2020 Facebook PhD Fellowship Finalist
- 2019 DFINITY Scholarship Winner

TEACHING AND ADVISING EXPERIENCE

University of Maryland College Park

- *Research Mentor, Undergraduate Research* — *Fall 2021 – Present*
- *Research Mentor, CMSC 499A (Undergraduate Independent Research)* — *Spring 2021*
- *Teaching Assistant, CMSC 414 (Computer and Network Security)* — *Fall 2020*
- *Teaching Assistant, CMSC 456 (Cryptology)* — *Spring 2019*

Haverford College

- *Teaching Assistant, ASTR 104 (Topics in Intro Programming: Physics and Astronomy)* — *Spring 2018*

ACADEMIC SERVICE AND OUTREACH

External Reviewer (selected conferences)

- 2022: CCS, Eurocrypt, PODC
- 2021: CCS, Eurocrypt, ICDCS, PODC
- 2020: CCS, CRYPTO

Graduate Student Elected Representative, CS Dept. Education Committee **2020 – 2021**
University of Maryland College Park

Peer Mentor, Iribe Initiative for Inclusion and Diversity in Computing **2018**
University of Maryland College Park

Student Leadership Committee Member, Astronomy Public Observing **2015 – 2018**

Haverford College

SELECTED PRESENTATIONS

- Asiacrypt 2021 (virtual): “Tardigrade: An Atomic Broadcast Protocol for Arbitrary Network Conditions,” Dec. 2021.
- TCC 2019 (Nuremberg, Germany): “Synchronous Consensus with Optimal Asynchronous Fallback Guarantees,” Dec. 2019.
- NY CryptoDay (New York, NY): “Synchronous Consensus with Optimal Asynchronous Fallback Guarantees,” Oct. 2019.
- D.C. Area CryptoDay (College Park, MD): “Provable Consistency Guarantees in Proof-of-Stake Blockchains,” Dec. 2018.
- National Council for Undergraduate Research REU Symposium (Arlington, VA): poster, “Disruptive Adversaries in Blockchain Protocols," Oct. 2017.