Elizabeth (Eli) Margolin

ecmargo@seas.upenn.edu · ecmargo.github.io · github.com/ecmargo

SUMMARY

PhD candidate in Computer and Information Science at the University of Pennsylvania working at the intersection of applied cryptography, zero-knowledge proofs, and formal methods. Builds and performance-optimizes fast, succinct non-interactive proof systems for formal languages, implemented in Rust and released open-source, with publications at IEEE S&P, USENIX Security, and SOSP. Pairs deep cryptography with three years of security engineering at Meta and a rigorous eye for soundness and correctness. Current focus: using cryptographic tools, including zero-knowledge proofs, to make AI systems auditable and accountable.

TECHNICAL SKILLS

Cryptography: zero-knowledge proofs / SNARKs; verifiable computation; ZK circuit design & prover performance optimization; protocol design & implementation; MPC, threshold signatures, distributed key generation, secret sharing (protocol-level); signature schemes (Schnorr, EdDSA, ECDSA, BIP-340)

Formal Methods: interactive theorem proving (Coq); SMT solvers; program analysis; circuit/constraint compilation (CirC); reasoning about soundness & correctness

Privacy & Security: differential privacy; federated / private analytics; threat modeling, threat & abuse detection, security-sensitive code & design review

Languages & Tools: Rust, C++, Python; Coq; LLVM / MLIR; distributed & privacy-preserving systems

EXPERIENCE

University of Pennsylvania — PhD Researcher (Applied Cryptography & Formal Methods) *2021–present*

- Build and performance-optimize fast, succinct non-interactive ZK proof systems for formal languages — regular expressions (Reef) and context-free grammars (Coral) — designing ZK circuits and constraint systems and tuning prover runtime and proof size; implemented in Rust and open-sourced
- Reason rigorously about the soundness, correctness, and security assumptions of cryptographic proof systems using SMT solvers and interactive theorem proving (Coq)
- Apply cryptographic tools, including zero-knowledge proofs, to bring auditability and accountability to AI systems; advised by Sebastian Angel (dissertation: Zero Knowledge Proofs of Formal Languages)

Brave Software — Research Intern *Summer 2024*

- Designed and implemented zero-knowledge protocols for privacy-preserving fraud detection, taking research designs through to deployable implementations
- Reviewed and hardened cryptographic tooling to interoperate with modern TLS stacks, bridging research prototypes and production

Meta Platforms — Security Engineer *2019–2021 (Contingent Worker, 2022)*

- Performed threat modeling and security analysis to design and own company-wide insider-threat and abuse-detection tooling for security and legal investigations teams
- Scaled alert-processing pipelines through automation, increasing throughput while driving down false-positive rates
- Led cross-functional security and privacy reviews with Legal and Policy to reduce the data footprint of detection systems without sacrificing efficacy

Duke University — Research Assistant (Differential Privacy) *2019*

- Quantified tradeoffs between differential-privacy guarantees and Voting Rights Act compliance for the 2020 U.S. Census, in collaboration with the U.S. Census Bureau

SELECTED PUBLICATIONS

Coral: Fast Succinct Non-Interactive Zero-Knowledge CFG Proofs
S. Angel, S. Celi, E. Margolin, P. Mishra, M. Sander, J. Woods · IEEE S&P 2026 · github.com/eniac/coral*

Reef: Fast Succinct Non-Interactive Zero-Knowledge Regex Proofs
S. Angel, E. Ioannidis, E. Margolin, S. Setty, J. Woods · USENIX Security 2024 · github.com/eniac/Reef*

Arboretum: A Planner for Large-Scale Federated Analytics with Differential Privacy
E. Margolin, K. Newatia, E. Roth, T. Luo, A. Haeberlen · SOSP 2023

** Authors listed in alphabetical order*

EDUCATION

University of Pennsylvania — PhD, Computer and Information Science *In progress*

Duke University — MS, Economics and Computation

Stanford University — BA, Political Science, with Honors in International Security

SELECTED ACTIVITIES

Team USA — National Team Athlete (Rowing); USRowing Athlete Council *2025–present*

- Competed at the 2025 World Rowing Championships, Shanghai