

# Joshua Gancher

gancher.dev | jgancher@andrew.cmu.edu

## Research Interests

---

I apply tools from Formal Methods and Programming Languages to construct, certify, and give formal semantics to secure systems. I am particularly interested in reasoning about security for cryptographic mechanisms used in practice. Broadly, I am interested in applied cryptography, distributed systems, type systems, compiler correctness, proof assistants, and formal methods. My work appears at **IEEE S&P**, **POPL**, **CCS**, **CSF**, **PLDI**, and **PETS**.

## Education

---

- **Ph.D. in Computer Science.** Cornell University. December 2021.
  - Co-advised by Elaine Shi and Greg Morrisett. Thesis: Equational Reasoning for Verified Cryptographic Security.
- **B.A. in Mathematics.** Reed College. May 2016.
  - Thesis: Fully Homomorphic Encryption.

## Experience and Appointments

---

- **Assistant Professor.** Northeastern University. Fall 2024.
- **Postdoctoral Fellow.** Carnegie Mellon University. 2021 - Present.
  - Advised by Bryan Parno. Research Focus: Type systems for secure cryptographic protocols.
- **Amazon Automated Reasoning Group.** Software Engineering Intern. Summer 2019.
  - Delivered formal proofs and specifications for Amazon Encryption SDK
  - Created a compiler from internal protocol description language to Dafny
- **Galois, Inc.** Software Engineering/Research Intern. Summer 2017.
  - Worked with Air Force Research Lab to migrate codebase to Rust
  - Extended Crucible symbolic execution engine to handle Rust

**Professional Activities:** Program Committees: FCS 2020, FC 2023, SPLASH SRC 2023; External/Shadow Reviewer for CCS 2017, CSF 2020, CCS 2021, POPL 2024

**Teaching:** Reed College Thesis Advisor, 2022-2023; TA for CS 3410 (Computer System Organization and Programming); TA for CS 4120 (Introduction to Compilers)

**Professional Service:** PhD Admissions Volunteer for Cornell, 2019

## Publications and Preprints

---

- **FlowCert: Formal Compiler Validation for Asynchronous Dataflow Programs.** In submission to ASPLOS 2024.  
Zhengyao Lin, Joshua Gancher, and Bryan Parno.

- **Secure Synthesis of Distributed Cryptographic Applications.**  
To appear at CSF 2024.  
Cosku Acay, Joshua Gancher, Rolph Recto, and Andrew Myers.
- **OWL: Compositional Verification of Security Protocols via an Information-Flow Type System.**  
IEEE S&P 2023.  
Joshua Gancher, Sydney Gibson, Pratap Singh, Samvid Dharanikota, and Bryan Parno.
- **A Core Calculus for Equational Proofs of Cryptographic Protocols.**  
POPL 2023.  
Joshua Gancher, Kristina Sojakova, Xiong Fan, Elaine Shi, and Greg Morrisett.
- **Viaduct: An Extensible, Optimizing Compiler for Secure Distributed Programs.**  
PLDI 2021.  
Cosku Acay, Rolph Recto, Joshua Gancher, Andrew Myers, and Elaine Shi.
- **Symbolic Proofs for Lattice-Based Cryptography.**  
CCS 2018.  
Gilles Barthe, Xiong Fan, Joshua Gancher, Benjamin Grégoire, Charlie Jacomme and Elaine Shi.
- **Externally Verifiable Oblivious RAM.**  
PETS 2017.  
Joshua Gancher, Adam Groce, and Alex Ledger.

## Funding

---

- **NSF: SatC: CORE: Small: Automating the End-to-End Verification of Security Protocol Implementations.** 2022.  
Award # 2224279. Award size: \$600,000. PIs: Bryan Parno and Joshua Gancher.  
Advancing the state of the art in modular, highly automated, end-to-end formal proofs for security protocols.

## Invited Talks

---

- IETF 118, November 2023: Owl: New Directions for Security Protocol Analysis
- CyLab Partners Conference 2023: Verifying Security Protocols End-to-End with Owl
- CMU Crypto Seminar, September 2023: Owl: Compositional Verification of Security Protocols
- CMU PoP Seminar, September 2023: Owl: Compositional Verification of Security Protocols
- INRIA Prosecco Seminar, June 2023: Owl: Compositional Verification of Security Protocols
- Boston University POPV Seminar, April 2023: Owl: Compositional Verification of Security Protocols via an Information-Flow Type System
- Galois Tech Talk, March 2023: End-to-End Verification for Security Protocols
- Stanford Software Research Lunch, November 2022: A Core Calculus for Equational Proofs of Cryptographic Protocols
- New England Systems Verification Day 2022: End-to-End Verification for Security Protocols
- PLCrypt Workshop, May 2022: End-to-End Verification for Security Protocols in F\*
- New England Systems Verification Day 2019: IPDL: Proving Compositional Security of Cryptographic Protocols