Joshua Gancher

gancher.dev | j.gancher@northeastern.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.

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.

Appointments

- **Assistant Professor**. Northeastern University. Fall 2024.
- **Postdoctoral Fellow**. Carnegie Mellon University. 2021 - 2024.
  - Advised by Bryan Parno. Research Focus: Type systems for secure cryptographic protocols.

Service

- **Program Committee**, FCS 2020
- **Program Committee**, FC 2023
- **Program Committee**, SPLASH Student Research Competition 2023
- **Program Committee**, SPLASH SRC 2023
- **Organizing Committee**, CMU Secure Blockchain Summit 2024
- **Program Committee**, FCS 2024
- **Program Committee**, CCS 2024
- **Program Committee**, USENIX 2025
- **Program Committee**, USENIX 2025
- **Program Committee**, PriSC 2025
- **Program Committee**, PLDI 2025
- **Program Committee**, PLDI SRC 2025
- **Program Committee**, ProTeCS 2025
- **Program Committee**, FCS 2025

- **Program Committee**, IEE S&P 2026
- **Expert Reviewer**, POPL 2026

Publications and Preprints

- **Concrete Security Bounds for Simulation-Based Proofs of Multi-Party Computation Protocols.** Kristina Sojakova, Mihai Codescu, and Joshua Gancher.
- **ILA: Correctness via Type Checking for Fully Homomorphic Encryption.** ACM CCS 2025. Tarakaram Gollamudi, Anitha Gollamudi, and Joshua Gancher.
- **Vest: Verified, Secure, High-Performance Parsing and Serialization for Rust.** USENIX Security 2025.
  Yi Cai, Pratap Singh, Zhengyao Lin, Jay Bosamiya, Joshua Gancher, Milijana Surbatovich, and Bryan Parno.
- **Towards Practical, End-to-End Formally Verified X.509 Certificate Validators with Verdict.** USENIX Security 2025.
  Zhengyao Lin, Michael McLoughlin, Pratap Singh, Rory Brennan-Jones, Paul Hitchcox, Joshua Gancher, and Bryan Parno.
- **OwlC: Compiling Security Protocols to Verified, Secure, High-Performance Libraries.** USENIX Security 2025.
  Pratap Singh, Joshua Gancher, and Bryan Parno.
- **FlowCert: Formal Compiler Validation for Asynchronous Dataflow Programs.** OOPSLA 2024.
  Zhengyao Lin, Joshua Gancher, and Bryan Parno.
- **Secure Synthesis of Distributed Cryptographic Applications**.
  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.
  Coşku 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.

Selected Talks

- IFIP WG 2.8, May 2025: Verifying Security Protocols with Owl
- BU PoPV + BUSec, December 2024: New Techniques for Secure-by-Construction Cryptography
- 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