New York, NY
elefthei@mit.edu
+1 (267) 968-3532

Lef Ioannidis

elefthei.me
github.com/elefthei
linkedin.com/in/elefthei

Education

Current PhD in Computer Science, *University of Pennsylvania*, Philadelphia, PA
Research: *Programming languages for formally verified cryptographic proof systems.*
Advised by Sebastian Angel & Steve Zdancewic. Graduation in summer 2025.

2015, 2019 BSc, MEng in Computer Science, *Massachusetts Institute of Technology*, Cambridge, MA
Research: *Extracting and optimizing low-level bytecode from high-level verified Coq*, PDOS group.

Employment

Summer '22 Research Scientist Intern, Amazon, Automated Reasoning Group, Arlington, VA
- Contributed in the type system formalization of the Cedar authorization language.
- Implemented a novel type inference algorithm for Cedar including singleton and capability types.

2018 - 2019 Investment Engineer, Bridgewater Associates, Westport, CT
- Created Programming languages for big-data analysis and visualization used by Quantitative Research.
- Implemented risk-controls and hedging algorithms used daily by Trade Generation.
- Taught the Scala programming language to more than 100 traders and engineers.

2016 - 2018 Principal Software Engineer, UnifyID (acquired by Prove), San Francisco, CA
- Designed and implemented the core back-end with more than 30 microservices.
- Implemented a Machine Learning (ML) service for high-throughput inference (3000 req/sec).
- Implemented certificate management and PKI systems for End-to-end encryption.

2015 - 2016 Software Security Engineer, Apple, Cupertino, CA
- Contributor to the LLVM compiler and the Swift programming language.
- Implemented cryptographic protocols for DRM.

Technologies and Languages

Computing: Compilers, Language design, Performance engineering, Formal verification, Cryptography, Smart Contracts, Zero-knowledge proofs, Distributed systems, Cloud security, Microservices.
Languages: Rust, Scala, Haskell, OCaml, Coq, C, C++, Python, Go, Java, Javascript, Elm, SQL.

Patents & Publications

Oct. 2024. "Cedar: A New Language for Expressive, Fast, Safe, and Analyzable Authorization". In: *Proceedings of the ACM on Programming Languages* OOPSLA.

Dec. 2024. "Choice Trees: Representing and reasoning about nondeterministic, recursive, and impure Programs in Coq". In: *Journal of Functional Programming, Special POPL 2025 edition.*

June 2024. "Reef: Fast Succinct Non-Interactive Zero-Knowledge Regex Proofs". In: *33rd USENIX Security Symposium.*

Dec. 2024. "Structural temporal logic for mechanized program verification". In: under submission.

June 2022. "Efficient representation of numerical optimization problems for SNARKs". In: *31st USENIX Security Symposium.*

Mar. 2020. *Privacy-preserving system for machine-learning training data.* US Patent 10,601,786.

Nov. 2019. "Extracting and optimizing formally verified code for systems programming". In: *NASA Formal Methods: 11th International Symposium.*